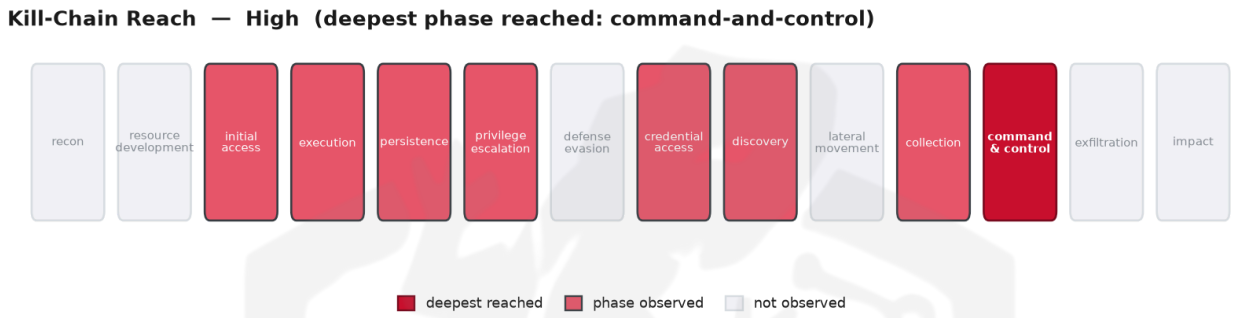
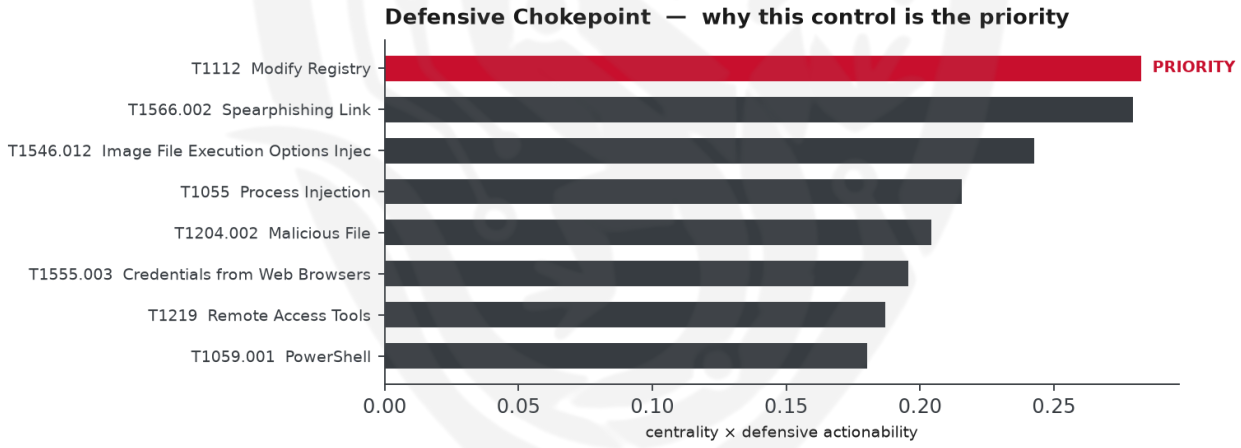
THREAT REPORT: UNKNOWN_ADVERSARY CRYSOME RAT INFECTION

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 CrySome RAT and WinDefCtl malware families, although the targeted country and sectors remain unknown. The threat actor's use of various techniques, including scheduled tasks and screen capture, allows for persistence and data theft. Priority should be given to monitoring sensitive registry keys for modification to mitigate the threat. The operational risk band is considered high due to the potential for command-and-control capabilities.

Threat Overview

The threat actor, whose identity is unknown, utilizes the CrySome RAT and WinDefCtl malware families to infect systems. The central vulnerability exploited is unknown, but the actor employs a range of techniques, including scheduled tasks, screen capture, keylogging, and bypassing user account control.

The victimology and targeted sectors are also unknown, making it challenging to determine the scope of the threat.

Attack Chain and Priority Control

The observed techniques used by the threat actor form a complex chain, starting with initial infection and leading to persistence and data theft. The priority technique is T1112 Modify Registry, which is a critical chokepoint in the attack chain. To counter this, the priority control is to "Monitor sensitive registry keys for modification; restrict registry-edit tools for unprivileged users."

Infrastructure and Corroboration

There is no available information on the hosting providers or ASNs observed, and no malware families have been corroborated by abuse.ch. Additionally, no indicators have been flagged with a confidence level of 80% or higher by AbuseIPDB, 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
- T1056.001 Keylogging
- T1548.002 Bypass User Account Control
- T1036.005 Match Legitimate Resource Name or Location
- T1204.002 Malicious File
- T1566.002 Spearphishing Link
- T1082 System Information Discovery
- T1140 Deobfuscate/Decode Files or Information
- T1219 Remote Access Tools
- T1055 Process Injection
- T1112 Modify Registry
- T1555.003 Credentials from Web Browsers
- T1546.012 Image File Execution Options Injection
- T1059.001 PowerShell
- T1562.001 Impair Defenses: Disable or Modify Tools
- T1027 Obfuscated Files or Information
- T1071.001 Web Protocols
- T1105 Ingress Tool Transfer

Analytical Scores

- Priority technique (graph chokepoint): T1112 Modify Registry (centrality 0.2974).
- 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 0.5173; 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
APT37	0.5173
Molerats	0.5004
Ajax Security Team	0.4869
Rancor	0.4811
APT42	0.4772

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.

Indicators of Compromise (defanged — non-clickable)

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

Type	Indicator
Domain	signindat[.]com
URL	hxxps://signindat[.]com/ElevatorShellCode[.]exe
URL	hxxps://signindat[.]com/update[.]exe
URL	hxxps://signindat[.]com/patch[.]exe
URL	hxxps://signindat[.]com/stage[.]ps1
URL	hxxps://signindat[.]com/Rate_Confirmation_LD-2026-0847[.]pdf
URL	hxxps://signindat[.]com

Type	Indicator
Hash	ff5dbdcf6d7ae5d97b6f3ef412df0b977ba4a844c45b30ca78c0eeb2653d69a8
Hash	f8a3f28ecbd0b08ecab73ef571f16c3d0bd5e009
Hash	2f4b5a0d98bc4e5616f2dd04337ae674
Hash	ec68666e8f0a3b9870d7177bab684c8dcfb8ca0bc7c8c484a71b2b33ea4e26f4
Hash	53f1da8a032115aa682749a114f4cfebcb5ef933400a89b4bbfa84f2057222ff
Hash	ced4407f4ac7e43c1a3010a394d111d2ad1b50a2e95668b4e9cfe739235e67bd
Hash	b7ca8fd9ebe0a76f16deea315fac7ee94dcb18e6ac2832b5c4cb562fbc6e0ed3
Hash	c380268d493e0cba914ce2bc55faa1d7c050c599893c3196fee01fa745e6466a
Hash	45a2228e44257169210cc5dc06e12a6c
Hash	de2df0905ece1a1e7f0a70adf36c75deb06b4e4b

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 leveraging the Windows Task Scheduler. This technique may allow the actor to blend in with legitimate system activity, making it more challenging to detect. The defensive control to counter this would be to alert on new scheduled tasks (Event ID 4698); restrict 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