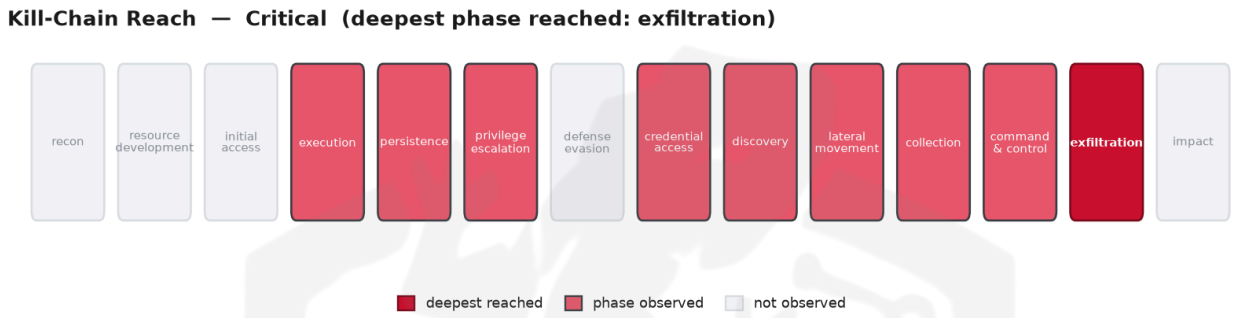
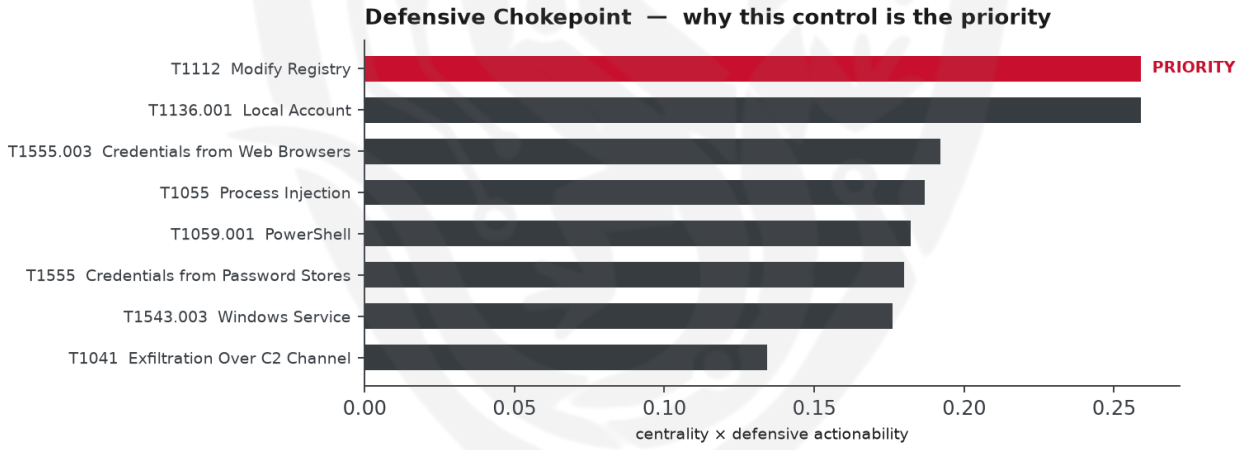
THREAT REPORT: UNKNOWN_ADVERSARY INFOSTEALER CAMPAIGN

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 various infostealer malware families, including StealC, Amadey, Lumma Stealer, RedLine, Raccoon, and Vidar, to target unspecified sectors and countries. The threat actor's goal is to exfiltrate sensitive information, and priority should be given to monitoring sensitive registry keys for modification. The campaign's operational risk band is considered Critical, as it reaches the stage of exfiltration. Defensive actions should focus on restricting registry-edit tools for unprivileged users.

Threat Overview

The threat actor, whose identity is unknown, utilizes a range of malware families to exploit unspecified vulnerabilities. The malware families used include StealC, Amadey, Lumma Stealer, RedLine, Raccoon,

and Vidar, with the latter two being associated with the technique codes S1025. The victimology of this campaign is unclear, but the techniques used suggest a focus on stealing sensitive information from compromised systems.

Attack Chain and Priority Control

The observed techniques used by the threat actor form a complex attack chain, involving techniques such as scheduled tasks, screen capture, system owner/user discovery, and symmetric cryptography. The priority technique, which is the graph chokepoint, is T1112 Modify Registry. To mitigate this, the priority control is to "Monitor sensitive registry keys for modification; restrict registry-edit tools for unprivileged users."

Infrastructure and Corroboration

The malicious infrastructure used in this campaign does not have any observed hosting providers or ASNs. However, abuse.ch has corroborated the presence of Amadey and Stealc malware families. Additionally, 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
- T1033 System Owner/User Discovery
- T1539 Steal Web Session Cookie
- T1573.001 Symmetric Cryptography
- T1543.003 Windows Service
- T1082 System Information Discovery
- T1005 Data from Local System
- T1140 Deobfuscate/Decode Files or Information
- T1555 Credentials from Password Stores
- T1055 Process Injection
- T1112 Modify Registry
- T1555.003 Credentials from Web Browsers
- T1136.001 Local Account
- T1083 File and Directory Discovery
- T1057 Process Discovery
- T1041 Exfiltration Over C2 Channel
- T1059.001 PowerShell
- T1027 Obfuscated Files or Information

- T1012 Query Registry
- T1059.003 Windows Command Shell
- T1071.001 Web Protocols
- T1018 Remote System Discovery
- T1105 Ingress Tool Transfer
- T1021.001 Remote Desktop Protocol

Analytical Scores

- Priority technique (graph chokepoint): T1112 Modify Registry (centrality 0.2725).
- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.6489; 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
Stealth Falcon	0.6489
APT3	0.4682
APT39	0.4375
BlackByte	0.4352
Wizard Spider	0.4239

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.
- Malware families corroborated by abuse.ch: Amadey, Stealc.
- 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	microsoft-telemetry[.]at	malware_download
Domain	svclsc[.]com	Amadey · malware_download
Domain	goodpanelforgoodjob[.]com	
Domain	bartsen284[.]online	
Domain	secure[.]controlpanel[.]asia	Stealc
Domain	cdntestconnect[.]com	Stealc
Domain	spasopro[.]at	Amadey · malware_download
Domain	bluescry[.]com	
Domain	neltron-geltron[.]shop	
Domain	polse[.]us	
Domain	rebustan[.]top	
Domain	roger99699[.]xyz	
URL	hxxp://microsoft-telemetry[.]at/cvdfnaFJBmC0/index[.]php	
URL	hxxp://svclsc[.]com/ms/index[.]php	
URL	hxxps://bartsen284[.]online/39d9612df78e45b5a4bb[.]php	
URL	hxxp://secure[.]controlpanel[.]asia/330311481fe14ab99814[.]php	
URL	hxxp://cdntestconnect[.]com/ed54b97a570943999715[.]php	
URL	hxxp://spasopro[.]at/Lsge63sd3/index[.]php	
URL	hxxp://bluescry[.]com/01f96fd710e905ca2326[.]php	

Type	Indicator	Context
URL	hxxp://goodpanelforgoodjob[.]com/hg8jjfSr5hy/index[.]php	
URL	hxxp://polse[.]us/62ea47cac2534aa18f74[.]php	
URL	hxxp://rebustan[.]top/gd7djkDveE2/index[.]php	
URL	hxxp://roger99699[.]xyz/425f1faf4b214434b8a3[.]php	
URL	hxxps://neltron-geltron[.]shop/e396586b99ee49d19cc3[.]php	
Hash	f89ad7e92c7de6945ce0878e470e388b	Amadey
Hash	d4f8f562b4a109cccbc0dbdf28bc6d033d7891fb	Amadey
Hash	8cef760d11d24fc2e9bbd9f770dca5105854f7ece3b0e6948d7c8b7fdd1765ea	Amadey
Hash	98e504cc7125b79eda5491f40b998605a05f4cd968b961aab4cce7beb074fefe	Amadey
Hash	0215f734867bd71c57ff5c524d8cc670be5b4f1861b2c390cf46d18784a53624	Stealc
Hash	349c233c4e1b6c0724e5ec84df16188d	
Hash	95b318d953fd939f284efe2be78fe95b	
Hash	a025b901a7979bff2a6c6e4e74c7c76a	Amadey
Hash	2f3d86e77248b23ef93b7b8c2a9915b2eace5d46	
Hash	72cab50156ba4e2d5f4de97f672d4635e98ddacc	Amadey
Hash	7493c316df2727dd19ef14593fcc014bdb2a0d4b	
Hash	1246c5b89ab668c1137f377507bc3e266a98e93248382aa026610ae1e764a497	
Hash	2a0f053855da59b3b56812e580d7baeba59fc9493694722aa9e3f121ee3363f1	
Hash	30cef3d3d956e83e2c50579cfbe57a49159cccbcc8b0b0422f27d55e1c401ad9	
Hash	43455f1ff4a623b783da670d052eb77eaaacb0c66a9f1e8508f802bf22e8129e	
Hash	5f5b25b2e35d404034d0d60975cf1ffbc6f141761ec3f4f15d6f7c6213a056f6	

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:** the threat actor used T1053.005 Scheduled Task here as an alternative persistence technique.
- **Projected pivot:** T1053.005 Scheduled Task (persistence)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

The actor could pivot to utilizing T1053.005 Scheduled Task to maintain persistence and execute malicious code at a later time, potentially bypassing initial defenses by scheduling tasks that blend in with legitimate system activity. This technique may allow the actor to regain a foothold in the system, as scheduled tasks can be used to execute commands or scripts without immediate detection. To counter this, the defensive control would involve alerting on new scheduled tasks (Event ID 4698); restricting schtasks/at to admins; baseline legitimate task creators.

Detection and hardening for the pivot (T1053.005 Scheduled Task/Job)

- **Telemetry:** Windows Security (Object Access audit); Microsoft-Windows-TaskScheduler/Operational; Sysmon
- **Detect:**
  - Security 4698 (task created), 4702 (updated), 4700/4701 (enabled/disabled), 4699 (deleted)
  - TaskScheduler/Operational 106 (registered), 140 (updated), 141 (deleted)
  - Sysmon 1 for schtasks.exe and at.exe; Sysmon 11 for writes under C:\Windows\System32\Tasks\
- **Harden:**
  - Restrict schtasks/at to administrators; disable the legacy at.exe
  - Baseline the legitimate task creators and alert on anything outside it
- **MITRE:** M1047 Audit, M1028 Operating System Configuration, M1026 Privileged Account Management · DS0003 Scheduled Job, DS0009 Process, DS0022 File