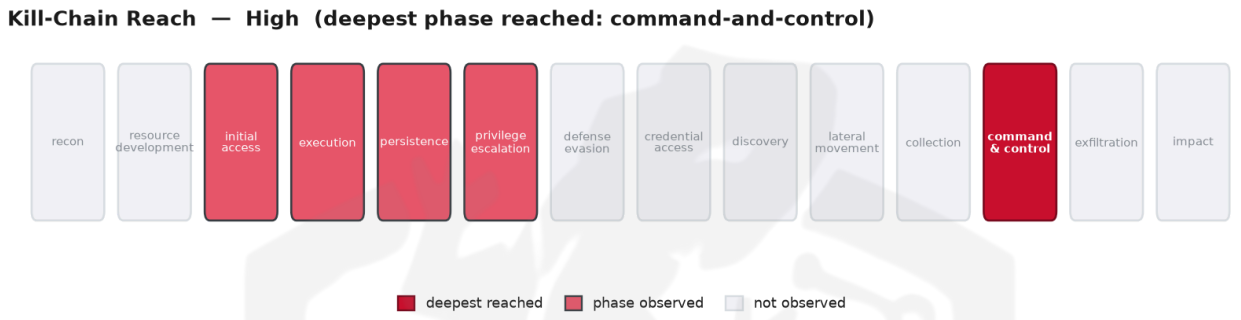
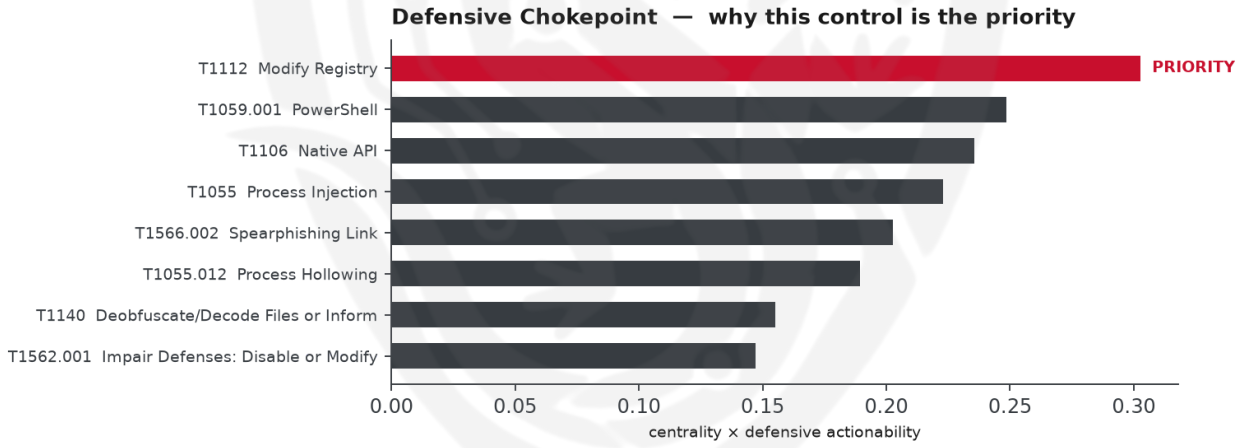
THREAT REPORT: UNKNOWN_ADVERSARY CAMPAIGN

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 has been linked to the use of AsyncRAT and ScreenConnect malware families, although the targeted country and sectors remain unknown. The threat actor's campaign has exposed a significant risk, warranting priority defensive action. Priority should be given to monitoring sensitive registry keys for modification to mitigate the threat. The operational risk band of this campaign is considered high, reaching command-and-control levels.

Threat Overview

The threat actor, whose identity is currently insufficient to determine, has been observed utilizing the AsyncRAT and ScreenConnect malware families. The central vulnerability exploited in this campaign is

unknown, but the actor has employed various techniques to achieve their goals. The victimology of this campaign also remains unclear due to insufficient data.

Attack Chain and Priority Control

The observed techniques used by the threat actor form a complex chain, including scheduled tasks, matching legitimate resource names, and malicious file usage, among others. The priority technique identified in this chain is T1112 Modify Registry, which serves as a critical chokepoint. To counter 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 associated with this campaign is hosted on providers such as dataforest GmbH and Dynu Systems Incorporated. Additionally, abuse.ch has corroborated the use of the AsyncRAT malware family in this campaign. However, according to AbuseIPDB, none of the indicators have reached an 80% confidence level, with the highest confidence seen being 1%.

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
- T1036.005 Match Legitimate Resource Name or Location
- T1204.002 Malicious File
- T1566.002 Spearphishing Link
- T1218.004 InstallUtil
- T1218.007 Msiexec
- T1106 Native API
- T1140 Deobfuscate/Decode Files or Information
- T1055 Process Injection
- T1112 Modify Registry
- T1059.001 PowerShell
- T1562.001 Impair Defenses: Disable or Modify Tools
- T1055.012 Process Hollowing
- T1027 Obfuscated Files or Information
- T1071.001 Web Protocols
- T1059.005 Visual Basic
- 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 0.6124; 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
Rancor	0.6124
Machete	0.5941
Molerats	0.5715
WIRTE	0.5354
Gorgon Group	0.5108

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 1%.
- Malware families corroborated by abuse.ch: AsyncRAT.
- 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	185[.]254[.]97[.]249	AbuseIPDB 0% (DE) · AS58212 dataforest G mbH
IP	2[.]59[.]134[.]97	AbuseIPDB 1% (DE) · AS58212 dataforest G mbH
IP	162[.]216[.]241[.]242	AbuseIPDB 1% (US) · AS398019 Dynu Systems Incorporated
IP	45[.]145[.]41[.]205	AbuseIPDB 0% (DE) · AS58212 dataforest G mbH

Type	Indicator	Context
Domain	corel-draw[.]net	
Domain	vlc-player[.]net	
Domain	processhacker[.]net	
Domain	km-player[.]com	
Domain	defender-control[.]com	
Domain	crusader-kings[.]com	
Domain	arma-reforger[.]com	
Domain	obs-studio[.]site	
Domain	obs-studio[.]pro	
Domain	studio-obs[.]com	
Domain	studio-obs[.]net	
Domain	winservec[.]net	
Domain	mora1987[.]work[.]gd	AsyncRAT
Domain	serverdnsplan[.]net	
Domain	free-download[.]camdvr[.]org	
Domain	managedevice[.]xyz	

Type	Indicator	Context
Domain	pingpanl[.]pro	
Domain	manageserver[.]xyz	
Domain	r[.]servermanagemen[.]xyz	
Domain	r[.]manage-server[.]xyz	
Domain	ehostservers[.]xyz	
Domain	crosshairx[.]pro	
Domain	crosshairx[.]site	
Domain	fileget[.]loseyourip[.]com	
Domain	km-player[.]pro	
Domain	kms-tools[.]com	
Domain	vlc-media[.]com	
Domain	vlc-media[.]net	
Domain	download-full-version[.]ooguy[.]com	
Domain	servermanagemen[.]xyz	
Hash	8e4c57358a66eb14d31abb614ddc68de	
Hash	c2679a152084f3ebdb39aacb6ec6a23c61a46ae6	
Hash	6ed15aec7504081c3e14a9f6064d7b754aa283e4adb1a59edf3beff65369bc55	

Type	Indicator	Context
Hash	01325880efffec546f59490089a3b415	
Hash	0eee9bad07e22415439e854657fa1366	
Hash	1e6a5c7b620d487d0cfc6874c3b77c90	

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 threat actor could pivot to utilizing Scheduled Task (T1053.005) to maintain persistence and execute malicious code at a later time, potentially evading detection by blending in with legitimate system activity. This technique may allow the actor to regain a foothold in the system, should they have previously established access. To counter this potential move, 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