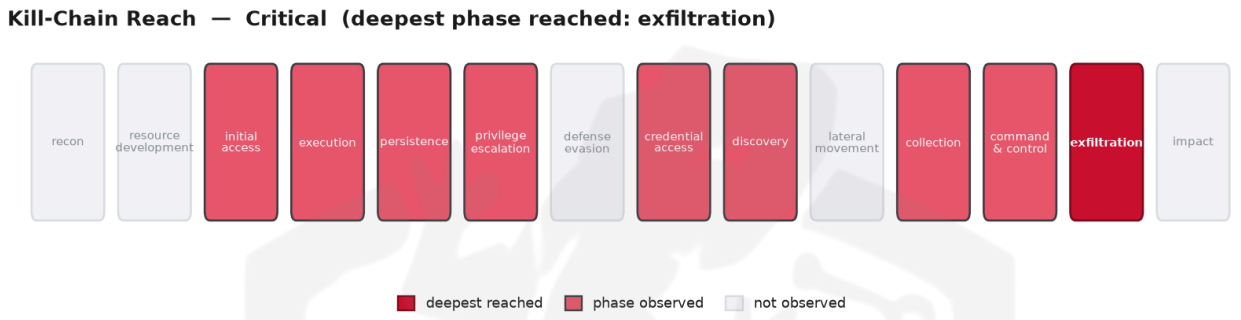
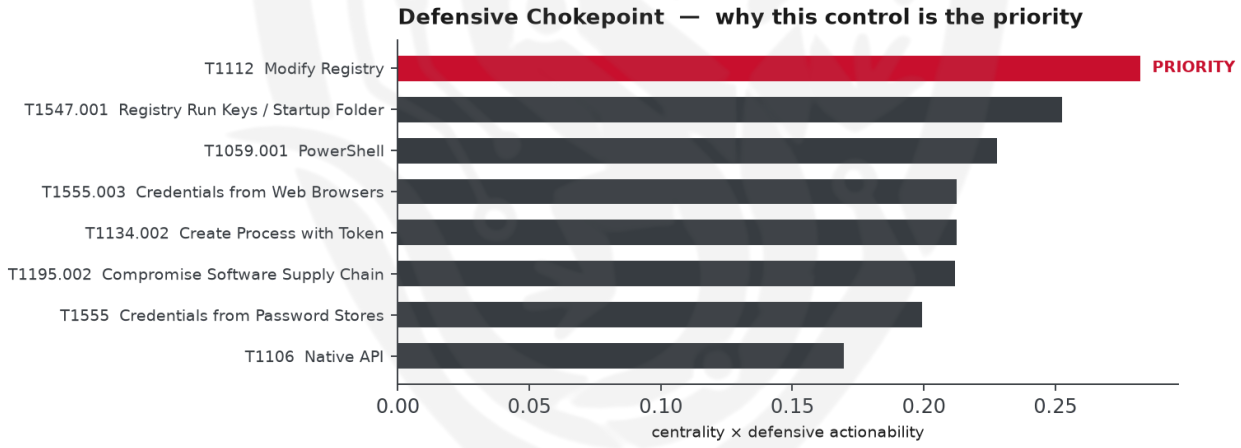
THREAT REPORT: UNKNOWN_ADVERSARY CAMPAIGN

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 identified as a potential threat to the technology sector, with a focus on exploiting various techniques to gain access to sensitive information. The threat actor's goals and motivations are unclear, but their methods involve a range of malicious activities, including file manipulation and system information discovery. Priority should be given to monitoring sensitive registry keys for modification to prevent potential data exfiltration. The lack of specific information on the threat actor and their targets makes it challenging to determine the full scope of the threat.

Threat Overview

The observed cluster of activity involves a range of techniques, including malicious file manipulation, symmetric cryptography, and system checks. The threat actor's use of these techniques suggests a focus

on gaining access to sensitive information and maintaining a presence on compromised systems. The victimology of this campaign is unclear, but it is known to target the technology sector.

Attack Chain and Priority Control

The observed techniques used by the threat actor can be described as a chain of events, starting with initial system checks and proceeding to malicious file manipulation and system information discovery. The priority technique in this chain is T1112 Modify Registry, which is a critical step in maintaining a presence on compromised systems. To mitigate this threat, 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 in this campaign, 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)

- T1204.002 Malicious File
- T1573.001 Symmetric Cryptography
- T1497.001 System Checks
- T1082 System Information Discovery
- T1106 Native API
- T1005 Data from Local System
- T1140 Deobfuscate/Decode Files or Information
- T1555 Credentials from Password Stores
- T1112 Modify Registry
- T1555.003 Credentials from Web Browsers
- T1134.002 Create Process with Token
- T1041 Exfiltration Over C2 Channel
- T1059.001 PowerShell
- T1547.001 Registry Run Keys / Startup Folder
- T1027 Obfuscated Files or Information
- T1195.002 Compromise Software Supply Chain
- T1027.002 Software Packing
- T1071.001 Web Protocols
- T1059.005 Visual Basic
- T1105 Ingress Tool Transfer

Analytical Scores

- Priority technique (graph chokepoint): T1112 Modify Registry (centrality 0.2973).
- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.5186; 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
Inception	0.5186
Stealth Falcon	0.4769
Molerats	0.4536
APT37	0.4482
Higaisa	0.4427

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	nvidiadriver[.]net
Domain	winpatch-xd7d[.]win
URL	hxxp://nvidiadriver[.]net/verv1432/winpatch-xd7d[.]win
Hash	208166120775a11cb6680139ea0f3372
Hash	4c1bdb2b045debf5b25e5be540ef99f0
Hash	c2875e2f45e5f1dfa04463de53b3fa5a

Type	Indicator
Hash	c5207f87b9103634b4db6f120eb6172a
Hash	f189c338a5f2bc3cce06cee37c0b7522
Hash	2890d90edfc08fb4cfafe0d5fa2a9fb6800dedf5
Hash	71c6cd37ddc0e5899174c72eefee8b224fd1f4bb
Hash	7b1919c35da92cf5fd2583783dc9364fd11b69d2
Hash	8e162d4fc8c5c74e16bfb4346f893cc7a71c2476
Hash	965e3d19c89f12ef730120b84d9ee38755841447
Hash	164e322d6fbc62e254d73583acd7f39444c884d3f5e6a5d27db143fc25bc88b3
Hash	17832aa629524ef6e8d8d6e9b6b902a8d324b559e3c36dbd0e221ab1690be871
Hash	282b9bc318ad1234cbd1b86424b784299b8be31545802a7c6b751166b814b990
Hash	50ffce607867d8fa8eaf6ef5cd25a3c0e7e4415e881b9e55c04a67bcddb74fdf
Hash	c8075bbff748096e1c6a1ea0aa67bb6762fdd7551427a12425b35b94c1f1ecf2
Hash	f6669bd504ce6b0e303be7ee47f2ebbc062989c88c41f0a3f436044a24869798

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 T1547.001 Registry Run Keys / Startup Folder here as an alternative persistence technique.
- **Projected pivot:** T1547.001 Registry Run Keys / Startup Folder (persistence)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

The actor could pivot to using T1547.001 Registry Run Keys / Startup Folder to maintain persistence, potentially by adding malicious entries to the Startup folder or Run/RunOnce registry keys, which may allow them to regain a foothold after the block on modifying the registry. This technique may be used to execute malicious code automatically when a user logs in, which would likely undermine the defender's previous control. To counter this, the mandated defensive 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.

Detection and hardening for the pivot (T1547.001 Boot or Logon Autostart Execution)

- **Telemetry:** Sysmon (registry + process); EDR autostart/ASEP inventory
- **Detect:**
  - Sysmon 13 (registry value set) on Run/RunOnce keys under HKLM & HKCU ...\CurrentVersion\Run*
  - Sysmon 11 for shortcuts/scripts created in Startup folders
  - Periodic ASEP (autostart extensibility point) diff against a known-good baseline
- **Harden:**
  - Restrict write access to autostart registry keys and Startup folders
  - Application control to block unsigned autostart binaries
- **MITRE:** M1047 Audit, M1038 Execution Prevention · DS0019 Service, DS0024 Windows Registry, DS0022 File