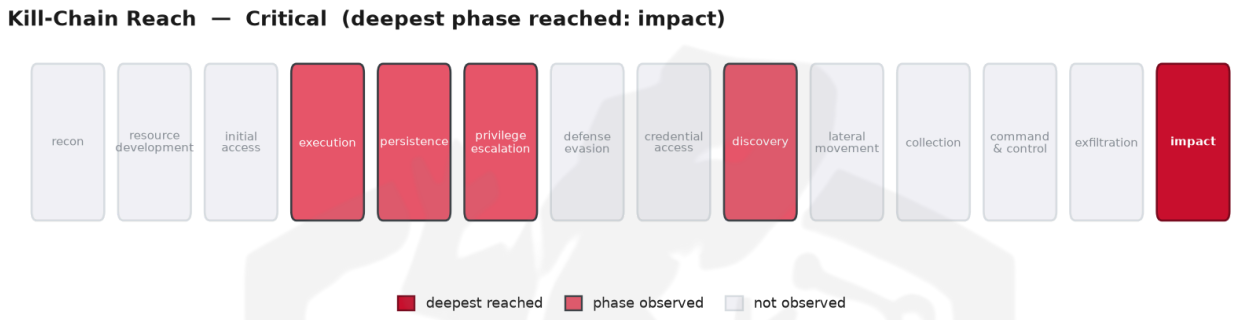
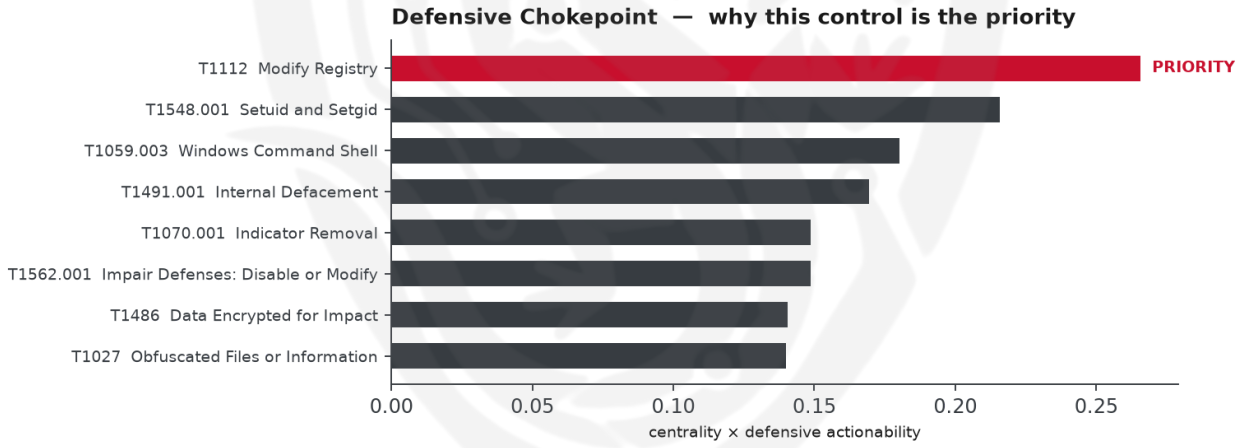
THREAT REPORT: DEADLOCK RANSOMWARE CAMPAIGN

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 DeadLock threat actor is attributed to a ransomware campaign that has targeted various sectors, including Technology, Mining, Transportation, Manufacturing, Hospitality, and Retail. The campaign involves the use of DeadLock, Lynx, and Brave Prince malware families. 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 campaign is Critical, indicating a high level of potential impact.

Threat Overview

The DeadLock threat actor is associated with the DeadLock, Lynx, and Brave Prince malware families. The campaign exploits various techniques, including bypassing user account control, stopping services,

and encrypting data for impact. The targeted sectors include multiple industries, but the specific country targeted is not available.

Attack Chain and Priority Control

The attack chain involves a series of techniques, including bypassing user account control, stopping services, and encrypting data. The priority technique is T1112 Modify Registry, which is a critical 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

There is no available information on the hosting providers or ASNs observed, and no malware families have been corroborated by abuse.ch. Additionally, no indicators have been flagged with a confidence level of 80% or higher 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, expert-tagged by source)

- T1548.002 Bypass User Account Control
- T1036.005 Match Legitimate Resource Name or Location
- T1489 Service Stop
- T1497.001 System Checks
- T1082 System Information Discovery
- T1140 Deobfuscate/Decode Files or Information
- T1112 Modify Registry
- T1070.001 Indicator Removal
- T1548.001 Setuid and Setgid
- T1083 File and Directory Discovery
- T1491.001 Internal Defacement
- T1562.001 Impair Defenses: Disable or Modify Tools
- T1027 Obfuscated Files or Information
- T1486 Data Encrypted for Impact
- T1059.003 Windows Command Shell
- T1485 Data Destruction
- T1134 Access Token Manipulation
- T1490 Inhibit System Recovery
- T1529 System Shutdown/Reboot

Analytical Scores

- Priority technique (graph chokepoint): T1112 Modify Registry (centrality 0.2797).
- Operational risk: Critical (score 1.0, reaches impact).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.3656; 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	0.3656
Sowbug	0.3548
APT38	0.3402
BlackByte	0.3149
Gamaredon Group	0.3129

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	deadlock[.]liveblog365[.]com
Domain	polygon[.]meowrpc[.]com
Domain	deadblogdbdu5wprek7wa2o4ce7rnt6u6ntqeud3hzjjcveosgpsqqqd[.]onion
Domain	deadlockblog[.]medianewsonline[.]com
Domain	deadlockblog[.]great-site[.]net
Domain	dlock[.]liveblog365[.]com
URL	hxxp://1rpc[.]io/matic

Type	Indicator
Hash	a1fdf65020ce4a0f0940c793c6425baf8a0b994ec48b9baaf72788661a9d29f4

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, DeadLock 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