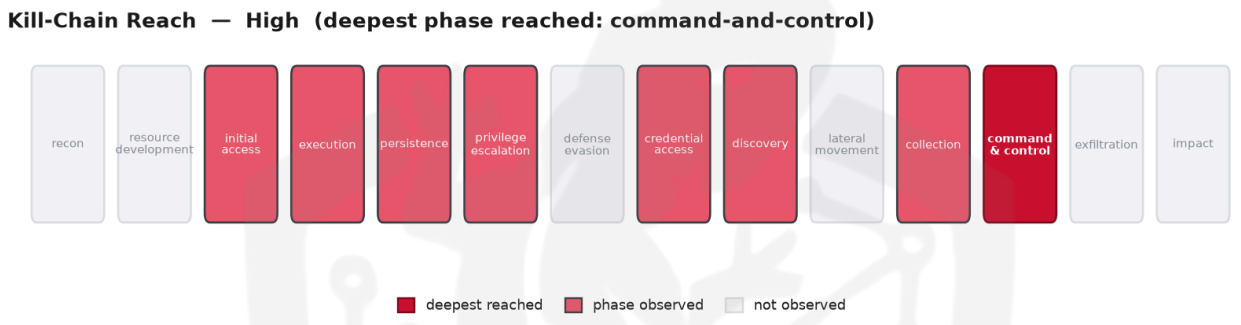
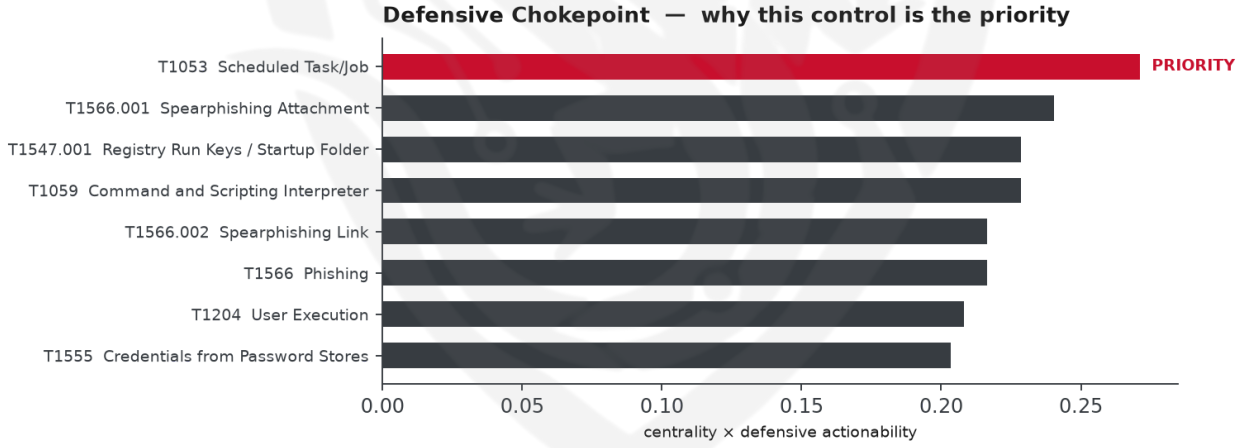
# THREAT REPORT: SILVERFOX, MUSTANG PANDA, AMARANTH-DRAGON, LOTUS BLOSSOM, SHADOW CAMPAIGNS, TRIPLEX, ICARUS, THE GEN

## 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, attributed to SilverFox, Mustang Panda, Amaranth-Dragon, Lotus Blossom, Shadow Campaigns, TripleX, ICARUS, and The Gen by the source, has been targeting the finance, government, technology, telecommunications, insurance, transportation, and aerospace sectors in several countries, including Indonesia, India, and Japan, leveraging the CVE-2025-8088 vulnerability. The threat actor is utilizing various malware families, such as ValleyRAT, ABCDoor, and Cobalt Strike, to compromise systems. Priority should be given to patching the CVE-2025-8088 vulnerability on all affected systems to mitigate the threat.

## Threat Overview

The source attributes this activity to SilverFox, Mustang Panda, Amaranth-Dragon, Lotus Blossom, Shadow Campaigns, TripleX, ICARUS, and The Gen. The malware families used include ValleyRAT, ABCDoor, LOTUSLITE, Cobalt Strike, and others. The central vulnerability exploited is CVE-2025-8088, which is used to target organizations in the finance, government, and other sectors. The victimology indicates that the threat actor is targeting countries such as Indonesia, India, and Japan.

## Attack Chain and Priority Control

The observed techniques used by the threat actor form a complex attack chain, involving scheduled tasks, screen capture, web session cookie theft, and other methods. The priority technique is T1053 Scheduled Task/Job, which serves as a chokepoint in the attack chain. To mitigate this threat, the priority control is to: Patch CVE-2025-8088 on all affected systems as the top priority, then: Alert on new scheduled tasks (Event ID 4698); restrict schtasks/at to admins; baseline legitimate task creators.

## Infrastructure and Corroboration

The malicious infrastructure is hosted on providers such as LLC Smart Ape and Hangzhou Alibaba Advertising Co. Ltd. According to abuse.ch, malware families such as Cobalt Strike and ValleyRAT have been corroborated. 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
- T1113 Screen Capture
- T1539 Steal Web Session Cookie
- T1547 Boot or Logon Autostart Execution
- T1204.002 Malicious File
- T1566.002 Spearphishing Link
- T1566.001 Spearphishing Attachment
- T1082 System Information Discovery
- T1071 Application Layer Protocol
- T1053 Scheduled Task/Job
- T1140 Deobfuscate/Decode Files or Information
- T1555 Credentials from Password Stores
- T1059 Command and Scripting Interpreter
- T1083 File and Directory Discovery
- T1204 User Execution
- T1547.001 Registry Run Keys / Startup Folder
- T1566 Phishing

- T1574 Hijack Execution Flow
- T1027 Obfuscated Files or Information
- T1056 Input Capture
- T1071.001 Web Protocols
- T1574.002 Hijack Execution Flow

## Analytical Scores

- Priority technique (graph chokepoint): T1053 Scheduled Task/Job (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 0.5674; 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 |
|---|---|
| Molerats | 0.5674 |
| Dark Caracal | 0.5507 |
| Confucius | 0.5361 |
| Windshift | 0.5345 |
| Higaisa | 0.5112 |

## Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.
- Malware families corroborated by abuse.ch: Cobalt Strike, Unknown malware, ValleyRAT.
- 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 |
|---|---|---|
| IP | 188[.]127[.]251[.]171 | AbuseIPDB 0% (RU) · AS56694 LLC Smart Ape |

| Type | Indicator | Context |
|---|---|---|
| IP | 59[.]110[.]7[.]32 | AbuseIPDB 0% (CN) · Cobalt Strike · AS37963 Hangzhou Alibaba Advertising Co. Ltd. |
| Domain | emezonhe[.]me | Cobalt Strike |
| Domain | skycloudcenter[.]com | Unknown malware |
| Domain | dog3rj[.]tech | |
| Domain | q74vn[.]live | |
| Domain | abwxjp5[.]me | |
| Domain | servgate[.]me | |
| Domain | pr0fu5a[.]me | |
| Domain | zamstats[.]me | |
| Domain | pickupweb[.]me | |
| Domain | zrheblirsy[.]me | |
| Domain | msonline[.]help | |
| Domain | gouvn[.]me | |
| Domain | abc[.]doublemobile[.]com | ValleyRAT |
| Domain | editor[.]gleeze[.]com | |
| Domain | www[.]cosmosmusic[.]com | |

| Type | Indicator | Context |
|---|---|---|
| Domain | mcagov[.]cc | ValleyRAT |
| Domain | roldco[.]com | ValleyRAT |
| Domain | abc[.]3mkorealtd[.]com | ValleyRAT |
| Domain | abc[.]fetish-friends[.]com | ValleyRAT |
| Domain | abc[.]haijing88[.]com | |
| Domain | abc[.]ilptour[.]com | ValleyRAT |
| Domain | abc[.]petitechanson[.]com | ValleyRAT |
| Domain | abc[.]sudsmama[.]com | ValleyRAT |
| Domain | abc[.]woopami[.]com | ValleyRAT |
| Domain | vnc[.]kcii2[.]com | ValleyRAT |
| Domain | gpsfinance[.]co[.]id | |
| Hash | 4741c2884d1ca3a40dadd3f3f61cb95a59b11f99a0f980dbadc663b85eb77a2a | |
| Hash | 09b0bc41f8838949d5a1c442ee2e2ec9ff892fdc | |
| Hash | a12db7b72879ac0f46079efd8c67e8ca0621f73b | |
| Hash | cc6fd90785a528883b0203138348df8bad69bb1a | |
| Hash | f0b182423107a04cf5f09b8559e656242a4fcc89 | |

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