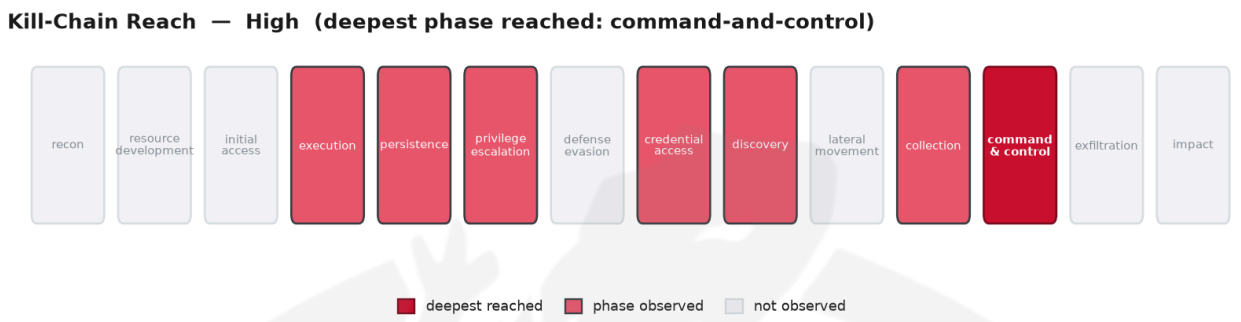
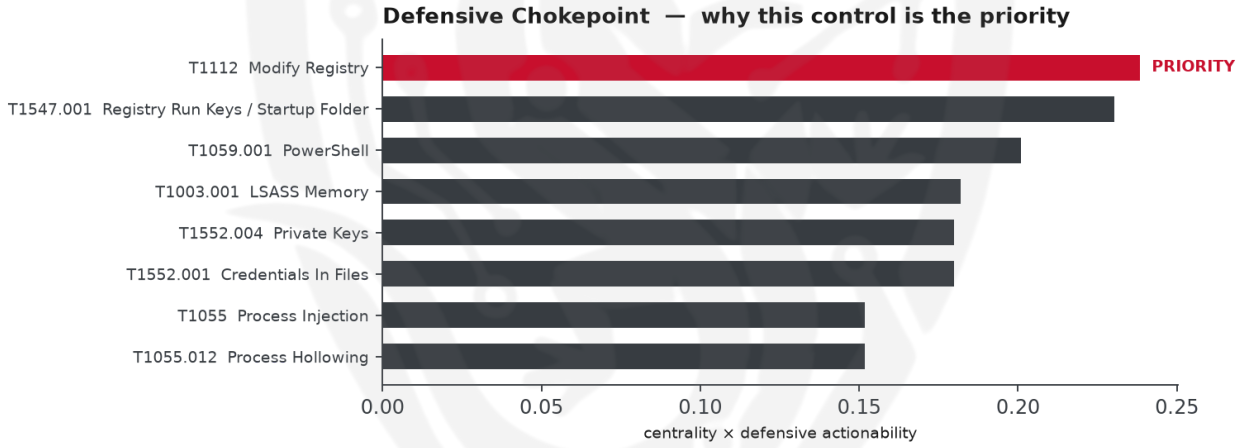
# THREAT REPORT: OPERATION STANDOFF

## 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, referred to as Operation STANDOFF, has been identified as utilizing various malware families, including Raccoon Stealer, RedLine, and Amadey, to target unspecified sectors and countries. The threat actor's campaign involves hiding command and control (C2) communications behind GitHub redirects. Priority should be given to monitoring sensitive registry keys for modification and restricting registry-edit tools for unprivileged users. The operational risk band of this campaign is considered high, reaching the level of command and control.

## Threat Overview

The threat actor, Operation STANDOFF, employs a range of malware families, including Raccoon Stealer, RedLine, Amadey, SmokeLoader, Socelars, Glupteba, and XMRig. The central vulnerability exploited is currently insufficiently documented. The victimology and targeted countries are also not specified due to insufficient data.

## Attack Chain and Priority Control

The attack chain involves multiple techniques, including scheduled tasks, matching legitimate resource names, and system checks, ultimately leading to the modification of registry keys. The priority technique identified is T1112 Modify Registry, which serves as a critical chokepoint in the attack chain. To mitigate this, the priority control is to "Monitor sensitive registry keys for modification; restrict registry-edit tools for unprivileged users."

## Infrastructure and Corroboration

The malicious infrastructure associated with Operation STANDOFF is hosted by various providers, including JSC Timeweb, 1337Team Limited, Reliable Communications s.r.o., and MivoCloud SRL, as observed in third-party enrichment data. Additionally, abuse.ch has corroborated the presence of Amadey and RedLine Stealer malware families. However, according to AbuseIPDB, there are no indicators with a confidence level 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)

- T1053.005 Scheduled Task
- T1036.005 Match Legitimate Resource Name or Location
- T1543.003 Windows Service
- T1497.001 System Checks
- T1082 System Information Discovery
- T1005 Data from Local System
- T1140 Deobfuscate/Decode Files or Information
- T1558 Steal or Forge Kerberos Tickets
- T1055 Process Injection
- T1497.003 Time Based Checks
- T1562.004 Impair Defenses: Disable or Modify System Firewall
- T1112 Modify Registry
- T1552.004 Private Keys
- T1003.001 LSASS Memory
- T1083 File and Directory Discovery
- T1552.001 Credentials In Files
- T1059.001 PowerShell
- T1547.001 Registry Run Keys / Startup Folder
- T1562.001 Impair Defenses: Disable or Modify Tools
- T1055.012 Process Hollowing
- T1027 Obfuscated Files or Information
- T1573 Encrypted Channel

- T1012 Query Registry
- T1518.001 Security Software Discovery
- T1059.003 Windows Command Shell
- T1027.002 Software Packing
- T1071.001 Web Protocols
- T1105 Ingress Tool Transfer

## Analytical Scores

- Priority technique (graph chokepoint): T1112 Modify Registry (centrality 0.251).
- 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 0.4638; 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 |
|---|---|
| Darkhotel | 0.4638 |
| BlackByte | 0.4577 |
| Rocke | 0.4542 |
| BRONZE BUTLER | 0.4439 |
| TA2541 | 0.4434 |

## Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.
- Malware families corroborated by abuse.ch: Amadey, RedLine Stealer.
- 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 |
|---|---|---|
| IP | 188[.]225[.]72[.]157 | AbuseIPDB 0% (RU) · AS9123 JSC Timeweb |

| Type | Indicator | Context |
|---|---|---|
| IP | 185[.]215[.]113[.]35 | AbuseIPDB 0% (SC) · AS51381 1337Team Limited |
| IP | 212[.]192[.]241[.]62 | AbuseIPDB 0% (AT) · AS2118 Reliable Communications s.r.o. |
| IP | 212[.]193[.]30[.]29 | AbuseIPDB 0% (RU) · AS9123 JSC Timeweb |
| IP | 185[.]225[.]19[.]18 | AbuseIPDB 0% (RO) · AS39798 MivoCloud SRL |
| IP | 185[.]215[.]113[.]44 | AbuseIPDB 0% (SC) · RedLine Stealer · AS51381 1337Team Limited |
| IP | 212[.]193[.]30[.]45 | AbuseIPDB 0% (RU) · AS9123 JSC Timeweb |
| IP | 147[.]45[.]183[.]198 | AbuseIPDB 0% (RU) · AS9123 JSC Timeweb |
| IP | 147[.]45[.]237[.]23 | AbuseIPDB 0% (RU) · AS9123 JSC Timeweb |
| IP | 185[.]247[.]185[.]85 | AbuseIPDB 0% (RU) · AS9123 JSC Timeweb |
| IP | 188[.]225[.]39[.]252 | AbuseIPDB 0% (RU) · AS9123 JSC Timeweb |
| IP | 188[.]225[.]82[.]125 | AbuseIPDB 0% (RU) · AS9123 JSC Timeweb |
| IP | 194[.]87[.]131[.]30 | AbuseIPDB 0% (RU) · AS9123 JSC Timeweb |
| IP | 194[.]87[.]56[.]156 | AbuseIPDB 0% (RU) · AS9123 JSC Timeweb |
| IP | 195[.]133[.]73[.]225 | AbuseIPDB 0% (RU) · AS9123 JSC Timeweb |
| IP | 212[.]60[.]21[.]249 | AbuseIPDB 0% (RU) · AS9123 JSC Timeweb |
| IP | 217[.]198[.]13[.]211 | AbuseIPDB 0% (RU) · AS9123 JSC Timeweb |
| IP | 37[.]252[.]21[.]227 | AbuseIPDB 0% (RU) · AS9123 JSC Timeweb |
| IP | 45[.]139[.]78[.]67 | AbuseIPDB 0% (RU) · AS9123 JSC Timeweb |
| IP | 46[.]149[.]70[.]18 | |
| IP | 5[.]129[.]196[.]85 | |
| IP | 89[.]223[.]71[.]207 | |
| IP | 90[.]156[.]224[.]57 | |
| IP | 92[.]51[.]22[.]34 | |
| IP | 93[.]183[.]80[.]126 | |
| Domain | listincode[.]com | |

| Type | Indicator | Context |
|---|---|---|
| Domain | www[.]listincode[.]com | |
| Domain | wfsdragon[.]ru | |
| Domain | topniemannpickshop[.]cc | |
| Domain | all-mobile-pa1ments[.]com[.]mx | |
| Domain | buy-fantasy-gxmes[.]com[.]sg | |
| Domain | buy-fantasy-football[.]com[.]sg | |
| Domain | new-androidapps[.]me | |
| Domain | rcacademy[.]at | |
| Domain | cloudjah[.]com | malware_download |
| Domain | www[.]wgqpw[.]com | |
| Domain | server5[.]trumops[.]com | |
| Domain | bull-drops[.]online | |
| Domain | bull-drops[.]ru | |
| Domain | bulldrops[.]online | |

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:** Operation STANDOFF 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 Operation STANDOFF actors could pivot to utilizing Scheduled Task (T1053.005) to maintain persistence and execute malicious actions, potentially leveraging this technique to bypass the blocked registry modification control. They may attempt to create new scheduled tasks to achieve their objectives, which would likely involve creating or modifying task schedules to run malicious code. The defensive

control to counter this potential move 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