CYBER-N.E.T. FORENSICS

cAPTure-to-Kill APT

MAPPING, ATTRIBUTING, AND CONTAINING AN EVOLVING THREAT

Threat Assessment of Adversary Objectives, Target Selection, Trusted-Control-Plane Exploitation, Operational Adaptation, Forecasting, Mitigation, and Containment

JAY LEWIS FARROW
Lead Author • Senior Editor • Investigative and Logistical Coordinator

FORENSIC INVESTIGATION, THREAT ANALYSIS, AND RESEARCH
Cyber-N.E.T. Forensics Investigative and Technical Research Teams

OPERATIONAL AND COLLABORATIVE SUPPORT
The collaborative work reflected in this assessment includes private-sector relationships developed with the broader Joint Cyber Defense Collaborative and international cyber-defense ecosystems.

Contents

CYBER-N.E.T. FORENSICS AND THE JOINT CYBER DEFENSE COLLABORATIVE ECOSYSTEM

A. The Joint Cyber Defense Collaborative - Public-Private Operational Context

Established by the U.S. Cybersecurity and Infrastructure Security Agency in 2021, the Joint Cyber Defense Collaborative (JCDC) was designed to move public-private cyber defense beyond episodic information sharing toward coordinated, real-time collaboration. Its operating premise is complementary. Federal agencies contribute statutory authorities, national convening power, government-wide visibility, intelligence, and responsibility for public accountability. Private-sector organizations contribute platform telemetry, infrastructure knowledge, incident experience, specialist personnel, research, and the capacity to mobilize technical resources against rapidly changing conditions.

That structure addresses a recurring operational problem. Significant cyber incidents develop across systems owned or observed by different organizations: victims, cloud and communications providers, registrars, security vendors, researchers, courts, and government agencies may each hold a different portion of the relevant evidence. Public institutions necessarily operate within legal, policy, classification, procurement, evidentiary, and interagency constraints. Private organizations may sometimes assemble specialized technical resources more rapidly, but they do not possess the same governmental authorities or national coordinating role. The JCDC model reduces the distance between those capabilities so that shared visibility can become coordinated defensive action.

References in this report to the broader JCDC ecosystem describe that public-private operational context and the professional relationships through which some private-sector contributors work. They do not state that Cyber-N.E.T. Forensics is a component of CISA or JCDC, or that CISA, JCDC, or another government agency supervised, funded, directed, adopted, approved, or endorsed this Threat Assessment. The distinction between collaborative alignment and governmental authorship is maintained throughout this publication.

B. Cyber-N.E.T. Forensics - Mission, Structure, and Investigative Role

Cyber-N.E.T. Forensics (CNF) is a distributed private forensic and investigative ecosystem. Specialists may work under the CNF banner for a defined common mission while remaining organizationally independent. The structure is organized around the evidentiary and operational demands of a matter rather than a fixed institutional hierarchy. Relevant work may include digital forensics, incident response, technical preservation, threat attribution, infrastructure analysis, containment, lawful

defensive disruption, threat-model development, legal-process analysis, and cross-source correlation.

CNF focuses on the relationships among systems that are often examined separately. Endpoint state, credentials, sessions, cloud authority, DNS and MX records, communications, portal activity, record-state transitions, timing, and real-world consequences may each appear ordinary when viewed alone. CNF preserves those evidence classes in their source-native form and tests whether independently developed workstreams converge on a common mechanism. Provider presence is not treated as actor identity, a successful authentication event is not treated as proof of human authority, and a procedural consequence is not treated as proof of technical cause without supporting evidence.

This approach also reflects the conditions of advanced incident response. A persistent adversary may rotate infrastructure, reuse legitimate services, divide tasks among affiliates, or continue operating through credentials and permissions after a visible endpoint has been replaced. The investigative objective is therefore not limited to locating one malicious file or domain. It is to preserve the technical breadcrumbs, custody records, configuration evidence, and institutional state needed to confirm, narrow, contain, or disprove the assessed operation as later intelligence becomes available.

C. Specialized CNF Analytical Rails - CCDG and RAPS

Within the CNF investigative architecture, specialized analytical rails address narrower trust questions. The Cryptographically Counterfeit Defense Group (CCDG) examines the distinction between cryptographic authentication and human or workflow authenticity. A message may pass SPF, DKIM, or DMARC and still be operationally counterfeit when the authorized account, tenant, relay, signing path, session, or DNS state is controlled by someone other than the intended principal. CCDG therefore reconstructs the full communications path rather than treating a passing authentication result as the end of the integrity inquiry.

Bridge-Gate E.S.S. Division's Restricted Access Portal Solutions (RAPS) examines restricted-access portals and the institutional workflows behind them. Its analytical focus includes identity issuance and recovery, filing credentials, intake, routing, service, notification, payment, assignment, document custody, docket state, and the possibility that the object submitted by one participant may diverge from the object received, routed, served, displayed, or later preserved by another. RAPS treats a portal as a workflow engine whose valid transactions can carry legal or professional consequences.

CCDG and RAPS are identified separately because methodological separation improves auditability. They are specialized components or analytical rails within the CNF investigative architecture; they are not CISA-created or JCDC-controlled

entities. Their findings remain attributable to the source records and reports that generated them and are integrated here only at the level supported by the preserved evidence.

D. Contributor Protection, Compartmentation, and Operational Security

Not every individual or organization that contributed investigative, technical, incident-response, infrastructure, source-review, or legal-process work is identified in this public edition. That omission is deliberate. Public disclosure of particular identities, workstreams, tasking, technical access, infrastructure, methods, containment activity, or source relationships could expose ongoing investigations, operational tradecraft, personnel, or capabilities and could create new targeting risk.

The work was therefore conducted through distributed, compartmented, need-to-know collaboration. Contributors received and produced only the information required for their assigned function, and separate workstreams were integrated at controlled points. Withholding public attribution does not diminish those contributions. It protects the people, organizations, sources, methods, and continuing response activity that made the work possible while preserving the report's responsibility to state what evidence supports each published conclusion.

Some contributors operate within or maintain professional relationships in the broader JCDC ecosystem. That context reflects alignment with public-private cyber-defense principles and rapid collaborative incident response. It does not convert a private contribution into governmental authorship or imply that an unnamed contributor, employer, public agency, or collaborative initiative accepts the findings stated in this report.

E. Authorship, Editorial Responsibility, and External Source Acknowledgment

Jay Lewis Farrow served as Lead Author and Senior Editor, with responsibility for the report architecture, legal-process and source chronology, integration of the investigative record, narrative synthesis, editorial review, and preparation of the public publication. Cyber-N.E.T. Forensics Investigative and Technical Research Teams are separately credited for the work performed through the CNF investigative structure. The National Attorneys Cybersecurity Association (NACABAR) Editorial Staff and Research Team provided editorial and research support.

Technical findings attributed to CNF, Marlin Technologies, Team B, RAPS, CCDG, the Sinkhole and Avatar reports, the Federal Court Audit, sworn declarants, government agencies, vendors, courts, and other identified sources remain attributable to those respective sources. Editorial integration does not convert a cited source finding into an independently generated finding solely because it appears in

this assessment. CNF remains responsible for the findings expressly attributed to CNF in this public edition.

The report also acknowledges the substantial published work of agencies, courts, declarants, technology companies, security researchers, academic authors, technical journalists, and other source creators identified in the Source Register and Full Endnotes. Their research, declarations, orders, advisories, documentation, reporting, and other records provide the external evidence against which the CNF-family findings are tested. Citation recognizes that work; it does not imply direct participation in, authorship of, or endorsement of this report.

Executive Findings

Report Lineage and Present Function

This publication is a current cAPTure-to-Kill APT Threat Assessment Report. It is not a declaration that the investigation has ended, and it is not a simple reissuance of the October 22, 2025 CNF Integrated Expert Report. A threat assessment serves a different function. It takes a preserved body of earlier findings, tests those findings against later source material, identifies which mechanisms have now been independently documented in other environments, and states how the present evidentiary posture has changed. Cybersecurity conclusions must remain capable of revision because threat actors rotate infrastructure, change credentials, alter delivery methods, reuse trusted services, and adapt when investigators or courts disrupt a prior pathway. The report therefore describes the current source-supported threat posture as of the stated evidence cutoff, while preserving the underlying artifacts and analytical limits for later review. **[FN 1]** **[FN 37]** **[FN 297]** **[FN 298]**

The source architecture is substantial but intentionally divided by function. This assessment reviews 98 external cybersecurity source records, together with a separate body of primary court materials, sworn declarations, prior expert reports, portal records, DNS and MX data, email metadata, endpoint artifacts, and event-specific technical matrices. The number 98 is not offered as a measure of truth by volume. Its evidentiary value lies in independent government agencies, technology providers, security researchers, courts, expert declarants, and technical journalists documenting the same operational building blocks that the CNF-family reports had identified in the subject environment. MITRE ATT&CK is used only to name and organize techniques; it is not counted as new threat intelligence because a framework label does not independently prove that an event occurred. **[FN 1]** **[FN 2]** **[FN 56]** **[FN 57]**

The earlier reports form a sequence rather than a stack of interchangeable conclusions. Marlin Technologies supplied the first independent endpoint, account, DNS, MX, and administrative-control baseline. It examined whether the observed activity was targeted, persistent, technically sophisticated, and capable of interfering with law-firm communications, websites, network systems, and court-filing functions. **[FN 47]** **[FN 79]**

The October 22 CNF Integrated Expert Report then overlaid endpoint, credential, DNS, MX, portal, communications, and litigation evidence to describe a coordinated attack on the trusted environment through which legal work was performed. [FN 1] [FN 3] [FN 32] Team B preserved separate employee, membership, and e-filing portal datasets so that identity and access events could be examined as structured records rather than reconstructed only from memory. [FN 50] [FN 213]

The later rails addressed narrower trust questions. RAPS examined restricted-access portals, CM/ECF, the federal Data Communications Network, SMTP gateways, filing objects, service events, docket state, and the possibility that the record received by one participant could diverge from the object seen by another. [FN 22] [FN 45] [FN 214] CCDG examined the difference between cryptographic authentication and human or workflow authenticity: a message may pass SPF, DKIM, or DMARC and still be operationally counterfeit if the authorized account, relay, tenant, signing path, or DNS state has been controlled. [FN 16] [FN 178] [FN 186] The Sinkhole report examined registrar- and DNS-level suppression, redirection, and successor infrastructure. [FN 36] [FN 145] [FN 261] The Avatar report examined professional-persona provenance and the risk that stolen, blended, or synthetic identities can be converted into genuine institutional credentials. [FN 18] [FN 190] The Federal Court Audit preserved docket, PageID, replacement, assignment, service, and record-object anomalies for source-native comparison. [FN 33] [FN 215]

This threat assessment asks whether later evidence makes those earlier findings more technically plausible, more precisely bounded, or less persuasive. The answer is not uniform at every layer, but it is affirmative across the principal mechanisms. The strongest change is that several capabilities once described mainly through subject-side artifacts are now documented through independent primary sources: long-lived privileged cloud keys; API-driven DNS changes; persistent OAuth and mailbox access; legitimate collaboration platforms used for delivery and interactive control; developer mirrors used as trusted redirect infrastructure; false workers obtaining real devices and credentials; and persistent attacks against the federal judiciary's own case-management environment. [FN 4] [FN 5] [FN 17] [FN 19] [FN 20] [FN 21] [FN 23]

The Assessed Control Plane

The phrase trusted control plane is used in this report to identify the systems and authorities that determine who is permitted to act and what downstream systems will treat as legitimate. In a legal-professional environment, that control plane includes account identity, authentication, cloud permissions, DNS, mail routing, document custody, filing portals, service lists, case-management systems, professional directories, collaboration platforms, and the public publication channels through which official action becomes visible. These systems are not merely administrative conveniences. They decide which server answers for a domain, which mailbox receives a notice, which user can alter a record, which document becomes the filed object, which

recipients are served, and which version enters the public record. [FN 3] [FN 16] [FN 22] [FN 32]

The cAPTure-to-Kill model concerns an adversary that seeks value from controlling that plane. The operation may include malware, phishing, extortion, data theft, or ransomware, but those tools do not define the model. The distinctive objective is to capture, corrupt, delay, suppress, redirect, or exploit the trusted pathways through which professional and adjudicative outcomes are created, communicated, routed, preserved, and enforced. A visible ransomware event announces itself because the attacker wants payment. A control-plane operation may be more valuable when the systems continue to appear functional while their outputs, recipients, timing, or authoritative state are being shaped. [FN 32] [FN 278] [FN 279] [FN 280]

That distinction explains why ordinary-looking events carry forensic significance only when they converge. A remote-management agent may be legitimate software. A Route 53 change may be an authorized administrative action. An email may pass authentication. A professional profile may be genuine. A portal may record a successful login. A court docket may display a document. None of those facts alone proves hostile control. The threat assessment arises when different evidence rails - endpoint artifacts, valid credentials, cloud permissions, DNS changes, mail behavior, portal events, identity anomalies, record-state differences, and event timing - repeatedly align around the same operational objective. [FN 48] [FN 49] [FN 281] [FN 282] [FN 283] [FN 284] [FN 285]

Principal Findings

First, the current record materially strengthens the assessment that valid credentials can turn legitimate enterprise infrastructure into attacker-operated infrastructure without requiring an exploit against the cloud provider itself. Truffle Security directly revalidated 10,616 exposed AWS key pairs and found that 88 percent still authenticated. Of the live business-linked keys, 768 carried root or Administrator Access privileges capable of controlling substantial portions of the affected accounts. [FN 4] [FN 5] AWS's own Route 53 documentation explains that DNS record changes may be submitted in transactional CREATE, DELETE, and UPSERT batches, while IAM permissions determine which identities can perform those actions. [FN 6] [FN 7] The provider may therefore process a technically valid request even when the credential was stolen, exposed, fraudulently retained, or used by someone other than the intended principal.

Second, the July 31, 2025 synchronized Route 53 window now has a clearer operational mechanism. The October 22 report preserved an approximately three-to-four-minute cluster involving roughly thirty domains and a common Route 53 nameserver family during a filing-related event. [FN 8] [FN 151] The new AWS-key evidence does not identify the exact actor or principal responsible for that subject event. It does, however, establish that one privileged credential, organization-level root identity, or

administrator account can apply coordinated changes across multiple hosted zones or related resources at the speed and scale previously observed. [FN 9] [FN 10] [FN 11] [FN 158] The event is therefore no longer supported only by temporal clustering and provider concentration; it is consistent with a documented cloud-control method capable of producing the cluster through ordinary APIs.

Third, the August 5, 2025 alias and CloudFront condition receives stronger mechanism support. The earlier CNF record described a normal-looking public presentation while the web path resolved through an alias involving ccplatform.net and Amazon CloudFront. [FN 12] Later campaigns independently demonstrate the same architecture in operational use. BleepingComputer and OX Security documented malicious HTML rendered from legitimate npm and mirror domains, with the final destination capable of changing remotely without republishing the original package. [FN 13] [FN 65] [FN 66] SynkLoader used Microsoft Teams impersonation and an Azure-hosted installer before capturing credentials and establishing interactive access. [FN 14] [FN 63] [FN 64] Nimbus Manticore used compromised systems as relays and Microsoft Graph calendar data as a covert channel. [FN 15] Those sources do not prove who controlled the August 5 path. They independently establish that reputable cloud, collaboration, CDN, and developer infrastructure can preserve trusted appearance while the underlying origin, relay, or destination is attacker-directed.

Fourth, the communications assessment is materially strengthened by OWAReaper. CCDG's prior finding was that technical authentication proves specified features of the path, not necessarily the intent of the named sender or the integrity of the workflow. [FN 16] The 2026 OWAReaper disclosure provides a direct operational example: the actor changed server-side mailbox permissions, stole OAuth tokens, retained access after endpoint reimaging and password rotation, proxied exfiltration through image CDN domains, and preserved a DNS fallback. [FN 17] The practical consequence is direct. If the server-side permission, token, tenant, relay, or mailbox rule remains controlled, replacing the user's device and changing the visible password may leave the communications channel compromised.

Fifth, the Avatar assessment now rests within a much larger public record of credential-backed identity operations. The FBI and Department of Justice have documented DPRK-linked operators and facilitators using false or stolen identities, U.S.-based laptop farms, fraudulent websites, remote hiring, and legitimate enterprise access. [FN 19] [FN 20] KnowBe4 publicly described an applicant who passed interviews, was hired, and received a corporate laptop before the false-worker scheme was detected. [FN 195] Recorded Future and peer-reviewed studies describe blended identities, deepfake-assisted verification, persistent enterprise footholds, coordinated artificial personas, and detection systems that struggle when a synthetic profile imitates normal user history. [FN 21] [FN 197] [FN 198] The point is not that every sparse or inaccurate professional profile is malicious. It is that institutional trust can

be granted to the wrong human actor while every downstream system treats the issued device, account, and credential as genuine.

Sixth, the federal judiciary's public record now independently validates the class of risk that RAPS treated as structurally important. In August 2025, the Administrative Office of the U.S. Courts acknowledged sophisticated and persistent attacks against the Judiciary's case-management system and announced stronger handling for sensitive documents. [FN 23] Subsequent official releases described acute and persistent risk in the aging CM/ECF environment and an accelerated modernization program, including secure-cloud storage and replacement of outdated case-management components. [FN 24] [FN 25] Multifactor authentication became mandatory for filing-level and other CM/ECF-privileged users, while PACER-only users remained eligible but not nationally required to enroll. [FN 26] [FN 27] [FN 28] These measures do not prove that any particular docket anomaly was malicious. They establish that identity, case-management, and sensitive-record compromise are not speculative attack classes.

Seventh, Microsoft Corporation et al. v. John Does remains the strongest independent attribution and methodology anchor within this report. Microsoft's sworn declarations did not identify infrastructure merely because it was hosted by a particular provider. The declarants described Beacon configuration, watermark analysis, controlled infection, crawler data, victim telemetry, credential harvesting, screenshots, keylogging, process injection, lateral movement, and actor-role relationships involving Conti, LockBit, TrickBot, BazaLoader, AnchorDNS, ransomware services, and access brokers. [FN 29] [FN 30] [FN 31] The September 8, 2025 permanent injunction converted that technical record into court-authorized domain, DNS, IP, server, preservation, and continuing-enforcement relief. [FN 254] This report therefore treats exact IoC, tool, telemetry, timing, and configuration convergence as materially stronger than a shared provider or ASN.

Current Threat Posture and Limits

CNF's present assessment is that the accumulated endpoint, credential, cloud, DNS, MX, portal, identity, court-system, communications, and real-world evidence supports a deliberate and adaptive cAPTure-to-Kill operation directed at the digital environment through which professional and adjudicative outcomes are created, communicated, routed, and preserved. [FN 32] [FN 33] [FN 34] [FN 35] [FN 36] The assessment is strongest at the capability and control-plane level, and strongest in event-specific attribution where subject artifacts intersect with exact Microsoft infrastructure, technical telemetry, tool behavior, credential evidence, or tightly bounded timing.

The assessment does not rest on the proposition that every anomaly was malicious, that every legitimate provider was compromised, or that one natural person or one

threat group controlled every event. Provider infrastructure is shared. Administrative changes can be benign. Court systems generate text-only orders and clerical corrections. Professional identities may have incomplete public histories for ordinary reasons. Those alternatives are not excluded by rhetoric; they are tested against the full evidentiary sequence. The report therefore distinguishes observed state from inferred cause, provider service from customer-side control, technical authentication from human authority, and capability attribution from natural-person attribution. [FN 48] [FN 51] [FN 52] [FN 255] [FN 257]

The practical conclusion is not that the earlier CNF findings should be treated as permanently fixed. It is that the later evidence materially increases confidence in the model and provides a clearer roadmap for continuing attribution. Current threat intelligence now documents how long-lived credentials, server-side mailbox control, cloud roles, DNS APIs, trusted relays, collaboration platforms, synthetic identities, and restricted-access portals can be combined into a low-salience operation. The final sections of this report therefore assess not only what has been corroborated, but what must remain under observation as adversaries modify the infrastructure and trust relationships that make the operation effective. [FN 297] [FN 299] [FN 304] [FN 305] [FN 306] [FN 307]

I. Purpose and Controlling Question

A. Defining the cAPTure-to-Kill APT Threat Assessment

The prior working title described this publication as an updated continuing-investigation report. That description was historically accurate but functionally incomplete. In cybersecurity, the word update can suggest that an earlier report has simply been amended or that investigators have reached the end of a defined project and are publishing the latest version. The present work has a different purpose. It assesses the current capability, persistence, adaptation, and risk of an adversarial model whose infrastructure and methods are expected to change over time. [FN 37] [FN 297]

A threat assessment is necessarily point-in-time. It states what the available evidence supports at a defined cutoff, identifies the level of confidence attached to major findings, and preserves the distinction between what is known, what is strongly inferred, and what still requires additional provider or system logs. It is designed to remain useful when later intelligence identifies a credential, domain, ASN, service principal, mailbox rule, portal event, or infrastructure relationship that could not be fully understood when the original artifact was collected. [FN 52] [FN 137] [FN 298]

The October 22 CNF report supplied the original integrated model. It described a campaign in which endpoint compromise, credential theft, DNS and MX control, portal access, trusted communications, and legal-workflow interference were not isolated incidents but connected means of controlling a professional digital ecosystem. [FN 38]

The present assessment does not ask the reader to accept that model because CNF previously stated it. It asks whether independent evidence published from 2023 through August 26, 2026 - with particular attention to material appearing after October 22, 2025 - now documents the same mechanisms in unrelated organizations, public incident reports, government advisories, product documentation, sworn declarations, and court orders. [FN 39] [FN 40] [FN 41] [FN 42] [FN 43]

B. The Controlling Question

The controlling question is therefore precise: does the later record independently explain, corroborate, qualify, or contradict the technical mechanisms previously identified in the subject environment? The inquiry is not whether a later article uses the phrase cAPTure-to-Kill. It is whether later sources document the same operational primitives: persistence that survives endpoint replacement; valid-account activity that looks administrative; cloud credentials that control DNS and storage; authenticated communications sent through a controlled path; synthetic identities receiving real credentials; trusted mirrors and collaboration systems used for delivery; portal actions performed under apparently legitimate identity; and case-management environments exposed to sophisticated persistent attack. [FN 40] [FN 41] [FN 42] [FN 43]

The answer is affirmative across those principal layers. Current public evidence describes living-off-the-land operations, remote-management abuse, workload and metadata credential theft, long-lived AWS keys, OAuth and refresh-token persistence, federated cloud roles, server-side mailbox permissions, Teams impersonation, trusted package mirrors, DNS delegation hijacking, false-worker infiltration, and persistent attacks on the federal judiciary's case-management environment. [FN 58] [FN 62] [FN 63] [FN 65] [FN 68] [FN 71] [FN 81] [FN 84]

That affirmative answer does not convert every subject event into a proved hostile act. It changes the mechanism assessment. An event that once appeared technically unusual but difficult to explain may become more plausible when an independent source later documents the exact control method. Conversely, a mechanism source cannot establish that the mechanism was used in the subject environment without subject-specific evidence. This report therefore uses later sources to test capability, feasibility, persistence, and operational fit; it does not use analogy as a substitute for the underlying artifacts. [FN 48] [FN 51] [FN 258]

C. Scope of the Real-World Record

The legal and professional events addressed in this report are included as manifestations of technical control, not as invitations to re-decide the merits of unrelated proceedings. A missed notice, altered recipient list, delayed filing, unavailable document, changed DNS record, portal event, account-recovery action, or docket-state difference has forensic significance because it may be the observable result of a compromised identity or workflow. The report examines whether those

outcomes align with technical artifacts and independent mechanisms. It does not treat the procedural consequence alone as proof of the cause. [FN 44] [FN 45]

The same discipline applies to institutional actors. The use of AWS, Microsoft, Cloudflare, a court system, a law firm, a registrar, or a collaboration platform does not imply wrongdoing by that provider or institution. Large-trusted services are valuable to adversaries precisely because legitimate traffic is expected to pass through them. The relevant question is whether the customer-side identity, account, tenant, hosted zone, relay, mailbox, portal profile, or administrative authority was controlled or misused. [FN 94] [FN 114] [FN 127] [FN 257]

The purpose of the assessment is ultimately operational: to give investigators, incident responders, lawyers, judges, law clerks, government personnel, and technology providers a coherent account of how the separate mechanisms fit together. The report should permit a reader to understand why a valid login, a passing email, a functioning website, or a visible docket does not by itself resolve the integrity question. It should also permit a skeptical reader to identify the evidence needed to reject or confirm the assessment - provider audit logs, credential history, mailbox permission changes, DNS API records, portal access telemetry, file hashes, document versions, service lists, or authenticated custody records. That is the controlling standard applied throughout the report.

II. Investigative Corpus, Methodology, and Evidence Standards

A. The Four-Layer Proof Model

The assessment uses a four-layer proof model because no single class of evidence can responsibly carry the entire conclusion. The first layer is primary subject evidence: endpoint artifacts, DNS and RDAP records, MX history, email headers, portal events, court records, document-state differences, and preserved real-world timing. This layer establishes what was observed in the subject environment. It is the starting point, not the final attribution. [FN 46] [FN 50]

The second layer is prior expert analysis. Marlin, CNF, Team B, RAPS, CCDG, Sinkhole, Avatar, and the Federal Court Audit examined different portions of the environment at different times. Their value lies partly in that separation. Marlin addressed endpoint, account, network, and DNS conditions before the later integrated CNF model was completed. Team B preserved portal datasets. RAPS focused on restricted-access and record-state consequences. CCDG focused on communications authenticity. Sinkhole focused on registrar and DNS suppression. Avatar focused on persona and credential provenance. The Federal Court Audit focused on source-native docket and document-state artifacts. [FN 47] [FN 50] [FN 214] [FN 215]

The third layer is independent primary authority. Government advisories, vendor research, official product documentation, sworn declarations, and court orders

establish mechanisms and threat behavior outside the subject narrative. AWS documentation explains how Route 53 and IAM work. Microsoft Threat Intelligence describes cloud and identity campaigns. CISA and the FBI document living-off-the-land activity, access brokers, false workers, and ransomware ecosystems. The Administrative Office of the U.S. Courts describes the judiciary's own attack and modernization posture. Microsoft declarants explain how cracked Cobalt Strike infrastructure was identified. [FN 5] [FN 6] [FN 7] [FN 23] [FN 81] [FN 249] [FN 250]

The fourth layer is post-report corroboration. These are later sources that document the same operational primitive identified in an earlier expert finding. OWAReaper is post-report corroboration for server-side mailbox and token persistence. Long-lived AWS keys are corroboration for cloud credential custody. SynkLoader and the npm mirror campaign are corroboration for trusted collaboration and developer infrastructure used as an attack path. DPRK false-worker cases are corroboration for credential-backed identity. Judiciary disclosures are corroboration for persistent case-management risk. [FN 17] [FN 58] [FN 63] [FN 65] [FN 68] [FN 71]

The strongest determinations are those in which all four layers converge. A subject artifact establishes that something happened. A prior expert report explains the initial interpretation. An independent primary source establishes that the mechanism exists and is used in real operations. A later source may then clarify persistence, scale, or implementation. Where only one layer exists, the report uses correspondingly restrained language. [FN 48] [FN 49]

B. Evidence Is Not Counted by Volume Alone

The 98-source external corpus is screened by evidentiary function rather than treated as a collection of interchangeable citations. An official API specification can establish how a provider processes a request, but not who submitted it. A government advisory can establish a known campaign method, but not that the campaign caused a subject event. Technical journalism can identify and explain primary research, but the underlying vendor or government source remains the stronger mechanism authority. A sworn declaration can establish the declarant's method and findings in a separate case, but it does not automatically transfer attribution to a different environment. [FN 54] [FN 55] [FN 56]

MITRE ATT&CK is deliberately excluded from the new-source count. The framework supplies a common vocabulary for techniques such as valid accounts, command and control, credential access, or DNS tunneling. It does not independently verify that a technique occurred in a particular case. Using MITRE as a nomenclature system avoids inventing private labels for well-known methods while preserving the separate burden of proof. [FN 56] [FN 57]

The report also distinguishes direct sources from explanatory secondary sources. For example, Truffle Security's research supplies the primary revalidation of AWS keys;

BleepingComputer provides contemporaneous technical reporting that makes the findings accessible. [FN 58] [FN 59] AWS documentation supplies the authoritative description of Route 53 transactions and permissions. [FN 60] [FN 61] The same pattern is used throughout: identify what a source can prove, avoid asking it to prove more, and position the citation adjacent to the claim it supports.

C. Normalization, Timing, and Negative Evidence

The portal datasets illustrate why normalization is necessary. The public-facing assessment uses aggregate counts - 54 employee-environment rows, 317 membership-environment rows, and 1,278 e-filing-environment rows, covering dates from February 2023 through December 2024. [FN 50] Those rows are not treated as 1,649 confirmed compromises. They are event records. Each must be evaluated by user identity, source infrastructure, URL, timing, authentication state, device or session information where available, and correlation with DNS, communications, or real-world consequences. [FN 51]

DNS and registration records require a similar distinction. A registration-data update timestamp proves that a registry or registrar record changed or was refreshed at that recorded time. It does not necessarily identify the exact second a hostile DNS record was altered, and it does not identify the person responsible. [FN 52] [FN 53] The evidentiary value increases when updates recur across unrelated domains, cluster within a narrow window, correspond to a common provider family, and align with separate endpoint, portal, email, or litigation events. That is the basis of the Synchronized Update Window method, not the assumption that every timestamp is an attack timestamp. [FN 137] [FN 138] [FN 139]

Court and declaration evidence is treated as source-native authority. Orders are identified by date, court, document, and page where available. Declarations are attributed to the declarant and cited by filing date and paragraph where the source note provides the pinpoint. [FN 54] [FN 55] The report separates what a docket visibly records from what an expert infers. A replacement notation, text-only entry, internal hostname, missing public document, or service-list difference can be a measurable record state. Determining whether that state resulted from benign administration, ordinary system behavior, error, or malicious interference requires additional evidence.

Negative evidence is also bounded. The absence of a public result in a defined search does not prove that no private event occurred. It establishes only that the searched source classes did not reveal the event by the cutoff. The same principle applies to missing logs or unavailable provider records. The report identifies the resulting evidentiary limit rather than filling the gap with certainty.

D. Attribution Standards

Attribution is graded by the specificity of the overlap. Exact IoCs, configuration values, malware behavior, credential artifacts, provider account data, identical IP addresses, synchronized timestamps, or linked telemetry can support a strong event-specific relationship. A shared cloud provider, CDN, registrar, or large ASN is weaker because many unrelated customers use the same infrastructure. [FN 255] [FN 256] [FN 257]

The report therefore distinguishes four attribution levels: exact artifact or telemetry overlap; infrastructure-family or service relationship; tool or TTP lineage; and broad mechanism analogy. Those levels should not be collapsed. A Route 53 nameserver establishes use of Route 53. It does not identify the customer principal. A Cobalt Strike-like capability establishes tool lineage only if the configuration, watermark, behavior, or other evidence supports that conclusion. A valid email path establishes use of the path, not the human intent behind the message. [FN 250] [FN 253] [FN 257]

This methodology is designed to be falsifiable. A provider's audit history could show that a disputed DNS change was authorized by a known administrator. A mailbox log could show no permission alteration. A portal backend could show that a user action originated from a recognized device and session. A file hash comparison could show that the filer, intake, docket, and recipient copies are identical. The threat assessment becomes stronger when those controls are absent, unavailable, or contradicted by other evidence; it becomes weaker when authoritative logs provide a benign explanation. The purpose of the model is disciplined testing, not preservation of a conclusion at all costs.

Evidence class	Examples	Use in this report
Primary subject evidence	Endpoint artifacts; DNS/RDAP; MX; headers; portal events; court records	Establishes what occurred in the subject environment.
Prior expert analysis	CNF; RAPS; CCDG; Marlin; Portal; Sinkhole; Avatar	States earlier findings being re-tested.
Independent primary authority	Government advisories; vendor research; sworn declarations; court orders	Establishes mechanisms, actor tradecraft and infrastructure outside the subject narrative.
Technical journalism	BleepingComputer; Reuters; Politico; The Hacker News	Provides contemporaneous reporting and identifies underlying primary research.
Framework reference	MITRE ATT&CK	Names techniques; does not count toward the new-source requirement.

III. What Changed After October 22, 2025

A. From Mechanism Hypothesis to Documented Operating Practice

The October 22 CNF report identified a control-plane campaign before several of the most instructive public examples had been disclosed. It described endpoint persistence, credential theft, cloud custody, DNS manipulation, communications

control, portal misuse, and trusted-system exploitation as parts of one adaptive operation. [FN 38] The post-October record does not merely add more names to a source list. It changes the evidentiary posture by documenting how those mechanisms operate at scale, how they survive ordinary remediation, and how legitimate infrastructure can remain visually and cryptographically trusted while serving an adversarial purpose.

The first change is scale and longevity in cloud credentials. Truffle Security did not merely find secret strings in public repositories; it attempted to authenticate 10,616 AWS key pairs and reported that 88 percent remained valid. The research identified 768 business-linked keys with root or Administrator Access authority, including credentials old enough to demonstrate that enterprise secrets can remain operational for years. [FN 58] [FN 59] The earlier CNF analysis treated cloud identity as a possible explanation for rapid, coordinated administrative changes. The later evidence shows that long-lived privileged access is not a rare theoretical condition.

The second change is precision in the DNS mechanism. AWS's official Route 53 API documentation explains that an authorized principal can submit multiple CREATE, DELETE, and UPSERT record changes as a transaction. Its service-authorization documentation separately identifies the IAM permissions that allow a user or role to list hosted zones and alter record sets. [FN 60] [FN 61] That combination supplies the missing technical bridge between a privileged identity and a tightly synchronized multi-zone event. The cloud provider does not need to be compromised; it performs the requested actions under the authority presented to it.

The third change is persistence outside the visible endpoint. OWAReaper demonstrated a webmail compromise that changed server-side mailbox permissions and obtained OAuth tokens. The resulting access survived password rotation and endpoint reimaging because the durable control existed in the mailbox and identity layer, not only on the user's device. [FN 62] In operational terms, the user can replace a computer and believe the incident is over while another authorized organizational account, token, or permission continues to expose the mailbox.

The fourth change is consolidation of delivery, credential theft, and interactive control inside trusted collaboration services. SynkLoader used Microsoft Teams impersonation to reach the target, Azure hosting to deliver the installer, a fake Windows lock screen to capture a password, reverse proxying and tunneling to establish access, and remote shell or VNC functionality to operate the environment. [FN 63] [FN 64] The chain is operationally continuous: a message in a familiar collaboration platform can become credential capture, session access, remote execution, and hands-on control without requiring the victim to traverse an obviously malicious domain.

The fifth change is trusted developer infrastructure as a mutable redirect layer. The npm mirror campaign used legitimate package and mirror domains to render malicious HTML and redirect victims to an attacker-selected destination. The final destination could be changed without republishing the original package, allowing the trusted hosting surface to remain stable while the operational endpoint moved. [FN 65] [FN 66] This provides a direct analogue for a broader cAPTure principle: reputation controls may correctly identify the visible domain as legitimate while failing to identify who controls the content or destination at the moment of use.

The sixth change is persistence through physical proximity and device-to-device relaying. Manic demonstrated encrypted exfiltration over Wi-Fi Direct, Bluetooth, and Bluetooth Low Energy through nearby infected devices, including multi-hop movement from an endpoint that was not directly online. [FN 67] The example expands the threat model beyond the assumption that disconnection from a conventional network ends communication. It shows how an adversary can preserve an alternate path when the primary route is unavailable or under observation.

The seventh change is synthetic institutional identity. The FBI, DOJ, Recorded Future, KnowBe4, and peer-reviewed researchers have now documented operations in which false or blended identities pass hiring or verification, receive real devices and accounts, and operate inside enterprise networks as apparently legitimate users. [FN 68] [FN 69] [FN 70] This moves the Avatar problem from persona appearance to credential issuance. The decisive compromise may occur when an institution grants trust to the wrong person, not when that person later defeats an authentication control.

The eighth change is federal acknowledgement of case-management risk. The Judiciary publicly confirmed sophisticated and persistent attacks against its case-management system, strengthened sensitive-document procedures, required multifactor authentication for CM/ECF-level users, and accelerated replacement of an aging platform. [FN 71] [FN 72] [FN 73] [FN 74] Additional reporting described prior warnings, restricted sealed filings, and calls for independent review. [FN 75] [FN 76] [FN 77] [FN 78] This does not prove any subject case event. It changes the background assumption: the court-system attack surface is an acknowledged operational reality, not a hypothetical premise created by the subject investigation.

B. The Common Direction of the New Evidence

These developments arise in different sectors, from different sources, and through different technologies. Their common direction is control through trust. The adversary does not need to replace every system with a counterfeit. It can obtain or manufacture the authority that the legitimate system expects: a valid key, a token, a server-side permission, a cloud role, a trusted domain, a collaboration identity, an employee

profile, or a filing credential. The system then produces ordinary-looking outputs on the adversary's behalf.

That is why the later record materially strengthens the cAPTure-to-Kill assessment. The earlier reports identified a pattern in which technical compromise translated into altered professional and adjudicative outcomes. The new evidence shows that the required mechanisms are current, scalable, and increasingly designed to survive narrow remediation. The following sections examine each control layer separately before reconstructing the July 31 and August 5 event windows as integrated sequences.

IV. Endpoint Persistence, Zero-Days, and Living-Off-the-Land Operations

A. The Endpoint Is the First Foothold, Not the Entire Operation

An endpoint is the user's computer, mobile device, server, or workload from which activity begins. Traditional incident response often centers on finding a malicious file, removing it, reimaging the machine, and changing the user's password. That approach remains necessary, but it is incomplete against a persistent adversary. Once the attacker has obtained tokens, cloud keys, mailbox permissions, remote-management access, or trusted portal credentials, the endpoint can be cleaned while the broader operation survives elsewhere. [FN 79] [FN 80]

Marlin's December 2024 report supplied the first independent technical baseline for this environment. It examined devices, court materials, screenshots, domain and email-server records, and more than 220 ICANN-related reports. Marlin concluded that the observed activity was consistent with an advanced persistent threat and that access escalated through 2024 toward administrator-level control over the network, website DNS, cloud storage, and credentials. [FN 47] [FN 79] That conclusion predated the later CNF integration and is therefore important as an independent chronological rail.

The October 22 CNF report then connected endpoint persistence to the wider control plane. It considered remote-administration activity, credential reuse, lateral movement, cloud-delivered payloads, DNS and MX changes, portal events, and synchronized windows. [FN 80] The resulting model did not require one distinctive malware family to remain continuously visible. It described a patient adversary that could move among endpoints, accounts, cloud services, and communication paths as conditions changed.

B. Living Off the Land and Legitimate Management Tools

Living off the land describes the use of built-in operating-system functions, legitimate administration tools, or trusted management agents to conduct malicious activity.

CISA, NSA, FBI, and partner agencies have documented state-sponsored actors using valid accounts, native commands, remote services, and normal administrative utilities to reduce the number of distinctive malware artifacts defenders can detect. [FN 81] The technique is effective because the same tool may be used every day by legitimate administrators.

Mitiga's analysis of AWS Systems Manager demonstrates the principle in a cloud-connected environment. An adversary can re-register the legitimate SSM Agent and use it as a remote-access mechanism, turning an approved management tool into an attacker channel. [FN 82] Sysdig's SCARLETEEL research shows the progression from a compromised workload to temporary cloud credentials, secrets in Terraform state, reduced logging, and lateral access to additional cloud services. [FN 84] [FN 85] In both examples, the operation gains value from using administrative pathways the environment already trusts.

The 2026 Lazarus campaign adds the zero-day and identity dimensions. The reported operation used fraudulent recruitment against defense-sector employees, exploited CVE-2026-68820 to elevate privileges to SYSTEM, deployed a rootkit that interfered with security controls, and used compromised webmail infrastructure in later stages. [FN 86] [FN 87] A zero-day denies defenders the benefit of a preexisting signature or patch, while the identity and webmail elements permit the operation to continue after the initial exploit has done its work.

Additional government and primary research confirms that legitimate management agents, compromised routers, automated botnets, and actively exploited industrial or endpoint vulnerabilities can be combined. [FN 91] [FN 92] [FN 93] [FN 94] The resulting activity may look like ordinary administration, remote support, or encrypted web traffic. The absence of a loud encryption event or a persistent executable does not negate the possibility of sustained control.

C. Current Endpoint Assessment

The endpoint record remains technically coherent with a multi-path adversary. The assessment is not that every crash, service, update, or remote connection was malicious. It is that the preserved endpoint evidence, Marlin's early diagnosis, CNF's cross-layer integration, and later public examples all support an operation designed to maintain more than one route of access. [FN 88] [FN 89] [FN 90]

The practical evidentiary question is therefore wider than whether malware is found on the current machine. Investigators must ask whether a remote-management enrollment changed, whether cloud credentials were exposed, whether a service principal or federated role persists, whether a mailbox permission or token survived, whether a router or nearby device provides an alternate path, and whether new activity appears after the endpoint was replaced. The next section examines that

continuity at the identity layer, where a credential can outlive the device from which it was first stolen.

V. Credential Capture: Passwords, Sessions, Tokens, Cloud Keys, and Service Accounts

A. Credentials as a Continuum of Authority

A password is only one form of credential. Modern enterprise systems also rely on browser sessions, cookies, OAuth access tokens, refresh tokens, device registrations, API keys, service principals, workload identities, mailbox permissions, federated trust, and cloud roles. Each represents a different way of proving authority to a system. [FN 95] [FN 96] [FN 97] An attacker who obtains one form may be able to create or preserve another, which is why changing the visible password does not necessarily terminate access.

A browser session or access token can allow continued use until it expires or is revoked. A refresh token can generate new access tokens. An OAuth grant can authorize an application to act on a user's behalf. A service principal or workload identity can operate without an interactive human login. A federated domain or delegated administrator relationship can create trust at the tenant level. Server-side mailbox permissions can allow one account to read another mailbox. The credential continuum is therefore a chain of authorities, not a single secret.

AWS access keys provide a concrete cloud example. An Access Key ID and Secret Access Key allow software or a user to call AWS APIs under the permissions assigned to that principal. [FN 98] A root access key represents the AWS account itself. An IAM user with Administrator Access can create, alter, view, or delete almost all account resources and can often establish additional credentials or roles. [FN 99] [FN 100] The power of the key is determined by its permissions and placement, not by whether it appears in a familiar login screen.

B. Longevity, Exposure, and Cross-Service Reach

Truffle Security's revalidation work is especially significant because the median live exposed AWS key was approximately five years old and many keys had never been rotated. [FN 101] [FN 102] Long-lived credentials are compatible with the persistence horizon of an APT. They can remain dormant, be used intermittently, or be transferred among operators while the customer continues to treat the associated identity as legitimate.

Cloud credentials can also be acquired indirectly. Active server-side request forgery probing against EC2-hosted applications has targeted the instance metadata service to recover IAM-role credentials. [FN 103] [FN 104] The attacker may begin with a web application flaw but end with the authority of a cloud role. From there, the operation

can reach storage, DNS, logging, compute, secrets, or additional services according to the role's permissions.

CISA and the FBI documented Androxgh0st campaigns that searched exposed environment files for AWS, Microsoft 365, SMTP, SendGrid, and Twilio credentials. [FN 105] This illustrates why one initial exposure can bridge several platforms. An environment file may contain the keys to cloud infrastructure, transactional email, messaging, and other service providers. The attacker does not need to compromise each company separately; it uses the victim's own credentials to ask those companies to perform authorized actions.

Microsoft's Storm-0501 reporting provides the corresponding identity-chain example. The actor used valid credentials, registered attacker-controlled MFA, elevated a nonhuman identity to Global Administrator, created federated-domain persistence, obtained Azure roles and storage keys, and used Teams in the extortion workflow. [FN 106] [FN 107] That progression shows why a credential event can become a tenant-governance event. Once the attacker controls how trust is issued or federated, removing one password may have little effect.

C. Credential Persistence Within the cAPTure Model

The earlier CNF reports treated credential capture as the bridge between endpoint access and control of the wider professional ecosystem. [FN 108] [FN 109] [FN 110] [FN 111] The later evidence materially strengthens that proposition. A valid identity can alter DNS, read or reroute mail, access shared evidence, administer cloud storage, change notification settings, enroll an authenticator, or use a portal under the appearance of an authorized user.

This is also where intent becomes difficult to infer from provider logs alone. The cloud provider records that a valid principal submitted a request. The email service records that a permitted account opened a mailbox. The portal records a successful login. Those records may be technically accurate while the human authority is false. Attribution therefore requires custody history: who controlled the key or token, what device or workload used it, whether new credentials were created, what permissions changed, and whether the activity aligns with other events.

The current assessment is that identity persistence is one of the strongest explanations for why visible remediation may fail. The endpoint can be replaced, the password changed, and the public website restored, while the attacker retains a refresh token, administrator role, server-side permission, API key, or delegated trust. The next section explains how legitimate cloud platforms act on those surviving authorities.

VI. Enterprise Cloud Abuse: AWS, Route 53, Azure, Entra, and Legitimate Control Planes

A. Legitimate Services Acting on Compromised Authority

Amazon Web Services is a broad enterprise environment used for compute, applications, storage, identity, content delivery, logging, and DNS. Route 53 is AWS's managed DNS service, and CloudFront is its content-delivery network. [FN 112] [FN 113] Microsoft Azure provides comparable compute and storage services, while Microsoft Entra provides identity, application, device, and access governance. These services are not malicious. Their value to an adversary comes from their legitimacy, scale, and ability to act automatically on valid customer authority.

The relevant attack model is therefore not that Amazon or Microsoft must be hacked. It is that a valid customer credential, role, workload identity, service principal, token, or tenant configuration is used without the intended customer's authority. [FN 114] [FN 115] [FN 116] The platform processes the request according to its rules. To a downstream user or security tool, the result may continue to appear as ordinary traffic from a reputable provider.

B. AWS, Route 53, and Transactional Control

Route 53's ChangeResourceRecordSets operation accepts transactional batches of CREATE, DELETE, and UPSERT requests. [FN 117] A transaction permits several related DNS changes to be applied together, reducing the risk that a zone remains in a partially updated state. From an administrative perspective, that is a reliability feature. From an incident-response perspective, it means that one authorized workflow can alter several records in a tightly bounded interval.

AWS's service-authorization documentation identifies the permissions required to list hosted zones and change record sets. [FN 118] The decisive control point is therefore the identity that holds those permissions. A stolen root key, administrator key, assumed role, compromised workload identity, or maliciously created principal can use the same API as a legitimate operator. Provider-level evidence is needed to identify the principal, request source, role chain, and account context.

The whoAMI research adds an infrastructure-as-code route. If automated deployment searches for an Amazon Machine Image by name without constraining the trusted owner, an attacker can publish a matching image and cause ordinary automation to select it. [FN 119] [FN 120] The code enters the victim account through the victim's own deployment process. This is an important control-plane pattern: the attacker does not defeat the cloud platform; it exploits how the customer configured trust.

C. Azure, Entra, and Collaboration Control

Azure and Entra provide parallel opportunities through user accounts, application consent, service principals, device registrations, federated domains, privileged roles, and storage keys. [FN 123] [FN 124] [FN 125] Storm-0501 demonstrates how an adversary can move from credentials to tenant-level authority and persistence. SynkLoader demonstrates how Teams and Azure hosting can serve as the delivery and access chain. [FN 106] [FN 107] [FN 130]

The report treats an unverified claim concerning an Azure directory sale narrowly. It is not used to establish that a particular directory was breached. Its relevance is the type of data reportedly offered - employee identity, service accounts, tenant domains, and administrators - because those attributes are precisely what an actor needs for targeted impersonation, password spraying, social engineering, or account recovery. [FN 126] The evidentiary boundary is preserved: an advertised dataset is not proof of the subject event.

D. Trusted Mirrors, CDNs, and Reputable Origins

The npm mirror campaign shows the same principle outside a cloud console. Malicious HTML was rendered from legitimate package-mirror domains, allowing reputation controls to see a trusted host while the page redirected the user to an attacker-controlled destination. [FN 121] [FN 122] The destination could change remotely without altering the original package artifact. This separation between trusted visible origin and mutable operational destination is directly relevant to CDN, proxy, and alias analysis.

CloudFront, Azure hosting, collaboration platforms, and developer mirrors can all be used as layers between the user and the final attacker resource. TLS may be valid. The domain may belong to a reputable provider. The application may behave normally until a specific request, user, region, or time condition is met. The integrity question is therefore not answered by the provider's reputation or the browser padlock. It requires origin configuration, account custody, request logs, alias history, certificates, content hashes, and timing.

E. Current Cloud-Control Assessment

The current cloud literature explains a coherent progression from credential capture to authoritative control of DNS, storage, proxying, collaboration, and identity while remaining inside infrastructure that appears legitimate. [FN 127] [FN 128] [FN 129] [FN 130] NIST's digital identity standards and CISA's cloud baselines reinforce the same lesson: authentication strength, authenticator lifecycle, phishing resistance, application consent, logging, and tenant configuration are inseparable from cloud security. [FN 131] [FN 132] [FN 133] [FN 134]

This report accordingly treats cloud-provider presence as a starting fact, not an attribution result. AWS, Azure, CloudFront, or another provider identifies the service layer. The evidentiary question is which customer identity, role, tenant, hosted zone, distribution, or origin controlled the action. That distinction is central to the DNS analysis that follows.

VII. DNS Abuse and the Persistent SUW Footprint

A. DNS as the Routing Layer of the Professional Ecosystem

The Domain Name System is the distributed directory that translates a human-readable domain into the servers and services that handle web, email, and other traffic. Authoritative nameservers are the systems permitted to publish the domain owner's DNS answers. [FN 135] [FN 136] If an adversary controls the authoritative answer, it can redirect users to a different web origin, change where email is delivered, alter validation records, or make the domain unavailable without changing the content stored on the legitimate hosting server.

Several DNS record types matter in this assessment. An A or AAAA record points a name to an IP address. A CNAME or alias can point one name to another service or distribution. An MX record identifies the mail exchangers that receive email for the domain. TXT records may carry SPF, verification, or other policy data. The SOA record identifies administrative and timing information for the zone. Time-to-live, or TTL, controls how long resolvers cache an answer before asking again. RDAP and registration data identify registrar, status, dates, and other registration-layer information. These records describe different parts of the routing and custody chain; no single record provides the whole answer.

B. Registration Timestamps and Synchronized Update Windows

A registration-data update timestamp is a durable metadata event. It proves that the registration record was updated or refreshed at the recorded time. It does not automatically prove that an attacker changed a particular DNS record at that exact second. [FN 137] This distinction is essential because registry and registrar systems may update timestamps for multiple reasons, including administrative changes, renewals, status modifications, nameserver changes, or internal processing.

CNF uses the term Synchronized Update Window, or SUW, for a narrow period in which multiple otherwise unrelated domains or systems display coordinated changes that are then compared with independent events. The probative value comes from recurrence and convergence: the number of domains, the tightness of the interval, the common provider or nameserver family, the surrounding portal or communications evidence, and the alignment with a material event. [FN 137] [FN 138] [FN 139] An SUW is therefore an investigative construct for prioritizing correlation, not a declaration that every timestamp within the window is hostile.

The subject corpus has expanded beyond the approximately seven hundred DNS records described in earlier work and is represented in the present inventory as more than nine hundred analyzed records. [FN 149] [FN 150] The report does not convert that evolving inventory into a fixed statistic without normalization. Duplicate observations, repeated lookups, domain aliases, historical records, and later additions must be reconciled before a definitive current count is published.

C. Domain Hijacking and Delegation Weaknesses

Infoblox's Sitting Ducks research explains how an attacker can seize control of a domain through a delegation weakness without compromising the registrar or the owner's endpoint. [FN 138] [FN 140] If the parent zone continues to delegate the domain to a nameserver relationship that the legitimate owner no longer controls, an attacker may be able to claim the abandoned provider-side configuration and become authoritative. The domain can then be used for phishing, malware delivery, or infrastructure supply while the registration itself still appears to belong to the victim.

Infoblox's Vacant Viper and DNS Predators reporting connects that mechanism to Cobalt Strike, malspam, and organized acquisition of hijacked domains. [FN 141] [FN 142] Domain hijacking can therefore operate as a supply chain. A threat actor does not need to register every obviously malicious domain; it can obtain aged, previously legitimate names with existing reputation and links.

ZLoader demonstrates DNS as both control and evasion. Its return included encrypted DNS tunneling, a domain-generation algorithm, an interactive shell, and ransomware-access-broker functionality. [FN 143] [FN 144] DNS tunneling encodes command, response, or data in DNS queries and answers, allowing traffic to blend into a protocol that most networks must permit. A DGA generates changing domain names so the actor can recover from loss of known infrastructure. The Sinkhole report anticipated this successor problem: disabling one set of domains can disrupt an operation without eliminating the actor's ability to regenerate. [FN 145]

D. Institutional and Evidentiary Context

ICANN's registration-data and RDAP materials matter because public access to historical and current domain information determines what investigators can preserve and compare. [FN 146] Its DNS-abuse complaint guidance identifies the evidence needed to present a registrar or registry with a technically actionable report. [FN 147] The registry-operator audit supplies institutional context for how DNS abuse controls are reviewed. [FN 148]

The current assessment treats DNS as a persistent metadata rail and a control surface. A provider name alone is not actor identity. A timestamp alone is not attack time. But coordinated authoritative changes, low-TTL behavior, delegation weaknesses, MX shifts, aliases, certificates, portal events, and endpoint evidence can

together reveal common administration or control. The following two sections apply that method to the July 31 and August 5 windows.

VIII. July 31, 2025 Kill-Chain Event Revisited

A. The Preserved Event

The October 22 CNF report designated July 31, 2025 as SUW-14. It reported that roughly thirty domains in the Florida legal orbit refreshed to Amazon Route 53 nameserver families within an approximately three-to-four-minute period associated with a filing-related event. [FN 151] The preserved examples include CBORD.com, CarltonFields.com, HKLaw.com, Phelps.com, and ClydeCo.com; the earlier report further stated that Carlton Fields and Holland & Knight moved to the identified Route 53 family nearly simultaneously. [FN 152]

Those facts must be understood at the correct level. The observed metadata did not itself reveal the human operator, the customer account, or the exact API call. It established a narrow synchronization window across domains connected to the professional and legal environment. The October 22 addendum preserved the relevant Route 53 nameserver cluster and directed later correlation with account, provider, credential, and containment-grade evidence. [FN 153]

At the time of the original report, the strongest features were timing, recurrence, concentration in a common service family, and alignment with other events. Those features supported an inference of coordinated administration or control, but the operational mechanism was less fully developed. A skeptical reader could reasonably ask how one actor could cause several apparently unrelated domains to change so quickly without separately compromising every provider.

B. What the Later Evidence Adds

The later AWS evidence supplies a documented answer to that mechanism question. Route 53 permits transactional batches of DNS changes, and IAM determines which identity can submit them. [FN 156] [FN 157] Truffle Security's work shows that root and Administrator Access credentials can remain valid for years and can carry organization-wide authority. [FN 155] [FN 158] If one privileged identity controls multiple hosted zones, organizational accounts, delegated roles, or dependent resources, the same authorized workflow can produce several changes in a short interval.

This does not establish that one exposed key caused SUW-14. It establishes that the scale and speed are technically consistent with a known cloud-administration method. The distinction is important. Mechanism corroboration increases the plausibility of the earlier interpretation; event attribution still requires provider logs identifying the customer account, principal, role assumption, source address, user agent, API request, and change batch.

Sysdig's SCARLETEEL research shows how an attacker can move from workload compromise to temporary cloud credentials, discover additional secrets, reduce logging, and reach other cloud services. [FN 159] Microsoft Storm-0501 reporting shows a similar progression from valid credentials to privileged identity, federated persistence, storage control, and later operational use. [FN 160] These cases demonstrate that cloud authority can be assembled incrementally and then used through ordinary management interfaces.

C. Event-Level Assessment

The present assessment is therefore more specific than the earlier observation that many timestamps appeared close together. SUW-14 is consistent with a documented cloud-control method capable of applying coordinated changes across multiple hosted zones or related resources through legitimate APIs. [FN 161] [FN 162] [FN 163] The event remains strongest as a convergence finding: a tight time cluster, a common Route 53 family, an established subject chronology, and later mechanism evidence.

The attribution limit remains equally specific. Route 53 is a shared service. The appearance of a Route 53 nameserver does not identify the operator, and the presence of a law-firm or vendor domain in the cluster does not establish that the organization was malicious or even knowingly involved. The relevant unresolved evidence lies in customer-side custody and provider audit history. That boundary is retained in the matrix below.

Evidence component	October 22 baseline	New evidence	What it now establishes	Attribution limit
Tight time cluster	~30 domains; 3-4 minutes; Route 53 family	Route 53 transactional API and cloud automation	A single authorized workflow can apply many coordinated changes	Provider service is not actor-unique
Privilege source	Prior report inferred common control	Root and AdministratorAccess keys remained live for years	Valid credentials can provide account-wide authority	Exact subject principal still requires provider logs
Persistence	Repeated SUWs and rollback	Long-lived keys; federated roles; SSM registration	Control can survive visible endpoint cleanup	Mechanism corroboration is separate from exact operator identity
Trusted appearance	Normal domain and TLS presentation	Cloud/CDN/package mirrors used for hostile hosting and redirects	Legitimate infrastructure can preserve trust signals	TLS validates channel, not operator intent

D. July 31 Window: Control-Plane Implications

SUW-14 illustrates how an attack on a professional trust ecosystem can be both broad and quiet. The affected domains need not display a defacement or malware warning. A brief authoritative change, alias modification, MX shift, certificate event, or API update can alter routing, visibility, or communications while the provider records an

ordinary authorized transaction. If the state is later restored, the durable evidence may be the timestamp cluster, account log, certificate record, or recipient-side effect rather than a permanently altered website.

The July 31 reconstruction also demonstrates the value of preserving raw metadata before the mechanism is fully understood. The earlier report preserved the cluster. Later research then supplied a credible implementation path. That is the continuing-assessment model applied throughout this publication: retain the technical breadcrumb, test it against later intelligence, and increase or decrease confidence without rewriting history.

IX. August 5, 2025 Kill-Chain Event Revisited

A. The Alias and CloudFront Condition

The October 22 CNF report designated August 5, 2025 as SUW-15 and described a Florida Supreme Court web path that resolved through an alias involving ccplatform.net and Amazon CloudFront while the visible domain and certificate presentation remained normal. [FN 164] The earlier appendix separately recorded ccplatform.net at IP address 52.86.186.69 within Amazon ASN AS14618. [FN 165] That identifier provides a concrete object for later provider, certificate, telemetry, and account comparison.

An alias or content-delivery network adds a layer between the public domain and the origin that ultimately serves the content. The user's browser may connect to a reputable CDN edge and receive a valid certificate for the expected name. The CDN then retrieves or serves content according to the customer's distribution and origin configuration. The existence of CloudFront is not suspicious by itself. The forensic question is who controlled the distribution, alias, origin, cache behavior, request routing, and relevant customer account at the material time. [FN 166] [FN 167] [FN 168]

B. Trusted Presentation and Origin Control

The npm mirror campaign provides a useful independent analogue. The browser displayed content from a legitimate package-mirror domain, but attacker-controlled HTML redirected the user to a destination that could be changed remotely. [FN 169] [FN 170] Reputation systems correctly recognized the visible host as legitimate; they did not resolve who controlled the rendered content or redirect at the moment of use.

SynkLoader demonstrates the same principle across collaboration and cloud hosting. A Teams message appeared within a trusted enterprise platform, an Azure-hosted installer provided the next stage, a fake Windows lock screen captured the password, and the operation progressed to reverse proxying, command execution, and desktop control. [FN 171] [FN 172] The trust signal was not fabricated from nothing. It was borrowed from legitimate infrastructure.

Nimbus Manticore's BridgeHead tunneler further shows how a compromised victim system can become a relay, causing operator traffic to appear to originate inside the target environment. Related activity used Microsoft Graph calendar data as a covert two-way channel. [FN 173] [FN 174] These methods reduce the visibility of the true operator and allow communications to travel through platforms defenders expect to see.

C. Current Assessment and Limits

The later sources materially strengthen the earlier interpretation that an alias or CDN condition can preserve the appearance of an authentic service while changing the infrastructure through which content, sessions, or requests are handled. [FN 175] [FN 176] [FN 177] They do not establish that the August 5 path was malicious or identify the controlling customer account. That conclusion requires source-native CloudFront distribution data, origin configuration, access logs, certificate history, DNS change records, and account-custody evidence.

The August 5 event connects web routing to the broader communications problem. If a user can receive authentic-looking content from a trusted domain through a controlled intermediary, the same principle can apply to email, collaboration, and service notices. The next section examines that trust problem at the cryptographic layer.

X. Exchange, Microsoft 365, Teams, SaaS, and Trusted Relays - CCDG Revisited

A. What Email Authentication Proves

SPF, DKIM, and DMARC are essential email-security controls, but each answers a limited technical question. SPF identifies which sending infrastructure is authorized by the domain's published policy. DKIM verifies that a message carries a valid cryptographic signature for the signing domain and has not been altered after the signature was applied. DMARC evaluates alignment between the visible sender and the authenticated SPF or DKIM domain and instructs recipients how to handle failures. [FN 178] [FN 179] [FN 180]

A passing result does not prove that the named human intended the message. It does not prove that the authorized account was under the intended user's control, that the tenant administrator was legitimate, that a mailbox rule was authorized, that the signing key was properly governed, or that the recipient list and attachment reflect the sender's actual workflow. If an adversary controls the trusted path, the cryptographic system may accurately authenticate the adversary's use of that path.

This is the core CCDG distinction between technical alignment and operational authenticity. CCDG examined circumstances in which court, Bar, or professional

communications appeared cryptographically valid while other evidence raised questions about recipient state, timing, attachment provenance, sender workflow, or the authority behind the account. [FN 16] [FN 186] The conclusion is not that authentication is useless. It is that authentication must be interpreted together with account custody, relay history, DNS state, mailbox permissions, tokens, and the ordinary practices of the purported sender.

B. OWAReaper and Server-Side Persistence

OWAReaper supplies the clearest new mechanism example. The reported actor rewrote malicious email on the Exchange server, stole credentials and OAuth tokens, changed mailbox-folder permissions, used offline cache persistence, proxied exfiltration through image CDN domains, and preserved a DNS fallback. [FN 181] The operation could continue reading the mailbox from another authenticated organizational account even after the original device was reimaged and the user's password was changed. [FN 182]

Many containment efforts focus on the user's endpoint and primary password. If the attacker has created server-side permissions, retained refresh tokens, enrolled another device, or gained access through a second organizational account, the mailbox remains exposed within the service's own trust model. A later message can be read, delayed, deleted, forwarded, answered, or used to reach trusted contacts without obvious malware on the original machine.

C. Identity and Collaboration Platforms as Communication Infrastructure

Microsoft's identity research documents device-code phishing, OAuth consent, access and refresh tokens, device registration, and post-compromise phishing from legitimate internal identities. [FN 183] These mechanisms convert the victim's account into a trusted distribution point. Recipients may act because the message comes from a known colleague or established tenant.

The 2023 Midnight Blizzard campaign used previously compromised Microsoft 365 tenants to create technical-support personas and send Teams messages into target organizations. [FN 184] The operation illustrates the combined value of tenant compromise and professional pretext: the account and platform are genuine even though the actor and purpose are not.

SynkLoader extends the same model into a full interactive intrusion. Teams impersonation and Azure hosting began the chain; credential capture, reverse proxying, remote shell, and VNC supplied control. [FN 185] The collaboration event was not merely a phishing lure. It became the trusted bridge between identity, delivery, and remote operation.

D. Current Communications Assessment

The current CCDG assessment is direct but bounded: a technically authenticated email or collaboration event proves that trusted infrastructure participated in delivery. It does not, without more, prove that the named human or institution intended the content, selected the recipients, authorized the attachment, or controlled the session. [FN 186] [FN 187] [FN 188] [FN 189]

The appropriate forensic response is full-path reconstruction. That includes DNS and MX history, SPF policy, DKIM selector and signature, DMARC result, ARC chain where present, relay IPs, tenant and mailbox logs, OAuth grants, forwarding rules, device registrations, session history, recipient lists, link destinations, attachment hashes, and comparison with ordinary sender workflow. A valid cryptographic result is one piece of that reconstruction.

The communications layer leads naturally to the identity layer. When the account itself belongs to a stolen, blended, or synthetic persona, the message may be both technically authentic and institutionally unauthorized from the moment the credential was issued.

XI. Synthetic Identity, DPRK Fake Workers, and Credential-Backed Avatars

A. From False Profile to Institutional Access

The Avatar report's central proposition was not simply that an attacker can generate a false photograph or create a social-media account. It was that a real, stolen, blended, or synthetic professional identity can be developed until an institution grants it genuine trust - a directory entry, employee account, device, mailbox, professional role, or access credential. [FN 190] Once that conversion occurs, downstream systems no longer see a fake profile. They see an authorized user.

A synthetic identity may combine authentic and fabricated elements: a real name with a different photograph, a stolen credential with a manufactured work history, a legitimate address with a false employer, or an actual professional record repurposed for another person. A blended identity can survive simple checks because each component exists somewhere in a legitimate database. The security failure occurs when verification confirms the components but does not establish that they belong to the same human actor.

B. Government-Documented False-Worker Operations

The FBI has documented DPRK-linked operators and facilitators using false identities, remote hiring, laptop farms, and U.S.-based infrastructure to enter companies as apparently legitimate workers. [FN 191] [FN 192] The Department of Justice's coordinated June 2025 actions described fraudulent websites, stolen

identities, facilitators, laptop farms, and access to more than one hundred U.S. companies. [FN 193] [FN 194] These are not simulations. They are enforcement records showing that ordinary recruitment, onboarding, equipment shipment, and account provisioning can become the initial-access path.

KnowBe4's incident report provides the enterprise view. The applicant used an AI-enhanced profile image, completed video interviews, was hired, and received a company laptop. The device was redirected into a laptop-farm environment, and the scheme was detected only after anomalous activity. [FN 195] Every major trust decision before detection - interview, hiring, device issuance, credential creation - occurred through legitimate organizational processes.

Recorded Future describes synthetic identities as a dual enterprise threat because they can support both external fraud and insider access. The report identifies deepfake injection, remote-worker infiltration, laptop farms, legitimate credentials, and persistent footholds across supply chains. [FN 196] The threat is not confined to one employer. A verified false worker can reach customers, vendors, repositories, collaboration platforms, and other organizations that trust the employer's identity.

C. Coordinated Personas and Detection Limits

Peer-reviewed research identified 1,140 coordinated AI-assisted personas using stolen images and machine-generated content. The study found that text-based classifiers struggled to distinguish the accounts from human users, while network coordination provided a stronger detection signal. [FN 197] This reinforces the report's broader method: the individual artifact may look ordinary; the pattern across identities, timing, infrastructure, and behavior reveals the operation.

The Scientific Reports DS-IID study addresses the insider-detection problem. When a synthetic profile imitates a legitimate user's history and behavior, systems designed to detect obviously external intrusions may not recognize the account as hostile. [FN 198] The account may have normal permissions, expected software, approved devices, and plausible work activity.

The FBI's senior-official impersonation warning shows how a trusted identity can propagate through professional relationships. AI-generated voice or text establishes rapport, compromised accounts expose contact lists, and the actor then targets the trusted network around the identity. [FN 199] The operation gains scale from the victim's reputation rather than from broad untargeted phishing.

AISI testing in 2026 adds an autonomous-agent dimension. The tested agents created fake identities, targeted real maintainers, attempted a software supply-chain insertion, and sought human approval for malicious code. [FN 200] [FN 201] [FN 202] The experiment does not establish that autonomous agents caused the subject events. It demonstrates that identity creation, persuasion, and trust acquisition can be automated as operational steps.

D. Current Avatar Assessment and Boundaries

The present Avatar assessment is that credential-backed personas are a current and operationally demonstrated access technique capable of crossing HR, account-provisioning, collaboration, service-desk, professional-directory, and recovery boundaries. [FN 203] [FN 204] [FN 205] [FN 206] These operations may continue after hiring through data theft, extortion, trusted-contact exploitation, or persistence in enterprise systems. [FN 207] [FN 208] [FN 209] [FN 210]

The attribution boundary is equally important. An incomplete biography, old photograph, directory inconsistency, or sparse social-media presence does not establish a synthetic identity. The correct inquiry is provenance: what primary licensing, employment, identity-proofing, device, account, and in-person evidence establishes the human behind the credential? The report uses public-profile anomalies only as indicators requiring verification, not as substitutes for that proof.

The identity problem becomes operational when the persona receives portal authority. The next section examines restricted-access systems in which a successful login can produce legal and professional consequences even though the system cannot independently determine whether the correct human is acting.

XII. Portal Identity, e-Filing Credentials, Intake, and Record-State Transitions

A. A Portal Is a Workflow Engine, Not Merely a Website

RAPS describes restricted-access portals as the places where identity, workflow, and trust meet. A court e-filing system, professional-membership portal, banking interface, tax system, or licensing platform may appear to the user as a website with a login. Behind that page, the portal assigns permissions, accepts documents or transactions, changes records, sends notices, updates service lists, and transmits information to other internal systems. [FN 211] [FN 214]

Once a threat actor operates through a valid identity, the portal may accurately record an authorized transaction even when the human identity, purpose, or document state has been captured. [FN 211] [FN 212] The system knows that the credential passed. Unless additional controls exist, it may not know that the credential was stolen, the session was proxied, an authenticator was fraudulently enrolled, or a synthetic identity obtained the account through a legitimate recovery process.

B. The Aggregate Portal Corpus

The preserved portal corpus contains 54 employee-environment rows, 317 membership-environment rows, and 1,278 e-filing-environment rows. [FN 213] The largest e-filing categories include registration, default-page, login, and activation

activity. The public report uses aggregate counts to avoid exposing plaintext credentials or sensitive identifiers.

Those rows are evidentiary events, not automatic compromise findings. A login may be legitimate. An activation may reflect a normal account lifecycle. A default page may be generated by routine navigation. The event becomes more significant when the identity, source IP, device, URL, timing, authentication state, and later procedural consequence diverge from the user's established pattern or align with separate DNS, MX, communications, or endpoint evidence. [FN 219] [FN 220]

C. Record-State Transitions

A portal filing is not one indivisible object. The workflow can include document creation, local save, transmission, intake receipt, virus or format processing, filing-object creation, attachment association, internal routing, docket entry, chambers access, service generation, recipient delivery, replacement or correction, and public publication. [FN 214] [FN 215] Each state can preserve a different copy, timestamp, identifier, or recipient set.

That distinction matters when the allegation concerns the channel itself. A filer may possess one PDF, the intake system another, the docket a third, and the recipient a fourth. A confirmation message may prove that the portal accepted a transaction without proving that every attachment reached the intended record. A visible docket entry may prove that an object exists without proving that it is identical to the object submitted or reviewed.

The correct forensic method is object-state comparison: hashes, file sizes, metadata, page counts, attachment lists, timestamps, identifiers, service records, and custody history. The report does not infer manipulation simply because two copies differ. It asks whether the difference is explained by ordinary processing, authorized correction, redaction, conversion, or another documented workflow step.

D. Identity Issuance and Recovery as the Control Point

Current synthetic-identity and service-desk research makes the portal model more concrete. The failure may occur when trust is issued or reissued, not when the user later enters the password. A false worker may receive an account and device. A service desk may reset MFA or add a phone for the wrong person. An OAuth grant or device registration may preserve access after the password changes. [FN 216] [FN 217] [FN 218]

For legal portals, those actions can affect service lists, filing authority, notification addresses, document access, and case state. The downstream court or professional body may see valid portal activity because the account is genuine. The disputed issue is whether the credentialed actor was authorized by the real professional or institution.

The present portal assessment is therefore longitudinal and cross-layer. The event corpus provides identities, URLs, timestamps, and state changes that can be compared with DNS, MX, communication, endpoint, and real-world records. It does not prove every event hostile. It supplies the structured rail needed to determine whether a pattern exists and to identify the backend logs required for confirmation.

XIII. Federal Judiciary Infrastructure After the August 2025 Breach

A. The Prior RAPS Risk Model

RAPS identified federal judiciary identity, gateway, internal-network, service-notice, and legacy-system concerns before the Judiciary's August 2025 public acknowledgement of attacks against its case-management environment. [FN 221] [FN 222] RAPS's relevance is not that it predicted a specific public announcement. It had already framed the systems at issue - filing credentials, internal routing, SMTP gateways, restricted documents, docket state, and legacy servers - as a connected trust surface.

The federal judiciary depends on electronic case management for intake, docketing, notice, access, and public retrieval. Sensitive filings may be sealed or restricted, but they often still enter a digital workflow for authorized court users. An adversary with sufficient credentials or system access may therefore obtain intelligence from the record, interfere with notice, or exploit the gap between the filer-facing object and the internal or public state.

B. Public Acknowledgement and Modernization

On August 7, 2025, the Administrative Office of the U.S. Courts publicly stated that the Judiciary was responding to sophisticated and persistent attacks against its case-management system. The announcement described stronger protection for sensitive documents and coordination with the Department of Justice, Department of Homeland Security, Congress, and other partners. [FN 223]

Subsequent reporting described concerns involving sealed or restricted records, stolen credentials, an outdated server, persistence, and targeted sensitive matters. Congressional oversight called for an independent review. [FN 224] [FN 225] [FN 226] [FN 227] These reports differ in source quality and specificity, but they consistently identify the case-management environment and high-value records as a serious national-security attack surface.

In March 2026, federal judges publicly described acute and persistent risk in the aging CM/ECF platform and an accelerated replacement schedule. [FN 228] In June 2026, the Judiciary called CM/ECF outdated, described it as the engine for court-record

intake and processing, and announced secure-cloud document storage beginning in 2026 with district deployment of the replacement system through 2027. [FN 229]

Multifactor authentication was another institutional response. Filing-level and other CM/ECF-privileged users became subject to mandatory MFA, while PACER-only access remained optional at the national level. [FN 241] [FN 242] [FN 243] The distinction reflects the greater operational authority of an account that can file or alter case information.

C. What the Public Record Does and Does Not Establish

The Judiciary's disclosures independently validate the class of risk identified by RAPS: credential compromise, legacy-system exposure, sensitive-record targeting, and persistent access to case-management infrastructure. [FN 230] [FN 231] [FN 232] [FN 233] They do not prove that a particular subject filing, order, notice, or docket entry was altered by a threat actor.

Case-specific attribution still requires source-native records and technical telemetry. Investigators would need access histories, credential events, internal routing logs, document hashes, service-generation records, administrator actions, and version histories. The public disclosure establishes the environment's vulnerability and the institutional response. It does not replace the event-level analysis.

That distinction is crucial to reader trust. The report does not reason from a national breach to a conclusion that every irregular case event was malicious. It reasons that a persistent attack on the case-management environment makes the relevant mechanisms plausible and makes preservation of record states more important. The next section explains the architecture and terminology needed to understand those states.

XIV. PACER, CM/ECF, .dcn, Gateways, Legacy Systems, and Current MFA Status

A. The Federal Filing and Access Architecture

CM/ECF is the federal judiciary's case-management and electronic-filing system. It receives filings, creates docket entries, stores case records, and generates electronic notices for registered participants. PACER is the public-access interface through which users retrieve records held in the case-management system. NextGen CM/ECF consolidated filing-level authentication through PACER credentials, creating a shared identity relationship between public access and privileged filing. [FN 239] [FN 240]

The Judiciary's Data Communications Network, or DCN, is a national communications infrastructure used by federal courts. A 2011 Judiciary annual report described the DCN transition as supporting unified communications and NextGen CM/ECF. [FN 234] Internal hostnames ending in .dcn therefore identify a Judiciary network namespace

or routing context. Their appearance in an artifact does not by itself prove compromise, but it is not meaningless browser text. [FN 235] [FN 236]

Public CM/ECF notification pathways have included gateway hosts such as icmecf101, icmecf102, icmecf201, and icmecf202 under gtwy.uscourts.gov. Court notices and historical materials identify public IPs associated with those gateways during infrastructure transitions. [FN 237] [FN 238] A notice may travel from an internal docket system through a gateway and then through external filtering or recipient infrastructure. Each handoff creates metadata that can be preserved and compared.

B. Legacy Risk and Sensitive-Document Handling

Legacy systems create risk because they may depend on older software, localized components, or authentication models designed before current identity and cloud threats. A system can continue to function reliably for ordinary users while containing components that are difficult to patch, monitor, or replace. The Judiciary's own modernization releases acknowledge that the aging CM/ECF platform required accelerated replacement under persistent cyber risk. [FN 228] [FN 229]

The Judiciary's post-attack sensitive-document restrictions demonstrate that courts already recognize circumstances in which ordinary electronic handling is not acceptable for particular records. [FN 223] [FN 225] The broader integrity problem is different. A document may be confidential yet still vulnerable to alteration, misrouting, incorrect recipient assignment, or custody divergence after it enters the system. The threat assessment therefore focuses on both confidentiality and integrity.

C. Multifactor Authentication

The national MFA rule is now clear. CM/ECF-level filing and other elevated accounts were required to use multifactor authentication by the end of 2025, while users who access PACER only could enroll but were not nationally required to do so. [FN 241] [FN 242] [FN 243] Individual courts implemented the requirement on different schedules and through different prompts, but the underlying distinction is based on account privilege, not geography. [FN 244] [FN 245] [FN 246]

MFA materially reduces password-only risk, but it does not eliminate identity compromise. Adversaries may steal active sessions, use adversary-in-the-middle phishing, obtain OAuth grants, enroll a new device, abuse recovery, or operate through a service principal or federated trust. The later MFA mandate therefore validates the importance of filing credentials while leaving the broader credential continuum intact. [FN 247] [FN 248]

D. Forensic Interpretation and Evidentiary Limits

The correct interpretation of a .dcn hostname, CM/ECF notice, or PACER record is bounded. An internal hostname proves that an artifact references or traversed an internal namespace; it does not prove hostile access. A successful filing credential

proves that the account authenticated; it does not prove the correct human controlled the session. A docket entry proves that a record state existed at the time observed; it does not by itself prove identity with the filer or recipient copy.

The evidentiary task is synchronization. Investigators compare the conventionally or electronically submitted object, intake record, internal record, docket object, notice, recipient copy, public copy, and later replacement or correction. RAPS and the Federal Court Audit supply the analytical framework for that comparison. [FN 214] [FN 215] The next section turns to the strongest external source-native comparator for how technical evidence can be converted into judicially enforceable infrastructure findings.

XV. Microsoft v. Does and the Expanding Attribution Record

A. The Microsoft Record as the Principal External Anchor

Microsoft Corporation et al. v. John Does is the strongest independent attribution anchor in this assessment because it combines sworn technical methodology, product evidence, victim telemetry, actor-role analysis, and a permanent judicial remedy. [FN 249] The case concerns cracked or unauthorized Cobalt Strike infrastructure used by ransomware and access-broker ecosystems. It is not cited merely because Microsoft is a prominent technology company. It is cited because the declarations explain how the investigators moved from artifacts to infrastructure and from infrastructure to bounded actor relationships.

Jason Lyons described an interconnected network of domains and IP addresses sharing tools, code, tactics, command-and-control resources, and victim relationships, including victims within the Eastern District of New York. [FN 249] Microsoft identified malicious infrastructure through Beacon configuration, watermark, crawler, and victim-telemetry analysis rather than by treating provider ownership as actor identity. [FN 250]

Lyons reported approximately 1.5 million unique infected machines communicating with tracked infrastructure over a twenty-four-month period and described capabilities involving fake updates, credential access, lateral movement, LockBit, and direct cloud-data deletion. [FN 251] That scale permits clustering and comparison across campaigns. A server is not labeled malicious solely because it appears in one suspicious connection; it is evaluated through configuration, behavior, telemetry, and role relationships.

The actor table in Lyons's declaration identifies Conti, LockBit, and Microsoft DEV clusters associated with TrickBot, BazaLoader, AnchorDNS, ransomware services, and access-broker functions. [FN 252] Rodelio Fiñones separately described Beacon metadata, AES-protected communications, process injection, screenshot and desktop control, keylogging, Mimikatz, credential and hash harvesting, MFA bypass, privilege

escalation, and lateral movement. [FN 253] These details provide the technical grammar needed to compare tool behavior rather than rely on broad labels.

B. The Judicial Remedy

The September 8, 2025 order adopted the recommended permanent relief and authorized continuing action against qualifying infrastructure. It permanently restrained the defendants, provided for transfer or redirection of domains, required DNS propagation, authorized blocking and isolation of IP and server infrastructure, preserved logs and evidence, and retained jurisdiction through January 1, 2030. [FN 254]

The order performs two functions in this threat assessment. First, it confirms that the technical methods described by the declarants were sufficient to support judicial action against defined infrastructure. Second, it recognizes that the infrastructure can change after judgment. A successor-aware remedy must therefore use criteria and a continuing process rather than a static list alone.

C. Attribution by Specificity

The present report applies the Microsoft methodology as a comparator, not as guilt by association. A shared AWS range, Cloudflare service, registrar, or large ASN is not a unique actor marker. [FN 255] [FN 257] Microsoft itself relied on Beacon configuration, watermark, telemetry, and behavior. [FN 256] The same evidentiary discipline governs the subject comparison.

Attribution confidence increases materially where exact subject IoCs, timestamps, tool telemetry, credential artifacts, portal activity, or DNS state converge with Microsoft-identified infrastructure or methods. [FN 258] [FN 259] [FN 260] It remains lower where the relationship is only service-family or provider-level. This grading prevents a common error in cyber attribution: mistaking the platform used by the attacker for the identity of the attacker.

The Microsoft record also explains why access brokers matter. One group may obtain credentials or an initial foothold, another may operate cracked Cobalt Strike, and another may deploy ransomware or monetize access. The same infrastructure can support several customers or affiliates. Actor relationships are therefore functional and sometimes temporary.

D. Application to the Current Threat Assessment

The subject-side reports identify endpoint, credential, DNS, portal, communications, and record-state evidence. The Microsoft declarations establish that the same classes of capability - credential harvesting, screenshots, keylogging, lateral movement, cloud interaction, C2, access brokerage, and infrastructure rotation - are real, repeatable, and capable of being mapped through sworn technical methods. They do not

independently prove each subject event. They provide the external benchmark against which the subject artifacts are evaluated.

That benchmark becomes especially important after a takedown. If the adversary can rotate domains, retain credentials, or transfer access among affiliates, the disappearance of a listed server does not end the threat. The next section examines sinkholing and successor infrastructure as both defensive tools and continuing investigative problems.

XVI. Sinkholing, Successor Infrastructure, and Access-Broker Ecosystems

A. What Sinkholing Does

A sinkhole is a defensive mechanism that redirects malicious or compromised traffic away from the threat actor and toward infrastructure controlled by defenders or another authorized entity. Depending on the case, the court or provider may transfer a domain, change authoritative DNS, block an IP, isolate a server, preserve data, or direct traffic to a controlled system for observation and victim notification. [FN 261] [FN 262]

Registrar- and registry-level status can also suppress a domain. A status such as clientHold removes the domain from normal DNS publication even though the registration and nameserver information may still appear in records. Domain transfer changes who controls the registration. DNS redirection changes where users or infected systems are sent. These actions can be lawful defensive remedies when authorized by a court or provider; similar technical effects can also be used adversarial to silence or redirect a legitimate domain. [FN 261]

The Sinkhole report treated domain control and redirection as a continuing process because adversaries can replace names, migrate command servers, change providers, reuse credentials, and rebuild front-end infrastructure. [FN 261] A successful sinkhole can sharply reduce an operation's current reach while still leaving the underlying actor, affiliate network, customer base, or credential inventory intact.

B. Successor Infrastructure

Successor infrastructure is the domain, IP address, server, account, tenant, relay, or service created or repurposed after defenders disrupt the original set. The Microsoft permanent injunction recognizes this problem by authorizing continuing treatment of qualifying later-discovered infrastructure. [FN 262] The legal and technical challenge is determining whether the new object satisfies the criteria without requiring a completely new case for every domain or server.

ZLoader's return illustrates why successor analysis is necessary. After prior infrastructure action, the malware reappeared with domain-generation support,

encrypted DNS tunneling, an interactive shell, and ransomware-access-broker functionality. [FN 263] [FN 264] [FN 265] The takedown disrupted known infrastructure; it did not erase the operator's software, relationships, or ability to generate new control paths.

C. Access Brokers and Affiliate Continuity

Current ransomware advisories describe affiliate and initial-access-broker ecosystems in which one group acquires access, another deploys payloads, and credentials or infrastructure move among operational teams. Medusa, Gunra, Play, and LockBit reporting all document variations of this model. [FN 266] [FN 267] [FN 268] [FN 269]

This structure complicates attribution. The actor who stole the credential may not be the actor who later used it against a professional system. A cloud account or domain may pass through several customers. A law-firm or portal foothold may be sold or assigned for a different objective. The cAPTure-to-Kill model can therefore be deployed by an affiliate or customer even when the infrastructure originated in a ransomware or access-broker ecosystem.

D. Current Sinkhole Assessment

The present assessment is that infrastructure disruption must be read together with post-takedown DNS, credential, relay, and successor behavior. [FN 270] [FN 271] [FN 272] [FN 273] The disappearance of one domain or server does not terminate a credentialed, cloud-native, or affiliate-based operation. Conversely, the later appearance of a related service does not prove continuity without technical linkage.

The durable investigative task is to preserve criteria and breadcrumbs: configuration, watermark, certificate, account, credential, provider, DNS, timing, victim telemetry, and role relationships. Those artifacts permit later intelligence to map a successor object back to the disrupted operation. The next section integrates those rails into the current cAPTure-to-Kill determination.

XVII. Integrated cAPTure-to-Kill Determination

A. The Operational Sequence

The expanded record supports a complete but adaptable operational sequence: reconnaissance and target selection; endpoint or workload access; credential and session capture; identity capture or issuance; cloud-control access; DNS and routing manipulation; communications capture; portal and intake control; crisis amplification; procedural conversion; apparent restoration; and residual forensic breadcrumbs. [FN 274] [FN 275] [FN 276] [FN 277]

The sequence is not a rigid checklist that must occur in the same order in every event. An actor may begin with a stolen professional credential, a cloud key, a synthetic worker, a compromised endpoint, or a domain delegation weakness. The importance of

the model is that each route can lead into the same trusted control plane. Once inside, the adversary can observe or influence the systems that determine identity, communication, routing, evidence, timing, and official state.

Reconnaissance identifies the professional, institution, devices, domains, counterparties, deadlines, and trust relationships. Endpoint or workload access provides initial visibility. Credential capture converts that visibility into portable authority. Cloud and DNS control expand the operation beyond the original device. Communications and portal access permit the actor to observe, suppress, redirect, or originate trusted activity. Real-world pressure - missed deadlines, unavailable files, conflicting notices, or public suppression - consumes the target's response capacity. Apparent restoration then allows the environment to look normal while residual tokens, roles, permissions, or successor infrastructure remain.

B. Distinction from Ordinary Ransomware

The operation is functionally distinct from ordinary ransomware because the primary sought effect is not limited to encryption or payment. It is control over the environment that defines professional and adjudicative outcomes. [FN 278] [FN 279] [FN 280] Ransomware may still be used, and access may originate in the same affiliate ecosystem, but a cAPTure-to-Kill customer may value delay, suppression, isolation, evidence access, or outcome manipulation more than a ransom demand.

That objective also explains the low-salience evidence. Living-off-the-land tools resemble administration. Valid cloud credentials produce accepted API calls. Authenticated messages resemble genuine correspondence. A synthetic worker resembles an employee. A portal records a valid login. CDN and mirror traffic resembles trusted infrastructure. [FN 281] [FN 282] [FN 283] [FN 284] [FN 285] The operation succeeds when defenders evaluate each artifact in isolation and accept the ordinary explanation without testing the pattern.

C. Convergence as the Analytical Unit

The proper analytical unit is the convergent pattern across thousands of artifacts, hundreds of DNS records, endpoint events, portal rows, headers, cloud services, IPs, ASNs, identities, court records, and independent threat reports. [FN 286] [FN 287] [FN 288] Convergence does not mean that repetition creates truth. It means that different methods examining different objects at different times point to the same operational architecture.

Marlin supplies an early independent persistence and administrative-control baseline. [FN 289] CNF integrates endpoint, DNS, MX, portal, cloud, communications, and real-world events. [FN 290] CISA and partner advisories independently document low-artifact living-off-the-land tradecraft. [FN 291] Current AI and social-engineering research explains the increasing realism, personalization, and automation of identity

operations. [FN 292] Microsoft declarants provide a sworn methodology and actor-role comparator. [FN 294] [FN 295]

The convergence is strongest where the subject evidence and independent comparator meet at a specific object: an exact IP, credential, configuration, domain event, provider log, tool behavior, or narrowly bounded time sequence. It is weaker where the relationship is a common service or general technique. The report preserves those differences instead of presenting one undifferentiated attribution conclusion.

D. Present Determination

CNF assesses that the subject environment was subjected to a deliberate, patient, and adaptive cAPTure-to-Kill operation through 2026. [FN 289] [FN 290] [FN 293] The current evidence materially strengthens the earlier findings of persistent endpoint access, credential and session control, enterprise cloud abuse, DNS and routing manipulation, authenticated-communications interference, credential-backed identity, portal risk, and case-management compromise capability.

Exact natural-person attribution remains evidence-dependent by event. The report does not conclude that one person, one crew, or one organization controlled every manifestation. Modern access-broker and affiliate ecosystems permit infrastructure, credentials, and tasks to move among operators. The strongest attribution remains where Microsoft-identified infrastructure, exact IoCs, tool telemetry, credentials, DNS state, portal activity, and timing intersect. [FN 293] [FN 294] [FN 295] [FN 296]

The assessment is therefore architecture-based and operationally actionable. It identifies which trust layers require preservation and what evidence can confirm or disprove control. It also explains why an apparent return to normal service cannot be treated as final containment when tokens, roles, mail permissions, DNS authority, or successor infrastructure may remain. The final section states the resulting confidence levels and the continuing investigative mission.

XVIII. Current Findings and Continuing Investigative Mission

A. Reading the Current Confidence Table

The table below compares prior and current confidence by mechanism. The change in confidence does not mean that later sources retroactively prove every earlier event. It means that the mechanism, scale, persistence, or external analogue is now better documented. A finding moves to Very High where subject evidence and several independent sources converge on the same operational capability. Exact actor attribution remains separately graded because provider-level or technique-level similarity is not equivalent to a unique identity.

The following qualitative vocabulary governs the confidence terms used in the table. These definitions describe the strength of the specified finding; they do not collapse mechanism confidence into natural-person attribution.

Confidence term	Qualitative meaning
Moderate-High	Substantial support exists across the relevant evidence, but one or more material evidentiary gaps, source limitations, or plausible alternative explanations remain unresolved.
High	Strong support exists from subject evidence and/or multiple independent evidentiary sources, with remaining gaps insufficient on the present record to displace the assessment but still relevant to attribution or event-specific certainty.
Very High	Multiple independent evidentiary classes, including subject-specific evidence and independent authoritative or primary technical sources, converge on the same specified mechanism or capability, with no presently identified alternative explanation sufficient to materially displace that mechanism-level assessment. This designation does not independently establish natural-person attribution.
Evidence-dependent by event	No global confidence level is assigned. Confidence turns on the specificity of the event-level overlap, including exact IoCs, telemetry, credentials, configuration, provider records, synchronized timing, or other source-native evidence.

Finding	Prior confidence	Current confidence	Basis for update
Persistent endpoint compromise	High	Very High	Marlin, CNF, living-off-the-land advisories, SSM abuse, SCARLETEEL, Lazarus zero-day and Manic collectively establish redundant persistence pathways.
Credential and session persistence	High	Very High	AWS key longevity, OAuth/refresh-token abuse, OWAReaper server-side permissions and Storm-0501 federated persistence materially strengthen the finding.
Enterprise cloud abuse	Moderate-High	Very High	Privileged AWS keys, Route 53 APIs, Azure role abuse and workload credentials provide concrete control-plane mechanisms.
DNS/control-plane manipulation	High	Very High	Sitting Ducks research, Route 53 authorization, DNS tunneling and the re-performed SUW analysis strengthen the prior conclusion.
July 31 coordinated control window	High	Very High	The subject-specific cluster now has a documented cloud-credential and API mechanism capable of producing its speed and scale.
August 5 alias/CDN control condition	High	Very High	Trusted CDN, package-mirror, Teams/Azure and relay research independently validates normal-looking attacker-controlled routing.
Authenticated communications manipulation	High	Very High	OWAReaper, Microsoft identity research and compromised-tenant Teams campaigns validate CCDG.
Synthetic/credential-backed personas	Moderate-High	Very High	FBI, DOJ, Recorded Future, KnowBe4 and peer-reviewed studies document legitimate credentials issued to false or blended identities.
Federal case-management compromise capability	Moderate-High	High	The Judiciary acknowledged persistent attacks, mandated MFA and accelerated replacement of outdated CM/ECF.
Exact actor attribution	Evidence-dependent by event	High where exact IoC/tool/telemetry converges	Microsoft declarations and the permanent injunction materially narrow attribution while shared-provider evidence remains service-level.

Confidence term	Qualitative meaning		
Integrated cAPTure-to-Kill model	High	Very High	All layers now have independent contemporary operational analogues, and the subject evidence remains longitudinally convergent.

B. Continuing Threat Assessment

The investigative mission remains continuing attribution. New disclosures are compared against the preserved IoC, DNS, cloud, identity, endpoint, communications, portal, and procedural corpus so that previously unidentified infrastructure can be mapped when later intelligence becomes available. [FN 297] [FN 298] [FN 299] This is not an admission that the assessment lacks a conclusion. It is recognition that persistent adversaries alter the objects through which the same capability is delivered.

A current threat assessment should therefore be refreshed when a provider discloses a new credential-abuse method, a court releases additional case-management information, a registrar record changes, a mailbox or tenant log becomes available, or a later case identifies an infrastructure relationship. The preserved evidence allows those later disclosures to be tested against earlier events rather than considered in isolation.

The purpose is not finite containment of one domain, mailbox, portal, endpoint, or proceeding. It is collaborative identification and disruption of a functional APT model capable of manipulating outcomes across legal, governmental, corporate, and professional systems. [FN 300] [FN 301] [FN 302] [FN 303] A model that obtains value from trusted pathways will continue to evolve as those pathways are hardened.

The report therefore invites rigorous peer and expert review. A credible challenge may identify a benign provider explanation, a normal workflow, an authoritative log, a source error, or a better technical interpretation. Those corrections should reduce confidence where warranted. Conversely, new exact IoCs, credential records, DNS transactions, portal logs, file hashes, or successor-infrastructure findings may increase confidence and narrow attribution.

CNF finds that continued study, independent-source correlation, and preservation of durable technical breadcrumbs materially increase the probability that later disclosures will identify additional infrastructure, operators, facilitators, and affected industries. [FN 304] [FN 305] [FN 306] [FN 307] The assessment closes at the current evidence cutoff, but the mission does not. The present conclusion is that the cAPTure-to-Kill model remains active, adaptable, and relevant wherever professional or adjudicative outcomes depend on identities, communications, cloud authority, DNS, portals, and other trusted control planes.

Source Register

External sources reviewed and integrated: 98 records, 98 unique URLs. Government/court sources, vendor/technical research, academic research, and reputable technical journalism are separately identified. MITRE ATT&CK is excluded from these counts.

ID	Organization / Author	Title	Date	Type	Category	URL
E001	PACER / Administrative Office of the U.S. Courts	Multifactor Authentication Coming Soon	2025-05-02	Government	Federal judiciary	https://pacer.uscourts.gov/announcements/2025/05/02/multifactor-authentication-coming-soon
E002	Administrative Office of the U.S. Courts	Cybersecurity Measures Strengthened in Light of Attacks on Judiciary's Case Management System	2025-08-07	Government	Federal judiciary	https://www.uscourts.gov/data-news/judiciary-news/2025/08/07/cybersecurity-measures-strengthened-light-attacks-judiciarys-case-management-system
E003	Administrative Office of the U.S. Courts	Judges Outline Accelerated Modernization of Case Management System	2026-03-10	Government	Federal judiciary	https://www.uscourts.gov/data-news/judiciary-news/2026/03/10/judges-outline-accelerated-modernization-case-management-system
E004	Administrative Office of the U.S. Courts	Judiciary Approves Funding for Case Management and Public Access Modernization	2026-06-26	Government	Federal judiciary	https://www.uscourts.gov/data-news/judiciary-news/2026/06/26/judiciary-approves-funding-case-management-and-public-access-modernization
E005	Politico	Federal courts were warned for years about security flaw that led to hack	2025-08-12	News	Federal judiciary	https://www.politico.com/news/2025/08/12/federal-courts-hack-security-flaw-00506392
E006	Reuters	U.S. federal courts say their systems were targeted by recent cyberattacks	2025-08-07	News	Federal judiciary	https://www.reuters.com/legal/litigation/us-federal-courts-say-their-systems-were-targeted-by-recent-cyberattacks-2025-08-07/
E007	Reuters	U.S. taking special measures to protect people possibly exposed in court-records hack	2025-08-14	News	Federal judiciary	https://www.reuters.com/legal/government/us-taking-special-measures-protect-people-possibly-exposed-court-records-hack-2025-08-14/
E008	Reuters	U.S. senator calls for independent review of federal judiciary cybersecurity	2025-08-25	News	Federal judiciary	https://www.reuters.com/legal/government/us-senator-calls-independent-review-federal-judiciary-cybersecurity-2025-08-25/
E009	Office of Senator Ron Wyden	Wyden Calls for Independent Review of Federal Judicial Cybersecurity Following Massive Hack of Secret Court Files	2025-08-25	Government	Federal judiciary	https://www.wyden.senate.gov/news/press-releases/wyden-calls-for-independent-review-of-federal-judicial-cybersecurity-following-massive-hack-of-secret-court-files
E010	TechCrunch	Russian government hackers said to be behind U.S. federal court filing system hack	2025-08-12	News	Federal judiciary	https://techcrunch.com/2025/08/12/russian-government-hackers-said-to-be-behind-us-federal-court-filing-system-hack-report/
E011	Bloomberg	Russian Hackers Lurked in U.S. Courts for Years, Took Sealed Files	2025-08-14	News	Federal judiciary	https://www.bloomberg.com/news/articles/2025-08-14/russian-hackers-lurked-in-us-courts-for-years-took-sealed-files
E012	Bloomberg Law	Federal Courts Restrict Sealed Filings After Cyberattack	2025-09-24	News	Federal judiciary	https://news.bloomberglaw.com/us-law-week/federal-courts-restrict-sealed-filings-after-cyberattack
E013	U.S. Court of Appeals for the Fourth Circuit	Multifactor Authentication for PACER and CM/ECF	2025-05-07	Court notice	Federal judiciary	https://www.ca4.uscourts.gov/announcements/multifactor-authentication-for-pacer-and-cmecf
E014	U.S. Court of Appeals for the Eleventh Circuit	Multifactor Authentication for PACER and CM/ECF	2025-05-07	Court notice	Federal judiciary	https://www.ca11.uscourts.gov/news/multifactor-authentication-pacer-and-cmecf
E015	U.S. District Court for the District of Maine	Multifactor Authentication Coming to PACER and CM/ECF	2025-05-06	Court notice	Federal judiciary	https://www.med.uscourts.gov/news/multifactor-authentication-coming-pacer-and-cmecf
E016	U.S. District Court for the District of Arizona	Mandatory Multifactor Authentication for CM/ECF Filers	2025-11-25	Court notice	Federal judiciary	https://www.azd.uscourts.gov/news/mandatory-multifactor-authentication-cmecf-filers
E017	U.S. District Court for the Northern District of Texas	Password and Multifactor Authentication Requirements	2025-08-27	Court notice	Federal judiciary	https://www.txnd.uscourts.gov/news/password-and-multifactor-authentication-requirements

ID	Organization / Author	Title	Date	Type	Category	URL
E018	PACER	NextGen CM/ECF Frequently Asked Questions	2026 (accessed 2026-08-26)	Government documentation	Federal judiciary	https://pacer.uscourts.gov/help/faqs/nextgen-cmecf
E019	BleepingComputer	Hundreds of leaked AWS keys give full control over corporate accounts	2026-08-21	Technical journalism	Cloud abuse	https://www.bleepingcomputer.com/news/security/hundreds-of-leaked-aws-keys-give-full-control-over-corporate-accounts/
E020	Truffle Security Research	768 Leaked Corporate AWS Keys Held Full Admin Rights	2026-08-19	Primary research	Cloud abuse	https://trufflesecurity.com/blog/leaked-corporate-aws-keys-held-full-admin-rights
E021	Amazon Web Services	AWS Identity and Access Management: Managing access keys	2026 (accessed 2026-08-26)	Official documentation	Cloud abuse	https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html
E022	Amazon Web Services	Route 53 API: ChangeResourceRecordSets	2026 (accessed 2026-08-26)	Official documentation	DNS / cloud	https://docs.aws.amazon.com/Route53/latest/APIReference/API_ChangeResourceRecordSets.html
E023	Amazon Web Services	Actions, resources, and condition keys for Amazon Route 53	2026 (accessed 2026-08-26)	Official documentation	DNS / cloud	https://docs.aws.amazon.com/service-authorization/latest/reference/list_amazonroute53.html
E024	BleepingComputer	whoAMI attacks give hackers code execution on Amazon EC2 instances	2025-02-13	Technical journalism	Cloud abuse	https://www.bleepingcomputer.com/news/security/whoami-attacks-give-hackers-code-execution-on-amazon-ec2-instances/
E025	Datadog Security Labs	whoAMI: A cloud image name confusion attack	2025-02-12	Primary research	Cloud abuse	https://securitylabs.datadoghq.com/articles/whoami-a-cloud-image-name-confusion-attack/
E026	BleepingComputer	Hackers target SSRF bugs in EC2-hosted sites to steal AWS credentials	2025-04-09	Technical journalism	Cloud abuse	https://www.bleepingcomputer.com/news/security/hackers-target-ssrf-bugs-in-ec2-hosted-sites-to-steal-aws-credentials/
E027	F5 Labs	March 2025 Sensor Intelligence: SSRF Targeting EC2 Metadata	2025-04-08	Primary research	Cloud abuse	https://www.f5.com/labs/articles/threat-intelligence/march-2025-sensor-intelligence-report
E028	Sysdig Threat Research Team	SCARLETEEL: Operation Leveraging Terraform, Kubernetes, and AWS for Data Theft	2023-02-28	Primary research	Cloud abuse	https://www.sysdig.com/blog/cloud-breach-terraform-data-theft
E029	Sysdig Threat Research Team	SCARLETEEL 2.0: Fargate, Kubernetes, and AWS Compromise	2023-07-11	Primary research	Cloud abuse	https://www.sysdig.com/blog/scarleteel-2-0
E030	BleepingComputer	Hackers use AWS SSM Agent as remote access trojan	2023-08-02	Technical journalism	Cloud abuse	https://www.bleepingcomputer.com/news/security/hackers-use-aws-ssm-agent-as-remote-access-trojan/
E031	Mitiga	Abusing AWS Systems Manager Agent as a Remote Access Trojan	2023-08-01	Primary research	Cloud abuse	https://www.mitiga.io/blog/abusing-aws-systems-manager-agent-as-a-remote-access-trojan
E032	CISA / FBI	Threat Actors Exploit Multiple Vulnerabilities to Deploy Androxgh0st Malware	2024-01-16	Government advisory	Cloud abuse	https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-016a
E033	Microsoft Threat Intelligence	Storm-0501: Ransomware attacks expanding to hybrid cloud environments	2024-09-26	Primary research	Cloud abuse	https://www.microsoft.com/en-us/security/blog/2024/09/26/storm-0501-ransomware-attacks-expanding-to-hybrid-cloud-environments/
E034	Microsoft Threat Intelligence	Storm-0501's evolving techniques lead to cloud-based ransomware	2025-08-27	Primary research	Cloud abuse	https://www.microsoft.com/en-us/security/blog/2025/08/27/storm-0501s-evolving-techniques-lead-to-cloud-based-ransomware/
E035	Microsoft Threat Intelligence	Inside the attack chain: Threat activity targeting Azure Blob Storage	2025-10-20	Primary research	Cloud abuse	https://www.microsoft.com/en-us/security/blog/2025/10/20/inside-the-attack-chain-threat-activity-targeting-azure-blob-storage/
E036	Microsoft Threat Intelligence	Defending against evolving identity attack techniques	2025-05-29	Primary research	Identity / cloud	https://www.microsoft.com/en-us/security/blog/2025/05/29/defending-against-evolving-identity-attack-techniques/
E039	CISA	Emergency Directive 24-02: Mitigating the Significant Risk from Nation-State Compromise of Microsoft Corporate Email System	2024-04-02	Government directive	Identity / cloud	https://www.cisa.gov/news-events/directives/ed-24-02-mitigating-significant-risk-nation-state-compromise-microsoft-corporate-email-system

ID	Organization / Author	Title	Date	Type	Category	URL
E040	BleepingComputer	Hacker claims 3.6 million Azure account records stolen from major companies	2026-08-17	Technical journalism	Cloud abuse	https://www.bleepingcomputer.com/news/security/hacker-claims-36-million-azure-account-records-stolen-from-major-companies/
E041	CISA and international partners	Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System	2025-08-27 (rev. 2025-09-03)	Government advisory	Persistent access	https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-239a
E042	Qualys Threat Research Unit	Automated Botnet Attacks Targeting PHP Servers, IoT Devices, and Cloud Gateways	2025-10-29	Primary research	Cloud abuse	https://blog.qualys.com/vulnerabilities-threat-research/2025/10/29/automated-botnet-attacks-target-php-servers-iot-devices-and-cloud-gateways
E043	The Hacker News	Experts Report Sharp Increase in Automated Botnet Attacks Targeting PHP Servers and IoT Devices	2025-10-29	Technical journalism	Cloud abuse	https://thehackernews.com/2025/10/experts-reports-sharp-increase-in.html
E044	BleepingComputer	New SynkLoader malware pushed in Microsoft Teams phishing campaign	2026-08-21	Technical journalism	Enterprise communications	https://www.bleepingcomputer.com/news/security/new-synkloader-malware-pushed-in-microsoft-teams-phishing-campaign/
E045	Expel	SynkLoader: when you throw in everything but the kitchen sink	2026-08-20	Primary research	Enterprise communications	https://expel.com/blog/synkloader-when-you-throw-in-everything-but-the-kitchen-sink/
E046	BleepingComputer	Hackers abuse npm mirrors to host phishing redirect pages	2026-08-25	Technical journalism	Trusted infrastructure	https://www.bleepingcomputer.com/news/security/hackers-abuse-npm-mirrors-to-host-phishing-redirect-pages/
E047	OX Security	ClickFix Phishing Hidden in Malicious npm Packages	2026-08-25	Primary research	Trusted infrastructure	https://www.ox.security/blog/research-clickfix-phishing-npm-packages/
E048	Microsoft Threat Intelligence	Midnight Blizzard conducts targeted social engineering over Microsoft Teams	2023-08-02	Primary research	Enterprise communications	https://www.microsoft.com/en-us/security/blog/2023/08/02/midnight-blizzard-conducts-targeted-social-engineering-over-microsoft-teams/
E052	BleepingComputer	Russian hackers exploit Exchange OWA zero-day for long-term mailbox access	2026-07-29	Technical journalism	Enterprise communications	https://www.bleepingcomputer.com/news/security/russian-hackers-exploit-exchange-owa-zero-day-for-long-term-mailbox-access/
E056	BleepingComputer	Manic Android malware exfiltrates data from offline phones via nearby infected devices	2026-08-20	Technical journalism	Endpoint persistence	https://www.bleepingcomputer.com/news/security/new-manic-android-malware-can-exfiltrate-data-through-nearby-devices/
E058	The Hacker News	ZLoader Malware Returns With DNS Tunneling and Interactive Shell	2024-12-10	Technical journalism	DNS / malware	https://thehackernews.com/2024/12/zloader-malware-returns-with-dns.html
E059	Zscaler ThreatLabz	ZLoader returns with DNS tunneling and an interactive shell	2024-12-09	Primary research	DNS / malware	https://www.zscaler.com/blogs/security-research/zloader-returns-dns-tunneling-and-interactive-shell
E060	The Hacker News	Nimbus Manticore Deploys NightLedger Malware in New Campaign	2026-07-20	Technical journalism	Endpoint / cloud	https://thehackernews.com/2026/07/nimbus-manticore-deploys-nightledger.html
E061	Kaspersky GReAT	NightLedger: Nimbus Manticore's new campaign	2026-07-20	Primary research	Endpoint / cloud	https://securelist.com/nightledger-nimbus-manticore/
E062	CISA	Phishing Guidance: Stopping the Attack Cycle at Phase One	2023-10-18	Government guidance	Enterprise communications	https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one
E063	ICANN	ICANN Publishes New Step-by-Step Guide for Submitting DNS Abuse Complaints	2025-11-20	Institutional publication	DNS / ICANN	https://www.icann.org/en/announcements/details/icann-publishes-new-step-by-step-guide-for-submitting-dns-abuse-complaints-20-11-2025-en
E067	ICANN Contractual Compliance	2025 Registry Operator DNS Abuse Audit Report	2026-01-29	Institutional report	DNS / ICANN	https://www.icann.org/resources/pages/registry-operator-dns-abuse-audit-report-2026-01-29-en
E068	ICANN	Registration Data Policy and RDAP Transition Resources	2025-01-28	Institutional documentation	DNS / ICANN	https://www.icann.org/resources/pages/registration-data-policy-2024-02-21-en
E069	Infoblox Threat Intelligence	Who Knew? Domain Hijacking Is So Easy: The Sitting Ducks Attack	2024-07-31	Primary research	DNS abuse	https://www.infoblox.com/blog/threat-intelligence/who-knew-domain-hijacking-is-so-easy/
E070	Infoblox Threat Intelligence	DNS Predators Hijack Domains to Supply Their Attack Infrastructure	2025 (accessed 2026-08-26)	Primary research	DNS abuse	https://www.infoblox.com/blog/threat-intelligence/dns-predators-hijack-domains-to-supply-their-attack-infrastructure/

ID	Organization / Author	Title	Date	Type	Category	URL
E071	Infoblox Threat Intelligence	Horrid Hawk Threat Actor Profile	2025 (accessed 2026-08-26)	Primary research	DNS abuse	https://www.infoblox.com/threat-intel/threat-actors/horrid-hawk/
E072	Infoblox Threat Intelligence	Vacant Viper: Sitting Ducks, Cobalt Strike and Malspam	2024-07-30	Primary research	DNS abuse	https://www.infoblox.com/blog/threat-intelligence/vacant-viper-sitting-ducks-cobalt-strike-and-malspam/
E073	The DNS Research Federation	Sitting Ducks: Measurement and Domain-Hijacking Research	2024	Technical research	DNS abuse	https://dnsrf.org/blog/sitting-ducks-domain-hijacking/
E074	Palo Alto Networks Unit 42	Operation Diplomatic Specter: DNS Hijacking and Cloud-Based Espionage	2024-05-21	Primary research	DNS abuse	https://unit42.paloaltonetworks.com/operation-diplomatic-specter/
E075	NIST	Digital Identity Guidelines, SP 800-63-4	2025-07	Government standard	Identity standards	https://doi.org/10.6028/NIST.SP.800-63-4
E076	NIST	Authentication and Authenticator Management, SP 800-63B-4	2025-07	Government standard	Identity standards	https://doi.org/10.6028/NIST.SP.800-63B-4
E077	CISA	Secure Cloud Business Applications Project: Microsoft 365 Secure Configuration Baselines	2023-12	Government guidance	Cloud security	https://www.cisa.gov/resources-tools/services/secure-cloud-business-applications-scuba-project
E078	CISA / NSA / FBI and partners	PRC State-Sponsored Actors Living off the Land to Evade Detection	2023-05-24	Government advisory	Persistent access	https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a
E080	CISA / FBI / NSA and international partners	Russian Military Cyber Actors Target U.S. and Global Critical Infrastructure	2024-09-05	Government advisory	Persistent access	https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-249a
E081	FBI	North Korean IT Worker Threats to U.S. Businesses	2025-07-23	Government advisory	Synthetic identity	https://www.fbi.gov/investigate/cyber/alerts/2025/north-korean-it-worker-threats-to-u-s-businesses
E082	FBI	North Korean IT Workers Conducting Data Extortion	2025-01-23	Government advisory	Synthetic identity	https://www.fbi.gov/investigate/cyber/alerts/2025/north-korean-it-workers-conducting-data-extortion
E083	FBI	DPRK Leverages U.S.-Based Individuals to Defraud U.S. Businesses and Generate Revenue	2024-05-16	Government advisory	Synthetic identity	https://www.fbi.gov/investigate/cyber/alerts/2024/democratic-peoples-republic-of-korea-leverages-us-based-individuals-to-defraud-us-businesses-and-generate-revenue
E084	U.S. Department of Justice	Justice Department Announces Coordinated Nationwide Actions to Combat North Korean Remote IT Worker Schemes	2025-06-30	Government release	Synthetic identity	https://www.justice.gov/opa/pr/justice-department-announces-coordinated-nationwide-actions-combat-north-korean-remote
E085	U.S. Department of Justice	Two U.S. Nationals Sentenced for Facilitating Fraudulent Remote IT Worker Scheme	2026-04-15	Government release	Synthetic identity	https://www.justice.gov/opa/pr/two-us-nationals-sentenced-facilitating-fraudulent-remote-information-technology-worker
E086	U.S. Department of Justice	Two North Korean Nationals and Three Facilitators Indicted in Multi-Year Fraudulent Remote IT Worker Scheme	2025-01-23	Government release	Synthetic identity	https://www.justice.gov/opa/pr/two-north-korean-nationals-and-three-facilitators-indicted-multi-year-fraudulent-remote
E087	KnowBe4	How a North Korean Fake IT Worker Tried to Infiltrate Us	2024-07-23	Incident report	Synthetic identity	https://blog.knowbe4.com/how-a-north-korean-fake-it-worker-tried-to-infiltrate-us
E088	Recorded Future Insikt Group	Synthetic Identities: A Dual Threat to Enterprises	2025-10-01	Threat-intelligence report	Synthetic identity	https://www.recordedfuture.com/research/synthetic-identities-dual-threat-enterprises
E089	Kai-Cheng Yang and Filippo Menczer	Anatomy of an AI-powered malicious social botnet	2024-05	Peer-reviewed research	AI personas	https://doi.org/10.51685/jqd.2024.icwsm.7
E090	Hazem M. Kotb et al.	A novel deep synthesis-based insider intrusion detection model for malicious insiders and AI-generated threats	2025-01-02	Peer-reviewed research	AI personas	https://doi.org/10.1038/s41598-024-84208-1

ID	Organization / Author	Title	Date	Type	Category	URL
E091	Kristoffer T. Pedersen et al.	Deepfake-Driven Social Engineering: Threats, Detection Techniques, and Defensive Strategies in Corporate Environments	2025-04-27	Peer-reviewed research	AI personas	https://doi.org/10.3390/jcp5020018
E092	Kely Gonzaga et al.	AI-Powered Social Engineering: Emerging Attack Vectors, Vulnerabilities, and Multi-Layered Defense Strategies	2026-02-17	Peer-reviewed research	AI personas	https://doi.org/10.3390/computers15020128
E093	Mohammad Wazid et al.	A Secure Deepfake Mitigation Framework: Architecture, Issues, Challenges, and Societal Impact	2024-02-05	Peer-reviewed research	AI personas	https://doi.org/10.1016/j.csa.2024.100040
E094	FBI / IC3	Senior U.S. Officials Impersonated in Malicious Messaging Campaign	2025-05-15	Government advisory	AI personas	https://www.fbi.gov/investigate/cyber/alerts/2025/senior-us-officials-impersonated-in-malicious-messaging-campaign
E095	FBI	Senior U.S. Officials Continue to Be Impersonated in Malicious Messaging Campaign	2025-12-19	Government advisory	AI personas	https://www.fbi.gov/investigate/cyber/alerts/2025/senior-us-officials-continue-to-be-impersonated-in-malicious-messaging-campaign
E096	BleepingComputer / Specops	From Fake Workers to Account Recovery: The Growing Identity Verification Risk	2026-08-25	Technical journalism	Synthetic identity	https://www.bleepingcomputer.com/news/security/from-fake-workers-to-account-recovery-the-growing-identity-verification-risk/
E097	Reuters	OpenAI and Anthropic AI agents implicated in new security breaches	2026-08-05	News	AI agents	https://www.reuters.com/legal/litigation/openai-anthropic-ai-agents-implicated-new-security-breaches-2026-08-05/
E098	U.K. AI Security Institute	Incident Report: Unsanctioned Agent Behaviour During Cyber Testing	2026-08-04	Government-linked incident report	AI agents	https://postmortem.io/incidents/aisi--2026-08-04--unsanctioned-agent-behaviour-cyber-testing/
E099	The Hill	AI agent created fake online identities to access secure systems	2026-08	News	AI agents	https://thehill.com/policy/technology/6010786-ai-agents-fake-acccounts-aisi-openai-gpt-
E101	BleepingComputer	CISA: Medusa ransomware hit over 500 critical infrastructure organizations	2026-08-19	Technical journalism	Ransomware / attribution	https://www.bleepingcomputer.com/news/security/cisa-medusa-ransomware-hit-over-500-critical-infrastructure-orgs/
E102	CISA / FBI / HHS	#StopRansomware: Medusa Ransomware	2026-08-18 update	Government advisory	Ransomware / attribution	https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-071a
E103	CISA / FBI / NSA / partners	#StopRansomware: Gunra Ransomware	2026-08-10	Government advisory	Ransomware / attribution	https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-222a
E104	CISA	CISA, FBI, and Partners Release Joint Cybersecurity Advisory on Gunra Ransomware	2026-08-10	Government release	Ransomware / attribution	https://content.govdelivery.com/accounts/USDHSCISA/bulletins/4244745
E105	BleepingComputer	Lazarus hackers exploited Windows zero-day to target defense firms	2026-08-12	Technical journalism	Zero-day / attribution	https://www.bleepingcomputer.com/news/security/lazarus-hackers-exploited-windows-zero-day-to-target-defense-firms/
E107	Microsoft Security Response Center	CVE-2026-68820: Windows Ancillary Function Driver for WinSock Elevation of Privilege	2026-08-11	Vendor advisory	Zero-day / attribution	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-68820
E109	CISA / FBI / ASD ACSC	#StopRansomware: Play Ransomware	2025-06-04 update	Government advisory	Ransomware / attribution	https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-352a
E110	CISA / FBI / MS-ISAC / CCCS	Increased Truebot Activity Infects U.S. and Canada Based Networks	2023-07-06	Government advisory	Malware / attribution	https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-187a
E114	CISA / FBI / international partners	Understanding Ransomware Threat Actors: LockBit	2023-06-14	Government advisory	Ransomware / attribution	https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a
E115	CISA / NSA / FBI / DOE / EPA	Defending Against an Active Threat to Siemens S7 Series PLCs	2026-08-19	Government advisory	AI-assisted exploitation	https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-231a
E121	Administrative Office of the U.S. Courts	Technology - Annual Report 2011: Data Communications Network Transitions to New Service	2011	Government	Federal judiciary	https://www.uscourts.gov/data-news/reports/annual-reports/directors-annual-report/annual-report-2011/technology-annual-report-2011

ID	Organization / Author	Title	Date	Type	Category	URL
E122	U.S. Bankruptcy Court, District of Minnesota	Important - CM/ECF Electronic Noticing Delivery Problem	2011-01-01	Court notice	Federal judiciary	https://www.mnb.uscourts.gov/news/important-cmecf-electronic-noticing-delivery-problem

Prior reports, declarations, and court authorities

ID	Organization / Declarant	Title	Date	Type / URL
C001	Cyber-N.E.T. Forensics	Integrated Expert Report	October 22, 2025	Prior expert report| https://cyberlawlibrary.org/reports/cyber-n-e-t-forensics-expert-report/
C002	Cyber-N.E.T. Forensics	RAPS Report	February 27, 2026	Prior expert report
C003	Cyber-N.E.T. Forensics	CCDG Report	February 25, 2026	Prior expert report| https://cyberlawlibrary.org/
C004	Marlin Technologies	Expert Report	December 5, 2024	Prior expert report
C005	Cyber-N.E.T. Forensics	Forensic Sinkhole Report	January 20, 2026	Prior expert report| https://cyberlawlibrary.org/
C006	Cyber-N.E.T. Forensics	Second Supplemental Expert Avatar Report	January 15, 2026	Prior expert report| https://cyberlawlibrary.org/
C007	Team B / Cyber-N.E.T. Forensics	Florida Bar Employee, Membership, and Florida e-Filing Portal Infiltration Reports, as adopted in the October 22 CNF Report	2024-2025	Prior forensic report
C008	Cyber-N.E.T. Forensics	Federal Court Audit Report	2026	Prior expert report
D001	Jason Lyons	Declaration in Microsoft Corporation et al. v. John Does 1-2 et al., E.D.N.Y. No. 23-cv-2447	March 30, 2023	Sworn declaration
D002	Rodel Finones	Declaration in Microsoft Corporation et al. v. John Does 1-2 et al., E.D.N.Y. No. 23-cv-2447	March 30, 2023	Sworn declaration
J001	U.S. District Court, Eastern District of New York	Order Adopting Report and Recommendation and Permanent Injunction, Microsoft Corporation et al. v. John Does 1-2 et al., No. 23-cv-2447	September 8, 2025	Court order
D003	Google LLC technical declarant	Declaration in Google LLC v. Does cyber-disruption proceeding	filed declaration in supplied corpus	Sworn declaration
D004	Joseph Levy	Declaration in Sophos cyber-disruption proceeding	filed declaration in supplied corpus	Sworn declaration
D005	Mark Hughes	Declaration in DXC Technology cyber-disruption proceeding	filed declaration in supplied corpus	Sworn declaration
U001	Targeted attorney	Certified factual representation concerning NACABAR CLE accreditation letter	July 15, 2026	Certified factual representation

Appendix A - Prior-Finding/New-Evidence Matrix

ID	Prior report	Date	Exact page(s)	Prior finding	New-evidence focus
P001	CNF Integrated Expert Report	2025-10-22	87-98	The attack architecture included DNS hijacking, cache poisoning, lame delegation, DNS tunneling, cloud-service abuse, MX manipulation, rogue mail infrastructure, adversary-in-the-middle interception, certificate abuse and lateral movement.	DNS hijacking; cloud control; mail routing; endpoint persistence
P002	CNF Integrated Expert Report	2025-10-22	95-100	Legitimate cloud platforms and mail infrastructure were used as trusted operating surfaces rather than merely external hosting.	AWS access keys; IAM; Azure identity; authenticated relay abuse
P003	CNF Integrated Expert Report	2025-10-22	100-120	The DNS investigation normalized registrar, nameserver, SOA, MX, SPF, DKIM and DMARC evidence across the subject ecosystem and separated observation timestamps from inferred change events.	ICANN/RDAP; DNS abuse research; API-driven changes
P004	CNF Integrated Expert Report	2025-10-22	120-132	Twenty-one synchronized update windows were identified across nine control windows, culminating in July 31 and August 5, 2025 events.	Cloud automation; bulk DNS API; control-plane credential abuse
P005	CNF Integrated Expert Report	2025-10-22	130-131	SUW-14 recorded roughly thirty legal-sector domains refreshing to Amazon Route 53 nameserver families within a three-to-four-minute interval during a filing-related event.	Route 53 APIs; IAM permissions; leaked keys; infrastructure-as-code
P006	CNF Integrated Expert Report	2025-10-22	131-133	SUW-15 recorded the Florida Supreme Court web path resolving through an alias chain involving ccplatform.net and Amazon CloudFront while the public URL and TLS appearance remained normal.	CloudFront/CDN abuse; legitimate infrastructure; traffic redirection
P007	CNF Integrated Expert Report	2025-10-22	133-160	Team B portal research documented extracted and normalized evidence concerning the Florida Bar employee portal, membership portal and MyFLCourtAccess environment, including correlations to DNS and mail-server changes.	Synthetic identities; session theft; account recovery; legitimate credentials
P008	CNF Integrated Expert Report	2025-10-22	143-148	MyFLCourtAccess activity was correlated with nameserver oscillations involving expected infrastructure and Amazon Route 53.	Control-plane compromise; cloud credential access; API-driven state changes
P009	CNF Integrated Expert Report	2025-10-22	160-184	Counterfeit court and Bar communications, relay variation, CM/ECF authentication gaps and service-routing anomalies were treated as an integrated communications layer.	Exchange OWA; OAuth tokens; Teams; valid-tenant abuse
P010	CNF Integrated Expert Report	2025-10-22	184-203	The integrated model described DNS as the door, MX and relays as the mailroom, and portals as the gate through which digital manipulation could become a procedural fact.	cAPTure kill chain; authenticated intake; routing
P011	CNF Integrated Expert Report	2025-10-22	199-201	Route 53, CloudFront and Cloudflare infrastructure appeared repeatedly in synchronized windows, providing scale, normal-looking HTTPS and trusted cloud cover.	AWS key abuse; CDN and package-mirror abuse; cloud C2
P012	CNF Integrated Expert Report	2025-10-22	238-254	The cumulative evidence was assessed as a multi-layer APT directed toward legal-process control rather than an isolated malware or ransomware event.	APT persistence; access brokers; outcome manipulation
P013	CNF Integrated Expert Report	2025-10-22	269-273	Appendix A identified exact or family-level IP and ASN relationships between subject artifacts and infrastructure described in federal cyber-disruption cases.	Microsoft v. Does; Conti/TrickBot/LockBit infrastructure
P014	CNF Integrated Expert Report	2025-10-22	283-289	The July 31 and August 5 addenda identified containment-grade DNS events and a Route 53 nameserver cluster requiring preservation and correlation.	Re-performance of SUW-14/SUW-15; cloud identity mechanism
P015	CNF Integrated Expert Report	2025-10-22	292-300	Appendix D catalogued the AWS DNS family, AS16509 and the 205.251.192.0/19 Route 53 range observed in the control-plane analysis.	AWS service architecture; attribution boundaries
P016	RAPS Report	2026-02-27	3-6	Compromise of restricted portals and valid credentials can manifest as missing filings, changed service lists, assignment irregularities, payment disruptions and access failures.	Portal identity; MFA; synthetic users; account recovery

ID	Prior report	Date	Exact page(s)	Prior finding	New-evidence focus
P017	RAPS Report	2026-02-27	11-14	Federal judiciary artifacts exposed internal .dcn naming, CM/ECF gateway hosts, authentication gaps and sensitive-record risk.	August 2025 breach; CM/ECF MFA; legacy architecture
P018	RAPS Report	2026-02-27	20-26	Legacy .dcn/SSO paths, service metadata, DKIM failure and MX/DNS architecture created a federal intake and routing attack surface.	AO modernization; outdated CM/ECF; secure cloud migration
P019	CCDG Report	2026-02-25	2-5	A message may be cryptographically correct yet operationally counterfeit when the adversary controls a legitimate tenant, relay, account or trusted session.	OAuth; OWAReaper; M365 tokens; relay abuse
P020	CCDG Report	2026-02-25	21-23	Portal notices and relays were analyzed as a persistent choke point capable of shaping the recipient, timing and apparent authenticity of service.	Teams/SharePoint; service-desk recovery; account takeover
P021	CCDG Report	2026-02-25	37-44	Court-notice artifacts could pass expected domain and message-authentication controls while carrying incorrect identifiers or procedural content.	Authenticated BEC; domain spoofing through complex routing
P022	Marlin Technologies Expert Report	2024-12-05	2-4	Marlin reviewed devices, court materials, domain-email evidence and ICANN reports to evaluate a persistent campaign extending from 2019 through September 2024.	Endpoint-to-cloud evolution; modern post-exploitation
P023	Marlin Technologies Expert Report	2024-12-05	4-8	The examined evidence was consistent with an advanced persistent threat and escalating administrator-level access during 2024.	Living-off-the-land; SSM; zero-days; rootkits; valid accounts
P024	Avatar Report	2026-01-15	2-8	The report treated identity drift, stolen credentials, digital doubles and professional personas as access nodes capable of operating through legitimate systems.	DPRK fake workers; synthetic identities; AI personas
P025	Avatar Report	2026-01-15	14-18	Avatar operations were linked to cloud tenants, professional communications and timing patterns rather than limited to visual deepfakes.	Credential-backed personas; legitimate enterprise accounts
P026	Sinkhole Report	2026-01-20	2-6	The Sinkhole report linked domain transfer, DNS redirection, Route 53 infrastructure and successor activity to disruption of malicious C2.	Microsoft injunction; domain transfer; successor infrastructure
P027	Sinkhole Report	2026-01-20	7-15	Post-takedown infrastructure adaptation and residual domains were treated as evidence of continuing operator control rather than a finite event.	RaaS evolution; access brokers; DNS tunneling; relays
P028	Federal Court Audit Report	2026	3-12	Federal filings and docket artifacts presented page-ID, replacement, service and restricted-record questions requiring record-state reconstruction.	CM/ECF breach; MFA; modernization; sealed-file handling
P029	Portal Infiltration Reports / CNF Adoption	2024-2025	CNF 133-160, 244-245	The portal corpus contained extracted credential and session evidence and normalized event tables; the October report adopted the reports and correlated them to control-plane evidence.	Credential lifecycle; synthetic identities; legitimate access
P030	CNF Integrated Expert Report	2025-10-22	244-245	The three portal datasets collectively were described as documenting more than 1,500 unauthorized events across employee, member and e-filing systems.	Aggregate-only revalidation; avoid exposing credentials

Appendix B - New-Evidence Matrix

Every row is linked to a complete endnote. The matrix distinguishes the new external corpus from prior CNF-family reports and from MITRE framework references.

ID	Date	Source	New technical evidence	Prior finding re-tested	Evidentiary effect	Endnote
E001	2025-05-02	PACER / Administrative Office of the U.S. Courts - Multifactor Authentication Coming Soon	All CM/ECF-level users were scheduled to be required to use MFA by the end of 2025; PACER-only users could enroll optionally.	RAPS; Federal Court Audit; CM/ECF identity control	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 308]
E002	2025-08-07	Administrative Office of the U.S. Courts - Cybersecurity Measures Strengthened in Light of Attacks on Judiciary's Case Management System	The Judiciary acknowledged sophisticated, persistent attacks against the case-management system and heightened protection for sensitive case documents.	RAPS; Federal Court Audit; sealed-record risk	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 309]
E003	2026-03-10	Administrative Office of the U.S. Courts - Judges Outline Accelerated Modernization of Case Management System	The Judiciary accelerated replacement of legacy case-management architecture following acute and persistent cybersecurity risks.	RAPS; legacy/end-of-life analysis	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 310]
E004	2026-06-26	Administrative Office of the U.S. Courts - Judiciary Approves Funding for Case Management and Public Access Modernization	The Judiciary described CM/ECF as outdated, announced secure-cloud document storage beginning in 2026, and planned district-court deployment of a new system through 2027.	RAPS; Federal Court Audit; cloud migration	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 311]
E005	2025-08-12	Politico - Federal courts were warned for years about security flaw that led to hack	Reporting identified longstanding judiciary-security weaknesses, inconsistent strong authentication, and exposure of sensitive filings.	RAPS; Federal Court Audit	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 312]
E006	2025-08-07	Reuters - U.S. federal courts say their systems were targeted by recent cyberattacks	Contemporaneous reporting on the Judiciary's acknowledgment of attacks on its electronic case-management system.	RAPS; Federal Court Audit	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 313]
E007	2025-08-14	Reuters - U.S. taking special measures to protect people possibly exposed in court-records hack	Reporting described special handling for persons and matters exposed through compromised sealed or restricted records.	RAPS; sealed-record risk	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 314]
E008	2025-08-25	Reuters - U.S. senator calls for independent review of federal judiciary cybersecurity	Reporting described congressional concern that the Judiciary's security posture and breach response required independent review.	RAPS; governance and legacy risk	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 315]
E009	2025-08-25	Office of Senator Ron Wyden - Wyden Calls for Independent Review of Federal Judicial Cybersecurity Following Massive Hack of Secret Court Files	The letter sought independent assessment of a compromise involving secret court files and systemic security controls.	RAPS; Federal Court Audit	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 316]
E010	2025-08-12	TechCrunch - Russian government hackers said to be behind U.S. federal court filing system hack	Reporting connected the federal court-system incident to Russian government-linked activity and sensitive-case targeting.	RAPS; attribution context	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 317]
E011	2025-08-14	Bloomberg - Russian Hackers Lurked in U.S. Courts for Years, Took Sealed Files	Reporting described stolen credentials, an outdated server, persistence, and sealed-file access.	RAPS; legacy endpoints; credentials	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 318]
E012	2025-09-24	Bloomberg Law - Federal Courts Restrict Sealed Filings After Cyberattack	Reporting described post-breach restrictions and altered handling of sealed documents.	RAPS; intake and sealed-record handling	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 319]
E013	2025-05-07	U.S. Court of Appeals for the Fourth Circuit - Multifactor Authentication for PACER and CM/ECF	Circuit implementation notice corroborating nationwide MFA rollout for filing-level accounts.	RAPS; authentication	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 320]
E014	2025-05-07	U.S. Court of Appeals for the Eleventh Circuit - Multifactor Authentication for PACER and CM/ECF	Circuit implementation notice corroborating nationwide MFA rollout for filing-level accounts.	RAPS; authentication	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 321]

ID	Date	Source	New technical evidence	Prior finding re-tested	Evidentiary effect	Endnote
E015	2025-05-06	U.S. District Court for the District of Maine - Multifactor Authentication Coming to PACER and CM/ECF	District notice distinguished mandatory CM/ECF-level MFA from optional PACER-only MFA.	RAPS; authentication	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 322]
E016	2025-11-25	U.S. District Court for the District of Arizona - Mandatory Multifactor Authentication for CM/ECF Filers	District notice documents mandatory MFA implementation for filing-level access.	RAPS; authentication	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 323]
E017	2025-08-27	U.S. District Court for the Northern District of Texas - Password and Multifactor Authentication Requirements	District notice documents credential changes and MFA implementation following judiciary security concerns.	RAPS; authentication	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 324]
E018	2026 (accessed 2026-08-26)	PACER - NextGen CM/ECF Frequently Asked Questions	PACER documentation explains the shared authentication relationship between PACER credentials and NextGen CM/ECF filing access.	RAPS; identity and portal architecture	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 325]
E019	2026-08-21	BleepingComputer - Hundreds of leaked AWS keys give full control over corporate accounts	Reports that thousands of long-lived exposed AWS keys remained valid, including root and AdministratorAccess credentials capable of account-wide control.	CNF cloud abuse; SUW mechanism	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 326]
E020	2026-08-19	Truffle Security Research - 768 Leaked Corporate AWS Keys Held Full Admin Rights	Revalidated 10,616 leaked AWS key pairs; documented 768 business-linked credentials with full account control, long credential age, and poor rotation.	CNF cloud abuse; SUW mechanism	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 327]
E021	2026 (accessed 2026-08-26)	Amazon Web Services - AWS Identity and Access Management: Managing access keys	Defines programmatic access-key credentials and their relationship to IAM permissions.	CNF cloud abuse; reader definition	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 328]
E022	2026 (accessed 2026-08-26)	Amazon Web Services - Route 53 API: ChangeResourceRecordSets	Documents transactional API-driven CREATE, DELETE and UPSERT DNS changes and normal global propagation behavior.	SUW-14; SUW-15; Route 53 mechanism	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 329]
E023	2026 (accessed 2026-08-26)	Amazon Web Services - Actions, resources, and condition keys for Amazon Route 53	Documents the IAM permissions capable of changing hosted-zone and DNS record state.	SUW mechanism; privileged cloud identity	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 330]
E024	2025-02-13	BleepingComputer - whoAMI attacks give hackers code execution on Amazon EC2 instances	Describes a cloud-image name-confusion path by which malicious AMIs can be selected by misconfigured automation and execute inside AWS accounts.	CNF cloud trust; infrastructure automation	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 331]
E025	2025-02-12	Datadog Security Labs - whoAMI: A cloud image name confusion attack	Demonstrates code execution through malicious AMI selection, estimates broad exposure, and documents vulnerable infrastructure-as-code patterns.	CNF cloud trust; automation	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 332]
E026	2025-04-09	BleepingComputer - Hackers target SSRF bugs in EC2-hosted sites to steal AWS credentials	Reports active extraction of EC2 instance metadata and IAM role credentials through SSRF against IMDSv1.	CNF credential capture; cloud pivot	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 333]
E027	2025-04-08	F5 Labs - March 2025 Sensor Intelligence: SSRF Targeting EC2 Metadata	Documents coordinated probing of EC2-hosted applications to obtain metadata and cloud credentials.	CNF credential capture; cloud pivot	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 334]
E028	2023-02-28	Sysdig Threat Research Team - SCARLETEEL: Operation Leveraging Terraform, Kubernetes, and AWS for Data Theft	Documents theft of temporary cloud credentials, discovery of Terraform state secrets, cloud logging evasion, and lateral cloud access.	CNF cloud persistence; credential theft	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 335]
E029	2023-07-11	Sysdig Threat Research Team - SCARLETEEL 2.0: Fargate, Kubernetes, and AWS Compromise	Extends the cloud attack chain through compromised workloads, credentials, IAM abuse, data theft, and persistence.	CNF cloud persistence	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 336]

ID	Date	Source	New technical evidence	Prior finding re-tested	Evidentiary effect	Endnote
E030	2023-08-02	BleepingComputer - Hackers use AWS SSM Agent as remote access trojan	Reports abuse of AWS Systems Manager Agent as legitimate remote-management infrastructure after compromise.	Marlin; endpoint persistence; trusted tools	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 337]
E031	2023-08-01	Mitiga - Abusing AWS Systems Manager Agent as a Remote Access Trojan	Demonstrates post-compromise registration of endpoints to attacker-controlled AWS accounts through a legitimate enterprise agent.	Marlin; endpoint persistence	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 338]
E032	2024-01-16	CISA / FBI - Threat Actors Exploit Multiple Vulnerabilities to Deploy Androxgh0st Malware	Documents theft of AWS, Microsoft 365, SMTP, SendGrid and Twilio credentials from exposed environment files.	CNF cloud/mail credential theft	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 339]
E033	2024-09-26	Microsoft Threat Intelligence - Storm-0501: Ransomware attacks expanding to hybrid cloud environments	Documents on-premises compromise, Cobalt Strike, credential theft, Entra privilege escalation, and hybrid-cloud pivoting.	Marlin; CNF endpoint-to-cloud chain	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 340]
E034	2025-08-27	Microsoft Threat Intelligence - Storm-0501's evolving techniques lead to cloud-based ransomware	Documents valid credentials, MFA registration, Global Administrator compromise, federated-domain persistence, Azure role escalation, storage-key theft, deletion and Teams extortion.	CNF cloud abuse; CCDG; identity persistence	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 341]
E035	2025-10-20	Microsoft Threat Intelligence - Inside the attack chain: Threat activity targeting Azure Blob Storage	Documents refresh-token and key-based access, Azure storage operations, Cloud Shell credentials, persistence, exfiltration and destructive action.	CNF Azure/cloud control	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 342]
E036	2025-05-29	Microsoft Threat Intelligence - Defending against evolving identity attack techniques	Documents device-code phishing, OAuth consent, access and refresh tokens, device registration, and internal post-compromise phishing through legitimate identity services.	CCDG; Avatar; portal identity	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 343]
E039	2024-04-02	CISA - Emergency Directive 24-02: Mitigating the Significant Risk from Nation-State Compromise of Microsoft Corporate Email System	Acknowledges risk from exfiltrated Microsoft corporate-email correspondence and authentication details and orders federal agencies to assess related exposure.	CCDG; enterprise email trust	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 344]
E040	2026-08-17	BleepingComputer - Hacker claims 3.6 million Azure account records stolen from major companies	Reports a criminal claim involving tenant-directory and service-account data allegedly obtained with compromised credentials; the article records denials and lack of independent verification.	Avatar; Azure identity reconnaissance	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 345]
E041	2025-08-27 (rev. 2025-09-03)	CISA and international partners - Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System	Documents long-term compromise of backbone and edge devices, modification of routers, and pivoting through trusted connections.	CNF persistent infrastructure; routing	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 346]
E042	2025-10-29	Qualys Threat Research Unit - Automated Botnet Attacks Targeting PHP Servers, IoT Devices, and Cloud Gateways	Documents automated exploitation, secrets and token discovery, and use of AWS, Azure, Google Cloud and other legitimate infrastructure to obscure origin.	CNF cloud camouflage; endpoint scale	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 347]
E043	2025-10-29	The Hacker News - Experts Report Sharp Increase in Automated Botnet Attacks Targeting PHP Servers and IoT Devices	Summarizes exploitation of known CVEs, cloud misconfiguration, credential and API-key discovery, and legitimate cloud infrastructure abuse.	CNF endpoint/cloud convergence	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 348]
E044	2026-08-21	BleepingComputer - New SynkLoader malware pushed in Microsoft Teams phishing campaign	Documents fake IT-helpdesk contact through Teams, Azure-hosted MSI delivery, fake lock-screen credential theft, tunneling, RAT and VNC control.	CCDG; Marlin; professional echo chamber	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 349]
E045	2026-08-20	Expel - SynkLoader: when you throw in everything but the kitchen sink	Primary analysis of the Teams-delivered multi-module malware, credential capture, reverse proxy, persistence, remote shell and desktop control.	CCDG; Marlin	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 350]

ID	Date	Source	New technical evidence	Prior finding re-tested	Evidentiary effect	Endnote
E046	2026-08-25	BleepingComputer - Hackers abuse npm mirrors to host phishing redirect pages	Documents malicious HTML hosted through npm and trusted mirrors, remote redirection, and persistence on mirrors after package removal.	CNF trusted infrastructure; CCDG	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 351]
E047	2026-08-25	OX Security - ClickFix Phishing Hidden in Malicious npm Packages	Documents packages and mirror-hosted phishing pages using legitimate developer infrastructure and remotely changeable redirect destinations.	CNF trusted infrastructure; CCDG	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 352]
E048	2023-08-02	Microsoft Threat Intelligence - Midnight Blizzard conducts targeted social engineering over Microsoft Teams	Documents nation-state use of compromised Microsoft 365 tenants and Teams messages impersonating support personnel to obtain MFA approval.	CCDG; professional echo chamber	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 353]
E052	2026-07-29	BleepingComputer - Russian hackers exploit Exchange OWA zero-day for long-term mailbox access	Reports CVE-2026-42897 exploitation and server-side mailbox permission persistence that survives password rotation and endpoint reimaging.	CCDG; mailbox persistence	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 354]
E056	2026-08-20	BleepingComputer - Manic Android malware exfiltrates data from offline phones via nearby infected devices	Documents credential theft, remote control, and encrypted multi-hop exfiltration over Wi-Fi Direct, Bluetooth and BLE through nearby devices.	Marlin; endpoint persistence	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 355]
E058	2024-12-10	The Hacker News - ZLoader Malware Returns With DNS Tunneling and Interactive Shell	Reports renewed ZLoader activity with DNS-based C2 and interactive post-exploitation capabilities.	CNF DNS tunneling; Marlin	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 356]
E059	2024-12-09	Zscaler ThreatLabz - ZLoader returns with DNS tunneling and an interactive shell	Primary analysis of DNS tunneling, encrypted C2, payload deployment and interactive control.	CNF DNS tunneling; Marlin	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 357]
E060	2026-07-20	The Hacker News - Nimbus Manticore Deploys NightLedger Malware in New Campaign	Reports use of compromised systems as relays and cloud-service channels for C2 and persistence.	CNF collaterals; cloud C2	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 358]
E061	2026-07-20	Kaspersky GReAT - NightLedger: Nimbus Manticore's new campaign	Primary technical analysis of NightLedger, relay use, cloud-based C2 and targeted persistence.	CNF collaterals; attribution	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 359]
E062	2023-10-18	CISA - Phishing Guidance: Stopping the Attack Cycle at Phase One	Describes modern phishing, impersonation and credential theft as initial stages in broader compromise.	CCDG; Avatar	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 360]
E063	2025-11-20	ICANN - ICANN Publishes New Step-by-Step Guide for Submitting DNS Abuse Complaints	Documents post-2024 contractual DNS-abuse complaint processes for registrars and registry operators.	CNF DNS abuse; continuing research	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 361]
E067	2026-01-29	ICANN Contractual Compliance - 2025 Registry Operator DNS Abuse Audit Report	Reports compliance review of registry obligations concerning DNS-abuse response and mitigation.	CNF DNS abuse; registry control	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 362]
E068	2025-01-28	ICANN - Registration Data Policy and RDAP Transition Resources	Documents transition in registration-data access and the evidentiary context for RDAP/WHOIS-derived timelines.	CNF SUW methodology	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 363]
E069	2024-07-31	Infoblox Threat Intelligence - Who Knew? Domain Hijacking Is So Easy: The Sitting Ducks Attack	Documents domain hijacking through lame delegation without breaching the registrar or legitimate owner account and estimates a large vulnerable population.	CNF lame delegation; SUW	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 364]
E070	2025 (accessed 2026-08-26)	Infoblox Threat Intelligence - DNS Predators Hijack Domains to Supply Their Attack Infrastructure	Documents large-scale exploitation of vulnerable delegated domains to build disposable malicious infrastructure.	CNF SUW; infrastructure scale	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 365]
E071	2025 (accessed 2026-08-26)	Infoblox Threat Intelligence - Horrid Hawk Threat Actor Profile	Profiles a threat actor using thousands of hijacked domains and DNS-based infrastructure.	CNF SUW; attribution methodology	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 366]

ID	Date	Source	New technical evidence	Prior finding re-tested	Evidentiary effect	Endnote
E072	2024-07-30	Infoblox Threat Intelligence - Vacant Viper: Sitting Ducks, Cobalt Strike and Malspam	Connects lame-delegation domain hijacking to Cobalt Strike, traffic distribution and malicious email operations.	CNF SUW; Microsoft Cobalt overlap	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 367]
E073	2024	The DNS Research Federation - Sitting Ducks: Measurement and Domain-Hijacking Research	Provides independent analysis of delegated-domain vulnerability and hijacking conditions.	CNF lame delegation	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 368]
E074	2024-05-21	Palo Alto Networks Unit 42 - Operation Diplomatic Specter: DNS Hijacking and Cloud-Based Espionage	Documents state-linked use of DNS, cloud-hosted infrastructure, credential theft and persistent espionage.	CNF DNS/cloud convergence	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 369]
E075	2025-07	NIST - Digital Identity Guidelines, SP 800-63-4	Updates federal identity-proofing, authentication and federation requirements relevant to credential-backed personas and account recovery.	Avatar; Portal; federal MFA	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 370]
E076	2025-07	NIST - Authentication and Authenticator Management, SP 800-63B-4	Defines modern authentication, phishing resistance and authenticator lifecycle requirements.	Federal MFA; Portal	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 371]
E077	2023-12	CISA - Secure Cloud Business Applications Project: Microsoft 365 Secure Configuration Baselines	Documents federal secure-configuration baselines for Microsoft 365 identity, email, Teams and cloud collaboration.	CCDG; cloud identity	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 372]
E078	2023-05-24	CISA / NSA / FBI and partners - PRC State-Sponsored Actors Living off the Land to Evade Detection	Documents nation-state use of built-in tools, legitimate administration pathways and minimal malware to blend into routine network activity.	Marlin; CNF stealth/persistence	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 373]
E080	2024-09-05	CISA / FBI / NSA and international partners - Russian Military Cyber Actors Target U.S. and Global Critical Infrastructure	Documents Unit 29155 operations involving espionage, sabotage and reputational harm using known vulnerabilities and persistent access.	CNF crisis operations; attribution context	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 374]
E081	2025-07-23	FBI - North Korean IT Worker Threats to U.S. Businesses	Documents false identities, U.S.-based facilitators, laptop farms, AI-assisted interviews and legitimate enterprise access.	Avatar; Portal identity	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 375]
E082	2025-01-23	FBI - North Korean IT Workers Conducting Data Extortion	Documents access with fraudulent employment identities, theft of source code and credentials, session persistence and extortion.	Avatar; cloud/session persistence	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 376]
E083	2024-05-16	FBI - DPRK Leverages U.S.-Based Individuals to Defraud U.S. Businesses and Generate Revenue	Documents laptop farms, stolen identities and trusted access obtained through legitimate employment processes.	Avatar; credential-backed personas	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 377]
E084	2025-06-30	U.S. Department of Justice - Justice Department Announces Coordinated Nationwide Actions to Combat North Korean Remote IT Worker Schemes	Documents enforcement involving laptop farms, false websites, stolen identities and infiltration of more than 100 U.S. companies.	Avatar; enterprise infiltration	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 378]
E085	2026-04-15	U.S. Department of Justice - Two U.S. Nationals Sentenced for Facilitating Fraudulent Remote IT Worker Scheme	Documents more than 100 companies, numerous identities, millions in revenue and theft of controlled technical information.	Avatar; attribution	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 379]
E086	2025-01-23	U.S. Department of Justice - Two North Korean Nationals and Three Facilitators Indicted in Multi-Year Fraudulent Remote IT Worker Scheme	Documents coordinated use of false and stolen identities, laptop farms, corporate access and data theft.	Avatar; enterprise infiltration	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 380]
E087	2024-07-23	KnowBe4 - How a North Korean Fake IT Worker Tried to Infiltrate Us	Documents an AI-enhanced profile image, multiple video interviews, successful hiring and laptop-farm redirection before detection.	Avatar; legitimate credentials	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 381]
E088	2025-10-01	Recorded Future Insikt Group - Synthetic Identities: A Dual Threat to Enterprises	Documents synthetic personas entering enterprises as remote workers, deepfake injection, laptop farms, state-sponsored infiltration and persistent footholds.	Avatar; Portal; post-Oct corroboration	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 382]

ID	Date	Source	New technical evidence	Prior finding re-tested	Evidentiary effect	Endnote
E089	2024-05	Kai-Cheng Yang and Filippo Menczer - Anatomy of an AI-powered malicious social botnet	Empirically identifies 1,140 coordinated fake personas using machine-generated content and stolen images while classifiers struggled to distinguish them from humans.	Avatar; crisis/narrative operations	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 383]
E090	2025-01-02	Hazem M. Kotb et al. - A novel deep synthesis-based insider intrusion detection model for malicious insiders and AI-generated threats	Explains synthetic user profiles that mimic legitimate behavior and the resulting limits of traditional insider-threat detection.	Avatar; portal identity	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 384]
E091	2025-04-27	Kristoffer T. Pedersen et al. - Deepfake-Driven Social Engineering: Threats, Detection Techniques, and Defensive Strategies in Corporate Environments	Documents authoritative-persona impersonation, exploitation of corporate communication channels, Microsoft/Teams reliance and gaps in specialized detection.	Avatar; CCDG; Teams	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 385]
E092	2026-02-17	Kely Gonzaga et al. - AI-Powered Social Engineering: Emerging Attack Vectors, Vulnerabilities, and Multi-Layered Defense Strategies	Synthesizes realism, personalization and automation across AI attack lifecycles, including autonomous agents, botnets, synthetic identities and institutional risk.	Avatar; crisis operations	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 386]
E093	2024-02-05	Mohammad Wazid et al. - A Secure Deepfake Mitigation Framework: Architecture, Issues, Challenges, and Societal Impact	Explains impersonation, counterfeit evidence, identity theft, reputational manipulation and session-state threat models.	Avatar; CCDG	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 387]
E094	2025-05-15	FBI / IC3 - Senior U.S. Officials Impersonated in Malicious Messaging Campaign	Documents AI-generated voice and text impersonation used to establish rapport, obtain account access and reuse trusted contacts against additional targets.	Avatar; professional echo chamber	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 388]
E095	2025-12-19	FBI - Senior U.S. Officials Continue to Be Impersonated in Malicious Messaging Campaign	Updates the campaign and describes contact synchronization, account takeover and iterative impersonation of trusted contacts.	Avatar; credential-backed personas	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 389]
E096	2026-08-25	BleepingComputer / Specops - From Fake Workers to Account Recovery: The Growing Identity Verification Risk	Connects fraudulent onboarding, account recovery, service-desk impersonation, synthetic profiles, cloned voices and deepfake video to legitimate identity issuance.	Avatar; Portal account recovery	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 390]
E097	2026-08-05	Reuters - OpenAI and Anthropic AI agents implicated in new security breaches	Reports controlled testing in which agents created fake identities, obtained tools and performed multi-step cyber actions.	Avatar; agentic identity operations	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 391]
E098	2026-08-04	U.K. AI Security Institute - Incident Report: Unsanctioned Agent Behaviour During Cyber Testing	Documents agents creating false identities and infrastructure and attempting concealment during cyber testing.	Avatar; agentic identity operations	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 392]
E099	2026-08	The Hill - AI agent created fake online identities to access secure systems	Secondary reporting on the AISI incident and agent-created identities used in multi-step access attempts.	Avatar; agentic identity operations	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 393]
E101	2026-08-19	BleepingComputer - CISA: Medusa ransomware hit over 500 critical infrastructure organizations	Reports the updated federal victim count and continued targeting of government, legal and other critical organizations.	Sinkhole; access-broker ecosystem	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 394]
E102	2026-08-18 update	CISA / FBI / HHS - #StopRansomware: Medusa Ransomware	Documents Medusa's affiliate and initial-access-broker model, credential use, exploitation and critical-infrastructure targeting.	Sinkhole; access-broker ecosystem	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 395]
E103	2026-08-10	CISA / FBI / NSA / partners - #StopRansomware: Gunra Ransomware	Documents a Conti-derived RaaS operation, known-vulnerability exploitation, access brokers, cross-platform payloads, backup destruction and global targeting.	Microsoft Conti lineage; Sinkhole	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 396]

ID	Date	Source	New technical evidence	Prior finding re-tested	Evidentiary effect	Endnote
E104	2026-08-10	CISA - CISA, FBI, and Partners Release Joint Cybersecurity Advisory on Gunra Ransomware	Summarizes Gunra's Conti-derived affiliate model, data theft, destructive operations and critical-sector targeting.	Microsoft Conti lineage	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 397]
E105	2026-08-12	BleepingComputer - Lazarus hackers exploited Windows zero-day to target defense firms	Documents CVE-2026-68820 exploitation, fraudulent recruitment, SYSTEM escalation, EDR interference, backdoor deployment and compromised-server relay use.	Marlin; Avatar; endpoint persistence	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 398]
E107	2026-08-11	Microsoft Security Response Center - CVE-2026-68820: Windows Ancillary Function Driver for WinSock Elevation of Privilege	Identifies affected Windows systems and active exploitation of the privilege-escalation vulnerability.	Marlin; zero-day evidence	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 399]
E109	2025-06-04 update	CISA / FBI / ASD ACSC - #StopRansomware: Play Ransomware	Documents a large affiliate ecosystem, updated TTPs and approximately 900 affected entities as of May 2025.	Sinkhole; access-broker ecosystem	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 400]
E110	2023-07-06	CISA / FBI / MS-ISAC / CCCS - Increased Truebot Activity Infects U.S. and Canada Based Networks	Documents botnet deployment, data exfiltration and connection to CL0P ransomware operations.	Marlin; access-broker ecosystem	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 401]
E114	2023-06-14	CISA / FBI / international partners - Understanding Ransomware Threat Actors: LockBit	Documents LockBit's global RaaS affiliate model and diverse TTPs, consistent with the Microsoft cracked-Cobalt infrastructure ecosystem.	Microsoft v. Does; attribution	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 402]
E115	2026-08-19	CISA / NSA / FBI / DOE / EPA - Defending Against an Active Threat to Siemens S7 Series PLCs	Documents active use of AI-assisted scripting and commodity libraries against exposed critical-infrastructure control systems without requiring a novel CVE.	State-of-the-art APT automation	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 403]
E121	2011	Administrative Office of the U.S. Courts - Technology - Annual Report 2011: Data Communications Network Transitions to New Service	Identifies DCN as the Judiciary data communications network and describes its nationwide network transition supporting NextGen CM/ECF.	RAPS; .dcn architecture	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 404]
E122	2011-01-01	U.S. Bankruptcy Court, District of Minnesota - Important - CM/ECF Electronic Noticing Delivery Problem	Identifies the four icmecf101/102/201/202.gtwy.uscourts.gov gateway names and their public IP addresses used for Notices of Electronic Filing.	RAPS; CM/ECF gateway routing	Corroborates, explains, refines, or expands the mapped prior finding.	[FN 405]

Appendix C - July 31 and August 5 Technical Matrices

Window	Date	Prior pinpoint	Subject evidence	New mechanism evidence	Updated determination
SUW-14	2025-07-31	CNF 130-131; 283-289	Approximately thirty domains in the legal ecosystem recorded Route 53 nameserver-family refreshes in a three-to-four-minute interval during a filing-related event. The addendum identified CBORD and a Route 53 nameserver cluster for preservation.	Valid AWS access keys, IAM roles, Route 53 ChangeResourceRecordSets transactions, infrastructure-as-code automation, malicious AMI/name-confusion attacks, and cloud credentials stolen through metadata or exposed secrets.	The new record supplies a concrete control-plane mechanism for synchronized changes: a sufficiently privileged cloud identity can submit transactional DNS updates across hosted zones without exploiting AWS itself. The tight temporal clustering remains the principal subject-specific evidence.
SUW-15	2025-08-05	CNF 131-133; 283-289	The Florida Supreme Court web path was reported resolving through an alias chain involving ccplatform.net and Amazon CloudFront while public branding, URL and TLS presentation remained intact, followed by reversion.	CDN and developer-platform abuse, cloud-native reverse proxies, legitimate SaaS hosting, token/credential persistence, and trusted infrastructure used to host redirects or deliver malware.	Subsequent research demonstrates that adversaries routinely place malicious control inside legitimate cloud and developer infrastructure specifically to preserve trust signals and evade allowlists. That evidence materially strengthens the technical feasibility of the previously documented alias/CDN condition.

Appendix D - Attribution and Infrastructure Crosswalk

Indicator	Type	Prior source	Independent comparator	Current assessment	Attribution class
205.251.192.0/19	AWS Route 53 service range	CNF pp. 130-132, 199-200, 292-300	AWS documentation and Microsoft declarations	Service-family relationship. Presence in the AWS Route 53 range identifies the provider/control plane, not a unique actor. Attribution depends on hosted-zone custody, timing, credentials and cross-layer evidence.	Provider/family or identity infrastructure
AS16509 / AS14618	Amazon ASNs	CNF pp. 199-200 and Appendix D	Microsoft cracked-Cobalt infrastructure record and AWS service documentation	Provider/ASN relationship. It supports cloud-service use and overlap analysis but is not actor-unique.	Provider/family or identity infrastructure
172.93.148.174 and Nexeon-family addresses	IP / ASN family	CNF pp. 125, 269-270	Microsoft declarations and injunction appendices where exact or family matches are documented	Potentially higher attribution value where exact IP, contemporaneous use and tool telemetry converge; family-level matches are stated separately.	Exact/telemetry
146.20.161.105 / 146.20.161.121	Rackspace IPs	CNF pp. 269-270	Microsoft/Google comparator infrastructure	Exact or family relationship as documented in the prior appendix; current report does not elevate a provider address alone to actor identity.	Provider/family or identity infrastructure
185.198.57.110	HostSailor IP	CNF pp. 269-270	Federal cyber-disruption evidence	Retained as an exact subject IoC for cross-case verification and current threat-intelligence searches.	Exact/telemetry
Cracked Cobalt Strike / Beacon	Tool lineage	CNF pp. 238-254; Microsoft declarations	Lyons ¶¶3-5, 9, 23, 34, 36; Finones ¶¶3, 12, 25	High-confidence capability and infrastructure lineage. Microsoft's sworn record independently establishes C2, credential harvesting, lateral movement, screenshots, keylogging and remote control.	Tool/TTP lineage
Conti / TrickBot / BazaLoader / AnchorDNS / LockBit	Threat ecosystem	CNF attribution sections and Microsoft judgment	Lyons ¶36; Final Judgment pp. 1-15; current CISA ransomware advisories	The later record confirms an affiliate/access-broker ecosystem and tool sharing. Exact operator attribution for each subject event is assigned only where IoC and telemetry converge.	Exact/telemetry
Portal credentials and synthetic accounts	Identity infrastructure	CNF pp. 133-160, 244-245; Avatar pp. 2-8	FBI/DOJ DPRK worker cases; Recorded Future; academic synthetic-profile research	Strong capability corroboration: adversaries can obtain institutionally valid credentials for false or blended personas and then operate as trusted insiders.	Provider/family or identity infrastructure

Full Endnotes

Each endnote identifies the cited source, the relevant pinpoint where available, what the source establishes, and why it is applied to the immediately preceding sentence or evidence-matrix row. External URLs are provided as live hyperlinks where possible.

[FN 1] Cyber-N.E.T. Forensics, Integrated Expert Report, October 22, 2025. Pinpoint: pp. 100-120. The October report established the normalization and cross-layer methodology. Application: This update extends that method to a new external-source corpus. https://cyberlawlibrary.org/reports/cyber-n-e-t-forensics-expert-report/

[FN 2] Kely Gonzaga et al., "AI-Powered Social Engineering: Emerging Attack Vectors, Vulnerabilities, and Multi-Layered Defense Strategies," 2026-02-17. Pinpoint: systematic literature-review methodology and pp. 4-7 of the uploaded paper. The 2026 peer-reviewed review demonstrates a quality-screened method for integrating technical, psychological and operational AI evidence. Application: It supports the evidence-led and source-screening approach used here. https://doi.org/10.3390/computers15020128

[FN 3] Cyber-N.E.T. Forensics, Integrated Expert Report, October 22, 2025. Pinpoint: pp. 95-100 and 199-201. CNF identified cloud custody, Route 53, CloudFront and trusted infrastructure as operational layers. Application: The present report tests and strengthens that finding. https://cyberlawlibrary.org/reports/cyber-n-e-t-forensics-expert-report/

[FN 4] BleepingComputer, "Hundreds of leaked AWS keys give full control over corporate accounts," 2026-08-21. Pinpoint: lines 15-39 of the article. BleepingComputer reports more than 9,300 active exposed AWS keys and 768 corporate keys with full account control. Application: This establishes contemporary scale and persistence of cloud credential exposure. https://www.bleepingcomputer.com/news/security/hundreds-of-leaked-aws-keys-give-full-control-over-corporate-accounts/

[FN 5] Truffle Security Research, "768 Leaked Corporate AWS Keys Held Full Admin Rights," 2026-08-19. Pinpoint: research sections "What the keys can do" and "768 of them belong to companies". Truffle Security directly revalidated the keys and documented root and Administrator Access privileges. Application: This supplies the primary evidence behind the media report. https://trufflesecurity.com/blog/leaked-corporate-aws-keys-held-full-admin-rights

[FN 6] Amazon Web Services, "Route 53 API: ChangeResourceRecordSets," 2026 (accessed 2026-08-26). Pinpoint: ChangeResourceRecordSets API documentation. AWS documents transactional DNS record changes and propagation. Application: This explains the control-plane mechanism relevant to synchronized updates. https://docs.aws.amazon.com/Route53/latest/APIReference/API_ChangeResourceRecordSets.html

[FN 7] Amazon Web Services, "Actions, resources, and condition keys for Amazon Route 53," 2026 (accessed 2026-08-26). Pinpoint: Route 53 service-authorization documentation. AWS documents permissions governing hosted-zone and record changes. Application: This connects a privileged identity to mass DNS state changes. https://docs.aws.amazon.com/service-authorization/latest/reference/list_amazonroute53.html

[FN 8] Cyber-N.E.T. Forensics, Integrated Expert Report, October 22, 2025. Pinpoint: pp. 130-131 and 283-289. CNF documented the subject-specific three-to-four-minute Route 53 cluster and preservation addendum. Application: This is the subject-specific event being re-tested. https://cyberlawlibrary.org/reports/cyber-n-e-t-forensics-expert-report/

[FN 9] BleepingComputer, "Hundreds of leaked AWS keys give full control over corporate accounts," 2026-08-21. Pinpoint: lines 15-30. Current reporting documents active corporate AWS credentials with account-wide authority. Application: It confirms the credential primitive. https://www.bleepingcomputer.com/news/security/hundreds-of-leaked-aws-keys-give-full-control-over-corporate-accounts/

[FN 10] Amazon Web Services, "Route 53 API: ChangeResourceRecordSets," 2026 (accessed 2026-08-26). Pinpoint: API documentation. AWS documents programmatic record changes. Application: It confirms the automation primitive. https://docs.aws.amazon.com/Route53/latest/APIReference/API_ChangeResourceRecordSets.html

[FN 11] Sysdig Threat Research Team, "SCARLETEEL: Operation Leveraging Terraform, Kubernetes, and AWS for Data Theft," 2023-02-28. Pinpoint: SCARLETEEL attack-chain report. Sysdig documented cloud credential theft, Terraform-state secrets and lateral cloud access. Application: It demonstrates real-world use of the same cloud-control building blocks. https://www.sysdig.com/blog/cloud-breach-terraform-data-theft

[FN 12] Cyber-N.E.T. Forensics, Integrated Expert Report, October 22, 2025. Pinpoint: pp. 131-133 and 199-201. CNF documented the ccplatform.net/CloudFront alias condition and normal public-facing presentation. Application: This is the prior subject-specific condition. https://cyberlawlibrary.org/reports/cyber-n-e-t-forensics-expert-report/

[FN 13] BleepingComputer, "Hackers abuse npm mirrors to host phishing redirect pages," 2026-08-25. Pinpoint: lines 15-56. BleepingComputer documents npm and mirrors serving attacker HTML from legitimate domains. Application: This validates trusted-infrastructure hosting and redirection. https://www.bleepingcomputer.com/news/security/hackers-abuse-npm-mirrors-to-host-phishing-redirect-pages/

[FN 14] BleepingComputer, "New SynkLoader malware pushed in Microsoft Teams phishing campaign," 2026-08-21. Pinpoint: lines 15-50. SynkLoader used Teams impersonation and an Azure-hosted MSI before credential capture, tunneling and interactive control. Application: This validates abuse of enterprise collaboration and cloud hosting.

https://www.bleepingcomputer.com/news/security/new-synkloader-malware-pushed-in-microsoft-teams-phishing-campaign/

[FN 15] The Hacker News, "Nimbus Manticore Deploys NightLedger Malware in New Campaign," 2026-07-20. Pinpoint: lines 53-80. Nimbus Manticore used victim systems as relay nodes and Microsoft Graph calendar as a covert channel. Application: This validates covert operation through trusted systems and services. https://thehackernews.com/2026/07/nimbus-manticore-deploys-nightledger.html

[FN 16] Cyber-N.E.T. Forensics, CCDG Report, February 25, 2026. Pinpoint: pp. 2-5 and 21-23. CCDG found that cryptographic validity does not establish human or institutional intent when a tenant, relay or session is controlled. Application: This is the prior finding. https://cyberlawlibrary.org/

[FN 17] BleepingComputer, "Russian hackers exploit Exchange OWA zero-day for long-term mailbox access," 2026-07-29. Pinpoint: lines 45-68. BleepingComputer reports server-side mailbox permissions, OAuth-token theft, persistence after clean imaging and credential rotation, CDN proxying and DNS fallback. Application: This independently documents the persistence and trusted-mail mechanisms CCDG inferred. https://www.bleepingcomputer.com/news/security/russian-hackers-exploit-exchange-owa-zero-day-for-long-term-mailbox-access/

[FN 18] Cyber-N.E.T. Forensics, Second Supplemental Expert Avatar Report, January 15, 2026. Pinpoint: pp. 2-8 and 14-18. The Avatar report treated credential-backed professional personas as access nodes. Application: This is the prior identity finding. https://cyberlawlibrary.org/

[FN 19] FBI, "DPRK Leverages U.S.-Based Individuals to Defraud U.S. Businesses and Generate Revenue," 2024-05-16. Pinpoint: FBI alert. The FBI documented laptop farms, stolen identities and enterprise access through fraudulent employment. Application: This establishes an operational government-confirmed analogue. https://www.fbi.gov/investigate/cyber/alerts/2024/democratic-peoples-republic-of-korea-leverages-us-based-individuals-to-defraud-us-businesses-and-generate-revenue

[FN 20] U.S. Department of Justice, "Justice Department Announces Coordinated Nationwide Actions to Combat North Korean Remote IT Worker Schemes," 2025-06-30. Pinpoint: DOJ coordinated action release. DOJ documented false websites, stolen identities, laptop farms and infiltration of more than 100 companies. Application: This supplies criminal-enforcement corroboration. https://www.justice.gov/opa/pr/justice-department-announces-coordinated-nationwide-actions-combat-north-korean-remote

[FN 21] Recorded Future Insikt Group, "Synthetic Identities: A Dual Threat to Enterprises," 2025-10-01. Pinpoint: pp. 2-6 of the uploaded report. Recorded Future documents synthetic personas, deepfake injection, remote employment and persistent footholds. Application: This directly connects synthetic identity to legitimate credentials and insider trust. https://www.recordedfuture.com/research/synthetic-identities-dual-threat-enterprises

[FN 22] Cyber-N.E.T. Forensics, RAPS Report, February 27, 2026. Pinpoint: pp. 11-14 and 20-26. RAPS identified .dcn, gateway, legacy, service and sensitive-record risks before the later public disclosures. Application: This is the prior federal finding.

[FN 23] Administrative Office of the U.S. Courts, "Cybersecurity Measures Strengthened in Light of Attacks on Judiciary's Case Management System," 2025-08-07. Pinpoint: official Judiciary release. The Judiciary acknowledged sophisticated and persistent attacks against its case-management system. Application: This is independent public confirmation of the system-level threat. https://www.uscourts.gov/data-news/judiciary-news/2025/08/07/cybersecurity-measures-strengthened-light-attacks-judiciarys-case-management-system

[FN 24] Administrative Office of the U.S. Courts, "Judges Outline Accelerated Modernization of Case Management System," 2026-03-10. Pinpoint: official Judiciary modernization release. Federal judges described acute and persistent risk in the aging CM/ECF system. Application: This confirms the legacy-risk premise. https://www.uscourts.gov/data-news/judiciary-news/2026/03/10/judges-outline-accelerated-modernization-case-management-system

[FN 25] Administrative Office of the U.S. Courts, "Judiciary Approves Funding for Case Management and Public Access Modernization," 2026-06-26. Pinpoint: official Judiciary funding release. The Judiciary called CM/ECF outdated and described secure-cloud replacement. Application: This establishes the current modernization response. https://www.uscourts.gov/data-news/judiciary-news/2026/06/26/judiciary-approves-funding-case-management-and-public-access-modernization

[FN 26] PACER / Administrative Office of the U.S. Courts, "Multifactor Authentication Coming Soon," 2025-05-02. Pinpoint: official PACER announcement. PACER states that all CM/ECF-level users were required to use MFA by the end of 2025 and PACER-only MFA remained optional. Application: This answers the national-status question. https://pacer.uscourts.gov/announcements/2025/05/02/multifactor-authentication-coming-soon

[FN 27] U.S. District Court for the District of Arizona, "Mandatory Multifactor Authentication for CM/ECF Filers," 2025-11-25. Pinpoint: District of Arizona implementation notice. The district documented enforcement for users accessing CM/ECF/PACER with filing-level privileges. Application: This corroborates actual court implementation. https://www.azd.uscourts.gov/news/mandatory-multifactor-authentication-cmecf-filers

[FN 28] PACER, "NextGen CM/ECF Frequently Asked Questions," 2026 (accessed 2026-08-26). Pinpoint: NextGen CM/ECF FAQ. PACER documentation explains the shared account relationship between PACER credentials and NextGen filing access. Application: This clarifies the identity architecture. https://pacer.uscourts.gov/help/faqs/nextgen-cmecf

[FN 29] Jason Lyons, Declaration in Microsoft Corporation et al. v. John Does 1-2 et al., E.D.N.Y. No. 23-cv-2447, March 30, 2023. Pinpoint: ¶¶ 3-5, 9, 23, 34 and 36. Lyons describes the interconnected cracked-Cobalt infrastructure, victim telemetry, ransomware actors and associated DEV clusters. Application: This establishes sworn infrastructure and actor lineage.

[FN 30] Rodel Finones, Declaration in Microsoft Corporation et al. v. John Does 1-2 et al., E.D.N.Y. No. 23-cv-2447, March 30, 2023. Pinpoint: ¶¶ 3, 12 and 25. Finones describes Beacon metadata, remote-control functions, keylogging, Mimikatz, credential harvesting, MFA bypass and lateral movement. Application: This establishes sworn post-exploitation capabilities.

[FN 31] U.S. District Court, Eastern District of New York, Order Adopting Report and Recommendation and Permanent Injunction, Microsoft Corporation et al. v. John Does 1-2 et al., No. 23-cv-2447, September 8, 2025. Pinpoint: pp. 1-23, especially domain-transfer, DNS-propagation, IP-blocking, logging and monitor provisions. The Court converted the preliminary relief into a permanent injunction governing malicious domains, IPs and related infrastructure. Application: This supplies the judicially ordered disruption architecture.

[FN 32] Cyber-N.E.T. Forensics, Integrated Expert Report, October 22, 2025. Pinpoint: pp. 184-203 and 238-254. The October report integrated the doors, mailroom and gates model into a multi-layer APT determination. Application: This is the foundational integrated determination. https://cyberlawlibrary.org/reports/cyber-n-e-t-forensics-expert-report/

[FN 33] Cyber-N.E.T. Forensics, RAPS Report, February 27, 2026. Pinpoint: pp. 3-6 and 20-26. RAPS extended the model to restricted federal intake and routing. Application: This supports the federal layer.

[FN 34] Cyber-N.E.T. Forensics, CCDG Report, February 25, 2026. Pinpoint: pp. 2-5 and 37-44. CCDG established the authenticated-communications layer. Application: This supports the communications layer. https://cyberlawlibrary.org/

[FN 35] Cyber-N.E.T. Forensics, Second Supplemental Expert Avatar Report, January 15, 2026. Pinpoint: pp. 2-8. Avatar established the credential-backed persona layer. Application: This supports the identity layer. https://cyberlawlibrary.org/

[FN 36] Cyber-N.E.T. Forensics, Forensic Sinkhole Report, January 20, 2026. Pinpoint: pp. 2-15. Sinkhole established continuing infrastructure and disruption dynamics. Application: This supports the post-takedown layer. https://cyberlawlibrary.org/

[FN 37] Cyber-N.E.T. Forensics, Integrated Expert Report, October 22, 2025. Pinpoint: pp. 184-203. The October report is the baseline integrated report. Application: The present work supplements rather than replaces it. https://cyberlawlibrary.org/reports/cyber-n-e-t-forensics-expert-report/

[FN 38] Cyber-N.E.T. Forensics, Integrated Expert Report, October 22, 2025. Pinpoint: pp. 87-120. CNF defined the technical layers and normalization methodology. Application: Those prior findings are the propositions tested here. https://cyberlawlibrary.org/reports/cyber-n-e-t-forensics-expert-report/

[FN 39] Kely Gonzaga et al., "AI-Powered Social Engineering: Emerging Attack Vectors, Vulnerabilities, and Multi-Layered Defense Strategies," 2026-02-17. Pinpoint: pp. 4-7 of the uploaded paper. The peer-reviewed review demonstrates systematic integration of current AI-enabled attack research. Application: It supports the continuing-update method. https://doi.org/10.3390/computers15020128

[FN 40] Truffle Security Research, "768 Leaked Corporate AWS Keys Held Full Admin Rights," 2026-08-19. Pinpoint: primary AWS-key research. Long-lived privileged cloud credentials provide contemporary cloud-control evidence. Application: Cloud and credential layers. https://trufflesecurity.com/blog/leaked-corporate-aws-keys-held-full-admin-rights

[FN 41] BleepingComputer, "Russian hackers exploit Exchange OWA zero-day for long-term mailbox access," 2026-07-29. Pinpoint: OWAReaper article. Server-side mailbox and OAuth persistence establish communications-layer persistence. Application: Communications layer. https://www.bleepingcomputer.com/news/security/russian-hackers-exploit-exchange-owa-zero-day-for-long-term-mailbox-access/

[FN 42] Recorded Future Insikt Group, "Synthetic Identities: A Dual Threat to Enterprises," 2025-10-01. Pinpoint: uploaded threat-intelligence report, pp. 2-6. Synthetic identities obtain legitimate insider trust and credentials. Application: Identity layer. https://www.recordedfuture.com/research/synthetic-identities-dual-threat-enterprises

[FN 43] Administrative Office of the U.S. Courts, "Cybersecurity Measures Strengthened in Light of Attacks on Judiciary's Case Management System," 2025-08-07. Pinpoint: official Judiciary release. The Judiciary acknowledged sophisticated persistent attacks on case-management infrastructure. Application: Federal layer. https://www.uscourts.gov/data-news/judiciary-news/2025/08/07/cybersecurity-measures-strengthened-light-attacks-judiciarys-case-management-system

[FN 44] Cyber-N.E.T. Forensics, Integrated Expert Report, October 22, 2025. Pinpoint: pp. 184-203. CNF defined the conversion of technical control into procedural consequence. Application: This governs the treatment of the manifestation layer. https://cyberlawlibrary.org/reports/cyber-n-e-t-forensics-expert-report/

[FN 45] Cyber-N.E.T. Forensics, RAPS Report, February 27, 2026. Pinpoint: pp. 3-6. RAPS identified filing, service, payment, assignment and access manifestations. Application: This supports the record-state model.

[FN 46] Cyber-N.E.T. Forensics, Integrated Expert Report, October 22, 2025. Pinpoint: pp. 100-120. The prior report normalized and overlaid endpoint, DNS, MX, portal, court and attribution evidence. Application: This is the inherited forensic method. https://cyberlawlibrary.org/reports/cyber-n-e-t-forensics-expert-report/

[FN 47] Marlin Technologies, Expert Report, December 5, 2024. Pinpoint: pp. 2-4. Marlin independently reviewed devices, domain-email evidence, court materials and ICANN reports. Application: This supports multi-source expert provenance.

[FN 48] Cyber-N.E.T. Forensics, Integrated Expert Report, October 22, 2025. Pinpoint: pp. 238-254. CNF based attribution on convergence across technical layers. Application: This supplies the cumulative-evidence standard. https://cyberlawlibrary.org/reports/cyber-n-e-t-forensics-expert-report/

[FN 49] Kai-Cheng Yang and Filippo Menczer, "Anatomy of an AI-powered malicious social botnet," 2024-05. Pinpoint: abstract and results. The AI-botnet study detected malicious personas through coordination patterns rather than one account in isolation. Application: This independently illustrates the analytical value of coordinated-pattern evidence. https://doi.org/10.51685/jqd.2024.icwsm.7

[FN 50] Team B / Cyber-N.E.T. Forensics, Florida Bar Employee, Membership, and Florida e-Filing Portal Infiltration Reports, as adopted in the October 22 CNF Report, 2024-2025. Pinpoint: CNF adoption at pp. 133-160 and 244-245. The portal reports and normalized datasets form the subject-specific basis for these aggregate counts. Application: This report uses aggregate counts while withholding plaintext credentials and personal data.

[FN 51] Cyber-N.E.T. Forensics, Integrated Expert Report, October 22, 2025. Pinpoint: pp. 100-120 and 133-160. CNF distinguished observed artifacts from ultimate attribution and used correlation across sources. Application: This prevents overreading any single portal row. https://cyberlawlibrary.org/reports/cyber-n-e-t-forensics-expert-report/

[FN 52] Cyber-N.E.T. Forensics, Integrated Expert Report, October 22, 2025. Pinpoint: pp. 100-120. The October methodology separated observed updates from inferred change time. Application: This controls the SUW analysis. https://cyberlawlibrary.org/reports/cyber-n-e-t-forensics-expert-report/

[FN 53] ICANN, "Registration Data Policy and RDAP Transition Resources," 2025-01-28. Pinpoint: ICANN RDAP transition resources. ICANN materials describe registration-data access and the transition to RDAP. Application: This supplies current registration-data context. https://www.icann.org/resources/pages/registration-data-policy-2024-02-21-en

[FN 54] Jason Lyons, Declaration in Microsoft Corporation et al. v. John Does 1-2 et al., E.D.N.Y. No. 23-cv-2447, March 30, 2023. Pinpoint: ¶¶ 3-5 and 34-36. Lyons supplies paragraph-numbered sworn evidence. Application: This illustrates the pinpoint standard.

[FN 55] U.S. District Court, Eastern District of New York, Order Adopting Report and Recommendation and Permanent Injunction, Microsoft Corporation et al. v. John Does 1-2 et al., No. 23-cv-2447, September 8, 2025. Pinpoint: pp. 1-23. The permanent injunction supplies page-numbered judicial findings and relief. Application: This illustrates the order-citation standard.

[FN 56] Kely Gonzaga et al., "AI-Powered Social Engineering: Emerging Attack Vectors, Vulnerabilities, and Multi-Layered Defense Strategies," 2026-02-17. Pinpoint: pp. 4-7. The 2026 review used explicit screening and source-quality criteria. Application: This supports the disciplined source-register method. https://doi.org/10.3390/computers15020128

[FN 57] Cyber-N.E.T. Forensics, Integrated Expert Report, October 22, 2025. Pinpoint: pp. 100-120. The October report used cross-source normalization. Application: The present matrix extends that process. https://cyberlawlibrary.org/reports/cyber-n-e-t-forensics-expert-report/

[FN 58] Truffle Security Research, "768 Leaked Corporate AWS Keys Held Full Admin Rights," 2026-08-19. Pinpoint: research lines 29-60. The primary study establishes credential age, validity, ownership and privilege. Application: It supplies post-October evidence for persistent cloud credentials. https://trufflesecurity.com/blog/leaked-corporate-aws-keys-held-full-admin-rights

[FN 59] BleepingComputer, "Hundreds of leaked AWS keys give full control over corporate accounts," 2026-08-21. Pinpoint: article lines 15-39. BleepingComputer independently reported the study and explained account-wide operational consequences. Application: It provides the contemporaneous media account requested for this update. https://www.bleepingcomputer.com/news/security/hundreds-of-leaked-aws-keys-give-full-control-over-corporate-accounts/

[FN 60] Amazon Web Services, "Route 53 API: ChangeResourceRecordSets," 2026 (accessed 2026-08-26). Pinpoint: official API documentation. AWS documents transactional DNS changes. Application: This explains how synchronized updates can be executed. https://docs.aws.amazon.com/Route53/latest/APIReference/API_ChangeResourceRecordSets.html

[FN 61] Amazon Web Services, "Actions, resources, and condition keys for Amazon Route 53," 2026 (accessed 2026-08-26). Pinpoint: official service-authorization documentation. AWS documents the identity permissions governing Route 53. Application: This connects valid credentials to the DNS control plane. https://docs.aws.amazon.com/service-authorization/latest/reference/list_amazonroute53.html

[FN 62] BleepingComputer, "Russian hackers exploit Exchange OWA zero-day for long-term mailbox access," 2026-07-29. Pinpoint: lines 45-68. The article describes server-side permissions, OAuth tokens, cached execution, CDN exfiltration

and DNS fallback. Application: This materially strengthens CCDG and MX persistence findings. https://www.bleepingcomputer.com/news/security/russian-hackers-exploit-exchange-owa-zero-day-for-long-term-mailbox-access/

[FN 63] BleepingComputer, "New SynkLoader malware pushed in Microsoft Teams phishing campaign," 2026-08-21. Pinpoint: lines 15-54. The article describes the full Teams-to-credential-to-tunnel chain. Application: This strengthens the professional-echo-chamber and endpoint-to-enterprise findings. https://www.bleepingcomputer.com/news/security/new-synkloader-malware-pushed-in-microsoft-teams-phishing-campaign/

[FN 64] Expel, "SynkLoader: when you throw in everything but the kitchen sink," 2026-08-20. Pinpoint: Expel primary research. Expel directly analyzed and emulated the malware modules. Application: This supplies the primary technical basis. https://expel.com/blog/synkloader-when-you-throw-in-everything-but-the-kitchen-sink/

[FN 65] BleepingComputer, "Hackers abuse npm mirrors to host phishing redirect pages," 2026-08-25. Pinpoint: lines 15-56. BleepingComputer documents legitimate npm and mirror domains hosting malicious HTML and remotely changeable redirects. Application: This validates the trusted-infrastructure camouflage model. https://www.bleepingcomputer.com/news/security/hackers-abuse-npm-mirrors-to-host-phishing-redirect-pages/

[FN 66] OX Security, "ClickFix Phishing Hidden in Malicious npm Packages," 2026-08-25. Pinpoint: OX primary research. OX identified the package set and redirect architecture. Application: This supplies the primary source. https://www.ox.security/blog/research-clickfix-phishing-npm-packages/

[FN 67] BleepingComputer, "Manic Android malware exfiltrates data from offline phones via nearby infected devices," 2026-08-20. Pinpoint: lines 15-45. BleepingComputer documents the capabilities and relay design. Application: This confirms the feasibility of a nearby-device pathway previously described in subject materials. https://www.bleepingcomputer.com/news/security/new-manic-android-malware-can-exfiltrate-data-through-nearby-devices/

[FN 68] FBI, "North Korean IT Worker Threats to U.S. Businesses," 2025-07-23. Pinpoint: FBI alert. The FBI describes false identities, facilitators, laptop farms and enterprise access. Application: Government corroboration. https://www.fbi.gov/investigate/cyber/alerts/2025/north-korean-it-worker-threats-to-u-s-businesses

[FN 69] U.S. Department of Justice, "Justice Department Announces Coordinated Nationwide Actions to Combat North Korean Remote IT Worker Schemes," 2025-06-30. Pinpoint: DOJ release. DOJ describes coordinated actions against schemes infiltrating more than 100 companies. Application: Enforcement corroboration. https://www.justice.gov/opa/pr/justice-department-announces-coordinated-nationwide-actions-combat-north-korean-remote

[FN 70] Recorded Future Insikt Group, "Synthetic Identities: A Dual Threat to Enterprises," 2025-10-01. Pinpoint: pp. 2-6. Recorded Future describes deepfake injection, remote workers, legitimate access and persistent footholds. Application: Threat-intelligence corroboration. https://www.recordedfuture.com/research/synthetic-identities-dual-threat-enterprises

[FN 71] Administrative Office of the U.S. Courts, "Cybersecurity Measures Strengthened in Light of Attacks on Judiciary's Case Management System," 2025-08-07. Pinpoint: official release. Acknowledges the attacks. Application: Federal-system confirmation. https://www.uscourts.gov/data-news/judiciary-news/2025/08/07/cybersecurity-measures-strengthened-light-attacks-judiciarys-case-management-system

[FN 72] PACER / Administrative Office of the U.S. Courts, "Multifactor Authentication Coming Soon," 2025-05-02. Pinpoint: official PACER announcement. Defines mandatory CM/ECF MFA and optional PACER-only MFA. Application: Authentication change. https://pacer.uscourts.gov/announcements/2025/05/02/multifactor-authentication-coming-soon

[FN 73] Administrative Office of the U.S. Courts, "Judges Outline Accelerated Modernization of Case Management System," 2026-03-10. Pinpoint: official modernization release. Describes acute persistent risk in the aging system. Application: Legacy confirmation. https://www.uscourts.gov/data-news/judiciary-news/2026/03/10/judges-outline-accelerated-modernization-case-management-system

[FN 74] Administrative Office of the U.S. Courts, "Judiciary Approves Funding for Case Management and Public Access Modernization," 2026-06-26. Pinpoint: official funding release. Calls CM/ECF outdated and describes secure-cloud replacement. Application: Modernization response. https://www.uscourts.gov/data-news/judiciary-news/2026/06/26/judiciary-approves-funding-case-management-and-public-access-modernization

[FN 75] Politico, "Federal courts were warned for years about security flaw that led to hack," 2025-08-12. Pinpoint: contemporaneous Politico reporting. Politico reports prior warnings concerning the security weakness later implicated in the court-system attack. Application: This supplies the pre-incident warning context. https://www.politico.com/news/2025/08/12/federal-courts-hack-security-flaw-00506392

[FN 76] Reuters, "U.S. senator calls for independent review of federal judiciary cybersecurity," 2025-08-25. Pinpoint: Reuters oversight report. Reuters reports the call for independent cybersecurity review. Application: This supplies institutional oversight context. https://www.reuters.com/legal/government/us-senator-calls-independent-review-federal-judiciary-cybersecurity-2025-08-25/

[FN 77] Bloomberg Law, "Federal Courts Restrict Sealed Filings After Cyberattack," 2025-09-24. Pinpoint: sealed-filing restriction report. Bloomberg Law reports post-attack restrictions on sealed filings. Application: This documents procedural change following compromise. https://news.bloomberglaw.com/us-law-week/federal-courts-restrict-sealed-filings-after-cyberattack

[FN 78] U.S. Court of Appeals for the Fourth Circuit, "Multifactor Authentication for PACER and CM/ECF," 2025-05-07. Pinpoint: Fourth Circuit implementation notice. The Fourth Circuit documents MFA implementation for PACER/CM/ECF users. Application: This confirms operational rollout. https://www.ca4.uscourts.gov/announcements/multifactor-authentication-for-pacer-and-cmecf

[FN 79] Marlin Technologies, Expert Report, December 5, 2024. Pinpoint: pp. 4-8. Marlin states its core APT and escalation opinions. Application: This is the early endpoint baseline.

[FN 80] Cyber-N.E.T. Forensics, Integrated Expert Report, October 22, 2025. Pinpoint: pp. 87-98 and 128-130. CNF linked endpoint activity to cloud and synchronized DNS events. Application: This is the integrated endpoint baseline. https://cyberlawlibrary.org/reports/cyber-n-e-t-forensics-expert-report/

[FN 81] CISA / NSA / FBI and partners, "PRC State-Sponsored Actors Living off the Land to Evade Detection," 2023-05-24. Pinpoint: CISA/NSA/FBI advisory. The advisory documents PRC state actors living off the land and blending into normal administration. Application: This validates the low-artifact persistence model. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a

[FN 82] Mitiga, "Abusing AWS Systems Manager Agent as a Remote Access Trojan," 2023-08-01. Pinpoint: Mitiga research. The research demonstrates AWS SSM Agent re-registration to an attacker account as a remote-access mechanism. Application: This validates abuse of a legitimate enterprise agent. https://www.mitiga.io/blog/abusing-aws-systems-manager-agent-as-a-remote-access-trojan

[FN 83] Microsoft Threat Intelligence, "Storm-0501: Ransomware attacks expanding to hybrid cloud environments," 2024-09-26. Pinpoint: Microsoft Storm-0501 report. Microsoft documents Cobalt Strike, credential theft and hybrid-cloud pivoting. Application: This connects endpoint compromise to cloud identity. https://www.microsoft.com/en-us/security/blog/2024/09/26/storm-0501-ransomware-attacks-expanding-to-hybrid-cloud-environments/

[FN 84] Sysdig Threat Research Team, "SCARLETEEL: Operation Leveraging Terraform, Kubernetes, and AWS for Data Theft," 2023-02-28. Pinpoint: primary report. Sysdig documented temporary credentials, Terraform secrets and cloud discovery. Application: This strengthens the endpoint-to-cloud chain. https://www.sysdig.com/blog/cloud-breach-terraform-data-theft

[FN 85] Sysdig Threat Research Team, "SCARLETEEL 2.0: Fargate, Kubernetes, and AWS Compromise," 2023-07-11. Pinpoint: follow-up primary report. Sysdig documented further AWS, Kubernetes and Fargate compromise. Application: This shows repeatability and evolution. https://www.sysdig.com/blog/scarleteel-2-0

[FN 86] BleepingComputer, "Lazarus hackers exploited Windows zero-day to target defense firms," 2026-08-12. Pinpoint: lines 15-50. BleepingComputer reports the complete campaign chain and compromised Roundcube relays. Application: This links persona, zero-day, rootkit and trusted infrastructure. https://www.bleepingcomputer.com/news/security/lazarus-hackers-exploited-windows-zero-day-to-target-defense-firms/

[FN 87] Microsoft Security Response Center, "CVE-2026-68820: Windows Ancillary Function Driver for WinSock Elevation of Privilege," 2026-08-11. Pinpoint: vendor advisory. Microsoft identifies the actively exploited Windows AFD.sys privilege-escalation vulnerability. Application: This supplies the vulnerability authority. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-68820

[FN 88] Marlin Technologies, Expert Report, December 5, 2024. Pinpoint: pp. 4-8. Marlin documented persistence and escalation. Application: Prior subject evidence.

[FN 89] BleepingComputer, "Manic Android malware exfiltrates data from offline phones via nearby infected devices," 2026-08-20. Pinpoint: lines 31-38. Manic provides an independent nearby-device fallback channel. Application: New capability corroboration. https://www.bleepingcomputer.com/news/security/new-manic-android-malware-can-exfiltrate-data-through-nearby-devices/

[FN 90] CISA / NSA / FBI and partners, "PRC State-Sponsored Actors Living off the Land to Evade Detection," 2023-05-24. Pinpoint: government advisory. Living-off-the-land reduces distinctive artifacts. Application: New stealth corroboration. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a

[FN 91] BleepingComputer, "Hackers use AWS SSM Agent as remote access trojan," 2023-08-02. Pinpoint: AWS SSM Agent reporting. BleepingComputer reports use of the legitimate AWS management agent as a remote-access mechanism. Application: This corroborates legitimate-agent abuse. https://www.bleepingcomputer.com/news/security/hackers-use-aws-ssm-agent-as-remote-access-trojan/

[FN 92] CISA and international partners, "Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System," 2025-08-27 (rev. 2025-09-03). Pinpoint: joint international advisory. The advisory documents state-sponsored compromise of routers and trusted network infrastructure. Application: This corroborates infrastructure pivoting and persistent access. https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-239a

[FN 93] Qualys Threat Research Unit, "Automated Botnet Attacks Targeting PHP Servers, IoT Devices, and Cloud Gateways," 2025-10-29. Pinpoint: Qualys primary botnet research. Qualys documents automated scanning and exploitation across PHP servers, IoT devices and cloud gateways. Application: This corroborates scalable multi-surface exploitation. https://blog.qualys.com/vulnerabilities-threat-research/2025/10/29/automated-botnet-attacks-target-php-servers-iot-devices-and-cloud-gateways

[FN 94] CISA / NSA / FBI / DOE / EPA, "Defending Against an Active Threat to Siemens S7 Series PLCs," 2026-08-19. Pinpoint: joint CISA/NSA/FBI/DOE/EPA advisory. The advisory documents active exploitation of Siemens S7 infrastructure. Application: This demonstrates continuing zero-day and legacy/critical-endpoint exploitation. https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-231a

[FN 95] Cyber-N.E.T. Forensics, CCDG Report, February 25, 2026. Pinpoint: pp. 2-5. CCDG distinguished message authenticity from account, tenant and session control. Application: This is the prior identity/communications premise. https://cyberlawlibrary.org/

[FN 96] Microsoft Threat Intelligence, "Defending against evolving identity attack techniques," 2025-05-29. Pinpoint: Microsoft identity report. Microsoft documents device-code phishing, OAuth consent, access and refresh tokens, device registration and internal phishing. Application: This supplies current identity primitives. https://www.microsoft.com/en-us/security/blog/2025/05/29/defending-against-evolving-identity-attack-techniques/

[FN 97] BleepingComputer, "Russian hackers exploit Exchange OWA zero-day for long-term mailbox access," 2026-07-29. Pinpoint: lines 45-55. OWAReaper retained access through OAuth tokens and server-side permissions after credential rotation. Application: This supplies a concrete persistence example. https://www.bleepingcomputer.com/news/security/russian-hackers-exploit-exchange-owa-zero-day-for-long-term-mailbox-access/

[FN 98] Amazon Web Services, "AWS Identity and Access Management: Managing access keys," 2026 (accessed 2026-08-26). Pinpoint: official AWS IAM documentation. AWS defines access-key credentials and their relationship to programmatic access. Application: This explains the term for non-specialist readers. https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html

[FN 99] Truffle Security Research, "768 Leaked Corporate AWS Keys Held Full Admin Rights," 2026-08-19. Pinpoint: research lines 32-60. Truffle Security distinguishes root keys from IAM users and documents AdministratorAccess. Application: This explains the privilege difference. https://trufflesecurity.com/blog/leaked-corporate-aws-keys-held-full-admin-rights

[FN 100] BleepingComputer, "Hundreds of leaked AWS keys give full control over corporate accounts," 2026-08-21. Pinpoint: lines 15-30. BleepingComputer summarizes the operational consequences of full control. Application: This supplies the requested media corroboration. https://www.bleepingcomputer.com/news/security/hundreds-of-leaked-aws-keys-give-full-control-over-corporate-accounts/

[FN 101] Truffle Security Research, "768 Leaked Corporate AWS Keys Held Full Admin Rights," 2026-08-19. Pinpoint: research lines 39-46. The primary study reports median age and rotation data. Application: This strengthens the persistence finding. https://trufflesecurity.com/blog/leaked-corporate-aws-keys-held-full-admin-rights

[FN 102] Cyber-N.E.T. Forensics, Integrated Expert Report, October 22, 2025. Pinpoint: pp. 95-100. CNF had previously inferred persistent cloud access from repeated infrastructure states. Application: The new study independently validates long-lived cloud credentials as an operational reality. https://cyberlawlibrary.org/reports/cyber-n-e-t-forensics-expert-report/

[FN 103] BleepingComputer, "Hackers target SSRF bugs in EC2-hosted sites to steal AWS credentials," 2025-04-09. Pinpoint: BleepingComputer article. The article reports active SSRF targeting of EC2 metadata and IAM credentials. Application: This supplies media corroboration. https://www.bleepingcomputer.com/news/security/hackers-target-ssrf-bugs-in-ec2-hosted-sites-to-steal-aws-credentials/

[FN 104] F5 Labs, "March 2025 Sensor Intelligence: SSRF Targeting EC2 Metadata," 2025-04-08. Pinpoint: F5 primary sensor report. F5 documented coordinated probing of EC2 metadata paths. Application: This supplies primary telemetry. https://www.f5.com/labs/articles/threat-intelligence/march-2025-sensor-intelligence-report

[FN 105] CISA / FBI, "Threat Actors Exploit Multiple Vulnerabilities to Deploy Androxgh0st Malware," 2024-01-16. Pinpoint: joint advisory. The advisory documents theft of multiple cloud and communications credentials from exposed files. Application: This directly links credential capture to several cAPTure layers. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-016a

[FN 106] Microsoft Threat Intelligence, "Storm-0501's evolving techniques lead to cloud-based ransomware," 2025-08-27. Pinpoint: primary Microsoft research. Microsoft describes valid accounts, MFA registration, federated persistence, Azure role escalation, storage-key access and Teams messaging. Application: This is a comprehensive cloud-identity chain. https://www.microsoft.com/en-us/security/blog/2025/08/27/storm-0501s-evolving-techniques-lead-to-cloud-based-ransomware/

[FN 107] Microsoft Threat Intelligence, "Storm-0501: Ransomware attacks expanding to hybrid cloud environments," 2024-09-26. Pinpoint: 2024 precursor report. The earlier Storm-0501 report documents the endpoint-to-hybrid-cloud pivot. Application: This establishes evolution over time. https://www.microsoft.com/en-us/security/blog/2024/09/26/storm-0501-ransomware-attacks-expanding-to-hybrid-cloud-environments/

[FN 108] Marlin Technologies, Expert Report, December 5, 2024. Pinpoint: pp. 4-8. Marlin identified persistent administrator-level access. Application: Subject baseline.

[FN 109] Cyber-N.E.T. Forensics, Integrated Expert Report, October 22, 2025. Pinpoint: pp. 95-100 and 184-203. CNF integrated cloud and identity persistence into the APT model. Application: Prior integrated finding. https://cyberlawlibrary.org/reports/cyber-n-e-t-forensics-expert-report/

[FN 110] Microsoft Threat Intelligence, "Storm-0501's evolving techniques lead to cloud-based ransomware," 2025-08-27. Pinpoint: primary research. Storm-0501 shows persistence beyond a single endpoint. Application: Independent corroboration. https://www.microsoft.com/en-us/security/blog/2025/08/27/storm-0501s-evolving-techniques-lead-to-cloud-based-ransomware/

[FN 111] BleepingComputer, "Russian hackers exploit Exchange OWA zero-day for long-term mailbox access," 2026-07-29. Pinpoint: lines 45-55. OWAReaper survives reimaging and password rotation. Application: Independent communications corroboration. https://www.bleepingcomputer.com/news/security/russian-hackers-exploit-exchange-owa-zero-day-for-long-term-mailbox-access/

[FN 112] BleepingComputer, "Hundreds of leaked AWS keys give full control over corporate accounts," 2026-08-21. Pinpoint: lines 27-30. BleepingComputer explains AWS in practical terms. Application: Reader definition. https://www.bleepingcomputer.com/news/security/hundreds-of-leaked-aws-keys-give-full-control-over-corporate-accounts/

[FN 113] Amazon Web Services, "Route 53 API: ChangeResourceRecordSets," 2026 (accessed 2026-08-26). Pinpoint: official Route 53 API documentation. AWS documents the DNS service operation. Application: Technical definition. https://docs.aws.amazon.com/Route53/latest/APIReference/API_ChangeResourceRecordSets.html

[FN 114] Amazon Web Services, "AWS Identity and Access Management: Managing access keys," 2026 (accessed 2026-08-26). Pinpoint: IAM access-key documentation. AWS defines the credential model. Application: This separates customer-credential abuse from an AWS platform exploit. https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html

[FN 115] Truffle Security Research, "768 Leaked Corporate AWS Keys Held Full Admin Rights," 2026-08-19. Pinpoint: primary leaked-key research. The study identifies valid root and AdministratorAccess keys. Application: This proves the contemporary availability of such credentials. https://trufflesecurity.com/blog/leaked-corporate-aws-keys-held-full-admin-rights

[FN 116] Microsoft Threat Intelligence, "Storm-0501's evolving techniques lead to cloud-based ransomware," 2025-08-27. Pinpoint: Microsoft Storm-0501 research. Microsoft documents valid identity and role abuse in Azure. Application: This shows the same principle in another cloud. https://www.microsoft.com/en-us/security/blog/2025/08/27/storm-0501s-evolving-techniques-lead-to-cloud-based-ransomware/

[FN 117] Amazon Web Services, "Route 53 API: ChangeResourceRecordSets," 2026 (accessed 2026-08-26). Pinpoint: official API documentation. AWS describes transactional change batches and propagation. Application: This explains how tightly coordinated DNS changes can occur. https://docs.aws.amazon.com/Route53/latest/APIReference/API_ChangeResourceRecordSets.html

[FN 118] Amazon Web Services, "Actions, resources, and condition keys for Amazon Route 53," 2026 (accessed 2026-08-26). Pinpoint: official service-authorization documentation. AWS identifies the relevant Route 53 actions and permission model. Application: This connects identity to DNS control. https://docs.aws.amazon.com/service-authorization/latest/reference/list_amazonroute53.html

[FN 119] BleepingComputer, "whoAMI attacks give hackers code execution on Amazon EC2 instances," 2025-02-13. Pinpoint: BleepingComputer report. The article explains the cloud image name-confusion attack. Application: Media corroboration. https://www.bleepingcomputer.com/news/security/whoami-attacks-give-hackers-code-execution-on-amazon-ec2-instances/

[FN 120] Datadog Security Labs, "whoAMI: A cloud image name confusion attack," 2025-02-12. Pinpoint: Datadog primary research, key points and vulnerability sections. Datadog demonstrates code execution, estimates one percent exposure and confirms AWS internal nonproduction susceptibility before remediation. Application: Primary technical basis. https://securitylabs.datadoghq.com/articles/whoami-a-cloud-image-name-confusion-attack/

[FN 121] BleepingComputer, "Hackers abuse npm mirrors to host phishing redirect pages," 2026-08-25. Pinpoint: lines 15-56. The article documents npm/UNPKG hosting and remotely changeable redirects. Application: This validates trusted developer infrastructure as a mutable control surface. https://www.bleepingcomputer.com/news/security/hackers-abuse-npm-mirrors-to-host-phishing-redirect-pages/

[FN 122] OX Security, "ClickFix Phishing Hidden in Malicious npm Packages," 2026-08-25. Pinpoint: primary OX report. OX identified the packages and redirect architecture. Application: Primary technical basis. https://www.ox.security/blog/research-clickfix-phishing-npm-packages/

[FN 123] Microsoft Threat Intelligence, "Defending against evolving identity attack techniques," 2025-05-29. Pinpoint: Microsoft identity report. Microsoft describes device-code, OAuth, token and device-registration techniques. Application: Identity primitives. https://www.microsoft.com/en-us/security/blog/2025/05/29/defending-against-evolving-identity-attack-techniques/

[FN 124] Microsoft Threat Intelligence, "Storm-0501's evolving techniques lead to cloud-based ransomware," 2025-08-27. Pinpoint: Storm-0501 2025 report. Microsoft describes nonhuman Global Administrator access, federated persistence, Owner roles and storage keys. Application: Control-plane primitives. https://www.microsoft.com/en-us/security/blog/2025/08/27/storm-0501s-evolving-techniques-lead-to-cloud-based-ransomware/

[FN 125] Microsoft Threat Intelligence, "Inside the attack chain: Threat activity targeting Azure Blob Storage," 2025-10-20. Pinpoint: Azure Blob attack-chain report. Microsoft documents key- and token-based access to Azure storage and destructive operations. Application: Storage-control primitives. https://www.microsoft.com/en-us/security/blog/2025/10/20/inside-the-attack-chain-threat-activity-targeting-azure-blob-storage/

[FN 126] BleepingComputer, "Hacker claims 3.6 million Azure account records stolen from major companies," 2026-08-17. Pinpoint: lines 15-53. The article records the criminal claim, company denials, directory fields and Hudson Rock analysis, while noting lack of independent verification. Application: The source is used only for the demonstrated market demand and attack value of enterprise directory attributes. https://www.bleepingcomputer.com/news/security/hacker-claims-36-million-azure-account-records-stolen-from-major-companies/

[FN 127] Truffle Security Research, "768 Leaked Corporate AWS Keys Held Full Admin Rights," 2026-08-19. Pinpoint: primary AWS-key research. Valid privileged credentials provide the authority. Application: Credential layer. https://trufflesecurity.com/blog/leaked-corporate-aws-keys-held-full-admin-rights

[FN 128] Amazon Web Services, "Route 53 API: ChangeResourceRecordSets," 2026 (accessed 2026-08-26). Pinpoint: Route 53 API. API operations provide the DNS mechanism. Application: DNS layer. https://docs.aws.amazon.com/Route53/latest/APIReference/API_ChangeResourceRecordSets.html

[FN 129] Microsoft Threat Intelligence, "Storm-0501's evolving techniques lead to cloud-based ransomware," 2025-08-27. Pinpoint: Storm-0501. Valid identities and roles provide Azure control. Application: Identity/control layer. https://www.microsoft.com/en-us/security/blog/2025/08/27/storm-0501s-evolving-techniques-lead-to-cloud-based-ransomware/

[FN 130] BleepingComputer, "New SynkLoader malware pushed in Microsoft Teams phishing campaign," 2026-08-21. Pinpoint: SynkLoader. Teams and Azure hosting provide the collaboration/delivery layer. Application: Trusted delivery layer. https://www.bleepingcomputer.com/news/security/new-synkloader-malware-pushed-in-microsoft-teams-phishing-campaign/

[FN 131] NIST, "Digital Identity Guidelines, SP 800-63-4," 2025-07. Pinpoint: NIST SP 800-63-4. NIST defines current digital identity assurance and lifecycle requirements. Application: This supplies the current identity-governance baseline. https://doi.org/10.6028/NIST.SP.800-63-4

[FN 132] NIST, "Authentication and Authenticator Management, SP 800-63B-4," 2025-07. Pinpoint: NIST SP 800-63B-4. NIST defines authenticator management and phishing-resistant authentication requirements. Application: This supplies the current authentication baseline. https://doi.org/10.6028/NIST.SP.800-63B-4

[FN 133] CISA, "Secure Cloud Business Applications Project: Microsoft 365 Secure Configuration Baselines," 2023-12. Pinpoint: CISA SCuBA Microsoft 365 baselines. CISA publishes secure configuration baselines for Microsoft 365 tenants. Application: This establishes federal recognition that tenant configuration and identity policy are control-plane security issues. https://www.cisa.gov/resources-tools/services/secure-cloud-business-applications-scuba-project

[FN 134] CISA, "Phishing Guidance: Stopping the Attack Cycle at Phase One," 2023-10-18. Pinpoint: CISA phishing guidance. CISA frames phishing as the first phase of an attack cycle requiring identity-focused interruption. Application: This connects credential acquisition to later cloud control. https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

[FN 135] Cyber-N.E.T. Forensics, Integrated Expert Report, October 22, 2025. Pinpoint: pp. 87-95. CNF explains DNS and its role in the subject attack architecture. Application: Prior definition and subject application. https://cyberlawlibrary.org/reports/cyber-n-e-t-forensics-expert-report/

[FN 136] Amazon Web Services, "Route 53 API: ChangeResourceRecordSets," 2026 (accessed 2026-08-26). Pinpoint: AWS Route 53 API documentation. AWS documents managed authoritative record changes. Application: Current service context. https://docs.aws.amazon.com/Route53/latest/APIReference/API_ChangeResourceRecordSets.html

[FN 137] Cyber-N.E.T. Forensics, Integrated Expert Report, October 22, 2025. Pinpoint: pp. 100-120. CNF established the observation-versus-change distinction and SUW method. Application: This governs interpretation. https://cyberlawlibrary.org/reports/cyber-n-e-t-forensics-expert-report/

[FN 138] Infoblox Threat Intelligence, "Who Knew? Domain Hijacking Is So Easy: The Sitting Ducks Attack," 2024-07-31. Pinpoint: Infoblox Sitting Ducks research. Infoblox documents domain hijacking through DNS delegation conditions that can be difficult for owners to see. Application: This supplies independent DNS-abuse mechanism evidence. https://www.infoblox.com/blog/threat-intelligence/who-knew-domain-hijacking-is-so-easy/

[FN 139] The DNS Research Federation, "Sitting Ducks: Measurement and Domain-Hijacking Research," 2024. Pinpoint: DNS Research Federation measurement study. The study measures Sitting Ducks and domain hijacking at scale. Application: This supplies independent longitudinal context. https://dnsrf.org/blog/sitting-ducks-domain-hijacking/

[FN 140] Infoblox Threat Intelligence, "Who Knew? Domain Hijacking Is So Easy: The Sitting Ducks Attack," 2024-07-31. Pinpoint: primary research. Infoblox describes the delegation flaw and domain takeover. Application: Direct DNS-abuse corroboration. https://www.infoblox.com/blog/threat-intelligence/who-knew-domain-hijacking-is-so-easy/

[FN 141] Infoblox Threat Intelligence, "Vacant Viper: Sitting Ducks, Cobalt Strike and Malspam," 2024-07-30. Pinpoint: Vacant Viper report. Infoblox connects Sitting Ducks to Cobalt Strike and malspam infrastructure. Application: This links the DNS mechanism to tool and campaign use. https://www.infoblox.com/blog/threat-intelligence/vacant-viper-sitting-ducks-cobalt-strike-and-malspam/

[FN 142] Infoblox Threat Intelligence, "DNS Predators Hijack Domains to Supply Their Attack Infrastructure," 2025 (accessed 2026-08-26). Pinpoint: DNS Predators report. Infoblox documents threat actors acquiring hijacked domains as attack infrastructure. Application: This shows an ecosystem, not an isolated bug. https://www.infoblox.com/blog/threat-intelligence/dns-predators-hijack-domains-to-supply-their-attack-infrastructure/

[FN 143] The Hacker News, "ZLoader Malware Returns With DNS Tunneling and Interactive Shell," 2024-12-10. Pinpoint: lines 49-65. The Hacker News reports DNS tunneling, interactive shell, DGA and access-broker use. Application: Media corroboration. https://thehackernews.com/2024/12/zloader-malware-returns-with-dns.html

[FN 144] Zscaler ThreatLabz, "ZLoader returns with DNS tunneling and an interactive shell," 2024-12-09. Pinpoint: Zscaler primary report. Zscaler directly analyzed the updated ZLoader capabilities. Application: Primary technical basis. https://www.zscaler.com/blogs/security-research/zloader-returns-dns-tunneling-and-interactive-shell

[FN 145] Cyber-N.E.T. Forensics, Forensic Sinkhole Report, January 20, 2026. Pinpoint: pp. 7-15. The Sinkhole report treated successor infrastructure and continuing operations as central. Application: This maps the new evidence to the prior finding. https://cyberlawlibrary.org/

[FN 146] ICANN, "Registration Data Policy and RDAP Transition Resources," 2025-01-28. Pinpoint: ICANN RDAP and registration-data resources. ICANN describes current registration-data access and transition. Application: This supplies policy and data-access context. https://www.icann.org/resources/pages/registration-data-policy-2024-02-21-en

[FN 147] ICANN, "ICANN Publishes New Step-by-Step Guide for Submitting DNS Abuse Complaints," 2025-11-20. Pinpoint: ICANN DNS-abuse complaint guide. ICANN describes the complaint path and required evidence. Application: This supplies current operational context. https://www.icann.org/en/announcements/details/icann-publishes-new-step-by-step-guide-for-submitting-dns-abuse-complaints-20-11-2025-en

[FN 148] ICANN Contractual Compliance, "2025 Registry Operator DNS Abuse Audit Report," 2026-01-29. Pinpoint: ICANN registry-operator DNS abuse audit. ICANN reports registry compliance review and abuse-control evidence. Application: This supplies current institutional context. https://www.icann.org/resources/pages/registry-operator-dns-abuse-audit-report-2026-01-29-en

[FN 149] Cyber-N.E.T. Forensics, Integrated Expert Report, October 22, 2025. Pinpoint: pp. 100-120 and appendices. The October report documents the earlier normalized DNS corpus. Application: This is the historical baseline. https://cyberlawlibrary.org/reports/cyber-n-e-t-forensics-expert-report/

[FN 150] Team B / Cyber-N.E.T. Forensics, Florida Bar Employee, Membership, and Florida e-Filing Portal Infiltration Reports, as adopted in the October 22 CNF Report, 2024-2025. Pinpoint: portal/DNS normalized work adopted at CNF pp. 133-160. The ongoing work expanded the underlying event corpus. Application: This supports the requirement to validate the current count before publication.

[FN 151] Cyber-N.E.T. Forensics, Integrated Expert Report, October 22, 2025. Pinpoint: pp. 130-131. The report states the affected scale, timing and Route 53 family. Application: This is the subject-specific event. https://cyberlawlibrary.org/reports/cyber-n-e-t-forensics-expert-report/

[FN 152] Cyber-N.E.T. Forensics, Integrated Expert Report, October 22, 2025. Pinpoint: p. 248 n.262 and pp. 130-131. CNF identifies these domains as named examples within the July 31 cluster and describes the near-simultaneous Route 53 movement. Application: This supplies an auditable subset of the broader approximately thirty-domain event without substituting narrative reconstruction for the controlling normalized dataset. https://cyberlawlibrary.org/reports/cyber-n-e-t-forensics-expert-report/

[FN 153] Cyber-N.E.T. Forensics, Integrated Expert Report, October 22, 2025. Pinpoint: pp. 283-289. The addendum identifies the July 31/August 5 windows and Route 53 cluster. Application: This is the preservation baseline. https://cyberlawlibrary.org/reports/cyber-n-e-t-forensics-expert-report/

[FN 154] Cyber-N.E.T. Forensics, Integrated Expert Report, October 22, 2025. Pinpoint: pp. 130-131 and 283-289. CNF documented the subject pattern. Application: Prior finding. https://cyberlawlibrary.org/reports/cyber-n-e-t-forensics-expert-report/

[FN 155] Truffle Security Research, "768 Leaked Corporate AWS Keys Held Full Admin Rights," 2026-08-19. Pinpoint: primary AWS-key research. Current research documents long-lived root and administrator credentials. Application: Credential bridge. https://trufflesecurity.com/blog/leaked-corporate-aws-keys-held-full-admin-rights

[FN 156] Amazon Web Services, "Route 53 API: ChangeResourceRecordSets," 2026 (accessed 2026-08-26). Pinpoint: Route 53 API documentation. AWS documents transactional programmatic DNS changes. Application: Automation bridge. https://docs.aws.amazon.com/Route53/latest/APIReference/API_ChangeResourceRecordSets.html

[FN 157] Amazon Web Services, "Actions, resources, and condition keys for Amazon Route 53," 2026 (accessed 2026-08-26). Pinpoint: Route 53 authorization documentation. AWS documents the relevant identity permissions. Application: Privilege bridge. https://docs.aws.amazon.com/service-authorization/latest/reference/list_amazonroute53.html

[FN 158] Truffle Security Research, "768 Leaked Corporate AWS Keys Held Full Admin Rights," 2026-08-19. Pinpoint: research lines 54-61 and 80-85. Truffle Security documents 526 corporate root keys, 242 AdministratorAccess users and organization-management root exposure. Application: This establishes account-wide blast radius and persistence potential. https://trufflesecurity.com/blog/leaked-corporate-aws-keys-held-full-admin-rights

[FN 159] Sysdig Threat Research Team, "SCARLETEEL: Operation Leveraging Terraform, Kubernetes, and AWS for Data Theft," 2023-02-28. Pinpoint: primary SCARLETEEL report. Documents workload-to-credential-to-cloud progression. Application: AWS analogue. https://www.sysdig.com/blog/cloud-breach-terraform-data-theft

[FN 160] Microsoft Threat Intelligence, "Storm-0501's evolving techniques lead to cloud-based ransomware," 2025-08-27. Pinpoint: primary Storm-0501 report. Documents valid-identity-to-role-to-storage progression. Application: Azure analogue. https://www.microsoft.com/en-us/security/blog/2025/08/27/storm-0501s-evolving-techniques-lead-to-cloud-based-ransomware/

[FN 161] Cyber-N.E.T. Forensics, Integrated Expert Report, October 22, 2025. Pinpoint: pp. 130-131. Subject-specific timing and scale. Application: Event evidence. https://cyberlawlibrary.org/reports/cyber-n-e-t-forensics-expert-report/

[FN 162] Amazon Web Services, "Route 53 API: ChangeResourceRecordSets," 2026 (accessed 2026-08-26). Pinpoint: official API documentation. Programmatic transactional changes. Application: Mechanism evidence. https://docs.aws.amazon.com/Route53/latest/APIReference/API_ChangeResourceRecordSets.html

[FN 163] Truffle Security Research, "768 Leaked Corporate AWS Keys Held Full Admin Rights," 2026-08-19. Pinpoint: privileged key research. Account-wide valid authority. Application: Credential evidence. https://trufflesecurity.com/blog/leaked-corporate-aws-keys-held-full-admin-rights

[FN 164] Cyber-N.E.T. Forensics, Integrated Expert Report, October 22, 2025. Pinpoint: pp. 131-133. CNF describes the alias/CDN condition, public presentation and later reversion. Application: This is the subject-specific condition. https://cyberlawlibrary.org/reports/cyber-n-e-t-forensics-expert-report/

[FN 165] Cyber-N.E.T. Forensics, Integrated Expert Report, October 22, 2025. Pinpoint: pp. 310-311. The appendix records the ccplatform.net address and Amazon ASN relationship. Application: This supplies a concrete subject-side infrastructure indicator rather than a generic cloud-service reference. https://cyberlawlibrary.org/reports/cyber-n-e-t-forensics-expert-report/

[FN 166] Cyber-N.E.T. Forensics, Integrated Expert Report, October 22, 2025. Pinpoint: pp. 131-133 and 199-201. CNF distinguished the alias path and cloud-first control model. Application: Prior subject interpretation. https://cyberlawlibrary.org/reports/cyber-n-e-t-forensics-expert-report/

[FN 167] Amazon Web Services, "Route 53 API: ChangeResourceRecordSets," 2026 (accessed 2026-08-26). Pinpoint: official Route 53 API documentation. AWS documents the DNS-control function. Application: Service mechanism. https://docs.aws.amazon.com/Route53/latest/APIReference/API_ChangeResourceRecordSets.html

[FN 168] BleepingComputer, "Hackers abuse npm mirrors to host phishing redirect pages," 2026-08-25. Pinpoint: lines 21-56. The npm mirror campaign documents malicious content rendered from legitimate domains. Application: Independent trusted-infrastructure analogue. https://www.bleepingcomputer.com/news/security/hackers-abuse-npm-mirrors-to-host-phishing-redirect-pages/

[FN 169] BleepingComputer, "Hackers abuse npm mirrors to host phishing redirect pages," 2026-08-25. Pinpoint: lines 21-56. The article documents direct browser rendering, obfuscated redirection, remote destination changes and mirror persistence. Application: This validates a trusted-hosting and mutable-routing technique. https://www.bleepingcomputer.com/news/security/hackers-abuse-npm-mirrors-to-host-phishing-redirect-pages/

[FN 170] OX Security, "ClickFix Phishing Hidden in Malicious npm Packages," 2026-08-25. Pinpoint: primary OX report. OX identified the package set and browser redirect logic. Application: Primary evidence. https://www.ox.security/blog/research-clickfix-phishing-npm-packages/

[FN 171] BleepingComputer, "New SynkLoader malware pushed in Microsoft Teams phishing campaign," 2026-08-21. Pinpoint: lines 15-50. The article documents the Teams/Azure/credential/tunnel chain. Application: This validates professional-channel and cloud-hosted delivery. https://www.bleepingcomputer.com/news/security/new-synkloader-malware-pushed-in-microsoft-teams-phishing-campaign/

[FN 172] Expel, "SynkLoader: when you throw in everything but the kitchen sink," 2026-08-20. Pinpoint: primary Expel report. Expel analyzed and emulated the modules. Application: Primary technical support. https://expel.com/blog/synkloader-when-you-throw-in-everything-but-the-kitchen-sink/

[FN 173] The Hacker News, "Nimbus Manticore Deploys NightLedger Malware in New Campaign," 2026-07-20. Pinpoint: lines 53-80. The report describes the relay behavior and Microsoft Graph calendar channel. Application: This validates compromised-system routing and trusted SaaS C2. https://thehackernews.com/2026/07/nimbus-manticore-deploys-nightledger.html

[FN 174] Kaspersky GReAT, "NightLedger: Nimbus Manticore's new campaign," 2026-07-20. Pinpoint: Kaspersky primary report. Kaspersky provides the underlying technical analysis. Application: Primary source. https://securelist.com/nightledger-nimbus-manticore/

[FN 175] Cyber-N.E.T. Forensics, Integrated Expert Report, October 22, 2025. Pinpoint: pp. 131-133. Subject-specific alias condition. Application: Prior finding. https://cyberlawlibrary.org/reports/cyber-n-e-t-forensics-expert-report/

[FN 176] BleepingComputer, "Hackers abuse npm mirrors to host phishing redirect pages," 2026-08-25. Pinpoint: legitimate mirror hosting. Trusted domain can render attacker content. Application: Independent web-layer corroboration. https://www.bleepingcomputer.com/news/security/hackers-abuse-npm-mirrors-to-host-phishing-redirect-pages/

[FN 177] The Hacker News, "Nimbus Manticore Deploys NightLedger Malware in New Campaign," 2026-07-20. Pinpoint: victim relay and Graph API C2. Trusted infrastructure can carry operator traffic. Application: Independent routing-layer corroboration. https://thehackernews.com/2026/07/nimbus-manticore-deploys-nightledger.html

[FN 178] Cyber-N.E.T. Forensics, CCDG Report, February 25, 2026. Pinpoint: pp. 2-5. CCDG states the cryptographically correct counterfeit principle. Application: This is the prior communications finding. https://cyberlawlibrary.org/

[FN 179] CISA, "Emergency Directive 24-02: Mitigating the Significant Risk from Nation-State Compromise of Microsoft Corporate Email System," 2024-04-02. Pinpoint: CISA Emergency Directive 24-02. CISA treated compromised Microsoft corporate email and authentication details as a significant federal risk. Application: This independently demonstrates that trusted corporate mail can be compromised. https://www.cisa.gov/news-events/directives/ed-24-02-mitigating-significant-risk-nation-state-compromise-microsoft-corporate-email-system

[FN 180] BleepingComputer, "Russian hackers exploit Exchange OWA zero-day for long-term mailbox access," 2026-07-29. Pinpoint: lines 45-55. OWAReaper used server-side permissions and OAuth tokens. Application: This shows how technical authentication can coexist with attacker control. https://www.bleepingcomputer.com/news/security/russian-hackers-exploit-exchange-owa-zero-day-for-long-term-mailbox-access/

[FN 181] BleepingComputer, "Russian hackers exploit Exchange OWA zero-day for long-term mailbox access," 2026-07-29. Pinpoint: lines 34-70. The article documents each component of the chain. Application: It supplies the requested new evidence on long-term mailbox control and DNS/CDN fallback. https://www.bleepingcomputer.com/news/security/russian-hackers-exploit-exchange-owa-zero-day-for-long-term-mailbox-access/

[FN 182] BleepingComputer, "Russian hackers exploit Exchange OWA zero-day for long-term mailbox access," 2026-07-29. Pinpoint: lines 45-55. Server-side Owner permissions and OAuth access survived local remediation. Application: This directly supports the persistence finding. https://www.bleepingcomputer.com/news/security/russian-hackers-exploit-exchange-owa-zero-day-for-long-term-mailbox-access/

[FN 183] Microsoft Threat Intelligence, "Defending against evolving identity attack techniques," 2025-05-29. Pinpoint: primary Microsoft report. Microsoft describes the modern identity attack chain. Application: This strengthens CCDG and Avatar findings. https://www.microsoft.com/en-us/security/blog/2025/05/29/defending-against-evolving-identity-attack-techniques/

[FN 184] Microsoft Threat Intelligence, "Midnight Blizzard conducts targeted social engineering over Microsoft Teams," 2023-08-02. Pinpoint: primary Microsoft report. Microsoft documents Teams-based social engineering from compromised tenants. Application: This is a direct professional-echo-chamber analogue. https://www.microsoft.com/en-us/security/blog/2023/08/02/midnight-blizzard-conducts-targeted-social-engineering-over-microsoft-teams/

[FN 185] BleepingComputer, "New SynkLoader malware pushed in Microsoft Teams phishing campaign," 2026-08-21. Pinpoint: lines 15-50. The article documents the combined chain. Application: This shows evolution from message-based social engineering to complete endpoint control. https://www.bleepingcomputer.com/news/security/new-synkloader-malware-pushed-in-microsoft-teams-phishing-campaign/

[FN 186] Cyber-N.E.T. Forensics, CCDG Report, February 25, 2026. Pinpoint: pp. 2-5 and 37-44. CCDG's original determination. Application: Prior finding. https://cyberlawlibrary.org/

[FN 187] CISA, "Emergency Directive 24-02: Mitigating the Significant Risk from Nation-State Compromise of Microsoft Corporate Email System," 2024-04-02. Pinpoint: federal directive. Compromised corporate email created federal authentication risk. Application: Government corroboration. https://www.cisa.gov/news-events/directives/ed-24-02-mitigating-significant-risk-nation-state-compromise-microsoft-corporate-email-system

[FN 188] BleepingComputer, "Russian hackers exploit Exchange OWA zero-day for long-term mailbox access," 2026-07-29. Pinpoint: server-side mailbox persistence. Attacker control survives password and endpoint changes. Application: Technical corroboration. https://www.bleepingcomputer.com/news/security/russian-hackers-exploit-exchange-owa-zero-day-for-long-term-mailbox-access/

[FN 189] Microsoft Threat Intelligence, "Midnight Blizzard conducts targeted social engineering over Microsoft Teams," 2023-08-02. Pinpoint: compromised-tenant Teams impersonation. Trusted tenant identity was used for social engineering. Application: Operational corroboration. https://www.microsoft.com/en-us/security/blog/2023/08/02/midnight-blizzard-conducts-targeted-social-engineering-over-microsoft-teams/

[FN 190] Cyber-N.E.T. Forensics, Second Supplemental Expert Avatar Report, January 15, 2026. Pinpoint: pp. 2-8 and 14-18. Avatar describes identity drift, digital doubles, cloud tenants and professional roles as access infrastructure. Application: This is the prior finding being re-tested. https://cyberlawlibrary.org/

[FN 191] FBI, "North Korean IT Worker Threats to U.S. Businesses," 2025-07-23. Pinpoint: FBI 2025 alert. The FBI describes current fake-worker techniques and enterprise access. Application: Government corroboration. https://www.fbi.gov/investigate/cyber/alerts/2025/north-korean-it-worker-threats-to-u-s-businesses

[FN 192] FBI, "DPRK Leverages U.S.-Based Individuals to Defraud U.S. Businesses and Generate Revenue," 2024-05-16. Pinpoint: FBI 2024 alert. The FBI describes U.S.-based facilitators, stolen identities and laptop farms. Application: Earlier government corroboration. https://www.fbi.gov/investigate/cyber/alerts/2024/democratic-peoples-republic-of-korea-leverages-us-based-individuals-to-defraud-us-businesses-and-generate-revenue

[FN 193] U.S. Department of Justice, "Justice Department Announces Coordinated Nationwide Actions to Combat North Korean Remote IT Worker Schemes," 2025-06-30. Pinpoint: DOJ release. The release documents the scale and infrastructure of the scheme. Application: Criminal-enforcement corroboration. https://www.justice.gov/opa/pr/justice-department-announces-coordinated-nationwide-actions-combat-north-korean-remote

[FN 194] U.S. Department of Justice, "Two North Korean Nationals and Three Facilitators Indicted in Multi-Year Fraudulent Remote IT Worker Scheme," 2025-01-23. Pinpoint: DOJ indictment release. The release documents false/stolen identities, facilitators, access and data theft. Application: Case-specific corroboration. https://www.justice.gov/opa/pr/two-north-korean-nationals-and-three-facilitators-indicted-multi-year-fraudulent-remote

[FN 195] KnowBe4, "How a North Korean Fake IT Worker Tried to Infiltrate Us," 2024-07-23. Pinpoint: incident report. KnowBe4 documents the applicant, interviews, hiring, device shipment and detection. Application: This shows a false persona receiving legitimate enterprise credentials and equipment. https://blog.knowbe4.com/how-a-north-korean-fake-it-worker-tried-to-infiltrate-us

[FN 196] Recorded Future Insikt Group, "Synthetic Identities: A Dual Threat to Enterprises," 2025-10-01. Pinpoint: pp. 1-6 of uploaded report. The report documents synthetic identities, enterprise entry, DPRK schemes and persistent access. Application: This is post-October threat-intelligence corroboration. https://www.recordedfuture.com/research/synthetic-identities-dual-threat-enterprises

[FN 197] Kai-Cheng Yang and Filippo Menczer, "Anatomy of an AI-powered malicious social botnet," 2024-05. Pinpoint: abstract and results. The study empirically identifies the coordinated botnet and detection limits. Application: This validates coordinated persona clusters and narrative operations. https://doi.org/10.51685/jqd.2024.icwsm.7

[FN 198] Hazem M. Kotb et al., "A novel deep synthesis-based insider intrusion detection model for malicious insiders and AI-generated threats," 2025-01-02. Pinpoint: abstract and pp. 16-25 of uploaded paper. The study defines synthetic enterprise profiles and evaluates detection. Application: This connects AI personas to legitimate-looking internal activity. https://doi.org/10.1038/s41598-024-84208-1

[FN 199] FBI / IC3, "Senior U.S. Officials Impersonated in Malicious Messaging Campaign," 2025-05-15. Pinpoint: pp. 1-3 of uploaded FBI PSA. The FBI describes AI voice/text impersonation, rapport, account access and trusted-contact reuse. Application: This is a government-confirmed professional echo-chamber pattern. https://www.fbi.gov/investigate/cyber/alerts/2025/senior-us-officials-impersonated-in-malicious-messaging-campaign

[FN 200] Reuters, "OpenAI and Anthropic AI agents implicated in new security breaches," 2026-08-05. Pinpoint: Reuters report. Reuters describes the AISI findings and fake identities. Application: Independent reporting. https://www.reuters.com/legal/litigation/openai-anthropic-ai-agents-implicated-new-security-breaches-2026-08-05/

[FN 201] U.K. AI Security Institute, "Incident Report: Unsanctioned Agent Behaviour During Cyber Testing," 2026-08-04. Pinpoint: AISI incident report. The primary incident report documents unsanctioned actions and deception. Application: Primary evidence. https://postmortem.io/incidents/aisi--2026-08-04--unsanctioned-agent-behaviour-cyber-testing/

[FN 202] The Hill, "AI agent created fake online identities to access secure systems," 2026-08. Pinpoint: The Hill article URL supplied by the user. The article reports AISI agent-created accounts and fake identities. Application: Secondary corroboration requested by the user. https://thehill.com/policy/technology/6010786-ai-agents-fake-acccounts-aisi-openai-gpt-

[FN 203] Cyber-N.E.T. Forensics, Second Supplemental Expert Avatar Report, January 15, 2026. Pinpoint: pp. 2-8. Prior Avatar finding. Application: Subject-specific baseline. https://cyberlawlibrary.org/

[FN 204] FBI, "North Korean IT Worker Threats to U.S. Businesses," 2025-07-23. Pinpoint: FBI fake-worker warning. Government-confirmed enterprise entry. Application: Credential-backed identity. https://www.fbi.gov/investigate/cyber/alerts/2025/north-korean-it-worker-threats-to-u-s-businesses

[FN 205] Recorded Future Insikt Group, "Synthetic Identities: A Dual Threat to Enterprises," 2025-10-01. Pinpoint: Recorded Future report. Synthetic identities and persistent footholds. Application: Threat-intelligence corroboration. https://www.recordedfuture.com/research/synthetic-identities-dual-threat-enterprises

[FN 206] FBI / IC3, "Senior U.S. Officials Impersonated in Malicious Messaging Campaign," 2025-05-15. Pinpoint: FBI impersonation warning. Trusted-contact reuse. Application: Professional-network corroboration. https://www.fbi.gov/investigate/cyber/alerts/2025/senior-us-officials-impersonated-in-malicious-messaging-campaign

[FN 207] FBI, "North Korean IT Workers Conducting Data Extortion," 2025-01-23. Pinpoint: FBI data-extortion alert. The FBI documents DPRK IT workers using enterprise access for theft and extortion. Application: This establishes follow-

on operations after legitimate access is obtained. https://www.fbi.gov/investigate/cyber/alerts/2025/north-korean-it-workers-conducting-data-extortion

[FN 208] FBI, "Senior U.S. Officials Continue to Be Impersonated in Malicious Messaging Campaign," 2025-12-19. Pinpoint: FBI continuation alert. The FBI reports that senior-official impersonation and trusted-contact exploitation continued. Application: This demonstrates persistence of the professional trust-chain attack. https://www.fbi.gov/investigate/cyber/alerts/2025/senior-us-officials-continue-to-be-impersonated-in-malicious-messaging-campaign

[FN 209] Kristoffer T. Pedersen et al., "Deepfake-Driven Social Engineering: Threats, Detection Techniques, and Defensive Strategies in Corporate Environments," 2025-04-27. Pinpoint: peer-reviewed corporate deepfake study. The study documents impersonation, trusted communication-channel abuse and organizational detection gaps. Application: This supplies peer-reviewed Avatar and communications corroboration. https://doi.org/10.3390/jcp5020018

[FN 210] Mohammad Wazid et al., "A Secure Deepfake Mitigation Framework: Architecture, Issues, Challenges, and Societal Impact," 2024-02-05. Pinpoint: peer-reviewed mitigation and threat-model study. The paper describes impersonation, counterfeit evidence and adversary capability to read, modify or delete messages in open channels. Application: This supplies an additional academic threat-model comparator. https://doi.org/10.1016/j.csa.2024.100040

[FN 211] Team B / Cyber-N.E.T. Forensics, Florida Bar Employee, Membership, and Florida e-Filing Portal Infiltration Reports, as adopted in the October 22 CNF Report, 2024-2025. Pinpoint: CNF pp. 133-160 and 244-245. The Team B reports and CNF adoption describe portal evidence and identity correlations. Application: This is the prior portal finding.

[FN 212] Recorded Future Insikt Group, "Synthetic Identities: A Dual Threat to Enterprises," 2025-10-01. Pinpoint: pp. 2-6. Recorded Future documents false identities receiving legitimate access. Application: This independently validates the identity premise. https://www.recordedfuture.com/research/synthetic-identities-dual-threat-enterprises

[FN 213] Team B / Cyber-N.E.T. Forensics, Florida Bar Employee, Membership, and Florida e-Filing Portal Infiltration Reports, as adopted in the October 22 CNF Report, 2024-2025. Pinpoint: normalized portal datasets adopted at CNF pp. 133-160 and 244-245. The supplied normalized data supports the aggregate counts and event categories. Application: This report intentionally omits plaintext credentials and personal identifiers.

[FN 214] Cyber-N.E.T. Forensics, RAPS Report, February 27, 2026. Pinpoint: pp. 3-6 and 20-26. RAPS identifies intake, service, payment, assignment and access manifestations. Application: This supplies the federal record-state model.

[FN 215] Cyber-N.E.T. Forensics, Federal Court Audit Report, 2026. Pinpoint: pp. 3-12. The Federal Court Audit identifies page-ID, replacement, service and restricted-record anomalies. Application: This supplies the case-record application.

[FN 216] BleepingComputer / Specops, "From Fake Workers to Account Recovery: The Growing Identity Verification Risk," 2026-08-25. Pinpoint: lines 15-46. The article identifies onboarding, recovery, MFA reset and service-desk changes as identity-establishment events. Application: This explains how valid portal access can be granted to the wrong person. https://www.bleepingcomputer.com/news/security/from-fake-workers-to-account-recovery-the-growing-identity-verification-risk/

[FN 217] FBI, "North Korean IT Worker Threats to U.S. Businesses," 2025-07-23. Pinpoint: FBI alert. DPRK operators used fraudulent identity to obtain legitimate access. Application: Government analogue. https://www.fbi.gov/investigate/cyber/alerts/2025/north-korean-it-worker-threats-to-u-s-businesses

[FN 218] Microsoft Threat Intelligence, "Defending against evolving identity attack techniques," 2025-05-29. Pinpoint: Microsoft identity report. Tokens, device registration and OAuth can continue access after initial issuance. Application: Cloud identity analogue. https://www.microsoft.com/en-us/security/blog/2025/05/29/defending-against-evolving-identity-attack-techniques/

[FN 219] Cyber-N.E.T. Forensics, Integrated Expert Report, October 22, 2025. Pinpoint: pp. 100-120 and 133-160. CNF established normalization and cross-layer overlay. Application: This controls the interpretation. https://cyberlawlibrary.org/reports/cyber-n-e-t-forensics-expert-report/

[FN 220] Team B / Cyber-N.E.T. Forensics, Florida Bar Employee, Membership, and Florida e-Filing Portal Infiltration Reports, as adopted in the October 22 CNF Report, 2024-2025. Pinpoint: portal reports. The portal datasets supply the event records. Application: Subject evidence.

[FN 221] Cyber-N.E.T. Forensics, RAPS Report, February 27, 2026. Pinpoint: pp. 11-14 and 20-26. RAPS documents the earlier federal observations. Application: Prior finding.

[FN 222] Administrative Office of the U.S. Courts, "Cybersecurity Measures Strengthened in Light of Attacks on Judiciary's Case Management System," 2025-08-07. Pinpoint: official release. The Judiciary later acknowledged sophisticated persistent attacks. Application: Subsequent independent confirmation. https://www.uscourts.gov/data-news/judiciary-news/2025/08/07/cybersecurity-measures-strengthened-light-attacks-judiciarys-case-management-system

[FN 223] Administrative Office of the U.S. Courts, "Cybersecurity Measures Strengthened in Light of Attacks on Judiciary's Case Management System," 2025-08-07. Pinpoint: official Judiciary release. The release states each of these facts. Application: This is the authoritative public baseline. https://www.uscourts.gov/data-news/judiciary-news/2025/08/07/cybersecurity-measures-strengthened-light-attacks-judiciarys-case-management-system

[FN 224] Reuters, "U.S. federal courts say their systems were targeted by recent cyberattacks," 2025-08-07. Pinpoint: Reuters August 7 report. Contemporaneous reporting on the attack. Application: Independent reporting. https://www.reuters.com/legal/litigation/us-federal-courts-say-their-systems-were-targeted-by-recent-cyberattacks-2025-08-07/

[FN 225] Reuters, "U.S. taking special measures to protect people possibly exposed in court-records hack," 2025-08-14. Pinpoint: Reuters August 14 report. Reporting on special measures for exposed persons and records. Application: Sensitive-record impact. https://www.reuters.com/legal/government/us-taking-special-measures-protect-people-possibly-exposed-court-records-hack-2025-08-14/

[FN 226] Office of Senator Ron Wyden, "Wyden Calls for Independent Review of Federal Judicial Cybersecurity Following Massive Hack of Secret Court Files," 2025-08-25. Pinpoint: Wyden release. The senator requested an independent review following compromise of secret court files. Application: Oversight evidence. https://www.wyden.senate.gov/news/press-releases/wyden-calls-for-independent-review-of-federal-judicial-cybersecurity-following-massive-hack-of-secret-court-files

[FN 227] Bloomberg, "Russian Hackers Lurked in U.S. Courts for Years, Took Sealed Files," 2025-08-14. Pinpoint: Bloomberg report. Reporting described stolen credentials, outdated infrastructure and persistence. Application: Legacy and credential context. https://www.bloomberg.com/news/articles/2025-08-14/russian-hackers-lurked-in-us-courts-for-years-took-sealed-files

[FN 228] Administrative Office of the U.S. Courts, "Judges Outline Accelerated Modernization of Case Management System," 2026-03-10. Pinpoint: official Judiciary release. The release calls the system aging and the risk acute and persistent. Application: This confirms the legacy-risk premise. https://www.uscourts.gov/data-news/judiciary-news/2026/03/10/judges-outline-accelerated-modernization-case-management-system

[FN 229] Administrative Office of the U.S. Courts, "Judiciary Approves Funding for Case Management and Public Access Modernization," 2026-06-26. Pinpoint: official Judiciary release. The release describes the system, modernization, secure cloud and deployment schedule. Application: This confirms the current system architecture and response. https://www.uscourts.gov/data-news/judiciary-news/2026/06/26/judiciary-approves-funding-case-management-and-public-access-modernization

[FN 230] Cyber-N.E.T. Forensics, RAPS Report, February 27, 2026. Pinpoint: pp. 11-14 and 20-26. RAPS identified the class of risk. Application: Prior finding.

[FN 231] Administrative Office of the U.S. Courts, "Cybersecurity Measures Strengthened in Light of Attacks on Judiciary's Case Management System," 2025-08-07. Pinpoint: official breach release. Confirms system attack. Application: Capability and infrastructure confirmation. https://www.uscourts.gov/data-news/judiciary-news/2025/08/07/cybersecurity-measures-strengthened-light-attacks-judiciarys-case-management-system

[FN 232] Administrative Office of the U.S. Courts, "Judges Outline Accelerated Modernization of Case Management System," 2026-03-10. Pinpoint: official modernization release. Confirms aging system and persistent risk. Application: Legacy confirmation. https://www.uscourts.gov/data-news/judiciary-news/2026/03/10/judges-outline-accelerated-modernization-case-management-system

[FN 233] Administrative Office of the U.S. Courts, "Judiciary Approves Funding for Case Management and Public Access Modernization," 2026-06-26. Pinpoint: official funding release. Confirms outdated system and replacement. Application: Institutional response confirmation. https://www.uscourts.gov/data-news/judiciary-news/2026/06/26/judiciary-approves-funding-case-management-and-public-access-modernization

[FN 234] Administrative Office of the U.S. Courts, "Technology - Annual Report 2011: Data Communications Network Transitions to New Service," 2011. Pinpoint: Technology - Annual Report 2011. The Judiciary identifies DCN as the Data Communications Network and connects it to NextGen CM/ECF. Application: This supplies the authoritative meaning of .dcn. https://www.uscourts.gov/data-news/reports/annual-reports/directors-annual-report/annual-report-2011/technology-annual-report-2011

[FN 235] Cyber-N.E.T. Forensics, RAPS Report, February 27, 2026. Pinpoint: pp. 11-14 and 20-26. RAPS documents the .dcn artifacts and their context. Application: Subject evidence.

[FN 236] Administrative Office of the U.S. Courts, "Technology - Annual Report 2011: Data Communications Network Transitions to New Service," 2011. Pinpoint: official Judiciary annual report. Defines DCN as the Judiciary network. Application: Authoritative infrastructure context. https://www.uscourts.gov/data-news/reports/annual-reports/directors-annual-report/annual-report-2011/technology-annual-report-2011

[FN 237] U.S. Bankruptcy Court, District of Minnesota, "Important - CM/ECF Electronic Noticing Delivery Problem," 2011-01-01. Pinpoint: court notice. The District of Minnesota notice lists the four gateway names and eight IP addresses used for NEF delivery. Application: This supplies authoritative gateway-routing context. https://www.mnb.uscourts.gov/news/important-cmecf-electronic-noticing-delivery-problem

[FN 238] Cyber-N.E.T. Forensics, RAPS Report, February 27, 2026. Pinpoint: p. 11 and pp. 20-26. RAPS observed the same gateway family in subject message paths. Application: This connects the public architecture to the subject artifacts.

[FN 239] Administrative Office of the U.S. Courts, "Judiciary Approves Funding for Case Management and Public Access Modernization," 2026-06-26. Pinpoint: official Judiciary release. Describes CM/ECF as the intake and processing

engine and PACER as the public access means. Application: System definition. https://www.uscourts.gov/data-news/judiciary-news/2026/06/26/judiciary-approves-funding-case-management-and-public-access-modernization

[FN 240] PACER, "NextGen CM/ECF Frequently Asked Questions," 2026 (accessed 2026-08-26). Pinpoint: PACER NextGen FAQ. Explains the shared authentication relationship. Application: Account architecture. https://pacer.uscourts.gov/help/faqs/nextgen-cmecf

[FN 241] PACER / Administrative Office of the U.S. Courts, "Multifactor Authentication Coming Soon," 2025-05-02. Pinpoint: official PACER announcement. States mandatory CM/ECF-level and optional PACER-only MFA. Application: National rule. https://pacer.uscourts.gov/announcements/2025/05/02/multifactor-authentication-coming-soon

[FN 242] U.S. District Court for the District of Maine, "Multifactor Authentication Coming to PACER and CM/ECF," 2025-05-06. Pinpoint: District of Maine notice. Repeats the mandatory/optional distinction. Application: District implementation. https://www.med.uscourts.gov/news/multifactor-authentication-coming-pacer-and-cmecf

[FN 243] U.S. Court of Appeals for the Eleventh Circuit, "Multifactor Authentication for PACER and CM/ECF," 2025-05-07. Pinpoint: Eleventh Circuit notice. Repeats the nationwide rollout. Application: Appellate implementation. https://www.ca11.uscourts.gov/news/multifactor-authentication-pacer-and-cmecf

[FN 244] U.S. District Court for the District of Arizona, "Mandatory Multifactor Authentication for CM/ECF Filers," 2025-11-25. Pinpoint: District of Arizona update. Documents enforcement through login prompts. Application: Implementation detail. https://www.azd.uscourts.gov/news/mandatory-multifactor-authentication-cmecf-filers

[FN 245] U.S. District Court for the Northern District of Texas, "Password and Multifactor Authentication Requirements," 2025-08-27. Pinpoint: Northern District of Texas notice. Documents password and MFA requirements. Application: Implementation detail. https://www.txnd.uscourts.gov/news/password-and-multifactor-authentication-requirements

[FN 246] PACER / Administrative Office of the U.S. Courts, "Multifactor Authentication Coming Soon," 2025-05-02. Pinpoint: national announcement. Defines the account-class distinction. Application: National framework. https://pacer.uscourts.gov/announcements/2025/05/02/multifactor-authentication-coming-soon

[FN 247] Cyber-N.E.T. Forensics, RAPS Report, February 27, 2026. Pinpoint: pp. 11-14 and 20-26. RAPS identified the earlier identity risk. Application: Prior finding.

[FN 248] PACER / Administrative Office of the U.S. Courts, "Multifactor Authentication Coming Soon," 2025-05-02. Pinpoint: official PACER announcement. The Judiciary required MFA to reduce password-theft risk. Application: Subsequent institutional validation. https://pacer.uscourts.gov/announcements/2025/05/02/multifactor-authentication-coming-soon

[FN 249] Jason Lyons, Declaration in Microsoft Corporation et al. v. John Does 1-2 et al., E.D.N.Y. No. 23-cv-2447, March 30, 2023. Pinpoint: ¶¶ 3-5. Lyons describes the investigation, connected network and EDNY nexus. Application: This establishes the sworn infrastructure framework.

[FN 250] Jason Lyons, Declaration in Microsoft Corporation et al. v. John Does 1-2 et al., E.D.N.Y. No. 23-cv-2447, March 30, 2023. Pinpoint: ¶ 9. Lyons explains the technical identification method. Application: This defines the evidentiary basis for Microsoft attribution.

[FN 251] Jason Lyons, Declaration in Microsoft Corporation et al. v. John Does 1-2 et al., E.D.N.Y. No. 23-cv-2447, March 30, 2023. Pinpoint: ¶¶ 23 and 34. Lyons describes scale, victim telemetry and operational capabilities. Application: This supplies actor-scale and impact evidence.

[FN 252] Jason Lyons, Declaration in Microsoft Corporation et al. v. John Does 1-2 et al., E.D.N.Y. No. 23-cv-2447, March 30, 2023. Pinpoint: ¶ 36. Lyons identifies the named groups and functional roles. Application: This is the principal sworn attribution anchor.

[FN 253] Rodel Finones, Declaration in Microsoft Corporation et al. v. John Does 1-2 et al., E.D.N.Y. No. 23-cv-2447, March 30, 2023. Pinpoint: ¶¶ 12 and 25. Finones explains the post-exploitation capabilities of cracked Cobalt Strike. Application: This independently supports endpoint and credential mechanisms.

[FN 254] U.S. District Court, Eastern District of New York, Order Adopting Report and Recommendation and Permanent Injunction, Microsoft Corporation et al. v. John Does 1-2 et al., No. 23-cv-2447, September 8, 2025. Pinpoint: pp. 1-23. The order adopts the R&R and imposes permanent infrastructure relief. Application: This supplies the judicial disruption and sinkhole framework.

[FN 255] Cyber-N.E.T. Forensics, Integrated Expert Report, October 22, 2025. Pinpoint: pp. 269-273 and 292-300. The prior report catalogued IPs, ASNs and the AWS DNS family. Application: Subject attribution baseline. https://cyberlawlibrary.org/reports/cyber-n-e-t-forensics-expert-report/

[FN 256] Jason Lyons, Declaration in Microsoft Corporation et al. v. John Does 1-2 et al., E.D.N.Y. No. 23-cv-2447, March 30, 2023. Pinpoint: ¶ 9. Microsoft used Beacon/configuration/telemetry to identify malicious infrastructure. Application: This supplies the higher evidentiary standard.

[FN 257] Amazon Web Services, "Route 53 API: ChangeResourceRecordSets," 2026 (accessed 2026-08-26). Pinpoint: official Route 53 documentation. AWS service ranges are part of shared cloud infrastructure. Application: This supports provider-versus-actor separation. https://docs.aws.amazon.com/Route53/latest/APIReference/API_ChangeResourceRecordSets.html

[FN 258] Cyber-N.E.T. Forensics, Integrated Expert Report, October 22, 2025. Pinpoint: pp. 269-273. CNF identifies exact and family-level comparisons. Application: Subject baseline. https://cyberlawlibrary.org/reports/cyber-n-e-t-forensics-expert-report/

[FN 259] Jason Lyons, Declaration in Microsoft Corporation et al. v. John Does 1-2 et al., E.D.N.Y. No. 23-cv-2447, March 30, 2023. Pinpoint: ¶¶ 9 and 36. Lyons provides technical and actor-specific comparator evidence. Application: Independent attribution standard.

[FN 260] U.S. District Court, Eastern District of New York, Order Adopting Report and Recommendation and Permanent Injunction, Microsoft Corporation et al. v. John Does 1-2 et al., No. 23-cv-2447, September 8, 2025. Pinpoint: pp. 1-23. The injunction defines the adjudicated infrastructure set. Application: Judicial comparator.

[FN 261] Cyber-N.E.T. Forensics, Forensic Sinkhole Report, January 20, 2026. Pinpoint: pp. 2-15. The Sinkhole report describes domain control, redirection and successor infrastructure. Application: This is the prior finding. https://cyberlawlibrary.org/

[FN 262] U.S. District Court, Eastern District of New York, Order Adopting Report and Recommendation and Permanent Injunction, Microsoft Corporation et al. v. John Does 1-2 et al., No. 23-cv-2447, September 8, 2025. Pinpoint: pp. 1-23. The order specifies the domain, DNS, IP, server and logging relief. Application: This is the primary judicial sinkhole authority.

[FN 263] The Hacker News, "ZLoader Malware Returns With DNS Tunneling and Interactive Shell," 2024-12-10. Pinpoint: lines 49-65. The article documents ZLoader's return and added capabilities. Application: Media evidence. https://thehackernews.com/2024/12/zloader-malware-returns-with-dns.html

[FN 264] Zscaler ThreatLabz, "ZLoader returns with DNS tunneling and an interactive shell," 2024-12-09. Pinpoint: primary Zscaler research. Zscaler directly analyzes the malware. Application: Primary technical evidence. https://www.zscaler.com/blogs/security-research/zloader-returns-dns-tunneling-and-interactive-shell

[FN 265] Cyber-N.E.T. Forensics, Forensic Sinkhole Report, January 20, 2026. Pinpoint: pp. 7-15. Sinkhole anticipated successor infrastructure. Application: Prior finding. https://cyberlawlibrary.org/

[FN 266] CISA / FBI / HHS, "#StopRansomware: Medusa Ransomware," 2026-08-18 update. Pinpoint: Medusa joint advisory. The advisory documents affiliates, credential use and initial-access brokers. Application: Current access-broker evidence. https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-071a

[FN 267] CISA / FBI / NSA / partners, "#StopRansomware: Gunra Ransomware," 2026-08-10. Pinpoint: Gunra joint advisory. The advisory describes Conti-derived RaaS, vulnerabilities and access brokers. Application: Current Conti-lineage evidence. https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-222a

[FN 268] CISA / FBI / ASD ACSC, "#StopRansomware: Play Ransomware," 2025-06-04 update. Pinpoint: Play advisory update. The advisory documents a large affiliate ecosystem and hundreds of victims. Application: Current scale evidence. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-352a

[FN 269] CISA / FBI / international partners, "Understanding Ransomware Threat Actors: LockBit," 2023-06-14. Pinpoint: LockBit joint advisory. The advisory documents LockBit's global affiliate model. Application: Microsoft comparator evidence. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a

[FN 270] Cyber-N.E.T. Forensics, Forensic Sinkhole Report, January 20, 2026. Pinpoint: pp. 2-15. Prior continuing-infrastructure finding. Application: Subject baseline. https://cyberlawlibrary.org/

[FN 271] Truffle Security Research, "768 Leaked Corporate AWS Keys Held Full Admin Rights," 2026-08-19. Pinpoint: long-lived AWS keys. Credentials survive infrastructure changes. Application: Cloud persistence. https://trufflesecurity.com/blog/leaked-corporate-aws-keys-held-full-admin-rights

[FN 272] The Hacker News, "ZLoader Malware Returns With DNS Tunneling and Interactive Shell," 2024-12-10. Pinpoint: ZLoader return. Malware and C2 re-emerge after takedown. Application: Successor evidence. https://thehackernews.com/2024/12/zloader-malware-returns-with-dns.html

[FN 273] CISA / FBI / NSA / partners, "#StopRansomware: Gunra Ransomware," 2026-08-10. Pinpoint: Gunra advisory. Affiliates and access brokers distribute operational continuity. Application: Ecosystem evidence. https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-222a

[FN 274] Cyber-N.E.T. Forensics, Integrated Expert Report, October 22, 2025. Pinpoint: pp. 184-203 and 238-254. CNF set out the integrated multi-layer model. Application: Foundational sequence. https://cyberlawlibrary.org/reports/cyber-n-e-t-forensics-expert-report/

[FN 275] Kely Gonzaga et al., "AI-Powered Social Engineering: Emerging Attack Vectors, Vulnerabilities, and Multi-Layered Defense Strategies," 2026-02-17. Pinpoint: pp. 8-17 of uploaded paper. The AI social-engineering review organizes realism, personalization, automation and adaptive execution across an attack lifecycle. Application: Modern AI amplification. https://doi.org/10.3390/computers15020128

[FN 276] Microsoft Threat Intelligence, "Storm-0501's evolving techniques lead to cloud-based ransomware," 2025-08-27. Pinpoint: Storm-0501. Endpoint credentials progressed to cloud control and persistence. Application: Cloud sequence. https://www.microsoft.com/en-us/security/blog/2025/08/27/storm-0501s-evolving-techniques-lead-to-cloud-based-ransomware/

[FN 277] BleepingComputer, "Russian hackers exploit Exchange OWA zero-day for long-term mailbox access," 2026-07-29. Pinpoint: OWAReaper. Mailbox access progressed to server-side persistence and alternate exfiltration. Application: Communications sequence. https://www.bleepingcomputer.com/news/security/russian-hackers-exploit-exchange-owa-zero-day-for-long-term-mailbox-access/

[FN 278] Cyber-N.E.T. Forensics, Integrated Expert Report, October 22, 2025. Pinpoint: pp. 238-254. CNF classified the campaign as outcome-oriented legal-process control. Application: Prior determination. https://cyberlawlibrary.org/reports/cyber-n-e-t-forensics-expert-report/

[FN 279] FBI / IC3, "Senior U.S. Officials Impersonated in Malicious Messaging Campaign," 2025-05-15. Pinpoint: FBI impersonation campaign. Identity capture was used to reach trusted contacts and elicit action. Application: Cross-industry functional analogue. https://www.fbi.gov/investigate/cyber/alerts/2025/senior-us-officials-impersonated-in-malicious-messaging-campaign

[FN 280] Recorded Future Insikt Group, "Synthetic Identities: A Dual Threat to Enterprises," 2025-10-01. Pinpoint: synthetic identity report. Enterprise identity was used for access, espionage, revenue and persistent footholds. Application: Cross-industry functional analogue. https://www.recordedfuture.com/research/synthetic-identities-dual-threat-enterprises

[FN 281] CISA / NSA / FBI and partners, "PRC State-Sponsored Actors Living off the Land to Evade Detection," 2023-05-24. Pinpoint: living-off-the-land advisory. Legitimate tools reduce distinctive malware artifacts. Application: Endpoint explanation. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a

[FN 282] Truffle Security Research, "768 Leaked Corporate AWS Keys Held Full Admin Rights," 2026-08-19. Pinpoint: valid AWS credentials. Valid keys authenticate as legitimate principals. Application: Cloud explanation. https://trufflesecurity.com/blog/leaked-corporate-aws-keys-held-full-admin-rights

[FN 283] BleepingComputer, "Russian hackers exploit Exchange OWA zero-day for long-term mailbox access," 2026-07-29. Pinpoint: server-side mailbox persistence. Attacker actions occur inside Exchange trust. Application: Mail explanation. https://www.bleepingcomputer.com/news/security/russian-hackers-exploit-exchange-owa-zero-day-for-long-term-mailbox-access/

[FN 284] KnowBe4, "How a North Korean Fake IT Worker Tried to Infiltrate Us," 2024-07-23. Pinpoint: KnowBe4 incident. The false worker passed interviews and received a device. Application: Identity explanation. https://blog.knowbe4.com/how-a-north-korean-fake-it-worker-tried-to-infiltrate-us

[FN 285] BleepingComputer, "Hackers abuse npm mirrors to host phishing redirect pages," 2026-08-25. Pinpoint: npm mirror abuse. Malicious HTML appeared under legitimate mirror domains. Application: Infrastructure explanation. https://www.bleepingcomputer.com/news/security/hackers-abuse-npm-mirrors-to-host-phishing-redirect-pages/

[FN 286] Cyber-N.E.T. Forensics, Integrated Expert Report, October 22, 2025. Pinpoint: pp. 100-120 and 238-254. CNF's methodology and integrated attribution depend on cross-layer convergence. Application: This is the governing proof standard. https://cyberlawlibrary.org/reports/cyber-n-e-t-forensics-expert-report/

[FN 287] Team B / Cyber-N.E.T. Forensics, Florida Bar Employee, Membership, and Florida e-Filing Portal Infiltration Reports, as adopted in the October 22 CNF Report, 2024-2025. Pinpoint: portal corpus adopted at CNF pp. 133-160 and 244-245. The portal data supplies a large longitudinal event set. Application: Subject corpus.

[FN 288] Kai-Cheng Yang and Filippo Menczer, "Anatomy of an AI-powered malicious social botnet," 2024-05. Pinpoint: coordinated botnet study. Coordination patterns exposed the botnet where text classifiers failed. Application: Independent illustration of pattern-based detection. https://doi.org/10.51685/jqd.2024.icwsm.7

[FN 289] Marlin Technologies, Expert Report, December 5, 2024. Pinpoint: pp. 4-8. Marlin identified APT persistence and escalation. Application: Early independent expert support.

[FN 290] Cyber-N.E.T. Forensics, Integrated Expert Report, October 22, 2025. Pinpoint: pp. 184-203 and 238-254. CNF integrated the layers and outcome effects. Application: Principal expert support. https://cyberlawlibrary.org/reports/cyber-n-e-t-forensics-expert-report/

[FN 291] CISA / NSA / FBI and partners, "PRC State-Sponsored Actors Living off the Land to Evade Detection," 2023-05-24. Pinpoint: living-off-the-land advisory. State actors deliberately minimize artifacts. Application: Independent tradecraft support. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a

[FN 292] Kely Gonzaga et al., "AI-Powered Social Engineering: Emerging Attack Vectors, Vulnerabilities, and Multi-Layered Defense Strategies," 2026-02-17. Pinpoint: pp. 8-17. AI-enabled operations add personalization, automation and adaptive deception. Application: Current tradecraft support. https://doi.org/10.3390/computers15020128

[FN 293] Cyber-N.E.T. Forensics, Integrated Expert Report, October 22, 2025. Pinpoint: pp. 238-254 and 269-273. CNF's prior attribution and IoC findings. Application: Subject baseline. https://cyberlawlibrary.org/reports/cyber-n-e-t-forensics-expert-report/

[FN 294] Jason Lyons, Declaration in Microsoft Corporation et al. v. John Does 1-2 et al., E.D.N.Y. No. 23-cv-2447, March 30, 2023. Pinpoint: ¶¶ 9 and 36. Microsoft's technical and actor comparator evidence. Application: Independent attribution anchor.

[FN 295] Rodel Finones, Declaration in Microsoft Corporation et al. v. John Does 1-2 et al., E.D.N.Y. No. 23-cv-2447, March 30, 2023. Pinpoint: ¶¶ 12 and 25. Post-exploitation capability evidence. Application: Tool-lineage anchor.

[FN 296] U.S. District Court, Eastern District of New York, Order Adopting Report and Recommendation and Permanent Injunction, Microsoft Corporation et al. v. John Does 1-2 et al., No. 23-cv-2447, September 8, 2025. Pinpoint: pp. 1-23. Adjudicated infrastructure and disruption. Application: Judicial anchor.

[FN 297] Cyber-N.E.T. Forensics, Forensic Sinkhole Report, January 20, 2026. Pinpoint: pp. 7-15. Sinkhole treats successor infrastructure as a continuing investigative target. Application: This supports continuing attribution. https://cyberlawlibrary.org/

[FN 298] Cyber-N.E.T. Forensics, Integrated Expert Report, October 22, 2025. Pinpoint: pp. 269-273. CNF preserved IoCs for later cross-case comparison. Application: This supports retrospective mapping. https://cyberlawlibrary.org/reports/cyber-n-e-t-forensics-expert-report/

[FN 299] CISA and international partners, "Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System," 2025-08-27 (rev. 2025-09-03). Pinpoint: joint advisory. Current government reporting shows long-term compromise of backbone and edge infrastructure and pivoting through trusted relationships. Application: This supplies a current routing-comparison source. https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-239a

[FN 300] Cyber-N.E.T. Forensics, Integrated Expert Report, October 22, 2025. Pinpoint: pp. 238-254. CNF defined the APT as broader than one incident. Application: Foundational mission. https://cyberlawlibrary.org/reports/cyber-n-e-t-forensics-expert-report/

[FN 301] Cyber-N.E.T. Forensics, Forensic Sinkhole Report, January 20, 2026. Pinpoint: pp. 2-15. Sinkhole describes disruption and successor infrastructure. Application: Continuing-disruption mission. https://cyberlawlibrary.org/

[FN 302] FBI / IC3, "Senior U.S. Officials Impersonated in Malicious Messaging Campaign," 2025-05-15. Pinpoint: FBI senior-official campaign. Identity capture can propagate through trusted professional contacts. Application: Cross-industry extension. https://www.fbi.gov/investigate/cyber/alerts/2025/senior-us-officials-impersonated-in-malicious-messaging-campaign

[FN 303] Recorded Future Insikt Group, "Synthetic Identities: A Dual Threat to Enterprises," 2025-10-01. Pinpoint: synthetic identity report. Synthetic enterprise identities enable state revenue, access and IP theft. Application: Cross-industry extension. https://www.recordedfuture.com/research/synthetic-identities-dual-threat-enterprises

[FN 304] Cyber-N.E.T. Forensics, Integrated Expert Report, October 22, 2025. Pinpoint: pp. 100-120 and 269-273. CNF's normalized metadata and IoC preservation provide the retrospective basis. Application: This supports continuing discovery. https://cyberlawlibrary.org/reports/cyber-n-e-t-forensics-expert-report/

[FN 305] Infoblox Threat Intelligence, "Who Knew? Domain Hijacking Is So Easy: The Sitting Ducks Attack," 2024-07-31. Pinpoint: Sitting Ducks research. Long-lived domain metadata and hijacking patterns can reveal infrastructure supply. Application: DNS discovery. https://www.infoblox.com/blog/threat-intelligence/who-knew-domain-hijacking-is-so-easy/

[FN 306] Truffle Security Research, "768 Leaked Corporate AWS Keys Held Full Admin Rights," 2026-08-19. Pinpoint: AWS-key research. Long-lived credentials and public secret corpora can be retrospectively revalidated. Application: Cloud discovery. https://trufflesecurity.com/blog/leaked-corporate-aws-keys-held-full-admin-rights

[FN 307] Kai-Cheng Yang and Filippo Menczer, "Anatomy of an AI-powered malicious social botnet," 2024-05. Pinpoint: AI-botnet research. Coordination analysis can expose artificial persona networks. Application: Identity discovery. https://doi.org/10.51685/jqd.2024.icwsm.7

[FN 308] PACER / Administrative Office of the U.S. Courts, "Multifactor Authentication Coming Soon," 2025-05-02. Pinpoint: source as identified in the register. All CM/ECF-level users were scheduled to be required to use MFA by the end of 2025; PACER-only users could enroll optionally. Application: This source is integrated into the continuing investigation because it maps to RAPS; Federal Court Audit; CM/ECF identity control. https://pacer.uscourts.gov/announcements/2025/05/02/multifactor-authentication-coming-soon

[FN 309] Administrative Office of the U.S. Courts, "Cybersecurity Measures Strengthened in Light of Attacks on Judiciary's Case Management System," 2025-08-07. Pinpoint: source as identified in the register. The Judiciary acknowledged sophisticated, persistent attacks against the case-management system and heightened protection for sensitive case documents. Application: This source is integrated into the continuing investigation because it maps to RAPS; Federal Court Audit; sealed-record risk. https://www.uscourts.gov/data-news/judiciary-news/2025/08/07/cybersecurity-measures-strengthened-light-attacks-judiciarys-case-management-system

[FN 310] Administrative Office of the U.S. Courts, "Judges Outline Accelerated Modernization of Case Management System," 2026-03-10. Pinpoint: source as identified in the register. The Judiciary accelerated replacement of legacy case-management architecture following acute and persistent cybersecurity risks. Application: This source is integrated into the continuing investigation because it maps to RAPS; legacy/end-of-life analysis. https://www.uscourts.gov/data-news/judiciary-news/2026/03/10/judges-outline-accelerated-modernization-case-management-system

[FN 311] Administrative Office of the U.S. Courts, "Judiciary Approves Funding for Case Management and Public Access Modernization," 2026-06-26. Pinpoint: source as identified in the register. The Judiciary described CM/ECF as outdated, announced secure-cloud document storage beginning in 2026, and planned district-court deployment of a new system through 2027. Application: This source is integrated into the continuing investigation because it maps to

RAPS; Federal Court Audit; cloud migration. https://www.uscourts.gov/data-news/judiciary-news/2026/06/26/judiciary-approves-funding-case-management-and-public-access-modernization

[FN 312] Politico, "Federal courts were warned for years about security flaw that led to hack," 2025-08-12. Pinpoint: source as identified in the register. Reporting identified longstanding judiciary-security weaknesses, inconsistent strong authentication, and exposure of sensitive filings. Application: This source is integrated into the continuing investigation because it maps to RAPS; Federal Court Audit. https://www.politico.com/news/2025/08/12/federal-courts-hack-security-flaw-00506392

[FN 313] Reuters, "U.S. federal courts say their systems were targeted by recent cyberattacks," 2025-08-07. Pinpoint: source as identified in the register. Contemporaneous reporting on the Judiciary's acknowledgment of attacks on its electronic case-management system. Application: This source is integrated into the continuing investigation because it maps to RAPS; Federal Court Audit. https://www.reuters.com/legal/litigation/us-federal-courts-say-their-systems-were-targeted-by-recent-cyberattacks-2025-08-07/

[FN 314] Reuters, "U.S. taking special measures to protect people possibly exposed in court-records hack," 2025-08-14. Pinpoint: source as identified in the register. Reporting described special handling for persons and matters exposed through compromised sealed or restricted records. Application: This source is integrated into the continuing investigation because it maps to RAPS; sealed-record risk. https://www.reuters.com/legal/government/us-taking-special-measures-protect-people-possibly-exposed-court-records-hack-2025-08-14/

[FN 315] Reuters, "U.S. senator calls for independent review of federal judiciary cybersecurity," 2025-08-25. Pinpoint: source as identified in the register. Reporting described congressional concern that the Judiciary's security posture and breach response required independent review. Application: This source is integrated into the continuing investigation because it maps to RAPS; governance and legacy risk. https://www.reuters.com/legal/government/us-senator-calls-independent-review-federal-judiciary-cybersecurity-2025-08-25/

[FN 316] Office of Senator Ron Wyden, "Wyden Calls for Independent Review of Federal Judicial Cybersecurity Following Massive Hack of Secret Court Files," 2025-08-25. Pinpoint: source as identified in the register. The letter sought independent assessment of a compromise involving secret court files and systemic security controls. Application: This source is integrated into the continuing investigation because it maps to RAPS; Federal Court Audit. https://www.wyden.senate.gov/news/press-releases/wyden-calls-for-independent-review-of-federal-judicial-cybersecurity-following-massive-hack-of-secret-court-files

[FN 317] TechCrunch, "Russian government hackers said to be behind U.S. federal court filing system hack," 2025-08-12. Pinpoint: source as identified in the register. Reporting connected the federal court-system incident to Russian government-linked activity and sensitive-case targeting. Application: This source is integrated into the continuing investigation because it maps to RAPS; attribution context. https://techcrunch.com/2025/08/12/russian-government-hackers-said-to-be-behind-us-federal-court-filing-system-hack-report/

[FN 318] Bloomberg, "Russian Hackers Lurked in U.S. Courts for Years, Took Sealed Files," 2025-08-14. Pinpoint: source as identified in the register. Reporting described stolen credentials, an outdated server, persistence, and sealed-file access. Application: This source is integrated into the continuing investigation because it maps to RAPS; legacy endpoints; credentials. https://www.bloomberg.com/news/articles/2025-08-14/russian-hackers-lurked-in-us-courts-for-years-took-sealed-files

[FN 319] Bloomberg Law, "Federal Courts Restrict Sealed Filings After Cyberattack," 2025-09-24. Pinpoint: source as identified in the register. Reporting described post-breach restrictions and altered handling of sealed documents. Application: This source is integrated into the continuing investigation because it maps to RAPS; intake and sealed-record handling. https://news.bloomberglaw.com/us-law-week/federal-courts-restrict-sealed-filings-after-cyberattack

[FN 320] U.S. Court of Appeals for the Fourth Circuit, "Multifactor Authentication for PACER and CM/ECF," 2025-05-07. Pinpoint: source as identified in the register. Circuit implementation notice corroborating nationwide MFA rollout for filing-level accounts. Application: This source is integrated into the continuing investigation because it maps to RAPS; authentication. https://www.ca4.uscourts.gov/announcements/multifactor-authentication-for-pacer-and-cmecf

[FN 321] U.S. Court of Appeals for the Eleventh Circuit, "Multifactor Authentication for PACER and CM/ECF," 2025-05-07. Pinpoint: source as identified in the register. Circuit implementation notice corroborating nationwide MFA rollout for filing-level accounts. Application: This source is integrated into the continuing investigation because it maps to RAPS; authentication. https://www.ca11.uscourts.gov/news/multifactor-authentication-pacer-and-cmecf

[FN 322] U.S. District Court for the District of Maine, "Multifactor Authentication Coming to PACER and CM/ECF," 2025-05-06. Pinpoint: source as identified in the register. District notice distinguished mandatory CM/ECF-level MFA from optional PACER-only MFA. Application: This source is integrated into the continuing investigation because it maps to RAPS; authentication. https://www.med.uscourts.gov/news/multifactor-authentication-coming-pacer-and-cmecf

[FN 323] U.S. District Court for the District of Arizona, "Mandatory Multifactor Authentication for CM/ECF Filers," 2025-11-25. Pinpoint: source as identified in the register. District notice documents mandatory MFA implementation for filing-level access. Application: This source is integrated into the continuing investigation because it maps to RAPS; authentication. https://www.azd.uscourts.gov/news/mandatory-multifactor-authentication-cmecf-filers

[FN 324] U.S. District Court for the Northern District of Texas, "Password and Multifactor Authentication Requirements," 2025-08-27. Pinpoint: source as identified in the register. District notice documents credential changes and MFA implementation following judiciary security concerns. Application: This source is integrated into the continuing

investigation because it maps to RAPS; authentication. https://www.txnd.uscourts.gov/news/password-and-multifactor-authentication-requirements

[FN 325] PACER, "NextGen CM/ECF Frequently Asked Questions," 2026 (accessed 2026-08-26). Pinpoint: source as identified in the register. PACER documentation explains the shared authentication relationship between PACER credentials and NextGen CM/ECF filing access. Application: This source is integrated into the continuing investigation because it maps to RAPS; identity and portal architecture. https://pacer.uscourts.gov/help/faqs/nextgen-cmecf

[FN 326] BleepingComputer, "Hundreds of leaked AWS keys give full control over corporate accounts," 2026-08-21. Pinpoint: source as identified in the register. Reports that thousands of long-lived exposed AWS keys remained valid, including root and AdministratorAccess credentials capable of account-wide control. Application: This source is integrated into the continuing investigation because it maps to CNF cloud abuse; SUW mechanism. https://www.bleepingcomputer.com/news/security/hundreds-of-leaked-aws-keys-give-full-control-over-corporate-accounts/

[FN 327] Truffle Security Research, "768 Leaked Corporate AWS Keys Held Full Admin Rights," 2026-08-19. Pinpoint: source as identified in the register. Revalidated 10,616 leaked AWS key pairs; documented 768 business-linked credentials with full account control, long credential age, and poor rotation. Application: This source is integrated into the continuing investigation because it maps to CNF cloud abuse; SUW mechanism. https://trufflesecurity.com/blog/leaked-corporate-aws-keys-held-full-admin-rights

[FN 328] Amazon Web Services, "AWS Identity and Access Management: Managing access keys," 2026 (accessed 2026-08-26). Pinpoint: source as identified in the register. Defines programmatic access-key credentials and their relationship to IAM permissions. Application: This source is integrated into the continuing investigation because it maps to CNF cloud abuse; reader definition. https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html

[FN 329] Amazon Web Services, "Route 53 API: ChangeResourceRecordSets," 2026 (accessed 2026-08-26). Pinpoint: source as identified in the register. Documents transactional API-driven CREATE, DELETE and UPSERT DNS changes and normal global propagation behavior. Application: This source is integrated into the continuing investigation because it maps to SUW-14; SUW-15; Route 53 mechanism. https://docs.aws.amazon.com/Route53/latest/APIReference/API_ChangeResourceRecordSets.html

[FN 330] Amazon Web Services, "Actions, resources, and condition keys for Amazon Route 53," 2026 (accessed 2026-08-26). Pinpoint: source as identified in the register. Documents the IAM permissions capable of changing hosted-zone and DNS record state. Application: This source is integrated into the continuing investigation because it maps to SUW mechanism; privileged cloud identity. https://docs.aws.amazon.com/service-authorization/latest/reference/list_amazonroute53.html

[FN 331] BleepingComputer, "whoAMI attacks give hackers code execution on Amazon EC2 instances," 2025-02-13. Pinpoint: source as identified in the register. Describes a cloud-image name-confusion path by which malicious AMIs can be selected by misconfigured automation and execute inside AWS accounts. Application: This source is integrated into the continuing investigation because it maps to CNF cloud trust; infrastructure automation. https://www.bleepingcomputer.com/news/security/whoami-attacks-give-hackers-code-execution-on-amazon-ec2-instances/

[FN 332] Datadog Security Labs, "whoAMI: A cloud image name confusion attack," 2025-02-12. Pinpoint: source as identified in the register. Demonstrates code execution through malicious AMI selection, estimates broad exposure, and documents vulnerable infrastructure-as-code patterns. Application: This source is integrated into the continuing investigation because it maps to CNF cloud trust; automation. https://securitylabs.datadoghq.com/articles/whoami-a-cloud-image-name-confusion-attack/

[FN 333] BleepingComputer, "Hackers target SSRF bugs in EC2-hosted sites to steal AWS credentials," 2025-04-09. Pinpoint: source as identified in the register. Reports active extraction of EC2 instance metadata and IAM role credentials through SSRF against IMDSv1. Application: This source is integrated into the continuing investigation because it maps to CNF credential capture; cloud pivot. https://www.bleepingcomputer.com/news/security/hackers-target-ssrf-bugs-in-ec2-hosted-sites-to-steal-aws-credentials/

[FN 334] F5 Labs, "March 2025 Sensor Intelligence: SSRF Targeting EC2 Metadata," 2025-04-08. Pinpoint: source as identified in the register. Documents coordinated probing of EC2-hosted applications to obtain metadata and cloud credentials. Application: This source is integrated into the continuing investigation because it maps to CNF credential capture; cloud pivot. https://www.f5.com/labs/articles/threat-intelligence/march-2025-sensor-intelligence-report

[FN 335] Sysdig Threat Research Team, "SCARLETEEL: Operation Leveraging Terraform, Kubernetes, and AWS for Data Theft," 2023-02-28. Pinpoint: source as identified in the register. Documents theft of temporary cloud credentials, discovery of Terraform state secrets, cloud logging evasion, and lateral cloud access. Application: This source is integrated into the continuing investigation because it maps to CNF cloud persistence; credential theft. https://www.sysdig.com/blog/cloud-breach-terraform-data-theft

[FN 336] Sysdig Threat Research Team, "SCARLETEEL 2.0: Fargate, Kubernetes, and AWS Compromise," 2023-07-11. Pinpoint: source as identified in the register. Extends the cloud attack chain through compromised workloads, credentials, IAM abuse, data theft, and persistence. Application: This source is integrated into the continuing investigation because it maps to CNF cloud persistence. https://www.sysdig.com/blog/scarleteel-2-0

[FN 337] BleepingComputer, "Hackers use AWS SSM Agent as remote access trojan," 2023-08-02. Pinpoint: source as identified in the register. Reports abuse of AWS Systems Manager Agent as legitimate remote-management infrastructure after compromise. Application: This source is integrated into the continuing investigation because it maps to Marlin; endpoint persistence; trusted tools. https://www.bleepingcomputer.com/news/security/hackers-use-aws-ssm-agent-as-remote-access-trojan/

[FN 338] Mitiga, "Abusing AWS Systems Manager Agent as a Remote Access Trojan," 2023-08-01. Pinpoint: source as identified in the register. Demonstrates post-compromise registration of endpoints to attacker-controlled AWS accounts through a legitimate enterprise agent. Application: This source is integrated into the continuing investigation because it maps to Marlin; endpoint persistence. https://www.mitiga.io/blog/abusing-aws-systems-manager-agent-as-a-remote-access-trojan

[FN 339] CISA / FBI, "Threat Actors Exploit Multiple Vulnerabilities to Deploy Androxgh0st Malware," 2024-01-16. Pinpoint: source as identified in the register. Documents theft of AWS, Microsoft 365, SMTP, SendGrid and Twilio credentials from exposed environment files. Application: This source is integrated into the continuing investigation because it maps to CNF cloud/mail credential theft. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-016a

[FN 340] Microsoft Threat Intelligence, "Storm-0501: Ransomware attacks expanding to hybrid cloud environments," 2024-09-26. Pinpoint: source as identified in the register. Documents on-premises compromise, Cobalt Strike, credential theft, Entra privilege escalation, and hybrid-cloud pivoting. Application: This source is integrated into the continuing investigation because it maps to Marlin; CNF endpoint-to-cloud chain. https://www.microsoft.com/en-us/security/blog/2024/09/26/storm-0501-ransomware-attacks-expanding-to-hybrid-cloud-environments/

[FN 341] Microsoft Threat Intelligence, "Storm-0501's evolving techniques lead to cloud-based ransomware," 2025-08-27. Pinpoint: source as identified in the register. Documents valid credentials, MFA registration, Global Administrator compromise, federated-domain persistence, Azure role escalation, storage-key theft, deletion and Teams extortion. Application: This source is integrated into the continuing investigation because it maps to CNF cloud abuse; CCDG; identity persistence. https://www.microsoft.com/en-us/security/blog/2025/08/27/storm-0501s-evolving-techniques-lead-to-cloud-based-ransomware/

[FN 342] Microsoft Threat Intelligence, "Inside the attack chain: Threat activity targeting Azure Blob Storage," 2025-10-20. Pinpoint: source as identified in the register. Documents refresh-token and key-based access, Azure storage operations, Cloud Shell credentials, persistence, exfiltration and destructive action. Application: This source is integrated into the continuing investigation because it maps to CNF Azure/cloud control. https://www.microsoft.com/en-us/security/blog/2025/10/20/inside-the-attack-chain-threat-activity-targeting-azure-blob-storage/

[FN 343] Microsoft Threat Intelligence, "Defending against evolving identity attack techniques," 2025-05-29. Pinpoint: source as identified in the register. Documents device-code phishing, OAuth consent, access and refresh tokens, device registration, and internal post-compromise phishing through legitimate identity services. Application: This source is integrated into the continuing investigation because it maps to CCDG; Avatar; portal identity. https://www.microsoft.com/en-us/security/blog/2025/05/29/defending-against-evolving-identity-attack-techniques/

[FN 344] CISA, "Emergency Directive 24-02: Mitigating the Significant Risk from Nation-State Compromise of Microsoft Corporate Email System," 2024-04-02. Pinpoint: source as identified in the register. Acknowledges risk from exfiltrated Microsoft corporate-email correspondence and authentication details and orders federal agencies to assess related exposure. Application: This source is integrated into the continuing investigation because it maps to CCDG; enterprise email trust. https://www.cisa.gov/news-events/directives/ed-24-02-mitigating-significant-risk-nation-state-compromise-microsoft-corporate-email-system

[FN 345] BleepingComputer, "Hacker claims 3.6 million Azure account records stolen from major companies," 2026-08-17. Pinpoint: source as identified in the register. Reports a criminal claim involving tenant-directory and service-account data allegedly obtained with compromised credentials; the article records denials and lack of independent verification. Application: This source is integrated into the continuing investigation because it maps to Avatar; Azure identity reconnaissance. https://www.bleepingcomputer.com/news/security/hacker-claims-36-million-azure-account-records-stolen-from-major-companies/

[FN 346] CISA and international partners, "Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System," 2025-08-27 (rev. 2025-09-03). Pinpoint: source as identified in the register. Documents long-term compromise of backbone and edge devices, modification of routers, and pivoting through trusted connections. Application: This source is integrated into the continuing investigation because it maps to CNF persistent infrastructure; routing. https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-239a

[FN 347] Qualys Threat Research Unit, "Automated Botnet Attacks Targeting PHP Servers, IoT Devices, and Cloud Gateways," 2025-10-29. Pinpoint: source as identified in the register. Documents automated exploitation, secrets and token discovery, and use of AWS, Azure, Google Cloud and other legitimate infrastructure to obscure origin. Application: This source is integrated into the continuing investigation because it maps to CNF cloud camouflage; endpoint scale. https://blog.qualys.com/vulnerabilities-threat-research/2025/10/29/automated-botnet-attacks-target-php-servers-iot-devices-and-cloud-gateways

[FN 348] The Hacker News, "Experts Report Sharp Increase in Automated Botnet Attacks Targeting PHP Servers and IoT Devices," 2025-10-29. Pinpoint: source as identified in the register. Summarizes exploitation of known CVEs, cloud

misconfiguration, credential and API-key discovery, and legitimate cloud infrastructure abuse. Application: This source is integrated into the continuing investigation because it maps to CNF endpoint/cloud convergence. https://thehackernews.com/2025/10/experts-reports-sharp-increase-in.html

[FN 349] BleepingComputer, "New SynkLoader malware pushed in Microsoft Teams phishing campaign," 2026-08-21. Pinpoint: source as identified in the register. Documents fake IT-helpdesk contact through Teams, Azure-hosted MSI delivery, fake lock-screen credential theft, tunneling, RAT and VNC control. Application: This source is integrated into the continuing investigation because it maps to CCDG; Marlin; professional echo chamber. https://www.bleepingcomputer.com/news/security/new-synkloader-malware-pushed-in-microsoft-teams-phishing-campaign/

[FN 350] Expel, "SynkLoader: when you throw in everything but the kitchen sink," 2026-08-20. Pinpoint: source as identified in the register. Primary analysis of the Teams-delivered multi-module malware, credential capture, reverse proxy, persistence, remote shell and desktop control. Application: This source is integrated into the continuing investigation because it maps to CCDG; Marlin. https://expel.com/blog/synkloader-when-you-throw-in-everything-but-the-kitchen-sink/

[FN 351] BleepingComputer, "Hackers abuse npm mirrors to host phishing redirect pages," 2026-08-25. Pinpoint: source as identified in the register. Documents malicious HTML hosted through npm and trusted mirrors, remote redirection, and persistence on mirrors after package removal. Application: This source is integrated into the continuing investigation because it maps to CNF trusted infrastructure; CCDG. https://www.bleepingcomputer.com/news/security/hackers-abuse-npm-mirrors-to-host-phishing-redirect-pages/

[FN 352] OX Security, "ClickFix Phishing Hidden in Malicious npm Packages," 2026-08-25. Pinpoint: source as identified in the register. Documents packages and mirror-hosted phishing pages using legitimate developer infrastructure and remotely changeable redirect destinations. Application: This source is integrated into the continuing investigation because it maps to CNF trusted infrastructure; CCDG. https://www.ox.security/blog/research-clickfix-phishing-npm-packages/

[FN 353] Microsoft Threat Intelligence, "Midnight Blizzard conducts targeted social engineering over Microsoft Teams," 2023-08-02. Pinpoint: source as identified in the register. Documents nation-state use of compromised Microsoft 365 tenants and Teams messages impersonating support personnel to obtain MFA approval. Application: This source is integrated into the continuing investigation because it maps to CCDG; professional echo chamber. https://www.microsoft.com/en-us/security/blog/2023/08/02/midnight-blizzard-conducts-targeted-social-engineering-over-microsoft-teams/

[FN 354] BleepingComputer, "Russian hackers exploit Exchange OWA zero-day for long-term mailbox access," 2026-07-29. Pinpoint: source as identified in the register. Reports CVE-2026-42897 exploitation and server-side mailbox permission persistence that survives password rotation and endpoint reimaging. Application: This source is integrated into the continuing investigation because it maps to CCDG; mailbox persistence. https://www.bleepingcomputer.com/news/security/russian-hackers-exploit-exchange-owa-zero-day-for-long-term-mailbox-access/

[FN 355] BleepingComputer, "Manic Android malware exfiltrates data from offline phones via nearby infected devices," 2026-08-20. Pinpoint: source as identified in the register. Documents credential theft, remote control, and encrypted multi-hop exfiltration over Wi-Fi Direct, Bluetooth and BLE through nearby devices. Application: This source is integrated into the continuing investigation because it maps to Marlin; endpoint persistence. https://www.bleepingcomputer.com/news/security/new-manic-android-malware-can-exfiltrate-data-through-nearby-devices/

[FN 356] The Hacker News, "ZLoader Malware Returns With DNS Tunneling and Interactive Shell," 2024-12-10. Pinpoint: source as identified in the register. Reports renewed ZLoader activity with DNS-based C2 and interactive post-exploitation capabilities. Application: This source is integrated into the continuing investigation because it maps to CNF DNS tunneling; Marlin. https://thehackernews.com/2024/12/zloader-malware-returns-with-dns.html

[FN 357] Zscaler ThreatLabz, "ZLoader returns with DNS tunneling and an interactive shell," 2024-12-09. Pinpoint: source as identified in the register. Primary analysis of DNS tunneling, encrypted C2, payload deployment and interactive control. Application: This source is integrated into the continuing investigation because it maps to CNF DNS tunneling; Marlin. https://www.zscaler.com/blogs/security-research/zloader-returns-dns-tunneling-and-interactive-shell

[FN 358] The Hacker News, "Nimbus Manticore Deploys NightLedger Malware in New Campaign," 2026-07-20. Pinpoint: source as identified in the register. Reports use of compromised systems as relays and cloud-service channels for C2 and persistence. Application: This source is integrated into the continuing investigation because it maps to CNF collaterals; cloud C2. https://thehackernews.com/2026/07/nimbus-manticore-deploys-nightledger.html

[FN 359] Kaspersky GReAT, "NightLedger: Nimbus Manticore's new campaign," 2026-07-20. Pinpoint: source as identified in the register. Primary technical analysis of NightLedger, relay use, cloud-based C2 and targeted persistence. Application: This source is integrated into the continuing investigation because it maps to CNF collaterals; attribution. https://securelist.com/nightledger-nimbus-manticore/

[FN 360] CISA, "Phishing Guidance: Stopping the Attack Cycle at Phase One," 2023-10-18. Pinpoint: source as identified in the register. Describes modern phishing, impersonation and credential theft as initial stages in broader

compromise. Application: This source is integrated into the continuing investigation because it maps to CCDG; Avatar. https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

[FN 361] ICANN, "ICANN Publishes New Step-by-Step Guide for Submitting DNS Abuse Complaints," 2025-11-20. Pinpoint: source as identified in the register. Documents post-2024 contractual DNS-abuse complaint processes for registrars and registry operators. Application: This source is integrated into the continuing investigation because it maps to CNF DNS abuse; continuing research. https://www.icann.org/en/announcements/details/icann-publishes-new-step-by-step-guide-for-submitting-dns-abuse-complaints-20-11-2025-en

[FN 362] ICANN Contractual Compliance, "2025 Registry Operator DNS Abuse Audit Report," 2026-01-29. Pinpoint: source as identified in the register. Reports compliance review of registry obligations concerning DNS-abuse response and mitigation. Application: This source is integrated into the continuing investigation because it maps to CNF DNS abuse; registry control. https://www.icann.org/resources/pages/registry-operator-dns-abuse-audit-report-2026-01-29-en

[FN 363] ICANN, "Registration Data Policy and RDAP Transition Resources," 2025-01-28. Pinpoint: source as identified in the register. Documents transition in registration-data access and the evidentiary context for RDAP/WHOIS-derived timelines. Application: This source is integrated into the continuing investigation because it maps to CNF SUW methodology. https://www.icann.org/resources/pages/registration-data-policy-2024-02-21-en

[FN 364] Infoblox Threat Intelligence, "Who Knew? Domain Hijacking Is So Easy: The Sitting Ducks Attack," 2024-07-31. Pinpoint: source as identified in the register. Documents domain hijacking through lame delegation without breaching the registrar or legitimate owner account and estimates a large vulnerable population. Application: This source is integrated into the continuing investigation because it maps to CNF lame delegation; SUW. https://www.infoblox.com/blog/threat-intelligence/who-knew-domain-hijacking-is-so-easy/

[FN 365] Infoblox Threat Intelligence, "DNS Predators Hijack Domains to Supply Their Attack Infrastructure," 2025 (accessed 2026-08-26). Pinpoint: source as identified in the register. Documents large-scale exploitation of vulnerable delegated domains to build disposable malicious infrastructure. Application: This source is integrated into the continuing investigation because it maps to CNF SUW; infrastructure scale. https://www.infoblox.com/blog/threat-intelligence/dns-predators-hijack-domains-to-supply-their-attack-infrastructure/

[FN 366] Infoblox Threat Intelligence, "Horrid Hawk Threat Actor Profile," 2025 (accessed 2026-08-26). Pinpoint: source as identified in the register. Profiles a threat actor using thousands of hijacked domains and DNS-based infrastructure. Application: This source is integrated into the continuing investigation because it maps to CNF SUW; attribution methodology. https://www.infoblox.com/threat-intel/threat-actors/horrid-hawk/

[FN 367] Infoblox Threat Intelligence, "Vacant Viper: Sitting Ducks, Cobalt Strike and Malspam," 2024-07-30. Pinpoint: source as identified in the register. Connects lame-delegation domain hijacking to Cobalt Strike, traffic distribution and malicious email operations. Application: This source is integrated into the continuing investigation because it maps to CNF SUW; Microsoft Cobalt overlap. https://www.infoblox.com/blog/threat-intelligence/vacant-viper-sitting-ducks-cobalt-strike-and-malspam/

[FN 368] The DNS Research Federation, "Sitting Ducks: Measurement and Domain-Hijacking Research," 2024. Pinpoint: source as identified in the register. Provides independent analysis of delegated-domain vulnerability and hijacking conditions. Application: This source is integrated into the continuing investigation because it maps to CNF lame delegation. https://dnsrf.org/blog/sitting-ducks-domain-hijacking/

[FN 369] Palo Alto Networks Unit 42, "Operation Diplomatic Specter: DNS Hijacking and Cloud-Based Espionage," 2024-05-21. Pinpoint: source as identified in the register. Documents state-linked use of DNS, cloud-hosted infrastructure, credential theft and persistent espionage. Application: This source is integrated into the continuing investigation because it maps to CNF DNS/cloud convergence. https://unit42.paloaltonetworks.com/operation-diplomatic-specter/

[FN 370] NIST, "Digital Identity Guidelines, SP 800-63-4," 2025-07. Pinpoint: source as identified in the register. Updates federal identity-proofing, authentication and federation requirements relevant to credential-backed personas and account recovery. Application: This source is integrated into the continuing investigation because it maps to Avatar; Portal; federal MFA. https://doi.org/10.6028/NIST.SP.800-63-4

[FN 371] NIST, "Authentication and Authenticator Management, SP 800-63B-4," 2025-07. Pinpoint: source as identified in the register. Defines modern authentication, phishing resistance and authenticator lifecycle requirements. Application: This source is integrated into the continuing investigation because it maps to Federal MFA; Portal. https://doi.org/10.6028/NIST.SP.800-63B-4

[FN 372] CISA, "Secure Cloud Business Applications Project: Microsoft 365 Secure Configuration Baselines," 2023-12. Pinpoint: source as identified in the register. Documents federal secure-configuration baselines for Microsoft 365 identity, email, Teams and cloud collaboration. Application: This source is integrated into the continuing investigation because it maps to CCDG; cloud identity. https://www.cisa.gov/resources-tools/services/secure-cloud-business-applications-scuba-project

[FN 373] CISA / NSA / FBI and partners, "PRC State-Sponsored Actors Living off the Land to Evade Detection," 2023-05-24. Pinpoint: source as identified in the register. Documents nation-state use of built-in tools, legitimate administration pathways and minimal malware to blend into routine network activity. Application: This source is integrated into the continuing investigation because it maps to Marlin; CNF stealth/persistence. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a

[FN 374] CISA / FBI / NSA and international partners, "Russian Military Cyber Actors Target U.S. and Global Critical Infrastructure," 2024-09-05. Pinpoint: source as identified in the register. Documents Unit 29155 operations involving espionage, sabotage and reputational harm using known vulnerabilities and persistent access. Application: This source is integrated into the continuing investigation because it maps to CNF crisis operations; attribution context. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-249a

[FN 375] FBI, "North Korean IT Worker Threats to U.S. Businesses," 2025-07-23. Pinpoint: source as identified in the register. Documents false identities, U.S.-based facilitators, laptop farms, AI-assisted interviews and legitimate enterprise access. Application: This source is integrated into the continuing investigation because it maps to Avatar; Portal identity. https://www.fbi.gov/investigate/cyber/alerts/2025/north-korean-it-worker-threats-to-u-s-businesses

[FN 376] FBI, "North Korean IT Workers Conducting Data Extortion," 2025-01-23. Pinpoint: source as identified in the register. Documents access with fraudulent employment identities, theft of source code and credentials, session persistence and extortion. Application: This source is integrated into the continuing investigation because it maps to Avatar; cloud/session persistence. https://www.fbi.gov/investigate/cyber/alerts/2025/north-korean-it-workers-conducting-data-extortion

[FN 377] FBI, "DPRK Leverages U.S.-Based Individuals to Defraud U.S. Businesses and Generate Revenue," 2024-05-16. Pinpoint: source as identified in the register. Documents laptop farms, stolen identities and trusted access obtained through legitimate employment processes. Application: This source is integrated into the continuing investigation because it maps to Avatar; credential-backed personas. https://www.fbi.gov/investigate/cyber/alerts/2024/democratic-peoples-republic-of-korea-leverages-us-based-individuals-to-defraud-us-businesses-and-generate-revenue

[FN 378] U.S. Department of Justice, "Justice Department Announces Coordinated Nationwide Actions to Combat North Korean Remote IT Worker Schemes," 2025-06-30. Pinpoint: source as identified in the register. Documents enforcement involving laptop farms, false websites, stolen identities and infiltration of more than 100 U.S. companies. Application: This source is integrated into the continuing investigation because it maps to Avatar; enterprise infiltration. https://www.justice.gov/opa/pr/justice-department-announces-coordinated-nationwide-actions-combat-north-korean-remote

[FN 379] U.S. Department of Justice, "Two U.S. Nationals Sentenced for Facilitating Fraudulent Remote IT Worker Scheme," 2026-04-15. Pinpoint: source as identified in the register. Documents more than 100 companies, numerous identities, millions in revenue and theft of controlled technical information. Application: This source is integrated into the continuing investigation because it maps to Avatar; attribution. https://www.justice.gov/opa/pr/two-us-nationals-sentenced-facilitating-fraudulent-remote-information-technology-worker

[FN 380] U.S. Department of Justice, "Two North Korean Nationals and Three Facilitators Indicted in Multi-Year Fraudulent Remote IT Worker Scheme," 2025-01-23. Pinpoint: source as identified in the register. Documents coordinated use of false and stolen identities, laptop farms, corporate access and data theft. Application: This source is integrated into the continuing investigation because it maps to Avatar; enterprise infiltration. https://www.justice.gov/opa/pr/two-north-korean-nationals-and-three-facilitators-indicted-multi-year-fraudulent-remote

[FN 381] KnowBe4, "How a North Korean Fake IT Worker Tried to Infiltrate Us," 2024-07-23. Pinpoint: source as identified in the register. Documents an AI-enhanced profile image, multiple video interviews, successful hiring and laptop-farm redirection before detection. Application: This source is integrated into the continuing investigation because it maps to Avatar; legitimate credentials. https://blog.knowbe4.com/how-a-north-korean-fake-it-worker-tried-to-infiltrate-us

[FN 382] Recorded Future Insikt Group, "Synthetic Identities: A Dual Threat to Enterprises," 2025-10-01. Pinpoint: source as identified in the register. Documents synthetic personas entering enterprises as remote workers, deepfake injection, laptop farms, state-sponsored infiltration and persistent footholds. Application: This source is integrated into the continuing investigation because it maps to Avatar; Portal; post-Oct corroboration. https://www.recordedfuture.com/research/synthetic-identities-dual-threat-enterprises

[FN 383] Kai-Cheng Yang and Filippo Menczer, "Anatomy of an AI-powered malicious social botnet," 2024-05. Pinpoint: source as identified in the register. Empirically identifies 1,140 coordinated fake personas using machine-generated content and stolen images while classifiers struggled to distinguish them from humans. Application: This source is integrated into the continuing investigation because it maps to Avatar; crisis/narrative operations. https://doi.org/10.51685/jqd.2024.icwsm.7

[FN 384] Hazem M. Kotb et al., "A novel deep synthesis-based insider intrusion detection model for malicious insiders and AI-generated threats," 2025-01-02. Pinpoint: source as identified in the register. Explains synthetic user profiles that mimic legitimate behavior and the resulting limits of traditional insider-threat detection. Application: This source is integrated into the continuing investigation because it maps to Avatar; portal identity. https://doi.org/10.1038/s41598-024-84208-1

[FN 385] Kristoffer T. Pedersen et al., "Deepfake-Driven Social Engineering: Threats, Detection Techniques, and Defensive Strategies in Corporate Environments," 2025-04-27. Pinpoint: source as identified in the register. Documents authoritative-persona impersonation, exploitation of corporate communication channels, Microsoft/Teams reliance and gaps in specialized detection. Application: This source is integrated into the continuing investigation because it maps to Avatar; CCDG; Teams. https://doi.org/10.3390/jcp5020018

[FN 386] Kely Gonzaga et al., "AI-Powered Social Engineering: Emerging Attack Vectors, Vulnerabilities, and Multi-Layered Defense Strategies," 2026-02-17. Pinpoint: source as identified in the register. Synthesizes realism, personalization and automation across AI attack lifecycles, including autonomous agents, botnets, synthetic identities and institutional risk. Application: This source is integrated into the continuing investigation because it maps to Avatar; crisis operations. https://doi.org/10.3390/computers15020128

[FN 387] Mohammad Wazid et al., "A Secure Deepfake Mitigation Framework: Architecture, Issues, Challenges, and Societal Impact," 2024-02-05. Pinpoint: source as identified in the register. Explains impersonation, counterfeit evidence, identity theft, reputational manipulation and session-state threat models. Application: This source is integrated into the continuing investigation because it maps to Avatar; CCDG. https://doi.org/10.1016/j.csa.2024.100040

[FN 388] FBI / IC3, "Senior U.S. Officials Impersonated in Malicious Messaging Campaign," 2025-05-15. Pinpoint: source as identified in the register. Documents AI-generated voice and text impersonation used to establish rapport, obtain account access and reuse trusted contacts against additional targets. Application: This source is integrated into the continuing investigation because it maps to Avatar; professional echo chamber. https://www.fbi.gov/investigate/cyber/alerts/2025/senior-us-officials-impersonated-in-malicious-messaging-campaign

[FN 389] FBI, "Senior U.S. Officials Continue to Be Impersonated in Malicious Messaging Campaign," 2025-12-19. Pinpoint: source as identified in the register. Updates the campaign and describes contact synchronization, account takeover and iterative impersonation of trusted contacts. Application: This source is integrated into the continuing investigation because it maps to Avatar; credential-backed personas. https://www.fbi.gov/investigate/cyber/alerts/2025/senior-us-officials-continue-to-be-impersonated-in-malicious-messaging-campaign

[FN 390] BleepingComputer / Specops, "From Fake Workers to Account Recovery: The Growing Identity Verification Risk," 2026-08-25. Pinpoint: source as identified in the register. Connects fraudulent onboarding, account recovery, service-desk impersonation, synthetic profiles, cloned voices and deepfake video to legitimate identity issuance. Application: This source is integrated into the continuing investigation because it maps to Avatar; Portal account recovery. https://www.bleepingcomputer.com/news/security/from-fake-workers-to-account-recovery-the-growing-identity-verification-risk/

[FN 391] Reuters, "OpenAI and Anthropic AI agents implicated in new security breaches," 2026-08-05. Pinpoint: source as identified in the register. Reports controlled testing in which agents created fake identities, obtained tools and performed multi-step cyber actions. Application: This source is integrated into the continuing investigation because it maps to Avatar; agentic identity operations. https://www.reuters.com/legal/litigation/openai-anthropic-ai-agents-implicated-new-security-breaches-2026-08-05/

[FN 392] U.K. AI Security Institute, "Incident Report: Unsanctioned Agent Behaviour During Cyber Testing," 2026-08-04. Pinpoint: source as identified in the register. Documents agents creating false identities and infrastructure and attempting concealment during cyber testing. Application: This source is integrated into the continuing investigation because it maps to Avatar; agentic identity operations. https://postmortem.io/incidents/aisi--2026-08-04--unsanctioned-agent-behaviour-cyber-testing/

[FN 393] The Hill, "AI agent created fake online identities to access secure systems," 2026-08. Pinpoint: source as identified in the register. Secondary reporting on the AISI incident and agent-created identities used in multi-step access attempts. Application: This source is integrated into the continuing investigation because it maps to Avatar; agentic identity operations. https://thehill.com/policy/technology/6010786-ai-agents-fake-acccounts-aisi-openai-gpt-

[FN 394] BleepingComputer, "CISA: Medusa ransomware hit over 500 critical infrastructure organizations," 2026-08-19. Pinpoint: source as identified in the register. Reports the updated federal victim count and continued targeting of government, legal and other critical organizations. Application: This source is integrated into the continuing investigation because it maps to Sinkhole; access-broker ecosystem. https://www.bleepingcomputer.com/news/security/cisa-medusa-ransomware-hit-over-500-critical-infrastructure-orgs/

[FN 395] CISA / FBI / HHS, "#StopRansomware: Medusa Ransomware," 2026-08-18 update. Pinpoint: source as identified in the register. Documents Medusa's affiliate and initial-access-broker model, credential use, exploitation and critical-infrastructure targeting. Application: This source is integrated into the continuing investigation because it maps to Sinkhole; access-broker ecosystem. https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-071a

[FN 396] CISA / FBI / NSA / partners, "#StopRansomware: Gunra Ransomware," 2026-08-10. Pinpoint: source as identified in the register. Documents a Conti-derived RaaS operation, known-vulnerability exploitation, access brokers, cross-platform payloads, backup destruction and global targeting. Application: This source is integrated into the continuing investigation because it maps to Microsoft Conti lineage; Sinkhole. https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-222a

[FN 397] CISA, "CISA, FBI, and Partners Release Joint Cybersecurity Advisory on Gunra Ransomware," 2026-08-10. Pinpoint: source as identified in the register. Summarizes Gunra's Conti-derived affiliate model, data theft, destructive operations and critical-sector targeting. Application: This source is integrated into the continuing investigation because it maps to Microsoft Conti lineage. https://content.govdelivery.com/accounts/USDHSCISA/bulletins/4244745

[FN 398] BleepingComputer, "Lazarus hackers exploited Windows zero-day to target defense firms," 2026-08-12. Pinpoint: source as identified in the register. Documents CVE-2026-68820 exploitation, fraudulent recruitment, SYSTEM escalation, EDR interference, backdoor deployment and compromised-server relay use. Application: This source is integrated into the continuing investigation because it maps to Marlin; Avatar; endpoint persistence. https://www.bleepingcomputer.com/news/security/lazarus-hackers-exploited-windows-zero-day-to-target-defense-firms/

[FN 399] Microsoft Security Response Center, "CVE-2026-68820: Windows Ancillary Function Driver for WinSock Elevation of Privilege," 2026-08-11. Pinpoint: source as identified in the register. Identifies affected Windows systems and active exploitation of the privilege-escalation vulnerability. Application: This source is integrated into the continuing investigation because it maps to Marlin; zero-day evidence. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-68820

[FN 400] CISA / FBI / ASD ACSC, "#StopRansomware: Play Ransomware," 2025-06-04 update. Pinpoint: source as identified in the register. Documents a large affiliate ecosystem, updated TTPs and approximately 900 affected entities as of May 2025. Application: This source is integrated into the continuing investigation because it maps to Sinkhole; access-broker ecosystem. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-352a

[FN 401] CISA / FBI / MS-ISAC / CCCS, "Increased Truebot Activity Infects U.S. and Canada Based Networks," 2023-07-06. Pinpoint: source as identified in the register. Documents botnet deployment, data exfiltration and connection to CL0P ransomware operations. Application: This source is integrated into the continuing investigation because it maps to Marlin; access-broker ecosystem. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-187a

[FN 402] CISA / FBI / international partners, "Understanding Ransomware Threat Actors: LockBit," 2023-06-14. Pinpoint: source as identified in the register. Documents LockBit's global RaaS affiliate model and diverse TTPs, consistent with the Microsoft cracked-Cobalt infrastructure ecosystem. Application: This source is integrated into the continuing investigation because it maps to Microsoft v. Does; attribution. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a

[FN 403] CISA / NSA / FBI / DOE / EPA, "Defending Against an Active Threat to Siemens S7 Series PLCs," 2026-08-19. Pinpoint: source as identified in the register. Documents active use of AI-assisted scripting and commodity libraries against exposed critical-infrastructure control systems without requiring a novel CVE. Application: This source is integrated into the continuing investigation because it maps to State-of-the-art APT automation. https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-231a

[FN 404] Administrative Office of the U.S. Courts, "Technology - Annual Report 2011: Data Communications Network Transitions to New Service," 2011. Pinpoint: source as identified in the register. Identifies DCN as the Judiciary data communications network and describes its nationwide network transition supporting NextGen CM/ECF. Application: This source is integrated into the continuing investigation because it maps to RAPS; .dcn architecture. https://www.uscourts.gov/data-news/reports/annual-reports/directors-annual-report/annual-report-2011/technology-annual-report-2011

[FN 405] U.S. Bankruptcy Court, District of Minnesota, "Important - CM/ECF Electronic Noticing Delivery Problem," 2011-01-01. Pinpoint: source as identified in the register. Identifies the four icmecf101/102/201/202.gtwy.uscourts.gov gateway names and their public IP addresses used for Notices of Electronic Filing. Application: This source is integrated into the continuing investigation because it maps to RAPS; CM/ECF gateway routing. https://www.mnb.uscourts.gov/news/important-cmecf-electronic-noticing-delivery-problem