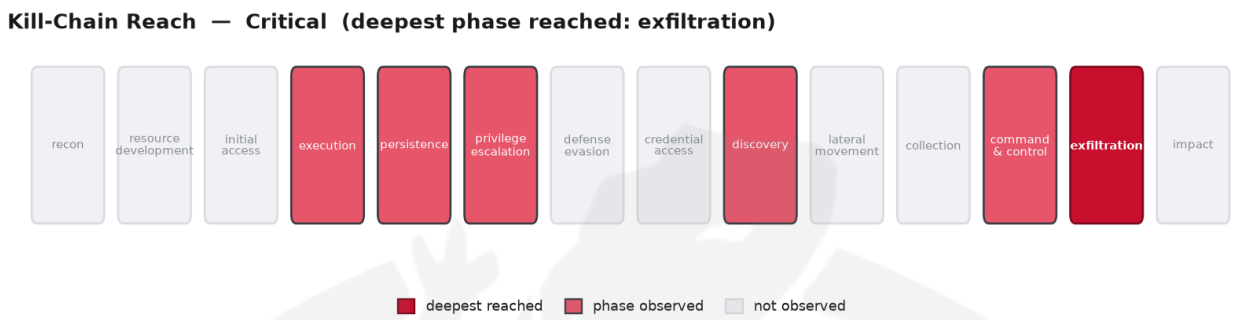
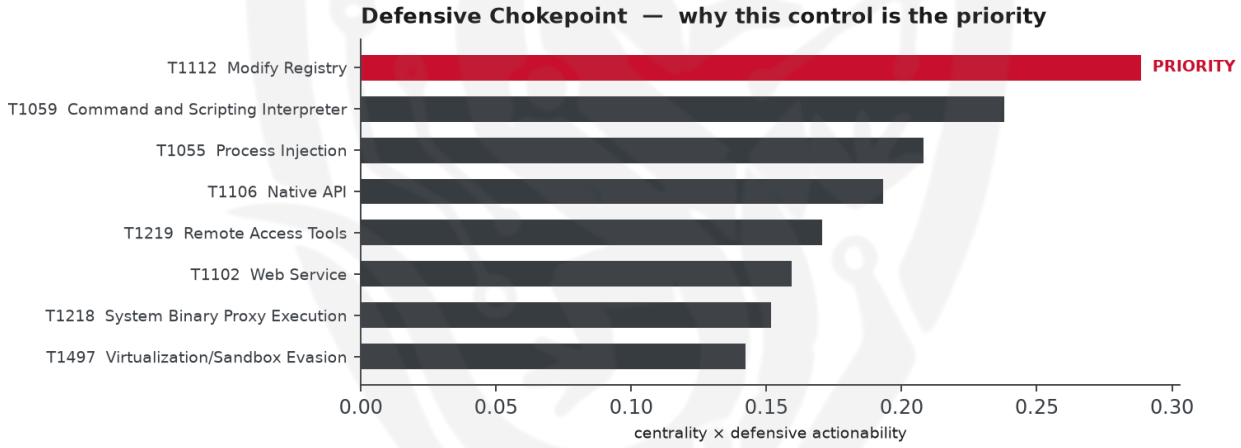
# THREAT REPORT: CHAOS

## 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 source attributes this activity to Chaos, a threat actor utilizing the msaRAT malware family to target unspecified countries and sectors. The threat actor is exploiting various techniques to build a covert command and control channel, with a priority defensive action being to monitor sensitive registry keys for modification. Priority should be given to restricting registry-edit tools for unprivileged users to mitigate the threat. The operational risk band is considered Critical due to the potential for exfiltration.

## Threat Overview

The threat actor, Chaos, is using the msaRAT malware family to carry out their operations. Although the central CVE is insufficient, the malware family is leveraging various techniques, including JavaScript, symmetric cryptography, and system information discovery, to achieve its goals. The victimology of this threat is currently unspecified, but the techniques used suggest a sophisticated attack chain.

## Attack Chain and Priority Control

The observed techniques used by the threat actor form a complex attack chain, involving techniques such as command and scripting interpreter, process injection, and web service exploitation. The priority technique, T1112 Modify Registry, is the graph chokepoint, indicating that the threat actor relies heavily on modifying registry keys to maintain their presence. The concrete control to mitigate this threat is to "Monitor sensitive registry keys for modification; restrict registry-edit tools for unprivileged users."

## Infrastructure and Corroboration

There is no observed hosting provider or ASN associated with this threat, and no malware families have been corroborated by abuse.ch. Additionally, no indicators have been flagged with an AbuseIPDB confidence 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)

- T1059.007 JavaScript
- T1036.005 Match Legitimate Resource Name or Location
- T1573.001 Symmetric Cryptography
- T1082 System Information Discovery
- T1218.007 Msiexec
- T1106 Native API
- T1140 Deobfuscate/Decode Files or Information
- T1219 Remote Access Tools
- T1055 Process Injection
- T1218 System Binary Proxy Execution
- T1112 Modify Registry
- T1059 Command and Scripting Interpreter
- T1497 Virtualization/Sandbox Evasion
- T1102 Web Service
- T1041 Exfiltration Over C2 Channel
- T1027 Obfuscated Files or Information
- T1012 Query Registry
- T1071.001 Web Protocols
- T1105 Ingress Tool Transfer
- T1090.001 Internal Proxy

### Analytical Scores

- Priority technique (graph chokepoint): T1112 Modify Registry (centrality 0.3037).

- Operational risk: Critical (score 0.968, reaches exfiltration).

### Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4463; 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 |
|---|---|
| Higaisa | 0.4463 |
| ZIRCONIUM | 0.441 |
| Gamaredon Group | 0.3852 |
| WIRTE | 0.378 |
| Stealth Falcon | 0.3746 |

### 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 | is-01-ast[.]ols-img-12[.]workers[.]dev |
| URL | hxxp://172[.]86[.]126[.]18:443/update_ms[.]msi |

---

## 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:** T1053 Scheduled Task/Job (persistence)
- **Basis:** 19 of 170 documented groups that use Modify Registry also use Scheduled Task/Job (conditional 0.66, lift 1.9, i.e. ~1.9x base rate). Strongest same-tactic neighbour.

The Chaos actor could pivot to utilizing T1053 Scheduled Task/Job to maintain persistence and execute malicious tasks at scheduled intervals, potentially evading detection by blending in with legitimate system activity. This technique may allow them to regain a foothold in the system, as scheduled tasks can be used to execute malicious code or scripts at specific times or intervals. To counter this potential move, the defensive control would involve alerting on new scheduled tasks (Event ID 4698); restricting schtasks/at to admins; and baselining legitimate task creators.

**Also plausible (same tactic):** T1078 Valid Accounts (n=18, lift 1.6), T1547 Boot or Logon Autostart Execution (n=17, lift 1.7)

**Detection and hardening for the pivot (T1053 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