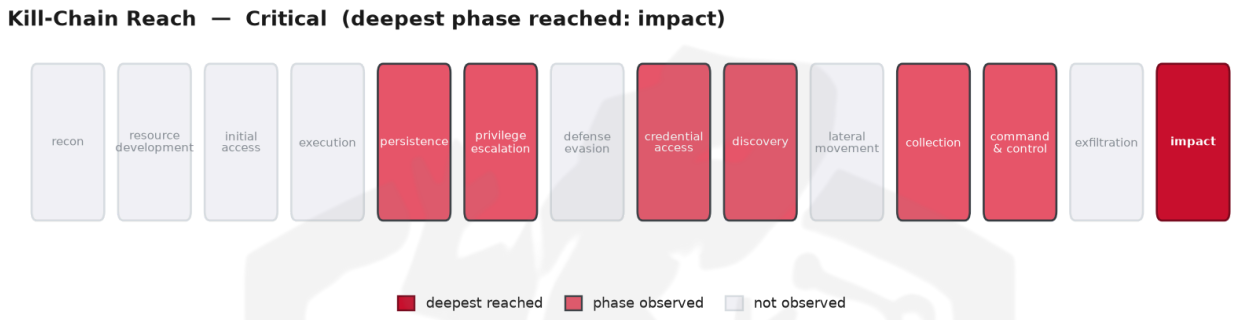
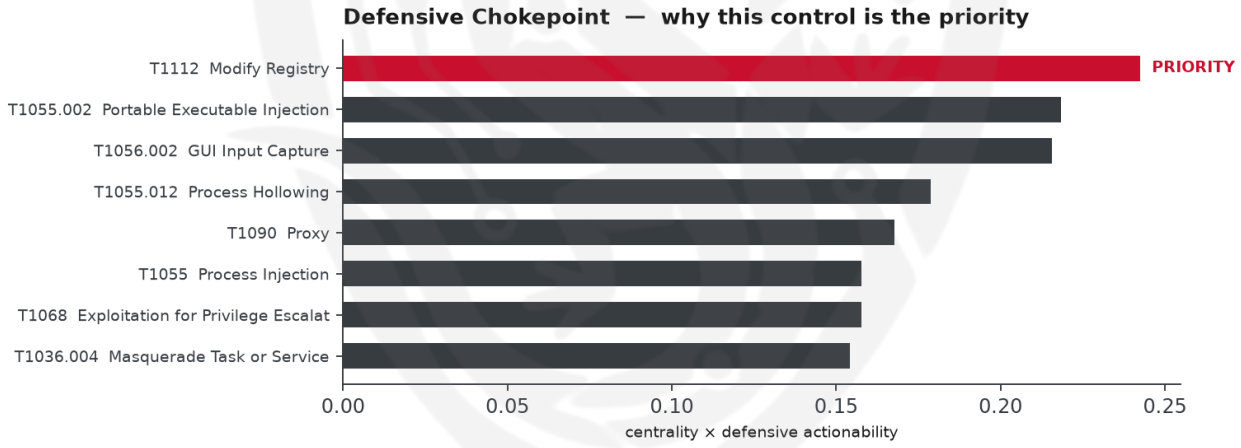
# THREAT REPORT: SAKDRIVER AND CRACKERDRV MALWARE CAMPAIGN

## 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 SakDriver and CrackerDrv malware families, targeting Windows kernel drivers. The priority defensive action should be to monitor sensitive registry keys for modification and restrict registry-edit tools for unprivileged users. The threat actor's identity and targeted country remain unknown. Priority should be given to defending against these malware families due to their potential impact.

## Threat Overview

The threat actor, whose identity is unknown, utilizes the SakDriver and CrackerDrv malware families. Although a central CVE is not identified, the malware exploits various techniques to compromise systems.

The victimology of this campaign is also unclear, but the use of these malware families poses a significant threat.

## Attack Chain and Priority Control

The attack chain involves a series of techniques, including rootkit and bootkit installation, service stop, system checks, process injection, and registry modification. The priority technique is T1112 Modify Registry, which is the graph chokepoint. 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 malicious infrastructure is hosted on providers such as Tencent and Hetzner Online GmbH. Additionally, abuse.ch has corroborated the presence of CobaltStrike malware families in relation to this campaign. However, AbuseIPDB has not flagged any 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)

- T1014 Rootkit
- T1542.003 Bootkit
- T1489 Service Stop
- T1497.001 System Checks
- T1055 Process Injection
- T1112 Modify Registry
- T1090 Proxy
- T1562.006 Impair Defenses: Indicator Blocking
- T1036.004 Masquerade Task or Service
- T1055.002 Portable Executable Injection
- T1056.002 GUI Input Capture
- T1070.005 Network Share Connection Removal
- T1562.001 Impair Defenses: Disable or Modify Tools
- T1055.012 Process Hollowing
- T1068 Exploitation for Privilege Escalation
- T1573 Encrypted Channel
- T1027.002 Software Packing
- T1071.001 Web Protocols
- T1055.001 Dynamic-link Library Injection

### Analytical Scores

- Priority technique (graph chokepoint): T1112 Modify Registry (centrality 0.2553).
- Operational risk: Critical (score 1.0, reaches impact).

## Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.2802; 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 |
|---|---|
| BITTER | 0.2802 |
| APT41 | 0.2665 |
| Rocke | 0.2598 |
| Lazarus Group | 0.2526 |
| Threat Group-3390 | 0.2465 |

## Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.
- Malware families corroborated by abuse.ch: CobaltStrike.
- 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 | 43[.]160[.]247[.]24 | AbuseIPDB 0% (SG) · AS132203 Tencent Building Kejizhongyi Avenue |
| IP | 91[.]99[.]165[.]207 | AbuseIPDB 0% (DE) · AS24940 Hetzner Online GmbH |
| Hash | 4e95aba17c1a423cda5cc9f9f04f7cf8db17e294eb31ed1aa85063601b82fe8d | CobaltStrike |
| Hash | b5f122f3f07f618c0a7678fa40801faa | CobaltStrike |

| Type | Indicator | Context |
|---|---|---|
| Hash | 7440358c5041eba34e8673100989df756a6426da | CobaltStrike |

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