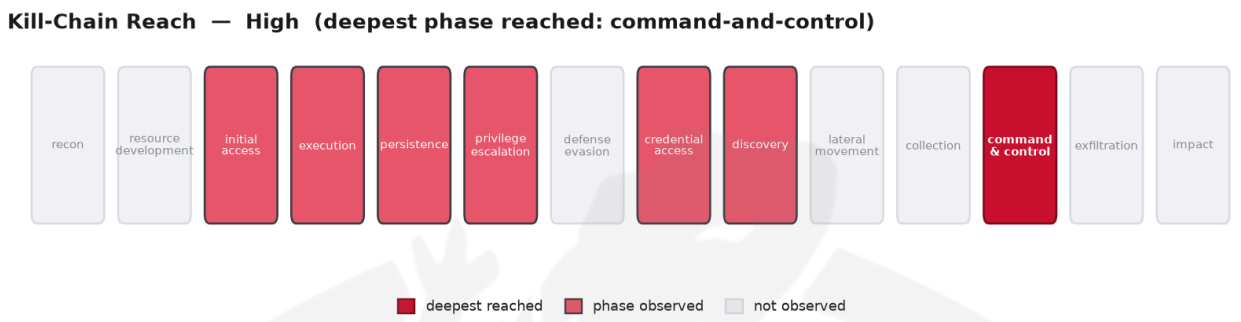
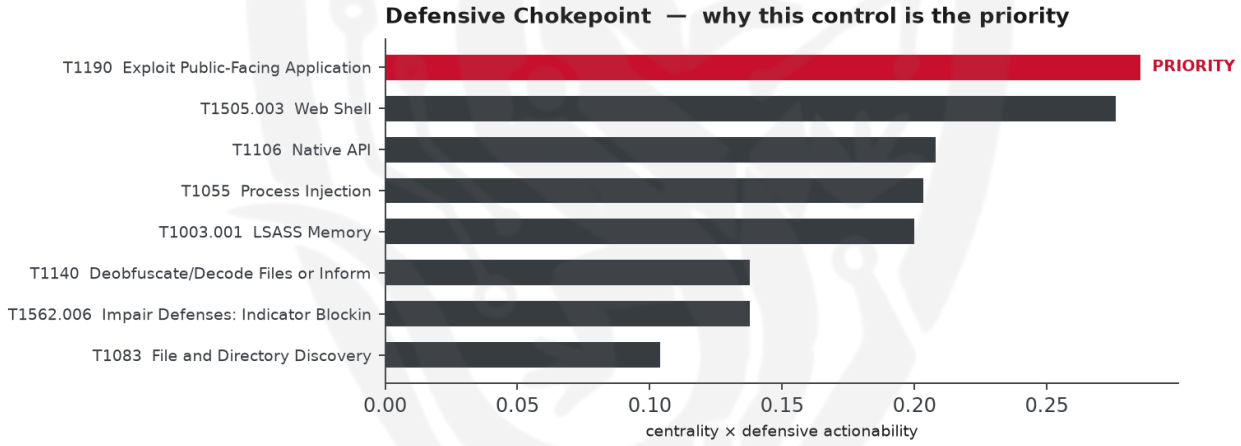
THREAT REPORT: STRIKESHARK CAMPAIGN

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 observed cluster of activity involves the use of custom SharkLoader and Cobalt Strike Beacon malware, targeting government and technology sectors in several countries, including Colombia, Hong Kong, and Indonesia. The threat actor is exploiting the CVE-2025-55182 vulnerability, among others, to gain access to systems. Priority should be given to patching the affected systems and applying a web application firewall (WAF) virtual patch to mitigate the risk. The campaign's impact is considered high, reaching command-and-control levels.

Threat Overview

The threat actor, whose identity is unknown, is utilizing a range of malware families, including SharkLoader, Cobalt Strike, FScan, Searchall, Pillager, and SharpGPOAbuse, to exploit vulnerabilities such as CVE-2025-55182. The targeted countries include Colombia, Hong Kong, Indonesia, Lebanon,

North Macedonia, Nepal, Serbia, Syrian Arab Republic, and Taiwan. The sectors primarily affected are government and technology.

Attack Chain and Priority Control

The observed techniques used by the threat actor form a complex chain, involving scheduled tasks, domain account manipulation, symmetric cryptography, and system checks, among others. The priority technique identified is T1190 Exploit Public-Facing Application, which serves as a chokepoint in the attack chain. To mitigate this risk, the priority control is to: Patch CVE-2025-55182 on all affected systems as the top priority, then: Patch the affected public-facing CVE immediately; apply a WAF virtual patch; restrict management interfaces to VPN-only.

Infrastructure and Corroboration

Although the hosting providers and ASNs observed are not available, abuse.ch has corroborated the use of Cobalt Strike malware in this campaign. However, AbuseIPDB has not flagged any indicators with a confidence level of 80% or higher, with the highest confidence seen being 0%.

Technical Appendix

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

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

- T1053.005 Scheduled Task
- T1087.002 Domain Account
- T1573.001 Symmetric Cryptography
- T1497.001 System Checks
- T1069.002 Domain Groups
- T1135 Network Share Discovery
- T1082 System Information Discovery
- T1106 Native API
- T1140 Deobfuscate/Decode Files or Information
- T1190 Exploit Public-Facing Application
- T1055 Process Injection
- T1505.003 Web Shell
- T1003.001 LSASS Memory
- T1562.006 Impair Defenses: Indicator Blocking
- T1083 File and Directory Discovery
- T1057 Process Discovery
- T1012 Query Registry
- T1027.002 Software Packing
- T1071.001 Web Protocols
- T1018 Remote System Discovery

- T1574.002 Hijack Execution Flow
- T1003.003 NTDS

Analytical Scores

- Priority technique (graph chokepoint): T1190 Exploit Public-Facing Application (centrality 0.2855).
- 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 0.4032; 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
Medusa Group	0.4032
Mustang Panda	0.3933
Volt Typhoon	0.3873
FIN13	0.3795
Stealth Falcon	0.377

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.
- Malware families corroborated by abuse.ch: Cobalt Strike.
- Note: enrichment raises the severity signal (an IOC at or above 80% AbuseIPDB confidence, or a confirmed malware-family hit). This is context, not a change to the source assessment.

Indicators of Compromise (defanged — non-clickable)

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

Type	Indicator	Context
Domain	connect-microsoft[.]com	
Domain	ms-record[.]com	
Domain	ms-record[.]top	

Type	Indicator	Context
Domain	ms-tray[.]top	
Hash	1f65544978b8ea0e745e573b8ee9684b	Cobalt Strike
Hash	24fcebdeecba65004fdb0923763d74fd	
Hash	9c872a0d5d5a38950e8b9ac9b488be3f	
Hash	9cbd560f820c95d7c38342cd558cb5c6	
Hash	a514d1bb62d7916475946fe7c07ac0aa	
Hash	aa3086be652c8b20b0b29b2730d57119	
Hash	b3352b42432dedc4a519f011dc8b5d5a	
Hash	c559cc68986933200fd5d9e4388e2f58	
Hash	d98f568496512e4f98670c61c97cb07a	
Hash	23fd50b3bcc06f5adcbd0122c32260786ec3b98a	
Hash	6a5f9bd0e4a0c385b98cc7b528be53a95ff9c4ccffa8c1f65448ab792a46186c	

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:** T1190 Exploit Public-Facing Application (initial-access)
- **Observed here:** T1190 Exploit Public-Facing Application was the only initial-access technique observed in this campaign, so the pivot is projected from cross-actor behaviour.
- **Projected pivot:** T1078 Valid Accounts (initial-access)
- **Basis:** 32 of 170 documented groups that use Exploit Public-Facing Application also use Valid Accounts (conditional 0.73, lift 1.9, i.e. ~1.9x base rate). Strongest same-tactic neighbour.

The actor could pivot to using T1078 Valid Accounts to maintain access and achieve their objectives, potentially by compromising or reusing existing credentials to bypass the blocked exploit. They may attempt to leverage valid accounts to blend in with normal user activity, making it more challenging to detect their presence. The defensive control to counter this would be to Enforce MFA on all accounts; disable dormant and over-privileged accounts; alert on impossible-travel and anomalous logons.

Also plausible (same tactic): T1133 External Remote Services (n=17, lift 2.3), T1199 Trusted Relationship (n=9, lift 2.9)

Detection and hardening for the pivot (T1078 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