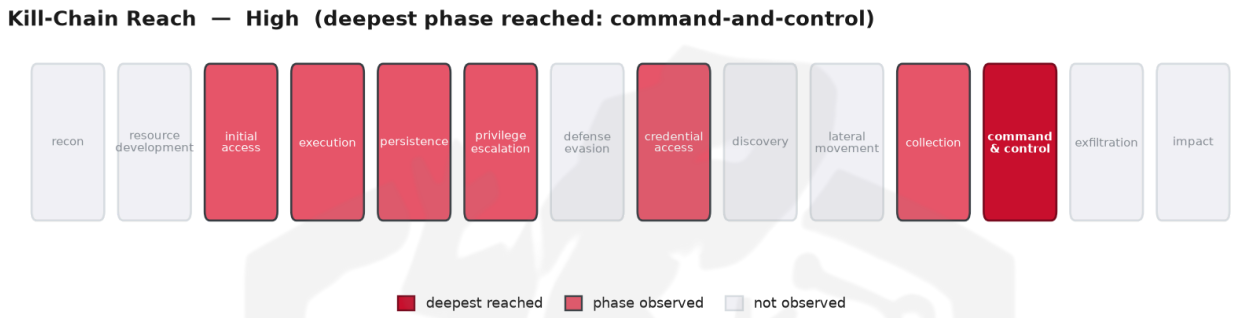
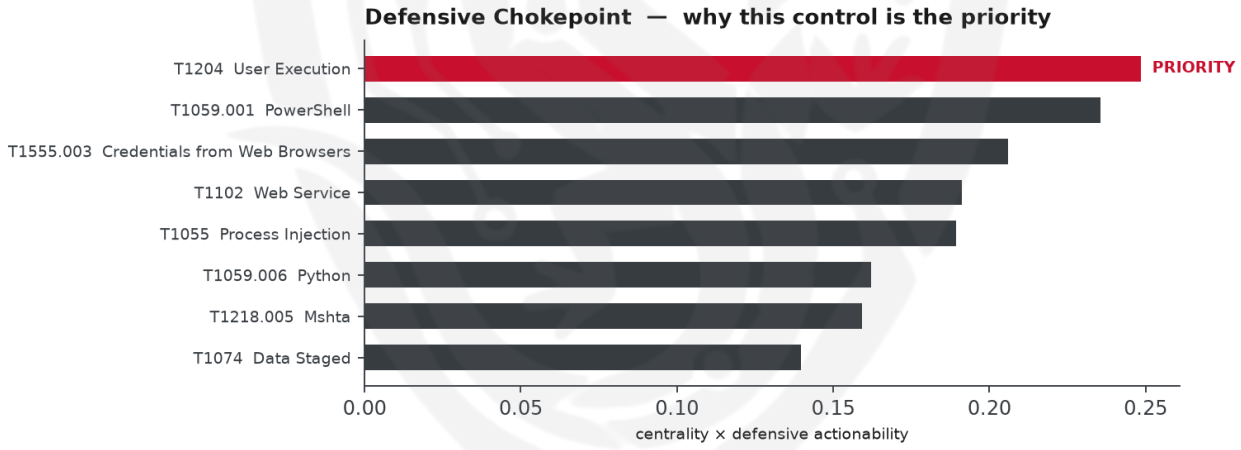
THREAT REPORT: UNKNOWN_ADVERSARY ACR STEALER CAMPAIGN

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 ACR Stealer and Amatera Stealer malware families, although the threat actor remains unidentified. The campaign's targets and sectors are currently unknown. Priority should be given to blocking the execution of potentially malicious files and raising user awareness about phishing lures. Defensive actions should focus on preventing the initial stages of the attack chain.

Threat Overview

The threat actor, whose identity is currently unknown, is utilizing the ACR Stealer and Amatera Stealer malware families. The central vulnerability exploited in this campaign is not specified. The victimology of this campaign is also not well understood, with targeted countries and sectors remaining unknown.

Attack Chain and Priority Control

The attack chain involves a series of techniques, including scheduled tasks, rundll32, and process injection, ultimately leading to the exfiltration of sensitive data. The priority technique in this chain is T1204 User Execution, which serves as a critical chokepoint. To mitigate this threat, the recommended priority control is to "Block execution of downloaded HTA/JS/LNK; enforce mark-of-the-web; disable Office macros from the internet; user awareness on lures."

Infrastructure and Corroboration

There is currently no available information on the hosting providers or ASNs used by the threat actor, and no malware families have been corroborated by abuse.ch. 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
- T1218.011 Rundll32
- T1070.003 Clear Command History
- T1005 Data from Local System
- T1036 Masquerading
- T1055 Process Injection
- T1555.003 Credentials from Web Browsers
- T1074 Data Staged
- T1102 Web Service
- T1218.005 Mshta
- T1204 User Execution
- T1059.001 PowerShell
- T1027 Obfuscated Files or Information
- T1027.003 Steganography
- T1059.006 Python
- T1059.003 Windows Command Shell
- T1189 Drive-by Compromise
- T1102.001 Dead Drop Resolver

Analytical Scores

- Priority technique (graph chokepoint): T1204 User Execution (centrality 0.3105).
- 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 0.4945; 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	0.4945
Machete	0.4551
Patchwork	0.4466
RedCurl	0.4307
BRONZE BUTLER	0.4107

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	proton-network[.]com
Domain	ux[.]strainedeasily[.]icu
Domain	looksta[.]icu
Domain	fast[.]raidher[.]icu
Domain	apigrokcloud[.]icu
Domain	deep-harborio[.]com
Domain	zealpraxis[.]com
Domain	prism-vertex[.]com
Domain	auramatrixa[.]com

Type	Indicator
Domain	cpppemwjewjoiwejow[.]sale
Domain	creativecommunityinfo[.]art
Domain	enhanceblabber[.]cc
Domain	prism-matrixs[.]com
Domain	breaksd[.]wifihot[.]icu
Domain	contrite[.]quirksturdy[.]icu
Domain	walter[.]filloco[.]icu

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:** T1204 User Execution (execution)
- **Observed here:** the threat actor used T1053.005 Scheduled Task here as an alternative execution technique.
- **Projected pivot:** T1053.005 Scheduled Task (execution)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

The actor could pivot to using T1053.005 Scheduled Task to maintain persistence and execute malicious code at a later time, potentially bypassing the block on user execution 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. To counter this, the defensive control 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