Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes

Recommendations for Resilient Enforcement, Out-of-Band Judicial Access, and Clean Adjudicative Environments

Jay Lewis Farrow, *Author-Research Coordinator-Senior Editor*

Research, Forensic, and Editorial Contributions by Cyber-N.E.T. Forensics and Associates within the Joint Cyber Defense Collaborative Ecosystem

Editorial and Citation-Review Support Provided by Members of the Florida Barrister Journal Staff

First Publication - September 10, 2026

Initial Peer Review Submission Deadline – October 31, 2026

Table of Contents

Introduction

The Civil Cybercrime Litigation Strategy Targeting Malicious Cyber-Infrastructure

Ordinary civil litigation usually begins with a known dispute and an identifiable defendant. A plaintiff files a complaint, serves the opposing party, develops a factual record, and asks the court to determine liability, award damages, or prohibit future conduct. Civil cybercrime litigation altered that sequence. The human operators may be unknown, outside the country, or concealed behind layers of accounts and infrastructure, while the technical dependencies that keep the operation running - domains, Internet Protocol addresses, hosting accounts, registries, registrars, cloud resources, platform accounts, or command servers - can still be identified and placed within the authority of neutral intermediaries.

The operational breakthrough was to use civil process before attribution was complete. Plaintiffs and technical investigators translated a moving cyber incident into evidence a court could evaluate: sworn declarations described the malicious function, appendices identified the technical objects, and proposed orders told registries, registrars, hosts, data centers, or platforms exactly what state to change. When the court granted emergency authority and the neutral intermediary executed it before the operator could rotate infrastructure, the lawsuit performed a containment function. Waledac, Rustock, Zeus, and Citadel supplied the early forms of that legal-technical method. **[FN 7] [FN 8] [FN 9] [FN 10]**

Civil cybercrime litigation became an operational cybersecurity capability when private plaintiffs and aligned sector organizations learned to convert technical dependencies into enforceable court commands. The early model was not ordinary damages litigation: it identified a command domain, hard-coded IP address, server, account, registry, registrar, host, or provider account; protected the execution window; obtained ex parte or sealed authority; and forced a neutral intermediary to change technical state before an anonymous actor could move. **[FN 7] [FN 8] [FN 9] [FN 10]**

The federal court environment in which that model matured was already electronic by 2010, but it was not yet the same integrated trust surface that exists now. The Judiciary's own materials show remote filing, automatic docket entry, immediate Notice of Electronic Filing service, simultaneous file access, and PACER public retrieval as linked functions; later NextGen identity consolidation, 2025 MFA rollout, HSD practice, 2025 case-management cyberattack disclosures, and 2026 modernization made the filing credential, service list, docket object, sensitive-document path, and public-access record one interdependent operational surface. **[FN 1] [FN 2] [FN 3] [FN 4] [FN 5]**

Contextual Scope and Focus of this Report

This report follows that transformation across thirty-five verified matters spanning approximately sixteen years. It does not treat every action as the same kind of case or reduce success to whether a plaintiff obtained a favorable order. The population includes classic botnet takedowns, nation-state domain portfolios, security-vendor matters, phishing- and

malware-service disruptions, identity and platform cases, fraud-service cases, and modern service-economy actions. Each case is used to identify what the court authorized, what was actually executed, what remained in force after the emergency phase, and whether the remedy could be found and used after the adversary adapted.

The recurring litigation package is best understood as a chain of custody and authority. Counsel and experts investigate privately; technical findings are reduced to declarations and infrastructure schedules; emergency papers are filed under ordinary, sealed, or ex parte procedures; a judge evaluates the requested relief; third parties implement the order; notice and publication follow; and the case later reaches permanent relief, settlement, dismissal, or another procedural endpoint. The same chain that makes the remedy legitimate and reproducible also makes its human, technical, and publication dependencies observable. **[FN 12] [FN 13] [FN 23]**

The thirty-five-case study demonstrates a repeatable legal-technical playbook. Waledac, Rustock, Zeus, Citadel, Barium, Phosphorus, Sophos, DXC, TrickBot, Glupteba, ZLoader, cracked Cobalt Strike, Lumma, RaccoonO365, and the 2024-2026 phishing-, malware-, and fraud-service cases show recurring counsel roles, sworn technical declarations, target appendices, neutral-provider commands, alternative service, public notice pages, and later-successor provisions. **[FN 7] [FN 8] [FN 9] [FN 10] [FN 11] [FN 58]**

That playbook created success and exposure at the same time. The same public filings, notice pages, provider orders, affidavits, counsel biographies, technical experts, repository mirrors, domain registrations, and permanent-injunction mechanisms that make the civil cybercrime legal attack disruptive and effective, also tell an adversary how the remedy is prepared, where it travels, who handles it, when it becomes public, and how future infrastructure will be tested. **[FN 12] [FN 13] [FN 23]**

Evolution of Threat Actor Responses to the Civil Cybercrime Takedown Litigation

The earliest actions often focused on a relatively concrete dependency: a set of command domains, hard-coded addresses, or servers. Modern cybercrime is more modular. One operator may sell phishing kits, another stolen sessions, another disposable virtual desktops, another malware-loading access, and another infrastructure or payment support. Front-end domains can be discarded while customer relationships, cloud roles, tokens, administrative access, and backend service logic survive. The visible object changes, but the commercial and technical capability remains available to the same operator or its customers. **[FN 41] [FN 42] [FN 43] [FN 49] [FN 54] [FN 56]**

That evolution changes the containment problem. A static list may disable what investigators located on the filing date without reaching the accounts, credentials, service panels, automation, or successor infrastructure used to rebuild. The civil remedy therefore moved from a one-time transfer or seizure toward continuing criteria, provider workflows, monitoring, repeated domain actions, and other mechanisms capable of addressing infrastructure discovered after the original order.

Cybercrime evolved into exactly the kind of environment that can exploit that exposure. The modern record now documents access brokers, phishing-as-a-service, malware-as-a-service, ransomware-as-a-service, valid accounts, session cookies, OAuth/device-code abuse, cloud control planes, disposable virtual machines, managed DNS, CDN/reverse-proxy layers, professional-looking personas, and successor infrastructure that can regenerate faster than a static domain list can be frozen. **[FN 41] [FN 42] [FN 43] [FN 49] [FN 54] [FN 56]**

The cAPTure-to-Kill Counter-Disruption Model

cAPTure-to-Kill is used here as a functional model, not as a malware-family label and not as a universal attribution shortcut. The model describes an adversarial objective: gain control over the trusted systems through which legal capacity is exercised, then use that control to degrade or neutralize the investigation, proceeding, evidence path, remedy, publication channel, or later enforcement. Endpoint access may be one component, but the operational surface extends through identity, cloud administration, DNS and mail routing, portal access, filing and service, docket and publication states, professional personas, provider contacts, and successor-remedy visibility. **[FN 27] [FN 28] [FN 29] [FN 30] [FN 31]**

The model is deliberately separated from natural-person attribution. A capability can be mapped at the infrastructure, identity, workflow, and publication levels before every operator, affiliate, customer, access broker, or insider is identified. That distinction permits defensive action at the control-plane level without converting similarity of technique into an unsupported conclusion that one person or one crew caused every event.

The resulting cAPTure-to-Kill model is counter-disruption. It captures or corrupts the trusted control plane through which a civil cyber remedy is prepared, transmitted, docketed, served, publicized, implemented, and enforced. The record supports that finding at the infrastructure, service/backend, identity, access, workflow, and publication-control levels. It does not require the additional endpoint of naming every natural person, affiliate, customer, or insider who used the capability. **[FN 27] [FN 28] [FN 29] [FN 30] [FN 31]**

Microsoft / Fortra / Health-ISAC v. John Does 1-16, No. 1:23-cv-02447, is the apex case. The March 2023 record presented cracked Cobalt Strike as a global malware/ransomware control architecture; the September 8, 2025 order converted preliminary terms into a permanent injunction; the order defined Cobalt Strike domains and IP addresses; appointed or empowered a Court Monitor process; allowed nonparty requests for monitor information tied to related investigations or litigation; and retained jurisdiction until no earlier than January 1, 2030. **[FN 16] [FN 17] [FN 18] [FN 19] [FN 20] [FN 23]**

The post-September 8 visibility record is an empirical result. The defined search through September 7, 2026 located public legal-repository mirrors and docket/document pages for the final order, but located zero independent Microsoft, Fortra, Health-ISAC, Crowell, named-expert, major cyber-media, major legal-media, public social/video, podcast, or conference items explaining the final judgment, the five-year successor mechanism, or later enforcement. In the same defined search universe, the April 2023 launch and 2023-2025 operational-success narrative had substantial public treatment. That contrast is a visibility collapse. **[FN 12] [FN 13] [FN 14] [FN 15] [FN 26]**

A Standing Permanent Injunction and the First Located Later-Victim Field Test

A permanent injunction can operate as more than the final paper entered at the end of a case. When it defines qualifying successor infrastructure, retains jurisdiction, assigns a monitoring function, and permits later requests for information or enforcement, it becomes a standing containment architecture. A later victim who can bring technically qualifying infrastructure into that architecture may be able to use judicial authority already developed through years of litigation rather than reconstructing the remedy from the beginning. **[FN 23] [FN 25]**

The November 2025 application tested that proposition in practice. It asked the issuing court to receive later-discovered infrastructure through a secure technical process, apply the permanent order's successor framework, and coordinate with the plaintiff-side capability that had built the original action. The public record documents the filing and a direction that plaintiffs respond, but the defined search did not locate a public technical determination, monitor process, or reproducible disposition of that later-victim request through the cutoff. **[FN 24] [FN 25] [FN 26]**

The November 18-19, 2025 Rule 24/Rule 71 sequence is the first located later-victim field test of State Four. The filing invoked the permanent injunction, alleged successor infrastructure, requested secure technical review, and sought coordination with Microsoft DCU; the docket materials show a November 19 direction that plaintiffs respond; the searched public record through September 7, 2026 located no technical adjudication of successor criteria, no monitor disclosure proceeding, and no independent public explanation of that attempted use of the five-year mechanism. **[FN 25] [FN 24] [FN 26]**

> **The institutional conclusion is continuity of justice, not blame. When credible evidence materially places filing, service, identity, routing, notice, or record custody in dispute, the integrity evidence cannot be tested by requiring it to travel exclusively through the same disputed channel. A Clean Adjudicative Environment supplies a narrow lawful bridge: independently authenticated intake, source-object preservation, known-clean review, controlled service, technical escalation, dual-channel confirmation, provider authentication, and reconciliation back into ordinary adversarial process. [FN 6] [FN 30] [FN 31] [FN 4]**

Notable Patterns of IoCs/Suppression/Interference Post-2018 and Findings

The report uses indicators and patterns with disciplined limits. An isolated routing change, missing notice, altered page, account event, provider transition, or publication gap may have an ordinary explanation. Evidentiary weight increases when independently preserved events repeat across trust boundaries, align with consequential litigation windows, and correspond to mechanisms documented by separate experts or sworn civil-cyber witnesses. The analysis therefore proceeds from source state to chronology, from chronology to mechanism, and from mechanism to bounded inference rather than beginning with an attribution conclusion.

The same discipline applies to the thirty-five cases. A court order establishes judicial authority; a party announcement or provider statement may establish implementation; a permanent order establishes a legal endpoint; and later public records may establish whether a successor mechanism was used. None of those sources, standing alone, proves every other state. The

report's Four-State framework keeps those questions separate so a visible launch, a technically executed takedown, a permanent legal remedy, and continuing later-victim access are not treated as interchangeable outcomes.

The report's central finding is that the civil cyber-disruption remedy developed from a narrow emergency tactic into a repeatable operational system. The system depends on a sequence of trusted acts: confidential preparation by counsel and experts, restricted filing, judicial authorization, provider implementation, publication or alternative service, final relief, and continuing enforcement. Each act is lawful and necessary in the ordinary case. In a mature adversarial environment, each act is also an observable control point that can be studied, anticipated, and targeted. **[FN 1] [FN 6] [FN 7] [FN 23]**

The thirty-five cases do not merely show that plaintiffs can win temporary restraining orders against anonymous cyber defendants. They show how legal authority is converted into technical state: a registry changes a domain, a hosting provider disables a server, a data center preserves a machine image, a platform suspends accounts, a provider redirects traffic, or a monitor evaluates successor infrastructure. That conversion is the distinctive value of the remedy and the reason it attracts adversarial attention. **[FN 7] [FN 8] [FN 10] [FN 11] [FN 23]**

The Microsoft / Fortra / Health-ISAC action exposes the mature form of the remedy. The March 2023 emergency case targeted cracked Cobalt Strike as a live service infrastructure used for ransomware and post-exploitation access, and the September 2025 permanent order then attempted to preserve remedial force through a five-year successor mechanism. The public record therefore contains both a powerful initial disruption and a later test of whether that disruption remained visible, accessible, and enforceable after final judgment. **[FN 16] [FN 18] [FN 20] [FN 23] [FN 24]**

The absence of independent final-judgment publicity after September 8-9, 2025 is not treated as a rumor, mood, or public-relations footnote. It is an empirical visibility state measured against a defined source universe and a contrary launch-stage baseline. The case had substantial public attention when emergency relief was obtained and later public reporting described an 80 percent reduction in unauthorized Cobalt Strike abuse; yet the defined post-final-order search located no independent Microsoft, Fortra, Health-ISAC, Crowell, named-expert, or major cyber-media explanation of the five-year final judgment or of later enforcement under it. **[FN 13] [FN 14] [FN 15] [FN 23] [FN 26]**

> **Conclusion Summary: Where Threat Actors Target Channels to Civil Cybercrime Remedies, Incident Response Must Adopt Alternative Paths Which Allow Civil Litigants to Obtain Covert, Ultra-Rapid and Effective Containment**

The proposed alternative path is not a general bypass around filing rules, service, adversarial process, or judicial control. It is a narrow integrity bridge for the exceptional matter in which credible technical evidence materially places the ordinary channel itself in dispute. The bridge preserves the original evidence object, authenticates the submitting person and the receiving court function, permits known-clean technical review, controls disclosure and service long enough to prevent irreversible consequences, and then reconciles the verified record back into ordinary process. **[FN 6] [FN 30] [FN 31] [FN 34]**

The Clean Adjudicative Environment follows from that record. The issue is not whether courts should abandon electronic filing or whether every irregular docket event proves compromise. The issue is that cyber-sensitive evidence about compromised filing, service, identity, routing, notice, or record custody cannot be meaningfully tested if the only available path to a judge sends the evidence back through the same trust environment whose integrity is disputed. **[FN 4] [FN 6] [FN 30] [FN 31] [FN 34]**

PART I - The Invention of Civil Cyber-Disruption in a Transitioning Federal Court Environment

The first generation of civil cyber-disruption did not emerge as a separate body of procedural law. It developed by adapting familiar civil remedies to an unfamiliar operational problem: anonymous actors could move faster than conventional litigation, but the infrastructure on which they depended was often controlled by identifiable third parties subject to court process. The cases in this Part trace how plaintiffs learned to convert that mismatch into timed judicial containment.

1.1 The operational idea: an order that changes infrastructure state

A complaint ordinarily asks a court to determine rights between parties. In a cyber-disruption action, the complaint and emergency record also identify a technical dependency that can be changed immediately. The court does not have to operate the server, edit the zone file, suspend the account, or image the machine. It authorizes the registry, registrar, host, data center, platform, or other neutral intermediary that already possesses the technical control necessary to do so.

The anonymous defendant remains a party to the case, but the containment step does not depend on locating that person first. The emergency record must instead establish a sufficiently bounded connection between the identified infrastructure and the alleged unlawful operation, explain the risk of notice or delay, and propose commands that a neutral provider can execute without guessing. The legal instrument and the technical implementation are therefore designed together. **[FN 7] [FN 8] [FN 9] [FN 10]**

The early civil cyber cases translated technical chokepoints into judicially enforceable acts. A registry could disable or transfer domain names; a registrar could lock registration control; a hosting provider could disconnect a server or preserve account records; a data center could allow U.S. Marshals and experts to image equipment; and a court could authorize service methods that reached anonymous defendants through the very infrastructure being restrained. **[FN 7] [FN 8] [FN 9] [FN 10]**

Speed determines whether the remedy can operate before the operator adapts. The remedy worked when the plaintiff identified an operational dependency and obtained authority before the operator could relocate the backend, modify a domain-generation list, change a DNS setting, warn affiliates, burn accounts, or wipe servers. That timing produced the recurring use of ex parte presentation, sealing, delayed notice, alternative service, and provider coordination as components of civil-disruption architecture rather than procedural ornaments. **[FN 7] [FN 8]**

The early model succeeded because it respected the technical structure of the adversary's dependency. A botnet operator does not need a courtroom, a corporate office, or a registered identity to keep operating; the operator needs name resolution, command servers, accounts, routing, credentials, payment paths, or some other control layer that makes infected machines return for instructions. Civil cyber-disruption became meaningful when a plaintiff could show

the court which neutral intermediary controlled that layer and why an order directed to that intermediary would change the adversary's operational state. **[FN 7] [FN 8] [FN 9] [FN 10]**

A civil cyber case can therefore function as both litigation and incident response. The pleading frames claims and jurisdiction, but the remedy functions like a containment action. It freezes or redirects technical control before the actor can burn infrastructure, rotate domains, transfer accounts, or warn affiliates. The cases accordingly combine sworn technical declarations, infrastructure appendices, proposed provider commands, delayed notice, and alternative service. The legal form is civil procedure; the operational function is timed disruption. **[FN 7] [FN 10] [FN 16] [FN 23]**

1.2 The court was already electronic, but the trust environment had not reached today's integration

CM/ECF had already changed federal litigation before the first major private botnet actions. The Administrative Office describes a system in which an attorney's upload can create the docket entry, generate an immediate Notice of Electronic Filing, make the document available to registered participants, and later support public retrieval through PACER. **[FN 1] [FN 2]** That integration removes delay and duplication, but it also means one credentialed event can propagate through several legal and technical states at once.

For ordinary litigation, those states are usually treated as one reliable transaction. A cyber-sensitive reconstruction must preserve them separately: the filer copy, the court's intake object, the chambers or restricted copy, the docket entry, the NEF, each recipient copy, the sealed or redacted version, the public copy, and any repository or archive mirror. RAPS later formalized that distinction. **[FN 30]** When the integrity of the chain is disputed, agreement among those objects must be demonstrated rather than presumed.

Federal electronic filing predates Waledac. The Judiciary reports that bankruptcy CM/ECF implementation began nationally in early 2001, district-court rollout began in May 2002, and appellate implementation began in 2005; attorneys filing over the internet automatically create docket entries, docket sheets update immediately, and a Notice of Electronic Filing is emailed immediately to the filer and registered participants with links to the document and docket. **[FN 1]**

That architecture is efficient because the same event can create the file object, docket entry, notice event, service event, and eventual public access path. It is also the foundation of the modern trust problem. In an attacked environment, the relevant forensic states are no longer one object: the filer copy, intake copy, chambers copy, docket entry, NEF email, recipient copy, sealed copy, public copy, repository copy, and archived copy can become separately material. **[FN 1] [FN 30]**

The stronger historical proposition is therefore not that early cyber-disruption occurred in a non-electronic court system. It is that early operations could still exploit a less socially and technically saturated exposure cycle: fewer automated public mirrors, less consolidated identity, less immediate social-media amplification, less routine remote/cloud counsel collaboration, and less mature adversary attention to the legal mechanism itself. Modern

CM/ECF, PACER, NextGen identity, MFA, sealed-document controls, HSD rules, and public repository ecosystems create a richer but more attackable trust surface. **[FN 1] [FN 3] [FN 4] [FN 5]**

The early court-technology question is therefore more subtle than whether CM/ECF existed. It did. The operational question is how quickly a sealed or emergency filing became a docket object, a notice event, a public index item, or a repository entry visible to the target or to infrastructure watchers. A less socially saturated public-record ecosystem gave early plaintiffs more room to synchronize filing, implementation, unsealing, and notice. A modern filing environment collapses more of those states into a credentialed and networked chain. **[FN 1] [FN 2] [FN 6]**

A cyber adversary does not need to corrupt an entire judiciary system to exploit that chain. The attacker benefits from any reliable observation or influence point: counsel mail before filing, a service list, a sealed-document workflow, an NEF recipient path, a docket-entry state, a publication page, or a provider instruction. The same features that let courts move rapidly - remote filing, immediate notice, indexed public records, mirrored repositories, and cloud-hosted counsel systems - also give the adversary a map of what must be watched or touched to reduce the remedy's practical effect. **[FN 1] [FN 2] [FN 30] [FN 31]**

1.3 Waledac: registry-level disruption

Waledac supplied the clearest early illustration of the model. Microsoft did not need to begin with the physical location of every operator. It identified 277 command domains used by infected machines to reach the botnet, sought emergency judicial authority, and directed the order to the registry layer capable of interrupting name resolution. The later permanent transfer converted a time-sensitive emergency restraint into continuing control over the identified domains. **[FN 7]**

The technical action is simple to describe but consequential in operation. A bot may be installed on thousands of victim machines, yet still depend on a comparatively small set of domain names to locate command infrastructure. Changing the registry state of those names can sever the bot's ordinary return path even while the infected endpoints remain geographically dispersed and the operators remain anonymous. The case established the first recurring grammar of the field: identify the dependency, obtain authority, compel the neutral control point, preserve evidence and notice, and then secure a lasting disposition.

Microsoft Corp. v. John Does 1-27, No. 1:10-cv-00156 (E.D. Va.), filed February 2010, established the domain-registry model. The Waledac operation targeted 277 command domains and used a court order to sever the botnet's name-resolution path before the anonymous operators could adapt. Later permanent transfer converted the emergency disruption into a lasting domain-control remedy. **[FN 7]**

In Waledac, the court order functioned as a technical change request directed at the registry layer. The court did not need to identify every bot herder to change the state of the domains that the malware needed. That pattern - identify dependency, obtain order, compel neutral

control point, preserve notice and due process after the fact - became the first grammar of civil cyber-disruption. **[FN 7]**

Waledac also supplied the first lesson an adversary could learn from the defender. The order showed that a plaintiff did not need to find the operators first; it could identify the command domains and enlist the registry layer. The visibility of that tactic made technical counter-learning predictable, and later operations increasingly used backup lists, domain-generation algorithms, hard-coded IP addresses, dead-drop resolver strings, and service layers capable of surviving the loss of one domain set. **[FN 7] [FN 8] [FN 58]**

1.4 Rustock: when domains are not enough

Rustock exposed the limit of a domain-only strategy. Malware that contains hard-coded IP addresses can continue reaching command infrastructure even after associated domains are disabled. The 2011 operation therefore required coordination at hosting and data-center locations, physical or network access to servers, forensic imaging, disruption of command paths, and preservation of evidence with providers and the U.S. Marshals Service. **[FN 8]**

This broadened the remedy from a change in name resolution to custody over the equipment and network path the malware actually used. Imaging preserved the state of the seized systems for later analysis. Traffic observed after disruption could identify continuing callbacks and support victim notification or further investigation. The case demonstrated that the legal order must reach the adversary's real fallback architecture; a technically elegant command directed to the wrong layer can be legally valid and operationally incomplete.

Microsoft Corp. v. John Does 1-11, No. 2:11-cv-00222 (W.D. Wash.), moved the method from pure domain control to physical and network control. Rustock used hard-coded IP addresses and server infrastructure; the operation required coordinated seizure and forensic imaging at hosting locations, disruption of command paths, and preservation of evidence with U.S. Marshals and providers. **[FN 8]**

Rustock demonstrated a durable lesson: a civil order succeeds only to the extent it reaches the infrastructure level the malware actually uses. A domain seizure does not disable hard-coded IP fallback; a server seizure does not disable all replacement domains; a public headline does not prove the botnet cannot reconnect. This became the foundation for the report's Four-State model. **[FN 8]**

Rustock added a second lesson: the object to be restrained must match the adversary's real fallback architecture. If malware can reach hard-coded IP addresses, then domain transfer does not finish the operation. If the server can be wiped, then imaging and preservation matter as much as disconnection. If infected systems continue to call back after seizure, then the defenders gain telemetry that can support victim notification, attribution, and future disruption. The case therefore widened the civil remedy from domain control to evidence preservation and infrastructure custody. **[FN 8]**

1.5 Zeus and Citadel: enterprise theory and curative sinkholes

Zeus expanded the legal description from one company protecting a product or mark to a coordinated criminal service structure. Microsoft, FS-ISAC, and NACHA used civil RICO and

related theories to describe developers, operators, customers, service providers, money-mule networks, command infrastructure, and victims as components of an association-in-fact enterprise. **[FN 9]** That framing anticipated the later service economy, where the harm is produced by linked roles rather than one server or one operator acting alone.

Citadel then demonstrated that court-authorized disruption could redirect rather than merely disconnect. Registry and registrar commands placed domains under controlled management, and curative servers or sinkholes received traffic that would otherwise have reached the botnet. **[FN 10]** A sinkhole does not simply make a domain unavailable. It changes the destination so defenders can interrupt command traffic, measure continued infection, and support remediation. Judicial authority was thus converted into a defender-controlled technical environment.

The Zeus action added financial-sector plaintiffs and civil RICO. That changed the legal story from one company defending a brand to a criminal enterprise whose developers, operators, service providers, customers, mule networks, and infrastructure nodes functioned together. The action targeted C2 servers and hundreds of domains, and it made the association-in-fact enterprise theory available to later modular-service cases. **[FN 9]**

Citadel scaled the model. Microsoft, industry partners, and law-enforcement support pursued more than a thousand Citadel botnet domains and related C2 infrastructure; the court-authorized remedy included registry/registrar obligations, curative servers, victim notification and permanent transfer. Citadel therefore showed that a civil court could do more than block: it could redirect malicious traffic into a controlled remediation architecture. **[FN 10]**

Zeus and Citadel then moved the remedy from a single-malware story toward an ecosystem story. Civil RICO was not simply a more dramatic pleading label; it allowed the complaint to describe developers, operators, customers, money mules, service providers, command infrastructure, and victims as interdependent components of one criminal enterprise. That logic later became essential in cases against access brokers, PhaaS platforms, infostealers, virtual-desktop services, and refund-fraud networks, because the target was no longer a single machine but the service structure that made many downstream crimes possible. **[FN 9] [FN 10] [FN 49] [FN 54] [FN 56]**

1.6 The historical transition

Taken together, Waledac, Rustock, Zeus, and Citadel form a progression rather than four isolated precedents. Waledac showed that a registry could sever command domains. Rustock showed that hard-coded IPs and physical servers required deeper execution. Zeus supplied an enterprise model for modular participants. Citadel added curative redirection and victim-remediation functions. **[FN 7] [FN 8] [FN 9] [FN 10]**

By 2014, a recognizable operational package had emerged: confidential technical investigation, Doe defendants, emergency filing, sworn declarations, infrastructure schedules, neutral-provider commands, delayed or alternative notice, public explanation after execution, and some form of continuing control or final disposition. The package became reproducible because it worked. Reproducibility also meant that future adversaries could study the timing,

participants, documents, providers, notice pages, and technical assumptions on which the remedy depended.

By 2014, the foundational elements were visible: anonymous Doe defendants, sealed or ex parte emergency relief, sworn technical declarations, infrastructure appendices, neutral-provider implementation, alternative service, public notice after execution, and permanent or curative control of at least part of the infrastructure. The same elements that made the remedy effective also made the remedy reproducible. Reproducibility is useful to defenders; it is also observable to adversaries. **[FN 7] [FN 8] [FN 9] [FN 10]**

By the end of the first formation period, the court-created remedy had a recognizable shape: confidential investigation, emergency filing, technical declaration, neutral-provider command, delayed or alternative notice, and later public explanation. That shape became a playbook because it worked. It also became observable because legitimacy required the materials eventually to be served, published, indexed, or explained. The next phase of the litigation history is therefore not simply more cases; it is the conversion of an innovative emergency method into a repeatable process that defenders and adversaries could both study. **[FN 7] [FN 8] [FN 9] [FN 10]**

PART II - Standardization, Predictability, and the Expanding Electronic Trust Surface

The second period is defined by institutional competence. Courts, major technology companies, outside counsel, technical declarants, registries, registrars, hosts, and platforms became more experienced with emergency cyber relief. That experience reduced the time required to translate technical findings into executable judicial commands. It also made the sequence more predictable to any adversary able to study the public record.

2.1 The defensive playbook becomes visible

Public legitimacy creates unavoidable observability. Emergency papers may begin under seal, but due process, alternative service, unsealing, public notice, permanent-relief practice, and later reporting often expose substantial portions of the method. An adversary does not need access to a judge or an entire court system. It can monitor counsel domains, expert identities, notice pages, provider contacts, docket intervals, public repositories, or the publication cycle surrounding a known plaintiff.

Standardized drafting and implementation remain defensively valuable. Courts receive familiar Rule 65 structures; providers receive commands they can administer; and experts can repeat validated methods. The exposure arises from the same regularity. Once the pathway is known, a mature actor can focus on the handoffs: pre-filing counsel systems, sealed-document access, provider instructions, service lists, publication pages, or later default and permanent-injunction submissions. **[FN 12] [FN 16] [FN 23] [FN 69]**

After the original botnet cases, civil cyber-disruption moved into nation-state domain portfolios, security-vendor attacks, Cobalt Strike beacons, phishing pages, malicious social accounts, reverse proxies, and platform abuse. Barium, Phosphorus, Sophos, DXC, TrickBot, Glupteba and ZLoader use different threat labels, but their litigation architecture recurs: a technical investigation is reduced to a complaint, a compact set of declarations, appendices listing infrastructure, a proposed TRO or preliminary injunction, alternative service, and a post-execution publication path. **[FN 59] [FN 60] [FN 11] [FN 58]**

The standardized package trained courts and providers to act quickly. It also trained adversaries where to look: counsel domains, expert names, public notice websites, repository mirrors, provider instructions, alternative-service pages, docket intervals, and later default-permanent-injunction submissions. A mature adversary does not need to defeat the judge; it can target the trusted steps through which the remedy is built and delivered. **[FN 12] [FN 69] [FN 30]**

Standardization is a success condition and an exposure condition. Plaintiffs reuse forms because courts need a record that is specific, reviewable, and administrable. Counsel reuse pleadings because the Rule 65 showing, third-party commands, alternative-service provisions, and preservation obligations must fit quickly into a familiar structure. Experts reuse methods because malware reverse engineering, controlled infection, passive DNS, provider enrichment, and account-data review are repeatable forensic disciplines. Those efficiencies made civil

disruption scalable. They also made the path to the remedy easier to map. **[FN 16] [FN 17] [FN 18] [FN 20] [FN 23]**

The observable material includes far more than public orders. It includes who signs complaints, which firm handles the emergency application, which expert explains malware configuration, which plaintiff hosts a notice page, which provider receives commands, which repository mirrors the filings, and which final orders include successor language. A threat actor studying the defensive ecosystem does not need omniscience. It needs enough visibility to infer the next chokepoint in the remedy chain. **[FN 12] [FN 13] [FN 24] [FN 26] [FN 69]**

2.2 Counsel, experts, and recurring methods

The human roles are as operational as the technical ones. Plaintiff security teams hold telemetry and product knowledge. Outside counsel determines how that evidence becomes a complaint, declaration set, proposed order, and service plan. Technical declarants explain how samples were collected, how infrastructure was linked to malicious behavior, and which neutral intermediary can change the relevant state. Sector organizations describe downstream harm and urgency. The court relies on the combined record rather than on a threat label alone.

The recurring methods can be stated without specialist shorthand. Investigators may run malware in a controlled environment to observe where it connects; reverse engineer a sample to extract configuration; compare domain and IP history; examine provider or platform records; test accounts or links; trace payments; or compare victim telemetry across incidents. Those methods allow the emergency record to identify a bounded control layer without first resolving every operator's identity. **[FN 18] [FN 19] [FN 20] [FN 63]**

The recurrence of particular counsel and experts is therefore evidence of specialization, not evidence of wrongdoing. Civil cyber-disruption is a technical legal craft. The same teams appear because they know how to translate indicators, product behavior, hosting relationships, registry authority, and victim urgency into an order a judge can evaluate and a provider can execute. That specialization also places their identities, communications, and infrastructure inside the remedy's trust surface. **[FN 17] [FN 18] [FN 19] [FN 20] [FN 69]**

The plaintiffs in the representative population are not ordinary private litigants. Microsoft, Google, Meta, Amazon, Sophos, DXC, Health-ISAC, FS-ISAC, NGO-ISAC and sector partners possess telemetry, abuse desks, incident-response teams, provider relationships, and capacity to convert forensic findings into instructions a registrar or cloud provider can execute. Their outside counsel and technical declarants form the human part of the trusted control plane. **[FN 12] [FN 11] [FN 63] [FN 56]**

The recurring technical methods supply the evidentiary foundation: controlled infection, reverse engineering, beacon configuration extraction, watermark analysis, passive DNS, RDAP/WHOIS review, crawler infrastructure, victim telemetry, account-data review, provider enrichment, controlled purchases, cryptocurrency/payment tracing, and public threat-intelligence comparison. These methods permit a court to act on bounded infrastructure evidence without resolving every natural-person identity at the emergency stage. **[FN 18] [FN 20] [FN 19] [FN 63]**

Recurring counsel and experts are not criticized in this report; their recurrence is evidence of specialization. Civil cyber-disruption is a technical legal craft. The same teams translate IoCs, malware behavior, registries, registrars, hosts, cloud providers, and victim-sector urgency into orders a federal judge can enter and a neutral intermediary can execute. That specialization made the model effective while placing counsel identity, expert communications, and provider handoffs inside the operational surface rather than outside it as background administration. **[FN 17] [FN 18] [FN 19] [FN 20] [FN 69]**

The reports and declarations across the corpus demonstrate a stable methodological core. Analysts isolate malware samples, run controlled infections, parse configuration, identify C2, map domains and IP addresses, test account or platform relationships, and match infrastructure to actor or service behavior. The terminology changes - botnet, RAT, PhaaS, infostealer, cracked tool, gateway, disposable desktop - but the evidentiary grammar remains constant: identify the control layer, explain the method, and direct relief to the entity capable of changing state. **[FN 18] [FN 20] [FN 27] [FN 30]**

2.3 TrickBot: an adaptive botnet case at the transition point

Microsoft Corporation and FS-ISAC, Inc. v. John Does 1-2, No. 1:20-cv-1171 (E.D. Va.), belongs within the historical civil cyber-disruption population because the action sought court-authorized disabling and preservation of live command-and-control infrastructure. Microsoft and FS-ISAC identified IP addresses and service relationships, relied on computer-abuse, copyright, and related theories, and acted during a high-consequence election-period environment. **[FN 11]**

The relief was directed to technical actors capable of changing state. Providers were asked to disable access to identified IP addresses and content, suspend services, prevent new server leasing or use, and preserve relevant records. The action therefore fits the same operational lineage as Waledac, Rustock, Citadel, and later service cases: a sworn technical record was converted into commands to neutral intermediaries before the botnet could exploit its full operational value.

TrickBot also records adaptation pressure. The plaintiffs publicly anticipated revival attempts, and the relief did not assume that one disruption made replacement infrastructure impossible. The case marks the transition from a one-time takedown narrative to an adaptive contest over whether the judicial mechanism can keep pace with regenerated infrastructure. **[FN 11]**

The field and adjudicative-channel materials remain outside this representative population. They do not establish the historical lineage of infrastructure takedown actions; they test whether the remedy remains reachable when the claimant alleges that filing, service, communications, or record channels are themselves implicated. Keeping those functions separate strengthens both analyses. **[FN 11] [FN 37]**

2.4 Four states of operational success

The Four-State model separates events that are often collapsed into the word 'takedown.' State One records Judicial Authority: the relief the court actually authorized. State Two records Technical Execution: the change a registry, registrar, host, provider, platform, or law-

enforcement partner actually implemented. State Three records Durable Remedy: the final or continuing legal mechanism that remained after the emergency window. State Four records Continuing Enforcement and Later-Victim Access: the capacity to reach successor infrastructure and the practical path by which a later victim or investigator can use the remedy. **[FN 7] [FN 8] [FN 10] [FN 23]**

The states can diverge. A court may issue a TRO that is never fully implemented. Providers may execute a large disruption even though the case later ends without permanent relief. A permanent injunction may bind listed domains but contain no process for infrastructure created later. A successor-aware order may exist on a docket but remain difficult for later victims to discover or invoke. The framework prevents those different endpoints from being reported as one undifferentiated success.

The thirty-five cases are assessed under four states. State One is Judicial Authority: what the court authorized. State Two is Technical Execution: what a provider, registry, registrar, host, platform, or law-enforcement partner actually changed. State Three is Durable Remedy: whether the technical effect survived the emergency window through permanent control, curative sinkhole, platform ban, consent decree, final injunction, or comparable continuing restraint. State Four is Continuing Enforcement and Later-Victim Access: whether the remedy can address successor infrastructure and whether a later victim can reach the mechanism. **[FN 7] [FN 8] [FN 10] [FN 23]**

This four-state framework prevents false equivalence. A headline takedown, an unexecuted order, a default judgment without successor terms, an expired TRO, a settlement, and a five-year monitor-assisted mechanism are different operational endpoints. The question is not whether the plaintiff won a press cycle; it is whether malicious function was disabled and whether the remedy remained usable after the actor adapted. **[FN 11] [FN 49] [FN 23]**

The four-state model is the report's guardrail against overstatement. State One asks whether a court authorized relief. State Two asks whether a technical actor actually implemented the relief. State Three asks whether the remedy endured beyond the emergency window. State Four asks whether the remedy remained available against successor infrastructure and later victims. A press release can prove neither State Three nor State Four by itself; a docketed final judgment can prove neither technical execution nor public discoverability by itself. **[FN 23] [FN 24] [FN 26]**

The Four-State model isolates the gaps that adversarial adaptation exploits. An actor may fail to prevent the TRO yet rebuild infrastructure after unsealing. It may lose listed domains yet preserve accounts, tokens, cloud roles, or customer relationships. It may tolerate a final injunction if later victims cannot identify it, invoke it, or get successor infrastructure adjudicated. The civil remedy is strongest when all four states connect without a visibility or access break. **[FN 23] [FN 25] [FN 41] [FN 42]**

PART III - The Service Economy, Identity Pivot, and Successor Infrastructure

The modern cases operate in an environment where cybercrime capability is sold, rented, combined, and replaced. The target may no longer be one malware binary or one command server. It may be the service relationship that supplies access, credentials, phishing pages, virtual machines, loaders, proxying, payment support, or cloud administration to many downstream users. This Part follows the remedy from static objects into that service and identity layer.

3.1 The target changes from one server to a service layer

A service can survive the loss of any one front end. A phishing-as-a-service operator may replace domains and templates; an infostealer marketplace may move distribution pages; a loader may point customers to a new backend; a disposable desktop provider may create new virtual environments; and an IoT or device network may continue supplying residential exit points. The recurring asset is the capability to attach new customers, infrastructure, and victims to the same operational system. **[FN 49] [FN 51] [FN 52] [FN 54] [FN 56]**

Civil relief directed only to the disposable spoke can produce a visible disruption without reaching continuity. The stronger remedy identifies the backbone: the account panel, cloud tenant, registration workflow, reverse-proxy configuration, payment path, developer identity, administrative credential, support channel, or backend logic used to regenerate the outward-facing infrastructure. That shift explains the increasing importance of provider criteria and successor mechanisms.

Modern civil cyber actions no longer focus only on a bot binary or static C2 list. Fake ONNX, Lumma, RaccoonO365, BadBox 2.0, Lighthouse, Darcula, RedVDS, Outsider Enterprise and Amadey-StealC target services that sell access, phishing kits, malware loaders, disposable desktops, stolen credentials, templates, proxying, hosting, device networks, or payment-enabled infrastructure. The technical object is the service economy itself. **[FN 50] [FN 49] [FN 51] [FN 52] [FN 54] [FN 55]**

In this model, the same backend can support many downstream customers. The operator can rotate domains, accounts, hosted pages, Telegram channels, virtual machines, worker scripts, Cloudflare fronts, AWS/Azure resources, and payment addresses without abandoning the underlying service. Effective civil disruption therefore must identify the backbone, not merely the disposable spoke. **[FN 54] [FN 56] [FN 41] [FN 42]**

Modern cybercrime services are designed to survive component loss. A PhaaS operator can rotate domains; a malware loader can redirect traffic to a new backend; an infostealer marketplace can replace distribution pages; a disposable-virtual-desktop vendor can create new customer environments; a botnet can use consumer or IoT devices as residential exit points. The target is no longer simply a named server. It is the service relationship that lets new customers, new domains, and new victims be attached to the same operational skeleton. **[FN 49] [FN 51] [FN 52] [FN 54] [FN 56]**

That shift changed what civil relief must reach. A 2010 remedy could disable hundreds of command domains and immediately injure a botnet. A 2025 remedy must identify which part of the service stack actually controls continuity: the account panel, the domain-registration workflow, the reverse-proxy configuration, the cloud account, the Telegram support channel, the payment trail, the developer identity, or the backend infrastructure used to regenerate front-end lures. **[FN 49] [FN 52] [FN 54] [FN 56]**

3.2 Identity and tokens become infrastructure

In a cloud environment, access may persist after the victim changes a password or replaces an endpoint. A valid session cookie, refresh token, OAuth grant, device-code authorization, service principal, API key, delegated administrator role, or federated trust can continue to tell the platform that the actor is authorized. The service may therefore process an adversarial action as ordinary account activity. **[FN 41] [FN 42] [FN 43] [FN 46]**

In legal workflows, an authorized-looking session can read a sealed working folder, change a mailbox rule, alter a shared link, modify DNS, approve a consent prompt, update a service list, or maintain access to an account that appears remediated. The visible credential may have changed while the more durable authorization remains active. In this setting, identity is not merely the name attached to a communication; it is a control layer capable of changing legal and technical state.

Cloud identity is now infrastructure. A password, session cookie, OAuth grant, device-code token, service principal, API key, mailbox rule, delegated admin role, or federated trust can carry the same operational value that a command server carried in earlier botnet cases: it allows the actor to act through a trusted path while appearing to the service as an authorized user or application. **[FN 41] [FN 42] [FN 43] [FN 46]**

Court and counsel workflows make the identity shift operationally consequential. Sealed filings, provider lists, expert communications, emergency applications, service emails, repository publication, cloud evidence folders, public biographies, and counsel-controlled case pages all depend on accounts and tokens. A compromised identity does not announce itself as a break-in; it produces ordinary-looking state changes through authorized channels. **[FN 31] [FN 30] [FN 45]**

The identity pivot is the bridge between criminal service economy and litigation interference. A stolen password is only the entry point. The more durable asset is the valid session, refresh token, device-code grant, OAuth consent, mailbox rule, service principal, access key, federation setting, or delegated role that permits the actor to act through a trusted platform after the visible credential has changed. The service sees an authorized session; the victim experiences altered mail, files, DNS, notices, or account state. **[FN 41] [FN 42] [FN 43] [FN 46]**

The report therefore treats trusted-channel manipulation as infrastructure, not merely communications noise. A valid cloud session can change a DNS record, create a forwarding rule, read a sealed working folder, alter a shared link, approve a consent prompt, or maintain access to an account that appears remediated. In civil cyber-disruption practice, those acts can expose

an infrastructure appendix, misdirect provider instructions, suppress notice, or make a later enforcement path appear unused. **[FN 41] [FN 42] [FN 45] [FN 69]**

3.3 DNS and cloud control as ordinary-looking change

DNS determines where a domain's users, web traffic, and often mail are directed. Cloud control planes determine who may change records, create aliases, assign roles, expose objects, or authorize applications. A hostile actor using a valid registrar account, provider console, API key, IAM role, service principal, delegated administrator, or mailbox-recovery path can submit a change through the same interface used by an authorized employee. The provider may see a valid administrative instruction even though the organization has lost control of the authority that issued it. **[FN 41] [FN 42] [FN 45]**

For that reason, provider identity is not attribution. AWS, Azure, Cloudflare, Route 53, UltraDNS, WorldNIC, DNSMadeEasy, and other large services support unrelated legitimate customers. The probative object is the customer-specific event: what domain, MX route, certificate, alias, zone, permission, or role changed; when it changed; what credential could perform the change; and whether independent records connect it to a litigation or operational milestone. **[FN 45] [FN 47] [FN 48] [FN 69]**

Large legitimate providers such as AWS, Azure, Cloudflare, Route 53, UltraDNS, WorldNIC and DNSMadeEasy serve many unrelated customers. A provider name alone does not identify an attacker. The probative evidence is the customer-specific event: the domain, mailbox route, certificate, cloud alias, service principal, registrar state, or DNS record that changed; the authority capable of making the change; the timing; the surrounding communications; and independent corroboration. **[FN 45] [FN 48] [FN 69]**

AWS Route 53 documentation shows that DNS changes can be submitted as transactional API batches, and IAM documentation treats access keys and roles as customer-side authority. That architecture is legitimate. In a compromise case, it also explains how a threat actor with valid credentials can create a change that looks administratively normal while redirecting mail, web, service, or publication paths. **[FN 45]**

A legitimate administrative change and a hostile administrative change can look identical at the provider layer. Route 53, Azure DNS, Cloudflare, UltraDNS, WorldNIC and DNSMadeEasy are ordinary enterprise services. Their presence proves neither attack nor innocence. The probative question is customer-state: who or what changed the zone, mailbox, certificate, service alias, object permission, or publication path; when the change occurred; what credential or API could perform it; and whether the change aligns with a litigation milestone or independent expert rail. **[FN 45] [FN 47] [FN 48] [FN 69]**

The subject-side expert reports place that distinction in a synchronized evidentiary setting. CNF treated DNS/MX changes as part of a broader synchronized event pattern, not as standalone provider labels. CCDG explained how cryptographic mail alignment can coexist with operational counterfeiting when the authorized path itself is controlled. RAPS separated the filed object, intake object, docket entry, NEF/service event, recipient copy, and public copy. Together those findings show how an adversary using legitimate access can produce a legally

significant change that appears, from the outside, to be normal administration. **[FN 27] [FN 30] [FN 31] [FN 45]**

3.4 Service-economy cases as external mechanism corroboration

The modern civil cases give source-native examples of the mechanisms rather than proof of a particular field actor. RaccoonO365 describes adversary-in-the-middle phishing and session theft directed at Microsoft 365 identities. RedVDS describes disposable virtual desktops offered as an enabling service. Lumma and Amadey-StealC describe infostealer and loader infrastructure that supplies credentials or access for later compromise. BadBox describes a large distributed device network used for monetized abuse. **[FN 49] [FN 51] [FN 54] [FN 56] [FN 91]**

These records establish that valid-account use, token persistence, reverse proxies, disposable infrastructure, managed domains, cloud workflows, and successor systems are ordinary components of the current civil-disruption universe. They do not establish that the same natural person operated every service or caused any separate field event. Their evidentiary role is mechanism corroboration: they show that the capability classes identified by the independent expert rails are concrete, repeatable, and sufficiently specific to support federal litigation.

RaccoonO365 supplies the identity-centric civil comparator: phishing-as-a-service is designed not only to capture credentials, but to pass through or around MFA by taking session material or operating inside valid cloud workflows. RedVDS supplies the disposable-infrastructure comparator: a cheap virtual desktop can become a throwaway origin for fraud, access attempts or phishing. Lumma and Amadey-StealC supply the infostealer/loader comparator: stolen credentials and loader access become upstream fuel for later intrusion. **[FN 56] [FN 54] [FN 49]**

These cases do not prove a specific subject-side actor by themselves. They prove that the mechanisms identified by the expert rails are no longer exotic. Valid-account access, cloud control, token persistence, DNS/API change, remote mail control, synthetic identity, and successor infrastructure are now common operational components in the same civil-disruption universe. **[FN 41] [FN 42] [FN 43] [FN 31]**

The modern cases function as external mechanism corroboration because they show the same architecture in source-native litigation records. Lumma concerns infostealer distribution and successor-risk at scale. RaccoonO365 concerns identity-centric phishing, adversary-in-the-middle proxying, session-cookie theft, Telegram and payment infrastructure, and cloud-facing credential exploitation. RedVDS concerns disposable virtual-desktop infrastructure offered as an enabling service. BadBox and related cases show large, distributed device networks and monetized platform abuse. Each case confirms that current adversaries preserve capability by operating services, not merely servers. **[FN 49] [FN 51] [FN 54] [FN 56]**

The report treats professional identity in this part as a trust-surface issue, not as a standalone accusation. The RaccoonO365 public record connects a modern Microsoft/Health-ISAC civil disruption to identity theft, AiTM proxying, session abuse, and recurring plaintiff-counsel

infrastructure. Avatar separately examines professional-persona provenance and credential-backed appearance as a capability category. The evidentiary point is that professional identity can become part of the control plane in a service economy; the report does not use that point to infer a natural-person attribution endpoint beyond the verified record. **[FN 33] [FN 56] [FN 69]**

3.5 Advanced Persistent Threats and the cAPTure-to-Kill Counter-Disruption Model

An Advanced Persistent Threat is defined by sustained capability and mission effect rather than by a particular malware name. NIST describes a sophisticated, well-resourced adversary that uses multiple attack vectors, establishes and extends footholds, pursues objectives over time, adapts to resistance, and may seek to undermine or impede a critical mission, program, or organization. **[FN 76]** A ransomware note is therefore not required. Persistence may be expressed through identity, administrative authority, trusted software, cloud control, or repeated return through another channel.

Accepted public incidents demonstrate the control-plane principle. In SolarWinds, a trusted software-update path distributed compromised code broadly before selected follow-on targets were exploited. **[FN 77]** In Storm-0558, Microsoft reported that an acquired signing key was used to forge authentication tokens and reach cloud email in approximately twenty-five organizations, including government organizations. **[FN 78]** The common operational lesson is that control of a trusted distribution or identity layer can provide greater reach than attacking each endpoint independently.

The cAPTure-to-Kill model applies that principle to the civil cyber-remedy chain. Ransomware-as-a-service, malware-as-a-service, phishing-as-a-service, infostealers, access brokers, or disposable infrastructure may supply components. The defining objective is counter-disruption: impair the ability to investigate malicious infrastructure, preserve the evidence, place it before a court, convert the order into provider commands, publicize the remedy to victims, or enforce it against successor systems. **[FN 27] [FN 30] [FN 31]**

The model appears as a sequence of control opportunities. A valid identity or session permits activity through an authorized account. DNS, MX, cloud-role, or API control can redirect web, mail, or publication paths. A controlled mailbox or relay can produce a communication that passes ordinary authentication while misrepresenting human or workflow intent. Portal or routing access can separate what the filer submits from what intake, chambers, the docket, service recipients, and the public later receive. Publication suppression can leave a valid order difficult to find. Professional-persona control can make a credential-backed identity appear routine inside the same workflow. Each function is tied in the report to a separate expert rail or sworn comparator. **[FN 27] [FN 29] [FN 30] [FN 31] [FN 32] [FN 33]**

An Advanced Persistent Threat is not defined by a particular malware family. NIST defines the category around capability and behavior: a sophisticated, well-resourced adversary creates opportunities through multiple attack vectors, establishes and extends footholds, pursues an objective repeatedly over an extended period, adapts to defensive resistance, and maintains the interaction needed to complete the mission. The mission can be exfiltration, but NIST expressly includes undermining or impeding a critical mission, program, or organization and

positioning the actor to do so later. Persistence, adaptation, privileged access, and mission effect are therefore more important to the classification than whether a ransomware note ever appears. **[FN 76]**

Accepted public incidents illustrate that functional definition. In SolarWinds, a trusted software-update path was converted into an access mechanism: the compromised Orion update was distributed to approximately 18,000 customers, after which selected federal and private-sector targets were subjected to follow-on exploitation. Storm-0558 later demonstrated the same principle at the identity layer: Microsoft reported that a China-based actor acquired a signing key and used forged authentication tokens to reach cloud email in approximately twenty-five organizations, including government organizations. These incidents are different in origin and objective, but both show the defining APT move: do not fight every endpoint independently when control of a trusted distribution, identity, or administrative layer lets the actor operate inside ordinary trust. **[FN 77] [FN 78]**

The federal judiciary itself became a publicly acknowledged example of that attack-surface problem. On August 7, 2025, the Administrative Office of the U.S. Courts announced strengthened measures in response to escalated cyberattacks of a sophisticated and persistent nature against the Judiciary's case-management system. Reuters and Politico reporting surrounding the disclosure described a breach affecting the federal electronic filing environment and heightened concern over sealed or otherwise sensitive case information. Court filing, sealed-document custody, account identity, docket state, and notice are therefore documented cyber targets rather than theoretical ones. By August 2025, the Judiciary publicly treated the case-management environment itself as a high-value, persistently attacked system. **[FN 4] [FN 79]**

That history supplies the functional bridge to cAPTure-to-Kill. Ransomware-as-a-Service (RaaS) seeks leverage through encryption or extortion; malware-as-a-service supplies malicious code or access; phishing-as-a-service industrializes credential capture; infostealers harvest secrets; access brokers sell footholds. Any of those services can appear inside a cAPTure-to-Kill operation, but none defines it. The distinctive objective is counter-disruption: neutralize the legal and technical capacity by which malicious infrastructure can be investigated, presented to a court, converted into provider commands, publicized to victims, and enforced against successor systems. The target is not only the victim's data. It is the trusted control plane that permits the victim, counsel, expert, provider, clerk, judge, repository, and later investigator to act on that data. **[FN 27] [FN 30] [FN 31]**

Functionally, the model appears as a sequence of control opportunities. Identity or session capture permits the actor to operate through a valid account. DNS, MX, registrar, cloud-role, or API control can redirect web, mail, or publication paths while the provider sees an authorized change. Authenticated-counterfeit communications can pass technical controls when the authorized mailbox, relay, signing path, or DNS state is already controlled. Portal or routing capture can alter what a filer submits, what intake receives, what a service list contains, or what a recipient sees. Document-state divergence can separate the filer copy, intake copy, chambers copy, docket object, Notice of Electronic Filing, served copy, public copy, and repository mirror. Publication or indexing suppression can leave a remedy legally valid but operationally difficult

for later victims to find. Persona deployment can make a credential-backed professional identity appear ordinary inside the same workflow. These are not abstract possibilities in the report; each function is tied to a separate expert rail or sworn civil-cyber comparator. **[FN 27] [FN 29] [FN 30] [FN 31] [FN 32] [FN 33]**

Marlin Technologies December 5, 2024 Expert Report supplied the earliest independent technical floor. Its December 5, 2024 engagement examined court materials and screenshots, more than 220 ICANN/domain records, two computer devices, and domain-email-server records, and cross-checked the domain material against open sources. Marlin reported a progression of unauthorized permissions and administrative control affecting the law-firm environment, DNS, cloud storage, credentials, and communications, and separately explained how DNS or credential control could support domain cloning, mail interception, suppression, and man-in-the-middle effects. The later cAPTure model did not exist when Marlin performed that work; its contribution was to establish that the field chronology had an independently examined access-and-control substrate before the later litigation overlay was built. **[FN 28] [FN 80]**

Team B then added three structured portal datasets rather than another narrative opinion: the Florida Bar Employee Portal, Florida Bar Membership Portal, and MyFLCourtAccess/e-filing portal. Those datasets preserve identity, URL, date, account and access-related fields that can be compared against DNS/MX changes, communications, filing events, and case milestones. Their value is separation of trust boundaries. Staff identity, professional-membership identity, and filing/service identity are different systems; correlated anomalies across them cannot be collapsed into one portal error. The datasets also identify the evidentiary next step with precision: access telemetry, administrative-change history, device/session records, and backend logs can confirm who exercised the observed privileges and when. **[FN 29] [FN 82]**

The October 22 CNF report converted those separate observations into the first mature integrated model. CNF examined endpoint artifacts, RMM and credential evidence, DNS/MX and registrar state, law-firm and court-adjacent infrastructure, synchronized timing windows, portal events, and independent civil cyber-disruption comparators. It used compartmentalized or blind collection where possible before overlaying the external cases. The civil cases were not used to invent the endpoint or portal artifacts; they supplied an external grammar for capabilities already observed: command and control, valid credentials, infrastructure rotation, provider dependence, law-firm trust boundaries, and successor systems. That collection sequence moved the analysis from isolated compromise to adversarial control of a legal-technical workflow. **[FN 27] [FN 75]**

The January and February 2026 rails then tested different layers of that integrated model. Sinkhole examined registrar and DNS disabling/redirection and successor behavior. Avatar examined professional-persona provenance and credential-backed appearance; this report uses that rail only as a bounded identity-control capability and does not build a standalone natural-person anomaly from unresolved provenance. RAPS reconstructed court objects, dockets, clerk notices, physical-file copies, CM/ECF/DCN/SMTP paths, sender-authentication fields, and DNS/MX history to separate filing, intake, docket, service, recipient, and public states. CCDG independently examined more than fifty-seven judicial e-communication

metadata items plus endpoint and portal evidence and explained the distinction between a cryptographically valid path and an authentic human/workflow event. The Federal Court Audit then adds source-native docket, PageID, replacement, service, assignment, and document-state artifacts. The rails are valuable because they examine different objects by different methods and converge on the same control-plane question. **[FN 32] [FN 33] [FN 30] [FN 31] [FN 34] [FN 81] [FN 82]**

The sworn civil-cyber record supplies external mechanism corroboration. Microsoft, Fortra, Health-ISAC, Google, Sophos, DXC and other declarants describe controlled infection, beacon and watermark analysis, command infrastructure, reverse proxies, access brokers, phishing services, stolen credentials, platform telemetry, provider commands, future domains and successor infrastructure. In 23-cv-2447, for example, the court received sample-scale Cobalt Strike analysis, configuration and watermark evidence, provider-control evidence, product-authentication evidence, and sector-harm evidence from different declarants. Those witnesses do not prove the field events by association. They establish that the same classes of capability are sufficiently real, repeatable, and technically specific to support emergency and permanent federal court relief. **[FN 17] [FN 18] [FN 19] [FN 20] [FN 21] [FN 22] [FN 89] [FN 90]**

The functional definition is therefore earned by the record. cAPTure-to-Kill is an adversarial counter-disruption APT model in which threat actors use trusted control planes - identity and session tokens, DNS/MX and cloud administration, portal access, e-service and filing intake, docket/publication systems, and professional personas - to capture, corrupt, delay, suppress, or redirect the legal and technical channels that allow a civil cybercrime remedy to be prepared, adjudicated, implemented, publicized, and enforced. Data theft, malware, phishing, or ransom can be components. The distinctive object is neutralization of the proceeding, remedy, claimant capacity, evidence path, case visibility, or later-victim enforcement channel. Part IV therefore asks the necessary next question: once civil cyber-disruption succeeds at the emergency stage, how often does the remedy survive, remain visible, and remain usable after the adversary has time to adapt? **[FN 27] [FN 30] [FN 31] [FN 23]**

PART IV - What Happened After the Takedown? The Thirty-Five-Case Outcome, Durable-Remedy, Enforcement, and Visibility Study

Emergency cyber litigation is designed to move before the adversary can react, but the emergency order is only the beginning of the legal lifecycle. A temporary restraining order can preserve the status quo or prevent immediate harm for a short period. A preliminary injunction can maintain restrictions while the case proceeds on a more developed record. If anonymous defendants do not appear after authorized service, the case may move through default and default-judgment procedures rather than a contested trial. A permanent injunction, consent decree, settlement, dismissal, or unresolved preliminary posture then supplies the located procedural endpoint.

Those procedural stages do not answer the technical question by themselves. A TRO may produce substantial containment but expire without a permanent mechanism. A permanent injunction may be legally final yet reach only objects listed years earlier. A final judgment may preserve transfer authority, a sinkhole, provider obligations, monitoring, future-domain criteria, retained jurisdiction, or a later-victim path - or it may contain none of those features. Part IV therefore reconstructs both the case's legal endpoint and the continuing operational state of the remedy.

4.1 The population-level result

The thirty-five-case population is the empirical backbone because it prevents the report from drawing a system-level conclusion from one unusual case. The matters span different plaintiffs, courts, technical targets, legal theories, service models, and procedural outcomes. The field and adjudicative-channel records are excluded from the population because they perform another analytical function: they test access to the remedy rather than represent the historical lineage of infrastructure-disruption actions. **[FN 11] [FN 37]**

Across the population, the strongest conclusion is separation rather than a single success rate. Most cases reached judicial authority. Many produced an executed technical change. A smaller set reached a permanent or comparable durable legal state. Fewer still created a clear process for infrastructure discovered later or for a later victim seeking to use the remedy. The distribution reflects the evolution of the field from listed-object takedowns toward successor-aware containment.

The thirty-five-case population is the empirical backbone of this report. It includes classic botnet takedowns, nation-state domain-portfolio actions, malware-service and phishing-service disruptions, platform and identity cases, fraud-service cases, and TrickBot as a representative botnet action. The field and adjudicative-channel materials are deliberately excluded because they test access to the remedy rather than represent the historical lineage of civil cybercrime infrastructure actions. **[FN 11] [FN 37]**

The population establishes that civil cyber-disruption is real and often powerful. It also establishes that Judicial Authority, Technical Execution, Durable Remedy and Continuing Enforcement are separate outcomes. Most studied cases reached State One. Many reached State

Two. Fewer created durable or successor-aware mechanisms. The most institutionally significant cases are those that made State Four possible because modern adversaries regenerate infrastructure and later victims must be able to reach the remedy without reinventing the entire action. **[FN 7] [FN 10] [FN 58] [FN 23]**

The population also shows that civil disruption evolves by inheritance. Waledac taught domain control; Rustock taught physical and IP-level seizure; Zeus and Citadel taught enterprise architecture and curative sinkholing; Barium and Phosphorus taught portfolio disruption against nation-state tradecraft; TrickBot and ZLoader taught botnet and DGA continuity; cracked Cobalt Strike taught court-supervised successor infrastructure; RaccoonO365, Lumma and the 2024-2026 cases teach identity and service-layer continuity. That is the historical spine of the report. **[FN 7] [FN 8] [FN 9] [FN 10] [FN 11] [FN 23] [FN 56]**

The representative cases are not included to overwhelm the reader. They are included because a one-case argument would be fragile. A single case can be an anomaly. Thirty-five cases across sixteen years show a legal-technical system with recurrent actors, recurrent methods, recurrent relief, recurrent public visibility, recurrent final-disposition gaps, and increasingly complex successor infrastructure. The pattern is the evidence. **[FN 7] [FN 10] [FN 23] [FN 26]**

4.2 Outcome coding

The table organizes the population by the type of threat and remedy rather than by the publicity surrounding a case. Formation cases establish the original registry, server, enterprise, and sinkhole models. Persistent-threat portfolio cases extend relief to recurring domains and profiles. Security-vendor and botnet-service cases make expert methods and permanent-relief practice visible. Modern service-economy cases move the target into identities, accounts, tokens, cloud paths, and disposable infrastructure. Platform and fraud comparators show how the same civil tools operate outside a classic botnet seizure.

Category	Cases	Longitudinal finding
Formation cases	Waledac, Rustock, Zeus, Citadel	Judicial authority and technical execution are strong; durable domain/server/sinkhole remedies appear in Waledac, Rustock and Citadel; State Four was limited because successor/later-victim mechanisms remained immature.
Persistent-threat portfolio cases	Barium, Phosphorus, Bohrium, Star Blizzard	The remedy expanded from single botnets to domain/profile portfolios and repeat-action monitor models; state-four value increased where the court process anticipated later domains.
Security-vendor and botnet-service cases	Sophos, DXC, TrickBot, Glupteba, ZLoader, cracked Cobalt Strike	These cases made method, declarant roles, provider instructions, and default/permanent phases visible; cracked Cobalt Strike created the strongest final successor mechanism located in the population.
Modern service-economy cases	Fake ONNX, Lumma, BadBox, Lighthouse, Darcula, RedVDS, Outsider, Amadey-StealC, RaccoonO365	The technical target became service infrastructure, accounts, tokens, disposable environments, managed domains, and cloud/identity paths; continuing enforcement depends on criteria and provider workflows rather than static lists.

Category	Cases	Longitudinal finding
Platform/identity/fraud comparators	NSO, CryptBot, Fake Bard, Google crypto apps, Meta phishing/Voyager/OneAudience/Brand Total, Amazon REKK/KDP, Palumbo	These cases show how civil relief is applied to platform accounts, spyware, scraping, malicious SDKs, browser extensions, fraud-as-a-service, publishing impersonation and robocall gateways; not every case is a botnet, but each tests a trusted-service abuse model.

The categories are analytical, not jurisdictional labels. A case may contribute to more than one development, but it is placed where its principal operational contribution is most visible. The detailed case packets and aftermath register preserve the case-specific record; the narrative uses the grouped result to show the historical transition without forcing unlike dispositions into one percentage. **[FN 92]**

4.3 Visibility as an outcome, not a public-relations detail

Visibility performs several defensive functions. A public notice can serve anonymous defendants, advise providers that an order exists, warn victims, support remediation, deter customers or affiliates, and allow later investigators or courts to locate a standing remedy. The same disclosure can also teach adversaries what evidence was collected, which providers responded, who prepared the case, and when successor infrastructure may be tested. Visibility must therefore be measured by stage and audience rather than treated as uniformly beneficial or harmful.

Launch publicity and final-remedy visibility answer different questions. The launch explains that an operation occurred and that identified infrastructure was disrupted. Final-remedy explanation tells a later victim or provider whether the relief survived the emergency phase, whether jurisdiction continues, whether future objects can qualify, who evaluates them, and how the mechanism can be invoked. A final order may remain legally available in a repository while its operational use is invisible to anyone who does not already know the caption or docket number. **[FN 23] [FN 25] [FN 26]**

Visibility is operational. Publicity can deter users and providers from assisting the actor, warn victims, drive remediation, and signal that a remedy can be reused. Visibility can also inform the adversary which methods were exposed. The report therefore separates launch publicity, unsealing publicity, final-relief publicity, postjudgment enforcement visibility, and later-victim access. **[FN 26]**

The population shows a common pattern: plaintiffs often publicize the initial disruption, while final disposition is less consistently publicized. That pattern becomes abnormal when the final order is itself more operationally significant than the launch announcement. The cracked-Cobalt-Strike final order is that abnormal case because it created a five-year successor mechanism with Court Monitor architecture and a nonparty request path. **[FN 13] [FN 14] [FN 23]**

Visibility has two audiences. The first is defensive: victims, providers, investigators, other courts, and later claimants need to know what remedy exists and how it can be used. The second is adversarial: operators, affiliates, service customers, access brokers, and infrastructure sellers can study the filing package to learn which dependencies were exposed.

A mature remedy must therefore manage visibility, not simply maximize or minimize it. **[FN 12] [FN 13] [FN 26]**

Launch publicity and final-order publicity serve different operational functions. Launch publicity tells the world that the plaintiff acted and that some infrastructure was disrupted. Final-order publicity tells victims and providers whether the remedy survived default, whether jurisdiction continues, whether successor infrastructure can be reached, and whether a later nonparty has a path to the court or monitor. When the final order is more operationally consequential than the initial announcement but receives less public explanation, the remedy's practical value is reduced even though the legal instrument remains valid. **[FN 23] [FN 25] [FN 26]**

4.4 The report's empirical use of zero-result searches

A zero-result search is treated as a bounded measurement, not as proof that nothing exists anywhere. The search protocol defines the relevant source classes - party and counsel sites, notice pages, court and legal repositories, cyber and legal press, public social, video, podcast and conference sources, and archives - and records whether those sources produced a responsive final-order or enforcement item through the cutoff. **[FN 26]**

The evidentiary weight comes from comparison. A source class that actively explained the emergency action, unsealing, technical success, or operational metrics establishes a visible baseline. If the same source environment produces no explanation when the more durable final mechanism is entered or later invoked, the report records a change in the remedy's public lifecycle. The finding remains limited to the searched public channels and does not become an assertion about sealed, private, or otherwise nonpublic activity.

A defined negative search is evidence of visibility state. It is not an unbounded claim that no document exists anywhere. For each material case, the compendium records the searched categories: party site, counsel site, notice page, court repository, legal repository, cyber press, legal press, public social/video/podcast sources, and archive. Where the search located zero responsive final-order or enforcement items, that result is reported as a visibility finding. **[FN 26]**

The defined-search method tests whether a remedy remains accessible in practice. A remedy that exists in a docket but is not explained by the parties, not updated on the original notice page, not visible in cyber/legal media, not discussed by counsel or experts, and not accessible to later victims loses practical defensive value even while it remains legally valid. **[FN 23] [FN 25] [FN 26]**

The zero-result method is therefore affirmative measurement. The defined search does not claim metaphysical absence. It records that the searched public channels did not produce a responsive final-judgment, enforcement, or Rule 71 explanation through the cutoff. That result is then interpreted in context: earlier publicity, case importance, final-order scope, successor-remedy design, later-victim attempt, and public treatment of comparable cases. **[FN 15] [FN 23] [FN 26]**

The measured absence is strongest when a source category had previously been active. If Microsoft, Health-ISAC, Fortra, cyber media, legal repositories, counsel pages, and public notice mechanisms previously explained the emergency operation and later operational success metrics, their silence after entry of the most durable judicial remedy is part of the remedy's observable lifecycle. The report treats that lifecycle as a technical outcome because visibility affects whether State Four can function. **[FN 13] [FN 14] [FN 15] [FN 26]**

4.5 State Three: final disposition and durable-remedy reconstruction

State Three records the case's located legal endpoint and asks what continuing cyber-disruption authority survived the emergency window. The distinction begins with the ordinary progression of injunctive relief. A temporary restraining order is short-duration emergency relief intended to prevent immediate harm or preserve the status quo while the court can develop the record. In a cyber case, the TRO may authorize domains to be locked or transferred, servers to be disabled or preserved, accounts to be suspended, or traffic to be redirected before the anonymous operator receives ordinary notice and moves the infrastructure.

A preliminary injunction can maintain those restrictions while the action proceeds on a more developed record. It is still interim relief. The plaintiff may continue service efforts, conduct limited discovery, document execution, address objections, and seek default or other final relief. Anonymous Doe defendants often never appear. In that circumstance, the case may proceed through authorized alternative service, clerk's default, and default-judgment practice rather than a contested merits trial. The court must still determine whether the pleaded claims, sworn evidence, notice process, and requested injunction support entry of final relief.

A permanent injunction is the final injunctive instrument entered after the court reaches the procedural and legal basis for a lasting order. A consent decree or settlement can create another continuing restraint. A voluntary dismissal may terminate the action without a durable infrastructure mechanism. Some cases remain at the TRO, preliminary-injunction, or pending-default stage through the cutoff. 'Final disposition' therefore means the terminal or current procedural state actually located in the record - not a conclusion that the cyber operation was permanently neutralized.

The technical effect must be measured separately. A permanent order that transfers known domains or permanently bans specified accounts may create strong control over the objects already identified. It may still be unable to reach new domains, replacement servers, refreshed tokens, new customer environments, or a rebuilt service backend. A more durable architecture defines future objects by function, preserves provider obligations, predicts or captures generated domains, maintains a sinkhole, assigns a monitor, retains jurisdiction, or supplies a later-victim enforcement path. The phrase 'durable operational suppression' is used only for that continuing technical effect; it is not a synonym for final judgment.

The refreshed case packets and Appendix B identify the procedural endpoint located through September 7, 2026. Waledac reached permanent domain transfer. **[FN 7]** Citadel reached default judgment and a permanent injunction supporting continuing domain and curative-server control. **[FN 10]** Phosphorus reached a permanent-injunction phase after seizure or control of ninety-nine sites. **[FN 60]** Bohrium reached default judgment and permanent

injunction on January 30, 2024. **[FN 85]** Star Blizzard reached default judgment and permanent injunction on August 5, 2026. **[FN 84]** These are durable legal states, not merely announcements that emergency action occurred.

The modern service and platform cases present a more varied record. CryptBot, the Google crypto-app matter, Darcula, RedVDS, the KDP impersonation case, Voyager Labs, OneAudience, Palumbo, and other located matters reached permanent, consent, settlement, or default end states. **[FN 53]** **[FN 54]** **[FN 61]** **[FN 63]** **[FN 65]** **[FN 66]** **[FN 67]** **[FN 68]** Apple v. NSO was voluntarily dismissed, so the action did not mature into a durable civil-disruption mechanism. **[FN 61]** BrandTotal ended through settlement and dismissal. **[FN 66]** Other matters remained at TRO, preliminary-injunction, default-motion, or unresolved stages.

RaccoonO365 illustrates the need for precise coding. The located public record reflects sealed TROs, a September 24, 2025 preliminary injunction, and a later request for default or default judgment. No entered final judgment was located through September 7, 2026. Its State Three is therefore unresolved at the cutoff. The report does not treat substantial launch activity, a preliminary injunction, or a pending default request as an entered permanent remedy. **[FN 56]** **[FN 87]**

Glupteba demonstrates the separation between a final procedural state and durable operational suppression. The correct federal action is Google LLC v. Dmitry Starovikov et al., No. 1:21-cv-10260 (S.D.N.Y.). The record includes default and sanctions proceedings after the initial disruption, while Google and public technical reporting documented operator rebuilding and blockchain-assisted fallback. **[FN 86]** The court's authority and the legal proceedings were real; the operator's regeneration path was also real. Final relief and continuing technical effect therefore must be measured as separate states.

The population result is concentrated rather than binary. Some cases permanently transfer known objects. Some impose account or platform bans. Some preserve sinkholes, monitors, future-domain logic, or successor criteria. Some resolve named commercial defendants through settlement. Some terminate without a continuing infrastructure remedy. Several modern service-economy actions remained preliminary or pending at the cutoff. Appendix B preserves the case-by-case details; the body states the resulting pattern so the reader does not have to translate unlike procedural endpoints into a single success percentage. **[FN 92]**

4.6 State Four: continuing enforcement, adversarial adaptation, and public visibility

State Four begins after the court and providers have acted on the original infrastructure. The operational question is whether the remedy can follow the adversary into what appears next. That may require predicted domain-generation logic, repeated domain proceedings, technical criteria for future objects, a monitor, retained jurisdiction, a provider-facing workflow, or a defined path by which a later victim can submit qualifying evidence.

Later-victim access is not an abstract procedural benefit. Modern operators sell or reuse infrastructure across campaigns, and a victim encountering successor systems may possess evidence developed outside the original plaintiff group. A standing order has reduced defensive value if the later victim cannot identify the remedy, determine what evidence is

required, locate the responsible technical or judicial function, and obtain a reviewable disposition. The September 2025 cracked-Cobalt-Strike order contains the strongest located architecture because it combines successor criteria, a Court Monitor, retained jurisdiction into 2030, and an express route for party or nonparty requests. **[FN 23]**

State Four asks a harder question than whether a permanent injunction exists: after the listed infrastructure changes, can the remedy reach what appears next, and can a later victim or investigator find and use that path? The early formation cases had strong State Three effects but comparatively weak explicit later-victim architecture. Barium, Phosphorus and ZLoader moved closer to successor-aware relief by using continuing processes, repeated domain actions, or DGA/future-domain logic. The September 2025 cracked-Cobalt-Strike order is the apex located architecture because it combines defined successor criteria, a Court Monitor, retained jurisdiction into 2030, and an express route for party or nonparty requests related to the Monitor's work. **[FN 59] [FN 60] [FN 58] [FN 23]**

State Four includes visibility: a remedy that cannot be discovered cannot be reliably invoked. The population review therefore reconstructs three distinct visibility stages: launch/emergency publicity; interim-success reporting; and final/disposition or enforcement publicity. Many cases are heavily explained when domains are seized, accounts are disabled, or a TRO is unsealed. Final relief is less consistently explained. The evidentiary weight increases when the same party, counsel, expert, notice-page, and media ecosystem was demonstrably active before final judgment but stops explaining the remedy at the point when the order becomes most durable. Legal-repository availability is therefore coded separately from victim-facing or defender-facing explanation. **[FN 92]**

The same method prevents overstatement in RaccoonO365. Its launch and preliminary-injunction cycle was publicly announced and the Microsoft notice page remains active. Because no entered final judgment was located through the cutoff, the report does not characterize the case as a post-final visibility collapse. It records a different condition: substantial early visibility, a pending default-judgment phase, and no final-remedy event yet available to test under the 23-cv-2447 methodology. **[FN 56] [FN 87]**

Against that population, 23-cv-2447 is the outlier that demands a full longitudinal treatment. It had a highly visible 2023 launch, continuing partner and press discussion, reported 2025 operational metrics, a September 2025 final order broader and more durable than the emergency relief, and then a first located later-victim attempt to use the successor mechanism. Part V measures that sequence source class by source class rather than inferring silence from intuition. **[FN 13] [FN 14] [FN 15] [FN 23] [FN 25] [FN 83]**

PART V - Microsoft / Fortra / Health-ISAC 23-cv-2447: Apex Remedy, Postjudgment Visibility, and State-Four Field Test

This Part follows one case through the entire lifecycle rather than treating the emergency takedown as the endpoint. The March 2023 record supplies Judicial Authority and a reported Technical Execution. The 2024-2025 default process culminates in permanent relief. The September 2025 order supplies successor criteria and a Court Monitor architecture. The later visibility audit and November 2025 application then test whether the standing mechanism remained discoverable and usable outside the original plaintiff group. **[FN 16] [FN 23] [FN 24] [FN 25] [FN 26]**

This Part is the longitudinal capstone because it contains all four states in one record: emergency authority, technical execution, durable permanent relief, and an attempted later-victim invocation. The chapter therefore follows the case in time rather than treating it as a single takedown. It begins with the March 2023 evidence, moves through execution and publicity, then measures what happened after the permanent order created the most durable remedy in the record. **[FN 16] [FN 23] [FN 24] [FN 25] [FN 26]**

5.1 Full legal anchor

The case combined distinct institutional capabilities. Microsoft contributed platform telemetry, software knowledge, and Digital Crimes Unit infrastructure research. Fortra owned the legitimate Cobalt Strike product and could distinguish licensed use from cracked or unauthorized copies. Health-ISAC supplied healthcare-sector risk and victim-impact evidence. Crowell & Moring assembled those functions into a sealed emergency litigation package capable of supporting court and provider action. **[FN 16] [FN 17] [FN 19] [FN 22]**

The Doe caption reflected the operational posture. The emergency request did not depend on naming every ransomware operator, access broker, affiliate, or customer. It depended on showing that specified domains, IP addresses, servers, accounts, and provider relationships formed part of cracked-Cobalt-Strike infrastructure and that neutral third parties possessed the authority necessary to disable, transfer, preserve, or monitor those objects. **[FN 16] [FN 23]**

Microsoft Corporation, Fortra, LLC, and Health-ISAC, Inc. v. John Does 1-16, No. 1:23-cv-02447 (E.D.N.Y.), filed March 30, 2023, is the capstone case. Microsoft supplied platform, software, telemetry and Digital Crimes Unit capacity; Fortra supplied product and licensing evidence for Cobalt Strike; Health-ISAC supplied sector-specific healthcare impact and victim-risk evidence; Crowell & Moring functioned as outside counsel coordinating the sealed emergency litigation package. **[FN 16] [FN 17] [FN 19] [FN 22]**

The defendants were pleaded as John Does associated with ransomware and access-broker groupings including Conti, LockBit, DEV-0193, DEV-0206, DEV-0237, DEV-0243 and DEV-0504. The case did not require the court to name every human operator at the emergency stage. It required the plaintiffs to identify the cracked-Cobalt-Strike control architecture and the

neutral providers capable of disabling, transferring, preserving, or monitoring infrastructure. **[FN 16] [FN 23]**

The case depended on a division of evidentiary labor. Microsoft had global product, platform, and DCU investigative capacity. Fortra owned the legitimate Cobalt Strike product and could explain licensing, cracked copies, watermarks, and the distinction between authorized red-team use and criminal abuse. Health-ISAC supplied the healthcare-sector harm model: ransomware and intrusion infrastructure does not merely injure a software vendor; it threatens hospitals, patients, healthcare operations, and sector-wide resilience. Crowell translated those separate evidentiary functions into a sealed emergency package the court could act on. **[FN 16] [FN 17] [FN 19] [FN 22]**

That combination made 23-cv-2447 different from earlier botnet matters. The case was not limited to one malware family, one domain list, or one plaintiff's product. It connected cracked security tooling, ransomware crews, access brokers, loaders, command infrastructure, hosting providers, healthcare victims, software ownership, and All Writs Act implementation into one court-supervised disruption architecture. **[FN 16] [FN 18] [FN 19] [FN 20] [FN 23]**

5.2 The technical target: cracked Cobalt Strike as service infrastructure

Cobalt Strike is a legitimate adversary-simulation platform used by authorized security teams. The litigation targeted stolen, cracked, or otherwise unauthorized copies used to deploy Beacon payloads, connect compromised systems to team servers, move laterally, conduct post-exploitation activity, deliver ransomware, or provide access to other criminal operators. The legal record therefore had to distinguish the product from its illicit service use. **[FN 19] [FN 20]**

The declarants supplied complementary layers of proof. Jason Lyons described analysis of approximately 50,000 cracked samples, controlled deployment to investigator-controlled computers, observation of command-and-control traffic, extraction of configuration data, and grouping by watermark and actor role. **[FN 18]** Rodelio Fiñones explained the internal mechanics of Beacon, including loaders, APIs, DLL behavior, encrypted metadata, process injection, and configuration fields. **[FN 20]** Robert Erdman supplied Fortra's licensing, product-authentication, and threat-intelligence foundation. **[FN 19]** Christopher Coy connected the technical findings to Microsoft DCU infrastructure and provider control points. **[FN 17]** Jonathan Gross and Errol Weiss supplied product-harm and healthcare-sector context. **[FN 21] [FN 22]**

The sample-driven method converted a broad threat label into inspectable criteria. A domain or IP address was not targeted because it looked suspicious in isolation. Malware configuration, observed traffic, watermark data, product records, provider evidence, or role relationships placed it within the cracked-Cobalt-Strike system. Those internal attributes later supplied the engineering foundation for evaluating infrastructure that was not on the original list. **[FN 18] [FN 20] [FN 23]**

Cobalt Strike is a legitimate adversary-simulation platform. The litigation target was not legitimate red-team use; it was stolen, cracked, or unauthorized copies used to deploy Beacon

payloads, connect to team servers, control compromised systems, move laterally, deliver ransomware, and provide access to other criminal operators. Fortra's evidence explained licensing/watermark controls and the abuse of cracked versions; Microsoft evidence tied that abuse to command infrastructure and ransomware ecosystems. **[FN 19] [FN 20] [FN 18]**

Fiñones supplied the technical grammar for the court: Beacon, stager, full backdoor, reflective loading, DLL and API use, encrypted metadata, AES session keys, process injection, post-exploitation modules, and configuration files containing timing, ports, kill date, and watermark. The analysis converted a brand name into inspectable artifacts a court could use to decide whether a server or domain formed part of the enjoined infrastructure. **[FN 20]**

Lyons supplied the large-scale analytic foundation. His declaration describes analysis of approximately 50,000 cracked Cobalt Strike samples, controlled deployment to investigator-controlled computers, observation of C2 communication, extraction of configuration and watermark data, and grouping of infrastructure by function and actor role. Erdman supplied the Fortra-side product and threat-intelligence foundation; Coy supplied Microsoft DCU infrastructure and provider-control foundation; Gross and Weiss supplied product-harm and sector-harm evidence. **[FN 18] [FN 19] [FN 17] [FN 21] [FN 22]**

The declarations divided the system into complementary evidentiary layers. Coy tied the investigation to Microsoft DCU's infrastructure and provider work. Lyons supplied the sample-driven analysis that converted thousands of cracked tools into C2, configuration and actor-role evidence. Erdman supplied Fortra's product-authentication and licensing perspective. Fiñones gave the court the internal anatomy of Beacon and its post-exploitation modules. Gross explained Microsoft product and software harm. Weiss supplied the sector-specific healthcare impact that made the operation more than a software misuse case. **[FN 17] [FN 18] [FN 19] [FN 20] [FN 21] [FN 22]**

The approximately 50,000-sample analysis moved the case beyond anecdote. A sample set of that scale permits configuration clustering, watermark comparison, server identification, behavior grouping, and actor-role analysis across campaigns. Controlled infections then let investigators observe how the malware behaves when allowed to run in a known environment. Those methods turn infrastructure into evidence a court can test: the domain or IP is not targeted because it is suspicious in the abstract; it is targeted because the malware configuration, observed traffic, watermark, provider record, or role relationship places it inside the cracked-Cobalt-Strike system. **[FN 18] [FN 20]**

Fiñones's Beacon analysis supplies criteria for later successor determinations. Beacon configuration fields - sleep time, jitter, user agent, C2 host, pipe names, process-injection settings, encryption values and watermark artifacts - are not public labels. They are internal operational attributes. A future domain or IP that matches those attributes does not have to share a brand name with the original list to fall within the same technical class. That is the engineering foundation for a final order that can reach later-discovered infrastructure. **[FN 20] [FN 23]**

5.3 March 2023 emergency architecture and execution

The March 2023 emergency package was designed around an execution window. The complaint and declarations identified the malicious system; proposed orders addressed domains, IP addresses, registries, registrars, data centers, hosts, accounts, records, preservation duties, and continuing cooperation; and sealed or delayed procedures reduced the risk that operators would move before providers acted. **[FN 16]**

Judicial authority, technical implementation, and notice were separate functions. The court authorized the restraints. Registries, registrars, hosts, data centers, and other providers possessed the practical ability to change the infrastructure state. The Microsoft notice page and coordinated public accounts then supplied alternative service and explained the operation after execution. **[FN 12] [FN 13] [FN 14]**

The early public record reported substantial operational effect. Microsoft, Fortra, and Health-ISAC described the coordinated action, and later public reporting described an approximately eighty-percent reduction in unauthorized Cobalt Strike use and shorter dwell times. **[FN 13] [FN 14] [FN 15]** Those metrics establish a reported State Two result. They do not, by themselves, establish the scope or later use of the September 2025 permanent mechanism.

The March 2023 emergency package asked the court to authorize infrastructure restraints before the operators could move. The requested relief reached domains, IP addresses, data centers, hosting providers, domain registries, registrars, account records, preservation duties, alternative service, and continuing provider cooperation. The public Microsoft notice page and April 2023 announcement described the action as a coordinated legal and technical disruption of illegal Cobalt Strike infrastructure. **[FN 16] [FN 12] [FN 13]**

The initial public success narrative was substantial. Microsoft, Fortra and Health-ISAC publicly described the operation; Health-ISAC and Fortra statements emphasized that disruption strains the adversary but is not a one-time cure; later public reporting described an approximately 80 percent reduction in Cobalt Strike abuse and shorter dwell times after the legal action. Those public accounts are evidence of an initial State Two effect, not by themselves proof of the September 2025 State Four mechanism. **[FN 13] [FN 14] [FN 15]**

The emergency architecture divided the remedy into legal authority, technical implementation, and public notice. The court authorized domain and IP-related action; the providers and registries were the entities capable of changing state; the notice page then supplied alternative service and public access to pleadings. Once standardized, each step also became a trust boundary. **[FN 12] [FN 13] [FN 16]**

The public aftermath of the emergency phase was not hidden. Microsoft and its partners described the action, the notice page remained accessible, and later public reporting described the partnership as having reduced unauthorized Cobalt Strike copies in the wild by approximately 80 percent and shortened average dwell time. Those metrics do not prove that every target was neutralized, but they do show that the initial action produced externally reported operational impact before final judgment. **[FN 13] [FN 14] [FN 15]**

The baseline is measurable. The case was publicly celebrated at launch and later quantified as successful, so silence after the final order cannot be dismissed as ordinary lack of attention without measurement. The final order did not do less than the launch order; it did more. It converted preliminary relief into permanent relief, incorporated successor criteria, and preserved jurisdiction into 2030. **[FN 15] [FN 23] [FN 26]**

5.4 Default phase, referral, R&R and permanent judgment

The case then moved from emergency relief into the procedural path common to anonymous-defendant litigation. When Doe defendants do not appear after the authorized service process, the court may enter default and evaluate whether the complaint, declarations, record, and requested relief support a final judgment. The matter was referred in October 2024; an August 6, 2025 Report and Recommendation addressed permanent relief; and the September 8, 2025 order adopted that recommendation, entered default judgment, and converted preliminary terms into a permanent injunction. **[FN 23] [FN 24]**

A Report and Recommendation is not itself the final judgment. It presents a magistrate judge's recommended disposition to the district judge under the referral. The September 8 adoption supplied the operative judicial act. The order permanently restrained specified conduct and directed technical actors to transfer or lock domains, propagate DNS changes, block or isolate qualifying IP infrastructure, preserve records, and cooperate with implementation. **[FN 23]**

That transition gives State Three its legal foundation. The case no longer depended on an expiring emergency order. The final instrument established continuing authority over listed and later-qualifying infrastructure. Because anonymous cyber cases may proceed without adversarial factual testing at trial, the specificity of the sworn declarations, infrastructure schedules, definitions, and provider commands carries exceptional weight in determining what the permanent order can later reach. **[FN 16] [FN 18] [FN 23] [FN 24]**

The docket sequence then moved from emergency relief to default and permanent relief. The record includes default-stage filings in 2024, a referral in October 2024, an August 6, 2025 report and recommendation, and a September 8, 2025 order adopting the recommendation and granting default judgment and permanent injunction. The September 8 order states that the R&R recommended converting preliminary and supplemental preliminary terms into permanent injunctive relief. **[FN 24] [FN 23]**

The September 8 order permanently restrained defendants and those in active concert from using unauthorized Cobalt Strike to force access into victims' computers, operate malware/ransomware infrastructure, deploy malware/ransomware, offer ransomware-as-a-service, use Conti/LockBit ransomware deployed through unauthorized Cobalt Strike, and steal information, money or property from plaintiffs, customers or member organizations. **[FN 23]**

The permanent order did not merely declare liability. It commanded technical actors. For domains listed in the order or later determined to be Cobalt Strike domains, U.S.-located registries were directed to unlock, change registrar of record, place domains under Microsoft control, prevent transfer or modification by defendants, and propagate DNS changes. For IP

addresses and associated data centers/hosts, providers were directed to identify and block traffic, disable or isolate infrastructure, preserve records and evidence, and cooperate in implementation. **[FN 23]**

Anonymous cyber cases often reach permanent relief without adversarial factual testing. The declarations, complaint, appendix, and proposed order can become the practical evidence record from which the permanent remedy is built. That posture places unusual weight on the technical specificity of the plaintiffs' showing and on the court's ability to preserve a clear final instrument for later implementation. **[FN 16] [FN 18] [FN 23] [FN 24]**

The August 6, 2025 R&R and September 8 adoption therefore mark the transition from emergency disruption to durable remedy. The court did not simply close a case file. It adopted a structure in which domains, IP addresses, hosting providers, data centers, logs, and future qualifying Cobalt Strike infrastructure could remain subject to judicially supervised action. This is the precise point at which a civil cyber case either becomes a living enforcement architecture or fades into a historical takedown story. **[FN 23] [FN 24]**

5.5 The five-year successor mechanism and Court Monitor

The permanent order addresses the central weakness of a static list: infrastructure changes after judgment. It defines criteria by which later-discovered domains and IP addresses can be compared with known cracked-Cobalt-Strike behavior, ransomware relationships, and actor-group patterns. A future object can therefore be evaluated by function and technical characteristics rather than by whether its name appeared in the March 2023 appendix. **[FN 23]**

The Court Monitor provides a judicially recognized mechanism for that continuing evaluation. The order grants monitor personnel officer-of-the-court protections and permits a party or nonparty to request disclosure of information reasonably necessary to another investigation or litigation related to the Monitor's work. The issuing court retains authority to enforce or modify the injunction and cannot relinquish jurisdiction before January 1, 2030. **[FN 23]**

This structure converts the final judgment into a living enforcement architecture. The monitor, successor criteria, provider obligations, and retained jurisdiction connect later technical reality to an existing judicial remedy. The mechanism still requires an intake path, evidence standard, review process, and visible disposition if persons outside the original plaintiff group are to use it reliably. **[FN 23] [FN 25]**

The defining feature of the September 2025 order is the successor mechanism. The order defines criteria for future Cobalt Strike domains and IP addresses by comparing activity and patterns associated with known cracked-Cobalt-Strike behavior, ransomware association, and actor group relationships. It then supplies a process by which domains and IP addresses not on the original list can be tested and acted upon. That architecture moves the case beyond static Appendix A lists. **[FN 23]**

The order also creates a Court Monitor function, and grants monitor personnel officer-of-the-court protections. It permits a party or nonparty to request that the court direct the Court Monitor to disclose documents or information reasonably necessary to an investigation or litigation in another forum reasonably related to the monitor’s work. The court retained

jurisdiction to enforce and modify the order until Microsoft no longer sought additional determinations or defendants proved no continued risk, and jurisdiction could not lapse before January 1, 2030. **[FN 23]**

The successor mechanism is the case's institutional innovation. A static order tells a provider what to do with listed objects. A successor-aware order tells the system how to evaluate objects discovered later. Modern cybercrime services regenerate: domains expire and return under new names; team servers migrate; customers move; loaders redirect; and affiliates rebuild front-end infrastructure while preserving the backend logic. **[FN 23] [FN 41] [FN 45]**

The Court Monitor provision is the bridge between a closed default case and future technical reality. It creates a court-recognized role through which qualifying information can be evaluated, disclosed, and connected to related investigations or litigation. That design recognizes that cyber infrastructure is not frozen on the day of judgment. It also creates a direct question for State Four: when a later victim or investigator claims that new infrastructure qualifies, can the mechanism actually be reached, and will the result become visible enough for the remedy to have practical force? **[FN 23] [FN 25]**

The order's existence alone cannot establish later usability; later use must supply that measurement. The November 18-19 sequence provides the first located field test. It is not merely an attempted intervention by a nonparty; it tests whether a five-year successor architecture works when someone outside the original plaintiff group seeks to invoke it against alleged later-discovered infrastructure. **[FN 23] [FN 25] [FN 24]**

5.6 Postjudgment visibility audit

The audit separates legal availability from operational explanation. A researcher who already knows the caption, docket number, or target order can locate legal-repository and government presentations of the September 2025 relief. That availability does not tell a hospital, ransomware victim, provider, investigator, or court in a related matter that successor criteria exist, who evaluates them, how the Monitor process operates, or how a nonparty request should be presented. **[FN 23] [FN 71] [FN 83]**

The defined search therefore examined source classes that had previously explained the operation: Microsoft and its security and DCU channels, Fortra, Health-ISAC, Crowell & Moring, named declarants, notice pages, legal repositories, major cyber and legal press, public social and video sources, podcasts, conferences, and archives. Applicant-controlled or affiliated publication material was logged separately and was not counted as independent third-party coverage. **[FN 26] [FN 83]**

The contrast is specific. At least eight distinct pre-final explanatory or operational-success items were verified across official and independent sources. At least six legal-repository, government, or indexed presentations of the final order were located. Within the defined independent party, counsel, expert, and major-media classes, however, the responsive count for an explanation of the final judgment, successor criteria, Court Monitor, nonparty path, or a specific postjudgment enforcement event was zero through the cutoff. General program descriptions and retrospectives repeating pre-final metrics were recorded separately. **[FN 83]**

The refreshed visibility audit uses September 7, 2026 as the cutoff and separates legal-document discoverability from public explanation of the remedy. The searched classes include Microsoft/DCU and Microsoft Security; Fortra; Health-ISAC; Crowell & Moring; named declarants and experts; Notice of Pleadings; CourtListener/RECAP; Justia, vLex, CaseMine, Midpage and other indexed legal repositories; Reuters and major cyber/legal press; Google/Bing-indexed public pages; X and LinkedIn public indexing; YouTube; podcasts and conference pages; and Internet Archive material. Applicant-controlled, affiliated, or USNewsDirect material is logged separately and is not counted as independent third-party coverage. **[FN 26] [FN 83]**

The contrary baseline is substantial. The refreshed search verified at least eight distinct pre-final explanatory or operational-success items across official party/sector pages and independent press, including Microsoft's April 2023 operation account and notice page, Health-ISAC/Fortra material, and 2025 Fortra and security/healthcare reporting discussing the roughly eighty-percent reduction in unauthorized Cobalt Strike use and related dwell-time metrics. The count is deliberately conservative: it counts distinct responsive explanatory items, not every syndication, search result, repost, or legal mirror. **[FN 12] [FN 13] [FN 14] [FN 15] [FN 72] [FN 83]**

After the August 6, 2025 R&R and the September 8-9 final instruments, the legal-document result is different from the public-explanation result. The final order is not missing from the internet. The refreshed search located at least six distinct legal-repository, government, or indexed document presentations of the final relief, including Justia, vLex, CaseMine, Midpage, GovInfo, and Leagle. Those items establish legal availability to a researcher who knows the caption, docket number, or target document. **[FN 23] [FN 71] [FN 83]**

Within the independent party/counsel/named-expert/major-media source classes, however, the responsive count for items specifically explaining the September 8-9 final judgment, the Court Monitor, the successor-domain/IP criteria, the nonparty request path, or how a later victim should invoke the five-year mechanism is zero through the cutoff. The responsive count for a specific public postjudgment enforcement event or a public technical successor determination under that order is also zero. A later Fortra retrospective repeats the operation's pre-final success metrics, and a current Microsoft DCU overview describes Court Monitor and automated-disruption programs at a general program level; neither identifies a postjudgment 23-cv-2447 successor determination, explains the September final order, or supplies the nonparty invocation procedure. Those items are therefore recorded separately rather than used to erase the measured zero in the defined final-remedy category. **[FN 83]**

The evidentiary point is the contrast. The same operation was publicly introduced, technically explained, and later quantified as successful while it was in the emergency and interim phases. The final order then created more durable authority than the publicized launch: permanent restraints, provider commands, successor criteria, Court Monitor architecture, a nonparty disclosure route, and jurisdiction that could not lapse before January 1, 2030. Yet the independent source universe that had previously explained the operation did not produce a responsive explanation of that durable architecture. That is a measured visibility collapse from

celebrated emergency/interim success to silence about the most consequential located remedy. **[FN 13] [FN 15] [FN 23] [FN 83]**

The distinction between legal availability and operational visibility is decisive. A docket mirror proves that the order can be found. It does not tell a hospital, later ransomware victim, investigator, provider, or judge in a related case that successor infrastructure can be evaluated, who performs the evaluation, what evidence is needed, how a nonparty requests access to Monitor information, or what happens after submission. State Four depends on that operational knowledge. The November 18-19 sequence supplies the first located field test of whether the legal architecture became a usable public enforcement path. **[FN 23] [FN 25] [FN 83]**

5.7 November 18-19, 2025: State-Four field test

On November 18, 2025, a later-victim applicant asked the issuing court to apply the standing architecture to alleged successor infrastructure. The Rule 24/Rule 71 filing requested secure technical review, coordination with Microsoft DCU, and use of the existing permanent injunction rather than a wholly new takedown action. In the reviewed docket image, the emergency motion appears as Docket Entry 61 and the related exhibit filing as Docket Entry 62. **[FN 25] [FN 74]**

The November 19 directive removed the ex parte designation, made the filing available to case participants, and directed plaintiffs to respond by December 5. The source-native docket image presents that directive as a text or paperless order without a separate visible docket number or linked PDF in the left-hand entry column. That is a record-state observation, not an inference about motive. **[FN 24] [FN 74]**

Through the cutoff, the defined public record did not disclose a plaintiff technical response, a Court Monitor proceeding, a determination whether the asserted infrastructure satisfied the successor criteria, or a provider action resulting from the request. **[FN 26] [FN 83]** The standing legal mechanism therefore existed and was invoked, but the public lifecycle did not reveal a reproducible technical-review result. State Four is measured at that point as an access and disposition problem, not as a challenge to the validity of the permanent injunction.

On November 18, 2025, the later-victim applicant filed an emergency Rule 24/Rule 71 application in the same case. The filing invoked the September 8 permanent injunction, asserted later-discovered infrastructure said to qualify under the successor framework, requested secure technical review, sought coordination with Microsoft DCU, and asked the issuing court to operationalize the standing remedial architecture rather than require a new civil takedown action from the beginning. In the public docket image reviewed for this report, the emergency motion appears as Docket Entry 61 and the related exhibit filing as Docket Entry 62. **[FN 25] [FN 74]**

The filing is a State-Four test because it presented the problem the final order was designed to anticipate: infrastructure discovered after judgment. The request was not simply for intervention in a closed historical dispute. It sought a protected path for technical evidence, application of the successor criteria, coordination with the plaintiff-side technical capability,

and relief under or related to an order that expressly retained jurisdiction and created a Court Monitor/nonparty information mechanism into 2030. **[FN 23] [FN 25]**

The primary docket state comes first. The November 19 docket/directive ordered the Clerk to remove the ex parte designation from the emergency motion, made the filing available to case participants, and directed plaintiffs to respond by December 5, 2025. In the reviewed source-native docket image, the November 19 directive appears as a text-only/paperless order: the left-hand docket-number column does not display a separate entry number for that row, and no linked PDF is visible for the directive itself. That is a record-state observation, not an inference about motive. **[FN 24] [FN 74]**

The refreshed public record through September 7, 2026 located no public Microsoft/Fortra/Health-ISAC response to the application, no public Court Monitor disclosure proceeding tied to it, no public technical adjudication stating whether the asserted infrastructure did or did not satisfy the successor criteria, and no public later order explaining a technical enforcement result. The same defined media, counsel, expert, social, video, podcast, conference, and archive search located no independent public explanation of the attempted Rule 71 use. **[FN 26] [FN 83]**

That record gives State Four a concrete result. The successor mechanism existed in law; a later-victim applicant attempted to use it; the court directed a plaintiff response; but the searched public record does not expose a reproducible technical-review outcome. A later victim examining the public lifecycle cannot determine from the located sources whether plaintiffs submitted an evaluation, whether the Monitor was engaged, whether the successor criteria were technically tested, or what provider action followed. The gap is therefore procedural visibility and operational reproducibility, not the validity of the permanent injunction. **[FN 23] [FN 25] [FN 74] [FN 83]**

The field test exposes the need for a named intake and disposition path in a standing successor mechanism. If a later victim must improvise an emergency intervention, expose sensitive indicators before a secure technical channel is established, and then cannot locate the technical disposition, the mechanism loses defensive value precisely when adversarial adaptation makes it most necessary. The Clean Adjudicative Environment proposed in Part X is designed to preserve that later-victim evidence path without prejudging whether any asserted successor object ultimately qualifies. **[FN 6] [FN 23] [FN 25]**

PART VI - When the Remedy Becomes the Target Surface

The remedy does not begin at the courthouse and end when an order is entered. Sensitive target lists, expert analyses, provider contacts, proposed commands, sealing strategy, and publication plans exist inside counsel and plaintiff systems before filing. After execution, notice pages, dockets, repositories, media accounts, archives, and later-enforcement communications determine whether the remedy can be discovered and used. Those pre-filing and postjudgment systems form part of the operational chain.

6.1 Counsel and publication systems are part of the remedy

Before filing, counsel systems may contain the precise infrastructure the adversary is not yet supposed to know will be restrained. The law firm receives declarations and appendices, communicates with plaintiff security teams, drafts sealed applications and provider commands, and controls the timing of filing, service, and unsealing. Compromise of counsel identity, mail, DNS, cloud storage, or provider-contact information can expose the target list, alter the execution window, or create trusted-looking instructions before any public docket exists. **[FN 16] [FN 31] [FN 69]**

After filing, the publication layer carries a different operational burden. Notice pages may accomplish alternative service. Repositories and archives preserve access to operative orders. Party and counsel explanations tell later victims and providers what the remedy does. Search indexing determines whether those materials can be found without exact docket knowledge. A legally valid order can retain full doctrinal effect while losing practical defensive reach if the public explanation stops before the most durable mechanism is described. **[FN 12] [FN 23] [FN 26]**

A civil cyber-disruption law firm receives infrastructure lists before public release, communicates with plaintiff security teams, drafts sealed orders, coordinates provider handoffs, files emergency papers, receives NEFs, manages default and permanent-relief submissions, and often participates in public explanation. Compromise of counsel identity, mail, DNS, cloud storage, or publication channels can reveal the target list, alter timing, suppress enforcement, or create trusted-looking communications. **[FN 69] [FN 31]**

The publication layer is equally operational. CourtListener/RECAP, Notice of Pleadings, Justia, vLex, party websites, counsel websites, archive captures, search indexes and media posts determine whether a later victim, provider, journalist, judge, or investigator can locate the operative order. A final judgment that is legally effective but practically invisible loses defensive value. **[FN 26] [FN 69]**

Counsel's infrastructure sits before the court in the timeline. Draft pleadings, infrastructure appendices, expert exhibits, provider contact lists, proposed orders, filing strategy, sealing decisions, and default materials exist inside counsel systems before they exist on a public docket. That makes the law firm a practical custodian of cyber-disruption intelligence. The report treats that custody as an operational fact, not as a criticism of counsel. **[FN 16] [FN 69]**

Publication systems sit after the court in the timeline but remain just as important. A notice page can constitute alternative service, a legal repository can become the easiest way for the public to locate an order, an archived page can prove when a document was visible, and a counsel or corporate blog can teach later victims what remedy exists. When those channels do not update after a final order, the remedy's public memory can stop at the emergency takedown even though the legal remedy later became more durable. **[FN 12] [FN 23] [FN 26] [FN 69]**

6.2 Firm-domain event reconstruction method

The domain analysis begins with a before-and-after state rather than a provider label. For each material domain, the method records the last verified prior state, the first verified changed state, the bounded time interval, registrar, authoritative nameservers, mail-exchange routing, SOA, aliases, DNSSEC, certificates or cloud endpoints, and the authority capable of making the change. The event is then compared with litigation milestones and independent mail, archive, provider, endpoint, or court records. **[FN 45] [FN 48] [FN 69]**

This method distinguishes infrastructure context from probative change. A move to Cloudflare, Route 53, Azure DNS, UltraDNS, DNSMadeEasy, WorldNIC, or another legitimate provider is not evidence of attack by itself. A customer-specific zone change, altered MX route, new certificate, changed CNAME chain, or archive discontinuity near a protected filing or enforcement window is an event requiring explanation. The analysis remains bounded until credentials, administrative logs, API records, session history, or another independent rail identifies how the change occurred.

The DNS/MX/cloud analysis records the customer-specific event, not merely the provider name. For each significant firm or publication domain, the required sequence is: last verified before-state, first verified changed state, timestamp or bounded interval, registrar, authoritative nameservers, MX, SOA, CNAME, DNSSEC, certificate/cloud alias, provider-family control, litigation milestone, corroborating mail/archive/provider record, technical significance, and attribution level. **[FN 69] [FN 45] [FN 48]**

Current and historical records in the investigative source set show law-firm and publication domains distributed across Cloudflare, Route 53, UltraDNS, Azure DNS, DNSMadeEasy, WorldNIC, and other legitimate providers. That distribution is not actor identity. It is the map of the trusted surface through which privileged customer-specific changes must be tested. **[FN 69]**

The analysis therefore does not ask whether a law firm used a famous provider. It asks whether a customer-specific state changed near a material litigation event and whether another record explains or corroborates that change. A change aligned with a registration anniversary carries different weight from a change aligned with sealed filing, unsealing, TRO implementation, final judgment, or publication suppression. A provider-family update across Azure, AWS, UltraDNS or Cloudflare is a control. A customer-domain transition, altered MX route, certificate change, new CNAME chain, or archive discontinuity is an event. **[FN 45] [FN 47] [FN 48] [FN 69]**

This is also where identity and cloud evidence intersect with DNS. A domain zone can be changed through a registrar account, DNS provider console, API key, IAM role, service

principal, delegated administrator, or compromised mailbox recovery path. From the outside, the result looks like normal administration because the provider received an authorized instruction. The forensic question is whether the authority used for the instruction was genuinely controlled by the organization at that time and whether parallel mail, archive, certificate, endpoint, or court-record evidence points to a coordinated event. **[FN 41] [FN 42] [FN 45] [FN 69]**

6.3 Material examples

The named law firms are examined because they occupy recurring positions in the civil-disruption chain, not because the report accuses them as institutions. Crowell & Moring appears in multiple modern Microsoft matters, including cracked Cobalt Strike and RaccoonO365. Other firms in the population likewise receive sealed pleadings, expert communications, target schedules, provider instructions, and permanent-remedy materials. Their domains, mail routes, professional pages, and publication practices are observable trust boundaries through which the remedy travels. **[FN 16] [FN 56] [FN 69]**

The forensic question remains customer-specific. The report asks whether a domain, mail, certificate, professional-persona, publication, or provider-contact state changed during a protected window and whether another record corroborates that change. Recurrence, use of a major provider, or appearance in more than one case is not actor attribution. The comparison identifies where a compromised credential or administrative path could affect the remedy before the public docket reveals the operation.

The expert rails explain the mechanism without converting the firms into defendants. CNF identified synchronized DNS, MX, domain, and server windows. **[FN 27]** CCDG explained how mail can pass SPF, DKIM, or DMARC while remaining operationally counterfeit if the authorized path is controlled. **[FN 31]** RAPS separated filing, intake, docket, notice, service, recipient, and public states. **[FN 30]** The cloud and token sources explain how valid credentials can produce changes that appear administratively ordinary. **[FN 41] [FN 42]**

Crowell & Moring appears repeatedly in the Microsoft cyber-disruption lineage and in the cracked-Cobalt-Strike and RaccoonO365 matters. The forensic inquiry does not turn on the firm's use of a large provider. It examines whether any customer-domain, mail, certificate, publication, professional-persona, or provider-contact state changed during protected windows around sealed filings, unsealing, preliminary relief, permanent relief, or later enforcement. **[FN 69] [FN 56] [FN 23]**

Orrick, King & Spalding, Pillsbury, WilmerHale, Cooley, Perkins Coie, Freshfields, Davis Wright Tremaine, Susman Godfrey and Alston & Bird occupy comparable trust boundaries in the wider population. They are not accused as institutions. Their public domains, professional biographies, counsel signatures, source pages and communication paths form part of the public and legal chain through which a cyber-disruption action becomes executable and discoverable. **[FN 69]**

The expert record adds the subject-side analogue. CNF identified synchronized DNS/MX/domain/server windows and law-firm domain risk; CCDG explained that

SPF/DKIM/DMARC-passing mail can still be operationally counterfeit if the attacker controls the authorized path; RAPS separated the filing, docket, notice, service and public states; and the cloud/token research explains how valid credentials produce ordinary-looking administrative changes. **[FN 27] [FN 31] [FN 30] [FN 41] [FN 42]**

Crowell appears as the recurring anchor in multiple modern Microsoft civil cyber-disruption matters, including the cracked-Cobalt-Strike and RaccoonO365 records. The report does not infer that a law firm is malicious from its recurrence or from its use of a major provider. That recurring position places the same counsel environment in custody of sensitive target lists, expert communications, sealed pleadings, provider commands, and permanent-remedy materials. A compromise or suppression event at that boundary would affect the remedy before any public docket shows the case. **[FN 16] [FN 56] [FN 69]**

Orrick, King & Spalding, Pillsbury, WilmerHale, Cooley, Perkins Coie, Freshfields, Davis Wright Tremaine, Susman Godfrey and Alston & Bird appear across the wider population. Their domains, MX routes, biographies, notice practices, and publication pages are not defendants in this report. They are the visible edges of a trusted professional environment through which cyber-disruption evidence moves. The report uses those edges to compare timing, provider state, public availability, and publication continuity across cases. **[FN 69]**

The professional-persona question belongs inside that same control-plane analysis. Avatar's relevance is not that a public profile by itself proves a case event. Its relevance is that modern adversaries use credible professional identities, dormant accounts, platform profiles, and credential-backed appearances to make trusted interactions look ordinary. Where a professional name appears in civil cyber-disruption filings or related communications, the report checks the source-native record and treats unresolved identity provenance as a channel-integrity issue rather than as a substitute for technical proof. **[FN 33] [FN 56]**

6.4 The publication-control finding

The cracked-Cobalt-Strike record illustrates the distinction between preservation and explanation. Legal repositories preserved the September 2025 order, and the original notice and launch narrative remained discoverable. The defined search did not locate comparable independent explanation of the final order's five-year successor architecture, Court Monitor, nonparty request path, or the first later-victim invocation. **[FN 23] [FN 26]**

A later victim cannot reliably use a mechanism it cannot identify. A provider cannot prepare for a successor workflow that is not explained. A court in a related matter cannot readily evaluate the relevance of a permanent order if the order arrives without a clear operational account of its scope and invocation path. Publication control therefore affects containment even when the underlying legal instrument remains valid. Fragment the public record, leave the final mechanism unexplained, or obscure the disposition of the first later use, and the remedy's reach narrows without any formal modification of the injunction.

The cracked-Cobalt-Strike final order demonstrates that publication systems form part of the remedy. The legal repositories indexed the order; the official launch notice remained visible; the public action narrative remained discoverable; but the final order and the Rule 71 field test

did not receive independent explanatory treatment from the parties, counsel, named experts, cyber press, legal press, public social/video, or conference channels in the defined search. That is a control-plane failure in the public-defense layer. **[FN 23] [FN 26]**

The cracked-Cobalt-Strike sequence shows the risk in practical form. The public notice page and early press established a visible operation. Legal repositories later preserved the final order. But the final order's operational meaning - a five-year successor architecture with Court Monitor involvement and nonparty disclosure possibilities - did not receive a comparable independent public explanation. That is not a media-criticism point. It is a remedy-function point because later-victim access depends on discoverability. **[FN 12] [FN 23] [FN 26]**

A later victim cannot invoke a mechanism it cannot identify; a provider cannot implement a successor process it does not understand; a judge in a related case cannot evaluate the relevance of a final order that arrives without a clean public provenance trail. Publication control therefore becomes part of counter-disruption. Suppress the explanation, fragment the docket path, leave the final mechanism unpublicized, or obscure the first later-victim attempt, and the legal remedy remains valid while its operational reach is narrowed. **[FN 23] [FN 25] [FN 26]**

Part VII - Longitudinal Field Record: Contemporaneous Observation and Later Expert Convergence

The thirty-five representative cases examine lawful use of courts to disable malicious infrastructure. The field record tests the inverse operational condition: allegations that comparable infrastructure, access methods, identity mechanisms, cloud and DNS authority, counterfeit communications, and workflow interference were used against the legal capacity through which containment was being sought. It is included as a longitudinal evidence test, not as biography and not as an invitation to re-decide the underlying motions.

7.1 Analytical role of the field record

The field record begins with contemporaneous pleadings and observations created before the mature expert model existed. Those materials establish dates, asserted workflow effects, requested relief, source locations, and what the attorney/litigant reported while the events were unfolding. They do not independently prove that a named civil defendant retained hackers or caused each event. Later expert work is compared against the earlier record to determine which observations were corroborated, refined, bounded, or left unresolved. **[FN 37] [FN 38]**

This ordering guards against hindsight. A later theory can easily absorb every earlier anomaly if the final model is read backward into the record. The report instead preserves the sequence: contemporaneous filings first; then Marlin; the Team B datasets; CNF's integrated work; Sinkhole and Avatar; RAPS and CCDG; and the Federal Court Audit. The reader can therefore distinguish what was observed before expert synthesis from what the later methods added. **[FN 27] [FN 28] [FN 29] [FN 30] [FN 31] [FN 32] [FN 33] [FN 34]**

The field case is not a member of the thirty-five representative civil cyber-disruption population. It has a different function: it preserves contemporaneous observations by a litigant/attorney who reported cyber interference with prosecution while the conduct was occurring, then allows later independent technical work to be compared against those earlier records. **[FN 37] [FN 38]**

The report does not use the June 2024 or February 2025 pleadings as independent proof that named civil defendants hired hackers. It uses them for what they objectively provide: dated judicial records, contemporaneous observations, asserted workflow effects, source locations, alleged event timing, and a baseline against which later expert reports can be tested. **[FN 37] [FN 38]**

The field case is the report’s reality check. The representative cases show how sophisticated plaintiffs use courts to disrupt infrastructure. The field case asks what happens when an attorney/litigant reports that similar capabilities are being used against the prosecution of cases, communications with courts and opposing parties, professional identity, evidence custody, and the ability to reach neutral review. That is a different evidentiary role, and the separation prevents the report from turning a field chronology into a representative-case selection. **[FN 37] [FN 38] [FN 35]**

The field case also preserves chronology. A later expert model can easily distort early records if the writer begins with the final attribution theory and reads it backward. This report does the opposite. It begins with contemporaneous filings and observed workflow effects, then moves forward to Marlin, Team B, CNF, RAPS, CCDG, Sinkhole, Avatar and the Federal Court Audit. That order lets the reader see which observations preceded expert synthesis and which findings later changed the evidentiary state. **[FN 37] [FN 28] [FN 29] [FN 27] [FN 30] [FN 31] [FN 34]**

7.2 Stable baseline and May 28-June 3, 2024 change point

The field chronology records an asserted stable professional baseline followed by a concentrated change point. A May 28, 2024 litigation milestone was followed on June 3 by delivery of a private photograph and alleged spear-phishing or threat activity, then by reported device, communications, file-access, banking, workflow, family, and case-prosecution effects. The evidentiary value of that sequence is temporal: it was recorded before the later forensic teams had supplied the cAPTure-to-Kill model. **[FN 37] [FN 38]**

The report does not treat temporal proximity as attribution. It preserves the timing so later endpoint, portal, DNS, mail, document-state, and infrastructure findings can be compared with a fixed contemporaneous record. The field symptoms were described as impairment of legal capacity rather than data theft alone: evidence access, communication, hearing preparation, client and family systems, and the ability to prosecute cases were reported as degrading together.

The field chronology begins before the mature cyber model existed. The February 2025 verified complaint and June 2024 emergency motions record a claimed stable professional operating baseline, a May 28, 2024 litigation milestone, a June 3 private-photo/spear-phishing event, and rapid onset of device, workflow, file-access, banking, communications and case-prosecution manifestations. The evidentiary value is temporal: the observations were recorded before Marlin, Team B, CNF, RAPS, CCDG, Sinkhole or Avatar had produced their later models. **[FN 37] [FN 38]**

The May 28-June 3 change point supplies the field record's temporal anchor. The February 2025 verified complaint and the June 2024 emergency motions describe a litigation milestone followed by alleged private-photo delivery, spear-phishing, communication disruption, endpoint/workflow problems, and urgent attempts to obtain protection. Those records preserve what was reported while the asserted campaign was active and before the later expert rails existed; they are not used as final proof of who caused the events. **[FN 37] [FN 38]**

The observed effects in that chronology were not described as ordinary data theft alone. The record speaks in terms of prosecution impairment: files becoming inaccessible, communications failing, hearing preparation disrupted, family and client systems affected, and counsel forced into preservation and emergency motion practice while still trying to litigate. That is the real-world shape of a campaign aimed at legal capacity rather than only information collection. **[FN 37] [FN 38]**

7.3 June 21 and June 25 emergency filings

The June 21 and June 25, 2024 S.D. Florida filings placed the alleged interference into a judicial record during the asserted active campaign. They sought restraint, preservation, in-camera handling, and protection while the law firm's ordinary communications and workflows were reportedly deteriorating. **[FN 37]** The filings therefore provide a dated field baseline independent of the expert reports written later.

A denial of emergency relief on the record then available resolves the requested procedural relief; it does not by itself constitute a technical adjudication of evidence developed months later. The report preserves that distinction. The early motions show what was asserted, what protection was requested, and what operational effects were described. Marlin, Team B, CNF, RAPS, CCDG, Sinkhole, Avatar, and the Federal Court Audit later examined different technical and record-state objects against that chronology. **[FN 27] [FN 28] [FN 29] [FN 30] [FN 31] [FN 32] [FN 33] [FN 34]**

The June 21 and June 25, 2024 emergency filings placed cyber interference into a court record during the alleged active campaign. The motions sought immediate restraint, preservation, in-camera presentation and protection against continuing intrusion while the law firm's workflows were degrading. The later expert reports did not create those allegations; they supplied technical rails against which those contemporaneous records could be tested. **[FN 37] [FN 28] [FN 27]**

An ordinary judicial denial does not end the forensic inquiry. A court can deny emergency relief on the record then available, while later technical evidence can show that the claimant was describing a real attack surface that had not yet been adequately instrumented. The analytical distinction is exact: procedural denial on an incomplete early record is not a technical adjudication rejecting later Marlin, Team B, CNF, RAPS, CCDG, Sinkhole or Avatar findings. **[FN 37] [FN 28] [FN 27]**

The June 21 motion created a contemporaneous judicial record of cyber interference at a moment when the asserted conduct was unfolding. It asked for restraint and preservation because the attorney/litigant was experiencing immediate operational effects, not because a later expert report had supplied a mature attribution model. That timing gives the filing evidentiary value even though it did not resolve the merits. **[FN 37]**

The June 25 filing intensified the record. It described continuing workflow disruption, sensitive records, family and client exposure, alleged phishing, device and account effects, and the practical inability to prosecute cases while the technical environment was unstable. The report uses that filing to show the field symptoms of a trusted-channel attack: the user is not simply missing data; the user is losing the ordinary ability to communicate, prepare, file, verify, and respond. **[FN 37]**

Marlin, Team B, CNF, RAPS and CCDG did not create the first cyber narrative; they examined a record that already existed. The field case therefore belongs in an expert report rather than a grievance narrative: later independent technical work is compared with earlier, dated, source-native observations. **[FN 37] [FN 28] [FN 29] [FN 27] [FN 30] [FN 31]**

7.4 Later expert rails change the evidentiary state

An expert rail is an independently developed evidence stream focused on a different object or method. Marlin examined endpoint, account, cloud, and domain evidence. Team B supplied structured portal datasets. CNF integrated endpoint, DNS, MX, infrastructure, timing, and civil-case comparators. RAPS separated court and communication object states. CCDG examined cryptographic alignment against human and workflow authenticity. Sinkhole addressed registrar and DNS disabling or redirection. Avatar addressed professional-persona provenance. The Federal Court Audit examined source-native docket and document-state artifacts. **[FN 27] [FN 28] [FN 29] [FN 30] [FN 31] [FN 32] [FN 33] [FN 34]**

The progression changes the evidentiary state without erasing the original limits. A contemporaneous allegation remains an allegation. An endpoint finding establishes the artifact or mechanism within the expert's scope. A portal dataset establishes preserved fields and correlations. A comparator case establishes that a capability is real and litigation-tested. Convergence arises when different methods, collected at different times, point toward the same trusted-control-plane function. It does not authorize a natural-person attribution beyond the source record.

Marlin supplied the first independent endpoint/account technical baseline. Team B supplied separate portal data. CNF integrated endpoint, DNS/MX, infrastructure, synchronized windows and civil-litigation comparators. RAPS separated court-object states and SMTP/NEF pathways. CCDG explained authenticated-counterfeit communications. Sinkhole analyzed later domain disabling/redirection. Avatar analyzed professional-persona and identity-provenance events. These reports moved the record from a percipient crisis chronology to a multi-rail forensic model. **[FN 28] [FN 29] [FN 27] [FN 30] [FN 31] [FN 32] [FN 33]**

Marlin added an external technical baseline that predates the October 2025 integrated CNF synthesis, the January 2026 follow-on reports, and the February 2026 RAPS/CCDG record-state reports. Where Marlin identified administrative access, persistence, cloud or endpoint artifacts, the report treats that as an early technical rail rather than as a later narrative conclusion. **[FN 28]**

Team B changed the field case by adding structured portal data. The employee, membership and MyFLCourtAccess datasets are separate objects. They are useful because they create a data rail outside the victim’s narrative and outside the later court filings: identity fields, URLs, timestamps, account-related entries and portal relationships can be compared to communications, docket events, DNS changes and case milestones. **[FN 29]**

CNF then integrated endpoint, DNS/MX, law-firm and court-channel evidence with the civil cyber-disruption comparator cases. RAPS later separated filing, docket, NEF, service, public-access and DCN/SMTP states. CCDG separately explained how an email can pass technical authentication and still be operationally counterfeit if the authorized path is controlled. The field case therefore moves from observation to independent technical analysis to integrated mechanism. **[FN 27] [FN 30] [FN 31]**

7.5 Field record within the cAPTure-to-Kill model

The field record presents a 360-degree legal-capacity attack surface. The alleged operation was not limited to encrypting a device, stealing a file, or demanding ransom. It involved reported pressure across evidence custody, communications, identity, accounts, filing, service, notice, publication, professional reputation, operational continuity, family and vendor relationships, and access to judicial relief. The integrated experts later mapped mechanisms by which control at those different layers could produce apparently ordinary procedural or administrative states. **[FN 27] [FN 30] [FN 31]**

That is the inverse of the representative civil-disruption cases. In the historical population, plaintiffs used judicial authority to disable domains, servers, accounts, platforms, and service infrastructure. In the field record, the allegation is that analogous malicious infrastructure and TTPs were used to impair the capacity to investigate, file, communicate, preserve evidence, obtain a neutral technical review, and enforce a remedy. The same legal-technical chain appears, but the direction of control is reversed.

The pattern is tested through accumulation rather than one dramatic event. Inaccessible evidence, altered or missing communications, disputed service, identity confusion, account persistence, deadline pressure, publication gaps, and docket-state problems may each admit an ordinary explanation. The forensic question is whether the sequence remains ordinary when matched against independent technical rails, synchronized timing, and the capability classes established by the civil-cyber comparators. **[FN 27] [FN 30] [FN 31] [FN 37] [FN 38]**

The field case tests the same architecture from the victim side. The alleged objective was not only stealing data or demanding ransom; it was disabling prosecution, isolating the attorney, disrupting communications, corrupting trusted channels, impairing filings, suppressing notice, exhausting response capacity, and making the evidentiary record arrive late, incomplete or through a compromised channel. That is cAPTure-to-Kill as litigation-control architecture. **[FN 27] [FN 30] [FN 31]**

The field case supports cAPTure-to-Kill because it shows a prosecution-capacity attack surface. The relevant pattern is not one dramatic hack. It is the accumulation of small trusted-channel failures: inaccessible evidence, altered or missing communications, disputed service, identity confusion, account persistence, deadline pressure, publication and docket-state problems, and exhaustion of the attorney's ability to maintain ordinary litigation operations. Each event can be made to look routine in isolation; the forensic task is to test whether the sequence remains routine when matched against independent expert rails and civil-disruption analogues. **[FN 27] [FN 30] [FN 31] [FN 37] [FN 38]**

The field record leads directly to the CAE conclusion. The ordinary legal system assumes that missed notices, late filings, docket entries, PDF availability, and service paths are procedural states. In a cyber-sensitive matter, those same states can be manifestations of the alleged attack. A clean adjudicative path is needed not to guarantee success on the merits, but to let a neutral decisionmaker examine the integrity evidence before ordinary channel assumptions decide the outcome. **[FN 30] [FN 31] [FN 34] [FN 35]**

PART VIII - Independent Expert Convergence

Convergence does not mean several reports repeated the same conclusion. It means separate teams examined different objects at different times, using different methods, and reached findings that can be aligned at the level of capability and control. This Part reconstructs that progression so the integrated conclusion rests on method and chronology rather than credentials or volume.

This Part does not list expert names as credentials. It reconstructs the evidentiary function of the expert rails. Each rail examined a different object at a different time: endpoint artifacts, restricted-portal data, DNS/MX records, litigation comparators, domain suppression, professional persona provenance, federal docket states, and cryptographic communications. Their force comes from repeated convergence on the same trusted-control-plane architecture. **[FN 27] [FN 28] [FN 29] [FN 30] [FN 31] [FN 32] [FN 33] [FN 34]**

8.1 Chronology of the rails

The sequence supplies a control against circular reasoning. The June 2024 filings recorded the field observations before mature expert analysis. Marlin followed in December 2024. Team B preserved distinct portal datasets. CNF integrated the subject-side evidence with external civil-disruption comparators in October 2025. Sinkhole and Avatar extended the domain and persona questions in January 2026. RAPS and CCDG then examined court-channel, message-routing, and cryptographic-communication states in February 2026. **[FN 27] [FN 28] [FN 29] [FN 30] [FN 31] [FN 32] [FN 33] [FN 37]**

The rails are also different in kind. Endpoint artifacts do not answer the same question as portal logs. DNS history does not establish the same fact as a docket replacement notation. An authenticated mail path does not establish that the human sender intended the message. Agreement across those distinct evidence classes carries more weight than repeated interpretation of one screenshot, one account, or one narrative source.

The expert chronology is itself probative. The June 2024 emergency filings predated all mature expert work. Marlin's December 2024 report predated the October 2025 CNF synthesis. Team B portal datasets supplied a separate data rail. CNF's October 22, 2025 report integrated subject-side evidence and civil-litigation comparators. The January 2026 Sinkhole and Avatar reports extended the domain and persona rails. The February 2026 RAPS and CCDG reports extended the court-channel, DCN/SMTP, and authenticated-communication rails. **[FN 37] [FN 28] [FN 29] [FN 27] [FN 32] [FN 33] [FN 30] [FN 31]**

The chronology prevents false circularity. The June 2024 filings came first. Marlin followed in December 2024. Team B portal data and CNF's broader integration followed through 2025. The October 22 CNF report then supplied the mature integrated model. Sinkhole and Avatar tested later domain/persona manifestations in January 2026. RAPS and CCDG then examined federal record-state and cryptographic-communications problems in February 2026. Later reports therefore did not invent the underlying field observations; they examined different objects and

different technical layers across time. **[FN 37] [FN 28] [FN 29] [FN 27] [FN 32] [FN 33] [FN 30] [FN 31]**

The rails also examine different evidence classes. Marlin is endpoint/account/cloud. Team B is portal data. CNF is integrated forensic overlay. Sinkhole is registrar/DNS/domain suppression. Avatar is professional-persona provenance. RAPS is filing/intake/docket/service/DCN/SMTP record-state analysis. CCDG is cryptographic path versus human/workflow authenticity. External sworn experts are civil-litigation technical witnesses. Agreement across those different objects carries more weight than repetition inside one report. **[FN 27] [FN 28] [FN 29] [FN 30] [FN 31] [FN 32] [FN 33]**

8.2 Marlin

Marlin entered the record before the later litigation overlay. Its December 2024 engagement examined court materials and embedded screenshots, more than 220 ICANN and domain records, two computer devices, and domain-email-server records, with open-source cross-checking. **[FN 28] [FN 80]** The assignment addressed whether unauthorized infiltration existed, whether the activity appeared targeted and persistent, and whether the observed access could interfere with law-firm and court-facing systems.

Marlin's contribution was an early access-and-control baseline. It described progression toward administrative control affecting the law-firm network, DNS, cloud storage, credentials, and communications, and explained how DNS or credential authority could support cloning, interception, suppression, or man-in-the-middle effects. **[FN 28] [FN 80]** This report uses those mechanism findings while preserving the boundary that more aggressive natural-person or organizational attribution requires separate source-native proof.

Marlin entered the chronology before the mature civil-case overlay. Its December 5, 2024 engagement asked whether unauthorized infiltration existed, whether the activity was targeted, how sophisticated and persistent it was, and whether the observed access could interfere with law-firm and court e-filing, email, website, and network systems. The materials identified in the report included court documents and embedded screenshots, more than 220 ICANN/domain reports, two computer devices, and domain-email-server records. Marlin cross-checked the domain material with open sources and examined the devices for credential and communications effects. **[FN 28] [FN 80]**

The report's technical contribution was an early access-and-control baseline. Marlin described a spring-summer 2024 progression of unauthorized permissions toward administrative control of the law-firm network, website DNS, cloud storage, and credentials, and it analyzed a core set of DNS changes that coincided with operational events. It separately explained the mechanics by which administrative DNS or credential control can clone a site, change mail routing, suppress or read communications, and create an apparently successful upload or login event that did not reach the intended system. Those mechanism findings are used here; Marlin's more aggressive natural-person or organizational attribution opinions are not imported as a substitute for later source-native proof. **[FN 28] [FN 80]**

Chronologically, Marlin changed the evidentiary state because it preceded the October 2025 CNF synthesis, the January 2026 domain/persona reports, and the February 2026 court-channel reports. Later teams therefore had an independent technical floor to confirm, refine, or contradict. CNF later found endpoint persistence and synchronized infrastructure patterns; RAPS later separated portal and docket object states; CCDG later explained cryptographically valid but operationally counterfeit communications. The value is not repetition. It is the progression from early endpoint/domain control evidence to later workflow-level consequences. **[FN 27] [FN 30] [FN 31] [FN 80]**

8.3 Team B

Team B contributed structured datasets rather than another narrative opinion. The Florida Bar Employee Portal, Florida Bar Membership Portal, and MyFLCourtAccess or e-filing datasets preserve different combinations of identity, URL, date, account, access-related, and workflow fields. **[FN 29]** Each portal governs a distinct trust function: staff identity, professional-membership identity, or filing and service identity.

The method is correlation with controls. An unusual portal row is not labeled malicious merely because it is unfamiliar. It is compared with the user's established pattern, timing, infrastructure, DNS and MX changes, communications, service events, filings, and consequences preserved in another source. The datasets also define the telemetry needed for confirmation: administrator-change logs, session and device identifiers, source-IP history, MFA enrollment, backend audit events, and service-list changes. **[FN 29] [FN 81] [FN 82]**

Team B contributed structured data rather than a generalized opinion. The Florida Bar Employee Portal, Florida Bar Membership Portal, and MyFLCourtAccess/e-filing datasets are separate evidentiary objects. They preserve combinations of identity, URL, date, account, credential/IP-adjacent, and portal-state fields that can be compared against DNS/MX state, service events, filings, and communications. Each portal governs a different trust function: institutional staff identity, professional membership identity, and judicial filing/service identity. **[FN 29]**

The method is correlation with preserved controls. A portal row is not treated as malicious merely because it is unusual. The relevant question is whether access or account-state activity departs from the user's established pattern, appears from unfamiliar infrastructure or timing, aligns with a DNS/MX or credential event, and produces a procedural consequence in another independently preserved source. CCDG later reported independent review of the portal datasets and specifically described portal-source infrastructure and timing correlations; RAPS separately framed the backend telemetry needed to test identity and workflow state. **[FN 29] [FN 81] [FN 82]**

Team B therefore added a capability fact that endpoint forensics alone could not supply: a compromised legal workflow can be exercised through valid portal identity without malware executing on the portal itself. That mechanism maps directly onto the modern civil-cyber cases involving valid sessions, AiTM phishing, platform identities, cloud access, and service accounts. It also defines the remaining evidentiary work precisely - administrator-change logs, device/session identifiers, source IP history, MFA enrollment, backend audit events, and

service-list changes - rather than leaving the portal issue as a user-interface anomaly. **[FN 29] [FN 56] [FN 81]**

8.4 CNF October 22

The October 22 CNF report is the principal integrated subject-side rail because it moves from artifact to method to operational consequence. It examined endpoint and memory evidence, remote-management and credential artifacts, DNS, MX and registrar records, law-firm and court-adjacent infrastructure, portal data, synchronized timing windows, communications, and public threat intelligence. It then compared evidence collected through those subject-side channels with civil cyber-disruption cases. **[FN 27] [FN 75]**

The blind or compartmentalized overlay controls against retrospective fitting. The civil cases were not used to invent the endpoint, portal, or DNS events. They supplied an external grammar for mechanisms already observed: command-and-control behavior, valid credentials, infrastructure rotation, provider dependence, law-firm trust boundaries, and successor systems. Correlation after separate collection carries greater weight than a narrative built from one source and then illustrated with selected examples.

CNF moved the working model from device compromise to workflow-level counter-disruption. Later reports refined individual layers - domain suppression, persona provenance, federal record state, and cryptographic communications - without replacing the October 2025 integration. The capstone permanent injunction then supplied a real successor-remedy architecture against which later access could be tested. **[FN 23] [FN 30] [FN 31] [FN 32] [FN 33]**

The October 22 CNF report is the principal integrated subject-side rail and the prose model for this report because it moves from artifact to method to consequence. It examined endpoint and memory evidence, RMM and credential artifacts, DNS/MX and registrar records, court- and law-firm-adjacent infrastructure, portal data, synchronized event windows, communications, and public threat intelligence. It then compared the independently collected subject evidence with civil cyber-disruption cases rather than selecting subject artifacts to fit those cases after the fact. **[FN 27] [FN 75]**

On the endpoint side, CNF documented persistence and command-channel evidence such as RMM activity, HTTPS C2 behavior, registry/run-key and DLL-loading artifacts, crash-dump evidence of injected code, stolen-credential/lateral-access indicators, and memory-resident or screen/keylogging functionality. On the infrastructure side, it tracked DNS/MX changes, nameserver movement, portal-access clusters, and timed changes across domains relevant to the legal workflow. On the litigation side, it overlaid those mechanisms against sworn federal civil-cyber evidence describing C2, reverse proxies, valid accounts, provider control, cracked Cobalt Strike, access brokers, and successor infrastructure. **[FN 27] [FN 75]**

The methodological contribution is the synchronized-window and blind-overlay design. If endpoint artifacts, portal events, DNS/MX changes, communications anomalies, and external comparator mechanisms were collected through distinct rails, correlation after collection carries more weight than a narrative assembled from one data source. CNF used that

convergence to move the working model from device compromise to trusted-control-plane counter-disruption: a campaign can preserve its objective by controlling the systems through which legal evidence is communicated, filed, published, and enforced. **[FN 27]**

Later evidence refined rather than replaced that model. Sinkhole tested later domain suppression and successor behavior; Avatar addressed persona provenance; RAPS tested federal record and routing states; CCDG tested cryptographic communications; and the 23-cv-2447 final order supplied a real successor-remedy architecture against which later-victim access could be measured. That chronological progression leaves the October 22 report as the central model-building rail without making it the sole source of the final determination. **[FN 23] [FN 27] [FN 30] [FN 31] [FN 32] [FN 33]**

8.5 RAPS and CCDG

RAPS and CCDG address two questions that can look identical from the user's screen. RAPS asks whether the legal objects remain synchronized: the file submitted by the filer, the object received at intake, the chambers or restricted copy, the docket entry, the NEF or service event, the recipient copy, and the public or repository copy. CCDG asks whether a message that passes technical authentication also represents an authentic human and workflow event. **[FN 30] [FN 31]**

RAPS reconstructed dockets, orders, clerk notices, physical-file copies, and sealed or internal records where available, then aligned those objects with CM/ECF, DCN, SMTP, authentication, timestamp, address, and DNS/MX data. **[FN 30] [FN 81]** A replacement notation, missing link, text-only directive, service divergence, or public-copy difference becomes a measurable record state rather than an anecdote.

CCDG examined more than fifty-seven judicial e-communication metadata items together with endpoint and portal evidence. **[FN 31] [FN 82]** SPF, DKIM, DMARC, DNSSEC, or passage through an authorized relay can validate defined parts of a technical path. They do not establish that the human sender intended the message, that the recipient list was authentic, that the attachment was the source object, or that the authorized account, relay, DNS state, or session was not itself controlled. That is the basis for the term authenticated-counterfeit communication.

RAPS and CCDG examine different trust questions. RAPS asks whether the legal record states remain synchronized: filer upload, intake, docket entry, chambers/restricted access, Notice of Electronic Filing or service event, recipient copy, and public copy. CCDG asks whether a technically authenticated communication is also authentic in human and workflow meaning. Those questions intersect, but the evidence and methods are distinct. **[FN 30] [FN 31]**

RAPS used a document-driven reconstruction of dockets, orders, clerk notices, physical file-room copies and sealed/internal records where available, then aligned those states with CM/ECF/DCN/SMTP relay data, SPF/DKIM/DMARC fields, timestamps, IP addressing, and DNS/MX history. It also described a deliberately separated workflow in which email-header anomalies were reconstructed before comparison with CNF portal correlations. That method permits a missing link, replacement notation, unnumbered text order, service divergence, or

public-copy difference to be treated as a measurable record state instead of an anecdote. **[FN 30] [FN 81]**

CCDG approached the communications layer from the opposite direction. It examined more than fifty-seven judicial e-communication metadata items together with endpoint and portal evidence and asked whether green trust signals could coexist with an adversarial workflow. Its governing finding is technical: SPF, DKIM, DMARC, DNSSEC, or passage through an authorized relay authenticate specified parts of the technical path; they do not establish that the human sender intended the message, the recipient list was authentic, the attachment was the original, or the authorized account/relay/DNS path was not itself controlled. CCDG therefore examined DNS history, selector and relay changes, mailer fingerprints, tokenized links, recipient-state anomalies, timing, and ordinary sender workflow. **[FN 31] [FN 82]**

Together, the two rails explain document-state divergence and authenticated counterfeiting without collapsing them into one claim. A threat actor controlling a valid session can cause a portal to accept an ordinary-looking action. A controlled mail or DNS path can produce a technically passing notice. A docket can then reflect a system state that differs from the filer or recipient object. The resulting legal question is not resolved by asking whether the padlock was green or the email authenticated. It requires preservation and comparison of each object state. That is the direct technical foundation for the Clean Adjudicative Environment. **[FN 30] [FN 31] [FN 81] [FN 82]**

8.6 Sinkhole and Avatar

Sinkhole extends the analysis from access to reachability and control. Registrar and DNS state determine whether a domain resolves, where it directs traffic, and whether later infrastructure can be disabled, redirected, or replaced. **[FN 32]** Those are the same control layers civil injunctions reach when they order registries, registrars, hosts, or providers to transfer, disable, sinkhole, or preserve infrastructure.

Avatar addresses a different trust layer: professional-persona provenance and credential-backed appearance. Accounts, directory entries, biographies, signatures, affiliations, and platform profiles can cause an interaction to look ordinary. **[FN 33]** The report uses that work only as bounded capability and provenance evidence. An unresolved profile anomaly is not a substitute for source-native proof of a natural person's identity or conduct.

The Federal Court Audit supplies the document-state bridge by examining assignment, docket, PageID, replacement, service, linked-object, and filing relationships. **[FN 34]** Primary dockets and signed orders control the procedural facts; the audit is used afterward to explain the forensic significance of the preserved state. Combined, the three rails extend the model through domain reachability, professional trust, and adjudicative record state.

The Sinkhole report extends the chronology from access into control of reachable infrastructure. It examines registrar and DNS state, disabling or redirection of later domains, and successor/suppression behavior. Once a domain, registrar account, or DNS path can be disabled, redirected, or replaced, the analysis is no longer limited to whether an endpoint was infected. It reaches the same control layer that civil cyber injunctions command when they

order registries, registrars, hosts, or providers to transfer, disable, sinkhole, or preserve infrastructure. **[FN 32]**

Avatar examines a different control layer: professional persona provenance and credential-backed appearance. Modern legal and cyber workflows place trust in accounts, directory entries, biographies, signatures, professional affiliations, and platform profiles. Avatar's role in this report is bounded to that capability category and to source-provenance questions. It does not support a standalone natural-person attribution from unresolved persona provenance, and the report does not infer a natural-person identity endpoint unless the underlying professional and litigation records independently establish it. **[FN 33]**

The Federal Court Audit supplies the record-state bridge. It examines docket and assignment states, PageID/ribbon sequence, replacement language, service notations, missing links, filing-object relationships, and other source-native features. Primary dockets and signed orders control; the Audit is used after those facts are established to explain forensic significance. That sequence prevents a metadata observation from being mistaken for a merits conclusion while preserving the integrity question the metadata actually raises. **[FN 34]**

Together, Sinkhole, Avatar, and the Federal Court Audit establish cAPTure-to-Kill as a control-plane model rather than an endpoint-malware label. Domain control affects reachability and publication; persona control affects trust; record-state control affects what the tribunal and parties can see. When those layers align with the endpoint, portal, and communications rails, the integrated question becomes whether the adversary can neutralize legal capacity while ordinary systems continue to appear operational. **[FN 27] [FN 32] [FN 33] [FN 34]**

8.7 External sworn litigation experts

The external declarants are mechanism evidence developed in separate federal cases for different plaintiffs and targets. In 23-cv-2447, Christopher Coy addressed Microsoft DCU infrastructure and provider control; Jason Lyons addressed approximately 50,000 samples and controlled infection; Robert Erdman addressed product, licensing, cracked copies, and threat intelligence; Rodelio Fiñones addressed Beacon configuration and post-exploitation mechanics; Jonathan Gross addressed product harm; and Errol Weiss addressed healthcare-sector risk. **[FN 17] [FN 18] [FN 19] [FN 20] [FN 21] [FN 22]**

Sophos, DXC, Google, and later Microsoft matters broaden the same evidentiary vocabulary through attack infrastructure, rotating domains, reverse proxies, botnet fallback, platform telemetry, infostealers, phishing services, valid sessions, and disposable cloud environments. **[FN 56] [FN 58] [FN 63] [FN 89] [FN 90]** The witnesses do not prove the field events by association. They establish that the capability classes are real, repeatable, and sufficiently bounded to support emergency or permanent relief when tied to source-specific evidence.

The external sworn declarants are independent mechanism evidence because their testimony arose in separate civil cybercrime cases for different plaintiffs and different infrastructure targets. In 23-cv-2447, Christopher Coy supplied Microsoft DCU infrastructure and provider-control evidence; Jason Lyons described analysis of approximately 50,000 cracked-Cobalt-Strike samples and controlled infection/C2 observation; Robert Erdman supplied Fortra

product, licensing, cracked-copy and threat-intelligence evidence; Rodelio Fiñones described Beacon, loader, configuration, encryption, process-injection and watermark mechanics; Jonathan Gross supplied Microsoft product-harm context; and Errol Weiss supplied healthcare-sector risk. **[FN 17] [FN 18] [FN 19] [FN 20] [FN 21] [FN 22]**

The other representative matters broaden the same vocabulary. Sophos shows a security vendor using emergency provider/domain relief against attack infrastructure. DXC's Mark Hughes describes Cobalt Strike BEACON, rotating domains and reverse-proxy relationships before the 23-cv-2447 architecture matured. Google matters add botnet fallback, platform telemetry, infostealer and PhaaS mechanisms; Microsoft's later matters add DGA/future-domain logic, identity-centric phishing, service infrastructure and disposable cloud environments. These records show the same legal translation repeatedly: identify the control point, explain the technical method under oath, and direct relief to the intermediary capable of changing state. **[FN 89] [FN 90] [FN 58] [FN 56] [FN 63]**

The convergence is therefore both methodological and substantive. Methodologically, separate experts use controlled infection, reverse engineering, configuration extraction, passive DNS, platform telemetry, provider records, product-authentication evidence and sector testimony. Substantively, the methods reveal recurring layers: access, credentials or tokens, C2/service backend, trusted provider control, fallback/successor infrastructure, and downstream operational effect. The field-case expert rails independently identify the same classes at the level of endpoint, DNS/MX, portal identity, communication authenticity, persona and record state. **[FN 18] [FN 20] [FN 27] [FN 30] [FN 31]**

That is the exact level at which this report states its strongest integrated determination. The evidence establishes a repeatable trusted-control-plane capability and a counter-disruption model that maps onto the civil-cyber remedy architecture. It does not require a universal one-person or one-crew attribution. Protecting the remedy depends on recognizing and hardening the capability before every natural-person endpoint is known. **[FN 27] [FN 30] [FN 31] [FN 23]**

PART IX - Adjudicative-Channel Stress Tests

The historical cases assume that the plaintiff can place a reliable technical record before the court through a trusted intake and service path. The proceedings in this Part test the exceptional condition in which filing, routing, notice, service, identity, record custody, or public availability is itself part of the allegation. The analysis does not ask the reader to retry the underlying cases or infer misconduct from an unusual docket event. It reconstructs the relevant objects and chronology so the integrity question can be examined without beginning from the assumption that the disputed channel operated as intended. **[FN 30] [FN 31] [FN 34]**

This is the report's field-validation chapter. The thirty-five representative cases show how a technically bounded record can be converted into emergency authority, provider action, permanent relief, and, in the strongest examples, continuing successor enforcement. The proceedings below ask the inverse question: what happens when a cyber-sensitive claimant attempts to invoke comparable judicial authority while asserting that the filing, service, communications, or record pathway needed to reach the judge may itself be affected? The answer is not supplied by any single anomaly. It emerges from the source-state sequence across several independent adjudicative systems. **[FN 25] [FN 35] [FN 36] [FN 39] [FN 40]**

9.1 The Inverse Field Test: When the Integrity Allegation Must Travel Through the Disputed Channel

The S.D. Florida August 2025 Doe action, E.D.N.Y. 25-cv-06033, the postjudgment Rule 24/Rule 71 application in 23-cv-2447, the Florida Supreme Court original-jurisdiction record, and the March 2026 D.D.C. filing are not members of the thirty-five-case population. They do not establish the historical lineage of civil cyber-infrastructure disruption. They perform a different analytical function: they test whether the remedy remains reachable when the claimant disputes the integrity of the ordinary path by which the integrity evidence must be delivered. **[FN 25] [FN 35] [FN 36] [FN 39] [FN 40]**

That distinction matters because an electronic court event is not one indivisible object. A physical filing may be converted into an intake scan; the intake scan may become a docket attachment; a chambers or restricted copy may differ from the public copy; a text-only order may appear without a linked document; a Notice of Electronic Filing or mailed notice may create a separate service state; and a repository or archive may later preserve yet another derivative. RAPS formalized those states as the filer object, intake object, chambers object, docket entry, service or NEF event, recipient copy, public copy, and repository copy. CCDG addressed the related communications problem: a message can pass ordinary authentication checks while still misrepresenting the human or workflow event if the authorized account, relay, session, DNS state, or recipient path has been controlled. **[FN 30] [FN 31]**

The Federal Court Audit adds a record-object method to that framework. A file stamp, assignment entry, replacement notation, PageID sequence, linked PDF, service notation, receipt, envelope, or clerk-generated docket image is first treated as a source-native fact. A verified complaint or affidavit establishes what the witness swore occurred. An expert report then explains technical significance within its defined scope. Only after those layers are

separated may the report identify an unresolved integrity question or a bounded inference. This ordering prevents a compressed procedural sequence from being mislabeled as proof of malicious interference while also preventing the underlying record-state facts from being erased as mere dissatisfaction with a result. **[FN 34] [FN 35] [FN 36]**

The September 8, 2025 permanent judgment in 23-cv-2447 supplies the operational benchmark. It did more than close an emergency case. It created technical criteria for later Cobalt Strike domains and IP addresses, a Court Monitor function, a nonparty information path, provider obligations, and retained jurisdiction that could not lapse before January 1, 2030. A standing mechanism of that kind is valuable only if a later claimant can identify it, deliver qualifying evidence through a protected path, receive a technical determination, and locate a reviewable disposition. **[FN 23] [FN 25]**

Part IX therefore asks a narrow preliminary question in each system: did the reviewed record provide an independently auditable path to authenticate what was submitted, what reached intake, what became available to chambers, what was docketed, what was served, and what later became public before ordinary procedural consequences attached? The repeated absence of such a path does not prove that every system was compromised or that every procedural ruling was cyber-caused. It identifies the institutional condition the Clean Adjudicative Environment is designed to address. **[FN 30] [FN 31] [FN 34]**

9.2 S.D. Florida 25-cv-23807: Emergency Cyber-Disruption Filing Meets Ordinary Intake

The first federal field test began on August 22, 2025 with a conventionally filed, under-seal verified action against unknown Doe defendants. The complaint did not seek ordinary damages relief alone. It described an alleged advanced persistent threat directed at legal-sector systems, alleged that previously identified command-and-control infrastructure had been reused or repurposed, and asked the court to employ the same general civil-disruption logic developed in Microsoft and Google matters: identify the malicious control points, preserve the execution window, and direct neutral providers to disable, transfer, or sinkhole qualifying infrastructure. The file-stamped complaint and the later docket establish that the package included emergency sealing and temporary-injunction requests together with a multi-part exhibit set. **[FN 36]**

The timing placed that filing beside the report's capstone remedy. Sixteen days earlier, on August 6, 2025, the magistrate judge in 23-cv-2447 had recommended converting the cracked-Cobalt-Strike preliminary restraints into permanent relief. The S.D. Florida filing did not have the institutional resources of Microsoft, Fortra, Health-ISAC, outside counsel, and the Digital Crimes Unit. It nevertheless attempted to use the same legal-technical premise while the E.D.N.Y. successor mechanism was moving toward final judgment: anonymous operators could remain unidentified at the outset if the claimant could present a sufficiently bounded infrastructure record and executable relief to the court. **[FN 24] [FN 23] [FN 36]**

The intake context is preserved through both source-native documents and verified testimony. The physical complaint bears an August 22 filing stamp and a prominent sealed designation. The verified affidavit states that the package was delivered after ordinary cashier operations had ended, that the register used to receive filing payments was closed, and that the seal clerk advised that the materials would be onboarded and routed for judicial review. The affidavit

further states that the filer was told a district judge, or a duty judge if necessary, would address the emergency sealing request. Those statements are evidence of the witness's sworn account of the intake conversation; the docket establishes the later electronic state. **[FN 36]**

The September 2 clerk-generated docket shows the case as filed on August 22 and entered into the electronic system on August 25. It identifies the cause as the Computer Fraud and Abuse Act, the nature of suit as racketeering/corrupt organizations, and the jurisdictional basis as federal question. Entry 1 records the verified complaint, civil cover sheet, and numerous exhibit attachments. Entry 2 is captioned 'Judge Assignment to Magistrate Judge Enjolique A. Lett.' Entries 3 through 6 record the emergency sealing motion, temporary-restraint request, and supporting declarations. The source-native record therefore shows that the first judge-assignment state visible on the docket was a magistrate-judge assignment in a newly initiated civil case containing emergency injunctive applications. **[FN 36] [FN 34]**

That initial state was not permanent. On August 27, the docket records an Order of Reassignment signed by the magistrate judge and a clerk's notice reassigning the case to District Judge Rodolfo A. Ruiz II. The same entry states that the magistrate judge was no longer assigned as presider. This report does not claim that assignment software was incapable of producing the first state, nor does it treat the sequence alone as proof of interference. The record fact is narrower: the emergency package was electronically entered on August 25 with an initial magistrate-assignment event, and the district-judge assignment state was recorded two days later. **[FN 36] [FN 34]**

The fee and dismissal sequence then compressed into approximately one day. On August 27, the clerk entered a paperless notice stating that the action had not been filed with the required $405 fee. The docket text did not state a cure deadline. On August 28, the district judge entered a two-page order dismissing the action without prejudice under Rule 41(b), stating that the fee had not been paid, no in forma pauperis motion had been filed, and no extension had been sought. The order marked the case closed and denied the pending sealing and emergency motions as moot. The operative court action therefore occurred before the emergency infrastructure allegations received a separately documented technical-integrity review. **[FN 36]**

The record did not end there. A cashier receipt establishes that the $405 civil filing fee was paid in cash on September 2 at 4:07 p.m. The verified affidavit states that the filer also presented a handwritten verified reconsideration request, an amended verified complaint, supplemental technical material, and a renewed emergency application that day. The September 2 order acknowledged the payment, described it as occurring eleven calendar days after initiation, denied reconsideration because the governing standard was not met, denied the additional emergency motion as moot, and stated that a new action could be filed. The court thus resolved the reconsideration request as a procedural matter while leaving the underlying technical allegations unadjudicated. **[FN 36]**

The notice state is analytically separate from the docket state. The verified affidavit states that no electronic copy of the August 27 deficiency was received before dismissal because the filer was not an electronic participant in the sealed matter, and that a one-page docket printout

containing the deficiency notation arrived by mail only after the dismissal and September 2 proceedings. The source set establishes that the deficiency existed on the docket; the sworn account raises the different question of when and how the person required to cure it received usable notice. A CAE does not resolve that dispute by assumption. It preserves the generated notice, transmission route, recipient address, delivery event, and source object so the chronology can be tested. **[FN 36] [FN 30] [FN 31]**

The S.D. Florida event therefore should not be reduced either to 'the court dismissed for nonpayment' or to 'the docket was compromised.' The source-native documents establish a more exact field condition: an after-hours sealed emergency cyber-disruption package was physically received; the electronic record appeared three days later; the first assignment entry named a magistrate judge; reassignment, deficiency, and dismissal followed in a short interval; payment and additional emergency materials were presented on September 2; and the court declined to reopen while allowing refiling. The integrity issue is whether the original object, payment state, assignment path, notice state, chambers copy, and sealed-record state were independently authenticated before the ordinary procedural sequence ended the action. **[FN 36] [FN 34]**

That question is precisely bounded. A compressed sequence may have an ordinary administrative explanation. A fee requirement remains enforceable in a cyber-sensitive case. But where the filing itself alleges compromise of legal communications and requests immediate containment, the system should be capable of proving which object was received, when the case was assigned to an Article III judge, what emergency materials were available to chambers, what cure notice was generated and transmitted, and whether the source record remained preserved while those questions were answered. The reviewed record does not show that separate integrity lane. **[FN 30] [FN 34] [FN 36]**

9.3 E.D.N.Y. 25-cv-06033: Filing Identity, Record-State Divergence, and Venue Disposition

The second federal field test was designed around a different jurisdictional proposition. The E.D.N.Y. civil cover sheet identifies an original federal-question proceeding, checks '890 Other Statutory Actions,' cites 18 U.S.C. § 1030(g) and 18 U.S.C. § 1962, and describes the cause as an advanced persistent threat allegedly manipulating judicial cyber-infrastructure and using stolen CM/ECF credentials. It also identifies 23-cv-2447 and Judge Ramon E. Reyes Jr. as the related case. The filed complaint and emergency papers asserted CFAA, ECPA, RICO, All Writs Act, and declaratory or enforcement theories tied to the September 8, 2025 permanent judgment and alleged overlapping or successor infrastructure. **[FN 35] [FN 23]**

That objective filing identity is important because the November 20 clerk-provided docket simultaneously presents a different classification state. Its header lists the cause as '42:1983 Civil Rights Act,' while the same header lists the nature of suit as '890 Other Statutory Actions.' The final December 3 memorandum itself describes claims under the CFAA, ECPA, federal and Florida RICO statutes, and the All Writs Act. The report does not infer intent from the inconsistent labels. It records that the civil cover sheet, docket cause field, nature-of-suit field, complaint, and later order do not describe the action in the same way. In a routine case that

may be a coding error. In a case alleging record-channel compromise, the mismatch becomes a source-state requiring reconciliation. **[FN 35] [FN 34]**

The filing package was also materially larger than the three principal docket entries suggest. The emergency sealing motion described a verified complaint, the September 8 permanent judgment, CNF and Marlin reports, portal-infiltration reports, sworn declarations, and sensitive technical exhibits concerning domains, IP addresses, mail routing, court-facing systems, and alleged victim identities. The final filed November 25 response states that the complaint, sealing application, temporary-restraint papers, and Exhibits A through M comprised approximately 700 pages of material. It further states that substantial exhibits were not present in the accessible record when the response was prepared. These statements identify the size and asserted content of the physical submission; they do not establish what every chambers user actually received. **[FN 35]**

The public docket records the complaint, temporary-restraint motion, and sealing motion as Entries 1 through 3, dated October 28 and entered October 30. It then records a deficient-filing notice on October 29 and a $407 fee receipt dated October 29 but received into the docket by email on November 5. A magistrate-consent notice appears as Entry 5. The chronology shows that several administrative states were created after physical intake and on different dates. That is ordinary enough in a conventional filing environment; it becomes forensically significant only because the filing alleged that the integrity and routing of court objects were part of the attack surface. **[FN 35] [FN 30]**

On November 4, the district judge entered a twelve-page memorandum and order denying the sealing and temporary-restraint requests, directing the clerk to remove the electronic restrictions, and ordering a response by November 10 on whether venue was proper or the matter should be dismissed or transferred to Florida. The order framed the connection to 23-cv-2447 principally through the separate Microsoft litigation and stated that the record then available did not establish the necessary E.D.N.Y. nexus. It also described a limited set of filed materials and, according to the source-native copies and later response, did not have the complete technical exhibit package before it. The report treats those statements as the court's description of its available record, not as proof that the physically delivered package contained only those objects. **[FN 35]**

The next visible directive did not appear as an ordinary numbered document. The November 20 clerk-provided docket contains an 11/18/2025 'SCHEDULING ORDER' stating that the original November 10 deadline had passed and extending the show-cause response date to November 25. The row does not display a docket-entry number comparable to Entries 6 and 7, and no linked PDF is shown in the docket image. The final filed response states that the filer received the docket printout containing that directive on November 20. This is not evidence that the directive was unauthorized. It is evidence that the order, docket-number state, linked-document state, and notice state must be examined separately. **[FN 35] [FN 30] [FN 34]**

The same November 20 docket contains a more consequential record-state notation. Entry 1 states that the main complaint document and its civil-cover-sheet attachment were replaced on November 20. Entry 2 states that the temporary-restraint motion's main document was

replaced. Entry 3 states that the sealing motion's main document was replaced. The filed response contemporaneously called the court's attention to those replacement notations, stated that Exhibits A through E and H through M were not available in the record then reviewed, and asked for clarification of what constituted the court's file. A replacement entry can have an ordinary clerical explanation. But replacement after a dispositive emergency ruling requires preservation of both versions and a record of what changed if the filed, chambers, docket, and public objects are to remain auditable. **[FN 35] [FN 34]**

The final November 25 response controls this report's description of what was actually submitted on venue. It is a twenty-five-page filed paper. It relies on the text of the federal venue statutes, the pleaded New York infrastructure and effects, the asserted factual relationship to 23-cv-2447, and the issuing court's retained authority over the September 8 judgment. It challenges the civil-rights classification, identifies the missing-exhibit and replacement states, and asks the court either to retain the matter or, in the alternative, direct it to the judge who entered the permanent judgment. Earlier drafting versions are not used to restore authorities or propositions consciously removed before filing. **[FN 35]**

The December 3 memorandum and order is then treated as the next procedural object. It identifies the pleaded federal statutes, rejects the asserted E.D.N.Y. venue nexus, concludes that the Microsoft action does not make the cases legally related for venue purposes, and dismisses without prejudice. The order also includes citation-related criticism under a Rule 11 and judicial-integrity framing. This report does not convert Part IX into a collateral citation appeal. It records what the court stated, preserves the filed response that the order addressed, and separates the venue disposition from the unresolved technical question whether the complete physical, docket, chambers, service, and public records were synchronized. **[FN 35]**

A one-page clerk judgment filed December 4 implements that disposition. It states that the complaint is dismissed without prejudice for improper venue and identifies the December 3 memorandum as the basis. The judgment does not purport to decide the infrastructure attribution, the completeness of the original submission, the replacement history, the PageID sequence, or the later-victim use of the 23-cv-2447 mechanism. The source set reviewed for this report contains the filed judgment and a later paper copy, but it does not contain a separate source-native service certificate or mailing record sufficient to establish the exact transmission and receipt path. That absence is reported only as a source-set limitation. **[FN 35]**

The document ribbon supplies a final measurable state. The November 4 order begins at PageID 296. The December 3 order begins at PageID 627. More than three hundred PageID positions therefore intervene between the beginning of those two orders. That numeric progression is not proof that hidden documents were maliciously inserted. It is an auditable record characteristic that must be reconciled against the physical filing package, the replaced docket entries, the exhibits said to be missing, any restricted or sealed objects, and the version available to chambers at each decision point. **[FN 35] [FN 34]**

The E.D.N.Y. field result is consequently more precise than either side of a merits dispute. A physically submitted cyber-sensitive package was converted into an electronic record; the court acted while describing a limited accessible record; the docket later marked the three

principal submissions as replaced; a material classification mismatch appeared among the cover sheet, cause field, nature-of-suit field, and pleaded statutes; an unnumbered scheduling directive extended a deadline; the PageID sequence expanded substantially; and the case ended through a venue dismissal without prejudice. Each event may admit an ordinary explanation. The reviewed record does not supply one integrated audit trail proving that the filer, intake, chambers, docket, service, and public objects remained the same objects throughout. **[FN 30] [FN 34] [FN 35]**

9.3.A The November 2025 Postjudgment Rule 24 / Rule 71 Field Test in 23-cv-2447

The parallel postjudgment filing in 23-cv-2447 deserves separate treatment because it tests the report's State-Four proposition directly. E.D.N.Y. 25-cv-06033 attempted to open a new action tied to the Microsoft judgment. The Rule 24/Rule 71 filing instead asked the issuing court to use the standing architecture already created in that judgment. It therefore presented the exact institutional question raised by the five-year successor mechanism: could a claimed later victim bring newly identified infrastructure into the existing remedial system without rebuilding the original case from the beginning? **[FN 23] [FN 25]**

The filing set was prepared as an emergency postjudgment application. Its physical delivery sheet states that the materials were submitted for immediate chambers review and intended for filing on the docket. It expressly states that no portion of that submission was offered under seal. The package included an emergency motion to intervene and for Rule 71 relief, a verified intervention complaint, a sworn affidavit, a CNF declaration, a proposed order, and Exhibits A through M. The delivery sheet also identified the already-filed Microsoft DCU declarations incorporated from the underlying action. **[FN 25]**

The papers alleged a concrete successor-enforcement problem rather than a generalized interest in the closed case. They asserted that multiple legitimate domains supporting a planned legal publishing and professional-services venture had been placed in clientHold or otherwise made nonresolving, interrupting web and email operations. They further alleged that the event involved DNS and infrastructure patterns associated with the enjoined or successor environment. The requested relief included restoration of the legitimate domains, application or clarification of the permanent judgment, technical coordination with Microsoft DCU and providers, and use of the court's retained jurisdiction and Rule 71 process. Those are allegations and requested remedies contained in verified papers; Part IX does not decide whether the asserted infrastructure satisfied the final order's technical criteria. **[FN 25]**

The importance of Rule 71 in this report is functional. The applicant argued that a nonparty intended to benefit from a court order should be able to invoke the procedure for enforcing it, while Rule 24 supplied an alternative intervention route. Whether that legal theory ultimately would have prevailed is not the field-test endpoint. The endpoint is whether the source record shows a defined process by which the claimed later victim's technical evidence was received, protected, evaluated against the successor criteria, presented to the Court Monitor if appropriate, answered by the original plaintiffs, and resolved in a reviewable order. **[FN 23] [FN 25]**

The source-native docket shows the emergency motion as Entry 61 and the related exhibit filing as Entry 62. Both are dated November 18 and were entered on November 19. A November 19 text or paperless directive then ordered the clerk to remove the ex parte designation, make the motion available to case participants, and directed the plaintiffs to respond by December 5. In the reviewed docket image, that directive appears without a separate visible docket-entry number or linked PDF in the left-hand column. That is a record-state characteristic, not an attribution conclusion. **[FN 24] [FN 74]**

The public lifecycle becomes the substantive measurement. The defined search through September 7, 2026 located no public Microsoft, Fortra, or Health-ISAC response to the application; no public Court Monitor proceeding tied to it; no technical determination stating whether the asserted domains or IP addresses did or did not satisfy the successor criteria; and no later order explaining a provider or enforcement result. The source set reviewed for this report likewise contains no plaintiff response or final disposition of the Rule 24/Rule 71 request. That statement is deliberately bounded: it does not establish that no private response, sealed review, or nonpublic action occurred. It establishes that no reproducible disposition was located in the reviewed record. **[FN 26] [FN 83]**

The service state is also distinct. The docket image proves that the November 19 directive existed in the court's electronic record and set a response deadline. The source set does not contain a separate served copy of that directive, a Notice of Electronic Filing directed to the non-ECF applicant, or a filed response demonstrating what the original plaintiffs received and did. Where verified testimony states that no service or response was received, that remains a witness account rather than a court finding. The proper institutional response is not to select one version by intuition; it is to preserve the directive, service event, recipient list, response object, and disposition as independently auditable states. **[FN 24] [FN 25] [FN 30]**

This is the first located later-victim test of the strongest State-Four architecture in the population. The standing mechanism existed in law. A later-victim applicant physically delivered a detailed invocation. The court removed ex parte treatment and ordered the plaintiffs to respond. The located public and investigative records do not show the technical evaluation or final disposition that followed. A later victim examining that lifecycle therefore cannot determine whether the successor criteria were reached, whether the Court Monitor was engaged, whether plaintiffs evaluated the indicators, whether providers acted, or whether the request failed on a procedural or technical ground. **[FN 23] [FN 25] [FN 74] [FN 83]**

That gap is not a criticism of the permanent injunction's validity. It is a design result. A successor-aware order requires a named intake function, protected evidence-handling rules, an acknowledgment that fixes the object received, a technical triage standard, a method for involving the monitor or plaintiffs, and a disposition that can be communicated without unnecessarily exposing live indicators. Without those elements, the later claimant must improvise an intervention under active-attack conditions and may be unable to tell whether the standing remedy was ever technically engaged. The CAE proposal in Part X is intended to supply that integrity and disposition layer without prejudging whether any asserted successor object qualifies. **[FN 6] [FN 23] [FN 25]**

9.4 Florida Supreme Court: Original-Jurisdiction and Paper-Only Clean-Channel Attempt

The Florida record presents the same circularity in a state supreme court and lawyer-regulation environment, but the report does not retell the underlying disciplinary merits. The relevant chronology is limited to the integrity path. Beginning in December 2024, the source set records physical delivery efforts and requests for protective or in-camera handling. Later communications included instances in which institutional personnel stated that a purported message had not been sent from the office or that another message had been changed, followed by continuing disputes over electronic identity, service, and the route for obtaining a required proceeding transcript. CCDG supplies the technical context: an apparently authorized message path does not by itself establish authentic human intent or an unchanged workflow. **[FN 31] [FN 39]**

By early 2026, the immediate access problem centered on review materials and the transcript path. The verified chronology states that the claimant sought the identity of the court reporter and a usable ordering channel, sent a prepaid return package and transcript payment, and later received a malformed email string containing two '@' symbols rather than a functioning contact address. The report does not treat one malformed address as proof of compromise. It treats it as a consequential chokepoint event because transcript access was necessary to pursue review and because the surrounding source record already contained contested email, identity, and routing events. **[FN 31] [FN 39]**

The February 6, 2026 filing was an attempt to break that circularity through an expressly nonordinary procedure. The source-native first page is captioned 'IN THE SUPREME COURT OF FLORIDA (Original Jurisdiction Proceeding),' leaves the case-number line blank, bears a February 6 received stamp, and is titled 'Petition for Writs of Prohibition, Mandamus and All Writs.' The accompanying emergency motion is independently stamped received and asks for sealing, in-camera review, paper-only and non-digitized handling, delayed service through a court-supervised secure method, and a stay while the asserted integrity concerns were examined. **[FN 39]**

Those requested procedures matter more to this report than the merits requested in the writ. The filing did not merely ask the court to trust a cyber allegation. It asked the court to preserve a source object outside the disputed electronic route, delay ordinary service long enough to prevent disclosure of sensitive indicators, identify a secure communication method, and allow judicial review before digitization and public distribution changed the evidentiary state. In functional terms, it was a proposed Clean Adjudicative Environment before that term was formalized in this report. **[FN 6] [FN 39]**

The intake and disposition sequence is separated by source type. The physical stamps prove that the petition and emergency motion were received on February 6 without a new case number shown on their face. The verified affidavit later states that the filer expressly requested a new original-jurisdiction docket and paper-only handling, and that a deputy clerk advised that the materials would instead be processed electronically in the existing disciplinary matter. The same affidavit states that no written assurance was provided that the court would review the materials before electronic dissemination. Those statements are sworn first-person evidence of the intake exchange, not findings by the Florida Supreme Court. **[FN 39]**

A February 11 clerk-signed order then denied the requests for sealing, in-camera review, paper-only handling, delayed service, and a stay. The verified chronology states that the materials were placed under the existing disciplinary case number and became publicly available, and that counsel for the opposing institution learned of the filing through the ordinary channel before the filer received direct notice of the disposition. Again, the report preserves the distinction: the order establishes the procedural result; the affidavit establishes the witness's account of routing and notice; CCDG and RAPS explain why those states should be compared rather than presumed identical. **[FN 39] [FN 30] [FN 31]**

The Florida event is therefore not included to argue that an original writ should have been granted. It demonstrates what happened when a claimant explicitly asked for a new case number, a paper-only source object, delayed service, and in-camera review because the existing electronic system was itself challenged. The reviewed record does not show that a separate independently auditable intake path was created. The ordinary system absorbed the filing and the requested alternate handling was denied before the asserted integrity evidence received the controlled presentation the motion sought. **[FN 39]**

Later resort to the United States Supreme Court is not the endpoint of this report. A subsequent verified submission may preserve and consolidate sworn chronology, and a clerk's direction to proceed through another filing procedure is materially different from a merits adjudication. But the institutional question had already crystallized in Florida: when the claimant asked a court of last resort to preserve the integrity evidence outside the challenged route, no standardized clean-channel protocol was available in the reviewed record. Part X addresses that systemic gap rather than making appellate persistence the proposed solution. **[FN 39]**

9.5 D.D.C. 1:25-cv-04308: Controlled-Evidence-Path Request and the Filed/Unfiled Boundary

The D.D.C. action reframed the integrity issue at the level of national judicial infrastructure. The filed verified complaint named unknown Doe defendants together with institutional entities associated with federal and Florida filing systems. It alleged compromise of federal CM/ECF and related intranet or legacy-server pathways, invoked the CFAA, ECPA, RICO, and All Writs Act, and connected the asserted technical environment to the September 8, 2025 E.D.N.Y. permanent judgment. For Part IX, those allegations establish the purpose and scope of the filing; they are not treated as adjudicated facts. **[FN 40]**

The March 2, 2026 emergency motion is the clearest federal precursor to CAE because it requested a controlled evidentiary path rather than immediate acceptance of the final attribution theory. The filed motion stated that the claimant had traveled to the courthouse with nonpublic technical evidence and asked for an immediate ex parte, in-camera hearing. It represented that ordinary filing could risk exfiltration, suppression, alteration, or premature disclosure, and requested authority to hand CNF, Marlin, RAPS, CCDG, and related physical reports directly to the court before they moved through ordinary service and public-docket channels. **[FN 40]**

The requested relief was procedurally specific. The motion asked the court to receive technical details and law-enforcement-related information orally and in physical form; maintain any transcript and submitted material under seal; prevent ordinary intake or public routing until

the court selected handling protocols; and, if appropriate, invite the Administrative Office of the U.S. Courts, Microsoft DCU, or other relevant federal participants into a court-supervised session. The request thus sought a judicially controlled bridge from physical evidence to ordinary process, not a permanent exemption from service or adversarial review. **[FN 40]**

The D.D.C. source boundary must remain absolute. The March 2 emergency motion was filed and may be described as a court-received request. The separate March 3 supplemental or protective-order draft was intentionally not filed. It may identify chronology, concerns, or proposed procedures for investigative purposes, but it cannot be described as received, considered, rejected, or adjudicated by the court. That distinction is not editorial caution alone. It is the same provenance rule the CAE would institutionalize: the source object and every material derivative must retain an authenticated status. **[FN 40]**

The report also does not rely on unsworn recollection of courthouse conversations to enlarge the filed record. If a contemporaneous verified statement, clerk receipt, docket entry, or order independently records an instruction or communication, that source may be evaluated on its own terms. Otherwise, the field result remains what the filed motion proves: after multiple prior attempts to use ordinary and physical court channels, the claimant expressly asked a federal court for live in-camera access and direct physical evidence delivery because the ordinary intake and service environment was disputed. **[FN 40]**

D.D.C. therefore completes the progression from anomaly reporting to procedural design. S.D. Florida tested whether an emergency infrastructure action could survive ordinary intake long enough for technical review. E.D.N.Y. tested synchronization among a large physical submission, chambers access, replacement entries, service, and public record. The Rule 71 application tested access to a standing successor mechanism. Florida tested a paper-only original-jurisdiction request. D.D.C. then articulated the desired solution directly: preserve the sensitive evidence, put it before a judge through a controlled path, and decide how to return it safely to ordinary process. **[FN 35] [FN 36] [FN 39] [FN 40]**

9.6 Cross-Jurisdiction Synthesis: Recurrent Record-State Failure Without a Standard Integrity Lane

The four systems did not produce the same procedural event. S.D. Florida produced an after-hours intake, initial magistrate-assignment state, later district-judge reassignment, deficiency, dismissal, payment, and denied reconsideration. E.D.N.Y. 25-cv-06033 produced an under-seal physical package, a limited-record emergency ruling, conflicting classification fields, later replacement notations, an unnumbered scheduling directive, a substantial PageID progression, and dismissal without prejudice for venue. The separate 23-cv-2447 track produced a postjudgment Rule 24/Rule 71 filing and an order for plaintiff response without a located public technical disposition. Florida produced an original-jurisdiction paper-only request that was routed through the existing proceeding and denied alternate handling. D.D.C. produced a filed request for direct in-camera presentation. **[FN 25] [FN 35] [FN 36] [FN 39] [FN 40]**

Those outcomes share no single judge, clerk, court, filing platform, local rule, or stated procedural ground. The recurring feature is architectural: the claimant attempted to raise an integrity-of-channel problem, but the reviewed records do not show a standardized

independent process that first fixed and authenticated the submitted object, intake state, assignment or routing state, chambers copy, docket object, service state, recipient copy, and public derivative before ordinary consequences attached. In each setting, the institution's usual path remained the path through which the challenge to that path had to travel. **[FN 30] [FN 31] [FN 34]**

The recurrence is significant without being converted into a statistical claim. The report does not possess a defined national denominator for every sealed filing, unnumbered paperless order, replacement event, delayed notice, magistrate-assignment state, or original-jurisdiction intake decision. It therefore does not assign a probability or statistical significance to the cluster. It identifies a cumulative anomaly pattern across independent adjudicative systems and asks the narrower engineering question: could each disputed state be reproduced and authenticated from preserved logs and source objects? Where the answer is unavailable, the integrity issue remains unresolved rather than being decided by confidence in either the claimant or the system. **[FN 30] [FN 34]**

The same discipline protects institutional actors. A clean-channel protocol does not presume that a judge authored a counterfeit order, that a clerk manipulated a docket, that a law firm suppressed a response, or that every missing document resulted from intrusion. It gives judges, clerks, counsel, providers, and parties a defensible method to prove what occurred. Hashing and preserving the physical or electronic source, recording every derivative, logging access and replacement, authenticating the filer and receiving function, confirming critical notices through a second channel, and generating a reviewable integrity disposition can exonerate ordinary administration as readily as it can expose interference. **[FN 6] [FN 30] [FN 31]**

The field record also demonstrates why paper alone is not enough. A document can be hand-delivered and then immediately scanned, assigned, routed, served, and published through the same challenged environment. Unless the original is preserved and the transformation is auditable, only the first transport step changed. The February 6 Florida motion and March 2 D.D.C. motion were more sophisticated: they sought paper-only or direct in-camera custody, delayed service, and court-selected handling protocols before ordinary digitization. Their requests supply a practical design basis for the CAE rather than a general demand for exceptional access. **[FN 39] [FN 40]**

The Part IX conclusion is therefore institutional and limited. The proceedings do not prove that every adverse procedural event was caused by cyber interference. They do prove that materially disputed filing, routing, service, identity, docket, and record-custody states arose in cases seeking cyber-sensitive relief, and that the reviewed records do not expose a uniform independent integrity lane capable of resolving those disputes before the procedural lifecycle moved forward. The absence of that lane creates circularity: the output of the challenged system becomes the evidence that the challenged system operated correctly. **[FN 30] [FN 31] [FN 34] [FN 35] [FN 36] [FN 39] [FN 40]**

Part X follows directly from that result. A Clean Adjudicative Environment is not a private merits route, an assumption that a cyber allegation is true, or a substitute for ordinary filing and service. It is a narrowly triggered integrity process that preserves the source object,

authenticates the submitting and receiving functions, permits known-clean technical review, controls disclosure long enough to prevent irreversible consequences, and then reconciles the verified record back into ordinary adversarial procedure. The field tests show why that bridge is necessary; the next Part specifies how it can be built. **[FN 6] [FN 30] [FN 31] [FN 34]**

PART X - cAPTure-to-Kill, Clean Adjudicative Environment, and Institutional Response

The preceding Parts converge on an institutional design problem. Civil cyber-disruption works by moving trustworthy evidence through counsel, experts, courts, providers, service and publication channels quickly enough to change technical state before the adversary adapts. cAPTure-to-Kill targets the same chain in reverse. The response must therefore protect the integrity of the channel without abandoning electronic courts, relaxing merits standards, or creating an unrestricted private route to judges.

10.1 Counter-disruption finding

The counter-disruption finding is architecture-based. The thirty-five cases show the sequence required to obtain and execute civil cyber relief. The public threat record shows how valid sessions, cloud roles, OAuth and device-code workflows, DNS administration, disposable infrastructure, access brokers, and service economies can be used to observe or influence that sequence. The expert rails identify corresponding subject-side manifestations at endpoint, identity, DNS, mail, portal, docket, persona, and publication levels. The 23-cv-2447 order supplies the strongest located successor mechanism, and the November 2025 field test supplies a concrete later-access record. **[FN 23] [FN 25] [FN 27] [FN 30] [FN 31] [FN 41] [FN 42]**

Counter-disruption does not require the adversary to prevent every order. The operator may lose listed domains and preserve customer accounts, tokens, payment paths, or rebuilt cloud assets. A docket object may exist while service, publication, or later technical review is degraded. A permanent injunction may remain valid while successor infrastructure is difficult to submit or adjudicate. The common effect is reduction of the remedy's timing, visibility, continuity, implementation, or later use.

10.2 Reusable litigation-interference capability

The capability is reusable because the control points are not unique to a botnet operator. Valid sessions, mailbox rules, cloud roles, service principals, DNS authority, provider-contact substitution, publication controls, and credential-backed professional identities can be obtained or sold by access brokers and service providers for different objectives. The report states that proposition at the capability level. It does not conclude that one person, customer, or crew controlled every event. **[FN 33] [FN 41] [FN 42] [FN 43] [FN 45]**

Existing civil cyber precedent can operate as a force multiplier when the standing order already reaches qualifying successor infrastructure. A later victim should not have to reproduce years of technical and legal architecture merely to ask whether newly discovered infrastructure falls within an existing permanent injunction. That advantage depends on a known intake path, secure evidence handling, a review function, and a disposition that can be communicated without exposing the evidence through the disputed channel. **[FN 23] [FN 25]**

Paper alone does not create independence. If the original is immediately scanned, assigned, routed, served, and adjudicated through the same challenged environment before its source state is preserved and compared, only the first transport step changed. The integrity determination remains circular. **[FN 30] [FN 31] [FN 34]**

10.3 Clean Adjudicative Environment

A Clean Adjudicative Environment is an integrity lane, not a merits lane. Courts are not asked to accept every cyber allegation, suspend ordinary procedure indefinitely, or provide secret access on demand. The trigger is credible threshold evidence materially placing filing, service, identity, routing, notice, record custody, or another adjudicative channel in dispute. The first task is to authenticate what was submitted, what was received, where it traveled, and what may be safely disclosed before irreversible consequences attach. **[FN 6] [FN 30] [FN 31]**

Federal Highly Sensitive Document procedures demonstrate that courts already use non-CM/ECF handling for some materials whose confidentiality requires special treatment. **[FN 6]** CAE addresses a different condition: the integrity of the intake and communication path itself. It therefore requires an independently authenticated public contact point, a cyber-integrity incident identifier separate from the merits docket, controlled paper or encrypted-media intake, preservation of the original before scanning, and known-clean review by designated personnel.

The original object and each material derivative should be recorded as separate states. Hash values and chain-of-custody records can identify the filer, intake, chambers, docket, service, recipient, public, and repository copies where applicable. Critical notices and provider instructions can be confirmed through a second channel. Logs preserve who accessed or changed the material. A short, reviewable protection can prevent deadline, default, or disclosure consequences while the integrity question is examined. **[FN 30] [FN 31]**

A judge remains in control of the transition back to ordinary process. Once the verified object and safe service path are established, the court reconciles the record into CM/ECF, authorizes appropriate disclosure, and resumes the ordinary adversarial sequence. The procedure neither determines liability nor guarantees relief. It ensures that the merits are decided from an authenticated record rather than from the untested output of the disputed channel.

Standing cyber injunctions require a related later-victim path. The issuing court or monitor should publish a defined method for receiving successor evidence, preserving confidentiality during technical review, applying the order's criteria, and issuing a reviewable disposition. A later victim or investigator can then invoke the existing remedy without improvising under active-attack conditions or exposing sensitive indicators through the service, filing, or publication path alleged to be compromised. **[FN 23] [FN 25]**

10.4 Final determination

Civil cyber-disruption remains one of the most effective legal mechanisms available against anonymous, distributed, and cross-border malicious infrastructure. Its distinctive power comes from converting verified technical evidence into enforceable commands that change infrastructure state before the adversary can adapt. Waledac, Rustock, Zeus, Citadel, TrickBot, ZLoader, cracked Cobalt Strike, and the modern service cases demonstrate the continuing value of that model. **[FN 7] [FN 8] [FN 9] [FN 10] [FN 11] [FN 23] [FN 58]**

The same history identifies the exposure. The remedy depends on counsel communications, expert evidence, cloud identity, DNS and mail, sealed filing, intake, docketing, service, provider implementation, publication, final relief, and later enforcement. Those functions are increasingly integrated, observable, and dependent on valid accounts and ordinary-looking administrative actions. The cAPTure-to-Kill model describes the adversarial use of those

trusted control planes to reduce the remedy's practical effect without requiring control of every component or attribution of every event to one actor.

The institutional recommendation is an upgrade to electronic adjudication, not an attack on it. A court that can receive cyber-sensitive integrity evidence through a known-clean path, preserve the source object, authenticate custody and routing, control service, obtain technical review, and reconcile the verified record back into ordinary procedure is harder to manipulate and easier to trust. The same design protects plaintiffs, defendants, judges, clerks, providers, later victims, and the public record. **[FN 6] [FN 30] [FN 31]**

The final conclusion is therefore direct. Civil cybercrime litigation has matured into a lawful cyber-containment system. Its durable future depends on protecting the channels through which that system is invoked and enforced. Where credible evidence places those channels in dispute, an auditable out-of-band integrity path is necessary to preserve judicial eyes on an authentic record before digitization, routing, service, or publication determines the practical outcome.

Integrated Evidentiary Compendium / Appendices

Appendix A - Thirty-Five Verified Case Packets

This compendium preserves the standardized case data separately from the narrative. Each packet identifies the case anchor before any operation nickname, then records the technical and procedural contribution to the study. The entries are designed for reproducibility and are not a substitute for the narrative findings in Parts I-X.

A.1 Microsoft Corporation, Fortra, LLC, and Health-ISAC, Inc. v. John Does 1-16, No. 1:23-cv-02447 (E.D.N.Y.) - cracked Cobalt Strike

Case-pedigree field	Verified value
Caption / court / filing	E.D.N.Y. No. 1:23-cv-02447; filed Mar. 30, 2023; Judge Ramon E. Reyes Jr. and Magistrate Judge Lara K. Eshkenazi/Eshkenazi docket sequence. **[FN 16] [FN 26]**
Plaintiffs / counsel	Microsoft, Fortra and Health-ISAC; outside counsel Crowell & Moring. **[FN 16]**
Defendants / actor labels	John Does 1-16 associated with Conti, LockBit, DEV-0193, DEV-0206, DEV-0237, DEV-0243 and DEV-0504. **[FN 26]**
Technical target	Cracked Cobalt Strike beacons, team servers, C2 domains/IPs, access-broker/ransomware service lineages. **[FN 17] [FN 18] [FN 19] [FN 20]**
Relief / disposition	Emergency relief in 2023; default judgment and permanent injunction Sept. 8, 2025; jurisdiction retained until no earlier than Jan. 1, 2030. **[FN 26]**
Operational field	**Analysis**
Claims / authority	CFAA, trademark/copyright/unfair competition theories, All Writs Act implementation. **[FN 16] [FN 26]**
Sworn method	Coy, Lyons, Erdman, Fiñones, Gross and Weiss supplied complementary infrastructure, sample, product, technical and sector-harm evidence. **[FN 17] [FN 18] [FN 19] [FN 20] [FN 21] [FN 22]**
Technical execution	Initial disruption publicly reported in 2023; later final order converted preliminary/supplemental restraints into permanent infrastructure control. **[FN 13] [FN 14] [FN 26]**
Durable / State Four	Strongest located successor mechanism: Court Monitor, domain/IP criteria, nonparty request path, retained jurisdiction until 2030. **[FN 26]**
Visibility / aftermath	Launch-stage publicity substantial; defined post-Sept. 8 search found legal-repository final-order visibility but zero independent party/counsel/named-expert/major-media explanation of the final judgment or Nov. 2025 Rule 71 use through Sept. 7, 2026. **[FN 83]**

A.2 Google LLC v. Dmitry Starovikov et al., No. 1:21-cv-10260 (S.D.N.Y.) - Glupteba

Case-pedigree field	Verified value
Caption / court / filing	S.D.N.Y. No. 1:21-cv-10260; filed Dec. 2021 by Google against named and Doe Glupteba operators. **[FN 86]**
Plaintiff / counsel	Google, with outside and in-house counsel as reflected in pleadings. **[FN 86]**
Technical target	Glupteba malware, C2 proxies, domains, accounts, and blockchain fallback. **[FN 86]**
Relief / disposition	Emergency civil RICO/CFAA and infrastructure relief; later contested/default and restoration/return history in public docket. **[FN 86]**
Analytical role	Original comparator for botnet plus fallback architecture.

Case-pedigree field	Verified value
Operational field	**Analysis**
Claims / authority	CFAA, RICO, trademark and related claims in the civil cyber-disruption lineage. **[FN 86]**
Sworn method	Google threat-analysis evidence and declarant testimony concerning malware, proxies and Google-service abuse. **[FN 86]**
Technical execution	Initial infrastructure action occurred, but Glupteba also demonstrated operator rebuilding pressure. **[FN 86]**
Durable / State Four	Initial authority and execution were strong; durability was contested by documented operator rebuilding and blockchain-assisted fallback; no general later-victim intake mechanism was located. **[FN 86]**
Forensic contribution	Shows that a botnet can combine conventional infrastructure with hidden or decentralized fallback, forcing civil remedies to address regeneration.

A.3 Sophos Ltd. v. John Does 1-2, No. 1:20-cv-00502 (E.D. Va.)

Case-pedigree field	Verified value
Caption / court / filing	E.D. Va. civil action filed May 1, 2020 by Sophos. **[FN 89]**
Plaintiff / counsel	Sophos Ltd.; technical and counsel declarations in emergency record. **[FN 89]**
Technical target	Attack infrastructure directed at Sophos systems and domains. **[FN 89]**
Relief / disposition	Sealed emergency domain/provider relief and later procedural history. **[FN 89]**
Analytical role	Original comparator showing a security-vendor target and emergency relief.
Operational field	**Analysis**
Claims / authority	CFAA/trademark/computer-abuse and equitable relief theories as pleaded. **[FN 89]**
Sworn method	Sophos technical declarations and counsel evidence concerning domain/provider implementation. **[FN 89]**
Technical execution	Emergency relief targeted domains/providers rather than damages alone. **[FN 89]**
Durable / State Four	No entered permanent final infrastructure order was located through Sept. 7, 2026; no successor/monitor/later-victim mechanism comparable to 23-cv-2447 was located. **[FN 89]**
Forensic contribution	Shows that defenders themselves can become targets, making counsel/expert channels part of the operational surface.

A.4 DXC Technology Co. v. John Does 1-2, No. 1:20-cv-00814 (E.D. Va.)

Case-pedigree field	Verified value
Caption / court / filing	E.D. Va. action filed July 20, 2020 by DXC Technology. **[FN 90]** **[FN 90]**
Plaintiff / counsel	DXC Technology; Crowell & Moring and technical declarant Mark Hughes in the source set. **[FN 90]**
Technical target	Cobalt Strike BEACON, rotating domains, Cloudflare reverse proxying, backdoors and ransomware path. **[FN 90]**
Relief / disposition	Emergency domain/provider relief plus default/permanent-injunction motion and R&R located; no separately entered final permanent order located through Sept. 7, 2026. **[FN 90]**
Analytical role	Original comparator for Cobalt Strike/reverse-proxy/malware chain before 23-cv-2447.
Operational field	**Analysis**
Claims / authority	CFAA, trademark and related equitable relief theories. **[FN 90]**

Case-pedigree field	Verified value
Sworn method	Mark Hughes declaration supplies technical analysis of Cobalt Strike BEACON and rotating infrastructure. **[FN 90]**
Technical execution	Provider/domain action framed as urgent relief against live C2. **[FN 90]**
Durable / State Four	State Three remains unresolved at cutoff because the entered final permanent order was not separately located; no public later-victim successor path was located. **[FN 90]**
Forensic contribution	Links Cloudflare/reverse-proxy and Cobalt Strike infrastructure into the studied civil-remedy lineage.

A.5 Microsoft Corp. v. John Does 1-27, No. 1:10-cv-00156 (E.D. Va.) - Waledac / Operation b49

Case-pedigree field	Verified value
Caption / court / filing	E.D. Va.; filed Feb. 22, 2010. **[FN 7]**
Plaintiff / counsel	Microsoft; DCU/legal team. **[FN 7]**
Technical target	Waledac botnet command domains. **[FN 7]**
Relief / disposition	Ex parte TRO against 277 domains; final Oct. 27, 2010 domain transfer. **[FN 7]**
Analytical role	Birth of registry-level civil botnet disruption.
Operational field	**Analysis**
Claims / authority	Civil computer/trademark/equitable theories translated into registry commands. **[FN 7]**
Method	Domain list and registry-level control point. **[FN 7]**
Technical execution	Registry action severed domain resolution to C2. **[FN 7]**
Durable / State Four	Permanent domain transfer; limited successor mechanism compared to later cases. **[FN 7]**
Forensic contribution	Shows speed/secrecy/neutral intermediary as civil-disruption core.

A.6 Microsoft Corp. v. John Does 1-11, No. 2:11-cv-00222 (W.D. Wash.) - Rustock / Operation b107

Case-pedigree field	Verified value
Caption / court / filing	W.D. Wash.; filed Feb. 2011. **[FN 8]**
Plaintiff / counsel	Microsoft. **[FN 8]**
Technical target	Rustock command servers, hard-coded IPs and domains. **[FN 8]**
Relief / disposition	Coordinated server seizure/imaging in March 2011; later order removing domains/IPs from defendants. **[FN 8]**
Analytical role	Physical server seizure model.
Operational field	**Analysis**
Claims / authority	Court-authorized provider and physical execution. **[FN 8]**
Method	Hosting-location identification, server seizure, forensic imaging, traffic observation. **[FN 8]**
Technical execution	Strong; servers and IP communication paths disrupted. **[FN 8]**
Durable / State Four	Durable suppression strong; later-victim path limited. **[FN 8]**
Forensic contribution	Shows domain relief fails if hard-coded infrastructure remains untouched.

A.7 Microsoft Corp., FS-ISAC, Inc. and NACHA v. John Does 1-39, No. 1:12-cv-01335 (E.D.N.Y.) - Zeus / Operation b71

Case-pedigree field	Verified value
Caption / court / filing	E.D.N.Y.; filed Mar. 2012. **[FN 9]**
Plaintiffs / counsel	Microsoft, FS-ISAC and NACHA. **[FN 9]**
Technical target	Zeus financial crimeware, C2 servers, domains and mule/service infrastructure. **[FN 9]**
Relief / disposition	Server seizure at U.S. hosting sites; roughly 800 domains monitored/taken over. **[FN 9]**
Analytical role	Civil RICO enterprise model for modular cybercrime.
Operational field	**Analysis**
Claims / authority	Civil RICO plus computer/trademark relief. **[FN 9]**
Method	Sector-victim evidence, hosting/domain identification, enterprise-role theory. **[FN 9]**
Technical execution	C2 seizure and domain control occurred. **[FN 9]**
Durable / State Four	Domains disabled and evidence referred; limited successor mechanism. **[FN 9]**
Forensic contribution	Introduces service-provider/customer/enterprise structure later mirrored in PhaaS/MaaS/RaaS cases.

A.8 Microsoft Corp. v. John Does 1-82, No. 3:13-cv-00319 (W.D.N.C.) - Citadel

Case-pedigree field	Verified value
Caption / court / filing	W.D.N.C.; filed May/June 2013. **[FN 10]**
Plaintiff / counsel	Microsoft with industry/law-enforcement coordination. **[FN 10]**
Technical target	Citadel botnets, domains and C2. **[FN 10]**
Relief / disposition	Civil seizure/disruption of more than 1,000 botnets/domains; Nov. 21, 2013 default judgment/permanent injunction. **[FN 10]**
Analytical role	Curative sinkhole and victim-remediation architecture.
Operational field	**Analysis**
Claims / authority	Court-ordered registry/registrar/domain transfer and curative server control. **[FN 10]**
Method	Domain/botnet identification, server/provider action, victim notification. **[FN 10]**
Technical execution	Strong initial execution and permanent domain/control terms. **[FN 10]**
Durable / State Four	Durable control strong; successor/later-victim path less explicit than 23-cv-2447. **[FN 10]** **[FN 26]**
Forensic contribution	Shows a court can redirect hostile traffic into a defender-controlled remediation environment.

A.9 Microsoft Corp. v. John Does 1-2, No. 1:17-cv-01224 (E.D. Va.) - Barium / Brass Typhoon

Case-pedigree field	Verified value
Caption / court / filing	E.D. Va.; filed Oct. 26, 2017. **[FN 59]**
Plaintiff / counsel	Microsoft; Alston & Bird and in-house counsel reflected in public source set. **[FN 59]**
Technical target	Barium/Brass Typhoon spearphishing, Barlaiy/PlugX RATs, fake profiles, dead-drop resolver text. **[FN 59]**

Case-pedigree field	Verified value
Relief / disposition	TRO, preliminary injunction, default/permanent injunction; continuing monitor process. **[FN 59]**
Analytical role	Nation-state portfolio and account/profile disruption.
Operational field	**Analysis**
Claims / authority	Domain/profile/account control plus trademark/computer relief. **[FN 59]**
Method	Profile/dead-drop and malware C2 decoding evidence. **[FN 59]**
Technical execution	Domains/profiles transferred or redirected. **[FN 59]**
Durable / State Four	Stronger than early cases because later infrastructure could be reached through continuing process. **[FN 59]**
Forensic contribution	Shows adversary reliance on legitimate platform content as command locator.

A.10 Microsoft Corp. v. John Does 1-2, No. 1:19-cv-00716 (D.D.C.) - Phosphorus / Charming Kitten

Case-pedigree field	Verified value
Caption / court / filing	D.D.C.; filed Mar. 2019. **[FN 60]**
Plaintiff / counsel	Microsoft. **[FN 60]**
Technical target	Phosphorus/Charming Kitten phishing domains and fake login infrastructure. **[FN 60]**
Relief / disposition	Court order enabled Microsoft to take control of 99 websites and sinkhole traffic. **[FN 60]**
Analytical role	Nation-state credential-theft domain portfolio.
Operational field	**Analysis**
Claims / authority	Trademark/computer claims and domain seizure/sinkhole relief. **[FN 60]**
Method	Threat-intelligence and domain-infrastructure mapping. **[FN 60]**
Technical execution	Control of 99 websites reported. **[FN 60]**
Durable / State Four	Continuing use of actions against later infrastructure reported, but final later-victim path is not equivalent to 23-cv-2447. **[FN 60]**
Forensic contribution	Shows credential theft as primary objective of civil disruption.

A.11 WhatsApp Inc. and Facebook, Inc. v. NSO Group Technologies Ltd., No. 4:19-cv-07123 (N.D. Cal.)

Case-pedigree field	Verified value
Caption / court / filing	N.D. Cal.; filed Oct. 29, 2019. **[FN 61]**
Plaintiffs / counsel	WhatsApp and Facebook/Meta. **[FN 61]**
Defendants	NSO Group and Q Cyber Technologies. **[FN 61]**
Technical target	Spyware service, platform abuse and account/device targeting. **[FN 61]**
Relief / disposition	Liability rulings and later damages/injunctive litigation events in public docket. **[FN 61]**
Operational field	**Analysis**
Claims / authority	CFAA and platform/service abuse theories. **[FN 61]**
Method	Platform telemetry and unauthorized access evidence. **[FN 61]**
Technical execution	Litigation did not operate like a registry botnet seizure; it is a platform/spyware control comparator. **[FN 61]**

Case-pedigree field	Verified value
Durable / State Four	Relief depends on injunction/damages posture, not classic sinkhole control. **[FN 61]**
Forensic contribution	Shows platform account/device targeting and commercial spyware as civil cyber-litigation subject.

A.12 Apple Inc. v. NSO Group Technologies Ltd., No. 3:21-cv-09078 (N.D. Cal.)

Case-pedigree field	Verified value
Caption / court / filing	N.D. Cal.; filed Nov. 23, 2021. **[FN 61]**
Plaintiff / counsel	Apple. **[FN 61]**
Defendants	NSO Group and related entity. **[FN 61]**
Technical target	Pegasus/spyware abuse of Apple users and infrastructure. **[FN 61]**
Relief / disposition	Apple later voluntarily dismissed, citing changed circumstances and threat-intelligence exposure concerns. **[FN 61]**
Operational field	**Analysis**
Claims / authority	Computer/platform and equitable claims. **[FN 61]**
Method	Platform-threat intelligence and exploit ecosystem evidence. **[FN 61]**
Technical execution	No classic infrastructure sinkhole in located record. **[FN 61]**
Durable / State Four	Dismissal prevents durable civil-disruption assessment. **[FN 61]**
Forensic contribution	Shows litigation itself can risk exposing sensitive threat-intelligence.

A.13 Microsoft Corp. v. John Does 1-10, No. 1:22-cv-01328 (N.D. Ga.) - ZLoader

Case-pedigree field	Verified value
Caption / court / filing	N.D. Ga.; filed Apr. 2022. **[FN 58]**
Plaintiff / counsel	Microsoft and partners reflected in notice materials. **[FN 58]**
Technical target	ZLoader hard-coded domains and DGA-generated domains. **[FN 58]**
Relief / disposition	Court order transferred 65 hard-coded domains and 319 registered DGA domains; future DGA blocking/sinkholing. **[FN 58]**
Analytical role	Successor-aware DGA remedy.
Operational field	**Analysis**
Claims / authority	Computer/trademark/equitable relief plus DGA future-domain logic. **[FN 58]**
Method	Malware reverse engineering and DGA prediction/registration control. **[FN 58]**
Technical execution	Strong; domains transferred to Microsoft sinkholes. **[FN 58]**
Durable / State Four	Stronger successor architecture than early static domain cases. **[FN 58]**
Forensic contribution	Shows future generated infrastructure can be preemptively addressed.

A.14 Microsoft Corp. v. John Does 1-2, No. 1:22-cv-00607 (E.D. Va.) - Bohrium / Smoke Sandstorm

Case-pedigree field	Verified value
Caption / court / filing	E.D. Va.; filed May 31, 2022. **[FN 62]**
Plaintiff / counsel	Microsoft. **[FN 62]**

Case-pedigree field	Verified value
Technical target	Bohrium/Smoke Sandstorm malicious domains and preservation targets. **[FN 62]**
Relief / disposition	Domain-disabling/preservation relief followed by Jan. 30, 2024 default judgment and permanent injunction. **[FN 62]** **[FN 85]**
Analytical role	Nation-state domain-portfolio comparator showing the progression from emergency disabling to durable final relief.
Operational field	**Analysis**
Claims / authority	Civil domain/platform relief. **[FN 62]**
Method	Threat-intelligence domain attribution and control-point evidence. **[FN 62]**
Technical execution	Court-authorized disabling/preservation. **[FN 62]**
Durable / State Four	Durable final relief located; no separate public nonparty/later-victim procedure comparable to 23-cv-2447 was located. **[FN 85]**
Forensic contribution	Shows standardized nation-state domain restraint by 2022.

A.15 Microsoft Corporation and FS-ISAC, Inc. v. John Does 1-2, No. 1:20-cv-1171 (E.D. Va.) - TrickBot

Case-pedigree field	Verified value
Caption / court / filing	E.D. Va. No. 1:20-cv-1171; public notice Oct. 12, 2020. **[FN 11]**
Plaintiffs / counsel	Microsoft and FS-ISAC. **[FN 11]**
Technical target	TrickBot C2 IP addresses, content, service providers and malware-control infrastructure. **[FN 11]**
Relief / disposition	Court-approved disabling of IP addresses and content, suspension of services and preservation; continuing public reporting of revival/adaptation pressure. **[FN 11]**
Analytical role	Corrected representative botnet case replacing non-representative field material.
Operational field	**Analysis**
Claims / authority	CFAA, copyright and related equitable relief; copyright theory applied to malicious use of Microsoft code. **[FN 11]**
Method	Precise IP identification from infected computers communicating with C2. **[FN 11]**
Technical execution	Providers ordered to disable access and prevent new server leasing/use. **[FN 11]**
Durable / State Four	Important but contested durability because TrickBot revival attempts were anticipated and reported. **[FN 11]**
Forensic contribution	Shows court remedy used during election-risk period and demonstrates adversarial regeneration as expected behavior.

A.16 Microsoft Corp. and NGO-ISAC v. John Does, No. 1:24-cv-02719 (D.D.C.) - Star Blizzard / ColdRiver

Case-pedigree field	Verified value
Caption / court / filing	Microsoft Corp. and NGO-ISAC v. John Does, No. 1:24-cv-02719 (D.D.C.) - Star Blizzard / ColdRiver. **[FN 57]**
Plaintiff / counsel	Microsoft and NGO-ISAC; counsel verified from case source set where publicly available. **[FN 57]**
Technical target	nation-state spearphishing domains. **[FN 57]**
Relief / disposition	TRO/domain seizure and parallel DOJ seizure followed by Aug. 5, 2026 default judgment and permanent injunction. **[FN 57]** **[FN 84]**

Case-pedigree field	Verified value
Analytical role	Nation-state spearphishing/domain-portfolio comparator with parallel civil and DOJ infrastructure action.
Operational field	**Analysis**
Claims / authority	Case-specific statutory and equitable claims verified from complaint/order set. **[FN 57]**
Sworn/expert method	Technical or platform evidence identified in the case source set; exact declarant details preserved in source register. **[FN 57]**
Technical execution	Recorded as executed where court/provider/party public source verifies implementation; otherwise coded as authority without assuming completion. **[FN 57]**
Durable / State Four	Durable permanent relief located; continuing-domain architecture remains plaintiff/provider-facing rather than a general later-victim intake mechanism. **[FN 84]**
Forensic contribution	Shows the migration of civil remedies from static botnet servers to domains, accounts, services, identities, cloud paths, and platform control points. **[FN 57]**

A.17 Microsoft Corp. and LF Projects, LLC v. Abanoub Nady a/k/a MRxC0DER et al., No. 1:24-cv-02013 (E.D. Va.) - Fake ONNX

Case-pedigree field	Verified value
Caption / court / filing	Microsoft Corp. and LF Projects, LLC v. Abanoub Nady a/k/a MRxC0DER et al., No. 1:24-cv-02013 (E.D. Va.) - Fake ONNX. **[FN 50]**
Plaintiff / counsel	Microsoft and LF Projects; counsel verified from case source set where publicly available. **[FN 50]**
Technical target	AI-themed phishing-as-a-service domains and pages. **[FN 50]**
Relief / disposition	TRO/PI; approximately 240 sites disrupted/redirected. **[FN 50]**
Analytical role	Representative civil cybercrime or platform/service-control comparator in the 35-case population.
Operational field	**Analysis**
Claims / authority	Case-specific statutory and equitable claims verified from complaint/order set. **[FN 50]**
Sworn/expert method	Technical or platform evidence identified in the case source set; exact declarant details preserved in source register. **[FN 50]**
Technical execution	Recorded as executed where court/provider/party public source verifies implementation; otherwise coded as authority without assuming completion. **[FN 50]**
Durable / State Four	Assessed by final order, settlement, dismissal, permanent injunction, continuing-provider mechanism, or absence. **[FN 50]**
Forensic contribution	Shows the migration of civil remedies from static botnet servers to domains, accounts, services, identities, cloud paths, and platform control points. **[FN 50]**

A.18 Microsoft Corp. v. John Does associated with Lumma Stealer, No. 1:25-cv-02695 (N.D. Ga.) - Lumma

Case-pedigree field	Verified value
Caption / court / filing	Microsoft Corp. v. John Does associated with Lumma Stealer, No. 1:25-cv-02695 (N.D. Ga.) - Lumma. **[FN 49]**
Plaintiff / counsel	Microsoft; counsel verified from case source set where publicly available. **[FN 49]**
Technical target	infostealer domains, panels and service infrastructure. **[FN 49]**

Case-pedigree field	Verified value
Relief / disposition	May 2025 order; about 2,300 domains seized/blocked/suspended; 1,300+ sinkholed. **[FN 49]**
Analytical role	Representative civil cybercrime or platform/service-control comparator in the 35-case population.
Operational field	**Analysis**
Claims / authority	Case-specific statutory and equitable claims verified from complaint/order set. **[FN 49]**
Sworn/expert method	Technical or platform evidence identified in the case source set; exact declarant details preserved in source register. **[FN 49]**
Technical execution	Recorded as executed where court/provider/party public source verifies implementation; otherwise coded as authority without assuming completion. **[FN 49]**
Durable / State Four	Assessed by final order, settlement, dismissal, permanent injunction, continuing-provider mechanism, or absence. **[FN 49]**
Forensic contribution	Shows the migration of civil remedies from static botnet servers to domains, accounts, services, identities, cloud paths, and platform control points. **[FN 49]**

A.19 Google LLC v. Does 1-25, No. 1:25-cv-04503 (S.D.N.Y.) - BadBox 2.0

Case-pedigree field	Verified value
Caption / court / filing	Google LLC v. Does 1-25, No. 1:25-cv-04503 (S.D.N.Y.) - BadBox 2.0. **[FN 51]**
Plaintiff / counsel	Google; counsel verified from case source set where publicly available. **[FN 51]**
Technical target	infected device/ad-fraud botnet and domain/IP infrastructure. **[FN 51]**
Relief / disposition	TRO, PI and later final/default relief with third-party service provisions. **[FN 51]**
Analytical role	Representative civil cybercrime or platform/service-control comparator in the 35-case population.
Operational field	**Analysis**
Claims / authority	Case-specific statutory and equitable claims verified from complaint/order set. **[FN 51]**
Sworn/expert method	Technical or platform evidence identified in the case source set; exact declarant details preserved in source register. **[FN 51]**
Technical execution	Recorded as executed where court/provider/party public source verifies implementation; otherwise coded as authority without assuming completion. **[FN 51]**
Durable / State Four	Assessed by final order, settlement, dismissal, permanent injunction, continuing-provider mechanism, or absence. **[FN 51]**
Forensic contribution	Shows the migration of civil remedies from static botnet servers to domains, accounts, services, identities, cloud paths, and platform control points. **[FN 51]**

A.20 Google LLC v. Does 1-25, No. 1:25-cv-09421 (S.D.N.Y.) - Lighthouse PhaaS

Case-pedigree field	Verified value
Caption / court / filing	Google LLC v. Does 1-25, No. 1:25-cv-09421 (S.D.N.Y.) - Lighthouse PhaaS. **[FN 52]**
Plaintiff / counsel	Google; counsel verified from case source set where publicly available. **[FN 52]**
Technical target	phishing-as-a-service websites, templates, payment and credential infrastructure. **[FN 52]**
Relief / disposition	Nov. 2025 TRO; Dec. 2025 preliminary injunction. **[FN 52]**

Case-pedigree field	Verified value
Analytical role	Representative civil cybercrime or platform/service-control comparator in the 35-case population.
Operational field	**Analysis**
Claims / authority	Case-specific statutory and equitable claims verified from complaint/order set. **[FN 52]**
Sworn/expert method	Technical or platform evidence identified in the case source set; exact declarant details preserved in source register. **[FN 52]**
Technical execution	Recorded as executed where court/provider/party public source verifies implementation; otherwise coded as authority without assuming completion. **[FN 52]**
Durable / State Four	Assessed by final order, settlement, dismissal, permanent injunction, continuing-provider mechanism, or absence. **[FN 52]**
Forensic contribution	Shows the migration of civil remedies from static botnet servers to domains, accounts, services, identities, cloud paths, and platform control points. **[FN 52]**

A.21 Google LLC v. Doe 1 a/k/a Yucheng Chang & Does 2-25, No. 1:25-cv-10440 (S.D.N.Y.) - Darcula / Magic Cat

Case-pedigree field	Verified value
Caption / court / filing	Google LLC v. Doe 1 a/k/a Yucheng Chang & Does 2-25, No. 1:25-cv-10440 (S.D.N.Y.) - Darcula / Magic Cat. **[FN 53]**
Plaintiff / counsel	Google; counsel verified from case source set where publicly available. **[FN 53]**
Technical target	smishing/PhaaS kit infrastructure and operator accounts. **[FN 53]**
Relief / disposition	TRO and preliminary injunction followed by Apr. 7, 2026 default judgment/permanent relief. **[FN 53]** **[FN 88]**
Analytical role	Modern smishing/phishing-as-a-service comparator with operator-account and infrastructure relief.
Operational field	**Analysis**
Claims / authority	Case-specific statutory and equitable claims verified from complaint/order set. **[FN 53]**
Sworn/expert method	Technical or platform evidence identified in the case source set; exact declarant details preserved in source register. **[FN 53]**
Technical execution	Recorded as executed where court/provider/party public source verifies implementation; otherwise coded as authority without assuming completion. **[FN 53]**
Durable / State Four	Durable final relief located; continuing enforcement remains plaintiff/provider-centered in the public record. **[FN 88]**
Forensic contribution	Shows the migration of civil remedies from static botnet servers to domains, accounts, services, identities, cloud paths, and platform control points. **[FN 53]**

A.22 Microsoft Corp., H2-Pharma, LLC and Gatehouse Dock Condominium Assn v. Does 1-7, No. 1:26-cv-20074 (S.D. Fla.) - RedVDS

Case-pedigree field	Verified value
Caption / court / filing	Microsoft Corp., H2-Pharma, LLC and Gatehouse Dock Condominium Assn v. Does 1-7, No. 1:26-cv-20074 (S.D. Fla.) - RedVDS. **[FN 54]**
Plaintiff / counsel	Microsoft, H2-Pharma and Gatehouse Dock Condominium Association; counsel verified from case source set where publicly available. **[FN 54]**
Technical target	disposable virtual desktop service used for fraud/phishing. **[FN 54]**

Case-pedigree field	Verified value
Relief / disposition	Jan. 2026 TRO/PI; May 2026 default final judgment. **[FN 54]**
Analytical role	Representative civil cybercrime or platform/service-control comparator in the 35-case population.
Operational field	**Analysis**
Claims / authority	Case-specific statutory and equitable claims verified from complaint/order set. **[FN 54]**
Sworn/expert method	Technical or platform evidence identified in the case source set; exact declarant details preserved in source register. **[FN 54]**
Technical execution	Recorded as executed where court/provider/party public source verifies implementation; otherwise coded as authority without assuming completion. **[FN 54]**
Durable / State Four	Assessed by final order, settlement, dismissal, permanent injunction, continuing-provider mechanism, or absence. **[FN 54]**
Forensic contribution	Shows the migration of civil remedies from static botnet servers to domains, accounts, services, identities, cloud paths, and platform control points. **[FN 54]**

A.23 Google LLC v. Does 1-25 associated with Outsider Enterprise, No. 1:26-cv-04982 (S.D.N.Y.)

Case-pedigree field	Verified value
Caption / court / filing	Google LLC v. Does 1-25 associated with Outsider Enterprise, No. 1:26-cv-04982 (S.D.N.Y.). **[FN 55]**
Plaintiff / counsel	Google; counsel verified from case source set where publicly available. **[FN 55]**
Technical target	China-based phishing-as-a-service platform, AI templates and fraudulent URLs. **[FN 55]**
Relief / disposition	June 2026 complaint and preliminary injunction; action pending at cutoff. **[FN 55]**
Analytical role	Representative civil cybercrime or platform/service-control comparator in the 35-case population.
Operational field	**Analysis**
Claims / authority	Case-specific statutory and equitable claims verified from complaint/order set. **[FN 55]**
Sworn/expert method	Technical or platform evidence identified in the case source set; exact declarant details preserved in source register. **[FN 55]**
Technical execution	Recorded as executed where court/provider/party public source verifies implementation; otherwise coded as authority without assuming completion. **[FN 55]**
Durable / State Four	Assessed by final order, settlement, dismissal, permanent injunction, continuing-provider mechanism, or absence. **[FN 55]**
Forensic contribution	Shows the migration of civil remedies from static botnet servers to domains, accounts, services, identities, cloud paths, and platform control points. **[FN 55]**

A.24 Microsoft Corp. v. Does 1-5, No. 1:26-cv-24064 (S.D. Fla.) - Amadey-StealC joint disruption

Case-pedigree field	Verified value
Caption / court / filing	Microsoft Corp. v. Does 1-5, No. 1:26-cv-24064 (S.D. Fla.) - Amadey-StealC joint disruption. **[FN 91]**
Plaintiff / counsel	Microsoft and partners; counsel verified from case source set where publicly available. **[FN 91]**
Technical target	loader/infostealer service infrastructure. **[FN 91]**
Relief / disposition	June/July 2026 TRO/PI sequence; preliminary relief at cutoff. **[FN 91]**

Case-pedigree field	Verified value
Analytical role	Representative civil cybercrime or platform/service-control comparator in the 35-case population.
Operational field	**Analysis**
Claims / authority	Case-specific statutory and equitable claims verified from complaint/order set. **[FN 91]**
Sworn/expert method	Technical or platform evidence identified in the case source set; exact declarant details preserved in source register. **[FN 91]**
Technical execution	Recorded as executed where court/provider/party public source verifies implementation; otherwise coded as authority without assuming completion. **[FN 91]**
Durable / State Four	Assessed by final order, settlement, dismissal, permanent injunction, continuing-provider mechanism, or absence. **[FN 91]**
Forensic contribution	Shows the migration of civil remedies from static botnet servers to domains, accounts, services, identities, cloud paths, and platform control points. **[FN 91]**

A.25 Microsoft Corp. and Health-ISAC, Inc. v. Joshua Ogundipe and John Does 1-4, No. 1:25-cv-07111 (S.D.N.Y.) - RaccoonO365

Case-pedigree field	Verified value
Caption / court / filing	Microsoft Corp. and Health-ISAC, Inc. v. Joshua Ogundipe and John Does 1-4, No. 1:25-cv-07111 (S.D.N.Y.) - RaccoonO365. **[FN 56]**
Plaintiff / counsel	Microsoft and Health-ISAC; counsel verified from case source set where publicly available. **[FN 56]**
Technical target	adversary-in-the-middle phishing-as-a-service and Microsoft 365 sessions. **[FN 56]**
Relief / disposition	Aug./Sept. 2025 sealed TROs; Sept. 24 preliminary injunction; later request for entry of default/default judgment visible, but no entered final judgment located through Sept. 7, 2026. **[FN 56]** **[FN 87]**
Analytical role	Identity-centric phishing-as-a-service/AiTM/session-control comparator in the 35-case population.
Operational field	**Analysis**
Claims / authority	Case-specific statutory and equitable claims verified from complaint/order set. **[FN 56]**
Sworn/expert method	Technical or platform evidence identified in the case source set; exact declarant details preserved in source register. **[FN 56]**
Technical execution	Recorded as executed where court/provider/party public source verifies implementation; otherwise coded as authority without assuming completion. **[FN 56]**
Durable / State Four	State Three remains unresolved at cutoff; no final-order-based State Four pathway can yet be measured. **[FN 87]**
Forensic contribution	Shows the migration of civil remedies from static botnet servers to domains, accounts, services, identities, cloud paths, and platform control points. **[FN 56]**

A.26 Google LLC v. Zubair Saeed et al., No. 1:23-cv-03369 (S.D.N.Y.) - CryptBot

Case-pedigree field	Verified value
Caption / court / filing	Google LLC v. Zubair Saeed et al., No. 1:23-cv-03369 (S.D.N.Y.) - CryptBot. **[FN 63]**
Plaintiff / counsel	Google; counsel verified from case source set where publicly available. **[FN 63]**
Technical target	infostealer/pay-per-install malware distribution. **[FN 63]**

Case-pedigree field	Verified value
Relief / disposition	Apr. 2023 TRO; May 2023 PI; June 2023 permanent/default relief. **[FN 63]**
Analytical role	Representative civil cybercrime or platform/service-control comparator in the 35-case population.
Operational field	**Analysis**
Claims / authority	Case-specific statutory and equitable claims verified from complaint/order set. **[FN 63]**
Sworn/expert method	Technical or platform evidence identified in the case source set; exact declarant details preserved in source register. **[FN 63]**
Technical execution	Recorded as executed where court/provider/party public source verifies implementation; otherwise coded as authority without assuming completion. **[FN 63]**
Durable / State Four	Assessed by final order, settlement, dismissal, permanent injunction, continuing-provider mechanism, or absence. **[FN 63]**
Forensic contribution	Shows the migration of civil remedies from static botnet servers to domains, accounts, services, identities, cloud paths, and platform control points. **[FN 63]**

A.27 Google LLC v. Does 1-3, No. 5:23-cv-05823 (N.D. Cal.) - Fake Bard malware

Case-pedigree field	Verified value
Caption / court / filing	Google LLC v. Does 1-3, No. 5:23-cv-05823 (N.D. Cal.) - Fake Bard malware. **[FN 64]**
Plaintiff / counsel	Google; counsel verified from case source set where publicly available. **[FN 64]**
Technical target	AI-brand impersonation pages and malware downloads. **[FN 64]**
Relief / disposition	Alternative service and platform identity relief; no infrastructure TRO located in reviewed public set. **[FN 64]**
Analytical role	Representative civil cybercrime or platform/service-control comparator in the 35-case population.
Operational field	**Analysis**
Claims / authority	Case-specific statutory and equitable claims verified from complaint/order set. **[FN 64]**
Sworn/expert method	Technical or platform evidence identified in the case source set; exact declarant details preserved in source register. **[FN 64]**
Technical execution	Recorded as executed where court/provider/party public source verifies implementation; otherwise coded as authority without assuming completion. **[FN 64]**
Durable / State Four	Assessed by final order, settlement, dismissal, permanent injunction, continuing-provider mechanism, or absence. **[FN 64]**
Forensic contribution	Shows the migration of civil remedies from static botnet servers to domains, accounts, services, identities, cloud paths, and platform control points. **[FN 64]**

A.28 Google LLC v. Yunfeng Sun and Hongnam Cheung, No. 1:24-cv-02559 (S.D.N.Y.) - crypto confidence-scam apps

Case-pedigree field	Verified value
Caption / court / filing	Google LLC v. Yunfeng Sun and Hongnam Cheung, No. 1:24-cv-02559 (S.D.N.Y.) - crypto confidence-scam apps. **[FN 65]**
Plaintiff / counsel	Google; counsel verified from case source set where publicly available. **[FN 65]**
Technical target	app-store/developer-account and crypto confidence scam infrastructure. **[FN 65]**
Relief / disposition	May 2024 alternative service; Oct. 2024 default/permanent injunction. **[FN 65]**

Case-pedigree field	Verified value
Analytical role	Representative civil cybercrime or platform/service-control comparator in the 35-case population.
Operational field	**Analysis**
Claims / authority	Case-specific statutory and equitable claims verified from complaint/order set. **[FN 65]**
Sworn/expert method	Technical or platform evidence identified in the case source set; exact declarant details preserved in source register. **[FN 65]**
Technical execution	Recorded as executed where court/provider/party public source verifies implementation; otherwise coded as authority without assuming completion. **[FN 65]**
Durable / State Four	Assessed by final order, settlement, dismissal, permanent injunction, continuing-provider mechanism, or absence. **[FN 65]**
Forensic contribution	Shows the migration of civil remedies from static botnet servers to domains, accounts, services, identities, cloud paths, and platform control points. **[FN 65]**

A.29 Meta Platforms, Instagram and WhatsApp v. Does 1-100, No. 3:21-cv-09797 (N.D. Cal.) - 39,000-site phishing

Case-pedigree field	Verified value
Caption / court / filing	Meta Platforms, Instagram and WhatsApp v. Does 1-100, No. 3:21-cv-09797 (N.D. Cal.) - 39,000-site phishing. **[FN 66]**
Plaintiff / counsel	Meta platforms; counsel verified from case source set where publicly available. **[FN 66]**
Technical target	mass phishing domains and impersonation pages. **[FN 66]**
Relief / disposition	Expedited discovery; final injunction/disposition not located in reviewed public set. **[FN 66]**
Analytical role	Representative civil cybercrime or platform/service-control comparator in the 35-case population.
Operational field	**Analysis**
Claims / authority	Case-specific statutory and equitable claims verified from complaint/order set. **[FN 66]**
Sworn/expert method	Technical or platform evidence identified in the case source set; exact declarant details preserved in source register. **[FN 66]**
Technical execution	Recorded as executed where court/provider/party public source verifies implementation; otherwise coded as authority without assuming completion. **[FN 66]**
Durable / State Four	Assessed by final order, settlement, dismissal, permanent injunction, continuing-provider mechanism, or absence. **[FN 66]**
Forensic contribution	Shows the migration of civil remedies from static botnet servers to domains, accounts, services, identities, cloud paths, and platform control points. **[FN 66]**

A.30 Meta Platforms, Inc. v. Voyager Labs Ltd., No. 3:23-cv-00154 (N.D. Cal.)

Case-pedigree field	Verified value
Caption / court / filing	Meta Platforms, Inc. v. Voyager Labs Ltd., No. 3:23-cv-00154 (N.D. Cal.). **[FN 66]**
Plaintiff / counsel	Meta; counsel verified from case source set where publicly available. **[FN 66]**
Technical target	scraping-for-hire accounts and platform access. **[FN 66]**
Relief / disposition	Motion to dismiss denied; Dec. 2024 settlement/permanent injunction. **[FN 66]**
Analytical role	Representative civil cybercrime or platform/service-control comparator in the 35-case population.

Case-pedigree field	Verified value
Operational field	**Analysis**
Claims / authority	Case-specific statutory and equitable claims verified from complaint/order set. **[FN 66]**
Sworn/expert method	Technical or platform evidence identified in the case source set; exact declarant details preserved in source register. **[FN 66]**
Technical execution	Recorded as executed where court/provider/party public source verifies implementation; otherwise coded as authority without assuming completion. **[FN 66]**
Durable / State Four	Assessed by final order, settlement, dismissal, permanent injunction, continuing-provider mechanism, or absence. **[FN 66]**
Forensic contribution	Shows the migration of civil remedies from static botnet servers to domains, accounts, services, identities, cloud paths, and platform control points. **[FN 66]**

A.31 Facebook, Inc. v. OneAudience, Inc., No. 3:20-cv-01461 (N.D. Cal.)

Case-pedigree field	Verified value
Caption / court / filing	Facebook, Inc. v. OneAudience, Inc., No. 3:20-cv-01461 (N.D. Cal.). **[FN 66]**
Plaintiff / counsel	Facebook; counsel verified from case source set where publicly available. **[FN 66]**
Technical target	malicious SDK and data-harvesting access. **[FN 66]**
Relief / disposition	Settlement with audit, permanent injunction, ban and monetary terms. **[FN 66]**
Analytical role	Representative civil cybercrime or platform/service-control comparator in the 35-case population.
Operational field	**Analysis**
Claims / authority	Case-specific statutory and equitable claims verified from complaint/order set. **[FN 66]**
Sworn/expert method	Technical or platform evidence identified in the case source set; exact declarant details preserved in source register. **[FN 66]**
Technical execution	Recorded as executed where court/provider/party public source verifies implementation; otherwise coded as authority without assuming completion. **[FN 66]**
Durable / State Four	Assessed by final order, settlement, dismissal, permanent injunction, continuing-provider mechanism, or absence. **[FN 66]**
Forensic contribution	Shows the migration of civil remedies from static botnet servers to domains, accounts, services, identities, cloud paths, and platform control points. **[FN 66]**

A.32 Meta Platforms, Inc. v. BrandTotal Ltd., No. 3:20-cv-07182 (N.D. Cal.)

Case-pedigree field	Verified value
Caption / court / filing	Meta Platforms, Inc. v. BrandTotal Ltd., No. 3:20-cv-07182 (N.D. Cal.). **[FN 66]**
Plaintiff / counsel	Meta; counsel verified from case source set where publicly available. **[FN 66]**
Technical target	browser-extension scraping and platform access. **[FN 66]**
Relief / disposition	Litigated motions/discovery; Oct. 2022 settlement/dismissal. **[FN 66]**
Analytical role	Representative civil cybercrime or platform/service-control comparator in the 35-case population.
Operational field	**Analysis**
Claims / authority	Case-specific statutory and equitable claims verified from complaint/order set. **[FN 66]**

Case-pedigree field	Verified value
Sworn/expert method	Technical or platform evidence identified in the case source set; exact declarant details preserved in source register. **[FN 66]**
Technical execution	Recorded as executed where court/provider/party public source verifies implementation; otherwise coded as authority without assuming completion. **[FN 66]**
Durable / State Four	Assessed by final order, settlement, dismissal, permanent injunction, continuing-provider mechanism, or absence. **[FN 66]**
Forensic contribution	Shows the migration of civil remedies from static botnet servers to domains, accounts, services, identities, cloud paths, and platform control points. **[FN 66]**

A.33 Amazon.com, Inc. et al. v. REKK et al., No. 2:23-cv-01879 (W.D. Wash.)

Case-pedigree field	Verified value
Caption / court / filing	Amazon.com, Inc. et al. v. REKK et al., No. 2:23-cv-01879 (W.D. Wash.). **[FN 67]**
Plaintiff / counsel	Amazon; counsel verified from case source set where publicly available. **[FN 67]**
Technical target	refund-as-a-service/fraud network and platform identities. **[FN 67]**
Relief / disposition	Stipulated PI and later default/damages orders. **[FN 67]**
Analytical role	Representative civil cybercrime or platform/service-control comparator in the 35-case population.
Operational field	**Analysis**
Claims / authority	Case-specific statutory and equitable claims verified from complaint/order set. **[FN 67]**
Sworn/expert method	Technical or platform evidence identified in the case source set; exact declarant details preserved in source register. **[FN 67]**
Technical execution	Recorded as executed where court/provider/party public source verifies implementation; otherwise coded as authority without assuming completion. **[FN 67]**
Durable / State Four	Assessed by final order, settlement, dismissal, permanent injunction, continuing-provider mechanism, or absence. **[FN 67]**
Forensic contribution	Shows the migration of civil remedies from static botnet servers to domains, accounts, services, identities, cloud paths, and platform control points. **[FN 67]**

A.34 Amazon.com, Inc. et al. v. Wasim et al., No. 4:23-cv-05580 (N.D. Cal.) - KDP impersonation network

Case-pedigree field	Verified value
Caption / court / filing	Amazon.com, Inc. et al. v. Wasim et al., No. 4:23-cv-05580 (N.D. Cal.) - KDP impersonation network. **[FN 67]**
Plaintiff / counsel	Amazon Publishing; counsel verified from case source set where publicly available. **[FN 67]**
Technical target	publishing impersonation and account fraud. **[FN 67]**
Relief / disposition	Feb. 2025 default judgment and permanent injunctive relief. **[FN 67]**
Analytical role	Representative civil cybercrime or platform/service-control comparator in the 35-case population.
Operational field	**Analysis**
Claims / authority	Case-specific statutory and equitable claims verified from complaint/order set. **[FN 67]**
Sworn/expert method	Technical or platform evidence identified in the case source set; exact declarant details preserved in source register. **[FN 67]**

Case-pedigree field	Verified value
Technical execution	Recorded as executed where court/provider/party public source verifies implementation; otherwise coded as authority without assuming completion. **[FN 67]**
Durable / State Four	Assessed by final order, settlement, dismissal, permanent injunction, continuing-provider mechanism, or absence. **[FN 67]**
Forensic contribution	Shows the migration of civil remedies from static botnet servers to domains, accounts, services, identities, cloud paths, and platform control points. **[FN 67]**

A.35 United States v. Nicholas Palumbo et al., No. 1:20-cv-00473 (E.D.N.Y.) - fraudulent robocall gateway

Case-pedigree field	Verified value
Caption / court / filing	United States v. Nicholas Palumbo et al., No. 1:20-cv-00473 (E.D.N.Y.) - fraudulent robocall gateway. **[FN 68]**
Plaintiff / counsel	United States; counsel verified from case source set where publicly available. **[FN 68]**
Technical target	telecommunications gateway used for fraudulent robocalls. **[FN 68]**
Relief / disposition	Jan. 2020 TRO; Mar. 2020 PI; Aug. 2020 permanent consent decree. **[FN 68]**
Analytical role	Representative civil cybercrime or platform/service-control comparator in the 35-case population.
Operational field	**Analysis**
Claims / authority	Case-specific statutory and equitable claims verified from complaint/order set. **[FN 68]**
Sworn/expert method	Technical or platform evidence identified in the case source set; exact declarant details preserved in source register. **[FN 68]**
Technical execution	Recorded as executed where court/provider/party public source verifies implementation; otherwise coded as authority without assuming completion. **[FN 68]**
Durable / State Four	Assessed by final order, settlement, dismissal, permanent injunction, continuing-provider mechanism, or absence. **[FN 68]**
Forensic contribution	Shows the migration of civil remedies from static botnet servers to domains, accounts, services, identities, cloud paths, and platform control points. **[FN 68]**

Appendix B - Disposition, State Three-State Four, Enforcement, and Public-Visibility Aftermath Register

Appendix B is the reproducible details register for Part IV. The population is coded through September 7, 2026. For every case, State Three records the located final or current disposition in operational terms; State Four records successor authority, later-victim access, adaptation, or the absence of a located mechanism; visibility distinguishes launch/emergency explanation from final-disposition or later-enforcement explanation. **[FN 92]**

The visibility search classes are consistent across the population to the extent applicable: official party and operation pages; counsel pages; public dockets and legal repositories; cyber and legal press; public social/video/podcast/conference indexing; and archived pages. A stated zero or "not located" is a bounded result for those source classes through the cutoff. It is not converted into a claim that no nonpublic event exists. Final orders and signed docket objects control the disposition field where available. **[FN 92]**

Representative case	State Three - final disposition / durable remedy	State Four - successor, later-victim access, adaptation	Visibility / reproducibility
1. cracked Cobalt Strike	Default judgment + permanent injunction entered Sept. 8, 2025; retained jurisdiction cannot lapse before Jan. 1, 2030. **[FN 23]**	Defined future domain/IP criteria, Court Monitor, nonparty disclosure path; Nov. 18-19 later-victim field test located; no public technical successor determination located. **[FN 23] [FN 25] [FN 74]**	Launch/interim: substantial Microsoft/Fortra/Health-ISAC + press. Final: >=6 legal mirrors; 0 independent final-remedy explanations and 0 specific public later-enforcement events through cutoff. **[FN 83]**
2. Glupteba	Initial disruption followed by default/sanctions proceedings; named/anonymous operator litigation continued. **[FN 86]**	Operator rebuilding and blockchain fallback made durability contested; no general later-victim intake path located. **[FN 86]**	Launch/rebuilding widely publicized; final procedural record available in legal sources. Correct case: 1:21-cv-10260. **[FN 86]**
3. Sophos	Emergency domain/provider relief located; no entered permanent final infrastructure order located in refreshed public set through cutoff. **[FN 89]**	No successor/monitor/later-victim mechanism comparable to 23-cv-2447 located. **[FN 89]**	Emergency action source-native/publicly available; final/enforcement visibility not located in defined public classes. **[FN 89] [FN 92]**
4. DXC	Emergency relief and default/permanent-injunction motion/R&R located; entered final permanent order not separately located in refreshed public set. **[FN 90]**	No public later-victim successor path located; reverse-proxy/Cobalt Strike method remains important comparator. **[FN 90]**	Emergency/default materials publicly available; no comparable later-enforcement publicity located. **[FN 90] [FN 92]**
5. Waledac	Permanent domain transfer entered Oct. 27, 2010. **[FN 7]**	Durable control of known domains; later-victim/successor mechanism limited by early-generation design. **[FN 7]**	Launch and final transfer publicly explained by Microsoft; classic durable State Three case. **[FN 7]**
6. Rustock	Coordinated server seizure/imaging followed by continuing orders removing domains/IPs from defendants. **[FN 8]**	Strong suppression of known server/IP paths; no express public nonparty intake mechanism located. **[FN 8]**	Takedown and implementation publicly explained; later-victim path not a central public feature. **[FN 8]**
7. Zeus	C2 seizure/domain control achieved; enterprise case did not mature into a 23-cv-2447-style successor architecture in located record. **[FN 9]**	Limited explicit later-victim path; downstream crimeware ecosystem remained adaptive. **[FN 9]**	Major launch publicity; final-successor visibility comparatively limited. **[FN 9] [FN 92]**
8. Citadel	Nov. 21, 2013 default judgment/permanent injunction; curative server/domain control. **[FN 10]**	Durable known-object control and victim-remediation architecture; less explicit later-victim successor procedure. **[FN 10]**	Launch and permanent relief publicly documented; strong State Three benchmark. **[FN 10]**
9. Barium / Brass Typhoon	Default/permanent-injunction and continuing monitor process located. **[FN 59]**	Continuing process permits later malicious domains/profiles to be reached; later-victim public intake remains case-specific. **[FN 59]**	Microsoft repeatedly publicized nation-state disruption; continuing mechanism more visible than many later cases. **[FN 59]**

Representative case	State Three - final disposition / durable remedy	State Four - successor, later-victim access, adaptation	Visibility / reproducibility
10. Phosphorus	Permanent-injunction/default phase located after seizure/control of 99 sites. **[FN 60]**	Microsoft reported repeated actions against rebuilt infrastructure; continuing plaintiff-led use, not general victim intake. **[FN 60]**	Strong launch and repeat-action publicity; later enforcement visible at program/party level. **[FN 60]**
11. WhatsApp/Facebook v. NSO	Liability/damages/injunctive litigation continued; not a registry/sinkhole final-state model. **[FN 61]**	Enforcement depends on platform injunction/damages posture rather than successor domain intake. **[FN 61]**	High sustained public/legal visibility; materially different platform/spyware comparator. **[FN 61]**
12. Apple v. NSO	Voluntarily dismissed after Apple cited changed circumstances and threat-intelligence exposure concerns. **[FN 61]**	No durable civil-disruption State Four mechanism after dismissal. **[FN 61]**	Filing and dismissal were publicly explained; useful contrast where litigation itself created intelligence-exposure concerns. **[FN 61]**
13. ZLoader	Court-ordered transfer/sinkhole of hard-coded and registered DGA domains; future-DGA blocking architecture. **[FN 58]**	Successor-aware DGA process is a strong State Four precursor, though not a general nonparty mechanism. **[FN 58]**	Launch/takedown and DGA method publicly explained; successor design visible. **[FN 58]**
14. Bohrium	Jan. 30, 2024 default judgment and permanent injunction located. **[FN 62] [FN 85]**	Durable final domain relief; no separate public later-victim procedure comparable to 23-cv-2447 located. **[FN 85]**	Launch/public notice available; final order locatable in docket sources, with thinner final-remedy publicity. **[FN 85] [FN 92]**
15. TrickBot	Emergency disabling/preservation relief and default/permanent-injunction phase reached in public notice record. **[FN 11]**	Revival/adaptation was anticipated; continuing defense remained plaintiff/provider/law-enforcement led. **[FN 11]**	Very high launch/election-period publicity; adaptation publicly discussed. **[FN 11]**
16. Star Blizzard / ColdRiver	Aug. 5, 2026 default judgment and permanent injunction located. **[FN 57] [FN 84]**	Durable domain-portfolio relief; continuing plaintiff/provider action possible, but no general later-victim intake path located. **[FN 84]**	Launch/DOJ coordination public; final 2026 order locatable in legal/docket sources. **[FN 84]**
17. Fake ONNX	TRO/PI and roughly 240-site disruption located; no entered final judgment located in refreshed public set through cutoff. **[FN 50]**	State Four remains plaintiff/provider centered; final successor procedure not located. **[FN 50]**	Strong launch/notice publicity; final-disposition visibility not located. **[FN 50] [FN 92]**
18. Lumma	May 2025 emergency order and large-scale domain seizure/blocking/sinkholing; entered permanent final judgment not located through cutoff. **[FN 49]**	Successor risk persists because infostealer service can regenerate domains/panels; continuing enforcement is operational rather than a public nonparty process. **[FN 49]**	Major launch and metrics publicity; final permanent-remedy event not located. **[FN 49] [FN 92]**
19. BadBox 2.0	TRO/PI followed by located final/default relief with third-party service provisions. **[FN 51]**	Durable provider/platform restraints; later-victim path remains case-specific. **[FN 51]**	Launch and disruption highly publicized; final materials available in docket sources. **[FN 51]**
20. Lighthouse PhaaS	Nov. 2025 TRO and Dec. 2025 preliminary injunction; no entered final judgment located through cutoff. **[FN 52]**	Pending State Three; no final-order State Four mechanism yet measurable. **[FN 52]**	Launch/TRO/PI publicity located; final-disposition visibility not yet applicable. **[FN 52] [FN 92]**
21. Darcula / Magic Cat	Apr. 7, 2026 default judgment/permanent relief located after TRO/PI. **[FN 53] [FN 88]**	Durable plaintiff/provider-facing relief; no separate public nonparty intake mechanism located. **[FN 88]**	Launch and preliminary relief public; final order locatable in legal repositories. **[FN 88]**
22. RedVDS	May 2026 default final judgment located after Jan. 2026 TRO/PI. **[FN 54]**	Durable service-enabling restraints; continuing enforcement remains plaintiff/provider led. **[FN 54]**	Strong Microsoft launch publicity; final disposition present in docket/public materials. **[FN 54]**
23. Outsider Enterprise	June 2026 complaint/preliminary injunction; action pending at cutoff. **[FN 55]**	No final State Four mechanism yet measurable. **[FN 55]**	Launch/preliminary publicity located; final-disposition stage not reached. **[FN 55]**

Representative case	State Three - final disposition / durable remedy	State Four - successor, later-victim access, adaptation	Visibility / reproducibility
24. Amadey-StealC	June/July 2026 TRO/PI sequence; preliminary-relief posture at cutoff. **[FN 91]**	State Four not yet measurable from a final order; loader/infostealer successor risk remains operational. **[FN 91]**	Launch/preliminary disruption public; no final-disposition item located through cutoff. **[FN 91]** **[FN 92]**
25. RaccoonO365	Sealed Aug./Sept. 2025 TROs; Sept. 24 PI; later default-judgment request visible; no entered final judgment located through Sept. 7, 2026. **[FN 56]** **[FN 87]**	State Three unresolved; final-order-based later-victim enforcement cannot yet be measured. **[FN 87]**	Substantial launch/TRO/PI publicity. No post-final visibility inference because a final judgment has not been located. **[FN 87]**
26. CryptBot	June 2023 default/permanent relief after Apr. TRO and May PI. **[FN 63]**	Durable platform/domain restraints; no broad public nonparty successor mechanism located. **[FN 63]**	Google publicly explained filing/takedown; final order available in legal record. **[FN 63]**
27. Fake Bard	Alternative service/platform identity relief; no classic infrastructure TRO/final injunction located in reviewed public set. **[FN 64]**	No comparable State Four infrastructure mechanism located. **[FN 64]**	Google publicized AI-brand malware action; disposition visibility remains limited. **[FN 64]** **[FN 92]**
28. Google crypto-app scams	Oct. 2024 default/permanent injunction after alternative service. **[FN 65]**	Durable platform/developer restraints; later-victim path case-specific. **[FN 65]**	Launch and final legal record publicly available. **[FN 65]**
29. Meta 39,000-site phishing	Expedited discovery and platform relief; final injunction/disposition not located in reviewed public set. **[FN 66]**	No located final successor/later-victim mechanism. **[FN 66]**	High launch publicity from Meta; final-disposition visibility not located. **[FN 66]** **[FN 92]**
30. Meta v. Voyager Labs	Dec. 2024 settlement/permanent injunction. **[FN 66]**	Durable platform-access restraint by settlement; no botnet-style successor domain process. **[FN 66]**	Litigation and settlement publicly visible; materially different scraping-for-hire comparator. **[FN 66]**
31. Facebook v. OneAudience	Settlement with audit, permanent injunction, ban and monetary terms. **[FN 66]**	Durable platform/account compliance mechanism rather than infrastructure successor process. **[FN 66]**	Public litigation/settlement record available. **[FN 66]**
32. Meta v. BrandTotal	Oct. 2022 settlement/dismissal after litigated motions/discovery. **[FN 66]**	No standing botnet-style State Four mechanism after settlement/dismissal. **[FN 66]**	Public litigation and settlement visibility; platform comparator. **[FN 66]**
33. Amazon v. REKK	Stipulated PI followed by default/damages orders. **[FN 67]**	Fraud-network enforcement through platform identities and judgments; no general later-victim infrastructure mechanism located. **[FN 67]**	Amazon publicly announced refund-fraud action; later orders available in legal record. **[FN 67]**
34. KDP impersonation	Feb. 2025 default judgment and permanent injunctive relief. **[FN 67]**	Durable impersonation/account restraints; no general successor-domain intake path located. **[FN 67]**	Amazon/public legal sources show action and final relief. **[FN 67]**
35. Palumbo robocall gateway	Aug. 2020 permanent consent decree after Jan. TRO and Mar. PI. **[FN 68]**	Durable telecommunications restraint under consent decree; enforcement path is government/decree-specific. **[FN 68]**	DOJ publicly announced action; permanent consent outcome is publicly locatable. **[FN 68]**

23-cv-2447 expanded visibility and State-Four mini-register

Stage/date	Headline / record	Source class	Measured result	Source
Apr. 2023	"Stopping cybercriminals from abusing security tools" + Notice of Pleadings	Microsoft / official	Launch legal-technical explanation; multi-institution participation	**[FN 12] [FN 13]**
Apr. 2023	Health-ISAC / Fortra coordinated legal-action account	Sector / party	Launch and sector-harm explanation	**[FN 14]**
Mar.-May 2025	80% reduction / shorter-dwell-time reporting and Fortra updates	Party + cyber/healthcare press	Interim success publicly quantified before final judgment	**[FN 15] [FN 72] [FN 83]**
Aug. 6, 2025	Report and Recommendation	Court / legal record	Recommended permanent conversion of preliminary relief	**[FN 24]**
Sept. 8-9, 2025	Order adopting R&R / final permanent relief	Court + legal repositories	Permanent injunction; Court Monitor; successor criteria; jurisdiction into 2030; >=6 legal mirrors located	**[FN 23] [FN 71] [FN 83]**
Post-final to Sept. 7, 2026	Party/counsel/expert/major-media explanation of final mechanism	Defined independent source universe	0 responsive final-remedy explanations located	**[FN 83]**
Post-final to Sept. 7, 2026	Specific public successor determination / later enforcement event	Defined independent source universe	0 specific public technical enforcement events located; general DCU program page logged separately	**[FN 83]**
Nov. 18, 2025	Rule 24/Rule 71 emergency application, DE 61; exhibit DE 62	Primary docket / filing	Later-victim applicant invokes or seeks use of successor architecture; secure review/DCU coordination requested	**[FN 25] [FN 74]**
Nov. 19, 2025	Text/paperless directive; response due Dec. 5	Primary docket	Ex parte designation removed; plaintiffs ordered to respond; no separate visible docket number/PDF in reviewed image	**[FN 24] [FN 74]**
Through Sept. 7, 2026	Public disposition of field test	Docket + party/counsel/expert/media/social	No public plaintiff response, monitor proceeding, technical successor adjudication, or independent explanation located	**[FN 83]**

Appendix C - Declarant and Methodology Crosswalk

Declarant / rail	Source type	Method / evidence	Contribution
Christopher Coy	Microsoft DCU	Infrastructure, provider, domains/IPs, control points	23-cv-2447; compare with other Microsoft DCU matters. **[FN 17]**
Jason Lyons	Microsoft threat intelligence	~50,000 samples, controlled infection, C2, watermark/configuration and actor-role mapping	23-cv-2447 scale/attribution method. **[FN 18]**
Robert G. Erdman II	Fortra	Cobalt Strike product, licensing, cracked copies, cyber intelligence and New York infrastructure	Fortra-specific product and abuse foundation. **[FN 19]**
Rodelio G. Fiñones	Microsoft DCU	Beacon, loader, API, DLL, metadata, encryption, process injection, configuration	Technical artifact grammar for cracked Cobalt Strike. **[FN 20]**
Jonathan Gross	Microsoft	Software, product-harm and legitimate/illegitimate use context	Product-harm and Microsoft ecosystem evidence. **[FN 21]**
Errol Weiss	Health-ISAC	Healthcare-sector risk and ransomware impact	Sector harm and urgency. **[FN 22]**
Mark Hughes	DXC expert	Cobalt Strike BEACON, rotating domains, reverse proxying and ransomware chain	Original comparator for Cobalt Strike/reverse-proxy infrastructure. **[FN 90]**
CNF	Expert team	Endpoint/DNS/MX/infrastructure/litigation overlay and synchronized windows	Subject-side integrated finding. **[FN 27]**
Marlin	Expert team	Endpoint/account/cloud baseline	Early independent technical rail. **[FN 28]**
RAPS	Expert team	CM/ECF, DCN, SMTP, object-state separation	Adjudicative-channel forensic rail. **[FN 30]**
CCDG	Expert team	SPF/DKIM/DMARC and authenticated-counterfeit communications	Trusted-channel/counterfeit-communication rail. **[FN 31]**
Team B - Employee Portal	Structured portal dataset	Identity/URL/date/access-related fields; separate staff-identity trust boundary	Structured portal rail compared with DNS/MX, service, and workflow events. **[FN 29]**
Team B - Membership Portal	Structured portal dataset	Membership identity/account and access-related fields	Professional-identity portal rail. **[FN 29]**
Team B - MyFLCourtAccess	Structured portal dataset	E-filing identity, URL/date/account and workflow fields	Filing/service portal rail; correlates with DNS/MX and notice events. **[FN 29]**
Sinkhole	Expert report	Registrar/DNS state, disabling/redirection, successor behavior	Infrastructure-control and publication-suppression rail. **[FN 32]**
Avatar	Expert report	Professional-persona provenance and credential-backed appearance	Bounded persona/trust rail; source-native identity verification required. **[FN 33]**
Federal Court Audit	Expert audit	Docket, PageID, replacement, assignment, service and record-object analysis	Record-state significance after primary docket facts are established. **[FN 34]**

Appendix D - Plaintiff-Counsel and Publication-Control Event Register

Surface	Cases / population link	Objects examined	Analytical significance
Crowell & Moring	Microsoft/Fortra 23-cv-2447; RaccoonO365 and other Microsoft matters	Public professional identity, counsel signatures, publication history, firm-domain/cloud state and postjudgment visibility	High-value remedy trust boundary; not accused as institution. **[FN 69]**
Orrick / King & Spalding / Pillsbury / WilmerHale / Cooley / Perkins Coie / Freshfields / DWT / Susman / Alston	Multiple cases in 35-case population	Public firm domains, counsel signatures, RDAP/DNS/MX/provider states, litigation milestones	Used to identify whether customer-domain events align with sensitive filing/enforcement windows. **[FN 69]**
CourtListener/RECAP / Justia / vLex / Notice of Pleadings	Publication layer	Legal repository pages, mirrored orders, notice pages, indexing/archive state	Determines practical discoverability of final orders and later enforcement. **[FN 26]**
Microsoft / Fortra / Health-ISAC official sites	Party/expert-publicity layer	Launch announcements, notice page, official operation narratives, absence/presence of final-order updates	Separates initial publicity from final-judgment visibility. **[FN 26]**

Appendix E - Adjudicative-Channel Timeline

Date / period	Record	What it establishes	Use in report
June 21 and June 25, 2024	Spagnuolo/Farrow emergency filings	Contemporaneous cyber-interference allegations, requested restraint and preservation before expert reports existed	Field-case baseline. **[FN 37]**
Dec. 5, 2024	Marlin report	Early endpoint/account findings	Independent baseline. **[FN 28]**
Dec. 27-30, 2024	Florida protective/in-camera motion and corrected response	Secure-channel request and accountability/no-trust posture	Florida channel-stress start. **[FN 39]**
Oct. 22, 2025	CNF integrated expert report	Integrated endpoint, DNS/MX, infrastructure and civil-case overlay	Main subject-side forensic rail. **[FN 27]**
Oct.-Dec. 2025	E.D.N.Y. 25-cv-06033	Conventional/sealed filing, order/exhibit-access state, replacement entries, venue response and dismissal	Federal channel-stress test. **[FN 35]**
Nov. 18-19, 2025	Rule 71/intervention in 23-cv-2447	Later-victim attempt to use successor mechanism; order directing plaintiff response	State-Four field test. **[FN 25]**
Jan.-Feb. 2026	Sinkhole, Avatar, RAPS, CCDG, Florida writ/motion/order	Domain/persona/court-channel/authenticated-communication rails and paper-only/in-camera request denial	Expert convergence and CAE trigger. **[FN 32] [FN 33] [FN 30] [FN 31] [FN 39]**
Mar. 2, 2026	D.D.C. filed in-camera material	Filed request for controlled technical evidence path	Federal CAE request. **[FN 40]**

Appendix F - Source Notes

[FN 1] Administrative Office CM/ECF FAQ. Source: Administrative Office of the U.S. Courts, FAQs: Case Management / Electronic Case Files (CM/ECF), accessed Sept. 7, 2026. Proposition/application: Establishes the operational architecture of remote filing, automatic docket entry, immediate NEF service, simultaneous file access, and national rollout dates for bankruptcy, district, and appellate CM/ECF. URL: https://www.uscourts.gov/court-records/file-a-case-cm-ecf/faqs-case-management-electronic-case-files-cm-ecf

[FN 2] PACER electronic filing overview. Source: PACER / U.S. Courts, Electronic Filing (CM/ECF) and File a Case materials, accessed Sept. 7, 2026. Proposition/application: Establishes that federal filing and public retrieval operate through account-mediated CM/ECF and PACER systems. URL: https://pacer.uscourts.gov/file-case/how-file-case

[FN 3] PACER MFA implementation. Source: PACER, "Multifactor Authentication Coming Soon," May 2, 2025, and representative circuit/district implementation notices. Proposition/application: Establishes that the Judiciary treated CM/ECF account credentials as a security boundary requiring MFA beginning in May 2025 and by year end for CM/ECF-level users. URL: https://pacer.uscourts.gov/announcements/2025/05/02/multifactor-authentication-coming-soon

[FN 4] Judiciary 2025 case-management cyberattack announcement. Source: Administrative Office of the U.S. Courts, "Cybersecurity Measures Strengthened in Light of Attacks on Judiciary's Case Management System," Aug. 7, 2025. Proposition/application: Establishes official acknowledgment of escalated sophisticated and persistent cyberattacks against the Judiciary case-management system and resulting sensitive-document protective measures. URL: https://www.uscourts.gov/data-news/judiciary-news/2025/08/07/cybersecurity-measures-strengthened-light-attacks-judiciarys-case-management-system

[FN 5] Judiciary modernization testimony. Source: Administrative Office of the U.S. Courts, March 2026 judiciary modernization and budget materials concerning replacement of legacy CM/ECF components and cybersecurity risk. Proposition/application: Establishes the Judiciary's post-attack modernization posture and the security rationale for reducing localized application risk and updating case-management systems. URL: https://www.uscourts.gov/data-news/judiciary-news/2026/03/10/judges-outline-judiciarys-fiscal-year-2027-funding-needs

[FN 6] Highly Sensitive Document procedures. Source: Representative federal HSD and sealed-document notices, including court-published instructions requiring non-CM/ECF submission of HSDs by encrypted media or paper. Proposition/application: Establishes that federal courts recognize a category of filings too sensitive for ordinary CM/ECF handling, while showing that HSD procedures are not the same as a cyber-integrity intake path. URL: https://www.uscfc.uscourts.gov/sites/default/files/HSD%20Procedures%20Notice%20and%20Order.pdf

[FN 7] Waledac / Operation b49. Source: Microsoft Digital Crimes Unit public account and public reporting concerning Microsoft Corp. v. John Does 1-27, No. 1:10-cv-00156 (E.D. Va.), Feb.-Oct. 2010. Proposition/application: Establishes the registry-level ex parte action against 277 Waledac command domains and the later permanent transfer of domains to Microsoft. URL: https://blogs.microsoft.com/on-the-issues/2010/02/22/cracking-down-on-botnets/

[FN 8] Rustock / Operation b107. Source: Microsoft Digital Crimes Unit and public reporting concerning Microsoft Corp. v. John Does 1-11, No. 2:11-cv-00222 (W.D. Wash.), 2011. Proposition/application: Establishes the move from domain-only disruption to coordinated seizure and imaging of C2 servers and hard-coded IP infrastructure. URL: https://blogs.microsoft.com/on-the-issues/2011/03/17/microsoft-leads-the-way-in-taking-down-rustock-botnet/

[FN 9] Zeus / Operation b71. Source: Microsoft, FS-ISAC, NACHA, and public case materials concerning Microsoft Corp. et al. v. John Does 1-39, No. 1:12-cv-01335 (E.D.N.Y.), 2012. Proposition/application: Establishes the use of civil RICO and multi-sector plaintiffs to describe modular financial crimeware infrastructure, command servers, and domains. URL: https://blogs.microsoft.com/on-the-issues/2012/03/25/microsoft-financial-services-industry-and-law-enforcement-collaborate-to-disrupt-zeus-botnets/

[FN 10] Citadel. Source: Microsoft, FBI, and public docket materials concerning Microsoft Corp. v. John Does 1-82, No. 3:13-cv-00319 (W.D.N.C.), 2013. Proposition/application: Establishes the curative sinkhole model, registry/registrar duties, broad civil seizure of Citadel infrastructure, and final default judgment/permanent injunction. URL: https://blogs.microsoft.com/on-the-issues/2013/06/05/microsoft-works-with-financial-services-industry-leaders-law-enforcement-and-others-to-disrupt-massive-financial-cybercrime-ring/

[FN 11] TrickBot civil disruption. Source: Microsoft Corp. and FS-ISAC, Inc. v. John Does 1-2, No. 1:20-cv-1171 (E.D. Va.), Microsoft notice of pleadings and DCU announcement, Oct. 2020. Proposition/application: Establishes the replacement representative case: court-approved disabling of TrickBot IP addresses and content, suspension of services, copyright theory against malicious code use, and election-period operational urgency. URL: https://www.microsoft.com/en-us/corporate-responsibility/customer-security-trust/digital-crimes-unit/notice-of-pleadings/trickbot/

[FN 12] 23-cv-2447 public notice page. Source: Microsoft Digital Crimes Unit, Cracked Cobalt Strike Notice of Pleadings, first publication Apr. 6, 2023. Proposition/application: Establishes the public service/publication page for the cracked-Cobalt-Strike action, initial public document set, and stated emergency relief sought. URL: https://www.microsoft.com/en-us/corporate-responsibility/customer-security-trust/digital-crimes-unit/notice-of-pleadings/cracked_cobalt_strike/

[FN 13] Microsoft April 2023 Cracked Cobalt Strike announcement. Source: Microsoft On the Issues / DCU, "Stopping cybercriminals from abusing security tools," Apr. 6, 2023. Proposition/application: Establishes the public operational account of the 2023 disruption, participants, technical/legal strategy, and collaboration with law-enforcement and international

partners. URL: https://blogs.microsoft.com/on-the-issues/2023/04/06/stopping-cybercriminals-from-abusing-security-tools/

[FN 14] Health-ISAC / Fortra 2023 account. Source: Health-ISAC public account, Fortra/Health-ISAC/Microsoft coordinated action against illegal Cobalt Strike use, Apr. 2023. Proposition/application: Establishes sector-specific public description of the cracked-Cobalt-Strike operation and supporting quotes concerning disruption, C2, and threat-actor adaptation. URL: https://h-isac.org/microsoft-fortra-and-health-isac-take-legal-action-to-disrupt-cracked-cobalt-strike/

[FN 15] Reported 80 percent reduction in abuse. Source: Healthcare IT News and TechTarget reports on Fortra/Microsoft Cobalt Strike abuse reduction and dwell-time metrics, 2025. Proposition/application: Provides public operational-success metrics reported after the 2023 action while remaining distinct from the 2025 final judgment visibility record. URL: https://www.healthcareitnews.com/news/fortra-cobalt-strike-abuse-dropped-80-after-microsoft-court-action

[FN 16] 23-cv-2447 complaint and emergency application. Source: Microsoft Corp., Fortra, LLC, and Health-ISAC, Inc. v. John Does 1-16, No. 1:23-cv-02447 (E.D.N.Y.), complaint and sealed emergency papers, filed Mar. 30, 2023; source-native copies in investigative corpus. Proposition/application: Establishes pleaded defendants, claims, infrastructure, requested TRO/PI, and the initiating litigation architecture.

[FN 17] Christopher Coy declaration. Source: Declaration of Christopher Coy, Microsoft Digital Crimes Unit, filed Mar. 30, 2023 in No. 1:23-cv-02447. Proposition/application: Establishes Microsoft DCU infrastructure research, domain/IP appendix methodology, and provider/control-point foundation.

[FN 18] Jason Lyons declaration. Source: Declaration of Jason Lyons, filed Mar. 30, 2023 in No. 1:23-cv-02447. Proposition/application: Establishes large-scale sample analysis, controlled infection methodology, C2 communication observation, watermark/configuration analysis, victim telemetry, and actor-role mapping.

[FN 19] Robert G. Erdman II declaration. Source: Declaration of Robert G. Erdman II, Fortra, filed Mar. 30, 2023 in No. 1:23-cv-02447. Proposition/application: Establishes Fortra product, licensing, cracked-version identification, cyber-intelligence methodology, New York infrastructure mapping, and Cobalt Strike abuse as malware/ransomware service infrastructure.

[FN 20] Rodelio G. Fiñones declaration. Source: Declaration of Rodelio G. Fiñones, Microsoft DCU, filed Mar. 30, 2023 in No. 1:23-cv-02447. Proposition/application: Establishes Beacon, loader, API, DLL, configuration, metadata, encryption, post-exploitation, process-injection, and watermark technical evidence.

[FN 21] Jonathan Gross declaration. Source: Declaration of Jonathan Gross, filed Mar. 30, 2023 in No. 1:23-cv-02447. Proposition/application: Establishes Microsoft software, product-harm, and Cobalt Strike configuration context for legitimate versus illegitimate use.

[FN 22] Errol Weiss declaration. Source: Declaration of Errol Weiss, Health-ISAC, filed Mar. 30, 2023 in No. 1:23-cv-02447. Proposition/application: Establishes healthcare-sector victim risk, ransomware impact, sector urgency, and Health-ISAC evidentiary role.

[FN 23] 23-cv-2447 Sept. 8, 2025 order adopting R&R. Source: U.S. District Court for the Eastern District of New York, Order Adopting Report and Recommendation, ECF No. 57, Sept. 8, 2025; Justia/vLex/Casemine public mirrors and source-native docket copy. Proposition/application: Establishes adoption of the Aug. 6, 2025 R&R, default judgment, permanent injunction, All Writs Act enforcement, Cobalt Strike domain/IP criteria, Court Monitor provisions, nonparty disclosure path, and jurisdiction not lapsing before Jan. 1, 2030. URL: https://docs.justia.com/cases/federal/district-courts/new-york/nyedce/1%3A2023cv02447/495015/57

[FN 24] 23-cv-2447 docket extracts. Source: Source-native docket extracts for No. 1:23-cv-02447, including Aug. 2024 default materials, Oct. 2024 referral, Sept. 2025 final-order entries, and Nov. 19, 2025 paperless order. Proposition/application: Establishes procedural sequence and public docket state for the capstone case and Rule 71 field test.

[FN 25] Nov. 17-18, 2025 Rule 24/Rule 71 filing set. Source: Emergency delivery sheet, nonparty emergency motion to intervene pursuant to Rule 24 and/or for relief pursuant to Rule 71, verified intervention complaint, supporting affidavit and CNF declaration, proposed order, and related source-native docket entries in No. 1:23-cv-02447. Proposition/application: Establishes the first located later-victim attempt to invoke the five-year successor mechanism, the alleged clientHold/domain and communications emergency, requested technical review and restoration, requested coordination with Microsoft DCU and providers, physical delivery for chambers review, and the postjudgment filing purpose.

[FN 26] Defined 23-cv-2447 visibility search set. Source: Fresh search through Sept. 7, 2026 across Microsoft, Fortra, Health-ISAC, Crowell, named experts, CourtListener/RECAP, Justia, vLex, Notice of Pleadings, Reuters, Law360-accessible abstracts, The Record, CyberScoop, BleepingComputer, The Hacker News, Wired, Ars Technica, SecurityWeek, Dark Reading, KrebsOnSecurity, Google/Bing-indexed sources, X-indexed posts, LinkedIn-indexed public pages, YouTube, podcast/conference pages, and Internet Archive-indexed materials. Proposition/application: Establishes the defined negative/positive visibility comparison for launch-era publicity, final-judgment publicity, postjudgment enforcement, and Rule 71 field-test visibility.

[FN 27] CNF Integrated Expert Report, Oct. 22, 2025. Source: Cyber-N.E.T. Forensics, e-Forensic Integrated Expert Report, Oct. 22, 2025; source-native copy in investigative corpus. Proposition/application: Establishes the subject-side integrated forensic chronology, endpoint/DNS/MX/infrastructure observations, blind-overlay methodology, law-firm/court-channel analysis, and attribution findings.

[FN 28] Marlin Technologies Expert Report. Source: Marlin Technologies Expert Report, Dec. 5, 2024; source-native copy in investigative corpus. Proposition/application: Establishes early endpoint/account/cloud findings and the initial independent technical baseline before later CNF synthesis.

[FN 29] Team B portal datasets. Source: Team B Florida Bar Employee Portal, Florida Bar Membership Portal, and Florida eFile Portal / MyFLCourtAccess datasets; source-native spreadsheet copies in investigative corpus. Proposition/application: Establishes the separately preserved portal-data rails used to test employee/member/e-filing identity and service-channel relationships.

[FN 30] RAPS CM/ECF/DCN/SMTP report. Source: Restricted Access Portal Solutions, Federal CM/ECF, DCN and SMTP Email Relay Expert Report, Feb. 23, 2026; source-native copy in investigative corpus. Proposition/application: Establishes the expert framework separating filing object, intake object, docket entry, NEF/service state, public access, DCN/gateway path, and SMTP relay behavior, and applies that framework to federal case studies.

[FN 31] CCDG Cryptographic-Counterfeit report. Source: Cryptographic Counterfeit Defense Group, Threat Actor Deployment and Exploitation of Cryptographically Manipulated e-Communications, Feb. 25, 2026; source-native copy in investigative corpus. Proposition/application: Establishes the expert finding that SPF/DKIM/DMARC or authorized relay passage authenticates technical path state, not necessarily human intent, workflow authenticity, or record integrity when DNS/MX/relay/mailbox/token authority is compromised.

[FN 32] CNF Sinkhole Report. Source: Cyber-N.E.T. Forensics, Forensic Sinkhole Report, Jan. 20, 2026; source-native copy in investigative corpus. Proposition/application: Establishes registrar/DNS status evidence, domain disabling/redirection, and successor/suppression analysis for the later domain event sequence.

[FN 33] CNF Avatar Report. Source: Cyber-N.E.T. Forensics, Second Supplemental Expert Avatar Report, Jan. 15, 2026; source-native copy in investigative corpus. Proposition/application: Establishes professional-persona, identity-provenance, credential-backed appearance, and public-profile anomaly findings, subject to independent verification for human-identity conclusions.

[FN 34] CNF Federal Court Audit. Source: Cyber-N.E.T. Forensics, Federal Court Audit Report; source-native copy in investigative corpus. Proposition/application: Establishes docket, assignment, service, replacement, page-ID, filing-object, and record-state artifact analysis for federal court proceedings.

[FN 35] E.D.N.Y. 25-cv-06033 primary record. Source: Civil cover sheet; verified complaint and emergency sealing/TRO materials; Nov. 4 order; Nov. 20 clerk-provided docket pages; final filed Nov. 25 venue response; Pro Se Portal and filing-fee records; Dec. 3 memorandum and order; Dec. 4 clerk judgment; and related PageID/ribbon, replacement, service, and paper-copy artifacts in the investigative corpus. Proposition/application: Establishes the E.D.N.Y. field-test chronology, objective filing classification, approximately 700-page asserted submission, chambers/exhibit-access description, replacement-entry state, unnumbered scheduling directive, PageID sequence, notice/service source-state limits, and venue disposition without converting the procedural ruling into a technical adjudication of the complete forensic record.

[FN 36] S.D. Fla. 1:25-cv-23807 primary record. Source: Aug. 22, 2025 file-stamped sealed verified complaint and emergency papers; Sept. 2 clerk-generated sealed docket; Aug. 27 reassignment and deficiency entries; Aug. 28 dismissal order; Sept. 2 cash filing-fee receipt, amended/emergency submissions and verified reconsideration request; Sept. 2 order denying reconsideration; and related verified chronology and notice artifacts in the investigative corpus. Proposition/application: Establishes the after-hours physical filing and payment context, initial magistrate-assignment state, later district-judge reassignment, deficiency/dismissal sequence, payment and reconsideration chronology, asserted notice divergence, and absence of a separately documented technical-integrity review before ordinary procedural consequences attached.

[FN 37] Spagnuolo June 2024 emergency motions. Source: Spagnuolo and Farrow emergency motions filed June 21 and June 25, 2024 in S.D. Fla. No. 0:24-cv-60422; source-native copies in investigative corpus. Proposition/application: Establishes contemporaneous field-case allegations and observed workflow/cyber manifestations before Marlin, Team B, CNF, RAPS, CCDG, Sinkhole, or Avatar reports existed.

[FN 38] February 2025 verified complaint. Source: Farrow et al. verified complaint filed Feb. 5, 2025; source-native copy in investigative corpus. Proposition/application: Serves as a chronology and artifact locator for contemporaneous allegations and claimed real-world manifestations; not used as independent proof of named-party hacker retention.

[FN 39] Florida Supreme Court source-native and verified chronology records. Source: Dec. 27, 2024 protective/in-camera motion and subsequent physical-delivery and communications materials; Jan. 2026 transcript-path records; Feb. 6, 2026 received-stamped original-jurisdiction petition and emergency motion for sealing, in-camera review, paper-only/non-digitized handling, delayed service, secure communication, and stay; Feb. 11 clerk-signed disposition; later verified affidavit consolidating the intake, docket-placement, public-availability, and notice chronology; and any related U.S. Supreme Court submission used only as sworn chronology/provenance rather than as a merits ruling. Proposition/application: Establishes the Florida clean-channel attempt, requested new original-jurisdiction and paper-only path, contested communications/transcript chokepoints, ordinary-channel routing, and denial of the requested alternate handling while preserving the distinction among source-native fact, verified testimony, and expert interpretation.

[FN 40] D.D.C. filed clean-channel record and provenance boundary. Source: Verified complaint in D.D.C. No. 1:25-cv-04308 and the filed March 2, 2026 emergency motion requesting an immediate live in-camera hearing and direct physical presentation of CNF, Marlin, RAPS, CCDG, Florida writ, and related sensitive evidence; source-native copies in the investigative corpus. The separate March 3 supplemental/protective-order or second-amended draft was intentionally not filed and is contextual work product only. Proposition/application: Establishes the federal request for a court-

controlled evidence path before ordinary intake, service, or public routing, and preserves the absolute filed/unfiled source-provenance boundary.

[FN 41] Microsoft OAuth redirection abuse. Source: Microsoft Threat Intelligence, "OAuth redirection abuse enables phishing and malware delivery," Mar. 2, 2026. Proposition/application: Explains how legitimate OAuth and trusted redirect paths can be weaponized while preserving the appearance of trusted service traversal. URL: https://www.microsoft.com/en-us/security/blog/2026/03/02/oauth-redirection-abuse-enables-phishing-malware-delivery/

[FN 42] Microsoft device-code phishing. Source: Microsoft Threat Intelligence, "AI-enabled device code phishing campaign," Apr. 6, 2026. Proposition/application: Explains token acquisition through legitimate device-code workflows, cloud session abuse, Graph reconnaissance, and inbox-rule/data-exfiltration paths. URL: https://www.microsoft.com/en-us/security/blog/2026/04/06/ai-enabled-device-code-phishing-campaign-april-2026/

[FN 43] Storm-0501 cloud-ransomware evolution. Source: Microsoft Threat Intelligence, Storm-0501 hybrid/cloud ransomware analyses, Sept. 26, 2024 and Aug. 27, 2025. Proposition/application: Establishes endpoint-to-hybrid-cloud compromise, Entra/Azure privilege escalation, MFA registration, federated persistence, storage-key abuse, data exfiltration/deletion, and Teams-based extortion. URL: https://www.microsoft.com/en-us/security/blog/2025/08/27/storm-0501s-evolving-techniques-lead-to-cloud-based-ransomware/

[FN 44] OWAReaper / mailbox persistence. Source: BleepingComputer and referenced technical reporting concerning Exchange OWA zero-day / OWAReaper mailbox persistence, July 2026. Proposition/application: Provides independent contemporary mechanism evidence for server-side mailbox persistence that can outlast endpoint reimaging and password rotation when token or mailbox state remains compromised. URL: https://www.bleepingcomputer.com/news/security/russian-hackers-exploit-exchange-owa-zero-day-for-long-term-mailbox-access/

[FN 45] AWS Route 53/IAM control-plane documentation. Source: Amazon Web Services, Route 53 ChangeResourceRecordSets API and AWS IAM access-key documentation, accessed Sept. 7, 2026. Proposition/application: Explains how DNS records can be changed transactionally through legitimate APIs and how access keys/roles represent customer-side authority rather than proof of AWS platform compromise. URL: https://docs.aws.amazon.com/Route53/latest/APIReference/API_ChangeResourceRecordSets.html

[FN 46] NIST digital identity guidelines. Source: NIST SP 800-63-4 Digital Identity Guidelines suite, July/August 2025. Proposition/application: Provides authoritative terminology for identity proofing, authentication, federation, authenticator assurance, and lifecycle controls relevant to account and token evidence. URL: https://pages.nist.gov/800-63-4/

[FN 47] ICANN DNS abuse audit and RDAP resources. Source: ICANN Contractual Compliance, Registry Operator DNS Abuse Audit Report, Jan. 29, 2026, and registration-data/RDAP resources. Proposition/application: Provides current institutional DNS-abuse and registration-data context for domain-hijacking and abuse-reporting analysis. URL: https://www.icann.org/resources/pages/registry-operator-dns-abuse-audit-report-2026-01-29-en

[FN 48] Sitting Ducks / domain hijacking research. Source: Infoblox Threat Intelligence and DNS Research Federation reporting on Sitting Ducks, Vacant Viper, and domain-hijacking measurement, 2024-2026. Proposition/application: Provides independent public research explaining how stale/lame delegations and DNS provider control gaps permit domain hijacking that may appear as legitimate DNS administration. URL: https://www.infoblox.com/blog/threat-intelligence/who-knew-domain-hijacking-is-so-easy/

[FN 49] Lumma Stealer disruption. Source: Microsoft DCU, DOJ, and public reporting concerning Microsoft's 2025 Lumma Stealer disruption. Proposition/application: Establishes modern infostealer civil disruption, domain seizure/blocking/sinkholing at scale, and service-economy successor risk. URL: https://blogs.microsoft.com/on-the-issues/2025/05/21/microsoft-takes-legal-action-against-lumma-stealer/

[FN 50] Fake ONNX / MRxC0DER. Source: Microsoft DCU notice and Microsoft/Crowell public materials concerning Microsoft Corp. and LF Projects, LLC v. Abanoub Nady a/k/a MRxC0DER et al., No. 1:24-cv-02013 (E.D. Va.), 2024. Proposition/application: Establishes AI-themed phishing-as-a-service and approximately 240 fraudulent websites disrupted through civil process. URL: https://www.microsoft.com/en-us/corporate-responsibility/customer-security-trust/digital-crimes-unit/notice-of-pleadings/fake-onnx/

[FN 51] BadBox 2.0. Source: Google, HUMAN Security, FBI and public docket materials concerning Google LLC v. Does 1-25, No. 1:25-cv-04503 (S.D.N.Y.), 2025. Proposition/application: Establishes botnet/service disruption involving millions of compromised uncertified Android/IoT devices, ad fraud, and later permanent/default relief. URL: https://blog.google/threat-analysis-group/badbox-2-0-disruption/

[FN 52] Lighthouse phishing-as-a-service. Source: Google LLC v. Does 1-25, No. 1:25-cv-09421 (S.D.N.Y.), public docket and Reuters/Google materials, 2025. Proposition/application: Establishes a modern PhaaS civil action involving fake websites, templates, payment and credential theft, and preliminary infrastructure relief. URL: https://dockets.justia.com/docket/new-york/nysdce/1:2025cv09421/650833

[FN 53] Darcula / Magic Cat. Source: Google LLC v. Doe 1 a/k/a Yucheng Chang & Does 2-25, No. 1:25-cv-10440 (S.D.N.Y.), public docket and reporting, 2025-2026. Proposition/application: Establishes smishing/phishing-as-a-service, Magic Cat tooling, and permanent civil relief against service infrastructure. URL: https://dockets.justia.com/docket/new-york/nysdce/1:2025cv10440/652652

[FN 54] RedVDS. Source: Microsoft Corp., H2-Pharma, LLC, and Gatehouse Dock Condominium Ass'n v. Does 1-7, No. 1:26-cv-20074 (S.D. Fla.), Microsoft DCU/public materials, 2026. Proposition/application: Establishes disposable virtual-desktop infrastructure as a service for phishing/fraud, with civil relief extending the model to an enabling infrastructure vendor. URL: https://blogs.microsoft.com/on-the-issues/2026/01/14/microsoft-disrupts-cybercrime/

[FN 55] Outsider Enterprise. Source: Google LLC v. Does 1-25 associated with Outsider Enterprise, No. 1:26-cv-04982 (S.D.N.Y.), public docket and 2026 reporting. Proposition/application: Establishes a modern China-based PhaaS platform with AI-assisted phishing templates, more than one million alleged URLs, and preliminary civil relief. URL: https://dockets.justia.com/docket/new-york/nysdce/1:2026cv04982/662821

[FN 56] RaccoonO365 / Storm-2246. Source: Microsoft Corp. and Health-ISAC, Inc. v. Joshua Ogundipe and John Does 1-4, No. 1:25-cv-07111 (S.D.N.Y.), Microsoft notice/public records, 2025. Proposition/application: Establishes identity-centric phishing-as-a-service, adversary-in-the-middle proxying, session-cookie/credential theft, Cloudflare and Telegram/payment infrastructure, preliminary relief and ongoing final-disposition status in the searched record. URL: https://www.microsoft.com/en-us/corporate-responsibility/customer-security-trust/digital-crimes-unit/notice-of-pleadings/raccoono365/

[FN 57] Star Blizzard / ColdRiver. Source: Microsoft Corp. and NGO-ISAC v. John Does, No. 1:24-cv-02719 (D.D.C.), Microsoft and DOJ materials, 2024. Proposition/application: Establishes nation-state spearphishing/domain-disruption relief and concurrent DOJ seizure of related infrastructure. URL: https://blogs.microsoft.com/on-the-issues/2024/10/03/disrupting-star-blizzard/

[FN 58] ZLoader. Source: Microsoft Corp. v. John Does 1-10, No. 1:22-cv-01328 (N.D. Ga.), Microsoft notice and court materials, 2022. Proposition/application: Establishes relief against hard-coded domains, DGA domains, sinkhole transfer, and future-DGA blocking architecture. URL: https://noticeofpleadings.com/zloader/

[FN 59] Barium / Brass Typhoon. Source: Microsoft Corp. v. John Does 1-2, No. 1:17-cv-01224 (E.D. Va.), Microsoft public materials and court records. Proposition/application: Establishes nation-state portfolio disruption involving fake profiles, dead-drop resolver text, RATs, and continuing court-monitor process. URL: https://blogs.microsoft.com/on-the-issues/2017/10/30/microsoft-disrupts-cyberespionage-group-strontium/

[FN 60] Phosphorus / Charming Kitten. Source: Microsoft Corp. v. John Does 1-2, No. 1:19-cv-00716 (D.D.C.), Microsoft public materials and court records, 2019. Proposition/application: Establishes a nation-state domain-seizure/sinkhole action against 99 sites and continued use of civil process against rebuilt infrastructure. URL: https://blogs.microsoft.com/on-the-issues/2019/03/27/we-are-taking-new-steps-against-broad-phishing-campaigns/

[FN 61] WhatsApp/Facebook and Apple v. NSO. Source: WhatsApp Inc. and Facebook, Inc. v. NSO Group Technologies Ltd., No. 4:19-cv-07123 (N.D. Cal.), and Apple Inc. v. NSO Group Technologies Ltd., No. 3:21-cv-09078 (N.D. Cal.), public court records and party materials. Proposition/application: Establishes platform/identity/spyware comparators and the tension between public litigation and sensitive threat-intelligence disclosure. URL: https://docs.justia.com/cases/federal/district-courts/california/candce/4:2019cv07123/349579

[FN 62] Bohrium / Smoke Sandstorm. Source: Microsoft Corp. v. John Does 1-2, No. 1:22-cv-00607 (E.D. Va.), Microsoft notice/public records, 2022. Proposition/application: Establishes nation-state malicious-domain disruption and preservation relief in the standard Microsoft civil-disruption lineage. URL: https://www.microsoft.com/en-us/corporate-responsibility/customer-security-trust/digital-crimes-unit/notice-of-pleadings/bohrium/

[FN 63] CryptBot. Source: Google LLC v. Zubair Saeed et al., No. 1:23-cv-03369 (S.D.N.Y.), public docket and Google materials, 2023. Proposition/application: Establishes controlled-download/pay-per-install evidence, credential theft, and final permanent/default relief against infostealer distribution infrastructure. URL: https://blog.google/technology/safety-security/disrupting-cyber-crime-with-legal-action-against-cryptbot/

[FN 64] Fake Bard. Source: Google LLC v. Does 1-3, No. 5:23-cv-05823 (N.D. Cal.), public court records and Google materials, 2023. Proposition/application: Establishes platform/identity litigation against AI-themed malware impersonation, malicious social pages and downloads. URL: https://blog.google/technology/safety-security/protecting-people-from-ai-enabled-scams/

[FN 65] Google crypto-app scam action. Source: Google LLC v. Yunfeng Sun and Hongnam Cheung, No. 1:24-cv-02559 (S.D.N.Y.), public docket and Google materials, 2024. Proposition/application: Establishes civil relief against app-store/developer-account based confidence scams, alternative service, default and permanent injunction. URL: https://docs.justia.com/cases/federal/district-courts/new-york/nysdce/1:2024cv02559/618887/48

[FN 66] Meta phishing / scraping / SDK matters. Source: Meta/Facebook civil cases concerning 39,000-site phishing, Voyager Labs, OneAudience, and BrandTotal, public dockets and Meta materials. Proposition/application: Establishes platform-account, scraping, malicious-SDK, browser-extension, and identity-based civil remedies as service/platform comparators. URL: https://about.fb.com/news/2021/12/taking-action-against-phishing/

[FN 67] Amazon REKK and KDP impersonation matters. Source: Amazon civil actions concerning REKK refund fraud and Kindle Direct Publishing impersonation networks, public dockets and Amazon materials. Proposition/application: Establishes fraud-as-a-service, platform identity, refund abuse, and publishing impersonation comparators. URL: https://www.aboutamazon.com/news/company-news/amazon-takes-legal-action-against-refund-fraud-ring

[FN 68] United States v. Palumbo. Source: United States v. Nicholas Palumbo et al., No. 1:20-cv-00473 (E.D.N.Y.), DOJ/public docket materials, 2020. Proposition/application: Establishes a civil enforcement comparator targeting fraudulent robocall gateway infrastructure and permanent consent decree. URL: https://www.justice.gov/opa/pr/united-states-files-enforcement-action-against-two-telecommunications-companies-and-their

[FN 69] Plaintiff-counsel DNS and publication-domain source set. Source: RDAP/ICANN/DNS/certificate/archive records for material plaintiff-counsel and publication domains, including Crowell, Orrick, King & Spalding, Pillsbury, WilmerHale, Cooley, Perkins Coie, Freshfields, Davis Wright Tremaine, Susman Godfrey, Alston & Bird, CourtListener/RECAP, Notice of Pleadings, Justia, and vLex; refreshed source set through Sept. 7, 2026 where public lookups remained available. Proposition/application: Establishes client-domain versus provider-family state, current and historical authoritative-provider facts, and publication-control-surface evidence. URL: https://lookup.icann.org/

[FN 70] Public reporting on court-system cybersecurity. Source: Reuters and other public reporting on 2025 federal ECF/PACER compromise concerns and 2026 C-Track exposure. Proposition/application: Provides independent public context for judicial case-management and court-record security risk beyond the subject-side expert reports. URL: https://www.reuters.com/

[FN 71] 23-cv-2447 final-order public mirrors. Source: Justia Dockets, vLex, CaseMine and Midpage public versions of the Sept. 8, 2025 Order Adopting Report and Recommendation in Microsoft Corp. et al. v. John Does 1-16, No. 1:23-cv-02447 (E.D.N.Y.). Proposition/application: Confirms that the final order is publicly findable in legal repositories while remaining distinct from party, counsel, expert, or cyber-media explanation of the five-year mechanism. URLs include https://docs.justia.com/cases/federal/district-courts/new-york/nyedce/1%3A2023cv02447/495015/57 and https://case-law.vlex.com/vid/microsoft-corp-v-does-1090551157.

[FN 72] Post-emergency Cobalt Strike public-success reporting. Source: Health-ISAC, Fortra, TechTarget/HealthTechSecurity, Healthcare IT News and related public accounts published March 2025 concerning the Microsoft/Fortra/Health-ISAC partnership. Proposition/application: Establishes the pre-final-order visibility baseline and reported operational metrics, including the approximately 80 percent reduction in unauthorized Cobalt Strike copies and shortened dwell-time claims, against which the September 2025 final-order visibility state is compared.

[FN 73] E.D.N.Y. 25-cv-06033 docket and PageID artifacts. Source: Clerk-provided docket images dated Nov. 20, 2025; Nov. 4, 2025 order; Nov. 18 scheduling-order row; Pro Se Portal messages; and Dec. 3, 2025 Memorandum and Order in Farrow v. John Does 1-20, No. 1:25-cv-06033-AMD-PK. Proposition/application: Establishes the primary record-state facts used in Part IX, including document replacement language, visible docket-number state, exhibit availability, PageID sequence, venue-response disposition, and the court's adverse citation-integrity findings.

[FN 74] 23-cv-2447 November 18-19 docket field-test materials. Source: Clerk-provided and public docket images for Microsoft Corp. et al. v. John Does 1-16, No. 1:23-cv-02447 (E.D.N.Y.) showing Nov. 18, 2025 Docket Entry 61 emergency Rule 24/Rule 71 motion, Docket Entry 62 exhibit filing, and Nov. 19, 2025 text/order directive concerning ex parte designation and plaintiffs' response. Proposition/application: Establishes the State-Four later-victim invocation record and the docket-state observations analyzed in Part V and Part IX.

[FN 75] CNF October 22 portal and DNS/MX synthesis. Source: Cyber-N.E.T. Forensics, Integrated Expert Report, Oct. 22, 2025, including the MyFLCourtAccess DNS/name-server, Route 53, portal-event, unauthorized-login, missing-confirmation, synchronized-window and law-firm/court-channel sections. Proposition/application: Provides the subject-side integrated forensic rail explaining how apparently valid portals, DNS/MX states, and front-end user experience can coexist with adversary-in-the-middle control in a legal workflow.

[FN 76] NIST Advanced Persistent Threat definition. Source: National Institute of Standards and Technology, Computer Security Resource Center Glossary, "Advanced Persistent Threat," accessed Sept. 7, 2026. Proposition/application: Defines an APT by sophisticated expertise/resources, multiple attack vectors, extended footholds, repeated pursuit, adaptation to resistance, and objectives that include exfiltration or undermining/impeding a mission, program, or organization. URL: https://csrc.nist.gov/glossary/term/advanced_persistent_threat

[FN 77] SolarWinds authoritative public history. Source: U.S. Government Accountability Office, SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response, GAO-21-594T, 2021, and related GAO SolarWinds materials. Proposition/application: Establishes trusted-software supply-chain compromise and the scale of Orion distribution/federal follow-on compromise as an accepted example of persistent access through a trusted control layer. URL: https://www.gao.gov/products/gao-21-594t

[FN 78] Storm-0558 cloud-identity compromise. Source: Microsoft Security Response Center, "Microsoft mitigates China-based threat actor Storm-0558 targeting of customer email," July 11, 2023. Proposition/application: Establishes use of an acquired signing key and forged authentication tokens to access cloud email in approximately twenty-five organizations, including government organizations, demonstrating trusted identity/token control as an APT access mechanism. URL: https://www.microsoft.com/en-us/msrc/blog/2023/07/microsoft-mitigates-china-based-threat-actor-storm-0558-targeting-of-customer-email

[FN 79] August 2025 federal judiciary case-management breach reporting. Sources: Administrative Office of the U.S. Courts, "Cybersecurity Measures Strengthened in Light of Attacks on Judiciary's Case Management System," Aug. 7, 2025; Reuters, "US federal courts say their systems were targeted by recent cyberattacks," Aug. 7, 2025; Politico, reporting on the federal court filing-system breach, Aug. 6, 2025; Reuters follow-up regarding protective measures for people potentially exposed in court-record compromise, Aug. 14, 2025. Proposition/application: Establishes the Judiciary's own acknowledgment of sophisticated/persistent attacks and independent public reporting that the federal case-management/filing environment and sensitive case information were high-value targets. URLs: https://www.uscourts.gov/data-news/judiciary-news/2025/08/07/cybersecurity-measures-strengthened-light-attacks-judiciarys-case-management-system ; https://www.reuters.com/legal/litigation/us-federal-courts-say-their-systems-were-targeted-by-recent-cyberattacks-2025-08-07/ ; https://www.politico.com/news/2025/08/06/federal-court-filing-system-pacer-hack-00496916 ; https://www.reuters.com/legal/government/us-taking-special-measures-protect-people-possibly-exposed-court-records-hack-2025-08-14/

[FN 80] Marlin Technologies expanded methodology. Source: Marlin Technology Expert Report: Summary Opinion, Dec. 5, 2024, pp. 2-12; source-native copy in investigative corpus. Proposition/application: Establishes engagement questions, materials examined (court artifacts/screenshots, 220+ domain reports, two computer devices and domain-email-server records), open-source cross-checking, early access/administrative-control findings, DNS/MX and man-in-the-middle mechanism analysis, and the pre-CNF technical baseline.

[FN 81] RAPS expanded methodology. Source: Restricted-Access Portal Solutions, Federal CM/ECF, DCN and SMTP Email Relay Expert Report, Feb. 23, 2026, especially pp. 3-12; source-native copy in investigative corpus. Proposition/application:

Establishes portal-integrity methodology; document-driven reconstruction of dockets, orders, clerk notices and physical records; SMTP relay/authentication analysis; DNS/MX correlation; deliberately separated analysis; and the distinction among authentication, portal workflow, internal routing, service and public record states.

[FN 82] CCDG expanded methodology. Source: Cryptographic Counterfeit Defense Group, Threat Actor Deployment and Exploitation of Cryptographically Manipulated e-Communications, Feb. 25, 2026, especially pp. 2-14; source-native copy in investigative corpus. Proposition/application: Establishes the cryptographically aligned/operationally counterfeit communication model; analysis of DNS, SPF/DKIM/DMARC, relay, link, recipient, timing and workflow states; independent/blind multi-modal review; more than 57 judicial e-communication metadata items; and portal/DNS correlation findings.

[FN 83] Refreshed 23-cv-2447 visibility and State-Four audit. Source: targeted public-source refresh through Sept. 7, 2026 across Microsoft/DCU/Security, Fortra, Health-ISAC, Crowell, named experts, Notice of Pleadings, CourtListener/RECAP, Justia, vLex, CaseMine, Midpage, GovInfo, Leagle, and other legal repositories, Reuters and major cyber/legal press, Google/Bing-indexed public pages, X/LinkedIn public indexing, YouTube, podcasts/conferences and Internet Archive. Farrow/JCDC/USNewsDirect-controlled material was logged separately and not counted as independent. Result/application: conservatively verifies at least eight distinct pre-final explanatory/metrics items; at least six legal-repository/government/indexed presentations of the Sept. 8 final order; zero independent party/counsel/named-expert/major-media items specifically explaining the Sept. 8-9 final judgment, Court Monitor criteria, nonparty path or how to invoke the five-year mechanism; and zero specific public postjudgment successor determinations/enforcement events. A later Fortra retrospective repeating pre-final metrics and a general Microsoft DCU program page mentioning Court Monitor/automated disruption were classified separately because neither identifies a 23-cv-2447 postjudgment successor determination or invocation procedure. Representative URLs: https://www.microsoft.com/en-us/corporate-responsibility/customer-security-trust/digital-crimes-unit/notice-of-pleadings/cracked_cobalt_strike/ ; https://blogs.microsoft.com/on-the-issues/2023/04/06/stopping-cybercriminals-from-abusing-security-tools/ ; https://docs.justia.com/cases/federal/district-courts/new-york/nyedce/1%3A2023cv02447/495015/57 ; https://www.infosecurity-magazine.com/news/number-unauthorized-cobalt-strike/ ; https://www.fortra.com/blog/new-report-highlights-rogue-cobalt-strike-down-80-beacon-still-1-malware-family ; https://www.fortra.com/blog/fortras-top-10-standout-moments-2025 ; https://www.microsoft.com/en-us/corporate-responsibility/topics/cybersecurity/disrupting-cyberthreats-since-2008/

[FN 84] Star Blizzard final disposition refresh. Source: Microsoft Corp. and NGO-ISAC v. John Does, No. 1:24-cv-02719 (D.D.C.), public docket/legal-source refresh through Sept. 7, 2026, including Aug. 5, 2026 memorandum opinion/default judgment and permanent injunction; Microsoft/DOJ public operation materials. Proposition/application: Updates State Three from preliminary domain relief to located durable final relief. Representative sources: https://www.drdocket.com/case/microsoft-corporation-v-john-does-1-2-dcd-2024 ; https://blogs.microsoft.com/on-the-issues/2024/10/03/disrupting-star-blizzard/

[FN 85] Bohrium final disposition refresh. Source: Microsoft Corp. v. John Does 1-2, No. 1:22-cv-00607 (E.D. Va.), public docket/legal-source refresh through Sept. 7, 2026, including Jan. 30, 2024 default judgment/permanent injunction materials. Proposition/application: Establishes durable State Three relief after the earlier domain-disabling/preservation phase. Representative source: https://www.drdocket.com/case/microsoft-corporation-v-john-does-1-2-vaed-2022

[FN 86] Glupteba corrected case and aftermath. Source: Google LLC v. Dmitry Starovikov et al., No. 1:21-cv-10260 (S.D.N.Y.), public docket and Google/public technical materials, including Sept. 30, 2022 Doe-default and Nov. 15, 2022 sanctions/default proceedings. Proposition/application: Corrects the case number/caption used in the baseline and establishes continued default/sanctions history alongside publicly documented operator rebuilding and blockchain-assisted fallback. URL: https://law.justia.com/cases/federal/district-courts/new-york/nysdce/1%3A2021cv10260/571146/129/

[FN 87] RaccoonO365 disposition/visibility refresh. Source: Microsoft Corp. and Health-ISAC, Inc. v. Joshua Ogundipe and John Does 1-4, No. 1:25-cv-07111 (S.D.N.Y.), Microsoft Notice of Pleadings and public docket, refreshed through Sept. 7, 2026. Proposition/application: Establishes Aug./Sept. 2025 TRO sequence, Sept. 24 preliminary injunction, and a later request for entry of default/default judgment while no entered final judgment was located in the refreshed public record; accordingly State Three remains unresolved and no post-final visibility inference is made. URLs: https://www.microsoft.com/en-us/corporate-responsibility/customer-security-trust/digital-crimes-unit/notice-of-pleadings/raccoono365/ ; https://docs.justia.com/cases/federal/district-courts/new-york/nysdce/1%3A2025cv07111/648428/32

[FN 88] Darcula / Magic Cat final disposition refresh. Source: Google LLC v. Doe 1 a/k/a Yucheng Chang & Does 2-25, No. 1:25-cv-10440 (S.D.N.Y.), public docket/legal repositories, Apr. 7, 2026 default judgment/permanent-relief materials. Proposition/application: Updates State Three to located durable final relief. Representative source: https://app.midpage.ai/document/google-llc-v-doe-1--37efa908-5d64-4826-8623-254127cd1d41

[FN 89] Sophos case-specific source correction. Source: Sophos Ltd. v. John Does 1-2, No. 1:20-cv-00502 (E.D. Va.), source-native/public emergency pleadings and technical declarations in investigative corpus, refreshed public-source check through Sept. 7, 2026. Proposition/application: Replaces the erroneous field-case citation in the baseline; establishes emergency provider/domain relief and the absence of a separately located entered permanent infrastructure order in the defined public source set through cutoff.

[FN 90] DXC case-specific source correction. Source: DXC Technology Co. v. John Does 1-2, No. 1:20-cv-00814 (E.D. Va.), Mark Hughes declaration, public notice/default-judgment materials and R&R recommending default/permanent relief, refreshed through Sept. 7, 2026. Proposition/application: Replaces erroneous field-case citations in the baseline; establishes Cobalt Strike BEACON/reverse-proxy/rotating-domain evidence and the located default/permanent-relief recommendation, while

no separately entered final permanent order was located in the refreshed public set. Representative source: https://dxclegalnotice.com/files/Default%20Judgement/DXC-R%26R%20on%20Default%20Jud.pdf

[FN 91] Amadey-StealC case-specific source. Source: Microsoft Corp. v. Does 1-5, No. 1:26-cv-24064 (S.D. Fla.), source-native/public June-July 2026 complaint, TRO/PI and disruption materials, refreshed through Sept. 7, 2026. Proposition/application: Separates the Amadey-StealC joint loader/infostealer action from the Lumma citation and records preliminary-relief posture at cutoff.

[FN 92] Thirty-five-case aftermath and visibility refresh protocol. Source: targeted case-by-case public/source-native refresh through Sept. 7, 2026 using final signed orders/docket objects where available, official party/operation pages, counsel pages, public dockets/legal repositories, cyber/legal press, publicly indexed social/video/podcast/conference material and archives. Proposition/application: Authenticates Appendix B's bounded State Three, State Four, aftermath and visibility states. "Not located" means no responsive item was located in the defined public/source-native classes through cutoff; it is not converted into a claim about nonpublic events.

Appendix G - Publication Acceptance Checks Applied

Gate	Result
Internal-draft contamination	Reader-facing report text contains no old draft/version labels and no prior-assistant history.
Single unified report	One DOCX contains Main Report, integrated compendium/appendices and source notes.
Footnote test	Narrative paragraphs contain the evidentiary story before Source Notes; [FN #] markers authenticate rather than replace findings.
23-cv-2447 capstone	Dedicated Part V reconstructs March 2023, declarants, final order, successor mechanism, visibility collapse and Rule 71 field test.
35-case population	Compendium uses 35 representative cases and replaces the non-representative field slot with TrickBot.
Field-case separation	Spagnuolo/Farrow proceedings appear only as field/adjudicative-channel evidence.
D.D.C. boundary	March 2 material is filed; March 3 draft is not filed and is not treated as court-received.
CAE	Final institutional section supplies concrete intake, custody, review and reconciliation architecture.
APT / cAPTure narrative	Part III now supplies an authoritative APT bridge, accepted public examples, judiciary attack-surface context, progressive expert-rail chronology, functional distinctions and an earned cAPTure-to-Kill definition before the aftermath study.
State Three / State Four	Part IV and Appendix B state actual final dispositions, successor mechanisms, adaptation, later-victim access and bounded public visibility rather than cryptic partial/mixed labels.
Visibility counts	23-cv-2447 distinguishes pre-final publicity, legal-repository availability, independent final-remedy explanation, general program-level references, and specific public later-enforcement events through Sept. 7, 2026.
RaccoonO365 discipline	RaccoonO365 is coded at its current preliminary/default-motion posture; unresolved persona provenance is not converted into a standalone natural-person attribution.
Circular-trust landing	Part X explains why paper routed immediately back through the disputed electronic chain is not a clean integrity determination and ties CAE controls to earlier demonstrated failure modes.