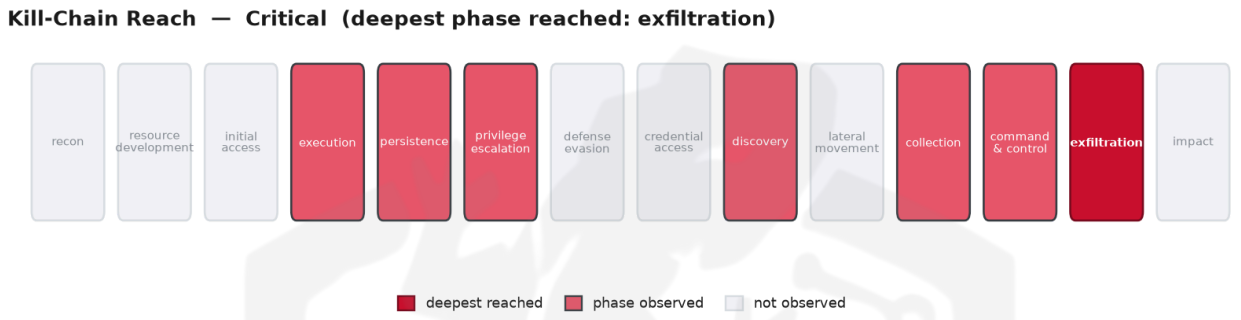
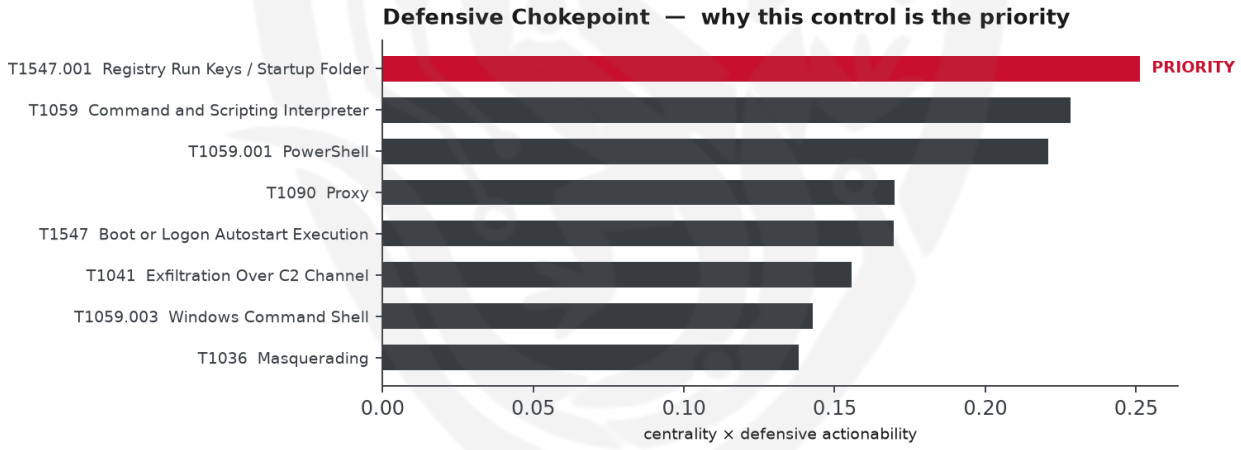
THREAT REPORT: UNKNOWN_ADVERSARY - LABUBARAT CAMPAIGN

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 is associated with the LabubaRAT malware family, which is masquerading as NVIDIA software. The threat actor is targeting unspecified countries and sectors, and the priority defensive action is to audit Windows Startup folders and Run/RunOnce registry keys for unauthorized entries. The actor's use of LabubaRAT allows for a range of malicious activities, including screen capture, system information discovery, and data exfiltration. Priority should be given to monitoring system startup processes and registry keys to prevent further malicious activity.

Threat Overview

The threat actor, referred to here as the observed cluster of activity, is utilizing the LabubaRAT malware family to carry out malicious activities. The malware is exploiting unspecified vulnerabilities, and the

victimology is currently unknown. The LabubaRAT malware family is a Rust-based remote access tool that is capable of a range of malicious activities, including screen capture, system information discovery, and data exfiltration.

Attack Chain and Priority Control

The observed techniques used by the threat actor form a complex attack chain, involving techniques such as screen capture, JavaScript execution, and DNS manipulation. The priority technique is T1547.001 Registry Run Keys / Startup Folder, which is a critical point 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

The malicious infrastructure associated with this campaign is hosted on Node Host Limited. There are no corroborated malware families from abuse.ch, and no indicators have been flagged with high confidence by AbuseIPDB, with the highest confidence seen being 0%. These findings are attributed to their respective sources, including Node Host Limited, abuse.ch, and AbuseIPDB.

Technical Appendix

Ground-truth telemetry from the source pulse; analytical scores are secondary and clearly labelled.

Observed Techniques (ATT&CK, expert-tagged by source)

- T1113 Screen Capture
- T1059.007 JavaScript
- T1071.004 DNS
- T1036.005 Match Legitimate Resource Name or Location
- T1547 Boot or Logon Autostart Execution
- T1082 System Information Discovery
- T1071 Application Layer Protocol
- T1005 Data from Local System
- T1140 Deobfuscate/Decode Files or Information
- T1036 Masquerading
- T1090 Proxy
- T1059 Command and Scripting Interpreter
- T1041 Exfiltration Over C2 Channel
- T1059.001 PowerShell
- T1547.001 Registry Run Keys / Startup Folder
- T1027 Obfuscated Files or Information
- T1573 Encrypted Channel
- T1518.001 Security Software Discovery
- T1059.003 Windows Command Shell

- T1071.001 Web Protocols
- T1518 Software Discovery
- T1105 Ingress Tool Transfer
- T1090.001 Internal Proxy

Analytical Scores

- Priority technique (graph chokepoint): T1547.001 Registry Run Keys / Startup Folder (centrality 0.2646).
- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4915; 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
APT18	0.4915
Higaisa	0.4885
Windshift	0.4682
Darkhotel	0.4649
Sidewinder	0.4504

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	Context
IP	168[.]222[.]254[.]204	AbuseIPDB 0% (DE) · AS198550 Node Host Limited
IP	191[.]44[.]109[.]130	AbuseIPDB 0% (DE) · AS198550 Node Host Limited

Type	Indicator	Context
IP	87[.]120[.]108[.]18	AbuseIPDB 0% (DE) · AS198550 Node Host Limited
Domain	pipicka[.]xyz	
URL	hxxps://pipicka[.]xyz	
Hash	d8bf355a198fb5db3ea65cfdfcdfbd19	
Hash	8c4e4804f21649e5ddc6a5670f3b3828a43bff304f02f184f9842c2569570f3d	
Hash	b7443b0ab48d2f5786d1b6f3a580f02621e9ae5a3877ee3a44e01df13d984328	

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 T1547 Boot or Logon Autostart Execution here as an alternative persistence technique.
- **Projected pivot:** T1547 Boot or Logon Autostart Execution (persistence)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

The threat actor could pivot to T1547 Boot or Logon Autostart Execution to maintain persistence and achieve their objective, potentially by exploiting other autostart locations that were not blocked by the initial control. This technique may allow the actor to execute malicious code automatically, which would likely undermine the defender's previous blocking effort. To counter this potential move, the mandated defensive control is to baseline and monitor autostart locations (Run keys, startup folders); alert on new persistence entries.

Detection and hardening for the pivot (T1547 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