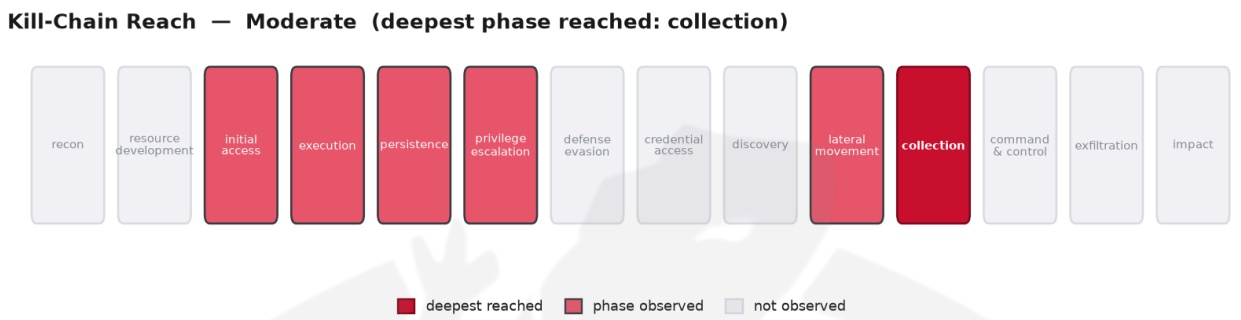
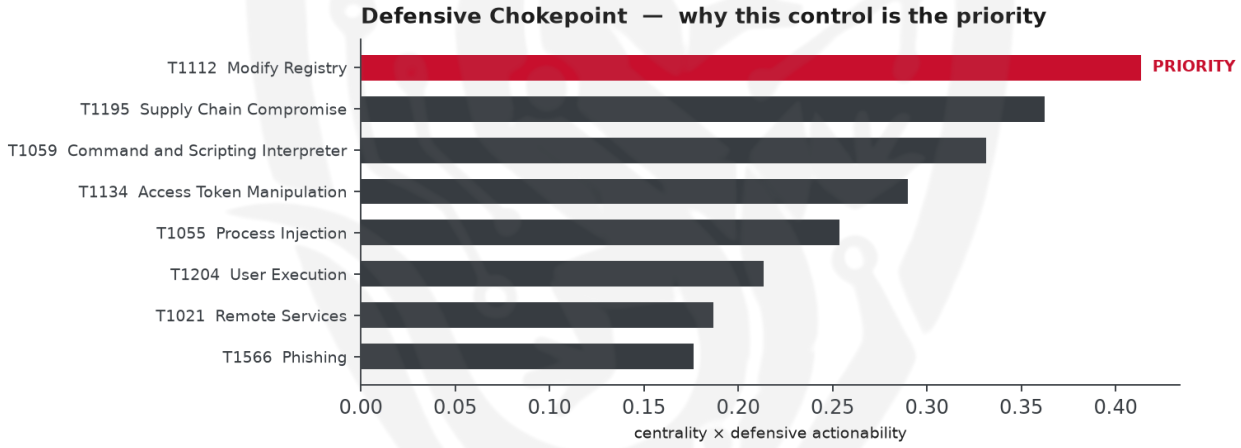
# THREAT REPORT: PHANTOM STEALER CAMPAIGN

## 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 involves the use of Phantom Stealer, Quasar RAT, and Lokibot malware families to target unspecified sectors and countries. The threat actor's identity and motivations are currently unknown. Priority should be given to monitoring sensitive registry keys for modification and restricting registry-edit tools for unprivileged users. The operational risk band for this threat is moderate, indicating a potential for collection of sensitive information.

## Threat Overview

The threat actor, whose identity is currently unknown, is utilizing the Phantom Stealer, Quasar RAT, and Lokibot malware families. The techniques inferred from the report include data extraction from local systems, remote services, process injection, and command and scripting interpreter manipulation, among others. The victimology and targeted sectors are not well-defined due to insufficient data.

## Attack Chain and Priority Control

The attack chain involves a series of techniques, including data extraction, process injection, and registry modification. The priority technique is T1112 Modify Registry, which serves as a chokepoint in the attack chain. 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

The Phantom Stealer malware family has been corroborated by abuse.ch, indicating a potential link to known malicious activity. However, there are no hosting providers or ASNs observed, and no indicators have been flagged with high confidence 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, machine-extracted from report text — reduced confidence)

*The source pulse carried no expert ATT&CK tags, so these techniques were inferred from its narrative by a self-consensus LLM extractor and validated against the ATT&CK catalogue. Treat this technique set, and the chokepoint, kill-chain and risk scores derived from it, as lower-confidence than an expert-tagged brief.* - T1005 Data from Local System - T1021 Remote Services - T1055 Process Injection - T1059 Command and Scripting Interpreter - T1112 Modify Registry - T1134 Access Token Manipulation - T1195 Supply Chain Compromise - T1204 User Execution - T1566 Phishing

### Analytical Scores

- Priority technique (graph chokepoint): T1112 Modify Registry (centrality 0.4352).
- Operational risk: Moderate (score 0.541, reaches collection).

### Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.3536; 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 |
|---|---|
| TA459 | 0.3536 |

| Historical Profile | Behavioural Overlap |
|---|---|
| Gorgon Group | 0.3475 |
| APT30 | 0.3333 |
| FIN8 | 0.3118 |
| Malteiro | 0.3059 |

## Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.
- Malware families corroborated by abuse.ch: PhantomStealer.
- 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 |
|---|---|---|
| Hash | 031ae066a8188e5fea8d3d7981a2166c | PhantomStealer |
| Hash | 9d79790ceacab47146df25e3704abe580441b2ab | PhantomStealer |
| Hash | 2d5003d9318ae85eb22de99d19705a3cd7bf8e5c3349df979dfb3bdfa080908e | PhantomStealer |
| Hash | b588caa5365451a6c60fd73fec5b73f13ac41bcc2a3a3bed7244df5917a62f32 | PhantomStealer |
| Hash | be119a21bedc3a79bf4dea8bcf5adf18304997a01ea23e276b9c31be37b789ab | PhantomStealer |
| Hash | 382233c398cbc35dcee845ee17046815f37588a382a8106bfb9b0252ea803961 | PhantomStealer |
| Hash | 790945e17a51691483455a11af2efcbe15f2b473b65b151f50287623d1468516 | PhantomStealer |
| Hash | 528a46842744366b57edfc6fe2810ca7df43900db75126cd1c78f32957143364 | PhantomStealer |
| Hash | 01f1e5369aa0332abb681df7c37818e197ec0a5b5d7b81836b3369a2b1780950 | PhantomStealer |
| Hash | 10cfcad907275497dab92af0d687674cec3a0333f80dd16d8d22254794bb2d60 | PhantomStealer |
| Hash | f82a4d30132b5a57cbfd81c7ab0a53d0cf0dda402c2731732a0097aceb4b0b76 | PhantomStealer |
| Hash | e3ceeb24bdca8842d426e87fa61cf185d68fd7783e1a2b97d4106832ca266724 | PhantomStealer |
| Hash | 390325e2d23bce8d8f63b047f64c3cd5 | PhantomStealer |
| Hash | b6ab80e1262197ebc4be80641aa03afa | PhantomStealer |

| Type | Indicator | Context |
|---|---|---|
| Hash | c4fda5f3a27a961149eeeb8bb3666c93 | PhantomStealer |
| Hash | c8821ed5d6b2cb2469abfc3cf83210ba | PhantomStealer |
| Hash | d18e6f0dd8a71742fd07125ae6fafcf2 | PhantomStealer |
| Hash | e1faeb1fac915fb6c11273d220e7b11f | PhantomStealer |
| Hash | ee4e04111fbe39c13a084ffbece4d284 | PhantomStealer |
| Hash | faa9be79966054ec706de4ed983d9644 | PhantomStealer |
| Hash | 362a370f117bc54e40a69c1808cfd020ac2fb00d | PhantomStealer |
| Hash | 3fe37d385eae5054cd919c570ebda8086d54686a | PhantomStealer |
| Hash | 5843beb38fe07ba4caee971961dc761218244757 | PhantomStealer |
| Hash | 59a5b8188a289d80d29e4943ef471ab19185aa82 | PhantomStealer |
| Hash | 5ad3f0d0d8e0276dad0b1cc64aee36774db5543f | PhantomStealer |
| Hash | 64c4707c9df2585ae93425b343df3df60ed585c2 | PhantomStealer |
| Hash | 752d07cadfe3f9f13a89f0be50d6bb18a0e16c61 | PhantomStealer |
| Hash | cb6d9d1c6aba200d0a2a45be3d474604b2b11861 | PhantomStealer |

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:** T1112 Modify Registry (persistence)
- **Observed here:** T1112 Modify Registry was the only persistence technique observed in this campaign, so the pivot is projected from cross-actor behaviour.
- **Projected pivot:** T1543 Create or Modify System Process (persistence)
- **Basis:** of the 14+ groups that use Modify Registry, this pairing runs 2.8x above base rate, a disproportionately-coupled move rather than the obvious one.

With T1112 Modify Registry blocked, the threat actor could preserve the same objective by pivoting to T1543 Create or Modify System Process, a technique disproportionately paired with it across tracked groups. Defensive countermeasure: Restrict service/daemon creation to admins; monitor service and driver installs.

**Also plausible (same tactic):** T1053 Scheduled Task/Job (n=19, lift 1.9), T1547 Boot or Logon Autostart Execution (n=17, lift 1.7)

**Detection and hardening for the pivot (T1543 Create or Modify System Process)**

- **Telemetry:** Windows Security / System log; Sysmon
- **Detect:**
  - System 7045 (new service installed); Security 4697 (service installed)
  - Sysmon 1 for sc.exe / services created; unusual ImagePath or user-context services
  - Registry writes under HKLM\SYSTEM\CurrentControlSet\Services
- **Harden:**
  - Restrict service creation to admins; application control on service binaries
  - Baseline installed services and alert on new/anomalous ones
- **MITRE:** M1047 Audit, M1028 Operating System Configuration, M1026 Privileged Account Management · DS0019 Service, DS0024 Windows Registry, DS0009 Process