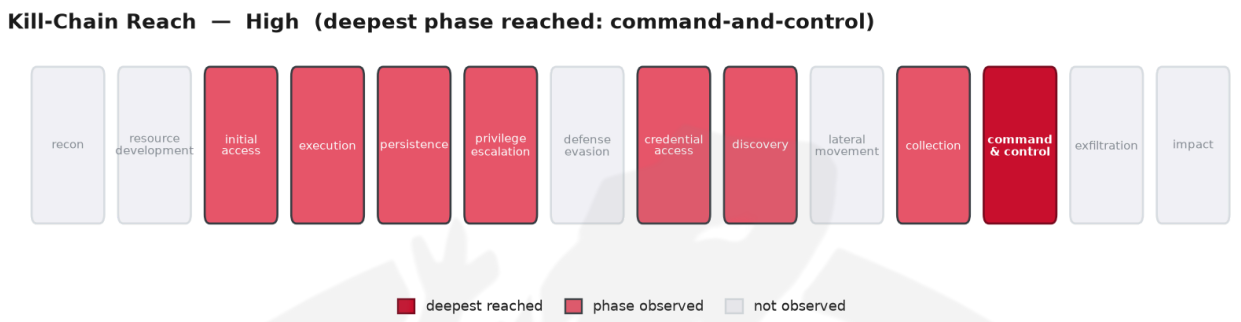
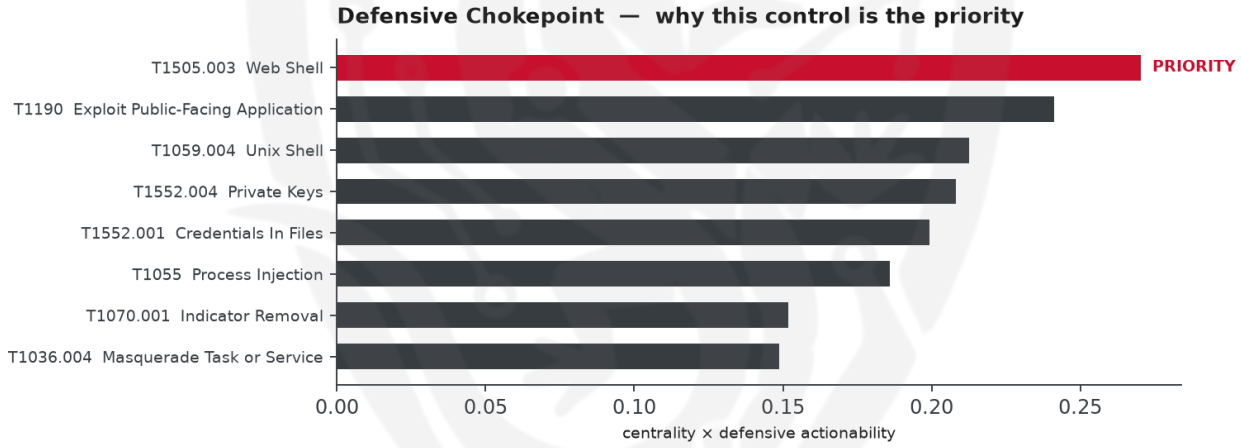
THREAT REPORT: WP-SHELLSTORM

Visual Summary



How far down the attack chain this campaign reached; deepest phase in crimson.



The control that most disrupts the attack (priority in crimson).

Summary

The source attributes this activity to WP-SHELLSTORM, a threat actor that has exposed 1.4 million WordPress sites. The actor has targeted sectors including Finance, Retail, and Technology, utilizing various malware families such as SNOWLIGHT, VShell, BestShell, and Godzilla. Priority should be given to defending against web shells, as this is the identified priority technique. The threat actor's activities pose a high operational risk, reaching command-and-control levels.

Threat Overview

The observed cluster of activity, attributed to WP-SHELLSTORM, involves the use of malware families including SNOWLIGHT, VShell, BestShell, and Godzilla. The victimology indicates that sectors such as Finance, Retail, and Technology have been targeted. However, specific details regarding the central CVE and targeted country are insufficient.

Attack Chain and Priority Control

The attack chain involves a range of techniques, including JavaScript, Cron, System Information Discovery, and others. The priority technique is T1505.003 Web Shell, which serves as a critical chokepoint in the attack chain. To mitigate this threat, the recommended priority control is to "Integrity-monitor web-server directories for web shells; restrict server module/plugin installation."

Infrastructure and Corroboration

The malicious infrastructure associated with WP-SHELLSTORM has been observed to be hosted by providers such as New Century InfoComm Tech Co. Ltd., Alibaba (US) Technology Co. Ltd., and Peg Tech Inc, according to third-party enrichment. However, no malware families have been corroborated by abuse.ch, and AbuseIPDB has reported indicators with a confidence level of up to 52%, but none have reached the 80% confidence threshold.

Technical Appendix

Ground-truth telemetry from the source pulse; analytical scores are secondary and clearly labelled.

Observed Techniques (ATT&CK, expert-tagged by source)

- T1059.007 JavaScript
- T1053.003 Cron
- T1082 System Information Discovery
- T1005 Data from Local System
- T1140 Deobfuscate/Decode Files or Information
- T1190 Exploit Public-Facing Application
- T1055 Process Injection
- T1505.003 Web Shell
- T1552.004 Private Keys
- T1070.001 Indicator Removal
- T1083 File and Directory Discovery
- T1036.004 Masquerade Task or Service
- T1552.001 Credentials In Files
- T1059.004 Unix Shell
- T1027 Obfuscated Files or Information
- T1070.004 File Deletion
- T1071.001 Web Protocols
- T1574.002 Hijack Execution Flow
- T1105 Ingress Tool Transfer
- T1078.004 Cloud Accounts

Analytical Scores

- Priority technique (graph chokepoint): T1505.003 Web Shell (centrality 0.2846).
- Operational risk: High (score 0.636, reaches command-and-control).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.499; reference threshold tau = 0.6).
- These are behavioural resemblances for defensive playbook cross-referencing, not an identity assessment. Where the source pulse names an actor, that attribution is authoritative; the overlaps below neither confirm nor contest it.

Nearest historical profiles by behavioural overlap (resemblance only):

Historical Profile	Behavioural Overlap
APT18	0.499
Rocke	0.4899
Tropic Trooper	0.4115
FIN13	0.4
APT5	0.386

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 52%.

Indicators of Compromise (defanged — non-clickable)

The network and file indicators observed in this activity are listed below for blocklisting:

Type	Indicator	Context
IP	43[.]108[.]17[.]80	AbuseIPDB 10% (KR) · AS45102 Alibaba (US) Technology Co. Ltd.
IP	137[.]175[.]93[.]126	AbuseIPDB 52% (US) · AS54600 Peg Tech Inc
IP	113[.]196[.]56[.]150	AbuseIPDB 22% (TW) · AS9919 New Century InfoComm Tech Co. Ltd.
IP	113[.]196[.]59[.]51	AbuseIPDB 11% (TW) · AS9919 New Century InfoComm Tech Co. Ltd.
Domain	xs[.]xxooonline[.]eu[.]cc	

Type	Indicator	Context
Hash	84f7e396a48913851a10cc78c5cc22a25634564abd0694465236d2f365e2bdee	

Reputation by AbuseIPDB · malware attribution by abuse.ch · Geo/ASN data by IP2Location LITE.

Flame Cell // Adversary Pivot [BETA]

BETA. A hypothetical tabletop projection, anchored to documented ATT&CK behaviour and technique co-occurrence across 170 tracked groups. It is not a prediction; treat it as a war-game prompt and review before acting. Spot a pivot that looks wrong? norbert@salacti.com

- **Control applied:** T1505.003 Web Shell (persistence)
- **Observed here:** WP-SHELLSTORM used T1078.004 Cloud Accounts here as an alternative persistence technique.
- **Projected pivot:** T1078.004 Cloud Accounts (persistence)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

The WP-SHELLSTORM actor could pivot to utilizing Cloud Accounts (T1078.004) as a means to maintain access and achieve their objectives, potentially leveraging compromised cloud account credentials to bypass the blocked web shell access. This may involve exploiting weak cloud account security controls to establish a new foothold, which would likely be a key step in their campaign. The defensive control to counter this potential move would be to Enforce MFA on all accounts; disable dormant and over-privileged accounts; alert on impossible-travel and anomalous logons.

Detection and hardening for the pivot (T1078.004 Valid Accounts)

- **Telemetry:** Windows Security (logon events); Azure AD / IdP sign-in logs; VPN and remote-access logs; Proxy / DLP / data-egress volume telemetry
- **Detect:**
  - Security 4624/4625 (logon success/fail), 4768/4769 (Kerberos TGT/TGS), 4776 (NTLM)
  - Impossible-travel, new-geo, and off-hours sign-ins from the IdP
  - Service or dormant accounts logging on interactively
  - Under valid credentials the identity signal goes quiet: baseline per-account data-egress volume and alert on peer-group and historical deviation (the real exfiltration tell)
- **Harden:**
  - Enforce MFA everywhere; disable stale accounts; rotate exposed credentials
  - Least-privilege review; separate admin from daily-driver accounts
  - Set per-account and per-partner egress baselines with DLP thresholds on sensitive stores
- **MITRE:** M1032 Multi-factor Authentication, M1026 Privileged Account Management, M1027 Password Policies, M1018 User Account Management · DS0028 Logon Session, DS0002 User Account