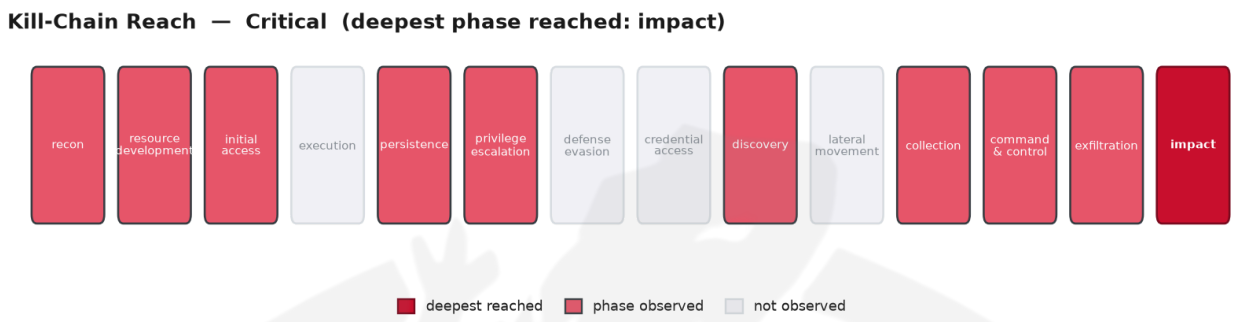
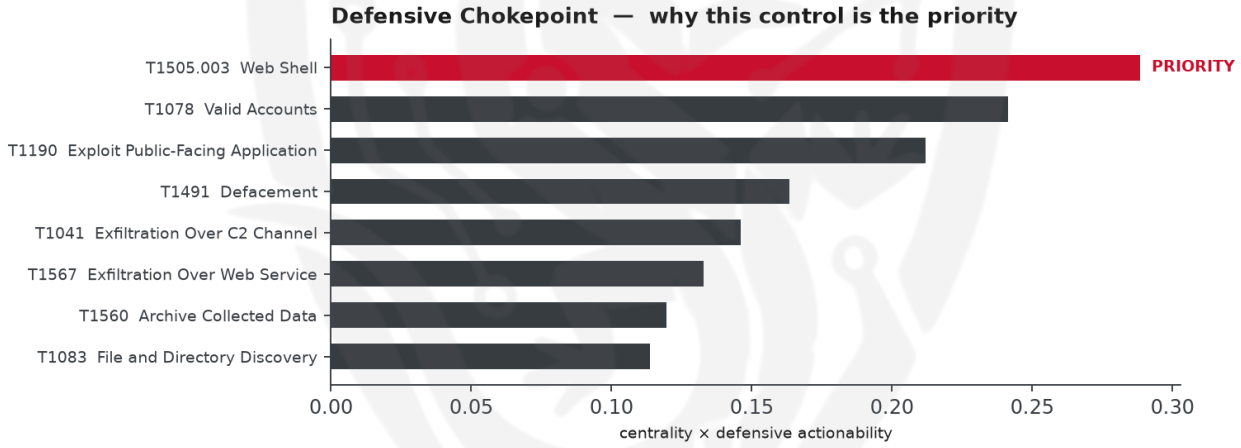
THREAT REPORT: CL0P RANSOMWARE CAMPAIGN

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 source attributes this activity to Cl0p, a threat actor utilizing the LEMURLOOT malware family to exploit the CVE-2023-34362 vulnerability. The targeted country and sectors are not specified due to insufficient data. Priority should be given to defending against this threat, particularly focusing on web-server security and patching the exploited vulnerability. The campaign's impact is considered critical, reaching the level of significant system and data compromise.

Threat Overview

Cl0p, the attributed threat actor, is using the LEMURLOOT malware family to exploit the CVE-2023-34362 vulnerability. The victimology of this campaign is not fully detailed due to insufficient data on targeted countries and sectors. However, the techniques employed by Cl0p include a range of actions from acquiring infrastructure to encrypting data for impact, indicating a sophisticated and potentially damaging attack chain.

Attack Chain and Priority Control

The observed techniques form a complex attack chain that includes acquiring infrastructure, stopping services, exploiting public-facing applications, and exfiltrating data over various channels. The priority technique identified is T1505.003 Web Shell, which serves as a critical chokepoint in the attack chain. To counter this, the recommended priority control is to "Integrity-monitor web-server directories for web shells; restrict server module/plugin installation. In parallel, patch CVE-2023-34362 on all affected systems."

Infrastructure and Corroboration

The malicious infrastructure associated with this campaign is hosted by providers including Sonic Inc Sal, Data Campus Limited, and Datahome S.A. According to AbuseIPDB, there are no indicators with a confidence level of 80% or higher, and the highest confidence seen is 0%. Abuse.ch does not corroborate any additional malware families beyond what is already identified in the campaign. These corroboration points provide additional context to the campaign's infrastructure without altering the primary threat assessment.

Technical Appendix

Ground-truth telemetry from the source pulse; analytical scores are secondary and clearly labelled.

Observed Techniques (ATT&CK, expert-tagged by source)

- T1583 Acquire Infrastructure
- T1489 Service Stop
- T1071 Application Layer Protocol
- T1005 Data from Local System
- T1190 Exploit Public-Facing Application
- T1567 Exfiltration Over Web Service
- T1560 Archive Collected Data
- T1595.002 Vulnerability Scanning
- T1491 Defacement
- T1505.003 Web Shell
- T1595 Active Scanning
- T1583.003 Virtual Private Server
- T1083 File and Directory Discovery
- T1041 Exfiltration Over C2 Channel
- T1078 Valid Accounts
- T1027 Obfuscated Files or Information
- T1486 Data Encrypted for Impact
- T1573 Encrypted Channel
- T1505 Server Software Component
- T1490 Inhibit System Recovery

Analytical Scores

- Priority technique (graph chokepoint): T1505.003 Web Shell (centrality 0.3361).
- Operational risk: Critical (score 1.0, reaches impact).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4226; 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
Volatile Cedar	0.4226
Ember Bear	0.3722
BlackByte	0.3578
Sandworm Team	0.3427
Agrius	0.3266

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	Context
IP	45[.]129[.]137[.]232	AbuseIPDB 0% (LB) · AS206485 Sonic Inc Sal
IP	92[.]118[.]36[.]233	AbuseIPDB 0% (SE) · AS215929 Data Campus Limited
IP	200[.]107[.]207[.]26	AbuseIPDB 0% (RU) · AS273045 Datahome S.A.
Domain	pubstorm[.]com	
Domain	pubstorm[.]net	

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:** T1505.003 Web Shell (persistence)
- **Observed here:** T1505.003 Web Shell was the only persistence technique observed in this campaign, so the pivot is projected from cross-actor behaviour.
- **Projected pivot:** T1136 Create Account (persistence)
- **Basis:** of the 12+ groups that use Web Shell, this pairing runs 2.9x above base rate, a disproportionately-coupled move rather than the obvious one.

Cl0p could pivot to creating a new local account using T1136 Create Account, as this technique would allow them to maintain access and escalate privileges, potentially bypassing the web shell block by leveraging a legitimate account for further malicious activities. This technique may be particularly appealing to Cl0p as it enables them to blend in with normal administrative tasks, making it harder to detect. To counter this potential move, the defensive control of alerting on new local/domain account creation (Event ID 4720/4728) and enforcing an approval workflow for account provisioning should be implemented.

Also plausible (same tactic): T1133 External Remote Services (n=13, lift 2.5), T1098 Account Manipulation (n=8, lift 2.4)

Detection and hardening for the pivot (T1136 Create Account)

- **Telemetry:** Windows Security (account management); IdP audit logs
- **Detect:**
  - Security 4720 (local user created), 4741 (computer account), 4728 (added to group)
  - New cloud/IdP accounts created outside HR/provisioning workflow
- **Harden:**
  - Restrict account creation to provisioning systems; alert on manual creation
  - Periodic review of recently created accounts
- **MITRE:** M1026 Privileged Account Management, M1032 Multi-factor Authentication · DS0002 User Account