



PHP2Shell Cyber Emergency and Implications to Existing Legal-Sector Vulnerabilities

Understanding the October 2026 PHP cyber-security emergency and contextual relationships with ongoing investigations into pre-existing legal sector cyber-empirical authority and trust-plane vulnerabilities

*Emergency research assessment and containment guide
for lawyers, law firms, courts, bar associations and service providers*

AUTHORSHIP • CONTRIBUTORS and RESEARCH INTEGRATION • EDITORIAL STAFF

Jay Lewis Farrow, Lead Author and Research Coordinator, Final Editor,
O-V.E.R. INT-DFIR Team, Cyber-N.E.T. Forensics (CNF)
Bridge-Gate E.S.S. Division's Restricted-Access Portal Solutions Unit (RAPS)
Cryptographic Cyber-Defense Group (CCDG), O.R.A.C.L.E. Detection Response Team

Journalists and Research Authors Acknowledged: [Raphael Satter](#) (Reuters) • [John Sakellariadis](#) (POLITICO) • [Matt Burgess](#) (WIRED) • [Sergiu Gatlan](#) (BleepingComputer) • [Swati Khandelwal](#) (The Hacker News) • [Davey Winder](#) (Forbes) • [Lily Hay Newman](#) (WIRED) • [Kevin Collier](#) (NBC News) • [Ionut Arghire](#) (SecurityWeek) • [Eduard Kovacs](#) (SecurityWeek) • [Lawrence Abrams](#) (BleepingComputer) • [Josh Gerstein](#) (POLITICO) • [Leo Marchandon](#) (Reuters) • [Kanjyik Ghosh](#) (Reuters) • [Rajveer Pardesi](#) (Reuters) • [Waqas](#) (HackRead) • [Greg Otto](#) (CyberScoop) • [Lindsay Clark](#) (The Register) • [Sarah Perez](#) (TechCrunch) • [CJ Moses](#) (AWS Security Blog) • [John Blackbourn](#) (WordPress.org)

Contents

The report begins with the emergency and the systems behind an ordinary website. The analysis then follows the research record into practical containment, court access, restoration and working checklists.

October 2026: the PHP2Shell emergency and the legal-sector response	4
How the emergency developed: from the earlier defect to the October 21 patches	4
What an affected website can expose in legal and judicial work	5
Purpose of this assessment and the research assembled for the response.....	6
Immediate actions for the responsible manager or administrator	7
A. Identify who operates the website and confirm the correction	7
B. Reduce exposure while keeping a usable contact route	7
C. Preserve the records of what happened	7
D. Check website additions and connected accounts.....	7
E. Protect instructions, filings and matters with approaching deadlines	7
F. Confirm that recovery reaches beyond the visible page	8
1. How a legal-sector website actually operates	8
1.1 The website, its host and the software running it	8
1.2 Accounts, permissions and connections between services	9
1.3 Website addresses, mail routing and encrypted connections.....	9
1.4 Reading signs of unauthorized activity and preserving evidence	10
1.5 The research record used in this report	11
1.6 Following connected events through time	11
2. How PHP2Shell works and what the patches correct	12
2.1 The first defect: interrupted request handling	12
2.2 The second defect: information left over from an earlier request	12
2.3 Which PHP installations require attention	13
2.4 The research and disclosure chronology behind the emergency	13
2.5 Attack observations and the period that requires investigation	14
2.6 National reporting and guidance relevant to the response.....	14
3. Establishing and verifying repairs across every website	15
3.1 Matching a website to the corrected PHP release	15
3.2 Checking every installation behind the website	16
3.3 Confirming what the hosting provider has done	17
3.4 Temporary restrictions while the correction is installed	17
3.5 The website owner's first check	18
3.6 Deciding whether to take a website offline	18
4. Rank Math PRO: examining a separate contaminated download	19
4.1 The affected download window and release history	19
4.2 Establishing whether the downloaded software ran	19
4.3 Identifiers to give the hosting provider or responder	20
5. Current incidents and the trusted connections they expose.....	21
5.1 Reconstructing control of cloud-hosted website and DNS services	22
6. From early forensic findings to the current legal-sector response model	23
6.1 Marlin Technology: the early computer and account findings	23
6.2 The October 22, 2025 CNF integrated investigation.....	23
6.3 Team B: structured records of portal activity	24
6.4 RAPS: following a document through the filing process.....	24
6.5 CCDG: examining authenticated communications	24
6.6 Avatar and ORACLE: identity, instructions and accepted authority	25

6.7 Sinkhole and court-audit research: availability and record custody.....	25
6.8 The September 2026 assessment: adaptation after the first investigation.....	26
6.9 Civil cyber-disruption research: preserving access to an effective remedy.....	26
6.10 The integrated response finding.....	27
7. Microsoft court evidence and historical infrastructure matches.....	27
7.1 The case, the declarations and the court's order	27
7.2 The recorded address comparisons.....	27
7.3 Reading a technical declaration with its exhibits and footnotes	28
7.4 Preservation and continuing relief under the permanent injunction	29
8. Establishing who authorized an email or online instruction	29
8.1 The separate functions of email authentication.....	29
8.2 Documented account and token abuse	30
8.3 Reconstructing the message and its consequences	30
9. Following a document from submission to institutional action	31
9.1 Reconstructing the recorded steps.....	31
9.2 Two source-specific applications	31
9.3 Correcting the input and the resulting record	32
10. Tracing an event to its mechanism and operator	32
10.1 Four stages of attribution	32
10.2 Findings and the action each supports	32
10.3 Documented commercial objectives and institutional consequences	33
11. Naming observed attack techniques with MITRE ATT&CK.....	33
12. Emergency response: preserve, contain and restore	35
12.1 First 30 minutes — establish control and stop avoidable harm	35
12.2 Minutes 30–120 — preserve the evidence that will otherwise disappear	36
12.3 Hours 2–6 — close runtime paths and remove persistent authority	36
12.4 Hours 6–24 — reconstruct the connected environment.....	37
12.5 Hours 24–72 — restore with measured acceptance criteria	37
13. Keeping legal and institutional work functioning during the response	38
13.1 Law firms, lawyers and litigation-support providers	38
13.2 Fiduciaries, accountants, advisers and other professionals	38
13.3 Insurance agencies, brokers and claims operations	39
13.4 Privately held companies and equity administration	39
13.5 Managed service providers and portfolio-wide operators	39
13.6 Court offices, clerks and bar associations: intake and verified public directions	40
13.7 Professional directories, firm reputation and public-facing identity	41
13.8 Specific role of NACABAR and other professional associations	41
13.9 Locating official guidance and court-specific instructions	41
14. Completion tests for restored websites, accounts and records	42
Appendix A. Recording indicators and connecting events	43
A.1 Maintaining three incident-specific indicator collections	43
A.2 Event record template.....	43
Appendix B. Hosting-provider and IT attestation request	44
Appendix C. Examination map for the research corpus.....	44
Appendix D. Source records and hyperlink status	45
Appendix E. Emergency decision and evidence-preservation checklists	46
E.1 Initial exposure and decision checklist	46
E.2 Legal-workflow continuity: additional checks for counsel and courts.....	47
E.3 Connecting warning signs to the affected system	47
E.4 A concise request for the responsible provider or court office	48
Endnotes and source register	48

October 2026: the PHP2Shell emergency and the legal-sector response

On October 21, 2026, the PHP security project released emergency corrections for two critical weaknesses in the software that operates many of the world's websites. An attacker can exploit either weakness to make a vulnerable website server execute instructions without first signing in. Depending on the server's permissions, the result can include exposure of information, alteration of website content, or access to credentials used by other services. Governments, hosting companies and cybersecurity teams moved to patch affected servers, and some public websites were temporarily taken offline while their exposure was addressed. [\[FN 1\]](#) [\[FN 2\]](#) [\[FN 26\]](#) [\[FN 108\]](#)

The affected software is PHP, a programming language that has been used to build interactive websites since the 1990s. WordPress and many other publishing systems rely on it to assemble pages, process forms, retrieve information and communicate with databases. When a person opens a website, a server—a computer maintained by the organization or its hosting company—runs the necessary PHP instructions behind the page. The security emergency concerns that server-side program. Updating a webpage or a WordPress plugin does not replace the PHP program installed by the server administrator. [\[FN 1\]](#) [\[FN 10\]](#)

How the emergency developed: from the earlier defect to the October 21 patches

The chronology begins before this week. The PHP Foundation describes an earlier memory-safety concern associated with work following a 2024 audit. By August 2026, security researchers had demonstrated practical routes to exploiting the problem. On October 20, information about two vulnerabilities circulated publicly ahead of the coordinated release. The PHP project accelerated its announcement and published corrected software on October 21. The two weaknesses are identified as CVE-2026-109618 and CVE-2026-109619. A CVE number is a reference assigned to a particular security defect so that administrators can identify the exact correction they need. [\[FN 1\]](#) [\[FN 2\]](#) [\[FN 3\]](#) [\[FN 4\]](#) [\[FN 108\]](#)

The initial corrected versions were PHP 8.2.35, 8.3.36, 8.4.27 and 8.5.12. A patch is a software correction that closes an identified defect. The hosting company or server administrator must place the corrected PHP package into service and replace older running copies of the program. A site owner can verify which PHP version the site uses through authenticated administration tools, then obtain a written answer identifying the fixed build and the domains covered. Some operating-system providers supply documented corrections to older package versions; their advisories identify the corrected build even when its leading version numbers look different. [\[FN 1\]](#) [\[FN 10\]](#) [\[FN 17\]](#)

The United States Cybersecurity and Infrastructure Security Agency (CISA), international government response teams and the PHP project issued urgent patching guidance. Both weaknesses received a critical severity rating of 9.2 on the Common Vulnerability Scoring System's ten-point scale. The rating concerns the seriousness of the technical defects. The operational question for each organization is whether its internet-facing services use an affected PHP installation, whether a corrected build is running, and whether activity before that correction requires an intrusion examination. [FN 2] [FN 3] [FN 5] [FN 6] [FN 7]

The investigation must begin before the public patch date. Amazon Web Services (AWS) reported that its MadPot research network recorded an attempted PHP2Shell exploit on October 17, four days before public disclosure. MadPot consists of monitored systems used to observe hostile internet activity. AWS subsequently recorded additional attempts and concluded that the vulnerabilities were being exploited broadly. These observations establish early attack activity in AWS's research environment. For any particular law firm, court office or association, the relevant server logs and account records establish whether attempted access reached its systems. Those records must be preserved while administrators patch and restrict exposure. [FN 13] [FN 14] [FN 15] [FN 48] [FN 108] [FN 109]

What an affected website can expose in legal and judicial work

A website's immediate exposure extends as far as the permissions granted to the program operating it. A law-firm site may hold client-intake submissions, a database password, an email-service credential or the ability to update public instructions. A clerk's public information site may publish the directions, forms and contact details that people rely upon before reaching a separately administered filing portal. A bar association may connect its website to registration, membership and course services. The person responsible for each site must identify which information the web-server program can read, which records it can change and which connected services its credentials can instruct. [FN 41] [FN 50]

Those connections create distinct professional consequences. Unauthorized changes to an intake address can prevent a prospective client from reaching a firm. A substituted payment instruction can divert funds. A changed notice recipient can leave an attorney unaware of a filing or deadline. Altered professional-directory contact information can misdirect inquiries long after the underlying site is repaired. Such events require verification of both the technical action and the version of the instruction, communication or record accepted by the recipient. The evidence should connect the change to its actual account, time and downstream result. [FN 43] [FN 86] [FN 87] [FN 88]

Courts, clerks and regulatory bodies often operate public websites separately from restricted filing and records systems. Those boundaries are determined by the applications, contracts, accounts and interfaces actually in use. The first task is to check public filing

directions and contact details against controlled institutional records; the second is to examine any connection through which the affected website could write to a separate service or use its credentials. For urgent filings, the applicable court rules and clerk-confirmed procedures continue to govern, including when a document delivered in person is later digitized and entered into the electronic case system. [FN 50] [FN 86] [FN 103]

Purpose of this assessment and the research assembled for the response

O-V.E.R. INT-DFIR is a collaborative private-sector research and cyber-defense team preparing emergency incident-response analysis and containment guidance. This edition addresses the October 2026 PHP2Shell disclosure and the particular responsibilities of law firms, court offices, bar associations and their service providers. Digital forensics is the preservation and examination of computer and communications records to reconstruct events. Incident response is the coordinated work of closing unauthorized access, protecting ongoing operations and restoring systems and records that others depend upon.

The work proceeds in three stages. The technical owner identifies and corrects every affected website installation, then inspects the period of exposure for evidence of unauthorized activity. The incident team removes any persistence, credentials or permissions established during that period. The professional owner then reconciles sensitive messages, filing instructions, client submissions, payment directions and institutional records with their verified originals. A functioning homepage demonstrates service availability; completion also requires trusted accounts and accurate consequential records. [FN 1] [FN 21] [FN 48] [FN 86] [FN 87] [FN 88]

The investigative research cited in this report supplies methods for each of those stages. Marlin Technology examined early device, account and domain-administration evidence. Cyber-N.E.T. Forensics (CNF) integrated computers, credentials, internet routing, communications and legal-procedure records; Team B separately preserved structured portal observations. The Restricted-Access Portal Solutions Unit (RAPS) examined how a submitted document moves through intake, docketing and delivery. The Cryptographic Cyber-Defense Group (CCDG) studied messages that pass technical authentication while carrying unauthorized instructions. O.R.A.C.L.E. traced how identities and communications become accepted institutional actions. CNF's Avatar and Sinkhole research examined professional identity, domain control and publication access. Section 6 introduces the reports individually and identifies the operational findings drawn from each. [FN 81] [FN 82] [FN 83] [FN 84] [FN 85] [FN 86] [FN 87] [FN 88] [FN 90]

The immediate response priorities follow. Section 1 explains the website, hosting, account and communications systems in ordinary language. Sections 2–5 examine the PHP emergency and related software incidents. Sections 6–11 reconstruct the forensic research and show what evidence can establish the reach of an intrusion. Sections 12–14 assign

containment and restoration responsibilities. The appendices provide checklists and requests that a managing partner, clerk, association director or hosting provider can put to work without first reading the entire technical analysis.

Immediate actions for the responsible manager or administrator

A. Identify who operates the website and confirm the correction

Locate the hosting contract and name the administrator responsible for the server. Ask that person to identify the PHP version serving every production website and every test or secondary site. The first corrected releases are 8.2.35, 8.3.36, 8.4.27 and 8.5.12; some providers supply their own documented corrections to older packages. Record the provider's answer, the installation time and the domains covered. Section 3 explains how to read that answer. [FN 1] [FN 17] [FN 18] [FN 19]

B. Reduce exposure while keeping a usable contact route

When a vulnerable service cannot be corrected promptly, have the responsible administrator restrict public access or take it offline while the correction is prepared. Keep independently verified telephone and contact arrangements available for clients and other affected users. The person directing the technical restriction and the person responsible for deadlines and client communication should make that decision together. Section 3.6 sets out the shutdown and reopening checks. [FN 6] [FN 7] [FN 102] [FN 106]

C. Preserve the records of what happened

Ask the provider to retain website activity records, account changes, file histories and copies of the site before cleanup overwrites them. These records are often called logs: dated entries showing what a computer or account did. Keep original messages, submitted documents, receipts and notices as well. Preservation and urgent restriction can proceed together, with the responder recording the time and effect of every change. [FN 48] [FN 49]

D. Check website additions and connected accounts

A plugin is an additional program installed to give a website a particular function. Rank Math PRO, a WordPress search-optimization plugin, is involved in a separate software-distribution incident. Certain copies downloaded during October 15–16 contained malicious software. Where an affected copy was activated, the vendor directs full site recovery and replacement of exposed account secrets. Section 4 identifies the precise acquisition window and the records needed to determine whether a site received one of those copies. [FN 20] [FN 21] [FN 23] [FN 24]

E. Protect instructions, filings and matters with approaching deadlines

Identify transactions for which an incorrect instruction would cause immediate loss: settlement payments, confidential disclosures, urgent filings, notices and account recovery. Verify changed instructions with the authorized person through a contact route established independently of the questioned message. Where court access is affected, contact the clerk using a verified number, obtain the applicable emergency procedure, and retain confirmation of what was accepted and how it will be handled. Section 13.6 addresses paper delivery and later scanning into court systems. [FN 43] [FN 86] [FN 88] [FN 103] [FN 104]

F. Confirm that recovery reaches beyond the visible page

Assign one owner to the technical repair and another to reconciliation of the affected business or legal records. Before ordinary service resumes, verify the corrected software, removal of unauthorized access, control of accounts, accuracy of consequential records and continuing monitoring. These five completion checks appear in Section 14. The investigation of the operator can continue while the organization carries out the protective actions already supported by the evidence. [FN 48] [FN 49] [FN 59] [FN 81] [FN 82] [FN 90]

1. How a legal-sector website actually operates

1.1 The website, its host and the software running it

A website consists of information and instructions stored on a server. When someone opens a page or submits a form, the server receives a request and returns a response. WordPress is a content-management application: it lets authorized users publish pages, add photographs and operate forms without writing the underlying program. PHP supplies part of the machinery carrying out those instructions. The installed PHP program is called the runtime or interpreter. Both terms refer here to the software executing PHP instructions on the server. [FN 1] [FN 10]

A hosting provider supplies the server, its operating environment or both. The operating system manages the computer's files, memory, users and running programs. The provider may maintain that operating system and PHP while a separate web designer maintains WordPress. In another arrangement, the organization's own administrator manages all of them. The service agreement and actual access arrangements identify who can install the emergency correction. [FN 17] [FN 18] [FN 19] [FN 38] [FN 39]

A running copy of a program is a process. A web worker is a process assigned to handle website requests. Several workers may operate together as a pool, allowing a site to serve many visitors. Installing a corrected program on disk and replacing the workers still using

the older program are separate steps. A provider's completion record should establish both. [FN 1] [FN 3] [FN 19]

An organization may have several versions or branches of PHP in use. A branch is a maintained line such as PHP 8.2 or PHP 8.4; a maintenance release adds the final number, such as 8.2.35. A package or build identifies the particular software prepared by a provider. A backport is a correction applied to an older package, sometimes without changing its familiar leading version number. The full package revision and the vendor's advisory show whether that correction includes the two defects under review. [FN 1] [FN 17] [FN 37]

A staging site is a separate copy used for testing. A container is a packaged application environment, and a container image is the stored package from which it is launched. An old test site or an older running container can remain exposed after the main site is corrected. The inventory must therefore identify each active installation, its owner and the provider or administrator responsible for changing it. [FN 17] [FN 19] [FN 38] [FN 39]

1.2 Accounts, permissions and connections between services

A credential is something a system accepts as evidence of access authority, such as a password or a software access key. After a person signs in, a session lets that person continue working without entering a password for each action. A token is a digital value that a service accepts to recognize a session or authorize a particular action. A session cookie is one way a browser stores such a value. Attackers who obtain these items can act through the permissions assigned to the account. [FN 57] [FN 69] [FN 76] [FN 77]

An application programming interface, or API, is a defined way for one program to ask another service to do something. A website may use an API to send mail, upload a file or record an intake request. An API key or application secret is a credential used for that connection. A service account is an identity used by software rather than an individual person. These connections explain how access to one website can lead to actions elsewhere when the website holds credentials with wider permissions. [FN 50] [FN 54] [FN 57]

Multifactor authentication, abbreviated MFA, requires more than one form of verification at sign-in. A recovery address, recovery device or delegated permission provides another route to obtain or exercise access. Delegation means that an account grants another person or application permission to act. OAuth is a commonly used system for granting applications access to services without giving them the user's password. Its grants and tokens need examination alongside passwords during recovery. [FN 57] [FN 66] [FN 70] [FN 77]

Cloud services are computing, storage or communications services operated in a provider's environment. A tenant is an organization's allocated account environment within such a service. Administrative accounts control the settings and permissions inside that

environment. The collection of identities and controls that decides who may change systems is called the control plane. The investigation follows the actual account authority, including any permission a website possesses to send email, change records or reach another service. [FN 50] [FN 54] [FN 55] [FN 90]

1.3 Website addresses, mail routing and encrypted connections

A domain is a name such as an organization's website address. A subdomain is a named part of it, often used for a portal or a separate service. The Domain Name System, or DNS, translates names into the network destinations used by computers. An Internet Protocol address, or IP address, identifies a network destination. The registrar maintains the domain's registration; the authoritative nameservers publish its DNS answers. The DNS records managed together for a domain form a hosted zone. [FN 42] [FN 54] [FN 55]

Different records perform different jobs. NS records identify nameservers. A and AAAA records supply network addresses. CNAME records identify another name to follow; provider-specific alias records can serve a related routing function. MX records identify where inbound email should go. TXT records hold text used for verification and other policies. An SOA, or Start of Authority record, contains administrative information for the zone. The provider's change history is needed to identify which record changed, when, and under whose account. [FN 42] [FN 51] [FN 54] [FN 55]

Amazon Web Services, or AWS, operates several distinct services. Route 53 manages DNS. CloudFront distributes website content through a content-delivery network, or CDN, which supplies content from servers between the visitor and the original host. AWS Identity and Access Management, or IAM, defines who can act on resources. CloudTrail records supported account and API activity. These names identify different functions in the investigation; the relevant record is the specific customer resource, account permission and change event. [FN 54] [FN 55] [FN 90]

Transport Layer Security, or TLS, protects information while it travels between a browser and a server. The browser's padlock reflects that encrypted connection. A certificate helps the browser validate the connection's identity. The application then processes the information after receipt, where account permissions and document handling determine what happens next. Section 8 examines those separate stages and the corresponding checks for email. [FN 27] [FN 50] [FN 86]

1.4 Reading signs of unauthorized activity and preserving evidence

An endpoint is a computer, phone, server or other operating device being examined. An artifact is a preserved item from that environment, such as a file, a message, a configuration entry or a log record. Telemetry means the activity measurements collected by systems and security tools. A hash is a calculated digital fingerprint of a file; comparing hashes helps

determine whether two copies contain identical bytes. Chain of custody records who acquired, stored, transferred or examined an item. [FN 49] [FN 81] [FN 82]

An indicator of compromise, or IoC, is an observable item associated with unauthorized access, such as an identified malicious file or an unauthorized administrator account. An indicator of attack, or IoA, is behavior or a sequence of actions indicating an attack, such as unusual requests followed by a server starting an unauthorized command. Tactics, techniques and procedures, abbreviated TTPs, describe the objective, method and working steps of an operation. Their practical value comes from relating the observed behavior to the affected system, time and consequence. [FN 49] [FN 65] [FN 67] [FN 90]

An exploit is the method used to take advantage of a vulnerability. Remote code execution, or RCE, means causing another computer to run instructions from a remote location. Malware is software used for unauthorized or harmful activity. A web shell is a server-side program that gives an intruder a command interface. Persistence is an arrangement that lets an intruder return or continue acting after an initial session ends. A command-and-control connection, abbreviated C2, carries instructions or results between an attacker and controlled software. [FN 2] [FN 3] [FN 65] [FN 72] [FN 80]

A web application firewall, or WAF, examines website traffic and applies rules intended to block unwanted requests. The origin is the server actually providing the application behind any protective or distribution service. Monitoring must cover both the protective layer and the origin. A request blocked at the first layer and a request that reached the server produce different evidence and different follow-up tasks. [FN 13] [FN 16]

In the legal setting, a workflow is the series of steps that turns an instruction or submission into an accepted result. A state is the recorded position at a particular step: received, routed, served, filed or approved. ORACLE uses the term authority rail for the connected identities, credentials, communications and records through which an action acquires institutional force. The response compares each transition with its source document, authorized participant and recorded time. [FN 86] [FN 88] [FN 89]

1.5 The research record used in this report

The original research edition assembled 15 artifacts: 13 PDFs totaling 1,339 pages and two Word documents. The collection includes court materials, expert reports, later forensic syntheses, a published private-equity article and the investigative protocol. Its examination record identifies narrative sections, appendices, endnotes, tables and source-object comparisons. Appendix C preserves the edition and page locators used for that work.

The October 21 register contains 80 external source records. Notes [FN 94]–[FN 107] add the journalism and institutional guidance incorporated in the October 22 publication revision. Thirty-five entries in the original register were published or updated during

August 21–October 21, 2026. The notes retain publication and update dates separately, together with their source-access records. The incident-specific Forge documentation is recorded without assigning a separate publication date.

The source roles are complementary. A vendor advisory identifies the defect and correction. Provider telemetry describes activity observed within that provider's systems. A declaration supplies a witness's methods and findings. An order sets out the court's directions. An expert report brings its own observations and analysis into the chronology. The endnotes explain the proposition supported by each source and the section in which it is used. [FN 2] [FN 13] [FN 59] [FN 62] [FN 81] [FN 90]

1.6 Following connected events through time

The examination begins with the last authenticated state, then follows the change, the account or credential used, the technical method, the next institutional action and the resulting consequence. Evidence collected at different stages is placed on the same chronology. A message-receipt discrepancy is examined alongside the account and routing history already established for that environment. An account event is examined alongside the filing or payment it affected. [FN 49] [FN 86] [FN 89] [FN 93]

The analysis also tracks how sources depend on one another. A later report quoting a spreadsheet carries forward that spreadsheet's observation. A separately collected message header, a provider's account log and an original filing receipt add different observations. Their agreement can strengthen a finding because each records a different part of the sequence. This approach preserves both the combined significance of connected evidence and the identity of the underlying sources. [FN 49] [FN 87] [FN 90]

CNF calls the sustained operation examined in its research cAPTure-to-Kill. An advanced persistent threat, or APT, is a sustained adversarial effort that maintains access and adapts its methods to pursue an objective. CNF's model concerns control over the systems through which professional and legal outcomes are produced. Its continuity is assessed through access relationships, timing, records and objectives, including periods when the actor replaces a domain, a tool or an account. Sections 6 and 10 apply that research to the response decisions in this report. [FN 80] [FN 82] [FN 90] [FN 91]

2. How PHP2Shell works and what the patches correct

2.1 The first defect: interrupted request handling

PHP uses temporary working memory while preparing a website request. Some internal records are built in stages. If the program reaches its memory limit at a particular stage, its error-handling routine can stop that preparation before the records are complete. The later

cleanup routine can then treat incomplete records as usable data. The advisory calls this out-of-memory corruption and identifies it as CVE-2026-109618. [FN 2]

An attacker can deliberately shape a request to reach this failure and turn the corrupted data into unauthorized instructions. The demonstrated Apache mod_php path reaches the condition before the website's own application code runs. Apache is web-server software; mod_php is the component that runs PHP within it. The resulting access begins with the permissions assigned to that server process, including the files and connected services it is allowed to use. [FN 2] [FN 12]

2.2 The second defect: information left over from an earlier request

A web worker normally releases temporary information when it finishes a request. The second defect can leave the worker retaining a reference to memory that has already been released. When that worker handles another request, it can follow the old reference and use information that no longer belongs to the earlier task. This is a use-after-free condition. The advisory identifies the defect as CVE-2026-109619 and describes information disclosure, process failure and remote code execution. [FN 3]

The request sequence therefore belongs in the investigation. Preserve the requests before and after the error, the identity of the worker where available, and any resulting file, account or process change. A load balancer distributes requests among servers; a process pool distributes work among running workers. Those arrangements affect which requests reach the same worker. Recording them lets the analyst connect an earlier memory error with a later unauthorized action. [FN 3]

2.3 Which PHP installations require attention

The PHP project places web-serving PHP installations within the remediation scope. These include PHP-FPM, which manages PHP worker processes; Apache mod_php; the Common Gateway Interface (CGI), one way a web server runs an application; and installations using FrankenPHP or LiteSpeed. A device or packaged application can contain its own PHP installation, so the inventory also needs to cover vendor appliances and bundled software. CERT-FR, France's government computer-security response service, issued a corresponding notice on October 21. [FN 1] [FN 7] [FN 8] [FN 9]

The advisories describe different paths through different server arrangements. SAPI, the Server Application Programming Interface, is PHP's connection to the surrounding web-server environment. The out-of-memory advisory explains FPM startup handling that differs from the mod_php path. The PHP Foundation's October 21 account also records confirmed FPM execution through application-level paths. Administrators should retain those configuration details when examining an incident and apply the PHP correction across the affected serving environments. [FN 2] [FN 4]

Both defects carry a 9.2 rating under version 4.0 of the Common Vulnerability Scoring System, or CVSS. That scoring method summarizes severity and the conditions relevant to exploitation. The operational response is to identify the serving software, apply the appropriate correction and inspect the affected environment. Compatibility testing should cover the website's forms, sign-in functions and connected services so that emergency repair preserves essential operations. [\[FN 2\]](#) [\[FN 3\]](#) [\[FN 6\]](#)

2.4 The research and disclosure chronology behind the emergency

The PHP Foundation traces the first memory-handling concerns to the period following a 2024 audit. Calif reported a concrete exploitation path on August 11, 2026; Wiz separately described discoveries and application-level demonstrations during August. The coordinated release was initially scheduled for October 22. Once the vulnerability identifiers and some technical details circulated publicly on October 20, the PHP team brought publication forward to October 21. The chronology shows why administrators had little time between public notice and a working correction, even though the underlying defects predated their disclosure. [\[FN 4\]](#) [\[FN 11\]](#) [\[FN 12\]](#)

The disclosure process included separate events: identifier leakage, release of demonstration materials, working exploit research and public patch distribution. Each has its own timestamp. In particular, AWS later identified an attempted exploit in MadPot observations on October 17. The relevant investigation period therefore begins with the earliest observable activity, not with the day the corrected PHP packages were installed. A website operator should preserve the applicable logs from at least October 17 and extend the review further back when its own evidence, threat intelligence or provider history supports doing so. [\[FN 4\]](#) [\[FN 108\]](#)

The repair decision is straightforward. Identify the PHP package running behind each exposed website; install the corrected build or documented supported backport; replace older running worker processes; then examine the period of exposure for successful access, changed files, new account authority and altered business records. A clean post-patch scan establishes only its own inspection result. The service, identity and record checks in Sections 12–14 complete the response. [\[FN 5\]](#) [\[FN 6\]](#) [\[FN 11\]](#) [\[FN 13\]](#)

2.5 Attack observations and the period that requires investigation

By October 21, Reuters documented websites being taken offline as European authorities and administrators evaluated the emergency. The PHP project released corrected code that day, while security vendors measured attempts to exploit exposed servers. AWS subsequently confirmed that at least one attempt reached its monitored MadPot environment on October 17 and reported wider exploitation after disclosure. Those are dated observations of attack traffic. The effect on any particular customer or court

environment must be reconstructed from that environment's own retained activity and account records. [FN 25] [FN 26] [\[FN 108\]](#)

Cloudflare reported active attack traffic against the vulnerabilities and adaptation in the requests reaching its protections. watchTowr published observations from its research honeypots; Huntress reported its own time-limited customer observations on October 21. These sources cover different monitored populations. The response team should preserve web requests, errors and worker activity, together with subsequent file and credential changes, rather than waiting for a named-victim list. The initial search window extends back to October 17 in light of AWS's later disclosure. [FN 13] [FN 14] [FN 15] [\[FN 108\]](#)

2.6 National reporting and guidance relevant to the response

Reuters coverage described the precautionary withdrawal of government websites while the security fixes were prepared. WIRED's reporting followed both the worldwide patching effort and the later discovery that AWS sensors had recorded exploitation attempts four days before disclosure. BleepingComputer reported the actual corrective releases; Forbes, HackRead and The Hacker News explained the urgency to website owners and security teams. The technical conclusions in this assessment are anchored to the PHP project and primary vendor observations, while those reports document how quickly public institutions and hosting operators were required to act. [FN 25] [FN 26] [FN 94] [FN 96] [FN 97] [FN 98] [FN 100] [\[FN 109\]](#)

A separate journalism record addresses the legal sector's existing exposure. POLITICO's 2025 investigation by John Sakellariadis and Josh Gerstein examined the federal judiciary's compromised case-management environment. The Administrative Office of the U.S. Courts separately acknowledged persistent attacks and changes in the handling of sensitive filings. The judiciary events and the current PHP defects involve different timelines and systems. In this report they are examined together for one operational purpose: restoring reliable instructions, filings, notices and records across services with different administrators. BBC and CNBC items supplied for the current news cycle remain in the source notes for provenance and follow-up. [FN 63] [FN 95] [FN 99] [FN 101]

The American Hospital Association's October 21 alert addressed institutional management as well as technology teams. The U.S. National Security Agency advised that exposed services unable to receive prompt updates be taken offline until mitigation can be completed. For legal-sector organizations, that decision must include a verified client contact route, an assigned incident owner and a court- or regulator-approved continuity procedure for pending obligations. [FN 102] [FN 105]

3. Establishing and verifying repairs across every website

3.1 Matching a website to the corrected PHP release

Use the PHP branch already assigned to the application to locate its first corrected release below. The technical owner should record the full installed package and confirm the running workers use it. For a vendor-maintained older build, attach the vendor's statement identifying the correction and the covered defects. [FN 1] [FN 17]

PHP branch	Upstream fixed release	Required verification
8.5	8.5.12	Installed package and running web workers both updated.
8.4	8.4.27	Check every selected handler and pool.
8.3	8.3.36	Check separate OS packages, alternate repositories and containers.
8.2	8.2.35	Patch now; plan migration within the branch's remaining support lifecycle.
7.x, 8.0, 8.1	No new supported upstream release for these branches	Use a specifically verified vendor backport or move to supported PHP; isolate an unremediated runtime.

The table identifies the first upstream corrections: the versions released by the PHP project itself. The project also supplied minimal source backports for PHP 7.4, 8.0 and 8.1. Providers maintaining older packages must identify the specific correction they applied and the package that contains it. A backport supplies a defined fix; the organization should separately record its plan for moving unsupported software to a maintained branch. [FN 1] [FN 37]

Canonical's Ubuntu advisory illustrates how to read a provider package. Ubuntu is a Linux operating-system distribution. Its USN-8948-1 notice lists corrected revisions including 8.3.6-0ubuntu0.24.04.13 for Ubuntu 24.04 and 8.1.2-1ubuntu2.28 for Ubuntu 22.04. The leading version digits remain older because the vendor applied the correction within its maintained package. The full revision, package source and advisory mapping supply the remediation record. [FN 17]

3.2 Checking every installation behind the website

One corrected PHP installation can serve several websites. A single hosting account can also use different PHP branches for different domains, separate worker pools, test sites and scheduled jobs. Cron is a scheduler used to run tasks automatically, including tasks that may invoke a separate PHP program. The inventory should follow provider, account, server or container, software package, worker arrangement and domain. Record a disposition for each installation reachable from the internet. [FN 18] [FN 19] [FN 38] [FN 39]

For each WordPress installation, record the domain, document root, database, responsible administrator, hosting account and actual web-served PHP version. The document root is the server directory holding the site; the database stores structured content and settings. A handler is the mechanism connecting the web server to its PHP process. WordPress's Site Health display helps identify the runtime serving that site. A command-line version check can describe a different installed program. Keep diagnostic information inside authenticated administration tools rather than publishing a phpinfo page that exposes server details. [FN 10] [FN 38] [FN 39]

The hosting arrangement determines who can perform the work. Shared hosting places the server under the provider's administration. A virtual private server, or VPS, gives a customer a separately managed server environment. cPanel and Plesk are tools for administering domains and server settings. A reseller may sell hosting while a different provider maintains PHP. Use the table to assign the technical action and the completion evidence to the correct party. [FN 17] [FN 18] [FN 19] [FN 38] [FN 39]

Environment	Infrastructure owner	Site owner's closure evidence
Shared hosting	Provider installs the corrected runtime and restarts affected workers.	Written account-specific confirmation and a per-domain runtime check.
cPanel / reseller	Provider or root administrator installs packages; account settings select domain runtimes.	MultiPHP assignments and inherited defaults reconciled for all domains.
Plesk	Server/subscription administrator manages packages and handlers.	Each domain's version, handler and pool identified and verified.
Managed WordPress	Provider normally handles infrastructure; customer handles remaining application obligations.	Provider notice tied to the actual account and sites, plus application recovery where indicated.
VPS / dedicated server	Administrator updates every installed serving package and restarts affected services.	Package provenance, service restart and web-path validation recorded.
Containers / images	Image or platform owner rebuilds and redeploys workloads.	New image digest, deployment inventory and termination of old workers confirmed.

Responsibility follows the actual hosting arrangement, not the public brand name on the website. For each domain, obtain the infrastructure owner's confirmation of the corrected build, the date it entered service and the worker restart or replacement. Include staging sites, secondary domains and externally reachable server paths. The table supplies a starting allocation of duties; the provider's final account-specific record must identify every service covered and each remaining exception. [FN 10] [FN 17] [FN 18] [FN 19] [FN 38] [FN 39]

3.3 Confirming what the hosting provider has done

SiteGround published a statement describing platform-level protection. Its customers should tie that statement to their own domains and accounts, recording the installed correction and remaining exceptions. Laravel Forge describes a different maintenance boundary: its automatic security-update mechanism does not update its separately sourced PHP packages. The server administrator must carry out that change. The same underlying operating system can therefore require different action depending on where PHP was obtained and who maintains it. [FN 18] [FN 19]

In cPanel, record the full package behind each selected PHP branch. In Plesk, record the domain's handler as well as the branch. Ask who installed the correction, when the previous workers stopped, how the serving path was tested and which domains still use an excluded version. An account-specific response should identify every exception and the person assigned to resolve it. [FN 38] [FN 39]

3.4 Temporary restrictions while the correction is installed

A workaround changes settings to reduce a particular attack path while the software correction is being deployed. The PHP project discusses request limits, upload-progress settings and worker handling for specific configurations. These measures must be applied using the vendor's instructions and tested for their effect on the application. Removing memory limits as a blanket response can allow a request to consume excessive server resources. The completion target remains corrected PHP running on every affected serving path. [FN 1] [FN 6]

A WAF can filter traffic during that interval. Confirm that the relevant rules are enabled and that traffic actually passes through them. Check whether a direct server address, alternate hostname or secondary route reaches the origin without the same protection. Retain both the blocked-request records and the origin's activity records. This establishes the coverage of the temporary control and preserves the evidence needed to examine attempts made during deployment. [FN 13]

3.5 The website owner's first check

For WordPress, use the administration address already established for the site. Open Tools > Site Health > Info > Server and record the PHP version. Also record the website address, hosting provider, account or support-ticket number, latest known update and responsible administrator. Check each installation separately. Keep this record with the provider's confirmation so that the displayed version and the actual maintained package can be compared. Use established administration tools rather than adding an unfamiliar scanner during the emergency. [FN 10] [FN 41] [FN 106]

Send the provider the request in Appendix B. Ask for the complete PHP package or build, the correction covering both CVEs, the domains and handlers covered, the deployment time, replacement of older workers, and any excluded legacy installation. Also ask whether the provider found suspicious requests or subsequent changes. An unanswered field should remain an assigned work item with a follow-up time; the incident lead then decides whether the affected service can remain available under a verified temporary restriction. [FN 1] [FN 17] [FN 18] [FN 19]

3.6 Deciding whether to take a website offline

Take an exposed PHP service offline, or restrict access through a separately controlled boundary, when the correction cannot be installed promptly and effective interim protection cannot be verified. WordPress, the United Kingdom's National Cyber Security Centre, CERT-EU and the U.S. National Security Agency provide emergency guidance supporting restriction or withdrawal while remediation is completed. Prioritize sites receiving client documents, handling payments, holding sensitive account secrets or providing administrative access. [FN 6] [FN 7] [FN 102] [FN 106]

The technical owner should coordinate restriction with the person responsible for continuing service. Preserve a verified contact route and accurate public instructions. A court or bar-operated site needs approval and coordination from its authorized technical and procedural officers. Counsel should obtain the court-specific method for urgent submissions and any required direction concerning deadlines. The continuity record should identify who will receive inquiries, which functions remain available and how users will be informed when reliable service resumes. [FN 103] [FN 104]

Reopen the affected service after confirming the corrected PHP program, disposition of older serving paths, examination of unauthorized changes, removal of persistent access, replacement of exposed secrets and testing of essential forms and communications. Verify filing or payment instructions that the server had permission to alter. Keep historical investigation and monitoring assigned after reopening, with unresolved records listed individually and an owner responsible for each. [FN 1] [FN 48] [FN 86] [FN 88]

A maintenance page generated by the same vulnerable PHP installation can leave the underlying request path exposed. Ask the provider how access is restricted at the server or a separately controlled protective layer. Where a replacement public notice is needed, use a secured service and verify its contact details before directing clients or litigants to it. Preserve the time the original service was withdrawn and the time the replacement became available. [FN 1] [FN 6] [FN 13]

4. Rank Math PRO: examining a separate contaminated download

4.1 The affected download window and release history

Rank Math PRO is an add-on used to manage search-engine information on WordPress sites. The vendor identified malicious software in selected version 3.0.123 downloads obtained between October 15, 2026, at 20:02 UTC and October 16 at 07:12 UTC. UTC is Coordinated Universal Time, the shared time standard used to compare records from different regions. The vendor released clean version 3.0.124. Preserve the original download or update record and any retained package so the affected acquisition can be identified. [FN 20] [FN 21]

Wordfence published its notice on October 16. SecurityWeek and The Hacker News reported the incident on October 19. The exposure period, activation date, discovery date and later news coverage belong on separate lines of the incident chronology. A site administrator should reconstruct when the package was obtained and first ran, including updates performed by a vendor or automated deployment service. [FN 21] [FN 23] [FN 24]

Wordfence identifies the contaminated-code incident as CVE-2026-111862, rated 9.8. The register also retains CVE-2026-104751, a different authorization defect involving deletion of search-engine optimization (SEO) analysis in the free plugin, corrected in 1.0.280. Track the free-plugin correction separately from the PRO download incident and from the PHP runtime corrections. Each has its own affected software, acquisition history and completion test. [FN 21] [FN 22]

4.2 Establishing whether the downloaded software ran

The vendor distinguishes three acquisition states. An affected package that was installed and activated requires compromise recovery. A package installed but never activated should be removed, replaced from the trusted source and examined as directed by the vendor. A downloaded archive that never ran should be retained as a provenance record while the installation history is confirmed. Record the applicable state before later updates obscure the original sequence. [FN 20] [FN 21]

Where the malicious package ran, recovery covers the website, database and other reachable hosting resources. A backdoor is a concealed means of returning to the system. This malware can recreate a removed backdoor through changes left elsewhere, including stored website settings. Preserve the evidence and disable the mechanism that rebuilds it before completing cleanup. Then review files, tasks, accounts and credentials. A restoration copy needs a known acquisition date and examination of its contents before it is accepted as the clean baseline. [FN 21] [FN 40]

4.3 Identifiers to give the hosting provider or responder

The vendor's identifiers below guide the Rank Math examination. A defanged domain uses [.] in place of a dot so the text is not accidentally opened as a web address. An options table is the database collection where WordPress stores settings; its prefix can differ between installations. A must-use plugin loads automatically. SSH, or Secure Shell, is an administration connection whose authorized_keys file can grant access. The .htaccess file contains web-server instructions, and cron entries schedule commands. Preserve the matching object and its history before removing or changing it. [FN 20]

Indicator	Investigative use
rank1cdn[.]com	Investigate outbound resolution and connection history; block the malicious destination.
_uf6qdn2hmm, t8krdk990phb, _np5pvf754c	Search the site's options table, using its actual table prefix.
wp-includes/class-wp-cache-util.php	Compare against trusted core files and preserve any matching artifact.
Administrator names beginning wpsupport_; email domain wp-mail[.]net	Preserve account creation, roles, sessions and activity before disabling.
.cache files made executable as PHP through .htaccess	Examine the file and the handler rule together.
System-cron marker #ms6v46	Inspect the owning account, command, environment and related files.
Unexpected PHP in must-use plugins or other plugins/themes; changed SSH keys	Examine persistence beyond the named plugin and beyond the document root.

Review other sites under the same hosting account where files or credentials are shared. The administrator should identify the directories the affected process could write, the accounts it could use and the services it could contact. Those permissions establish the practical recovery boundary for sibling sites and resources outside the original WordPress directory. [FN 20] [FN 41]

The file names and database entries in the table are examination targets for an authorized administrator. A professional responsible for the office can record the plugin version and acquisition history, open the preservation request and identify the affected client-facing functions. The provider or responder should perform file, database and server cleanup with an evidence record and a recovery plan. [FN 20] [FN 21]

5. Current incidents and the trusted connections they expose

The following comparison follows the functions repeatedly encountered in recent incident reports: an internet-facing application, an accepted credential, a trusted administrative service, continued access and a consequential record. The source column identifies the investigation; the middle column describes observed activity; the final column identifies the response task. Each event retains its own initial defect, observed tools and chronology.

The comparison includes Citrix NetScaler appliances, which manage or provide access to network services; Adobe Commerce, an online-commerce application; and WordPress publishing software. A web shell supplies an intruder with server-side commands, while a tunneler carries traffic through an intermediary connection. The matrix records these tools under the incident in which the cited investigators observed them. [FN 28] [FN 29] [FN 33]

Several terms in the comparison describe connections rather than individual computers. A virtual private network, or VPN, creates a protected connection into another network. A tunneling tool carries one connection through another; an attacker can use it to maintain remote access. NetScaler appliances manage application traffic and remote connections. The cited Mandiant research, published through Google Threat Intelligence Group (GTIG), identifies particular tools found after NetScaler exploitation. [FN 28] [FN 29] [FN 32]

A certificate authority issues digital certificates used to validate encrypted connections. A trust store is the collection of authorities a browser or application accepts. Compromise of a signing key therefore requires a different correction from a defect in PHP. The government sources in the table include the Federal Bureau of Investigation (FBI), the National Security Agency (NSA) and the U.S. Department of Justice (DOJ), alongside CISA and international partners. Their notices identify the conduct and affected systems examined in each investigation. [FN 27] [FN 32] [FN 36]

Source and date	Established external observation	Application to this report
Mandiant / GTIG, September 29	Active NetScaler exploitation includes legal/professional-services targets; post-exploitation tooling includes the WHIPSHOT PHP web shell and SLAPSHOT tunneler.	Legal-sector exposure is documented in a current, separate incident-response population. Hunt for execution and persistence beyond the initial appliance flaw. [FN 28]
Citrix bulletin; CISA September 27 alert	The vendor describes separate NetScaler defects and confirms exploitation of specified vulnerabilities.	Keep appliance entry routes distinct from PHP engine flaws even when a later implant is written in PHP. [FN 29] [FN 30]
CERT-FR, September 24	A prior PHP security cycle preceded the emergency releases.	“Patched in September” is not an adequate answer to the October runtime exposure. [FN 31]

Source and date	Established external observation	Application to this report
FBI/CISA/NSA and partners, October 8	Known vulnerabilities, automated scanning, manual access, persistent VPN tooling and mailbox theft are combined in a documented operation.	Old weaknesses and accepted credentials remain operationally important; a fresh zero-day is not required for an adaptive campaign. [FN 32]
Adobe, September 7	CVE-2026-75650 is a separate, exploited Commerce template-injection RCE issue.	Application-specific fixes and PHP-runtime fixes are separate change records. [FN 33]
WordPress, September 22 and October 6	Core security releases 7.1.2 and 7.1.3 address application issues.	Maintain core independently while verifying the interpreter underneath it. [FN 34] [FN 35]
DOJ, October 13	Charges, arrests and device seizures concern false/stolen identities used to obtain remote enterprise work.	An institution can issue genuine credentials to an unauthorized operator; verify identity issuance and recovery, not just login success. [FN 36]
Cloudflare, October 20	A certificate-authority key incident affects cryptographic trust assumptions and requires coordinated trust-store action.	Review signing/key custody and certificate validation paths; do not equate a familiar encrypted connection with authorized institutional intent. [FN 27]

The October 8 joint advisory's appendices connect observed behavior, previously known vulnerabilities, infrastructure and indicators. The investigators document how automated discovery and hands-on activity can be combined with credential use and mailbox collection. The comparison directs responders to examine those connected functions in the affected environment, while retaining the advisory's own actor and incident attribution. [FN 32]

The certificate event concerns the custody of cryptographic signing keys. A certificate authority issues the credentials browsers and other programs use to validate encrypted connections; an intermediate authority operates under a higher-level authority. Cloudflare described compromised intermediate keys and reported no active exploitation in its own services at that cutoff. The response is to apply the relevant provider's trust-store updates, including applications carrying their own stored certificate authorities. Track that change separately from PHP deployment and account recovery. [FN 27]

5.1 Reconstructing control of cloud-hosted website and DNS services

The September 2026 CNF assessment examines how an exposed or compromised cloud credential can instruct a legitimate hosting service to change customer-controlled DNS records through its ordinary administrative interface. In AWS, Route 53 supplies domain-routing information and CloudFront distributes website content. These systems can be used legitimately even when an intruder operates a customer account. The decisive record is the identity and permission used for the particular change, the before-and-after record, and the resulting destination. A shared AWS nameserver or provider address identifies the

service involved; it does not identify the human who initiated a transaction. [FN 54] [FN 55] [FN 82] [FN 90]

Obtain the hosted-zone identifier, before-and-after DNS record, acting IAM identity, CloudTrail event, time, source session and service role. A principal is the user or software identity recognized by the provider. Compare those records with the endpoint, mail, registrar and portal chronology. Preserve the actual record change as well as the public registration timestamp, because the two records describe different events. An autonomous system number, or ASN, identifies a network operator; it supplies infrastructure context alongside the more specific account and event records. [FN 55] [FN 82] [FN 90]

6. From early forensic findings to the current legal-sector response model

6.1 Marlin Technology: the early computer and account findings

Marlin Technology's December 5, 2024 expert report examined two devices, registration records and email-related material. Jepp Walter concluded that the investigated law practice and associated users were subjected to a targeted, persistent intrusion. The report described escalation to administrator-level control over the network, website DNS and OneDrive storage by July 2024. This establishes the early technical context carried into the later research sequence. [FN 81: pp. 2–5]

The recovery implication follows the location of the access. Replacing a computer leaves separately held mailbox permissions, account-recovery arrangements and domain administration to be examined. Microsoft's OAuth investigation documents one means of continued application access after the initial user account is lost. The incident team should therefore keep an inventory of the authority held outside the replaced device and record how each route is removed or re-established under the legitimate owner. [FN 57] [FN 81]

6.2 The October 22, 2025 CNF integrated investigation

The 382-page CNF Integrated Expert Report connects computer examinations with credential records, DNS and mail-routing histories, portal observations, communications and litigation events. Its portal section explains the separately collected datasets and their later correlation with infrastructure changes. Its appendices preserve addresses and infrastructure comparisons for source-level examination. The later September assessment refines how exact matches and broader service relationships are classified. [FN 82: printed pp. 26–68, 100–160, 269–300] [FN 90]

The CNF operating sequence follows an initial foothold, acquisition of credentials, expansion of administrative access and use of trusted communications or portal paths to influence what others receive and record. PHP2Shell now provides a documented means by which an exposed web server could become one such foothold. Reconstructing a given

intrusion requires the server's request and process records, subsequent account activity and any change made through those accounts. The earlier CNF evidence supplies the connected systems and data classes to inspect; the new PHP disclosure identifies an immediate software entry route to close. [FN 2] [FN 3] [FN 82] [FN 90]

6.3 Team B: structured records of portal activity

The September assessment describes Team B's separate collections of 54 employee-environment rows, 317 membership-environment rows and 1,278 e-filing-environment rows covering February 2023 through December 2024. Together they contain 1,649 recorded observations. Their evidentiary use depends on the fields preserved with each observation: account, source address, route, time, authorization and relation to other records. Preserve the original export, collection history and column definitions, including whether each row records an attempted or accepted action. [FN 82] [FN 87] [FN 90]

Those structured records support several different examinations. RAPS compares the submitted and accepted filing. CCDG reconstructs the communication and its authorizing account. ORACLE follows the later institutional state back to the original instruction. Each analysis should identify its underlying acquisition so the combined chronology shows where separate evidence converges and where one report carries forward another report's observation. [FN 86] [FN 87] [FN 88]

6.4 RAPS: following a document through the filing process

The Restricted-Access Portal Solutions Unit, within the Bridge-Gate E.S.S. Division, studies systems in which users sign in to perform consequential transactions. Its Federal CM/ECF, DCN and SMTP Email Relay Expert Report examines filing, receipt, routing, service and document display. CM/ECF means Case Management/Electronic Case Files; DCN is the federal judiciary's Data Communications Network; SMTP is the mail-transfer protocol used by email servers. These are different parts of the filing and notice process. [FN 86: pp. 3–11, 24–31, 38–44]

RAPS concludes that the subject matters exhibit active interference within compromised judicial workflows. Its method compares the filer's original document, the version accepted at intake, the docket-associated copy and the item delivered to each recipient. During the PHP response, identify any website permission or API connection that writes to those stages. Preserve transaction identifiers and compare the actual document contents and recipients at each handoff. [FN 49] [FN 86]

6.5 CCDG: examining authenticated communications

The Cryptographic Cyber-Defense Group's February 25, 2026 report concludes that the examined Florida e-filing and Bar-portal environment remained compromised through that period. Its described work includes endpoint examination, native email headers and

portal datasets. An email header is the technical information accompanying a message, including its route and identifiers. The report's Appendix 1 links its determinations to the source records and methods used. [FN 87: pp. 7–15, 56–60]

CCDG identifies the address 172.93.148.174 in membership-portal rows dated June 19, 2024. That observation places a recorded address in a portal dataset as well as in the broader infrastructure analysis. Section 7 preserves its network-family relationship separately from the two exact addresses matched to the Microsoft schedule. The distinct classifications tell a responder which comparison to reproduce and which source record to request next. [FN 87: p. 14; Appendix 1] [FN 59]

6.6 Avatar and ORACLE: identity, instructions and accepted authority

The January Avatar report examines professional personas and official-looking communications. A persona is the professional identity presented through a profile, account, biography or role. The later ORACLE report follows the wider system through which such an identity gains authority: the credential used, the message or document sent, the role represented, the state recorded and the decision made in reliance on it. [FN 83: pp. 55–86] [FN 88: printed pp. 1–10]

The FBI's January 2025 notice documents false-worker access and data-extortion behavior. The October 2026 enforcement record adds later government findings concerning false or stolen identities used to obtain enterprise access. These sources explain how apparently ordinary recruitment and account-issuance processes can give an unauthorized operator genuine access to organizational systems. [FN 44] [FN 36]

ORACLE reconstructs an act separately from the name displayed on it. For the March 2025 correspondence in the source record, it examines repudiated authorship and an investigator's statement that an email had changed. The examination requires sender and recipient copies, headers, provider account activity and the later actions taken in reliance on the message. Preserving those objects allows the responding team to identify the responsible account and correct the consequential record. [FN 88] [FN 89: pp. 5–6]

6.7 Sinkhole and court-audit research: availability and record custody

The Sinkhole report examines registrar holds, DNS resolution and loss of publication and communications capacity. A registrar hold is a registration status that can prevent normal use or resolution of a domain. Preserve the support tickets, the history of those statuses, nameserver delegation and provider account changes. EPP is the protocol used for registration operations; its status codes help identify restrictions on a domain. Website-file restoration and correction of domain or mail routing require separate completion records. [FN 84: pp. 2–10, 24–38]

The Federal Court Audit records assignment, service, document-replacement and access discrepancies. Its practical use is to preserve the state of the official record at each relevant time and relate it to the technical chronology. The judiciary's August 2025 disclosure and March 2026 modernization statement supply the wider institutional context. Retain the filing, docket and service evidence needed to resolve each case-level discrepancy, including records held by the clerk or provider. [FN 63] [FN 64] [FN 85]

6.8 The September 2026 assessment: adaptation after the first investigation

CNF's September 2026 cAPTure-to-Kill assessment examines how the earlier findings developed as further evidence became available. It evaluates continued computer access, passwords and session material, cloud permissions, DNS and mail routing, professional identity, portals and case-management systems. Its findings describe a deliberate, adaptive operation through 2026 and strengthened support for the principal mechanisms identified in the earlier record. [FN 90: pp. 7–12, 43–47]

The assessment follows access that survives a narrow repair. An attacker can lose one computer while retaining a mailbox permission, a token, a cloud role or a recovery route. The restored endpoint and the surviving remote authority are different recovery tasks. For the current emergency, the administrator should list every credential and permission reachable from the affected PHP service, then verify its custody and disposition. The professional owner should follow the instructions and records created through that authority. [FN 57] [FN 90: pp. 20–25, 31–36]

The assessment's appendices connect earlier findings to later source material and retain the dates and precision of each match. That structure allows new provider disclosures to be compared with preserved events. It also gives the recovering organization a monitoring plan: watch for renewed access, recreated permissions, changed routing and repeated record discrepancies after the initial correction. The objective is sustained control of the environment through which the legal work is performed. [FN 90: pp. 43–47; Appendices A–D]

6.9 Civil cyber-disruption research: preserving access to an effective remedy

The September 10, 2026 Civil Cyber-Infrastructure Disruption Litigation report, led by Jay Lewis Farrow with CNF contributions, follows thirty-five matters across the development of court-directed cyber disruption. It separates the announcement of an action, the technical change made by a provider, the lasting judicial remedy and the continuing ability to address replacement infrastructure. Those stages supply different records of whether containment has endured. [FN 91]

A sinkhole is a controlled destination used to receive traffic that would otherwise reach malicious infrastructure. Court-directed domain changes, server restrictions and

preservation orders can alter the operation’s technical dependencies. Later access can still depend on replacement resources, retained credentials and service relationships. Preserve that continuity when an operation changes its visible address, and present qualifying evidence through the applicable judicial and provider procedures. [FN 62] [FN 84] [FN 91]

The legal-sector implication concerns the route used to request relief. When the ordinary intake or communications channel is itself under examination, identify an authorized method that preserves the submitted evidence, authenticates receipt and records its later handling. The report’s Clean Adjudicative Environment proposal connects those safeguards to the court’s own authority. Section 13.6 translates that issue into the questions counsel should ask the clerk before relying on physical delivery or an alternative electronic route. [FN 86] [FN 91] [FN 103] [FN 104]

6.10 The integrated response finding

The combined record directs recovery toward control over trusted activity. Marlin supplies the early administrative-access baseline; CNF connects events across computers and services; Team B preserves structured portal observations; RAPS follows documents through filing and service; CCDG examines communications; Avatar and ORACLE reconstruct identity and authority; and the sinkhole, court-audit and civil-disruption work address continuing access and the preservation of remedies. The responding organization should apply the same connected approach to its own accounts, records, deadlines and provider relationships. [FN 56] [FN 57] [FN 65] [FN 81] [FN 82] [FN 83] [FN 84] [FN 85] [FN 86] [FN 87] [FN 88] [FN 90] [FN 91]

7. Microsoft court evidence and historical infrastructure matches

7.1 The case, the declarations and the court’s order

Microsoft Corporation, Fortra and Health-ISAC v. John Does, No. 1:23-cv-02447, in the Eastern District of New York, supplies the court record examined here. Fortra is the maker of Cobalt Strike, a security-testing tool whose unauthorized copies were the subject of the action. Health-ISAC is a health-sector information-sharing organization. Cobalt Strike’s Beacon component communicates with a control server and supports actions on the connected computer. The declarations describe the investigation; the court’s later order specifies the remedy. Use the filed caption and document identifier when locating those materials. [FN 58] [FN 59] [FN 62]

Christopher Coy’s declaration was filed as Document 2-2 on March 30, 2023. It contains a signed narrative and exhibits, including the command-and-control address schedule used below. The date in a website’s download directory identifies a hosting path; the filed record establishes the declaration’s date. Preserve the location of each cited item within the narrative or exhibit so another reader can reproduce the comparison. [FN 59]

7.2 The recorded address comparisons

The original 0-VER examination extracted and validated IPv4-form addresses from Coy's C2 schedule at physical PDF pages 37–47 and recorded 268 distinct addresses. IPv4 is the four-number address format shown in the table. Two addresses also listed in CNF Appendix A occur on Coy Exhibit 2/Appendix A page 5, physical PDF page 41, filed PageID 370. A PageID is the page identifier applied within the court filing record. CNF lists those addresses at printed pages 269–270, physical PDF pages 287–288. [FN 59] [FN 82]

Indicator	Subject source	Coy schedule result	Finding and use
172.93.181.244	CNF Appendix A, printed p. 269	Exact entry on PDF p. 41	Historical exact C2 match. Retrieve the dated source connection and process records for the subject event.
172.93.193.41	CNF Appendix A, printed p. 270	Exact entry on PDF p. 41	Historical exact C2 match. Retain the acquisition date and relevant source-event records.
172.93.148.174	CNF printed p. 269; CCDG p. 14, portal rows 5–8	No literal entry in the supplied Coy schedule	Reported portal indicator. Preserve the portal rows and examine the dated network-family relationship.
146.20.161.105 / 146.20.161.121	CNF Appendix A	No literal entry in that schedule	Subject/report comparators requiring their separately cited source chain.
185.198.57.110	CNF Appendix A	No literal entry in that schedule	Retain the separately cited Glupteba source chain and its own comparison record.
205.251.192.0/19	CNF DNS/Route 53 discussion	Not a literal range in the supplied declaration	Route 53 service relationship. Obtain hosted-zone custody, acting identity and change records.

The provider labels should travel with their respective source dates. Coy's schedule lists the two exact addresses under FranTech Solutions; CNF lists them under Nexeon / AS20278. The numeric comparison is exact. Dated ownership, leasing and customer-account records provide the further history needed to place each address under particular control during a subject event. [FN 59: Exhibit 2, p. 5] [FN 82: pp. 269–270]

The September assessment classifies the Route 53 range as a service-family relationship. Use that relationship to identify the relevant provider and change records. Use exact addresses, configuration values and dated activity to reconstruct the particular event. A targeted containment decision should name the affected resource and responsible authority, preserving access to unrelated legitimate services. [FN 90: p. 64]

7.3 Reading a technical declaration with its exhibits and footnotes

Coy's footnote 3 explains that a watermark can be changed in cracked software. A watermark is a configuration identifier embedded in the tool; a payload is the program or

instructions delivered to the target. The examination combines those identifiers with the server’s behavior and recorded communications. Coy’s paragraphs 20–22 describe partner information, security signals, crawling, sample analysis and controlled observation. Crawling here means systematically checking reachable services. Jason Lyons and Rodelio G. Fiñones add configuration and post-exploitation analysis. [FN 59: p. 4 n.3; ¶¶20–22] [FN 60] [FN 61]

Coy’s footnote 7 reports more than 1.5 million detected machines during a historical 24-month period in Microsoft’s Cobalt Strike observations. Keep that population and time period attached to the figure. Similarly, distinguish an address used as an explanatory example from an address listed as investigated infrastructure. The location and function of the source entry determine how it belongs in an operational indicator register. [FN 59: p. 6 n.7; p. 14]

The Sinkhole appendix preserves anonymized device identifiers, partial addresses and a hash rendered as ‘XYZ...’ with a reference to a separate hash report. Those entries direct the investigator to underlying records. Machine-actionable searches require the complete value, its source and its collection date. Retain the redacted entry in the research record and obtain the full authorized value before using it in an automated detection or blocking rule. [FN 84: pp. 34–38]

7.4 Preservation and continuing relief under the permanent injunction

The September 8, 2025 order grants permanent relief concerning the described cracked Cobalt Strike operation and defines qualifying domains/IP addresses and a continuing determination process. It requires preservation and includes measures to avoid affecting unrelated hosted content. Pages 15–22 establish the Court Monitor framework; page 21 permits a party or non-party to request court-directed disclosure of reasonably related information, with notice and an opportunity to be heard. Jurisdiction cannot lapse before January 1, 2030. [FN 62: pp. 7–8, 15–22]

A technically qualifying escalation package can be presented through the order’s procedures for continuing relief. Identify the infrastructure, its relationship to the enjoined activity, the source evidence and the requested action by the proper intermediary. The order also allows specified uncontested monitor determinations to remain off the public docket while requiring records and periodic reporting. A visibility review must therefore distinguish public publication, retained monitor records and the court’s disclosure procedure. [FN 62: pp. 18–22] [FN 91]

8. Establishing who authorized an email or online instruction

8.1 The separate functions of email authentication

Email authentication uses several checks with different functions. Sender Policy Framework (SPF) checks whether a sending server is authorized for the relevant domain identity. DomainKeys Identified Mail (DKIM) verifies a digital signature over specified message material. Domain-based Message Authentication, Reporting and Conformance (DMARC) checks alignment with the visible sender domain and supplies handling and reporting policy. A relay is a server that passes mail onward. These checks describe the sending infrastructure, signature and domain relationships recorded in the message. [FN 51] [FN 52] [FN 53]

The next examination concerns the person or application that used that infrastructure. Someone controlling an authorized mailbox, an approved sending service or an application permission can cause the real service to send an unauthorized instruction. The service can then apply its valid signature to that content. Preserve the account activity and instruction alongside the authentication result so the team can determine who acted and what authority was used. [FN 52] [FN 57] [FN 87]

Inbound routing and outbound sending require separate records. An MX change directs incoming mail to a destination. Sending a signed message requires control of the relevant mailbox, relay, service permission or signing material. Collect each side of the path, including the message as signed and the recipient copy. This establishes whether the disputed instruction originated through an accepted account, changed during handling or diverged at a later stage. [FN 51] [FN 52] [FN 53] [FN 87]

8.2 Documented account and token abuse

Microsoft's Storm-0558 analysis describes forged authentication tokens accepted by legitimate mail services. The Cyber Safety Review Board's report examines the governance and events surrounding that intrusion. Microsoft's separate OAuth investigation describes continued application authority and abusive sending through an organization's resources. These mechanisms explain why the recovery record must include signing material, application grants and tokens as well as the visible user account. [FN 47] [FN 56] [FN 57]

The certificate-authority incident in Section 5 concerns connection validation. Email authorship, account authority and the integrity of a stored filing concern additional stages. Preserve the certificate and trust-store changes relevant to the connection, then examine the application and records it reaches. A trusted connection should lead to an authorized service action and an intact source record; each stage has its own evidence. [FN 27] [FN 50] [FN 86]

8.3 Reconstructing the message and its consequences

Retain the original message in .eml or another native export format, together with full headers, identifiers, attachments and recipients. MIME is the format that organizes a message's body and attachments; preserve it with the original export. Ask the provider for message traces, mailbox access records, delegated permissions, OAuth grants, application secrets and connector changes. A connector is a configured link between mail systems. Compare sender and recipient copies, and confirm the consequential instruction through a separately verified contact. Keep screenshots as a record of appearance alongside the native material. [FN 43] [FN 49] [FN 55] [FN 57] [FN 87]

Where the website sends mail, list the credential it uses and the permission attached to that credential. Give the website a sending identity limited to its operational purpose. Keep executive mail, filing accounts, claims instructions, treasury approvals and registrar administration under separate, controlled authority. Record the change and test the approved website functions after excessive permissions are removed. [FN 41] [FN 50]

For an unexpected instruction from opposing counsel, preserve the original message and attachment, then verify the requested change using an established contact route. Ask the other office to retain its sending record and confirm the authorized instruction. Record any difference between the versions and assess the upcoming deadline or transaction with responsible counsel. The same process applies to a changed clerk notice, settlement direction or request for protected client material. [FN 43] [FN 86] [FN 87] [FN 88]

9. Following a document from submission to institutional action

9.1 Reconstructing the recorded steps

ORACLE examines how an institutional record acquired its accepted state. A claim becomes received, a payment approved, an ownership entry changed or a filing served. Each transition should trace to the source material, the account that acted, its authority and the time. Reconstructing those steps gives technical responders and the responsible professional a common account of the event. [FN 88] [FN 89]

For every significant event, preserve the prior state, requested action, account or session, identified operator, document or transaction number, before-and-after content, receiving system, subsequent decision and consequence. Relate those records to the preceding computer, cloud, DNS and communication history. The resulting chronology makes a later discrepancy testable against the source event and shows which action is needed to correct it. [FN 49] [FN 86] [FN 89]

9.2 Two source-specific applications

The ORACLE supplement records an October 14 submission and October 15 acknowledgment followed by a later nonresponse position. Reconstruct how the received package was associated with each matter, assessed for completeness and carried into later records. Keep the file-specific obligation, submitted copy, receipt and later representation together. This permits the receiving institution to compare the accepted package with the record on which it acted. [FN 89: pp. 4–5]

The same supplement records two case containers in Florida’s Appellate Case Information System (ACIS) displaying shared event and document-link identifiers. The event identifier is 09a9c17e-eb50-477a-85a7-ebce71fcac53; the document link is 60db4494-096e-426d-91e0-c1fbd4631a93. These UUIDs are system-generated identifiers used to track records. Preserve the objects and request the history of their creation, association, correction, replacement and publication across both case routes. [FN 89: pp. 7–9]

The supplement also identifies a normal NEW CASE state before permanent assignment. A verified example of normal processing supplies a control against which the disputed event can be compared. Record that resolved question and continue examining the remaining differences that affected receipt, notice, assignment or disposition. [FN 89: p. 7]

9.3 Correcting the input and the resulting record

A valid institutional decision can carry forward an unauthorized upstream instruction. The receiving clerk, lawyer, insurer or director may have acted on the record presented to them. ORACLE therefore follows both the input and the later reliance: identify what entered the process, what authority it represented, how it was accepted and what action followed. The correction should address each affected record and participant rather than ending when the original account is repaired. [FN 88: printed pp. 1–10] [FN 89]

For law firms, maintain separate confirmation of urgent filings and service. For insurers, confirm claim receipt, changed payees and coverage-related correspondence. For privately held companies, preserve the records behind ownership, vesting, employment and valuation decisions. Each is a sector application of the same method: authenticate the source instruction, reconstruct the transition and reconcile the resulting state. [FN 88] [FN 92]

10. Tracing an event to its mechanism and operator

10.1 Four stages of attribution

Attribution means assigning a supported cause or responsibility to an event. The inquiry proceeds through four connected stages. Event attribution establishes what happened to a process, account, record or route. Mechanism attribution identifies the exploit, credential

or administrative action producing the change. Infrastructure and campaign attribution connect the event to recorded resources and operational continuity. Operator attribution identifies the responsible person or organization. Preserve the evidence supporting each completed stage. [FN 59] [FN 60] [FN 90] [FN 93]

The record preserves exact matches between two CNF-listed addresses and Microsoft's historical C2 schedule, alongside CNF's continuing campaign assessment and independently documented mechanisms. To join a historical address to a particular subject event, retain the dated flow or process record, destination, payload or configuration, account custody and surrounding actions. Historical ownership and customer records establish who controlled a resource at the relevant time. [FN 59] [FN 82] [FN 90]

10.2 Findings and the action each supports

For each row, the response record should include the cited source, the affected resource and the action assigned to its owner. The table separates the conclusion already supported from the further record needed to assign responsibility. This permits immediate protection of the service while preserving a usable investigation trail.

Question	Present finding	Operational consequence
Are the two PHP defects real and urgent?	Yes: vendor advisories, fixes and independent research are available.	Patch or restrict exposure immediately. [FN 1] [FN 2] [FN 3]
Is attack activity publicly reported?	Yes: provider and honeypot observations, with different coverage and cutoffs.	Preserve requests, worker errors and post-exploitation telemetry. [FN 13] [FN 14] [FN 15]
Is poisoned Rank Math software a separate incident?	Yes: bounded vendor distribution window and persistent malware recovery instructions.	Determine package provenance and activation; recover beyond the plugin. [FN 20] [FN 21]
Are there exact subject/Microsoft IP matches?	Yes: two addresses confirmed against the actual schedule.	Use them as historical joins, not an undated universal blocklist. [FN 59] [FN 82]
What does the Route 53 relationship identify?	The DNS service and its customer-controlled configuration layer.	Obtain hosted-zone, credential and change-event custody. [FN 54] [FN 55] [FN 90]
What record identifies an operator of a current PHP incident?	The event-specific account, request, process and provider-custody evidence.	Contain the observed activity and preserve the records needed to identify the operator. [FN 11] [FN 12] [FN 14]

10.3 Documented commercial objectives and institutional consequences

The Aviram Azari sentencing supplies an adjudicated hacking-for-hire comparison involving paid projects, account intrusion, target tracking and selective publication of stolen material. The Nickolas Sharp sentencing supplies another sequence: administrative

access, concealed theft, altered logs and a false incident narrative with economic consequences. Both demonstrate that unauthorized access can be used to control information and business outcomes as well as to demand ransom. [FN 45] [FN 46]

An investigation applying those mechanisms should preserve payment, tasking, customer-account custody, access-broker records and exact technical continuity. An access broker is an operator who supplies access to another actor. The underlying case records identify their own participants; subject-event evidence establishes the additional connections in the environment being examined. This allows containment of the recorded capability while the responsibility inquiry continues. [FN 45] [FN 46] [FN 90] [FN 92]

11. Naming observed attack techniques with MITRE ATT&CK

MITRE ATT&CK is a public knowledge base of adversary behavior. Its name refers to Adversarial Tactics, Techniques, and Common Knowledge. The identifiers in the table provide a shared vocabulary so a provider, forensic analyst and institutional incident lead can describe the same observed behavior. Record the supporting artifact and event alongside the technique. One operation can move among several techniques as access and conditions change.

The technique names are shorthand for actions already described in this report. Exploiting a public-facing application concerns the entry into the server. A software-supply-chain compromise concerns a contaminated distribution package. Valid-account use and account manipulation concern accepted credentials and changed authority. Data manipulation concerns alteration of the stored, transmitted or actively processed record. Record these actions separately when several appear in one sequence.

Identifier	Current name	Application and evidence needed
T1190	Exploit Public-Facing Application	PHP exploit attempt or execution: affected path, request sequence and resulting process evidence. [FN 67]
T1195.002	Compromise Software Supply Chain	Poisoned Rank Math distribution: package provenance and activation history. [FN 68]
T1078	Valid Accounts	Unauthorized use of accepted web, mail, cloud or portal accounts. [FN 69]
T1098	Account Manipulation	Changed credentials, delegates, roles, recovery devices or SSH authority. [FN 70]
T1114.003	Email Forwarding Rule	Rule or forwarding configuration used to collect mail. [FN 71]
T1505.003	Web Shell	Persistent server-side command facility with file/process/request evidence. [FN 72]
T1565	Data Manipulation	Stored (.001), transmitted (.002) or runtime (.003) data alteration; preserve the changed object. [FN 73]

Identifier	Current name	Application and evidence needed
T1584.001	Compromise Infrastructure: Domains	Compromised domain infrastructure, supported by control/custody evidence. [FN 74]
T1557	Adversary-in-the-Middle	Supported interception or traffic mediation, with path evidence. [FN 75]
T1539	Steal Web Session Cookie	Theft of session material; distinguish it from a password reset. [FN 76]
T1550.001	Use Alternate Authentication Material: Application Access Token	Unauthorized use of tokens accepted by the service. [FN 77]
T1585	Establish Accounts	Accounts cultivated for an operation or persona; trace creation and custody. [FN 78]
T1053.003	Scheduled Task/Job: Cron	Persistent scheduled execution, including relevant Rank Math artifacts. [FN 79]
S0154	Cobalt Strike	Software identifier; validate configuration and behavior rather than inferring an actor from the label. [FN 80]

Use T1557.003 specifically for DHCP Spoofing: manipulation of the service that supplies network configuration to devices. Use the parent T1557 category for the broader interception behavior described in the relevant evidence. Email forwarding belongs under T1114.003; T1565.002 describes manipulation of data during transmission. Record changes to these labels without altering the source observation. Account creation and valid-account use should similarly retain their own T1585 or T1078 classification when examining professional-persona activity. [FN 68] [FN 69] [FN 71] [FN 73] [FN 75] [FN 78]

12. Emergency response: preserve, contain and restore

The incident lead coordinates three streams of work: restricting the exposed system, preserving the evidence and protecting obligations that continue during the interruption. The intervals below organize priority and handoff. Begin urgent isolation and preservation together, then record the completion evidence for each stage. A small practice can assign these responsibilities to its principal and hosting provider; a court or larger organization can allocate them to established operational teams. [FN 1] [FN 21] [FN 48] [FN 49] [FN 88]

12.1 First 30 minutes — establish control and stop avoidable harm

Name the incident lead, the technical owner and the person responsible for business or legal records. Establish a device and contact route checked independently of the accounts being examined. This is the out-of-band coordination route: it operates outside the questioned communications path. Record who may authorize restrictions and who may approve restoration. Verify the participants' identities before sharing account-recovery information or protected records. [FN 43] [FN 48] [FN 88]

List public websites, portals, test sites, hosting accounts and products containing PHP. Include remote-access appliances, which allow staff or providers to enter the organization's network. Identify sites that obtained Rank Math PRO during the affected window. Assign an owner and follow-up time to each unknown software or activation state. Preserve the initial inventory so later changes can be reconstructed. [FN 7] [FN 8] [FN 20]

Have the administrator restrict an unpatched exposed service when effective interim protection cannot be verified. Restrict administration to independently checked access. Where contaminated Rank Math software ran, stop its execution and external retrieval while preserving evidence. Confirm that the restriction reaches direct server addresses and alternate access paths as well as the visible website name. [FN 6] [FN 13] [FN 21]

Require independent confirmation before changing wire destinations, trust-account instructions, claims payees, ownership records, privileged access or imminent service lists. A capitalization table, or cap table, records an organization's ownership interests. Put two-person approval around transactions whose immediate consequences justify a temporary hold, and keep unaffected operations moving through verified channels. Record the reason, scope and owner of each hold. [FN 43] [FN 88] [FN 92]

Exit record: accountable lead; clean coordination route; prioritized asset list; exposure restriction decisions; preserved initial state; named owners for urgent professional obligations.

12.2 Minutes 30–120 — preserve the evidence that will otherwise disappear

Ask the technical owner to export web-access records, error logs, WAF events, PHP and server errors, process-monitoring records, and relevant network and DNS activity. Keep original time zones alongside a normalized UTC chronology; record any difference between system clocks. Link requests to workers or containers where that information is available. Include failed requests and worker crashes, which can identify the transition into a later unauthorized action. [FN 3] [FN 16] [FN 49]

Preserve the site files, database, downloaded plugin packages, scheduled tasks, SSH authorized keys, configurations and deployment records. A snapshot is a captured state of the files or database at a recorded time. Calculate hashes of exports, record who collected them and how, and store original copies under controlled read-only custody. Work from separate copies. Record whether file and database snapshots describe the same moment or different stages of the incident. [FN 40] [FN 49]

Ask the provider to retain account access, installation history, deployment history, control-panel activity, registrar and DNS changes, mail traces and identity audit records. Obtain the ticket number, retention period and authorized transfer route. The provider's account-side

records connect an action to an identity and resource; retain them alongside the public website or DNS observations. [FN 55] [FN 84] [FN 89]

Preserve the affected website's files, databases, web requests and error records in their original state, then record any changes made to contain further exposure. Record dates and time zones and request provider-held records before retention limits expire. Begin the review on or before October 17 for PHP2Shell, the earliest attempted exploitation date reported by AWS; extend the period where the site's own logs indicate earlier suspicious activity. Retain records sufficient to identify the server process, user account, file or credential changed after a suspicious request. [\[FN 108\]](#)

12.3 Hours 2–6 — close runtime paths and remove persistent authority

Install the corrected PHP package or verified provider backport in every serving environment, then restart or replace older workers. Confirm that each domain uses the corrected build. Check older packages, test sites and scheduled tasks that can invoke separate PHP installations. Test sign-in, forms, uploads and other essential functions, and record the result and time of each check. [FN 1] [FN 17] [FN 19]

For a compromised site, the qualified responder should rebuild from trusted components or complete an evidence-preserving cleanup. Examine plugins, automatically loaded plugins, themes, lookalike core files, database settings, scheduled tasks, SSH access and writable hosting directories. Review stored settings capable of recreating removed code. Retain a record of each finding and its disposition so restoration can be checked against the original incident state. [FN 20] [FN 21] [FN 40]

Revoke exposed sessions, refresh tokens, application secrets and unnecessary permissions from the independently checked administration environment. A refresh token allows an application to obtain renewed access and can outlast an ordinary sign-in session. Contain active misuse promptly, coordinate replacement credentials with control of the persistence mechanism, and review MFA enrollment, recovery addresses, delegates and administrative roles. Verify that the old access no longer works and the intended services still do. [FN 57] [FN 66] [FN 70] [FN 77]

Exit record: patched runtime/worker attestation; trusted application baseline; persistence findings and disposition; revoked authority inventory; tested critical functions.

12.4 Hours 6–24 — reconstruct the connected environment

Compare domain-registration, DNS and mail settings with the last authenticated baseline. Preserve the changed NS, address, alias, MX or TXT record and its before-and-after values. Obtain the requested change, acting principal, session, permission and resulting configuration. For Route 53, collect the applicable CloudTrail record and hosted-zone

identifier. Match the actual changes to the mail, account and portal chronology. [FN 54] [FN 55] [FN 84] [FN 90]

Review mail connectors, signing paths, forwarding rules, delegates and software accounts. Establish whether a website credential could send in a professional's name or reset a filing, claims or payment account. Confirm consequential instructions with the authorized person through the independent route. Keep divergent sender and recipient copies so the investigation retains the record of what each participant received. [FN 43] [FN 51] [FN 52] [FN 53] [FN 87]

List consequential actions during the exposure period: filings, notices, client instructions, payments, claims changes, document replacements and ownership decisions. Compare the original, accepted, stored and delivered copies. Assign both a technical owner and a professional or business owner to each discrepancy. Recovery then addresses the recorded consequence as well as the access that produced it. [FN 86] [FN 88] [FN 89]

Exit record: reconciled control-plane changes; communications integrity review; affected transaction list; escalation packages for unresolved high-consequence states.

12.5 Hours 24–72 — restore with measured acceptance criteria

Approve external access when the affected service meets the completion conditions in Section 14. Monitor for renewed execution, recreated files, unusual outbound connections and reappearing permissions. Test restoration copies in a separate environment before relying on them. Continue independent verification for unresolved high-consequence transactions, with a named owner responsible for closing each exception. [FN 40] [FN 41] [FN 48] [FN 88]

Report established incident facts through verified provider and official reporting channels. Include the affected resources, dates, observed behavior, evidence provenance, impact and a reliable contact. For diverted payments, contact the financial institution immediately using an established number and report through the FBI's Internet Crime Complaint Center, IC3. Obtain current reporting details independently of the questioned message or website. [FN 32] [FN 43]

Exit record: signed restoration decision; continuing monitoring owner; corrected business records or documented unresolved exceptions; retained original evidence and recovery history.

13. Keeping legal and institutional work functioning during the response

13.1 Law firms, lawyers and litigation-support providers

Prioritize systems that can affect deadlines, service, confidentiality and client instructions. A public marketing site may hold form submissions, mail keys or credentials reused elsewhere. Map those actual relationships instead of assuming the website is isolated from practice operations. Keep the public site and privileged legal workflows under separate accounts and minimum necessary permissions. [FN 41] [FN 50] [FN 81] [FN 88]

For every time-critical matter during a confirmed exposure period, reconcile the intended filing, transmitted object, receipt, docket association and service population. Preserve native notices and attachments. Confirm disputed receipt or deadline information through a known independent institutional contact and the applicable authorized process. Maintain a matter-level exception register rather than allowing a technical incident ticket to obscure an imminent legal obligation. This is the RAPS/ORACLE method applied as a continuity control. [FN 86] [FN 88] [FN 89]

Where an ordinary filing or service route is in dispute, seek a court-authorized path for receiving and examining the integrity evidence. The civil-disruption report describes a Clean Adjudicative Environment: independently authenticated intake, preserved originals, controlled technical review and reconciliation into the official record. Identify the governing court procedure and request the necessary direction before transmitting protected materials through an alternative channel. [FN 91] [FN 103] [FN 104]

13.2 Fiduciaries, accountants, advisers and other professionals

Protect instructions that move money, disclose confidential information or change legal/business authority. Separate verification of the sender's technical domain from verification of the person's transaction-specific authority. Use a known telephone number or separately established channel for changed payment details, emergency confidentiality requests and account-recovery demands. Preserve the original instruction and the independent confirmation together. [FN 43] [FN 88]

Review shared service accounts and outsourced administrators. The person who maintains a website should not automatically possess control over the firm's registrar, executive mail, document system and banking-recovery channel. Record exactly which authority each account needs and remove unnecessary links. The objective is to prevent one compromised component from becoming a universal professional identity. [FN 50] [FN 57]

13.3 Insurance agencies, brokers and claims operations

Maintain continuity of claim receipt and policyholder communication. Independently verify changed payees, bank details, repair-provider instructions, broker contacts and portal-

recovery information. Preserve original submission objects and receipt timestamps so a technical routing failure does not silently become a business state of “not received.” The same method applies when an attachment or beneficiary record differs across sender, portal and claims system. [FN 43] [FN 86] [FN 88]

During containment, maintain a separately secured claims-intake route with a documented handoff into the official claims record. Require two-person approval for changes that release funds or change authority. Identify the web applications permitted to write claims data, send branded messages or reach recovery credentials, and narrow those permissions before restoration. Test the authorized receipt, acknowledgment and routing sequence. [FN 50] [FN 88]

13.4 Privately held companies and equity administration

The Private Stock News article examines the source records behind ownership and valuation decisions: employment status, cap tables, board materials, forecasts and transaction timing. Preserve those inputs and their revision histories when a connected account or communications environment is compromised. Compare the information supplied to the decisionmaker with the authenticated source and record any change that affected the resulting action. [FN 88] [FN 92]

Require separately verified approval for repurchase instructions, vesting changes, terminations affecting equity, capitalization edits, tender eligibility and valuation submissions. Place a hold on the disputed input while maintaining the unaffected business functions. Reconstruct who supplied it, which system accepted it, what earlier version existed and which decision relied on it. The Sharp case supplies a public comparison linking access and narrative manipulation to economic harm; its chronology begins with the December 2020 intrusion and continues through March 2021 publicity. [FN 46] [FN 92]

13.5 Managed service providers and portfolio-wide operators

Managed service providers should organize recovery around shared dependencies. Identify common PHP packages and deployment images, operating-system accounts, control-panel administrators, mail services and backup credentials. A shared operating-system account can grant the same process access to several site directories. A shared provider account can hold authority over many customer environments. Deliver a per-customer record listing corrected resources, examined access, unresolved exceptions and the operator responsible for each remaining task. [FN 17] [FN 19] [FN 38] [FN 39] [FN 50]

13.6 Court offices, clerks and bar associations: intake and verified public directions

A filing transaction has at least four records worth retaining: the submitted file, the receiving acknowledgment, the case association and the notice sent to recipients. PACER is the federal system for public access to court records; CM/ECF manages filing and case

activity. The filer's screen, the clerk's intake record and the public display can represent different stages. The response should reconcile the relevant stages through the authorized court office. [FN 86] [FN 103]

Map the public website and the restricted filing or membership system as separate services, then identify their actual connections. Those connections can include published filing directions, hearing information, payment links, notification addresses, forms and credentials used to transfer data. Verify affected public instructions against the institution's controlled records. Assign both an authorized procedural officer and a technical owner to any correction affecting public reliance or case handling. [FN 50] [FN 63] [FN 86]

Paper delivery provides a physical receipt stage, but the next handling step can return the document to electronic processing. A clerk may scan, index and route the submission through the same case-management environment under review. Federal courts set electronic-filing requirements and exceptions through local rules and orders; specified emergency nonelectronic routes exist in some courts. Obtain the procedure for the particular court and document, including any special handling for highly sensitive material. Record both physical receipt and the subsequent custody, image, docket and service stages. [FN 103] [FN 104] [FN 86]

Call the clerk or filing help desk using a number confirmed independently of the disputed communication. When an urgent integrity issue requires an in-person visit, ask where the authorized intake staff can receive the inquiry and what materials may be brought. Request the applicable rule or standing order, emergency submission method, receipt process and confidentiality controls. Record the staff member, time, instructions and accepted file. Obtain judicial direction for any required deadline relief or special handling; keep protected evidence within the authorized route. [FN 103] [FN 104]

For physical delivery, retain a complete copy of the package and request a receipt identifying the matter, date, time and documents accepted. Ask whether the papers will be scanned, which office will receive the scan, how attachments will be associated with the case, and how confirmation will be provided. After authorized processing, compare the received or docketed copy with the delivered package. Where the court orders paper-only or other special handling, preserve that direction with the custody record. [FN 86] [FN 103] [FN 104]

Bar associations, licensing bodies and referral services should reconcile member identities, directory contact information, recovery routes, payment instructions, education-registration channels and public notices. Preserve the role and profile-edit histories before correcting an unauthorized change. Name a staff member who can authenticate inquiries from affected members while IT examines the service. Track the membership database,

public website and referral channel separately, with the connection between them recorded. [FN 50] [FN 70] [FN 88]

13.7 Professional directories, firm reputation and public-facing identity

Professional identity is published across the firm website, Bar records, court appearances, directories and search-indexed articles. Include Avvo, Martindale-Hubbell, Lawyers.com, Super Lawyers and publisher biographies in the organization's identity inventory. Compare names, affiliations, contact information and intake links with the approved record. Preserve a dated screenshot and URL for each discrepancy, then ask the relevant platform for the account and edit history needed to establish how it arose. [FN 88] [FN 90]

When a profile or announcement requires correction, preserve the displayed version and contact the platform's verified support or editorial channel. Identify the original source, later copies and the supporting document or authorized instruction. Retain the correction request and resulting version. An inaccurate phone number, diverted intake link or misassigned biography can continue to affect clients and employers after the original website has been repaired, so the closure record should include the downstream publications. [FN 88] [FN 91]

Maintain one approved identity record containing the firm's current address, telephone number, website, authorized personnel and intake destinations. Assign an owner to compare public profiles against it and a second reviewer to approve consequential changes. Preserve provider ticket numbers and the date each correction became visible. This gives the incident team a verifiable closure test for professional identity as well as for the server. [FN 88] [FN 90]

13.8 Specific role of NACABAR and other professional associations

NACABAR and other professional associations can organize incident orientation, provider questions, responder referrals and communications-continuity materials for their members. Publish a verified contact route, its operating hours and the information required for an initial inquiry. Route sensitive evidence through an agreed secure process. Court submissions remain with the authorized clerk and filing procedure; technical incident work remains with the responsible provider or responder. Record the handoff so members know who has accepted the task and how they will receive an update. [FN 48] [FN 86]

13.9 Locating official guidance and court-specific instructions

The PHP Project, WordPress, the United Kingdom's National Cyber Security Centre, CERT-EU and the United States National Security Agency published emergency guidance for affected PHP installations. The American Hospital Association issued a sector-specific executive alert. The review performed for this edition located no PHP2Shell-specific public announcement in the searched Florida Bar, American Bar Association or federal

Administrative Office channels as of October 22. Contact the responsible authority using an independently verified number and obtain current instructions for the specific court or professional service affected by an outage. [FN 1] [FN 6] [FN 7] [FN 102] [FN 103] [FN 105] [FN 106]

Keep a dated local copy of the advisory used for a repair decision and check for updates before reopening a service. Confirm that a court notice applies to the relevant court, case type and filing method. Record the institution's answer where public instructions do not resolve the incident-specific question. The resulting response file should show which source supported each technical or procedural decision. [FN 1] [FN 48] [FN 103] [FN 104]

14. Completion tests for restored websites, accounts and records

A restoration decision needs five documented completion checks. The technical owner records the corrected software and removed access. The professional or business owner confirms the consequential instructions and records. The incident lead reviews the combined evidence, remaining restrictions and monitoring arrangements before approving the affected service for ordinary use.

Completion check	Evidence required for closure
Corrected PHP and serving processes	Every serving PHP path has an identified corrected build or validated backport; old workers/images have been replaced; application functions tested.
Removal of continuing unauthorized access	Relevant files, options, scheduled tasks, accounts and hosting paths examined; unauthorized mechanisms removed or systems rebuilt from a trusted baseline.
Restored account and administrative control	Exposed credentials/tokens revoked; grants, delegates, MFA and recovery paths reconciled; registrar/DNS/mail authority authenticated.
Verified records and professional instructions	High-consequence submissions, receipts, recipients, payment/claims/ownership changes compared against source objects and independently verified.
Preserved evidence and monitoring	Originals retained with hashes and custody; provider records requested; recurrence detection and exception ownership assigned.

Apply these checks to the service being restored and record the scope of the decision. When a lower-risk function can resume while another remains restricted, identify the permitted function, remaining exposure, compensating control and accountable owner. Preserve the supporting evidence with the restoration approval so later operators can understand what was checked and what remained assigned for follow-up. [FN 1] [FN 21] [FN 48] [FN 49] [FN 86] [FN 88]

The response finding is direct: correct the entry route, remove continuing unauthorized access, restore the legitimate accounts and verify the records created through them. For a law firm, court, Bar or service provider, recovery reaches completion when both the technology and the consequential work can be relied upon again. The combined software advisories, investigative reports and institutional records support that integrated containment standard.

Appendix A. Recording indicators and connecting events

A.1 Maintaining three incident-specific indicator collections

Maintain a current Rank Math collection using the identifiers in Section 4.3 and the package's acquisition and activation history. Maintain a PHP2Shell collection covering suspicious request sequences, memory errors, worker crashes and subsequent access or execution. Maintain the historical Cobalt Strike and subject-case addresses with their original dates and sources. A multipart request is a web request divided into parts, commonly used for file uploads; its filename, ordering and later server behavior can assist investigation. [FN 2] [FN 3] [FN 16] [FN 20] [FN 59]

The SANS Internet Storm Center examined a proof of concept, or PoC: a demonstration of an exploitation method. The described request used an unusually long multipart filename and session-upload-progress behavior. SANS recorded reliability limits for that demonstration. Retain those details as dated investigation inputs alongside the actual request sequence and server effects. The operational collection should contain source-supported identifiers with complete values and recorded acquisition context. [FN 16]

Prioritize unexpected commands started by a web-serving process, new executable files, unauthorized accounts, outbound downloads and scheduled persistence. A shell is a program that accepts operating-system commands. Preserve the process relationship showing what started it, the request that preceded it, the files or accounts it affected and the resulting connections. That joined sequence gives the responder a concrete basis for containment and further attribution. [FN 65] [FN 72] [FN 79]

A.2 Event record template

Field	What the responder records
Event ID and scope	Unique incident/event ID; organization; asset; domain; account; matter/claim/transaction if applicable.
Prior state	Last authenticated configuration or record version, with timestamp and source.
Observed action	Request, login, API call, file change, submission, service or publication event.
Identity and authority	Account, principal, session/token, role, recovery method and authorizing instruction.
Technical objects	Host/process/container ID; request ID; object UUID; path; hash; database key; provider resource ID.
Time	Original timestamp/timezone, UTC normalization, clock offset and collection time.
Consequence	What changed; who or what relied on it; financial, legal or operational result.
Correlations	Preceding and subsequent events, exact matching fields, shared-source dependencies.
Disposition	Containment action, restored baseline, unresolved field and accountable owner.

The worksheet preserves the report's connected-event method. Complete it with the source-native record and its original time, then add the linked records from the other systems involved. Where several reports use one artifact, retain that dependency. Where separate acquisitions describe the same transition, identify each acquisition and the specific point of agreement. [FN 49] [FN 89] [FN 93]

Appendix B. Hosting-provider and IT attestation request

Send this request through the provider contact already established for the account. Keep the reply with the incident record and assign a person to follow up on every unanswered field. The provider can attach its technical record while the client retains a short summary of the domains covered, work completed and remaining restrictions.

Subject: Emergency runtime and compromise-status verification — PHP2Shell / Rank Math PRO

Please provide an account-specific response covering every production, staging, subdomain and separately configured PHP environment under the account. Identify the affected domains, server/container identifiers, PHP branch, full package/build revision, package source, handler and pool. State which advisory or vendor backport covers CVE-2026-109618 and CVE-2026-109619, when it was installed, when affected workers were restarted or replaced, and how the web-served runtime was verified.

Identify any excluded or end-of-life runtime, alternate origin path or package source not covered by automatic updates. State any temporary protection in force and its scope. For sites that obtained Rank Math PRO 3.0.123 during the vendor window, provide the available acquisition and activation history, persistence review and credential-containment status.

Preserve relevant web/error logs, account access, control-panel changes, package/deployment history, snapshots, DNS/registrar changes and administrative audit records. Provide the preservation ticket number, retention period and secure transfer method. Do not send passwords, private keys or raw client-confidential evidence through ordinary email.

Attach the per-domain inventory, complete corrected-build information, restart or deployment record, remaining exceptions and responsible administrator’s confirmation. Identify the PHP program serving the site separately from WordPress and the site’s other software. Record any temporary restriction and the conditions for lifting it. This request follows the provider-specific responsibilities described in Sections 3 and 12. [FN 10] [FN 17] [FN 18] [FN 19] [FN 38] [FN 39]

Appendix C. Examination map for the research corpus

The examination map retains the source edition and relevant page locators. Printed page numbers and PDF viewer positions are identified where they differ. Use the document’s actual page and section heading together to locate the cited material. The source report’s own table of contents remains part of that edition’s record.

Supplied artifact	Principal examination and application
Marlin Technology, December 5, 2024; 13 pp.	pp. 2–5: acquisition scope and administrative-control findings; pp. 6–13: persistent-threat model and conclusions. Baseline for cross-system response. [FN 81]
CNF Integrated Report, October 22, 2025; 382 pp.	Printed pp. 26–68: endpoints; 100–160: DNS/portal analysis; 160–184: communications; 269–273: Appendix A; 283–300: event/attribution addenda. Printed Arabic pages are PDF position minus 18. [FN 82]
Avatar supplement, January 15, 2026; 86 pp.	pp. 2–54: persona/infrastructure analysis; 55–69: official-communication case studies; 70–86: supplemental persona studies. Read with later ORACLE authority distinctions. [FN 83]

Supplied artifact	Principal examination and application
Sinkhole report, January 20, 2026; 38 pp.	Main text: registrar/DNS suppression and response; pp. 34–38: device/IP/obfuscation appendix. Partial/redacted values excluded from actionable IoCs. [FN 84]
Federal Court Audit; 24 pp.	Docket, service, replacement, internal-path and exhibit-access chronology; source for record-state preservation. No date inferred from the upload timestamp. [FN 85]
RAPS; 44 pp.	Cover date February 23, 2026, although filename says February 27. pp. 3–11, 24–31 and 38–44: workflow method and findings. [FN 86]
CCDG, February 25, 2026; 60 pp.	pp. 7–15: method and portal/identity findings; p. 14: specific portal IP; pp. 56–60: Appendix 1 determinations. [FN 87]
ORACLE Authority-Rail Report; 198 pp.	Cover label July 7, 2026. Printed pp. 1–10: authority model; PDF pp. 82–90: detection and timed response; full endnotes begin PDF p. 108 / printed p. 102. The edition contains 574 numbered notes and references later September material. [FN 88]
ORACLE supplement; DOCX rendered as 22 pp.	Cover date September 24, 2026, despite filename “0925.” pp. 4–9: receipt, communications and shared ACIS object-state findings; concluding notes retain source dependencies. [FN 89]
CNF September 2026 assessment; 91 pp.	pp. 14–17: evidence/attribution method; Appendix A p. 54; B p. 56; C p. 63; D p. 64; endnotes p. 65 onward. These actual locations supersede stale TOC references. [FN 90]
Civil Cyber-Infrastructure Disruption Litigation, September 10, 2026; 111 pp.	Case/outcome framework and channel stress tests; actual Appendix A p. 79, B p. 96, C p. 100, D p. 101, E p. 102, F pp. 103–110, G p. 111. [FN 91]
Private Stock News article; 10 pp.	Page 1 says October 17, 2026; body says October 18. Economic/ownership application and cited public comparators; treated as editorial synthesis. [FN 92]
Microsoft final order; 23 pp.	Caption, pp. 7–8 preservation/nonparty-hosting protections; pp. 15–22 monitor, review, disclosure and jurisdiction. Public counterpart is [FN 62].
Coy declaration; 259 pp.	Narrative and footnotes; C2 schedule PDF pp. 37–47; exact matches PDF p. 41 / PageID 370; preserve exhibit origins throughout. Public counterpart is [FN 59].
Master Investigative Protocol; DOCX rendered as 8 pp.	Conjunctive analysis, evidence dependencies, affirmative supported findings and precise attribution. It supplies method, not independent incident telemetry. [FN 93]

The ORACLE edition carries a July 7 cover label and includes later September material. Cite that supplied revision with its later content dates preserved. The civil-litigation and September-CNF maps use the actual appendix locations recorded in the examination, allowing the reader to locate the source even where its original contents labels differ. [FN 88] [FN 90] [FN 91]

Appendix D. Source records and hyperlink status

The source notes preserve the original October 21 research-access record and the subsequent October 22 review. The current edition adds the AWS Security Blog’s October 17 attack-traffic chronology and WIRED’s October 21 follow-up as separately identifiable sources. Core vendor advisories, official guidance and relevant judiciary records remain connected to the statements they support. The source ledger identifies which records describe an actual event, which establish technical capability, and which provide an investigative or response method.

The original 80 external records retain their source identities and access dates. The supplementary journalism and institutional-guidance entries now run from [FN 94] through [FN 109]. The 35 original recent-window items remain indexed to their own publication or update dates. Source descriptions state the evidence each item supplies. Reporting that repeats an official advisory is cited for its distinct public account, while the underlying project or provider advisory controls the technical finding. [FN 94]–[FN 107] preserve the supplementary reporting and institutional guidance, including the separately retained WordPress reference. Each entry has its own purpose in the report, and repeated reporting of a vendor notice retains that underlying source relationship.

Every numbered citation links to the corresponding source note. Public-source titles link to the original destinations retained in the document. Supplied expert-report notes identify the edition and page locations; public archive links are retained where provided. The note’s summary explains what the source contains and which factual statement, analytical comparison or response direction it supports.

Appendix E. Emergency decision and evidence-preservation checklists

Use the checklists to assign work during the first response period. Enter the responsible person, completion time and supporting record for each task. The senior partner, clerk or association executive records the operational decisions while the provider records the server and account checks. Begin the PHP2Shell log review at least October 17 in light of the AWS MadPot findings, and extend the window when local records support it. Keep unresolved items assigned with a follow-up time and an identified protective restriction. [FN 1] [FN 48] [FN 86] [\[FN 108\]](#)

E.1 Initial exposure and decision checklist

ACTION	DOCUMENTED COMPLETION TEST	REFERENCE
☐ Identify every public domain, subdomain and staging site	Owner + date/time inventory; host, account and internal contact	FN 10; FN 38
☐ Verify PHP runtime, full patched build and web worker restart	Site Health plus host package/backport and deployment attestation	FN 1; FN 17
☐ Restrict an unpatched public service when no adequate control exists	Change approval, offline/isolated status and continuity contact	FN 7; FN 102
☐ Check Rank Math PRO provenance separately	Acquisition/activation history for Oct 15–16; trusted rebuild plan if activated	FN 20; FN 21
☐ Open a secure, independent coordination channel	Names, alternate contact verification and incident ownership	FN 48; FN 88
☐ Preserve web, PHP, WAF, DNS, identity and provider logs	Snapshots, retention request, UTC time, hashes and custodian	FN 49; FN 55
☐ Hunt for new process/file/task/account changes	Connected request, error and process records, with the source and time of each finding	FN 3; FN 16
☐ Revoke exposed credentials, tokens and app grants	Successful revocation, changed MFA/recovery and review of delegates	FN 57; FN 70

ACTION	DOCUMENTED COMPLETION TEST	REFERENCE
☐ Verify any changed payment, filing or confidential instructions	Independent call, preserved original message and confirmed human authority	FN 43; FN 88
☐ Decide on reopening through five documented acceptance gates	Runtime, persistence, control, records, custody/monitoring signed off	FN 48; Section 14

E.2 Legal-workflow continuity: additional checks for counsel and courts

TASK	EVIDENCE / CONFIRMATION
☐ Identify every deadline or sealed/privileged matter at immediate risk	Matter list, owner, deadline source and court-specific filing rule
☐ Keep the original submitted document and receipt as different objects	Native file, timestamp, hash and transaction/docket identifier
☐ Compare notice recipients and electronic service lists	Source/accepted/served copies, addresses and missing or added recipients
☐ Use a clerk contact verified independently of a disputed website	Telephone/source, person spoken to, instructions, incident or ticket number
☐ Verify availability and authority for emergency nonelectronic filing	Local rule or judicial instruction; distinguish physical receipt from later digitization
☐ Protect confidentiality when requesting alternate handling	Do not transmit sealed records through unauthorized ordinary email
☐ Reconcile official docket/publication state after any corrected intake	Compare accepted document, docket listing and recipient copy
☐ Check public directory and law-firm identity records for unauthorized edits	URLs, screenshots, record snapshots, platform support or change logs

E.3 Connecting warning signs to the affected system

A warning sign is most useful when its source and consequence are preserved. A partner or clerk can record an unexpected changed instruction, a missing acknowledgment or a document mismatch. The technical owner then connects that observation to the server, account and message records. Use the same incident identifier on both records so the inquiry retains the whole sequence.

Give priority to unusual upload-request clusters, PHP memory failures or worker restarts followed by unexpected commands, changed files, new administrators, outbound retrieval or scheduled jobs. Include changed mail delegation, DNS instructions and discrepancies between filings and receipts. Preserve the request, process, account, transaction and before-and-after record together, with timestamps and custody. This provides the evidence needed to identify the actual transition and direct the response. [FN 2] [FN 3] [FN 16] [FN 20] [FN 49]

Target restrictions to the resource and behavior established in the incident record. Keep historical address matches attached to their dates and acquisition sources. Preserve service-family information

for identifying the provider and administrative history. Confirm both the technical authentication of a message and the authority for its consequential instruction. These steps protect the investigated service while maintaining access to unrelated legitimate resources. [FN 51] [FN 52] [FN 59] [FN 82] [FN 90]

E.4 A concise request for the responsible provider or court office

“We are reviewing PHP2Shell exposure affecting our website or connected communications. Please identify the responsible technical officer, the affected domains and the corrected PHP build serving each site. Preserve the relevant activity, account-change and transaction records, and give us the preservation ticket number. For urgent court business, please identify the controlling filing procedure, authorized intake contact and method for confirming receipt and subsequent handling. We will use the approved secure route for protected materials.” [FN 1] [FN 48] [FN 103]

Endnotes and source register

The original research register contains [FN 1]–[FN 93]. Supplementary media and institutional guidance appears at [FN 94]–[FN 109]. The source numbers from the earlier edition remain unchanged, and the two newly added records are indexed independently. Entries identify publisher, document or report, publication date, evidence supplied and use in the analysis. Public-source titles retain their linked destinations, and expert-report notes retain the source edition and pinpoint locations. [FN 1]–[FN 93]. Supplementary reporting and institutional guidance remain at [FN 94]–[FN 107]. All source numbers are preserved in this edition. The source descriptions identify the document, date, relevant subject matter and analytical or operational use. The original access records are retained, with this revision’s targeted rechecks described in Appendix D. The public and supplied copies of the Coy declaration and permanent order remain linked to the same source identities at [FN 59] and [FN 62].

[FN 1] PHP Project. [Critical PHP security release](#). Date: 2026-10-21. Source and use: Controlling runtime scope, fixed releases, vendor packages, source backports and bounded temporary mitigations. Original access record: Full text retrieved; 2026-10-21. [Recent-window record]

[FN 2] PHP / GitHub Security Advisory. [GHSA-w8hw-w9fx-j79w: RCE via OOM corruption; CVE-2026-109618](#). Date: 2026-10-21. Source and use: Defines the memory-exhaustion root cause, startup/shutdown paths, exploit conditions and CVSS assessment. Original access record: Full text retrieved; 2026-10-21. [Recent-window record]

[FN 3] PHP / GitHub Security Advisory. [GHSA-6wmf-4rv5-p3rp: RCE via stale state; CVE-2026-109619](#). Date: 2026-10-21. Source and use: Defines cross-request stale state and use-after-free; supports worker-aware, multi-request investigation. Original access record: Full text retrieved; 2026-10-21. [Recent-window record]

[FN 4] PHP Foundation. [Today's PHP Security Release, and How We're Strengthening PHP Security](#). Date: 2026-10-21. Source and use: Establishes the 2024 precursor, August 2026 exploitability escalation and accelerated disclosure chronology; records same-day validation differences. Original access record: Full text retrieved; 2026-10-21. [Recent-window record]

[FN 5] CISA. [Critical Vulnerabilities in PHP Require Immediate Patching](#). Date: 2026-10-21. Source and use: Confirms the federal emergency-patching notice. Detailed technical conclusions in this report use PHP and other retrieved primary advisories. Original access record: Official search-index record verified; direct retrieval returned HTTP 403; 2026-10-21. [Recent-window record]

[FN 6] CERT-EU. [Security Advisory 2026-018: PHP critical vulnerabilities](#). Date: 2026-10-21. Source and use: Supports immediate patching and exposure restriction where patching cannot be completed; HTML and associated PDF examined. Original access record: Full text retrieved; 2026-10-21. [Recent-window record]

[FN 7] UK NCSC. [Critical security issue affecting PHP](#). Date: 2026-10-21. Source and use: Independent government warning supporting urgent identification of PHP-dependent services. Original access record: Full text retrieved; 2026-10-21. [Recent-window record]

[FN 8] Netherlands NCSC. [php2shell operational advisory repository](#). Date: Updated 2026-10-21. Source and use: Tracks operational scope and legacy-runtime considerations. An updated operational advisory record. Original access record: Full text retrieved; 2026-10-21. [Recent-window record]

[FN 9] CERT-FR / ANSSI. [CERTFR-2026-AVI-1359: PHP vulnerabilities](#). Date: 2026-10-21. Source and use: French government notice independently anchors affected products and urgent runtime remediation. Original access record: Full text retrieved; 2026-10-21. [Recent-window record]

[FN 10] WordPress. [Critical PHP Security Release](#). Date: 2026-10-21. Source and use: Separates WordPress application maintenance from the PHP fix and identifies the per-site runtime verification route. Original access record: Full text retrieved; 2026-10-21. [Recent-window record]

[FN 11] Calif. [php2shell technical research and disclosure chronology](#). Date: 2026-10-21. Source and use: Provides researcher-side historical context and reproduction development; distinguishes discovery from later public exploitation. Original access record: Full text retrieved; 2026-10-21. [Recent-window record]

[FN 12] Wiz. [PHP2Shell: PHP remote code execution research](#). Date: 2026-10-21. Source and use: Documents independent research, application demonstrations and memory-disclosure/execution implications. Original access record: Full text retrieved; 2026-10-21. [Recent-window record]

[FN 13] Cloudflare. [PHP vulnerabilities: WAF protection](#). Date: 2026-10-21. Source and use: Provides direct provider telemetry about attack traffic and payload adaptation, plus WAF deployment context. Original access record: Full text retrieved; 2026-10-21. [Recent-window record]

[FN 14] watchTower. [PHP RCE FAQ: PHP2Shell](#). Date: 2026-10-20; updated 2026-10-21. Source and use: Reports honeypot exploitation observations. The updated telemetry statement is separated from older unamended FAQ text. Original access record: Full text retrieved; 2026-10-21. [Recent-window record]

[FN 15] Huntress. [Rapid Response: php2shell. Leaked Critical PHP Vulnerabilities](#). Date: 2026-10-20; updated 2026-10-21. Source and use: Provides a time-bounded non-observation in its customer base and explicitly distinguishes an older PHP incident from PHP2Shell. Original access record: Full text retrieved; 2026-10-21. [Recent-window record]

[FN 16] SANS Internet Storm Center. [Critical PHP Vulnerability — Infocon yellow](#). Date: 2026-10-20/21 live incident diary. Source and use: Supplies a concrete public PoC request pattern and explains reliability limits; used for behavioral hunting rather than actor attribution. Original access record: Full text retrieved; 2026-10-21. [Recent-window record]

[FN 17] Canonical / Ubuntu. [USN-8948-1: PHP vulnerabilities](#). Date: 2026-10-21. Source and use: Shows why distribution package revisions, not upstream version strings alone, establish remediation. Original access record: Full text retrieved; 2026-10-21. [Recent-window record]

[FN 18] SiteGround. [Critical PHP vulnerabilities: October 2026](#). Date: 2026-10-21. Source and use: Provider-specific statement about deployed protection; guides the request for account- and site-specific confirmation. Original access record: Full text retrieved; 2026-10-21. [Recent-window record]

[FN 19] Laravel Forge. [PHP security advisory: October 2026](#). Date: October 2026 incident-specific documentation; no separate publication date shown. Source and use: States that Forge automatic security updates do not patch its separately sourced PHP packages; requires server-level action. Original access record: Full text retrieved; 2026-10-21.

[FN 20] Rank Math. [PRO 3.0.123 Security Incident: How to Secure Your Website](#). Date: Notice public 2026-10-16; live revision checked 2026-10-21. Source and use: Controlling distribution window, clean replacement, persistence indicators and recovery sequence. Publication date corroborated by contemporaneous notices. Original access record: Full text retrieved; 2026-10-21. [Recent-window record]

[FN 21] Wordfence. [PSA: Malware Found in Some Rank Math SEO PRO 3.0.123 Downloads](#). Date: 2026-10-16. Source and use: Assigns CVE-2026-111862 and explains why an update alone does not eradicate an activated malicious package. Original access record: Full text retrieved; 2026-10-21. [Recent-window record]

[FN 22] WPScan. [Rank Math SEO: unauthenticated SEO analysis deletion](#). Date: 2026-10-12. Source and use: CVE-2026-104751 is a separate authorization defect, fixed in 1.0.280; prevents conflation with the PRO supply-chain incident. Original access record: Full text retrieved; 2026-10-21. [Recent-window record]

[FN 23] SecurityWeek. [Rank Math PRO WordPress Plugin Compromised in Supply Chain Attack](#). Date: 2026-10-19. Source and use: Documents public alarm and reporting chronology; technical facts are anchored to the vendor and Wordfence. Original access record: Full text retrieved; 2026-10-21. [Recent-window record]

[FN 24] The Hacker News. [Popular WordPress SEO Plugin Rank Math PRO Hijacked to Deliver Self-Restoring Backdoor](#). Date: 2026-10-19. Source and use: Documents public reporting during the requested October 18–20 period and distinguishes distribution from reporting dates. Original access record: Full text retrieved; 2026-10-21. [Recent-window record]

[FN 25] WIRED (Matt Burgess and Lily Hay Newman). [‘This Is Not a Drill’: Critical PHP Vulnerabilities Are Setting the Internet on Fire](#). Date: 2026-10-21. Source and use: Establishes the seriousness of mainstream security coverage; documents the international response and urgency surrounding the release. Original access record: Full text retrieved; 2026-10-21. [Recent-window record]

[FN 26] Reuters (Raphael Satter, Leo Marchandon, Kanjyik Ghosh and Rajveer Pardesi). [EU agency warns websites may need to be taken offline as PHP prepares patches](#). Date: 2026-10-21. Source and use: Records international precautionary disruption and urgency; distinguishes preventive shutdown from confirmed intrusion. Original access record: Full text retrieved; 2026-10-21. [Recent-window record] October 22 display: Government websites go dark after AI-discovered flaw sparks security scramble. The original URL and earlier headline are retained above.

[FN 27] Cloudflare. [eMudhra certificate compromise](#). Date: 2026-10-20. Source and use: Recent cryptographic-trust comparator involving compromised intermediate-certificate keys; supports trust-store and key-custody review. Original access record: Full text retrieved; 2026-10-21. [Recent-window record]

[FN 28] Google Threat Intelligence / Mandiant. [Defending against active exploitation of Citrix NetScaler ADC and Gateway appliances](#). Date: 2026-09-29. Source and use: Direct incident-response evidence includes legal/professional-services targeting, PHP web shells and tunneling after a different initial vulnerability. Original access record: Full text retrieved; 2026-10-21. [Recent-window record]

[FN 29] Citrix. [CTX697096: NetScaler ADC and Gateway security bulletin](#). Date: September 2026; updated 2026-10-12. Source and use: Vendor definitions, configuration conditions, fixes and confirmed exploitation for the NetScaler comparator. Original access record: Full text retrieved; 2026-10-21. [Recent-window record]

[FN 30] CISA. [Critical Zero-Day Vulnerabilities Exploited in Citrix NetScaler ADC, Gateway](#). Date: 2026-09-27; updated 2026-10-09. Source and use: Federal alert corroborates urgency of the separate NetScaler exposure; detailed analysis uses Citrix and Mandiant. Original access record: Official search-index record verified; direct retrieval returned HTTP 403; 2026-10-21. [Recent-window record]

[FN 31] CERT-FR / ANSSI. [CERTFR-2026-AVI-1227: PHP vulnerabilities](#). Date: 2026-09-24. Source and use: Shows that September PHP maintenance levels preceded the October emergency fixes and cannot close the new exposure. Original access record: Full text retrieved; 2026-10-21. [Recent-window record]

[FN 32] FBI, CISA, NSA and international partners. [AA26-281A: Chinese government-linked cyber threat actors combine automated and hands-on hacking tools](#). Date: 2026-10-08. Source and use: 58-page joint advisory; pp. 2, 5–11 and appendices support the known-vulnerability, credential, mailbox-theft and persistent-access comparator. FBI-hosted primary copy retrieved and key pages visually checked. Original access record: Full text retrieved; 2026-10-21. [Recent-window record]

[FN 33] Adobe. [APSB26-146: Adobe Commerce security update](#). Date: 2026-09-07. Source and use: CVE-2026-75650 template-injection RCE and known exploitation demonstrate a separate recent PHP-application emergency. Original access record: Full text retrieved; 2026-10-21. [Recent-window record]

[FN 34] WordPress. [WordPress 7.1.2 Release](#). Date: 2026-09-22. Source and use: Separately tracks WordPress core security maintenance; not a substitute for runtime remediation. Original access record: Full text retrieved; 2026-10-21. [Recent-window record]

[FN 35] WordPress. [WordPress 7.1.3 Maintenance and Security Release](#). Date: 2026-10-06. Source and use: Current application-maintenance reference independently of the October PHP releases. Original access record: Full text retrieved; 2026-10-21. [Recent-window record]

[FN 36] **U.S. Department of Justice.** [Coordinated actions against North Korean remote IT worker schemes affecting more than 70 U.S. companies](#). Date: 2026-10-13. Source and use: Recent official account of false/stolen identities and enterprise access. Charges, arrests and seizures are identified as such, not converted into convictions. Original access record: Full text retrieved; 2026-10-21. [Recent-window record]

[FN 37] **PHP Project.** [Supported Versions](#). Date: Live support schedule checked 2026-10-21. Source and use: Separates upstream lifecycle support from vendor-maintained backports and informs the migration decision. Original access record: Full text retrieved; 2026-10-21.

[FN 38] **cPanel.** [MultiPHP Manager for cPanel](#). Date: Modified 2026-07-08. Source and use: Explains per-domain PHP assignment and inheritance; the selector does not itself attest to a patched package. Original access record: Full text retrieved; 2026-10-21.

[FN 39] **Plesk.** [PHP Settings](#). Date: Live documentation checked 2026-10-21. Source and use: Supports verification of each domain's PHP version, handler and execution context. Original access record: Full text retrieved; 2026-10-21.

[FN 40] **WordPress.** [FAQ: My site was hacked](#). Date: Live documentation checked 2026-10-21. Source and use: Recovery baseline for compromised sites, clean files and credentials; applied to persistent site compromise. Original access record: Full text retrieved; 2026-10-21.

[FN 41] **WordPress Developer Resources.** [Hardening WordPress](#). Date: Live documentation checked 2026-10-21. Source and use: Supports least privilege, trusted software and separation of web-hosting and application responsibilities. Original access record: Full text retrieved; 2026-10-21.

[FN 42] **CISA.** [ED 19-01: Mitigate DNS Infrastructure Tampering — Closed](#). Date: Originally 2019-01-22; closure 2026-01-08. Source and use: Historical DNS-control precedent. Closure status is preserved; the directive is not presented as a current private-sector legal mandate. Original access record: Official search-index record verified; direct site access restricted; 2026-10-21.

[FN 43] **FBI.** [Business Email Compromise](#). Date: Live guidance checked 2026-10-21. Source and use: Independent contact verification and rapid bank/FBI escalation support trusted-channel recovery for consequential instructions. Original access record: Full text retrieved; 2026-10-21.

[FN 44] **FBI.** [North Korean IT Workers Conducting Data Extortion](#). Date: 2025-01-23. Source and use: Earlier government baseline for credential-backed false workers, code theft and post-employment extortion. Original access record: Full text retrieved; 2026-10-21.

[FN 45] **DOJ / Southern District of New York.** [Israeli Hacker-for-Hire Sentenced to 80 Months](#). Date: 2023-11-16. Source and use: Adjudicated commercial hack-for-hire comparator involving paid projects, account theft and selective publication of stolen material. Original access record: Full text retrieved; 2026-10-21.

[FN 46] **DOJ / Southern District of New York.** [Former technology-company employee sentenced for data theft and extortion](#). Date: 2023-05-10. Source and use: Nickolas Sharp case links credential misuse, altered logs, false incident narrative and economic damage; intrusion began December 2020. Original access record: Full text retrieved; 2026-10-21.

[FN 47] **DHS / Cyber Safety Review Board.** [Review of the Summer 2023 Microsoft Exchange Online Intrusion](#). Date: Report 2024-03-20; public release 2024-04-02. Source and use: Government review record for cloud-authentication governance. Specific token mechanics here are grounded in Microsoft's retrieved technical analysis. Original access record: Official report/index and HSDL metadata verified; direct CISA/DHS retrieval blocked (HTTP 403); 2026-10-21.

[FN 48] **NIST.** [SP 800-61 Rev. 3: Incident Response Recommendations and Considerations for Cybersecurity Risk Management](#). Date: 2025-04. Source and use: Organizational incident-response framework supporting the proposed cross-functional containment and recovery work plan. Original access record: Full text retrieved; 2026-10-21.

[FN 49] **NIST.** [SP 800-86: Guide to Integrating Forensic Techniques into Incident Response](#). Date: 2006-08. Source and use: Forensic collection and multi-source analysis foundation; supports provenance, preservation and event correlation. Original access record: Full text retrieved; 2026-10-21.

[FN 50] **NIST.** [SP 800-207: Zero Trust Architecture](#). Date: 2020-08. Source and use: Resource- and identity-centered trust assessment supports rebuilding authority rather than trusting location or appearance. Original access record: Full text retrieved; 2026-10-21.

[FN 51] IETF / RFC Editor. [RFC 7208: Sender Policy Framework](#). Date: 2014-04. Source and use: Defines what SPF evaluates; it is domain authorization for sending infrastructure, not a cryptographic content guarantee. Original access record: Full text retrieved; 2026-10-21.

[FN 52] IETF / RFC Editor. [RFC 6376: DomainKeys Identified Mail Signatures](#). Date: 2011-09. Source and use: Distinguishes the signing domain and signed material from the natural person who purportedly authored an instruction. Original access record: Full text retrieved; 2026-10-21.

[FN 53] IETF / RFC Editor. [RFC 7489: DMARC](#). Date: 2015-03. Source and use: Protocol basis for domain alignment and receiver policy; passing alignment is distinct from authorized business intent. Original access record: Full text retrieved; 2026-10-21.

[FN 54] Amazon Web Services. [Route 53: ChangeResourceRecordSets](#). Date: Live API reference checked 2026-10-21. Source and use: Defines transactional change batches within a hosted zone; automation can coordinate separate changes across zones. Original access record: Full text retrieved; 2026-10-21.

[FN 55] Amazon Web Services. [Logging Route 53 API calls with AWS CloudTrail](#). Date: Live documentation checked 2026-10-21. Source and use: Identifies provider-side identity, request and time evidence needed to reconstruct DNS control; Route 53 event history is in us-east-1. Original access record: Full text retrieved; 2026-10-21.

[FN 56] Microsoft Threat Intelligence. [Analysis of Storm-0558 techniques for unauthorized email access](#). Date: 2023-07-14. Source and use: Primary comparator showing legitimate services accepting forged authentication tokens; used for the described authentication mechanism. Original access record: Full text retrieved; 2026-10-21.

[FN 57] Microsoft Threat Intelligence. [Threat actors misuse OAuth applications to automate financially driven attacks](#). Date: 2023-12-12. Source and use: Documents application-secret and OAuth persistence surviving loss of the initial account; informs token/app-grant containment. Original access record: Full text retrieved; 2026-10-21.

[FN 58] Microsoft Digital Crimes Unit. [Cracked Cobalt Strike: Notice of Pleadings](#). Date: 2023-04-06 public notice. Source and use: Canonical public case portal identifies the action and links sworn declarations; case number is 1:23-cv-02447. Original access record: Full text retrieved; 2026-10-21.

[FN 59] Microsoft DCU / Christopher Coy. [Declaration in support of emergency TRO, Document 2-2](#). Date: Filed 2023-03-30. Source and use: Paragraphs 20–22 and Exhibit 2, p. 5 (PDF p. 41; PageID 370) supply methodology and exact C2 IP matches. URL directory date is not the filing date. Original access record: Full text retrieved; 2026-10-21.

[FN 60] Microsoft / Jason Lyons. [Declaration in support of emergency TRO](#). Date: Filed 2023-03-30. Source and use: Crawling, watermark/configuration and actor-role evidence explain high-fidelity infrastructure attribution. Original access record: Full text retrieved; 2026-10-21.

[FN 61] Microsoft DCU / Rodelio G. Fiñones. [Declaration in support of emergency TRO](#). Date: Filed 2023-03-30. Source and use: Beacon, loader, credential and post-exploitation analysis provides a technical comparator for endpoint claims. Original access record: Full text retrieved; 2026-10-21.

[FN 62] U.S. District Court, E.D.N.Y.. [Microsoft et al. v. John Does, Document 57: permanent injunction](#). Date: 2025-09-08. Source and use: Primary judicial order, publicly mirrored by Justia; defines qualifying infrastructure, preservation, successor process and court control. Original access record: Full text retrieved; 2026-10-21.

[FN 63] Administrative Office of the U.S. Courts. [Cybersecurity Measures Strengthened in Light of Attacks on Judiciary's Case Management System](#). Date: 2025-08-07. Source and use: Official acknowledgment of sophisticated persistent attacks and stronger sensitive-document handling; establishes institutional exposure context. Original access record: Full text retrieved; 2026-10-21.

[FN 64] Administrative Office of the U.S. Courts. [Judges Outline Accelerated Modernization of Case Management System](#). Date: 2026-03-10. Source and use: Official current modernization rationale and acute/persistent CM/ECF risk; distinct from case-specific causation. Original access record: Full text retrieved; 2026-10-21.

[FN 65] NSA, CISA, FBI and partners. [Combatting Cyber Threat Actors Perpetrating Living Off the Land Intrusions](#). Date: 2024-02-07. Source and use: Primary joint guidance describes legitimate-tool abuse, baseline comparison and logging rather than malware-only detection. Original access record: Full text retrieved; 2026-10-21.

- [FN 66] **FBI, CISA and international partners.** [AA23-320A: Scattered Spider](#). Date: Updated 2025-07-29. Source and use: Pages 3 and 6 document help-desk impersonation, MFA transfer and persistent access; supports independent recovery-channel validation. Original access record: Full text retrieved; 2026-10-21.
- [FN 67] **MITRE ATT&CK.** [T1190 — Exploit Public-Facing Application](#). Date: Live classification checked 2026-10-21. Source and use: PHP runtime exploitation is classified by the initial-access behavior. Original access record: Full text retrieved; 2026-10-21.
- [FN 68] **MITRE ATT&CK.** [T1195.002 — Compromise Software Supply Chain](#). Date: Live classification checked 2026-10-21. Source and use: Classifies the poisoned Rank Math distribution path, distinct from a public-facing runtime exploit. Original access record: Full text retrieved; 2026-10-21.
- [FN 69] **MITRE ATT&CK.** [T1078 — Valid Accounts](#). Date: Live classification checked 2026-10-21. Source and use: Classifies use of stolen or unauthorized but accepted accounts. Original access record: Full text retrieved; 2026-10-21.
- [FN 70] **MITRE ATT&CK.** [T1098 — Account Manipulation](#). Date: Live classification checked 2026-10-21. Source and use: Covers persistence through changed account authority, credentials, delegates or devices. Original access record: Full text retrieved; 2026-10-21.
- [FN 71] **MITRE ATT&CK.** [T1114.003 — Email Forwarding Rule](#). Date: Live classification checked 2026-10-21. Source and use: Correct technique for malicious mail-forwarding rules; not T1565.002. Original access record: Full text retrieved; 2026-10-21.
- [FN 72] **MITRE ATT&CK.** [T1505.003 — Web Shell](#). Date: Live classification checked 2026-10-21. Source and use: Classifies persistent server-side command access. Original access record: Full text retrieved; 2026-10-21.
- [FN 73] **MITRE ATT&CK.** [T1565 — Data Manipulation](#). Date: Live classification checked 2026-10-21. Source and use: Separates stored, transmitted and runtime data manipulation from the institutional consequence. Original access record: Full text retrieved; 2026-10-21.
- [FN 74] **MITRE ATT&CK.** [T1584.001 — Compromise Infrastructure: Domains](#). Date: Live classification checked 2026-10-21. Source and use: Classifies compromised domain infrastructure; does not classify every provider change as compromise. Original access record: Full text retrieved; 2026-10-21.
- [FN 75] **MITRE ATT&CK.** [T1557 — Adversary-in-the-Middle](#). Date: Live classification checked 2026-10-21. Source and use: Parent technique for supported interception; T1557.003 specifically means DHCP Spoofing. Original access record: Full text retrieved; 2026-10-21.
- [FN 76] **MITRE ATT&CK.** [T1539 — Steal Web Session Cookie](#). Date: Live classification checked 2026-10-21. Source and use: Identifies session-cookie theft independently of password theft. Original access record: Full text retrieved; 2026-10-21.
- [FN 77] **MITRE ATT&CK.** [T1550.001 — Use Alternate Authentication Material: Application Access Token](#). Date: Live classification checked 2026-10-21. Source and use: Classifies use of application access tokens to impersonate authorized activity. Original access record: Full text retrieved; 2026-10-21.
- [FN 78] **MITRE ATT&CK.** [T1585 — Establish Accounts](#). Date: Live classification checked 2026-10-21. Source and use: Classifies account/persona development; institutional authority requires separate provenance analysis. Original access record: Full text retrieved; 2026-10-21.
- [FN 79] **MITRE ATT&CK.** [T1053.003 — Scheduled Task/Job: Cron](#). Date: Live classification checked 2026-10-21. Source and use: Classifies cron-based persistence relevant to the Rank Math investigation. Original access record: Full text retrieved; 2026-10-21.
- [FN 80] **MITRE ATT&CK.** [S0154 — Cobalt Strike](#). Date: Live classification checked 2026-10-21. Source and use: Software identifier for the tool; used to identify the software examined in the technical record. Original access record: Full text retrieved; 2026-10-21.
- [FN 81] **Marlin Technology.** *Expert Report: Summary Opinion*. Date: December 5, 2024. Pinpoint: pp. 2–5 and 10–13. Source and use: Early independently described device, account, DNS and administrative-control findings; conclusions remain attributed to Marlin. Source: supplied edition; see Appendix C.

[FN 82] Cyber-N.E.T. Forensics. *e-Forensic Integrated Expert Report: Anatomy of the Strategic cAPTure-to-Kill Operation*. Date: October 22, 2025. Pinpoint: printed pp. 26–68, 100–184, 269–300; Appendix A printed pp. 269–271 (PDF pp. 287–289). Source and use: Integrates the subject endpoint, credential, DNS/MX, portal and institutional chronology. Appendix A is compared directly with Coy’s schedule. Source: supplied edition; see Appendix C. Archive location: [Public source archive](#) (public location supplied or indexed; automated retrieval not independently confirmed at this edition).

[FN 83] Cyber-N.E.T. Forensics. *Second Supplemental Expert Report: APT Avatar and E-Court Service Counterfeit Tradecraft*. Date: January 15, 2026. Pinpoint: pp. 2–54, 55–69 and 70–86. Source and use: Persona and official-communication findings read together with the later ORACLE model of event-specific authority. Source: supplied edition; see Appendix C.

[FN 84] Cyber-N.E.T. Forensics. *Forensic Sinkhole Report and Emergency Cyber-Threat Assessment*. Date: January 20, 2026. Pinpoint: pp. 2–10, 24–33; appendix pp. 34–38. Source and use: Registrar/DNS suppression and response findings; appendix redactions and partial indicators are kept out of machine-actionable outputs. Source: supplied edition; see Appendix C.

[FN 85] Cyber-N.E.T. Forensics. *Federal Court Audit Report*. Date: Undated supplied edition. Pinpoint: pp. 1–24, especially 9–13. Source and use: Preserves case-level assignment, exhibit-access, service, replacement and record-state observations for source-native comparison. Source: supplied edition; see Appendix C.

[FN 86] Restricted-Access Portal Solutions Unit / Bridge-Gate ESS. *Federal CM/ECF, DCN and SMTP Email Relay Expert Report*. Date: Cover: February 23, 2026. Pinpoint: pp. 3–11, 24–31 and 38–44. Source and use: Portal workflow, sender/recipient and source/intake/docket object-state examination; filename date is not substituted for cover date. Source: supplied edition; see Appendix C.

[FN 87] Cryptographic Cyber-Defense Group. *Threat Actor Deployment and Exploitation of Cryptographically Manipulated e-Communications*. Date: February 25, 2026. Pinpoint: pp. 7–15; p. 14; Appendix 1, pp. 56–60. Source and use: Communications and portal findings, the specific June 19, 2024 portal indicator and independent-method description; repeated CNF material retains its dependency. Source: supplied edition; see Appendix C.

[FN 88] O.R.A.C.L.E. Detection Response Team. *Institutional, Private Entity and Individual Credential Laundering and Resulting Authority-Rail Compromises*. Date: Cover: July 7, 2026; supplied v52 edition also contains later September references. Pinpoint: printed pp. 1–10; PDF pp. 82–90; full endnotes PDF pp. 108–198 (beginning printed p. 102). Source and use: Identity-to-state-to-reliance model and timed response. Version chronology and actual pagination are preserved; source relationships are preserved across the 574 numbered notes. Source: supplied edition; see Appendix C.

[FN 89] O.R.A.C.L.E.. *Supplemental Authority-Rail Convergence Report*. Date: September 24, 2026. Pinpoint: pp. 1–9 and concluding source notes. Source and use: Receipt/nonresponse transitions, disputed communication authorship, positive controls and the shared ACIS event/document identities. Source: supplied edition; see Appendix C.

[FN 90] Cyber-N.E.T. Forensics. *cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat*. Date: September 2026. Pinpoint: pp. 14–17; Appendix A p. 54; B p. 56; C p. 63; D p. 64; endnotes pp. 65–91. Source and use: Current evidence-dependency and attribution categories; distinguishes exact telemetry from provider/service-family relationships. Source: supplied edition; see Appendix C.

[FN 91] Jay Lewis Farrow / CNF contributors. *Civil Cyber-Infrastructure Disruption Litigation: Report and Recommendations*. Date: September 10, 2026. Pinpoint: main analysis pp. 4–78; actual appendices A p. 79, B p. 96, C p. 100, D p. 101, E p. 102, F pp. 103–110, G p. 111. Source and use: Four-state remedy model, later-victim access and clean-channel proposal. Order-specific monitor provisions are applied to the visibility analysis. Source: supplied edition; see Appendix C. Archive location: [Publisher-supplied public report PDF](#) (public location supplied or indexed; automated retrieval not independently confirmed at this edition).

[FN 92] Jay Lewis Farrow / Private Stock News. *Hired Hackers Use Cyber-Crime Template to Insulate Majority Holders’ Redistribution Schemes*. Date: Header: October 17, 2026; body: October 18, 2026. Pinpoint: pp. 1–10. Source and use: Editorial application to ownership and valuation inputs. Its cited public comparators retain their own evidence records. Source: supplied edition; see Appendix C.

[FN 93] Supplied investigative protocol. *Master Investigative Non-Hedging Protocol*. Date: Undated supplied edition. Pinpoint: sections 1–18 and final refinement; rendered pp. 1–8. Source and use: Methodological instruction: cumulative analysis, sound dependency handling, precise attribution and decisive source-supported conclusions; used for the investigation’s analytical method. Source: supplied edition; see Appendix C.

[FN 94] Forbes / Davey Winder. Critical PHP Security Warning Issued—Apply Emergency Patch Today. 21 Oct 2026.

[Source](#). Summary and use: Contemporaneous pre-patch reporting and risk communication for website owners. Technical version claims are checked against the later PHP advisory. Access: public or indexed result examined October 22, 2026 unless specifically marked otherwise.

[FN 95] BBC News. PHP-related October 2026 coverage: supplied editorial URL. [Source](#). Summary and use: User-supplied reporting route; direct text unavailable in this editorial review. Retained as a reader-follow-up link; technical determinations use the retrieved advisories. Access: public or indexed result examined October 22, 2026 unless specifically marked otherwise.

[FN 96] BleepingComputer / Lawrence Abrams. PHP warns admins of two critical flaws, emergency patches coming tomorrow. 20 Oct 2026. [Source](#). Summary and use: Documents the advance-warning and leak chronology; pre-release statements are not used to override corrected official release facts. Access: public or indexed result examined October 22, 2026 unless specifically marked otherwise.

[FN 97] BleepingComputer / Sergiu Gatlan. PHP ships emergency patches for critical PHP2Shell flaws. 21 Oct 2026. [Source](#). Summary and use: Reports the actual patched versions, deployment scope and late-stage disclosure; checked against the PHP project. Access: public or indexed result examined October 22, 2026 unless specifically marked otherwise.

[FN 98] HackRead / Waqas. PHP Releases Emergency Fixes for Critical PHP2Shell Vulnerabilities. 21 Oct 2026. [Source](#). Summary and use: Explains mod_php/FPM technical distinctions, fixed versions and incomplete workarounds for general readers. Access: public or indexed result examined October 22, 2026 unless specifically marked otherwise.

[FN 99] CNBC. PHP / Google / OpenAI / Amazon cybersecurity report: user-supplied Oct 22 URL. [Source](#). Summary and use: User-provided media reference; direct text was unavailable at the October 22 check. Retained as lead only, retained for reader follow-up with its retrieval status. Access: public or indexed result examined October 22, 2026 unless specifically marked otherwise.

[FN 100] The Hacker News / Swati Khandelwal. PHP Issues Emergency Patches for Two Critical PHP2Shell RCE Flaws as Exploit Attempts Emerge. 21 Oct 2026. [Source](#). Summary and use: Covers the post-release fixed versions, exploit-attempt distinction, possible runtime memory exposure and incomplete temporary mitigations. Access: public or indexed result examined October 22, 2026 unless specifically marked otherwise.

[FN 101] POLITICO / John Sakellariadis and Josh Gerstein. Federal court filing system hit in sweeping hack. 6 Aug 2025. [Source](#). Summary and use: Independent contemporaneous reporting on the judiciary case-management breach; supports the separate 2025 judiciary-security chronology. Access: public or indexed result examined October 22, 2026 unless specifically marked otherwise.

[FN 102] National Security Agency. NSA Advisory: PHP Updates. 21 Oct 2026. [Source](#). Summary and use: U.S. government warning expressly advises taking an unpatchable system offline until fully mitigated; grounds the stop-or-isolate decision. Access: public or indexed result examined October 22, 2026 unless specifically marked otherwise.

[FN 103] Administrative Office of the U.S. Courts. CM/ECF Frequently Asked Questions; governing local-rule principle. [Source](#). Summary and use: Official explanation that electronic filing requirements and alternative procedures arise from each court's local rules and orders, not a single nationwide manual-filing policy. Access: public or indexed result examined October 22, 2026 unless specifically marked otherwise.

[FN 104] U.S. Bankruptcy Court, Southern District of Florida. Filing Papers / Emergency Nonelectronic Filing During Technical Problems. [Source](#). Summary and use: Concrete local-court example permitting specified emergency nonelectronic filings; demonstrates why clerk arrangements must follow the governing court-specific process. Access: public or indexed result examined October 22, 2026 unless specifically marked otherwise.

[FN 105] American Hospital Association. Critical Vulnerabilities Discovered Impacting Popular Programming Language for Websites. 21 Oct 2026. [Source](#). Summary and use: Sector-association alert to executives and IT calling for patch installation and examination of access established before the correction. Access: public or indexed result examined October 22, 2026 unless specifically marked otherwise.

[FN 106] WordPress / John Blackbourn. Critical PHP Security Release. 21 Oct 2026. [Source](#). Summary and use: Official owner-facing step for checking PHP under Site Health; states WordPress update alone does not fix PHP and advises offline status when timely mitigation is unavailable. Access: public or indexed result examined October 22, 2026 unless specifically marked otherwise.

[FN 107] NHS England Digital. Critical Vulnerabilities in PHP (PHP2Shell), CC-4875. 21 Oct 2026. [Source](#). Summary and use: Public-sector advisory provides plain-language attack significance and sector remediation urgency, independent of legal-sector subject attribution. Access: public or indexed result examined October 22, 2026 unless specifically marked otherwise.

[FN 108] Amazon Web Services Security Blog / CJ Moses. Amazon Threat Intelligence identifies PHP2Shell exploitation prior to public disclosure in MadPot. October 21, 2026. [Primary source](#) Evidence supplied: AWS MadPot recorded an October 17 exploitation attempt, followed by additional attack traffic around disclosure; recommends investigation beginning at least October 17. Application: fixes the earliest public attempted-exploitation date and informs log-preservation scope. Retrieved October 22, 2026.

[FN 109] WIRED / Lily Hay Newman. Hackers Exploited the PHP Vulnerabilities Days Before They Were Patched. October 21, 2026. [Primary source](#) Evidence supplied: Independent reporting on the AWS October 17 discovery, the accelerated exploit timeline and response urgency. Application: contemporaneous journalist account; underlying telemetry and precise dates are supported by AWS primary research. Retrieved October 22, 2026.