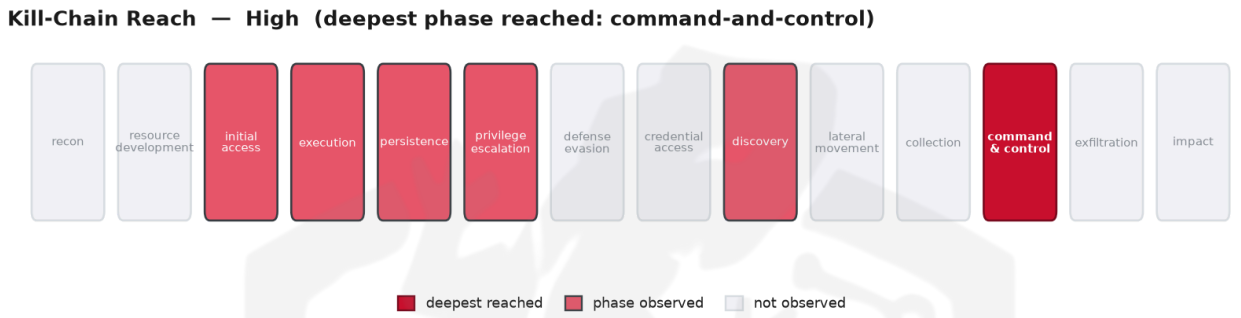
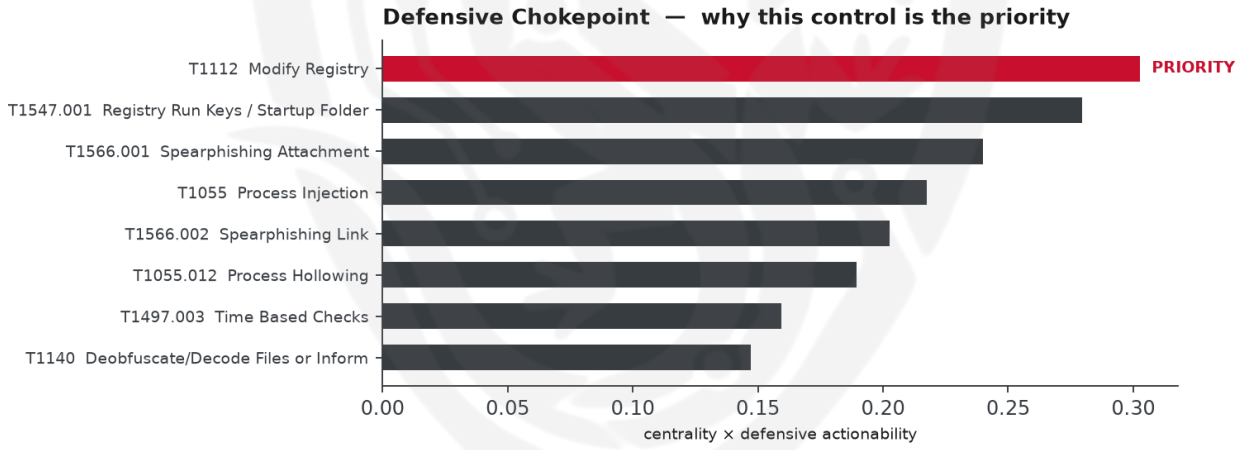
THREAT REPORT: SILVERFOX VALLEYRAT INFECTION CAMPAIGN

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 source attributes this activity to SilverFox, who has been observed distributing ValleyRAT malware through fake installers and Japanese malicious emails. The targeted country and sectors are not specified, but the campaign's operational risk band is considered High, reaching 'command-and-control' levels. Priority should be given to monitoring sensitive registry keys for modification to mitigate the threat. The malware's infection chain involves various techniques, including system checks, spearphishing, and process injection.

Threat Overview

SilverFox is the threat actor behind the ValleyRAT malware family, which is used to infect systems through fake installers and malicious emails. The malware exploits unknown vulnerabilities, and its victimology is

not well-defined due to insufficient data. The techniques used by SilverFox include system checks, spearphishing, process injection, and registry modification.

Attack Chain and Priority Control

The observed techniques used by SilverFox form a complex attack chain, involving initial infection through fake installers or malicious emails, followed by system checks, spearphishing, and process injection. The priority technique is T1112 Modify Registry, which is the graph chokepoint. To mitigate this threat, the priority control is to "Monitor sensitive registry keys for modification; restrict registry-edit tools for unprivileged users."

Infrastructure and Corroboration

The malicious infrastructure associated with this campaign is hosted on Yisu Cloud Ltd, according to third-party observations. Abuse.ch has corroborated the presence of ValleyRAT malware, providing additional context to the threat. However, AbuseIPDB has not flagged any indicators with high confidence, 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)

- T1218.011 Rundll32
- T1204.002 Malicious File
- T1497.001 System Checks
- T1566.002 Spearphishing Link
- T1566.001 Spearphishing Attachment
- T1082 System Information Discovery
- T1140 Deobfuscate/Decode Files or Information
- T1055 Process Injection
- T1497.003 Time Based Checks
- T1112 Modify Registry
- T1083 File and Directory Discovery
- T1547.001 Registry Run Keys / Startup Folder
- T1055.012 Process Hollowing
- T1027 Obfuscated Files or Information
- T1070.004 File Deletion
- T1027.002 Software Packing
- T1574.002 Hijack Execution Flow
- T1105 Ingress Tool Transfer

Analytical Scores

- Priority technique (graph chokepoint): T1112 Modify Registry (centrality 0.3187).
- 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 0.4815; 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
Elderwood	0.4815
The White Company	0.4815
APT19	0.4792
Gorgon Group	0.4783
Patchwork	0.4729

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.
- Malware families corroborated by abuse.ch: 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	154[.]92[.]16[.]22	AbuseIPDB 0% (HK) · ValleyRAT · AS142403 Yisu Cloud Ltd
Domain	frehf[.]oss-cn-hongkong[.]aliyuncs[.]com	malware_download
URL	hxxp://154[.]92[.]16[.]22/xz[.]bin	
Hash	e8be03f19ada1f5cec74b143e21d4939e781671d	

Type	Indicator	Context
Hash	65168c8dd93b16d3b77092fb70c0fa6fba4dffcc	
Hash	eca7ed7b699835fadc2c2997a2845864e02b8dfe	

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:** T1112 Modify Registry (persistence)
- **Observed here:** SilverFox used T1547.001 Registry Run Keys / Startup Folder here as an alternative persistence technique.
- **Projected pivot:** T1547.001 Registry Run Keys / Startup Folder (persistence)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

SilverFox could pivot to using T1547.001 Registry Run Keys / Startup Folder to maintain persistence, potentially by adding malicious entries to the Startup folder or Run/RunOnce registry keys, which may allow them to regain a foothold after the block on modifying the registry. This technique would likely enable SilverFox to execute malicious code automatically when a user logs in, potentially bypassing some security controls. To counter this, the mandated defensive control is to Audit Windows Startup folders and Run/RunOnce registry keys for unauthorized entries; alert on .lnk or script creation in Startup by browser/email temp paths.

Detection and hardening for the pivot (T1547.001 Boot or Logon Autostart Execution)

- **Telemetry:** Sysmon (registry + process); EDR autostart/ASEP inventory
- **Detect:**
  - Sysmon 13 (registry value set) on Run/RunOnce keys under HKLM & HKCU ...\CurrentVersion\Run*
  - Sysmon 11 for shortcuts/scripts created in Startup folders
  - Periodic ASEP (autostart extensibility point) diff against a known-good baseline
- **Harden:**
  - Restrict write access to autostart registry keys and Startup folders
  - Application control to block unsigned autostart binaries
- **MITRE:** M1047 Audit, M1038 Execution Prevention · DS0019 Service, DS0024 Windows Registry, DS0022 File