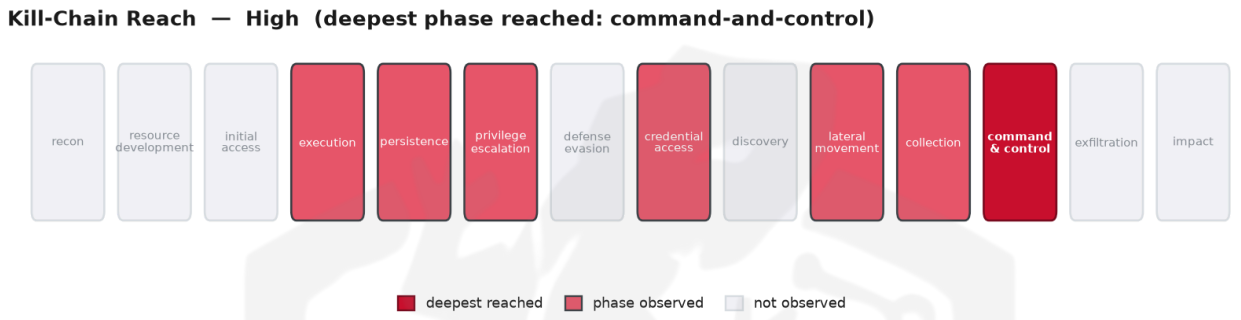
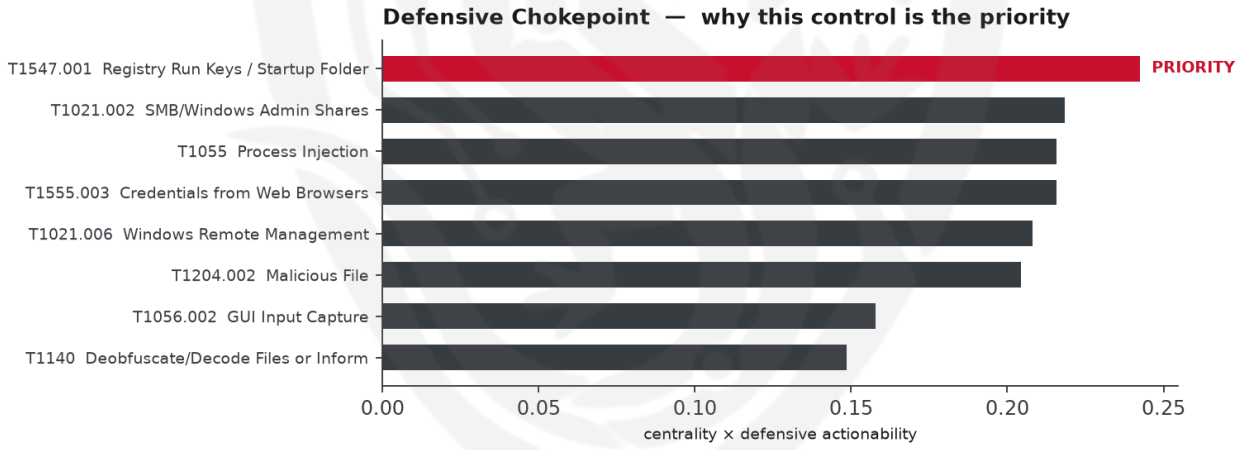
THREAT REPORT: UNKNOWN_ADVERSARY CAMPAIGN

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 involves the use of multiple malware families, including Potemkin, RMMProject, EtherRAT, and Chisel, to target unknown sectors and countries. The threat actor's goals and motivations are unclear, but the priority defensive action should be to audit Windows Startup folders and Run/RunOnce registry keys for unauthorized entries. Priority should be given to monitoring for suspicious activity, particularly the creation of .lnk or script files in Startup by browser or email temporary paths. The operational risk band for this threat is considered High, indicating a potential command-and-control capability.

Threat Overview

The threat actor, whose identity is unknown, utilizes a range of malware families and techniques to achieve their objectives. The malware families involved include Potemkin, RMMProject, EtherRAT, and Chisel, although the central vulnerability exploited is insufficiently documented. The victimology of this campaign is also unclear, with insufficient data on targeted countries and sectors.

Attack Chain and Priority Control

The observed techniques employed by the threat actor form a complex chain, involving scheduled tasks, Windows Management Instrumentation, keylogging, and domain generation algorithms, among others. The priority technique identified is T1547.001 Registry Run Keys / Startup Folder, which serves as a critical chokepoint in the attack chain. To mitigate this threat, the priority 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."

Infrastructure and Corroboration

Although the hosting providers and ASNs observed are not available, third-party corroboration from abuse.ch indicates the presence of the MetaStealer malware family. However, according to AbuseIPDB, there are no indicators with a confidence level of 80% or higher, and the highest confidence seen is 0%. These findings provide additional context but do not override the primary source pulse.

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
- T1047 Windows Management Instrumentation
- T1056.001 Keylogging
- T1568.002 Domain Generation Algorithms
- T1036.005 Match Legitimate Resource Name or Location
- T1204.002 Malicious File
- T1218.007 Msiexec
- T1140 Deobfuscate/Decode Files or Information
- T1055 Process Injection
- T1021.002 SMB/Windows Admin Shares
- T1555.003 Credentials from Web Browsers
- T1021.006 Windows Remote Management
- T1218.005 Mshta
- T1547.001 Registry Run Keys / Startup Folder
- T1056.002 GUI Input Capture
- T1562.001 Impair Defenses: Disable or Modify Tools
- T1027 Obfuscated Files or Information

- T1573 Encrypted Channel
- T1071.001 Web Protocols

Analytical Scores

- Priority technique (graph chokepoint): T1547.001 Registry Run Keys / Startup Folder (centrality 0.2553).
- 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 0.4536; 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
Molerats	0.4536
TA2541	0.4374
RedCurl	0.4148
TA551	0.3941
Inception	0.3889

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.
- Malware families corroborated by abuse.ch: MetaStealer.
- 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	resumeacceptable[.]com	
Domain	cl[.]distritovagas[.]com	malware_download

Type	Indicator	Context
Domain	sonra[.]eutialyson[.]com	malware_download
Domain	pestrear-lamp[.]xyz	
Domain	anus-staylard[.]xyz	
Domain	fair-bath-fond[.]xyz	
Domain	rule-bead-dust[.]xyz	
Domain	uglyshop-mare[.]xyz	
URL	hxxp://sonra[.]eutialyson[.]com/inst24[.]msi	
URL	hxxps://cl[.]distritovagas[.]com/hte[.]hta	malware_download
URL	hxxp://77[.]110[.]122[.]58:23205/cons_1[.]0[.]1[.]msi	
URL	hxxp://77[.]110[.]122[.]58:23205/lQhEQui9a4lZ[.]exe	
URL	hxxp://77[.]110[.]122[.]58:23205/lQhEQui9a4lZ[.]exe'	
URL	hxxp://77[.]110[.]122[.]58:44479/bjxxUmG8K3uy[.]ps1	
URL	hxxps://resumeacceptable[.]com	
Hash	79f7b67ce8b39070f3e1c2b90fce0ce84134782a7dedcccc1edac197ee9e089b	MetaStealer
Hash	d37cc44db90a65341263deb162024447	MetaStealer
Hash	4537b37b65e9dc35640d750f3fa7f4944534f6b1	MetaStealer
Hash	2abe5dd3a057fdef935722e50e9251c272d29fd26113187b853a1f9a9cb89d9b	
Hash	2ada24dd6e517f37942b749c2bd57ddd97445e9853002cee70a0bc30d0b0ce3a	
Hash	3b7ae925e2d64522b4f69b56285b05aeca8c5aab5ab46a9c02c4fafb69d881ce	
Hash	cd4e5e2c65b1660470d3446539ee68adf5faeece3eaeb46583623be9911ee145	

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:** T1547.001 Registry Run Keys / Startup Folder (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 Scheduled Task (T1053.005) to maintain persistence and execute malicious code at a later time, potentially bypassing the blocked Registry Run Keys / Startup Folder control. This technique may allow the actor to blend in with legitimate system activity, making it more challenging to detect. To counter this potential move, 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