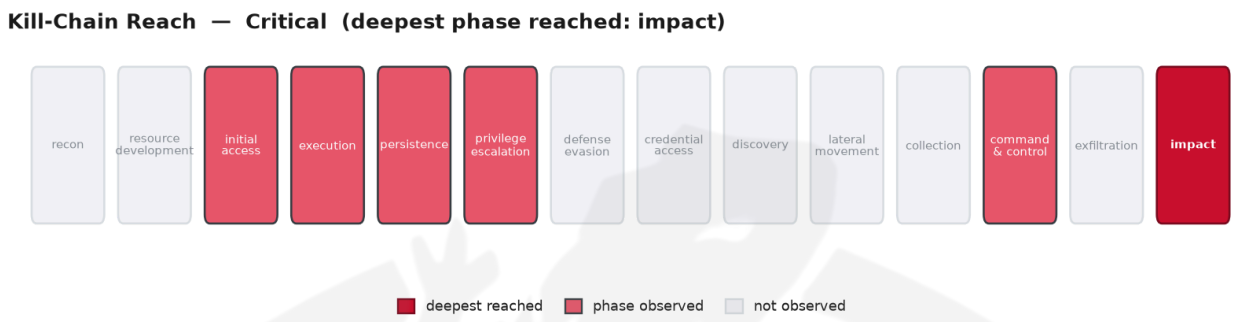
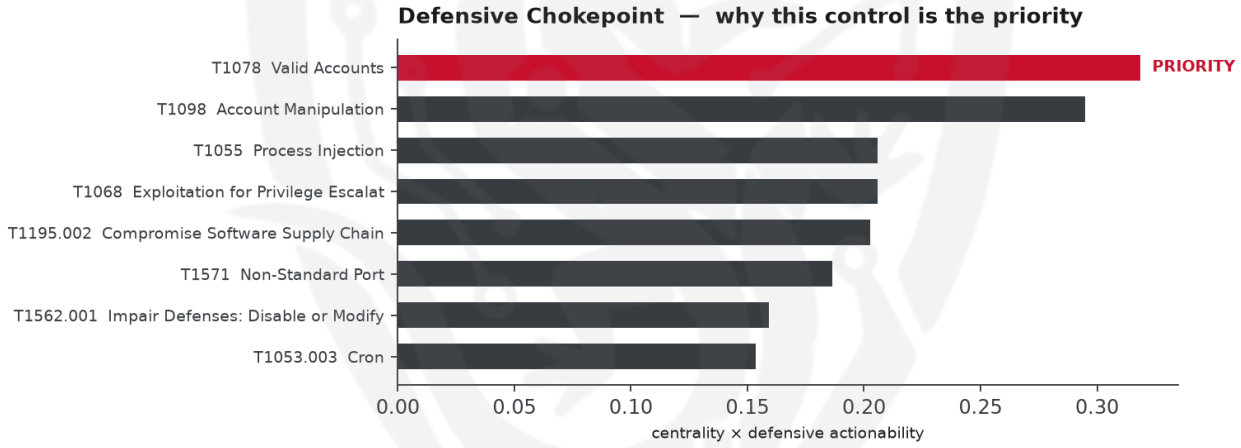
THREAT REPORT: XMRIG CRYPTOMINING CAMPAIGN

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 has been linked to the deployment of XMRig malware, targeting unspecified sectors and countries. The threat actor's identity remains unknown. Priority should be given to enforcing multi-factor authentication and disabling dormant accounts to mitigate the campaign's impact. The lack of specific attribution and targeted information underscores the need for proactive defensive measures.

Threat Overview

The threat actor, whose identity is not specified, is utilizing the XMRig malware family to conduct their operations. Although the central CVE exploited in this campaign is not identified, the actor employs various techniques to achieve their objectives, including masquerading, process injection, and account manipulation. The victimology of this campaign remains unclear due to insufficient data.

Attack Chain and Priority Control

The attack chain involves a series of techniques, including sudo and sudo caching, masquerading, and exploitation for privilege escalation, ultimately leading to the deployment of XMRig malware. The priority technique identified is T1078 Valid Accounts, which highlights the importance of securing and monitoring account access. The priority control, as recommended, is to "Enforce MFA on all accounts; disable dormant and over-privileged accounts; alert on impossible-travel and anomalous logons."

Infrastructure and Corroboration

There is no specific information available on the hosting providers or ASNs observed in this campaign, as indicated by the lack of data in the infrastructure and corroboration section. Similarly, no malware families have been corroborated by abuse.ch, and no indicators have been flagged with high confidence 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)

- T1548.003 Sudo and Sudo Caching
- T1036.005 Match Legitimate Resource Name or Location
- T1053.003 Cron
- T1070.002 Indicator Removal
- T1070.003 Clear Command History
- T1036 Masquerading
- T1055 Process Injection
- T1098 Account Manipulation
- T1562.001 Impair Defenses: Disable or Modify Tools
- T1078 Valid Accounts
- T1571 Non-Standard Port
- T1068 Exploitation for Privilege Escalation
- T1027 Obfuscated Files or Information
- T1573 Encrypted Channel
- T1195.002 Compromise Software Supply Chain
- T1496 Resource Hijacking
- T1027.002 Software Packing
- T1071.001 Web Protocols

Analytical Scores

- Priority technique (graph chokepoint): T1078 Valid Accounts (centrality 0.3187).
- Operational risk: Critical (score 1.0, reaches impact).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.3795; 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
Rocke	0.3795
Cobalt Group	0.3411
RedEcho	0.3162
APT18	0.3162
APT41	0.3128

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	unable[.]download
Hash	17b60d650fc5d1718d7f2ac3a6075d11
Hash	88520bcfc741610591a23592f9d4ecb31e34deb5
Hash	55c67c844258807c4335f40262777a5307bcf5b537c0492cf869b3328796f838

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:** T1078 Valid Accounts (initial-access)

- **Observed here:** T1078 Valid Accounts was the initial-access control point; blocking a means-of-entry rarely stops a determined actor, so the pivot projects forward to the execution stage they must still reach.
- **Projected pivot:** T1059 Command and Scripting Interpreter (execution)
- **Basis:** of the 56+ groups that use Valid Accounts, this pairing runs 1.2x above base rate, a disproportionately-coupled move rather than the obvious one.

The actor could pivot to utilizing T1059 Command and Scripting Interpreter, leveraging its versatility to execute commands and scripts, potentially bypassing the restrictions imposed by the blocked T1078 Valid Accounts technique, as this would allow them to interact with the system without relying on compromised credentials. This technique may be particularly appealing as it enables the actor to execute scripts and commands in a way that could blend in with normal administrative activity, making detection more challenging. To counter this potential move, the mandated defensive control of constraining PowerShell for unprivileged users, enabling script-block logging, and blocking wscript/cscript where unneeded, would likely be an effective measure.

Also plausible (same tactic): T1569 System Services (n=13, lift 2.0), T1072 Software Deployment Tools (n=6, lift 2.3)

Detection and hardening for the pivot (T1059 Command and Scripting Interpreter)

- **Telemetry:** Sysmon / EDR process + command line; PowerShell Script Block Logging (4104); AMSI
- **Detect:**
  - Security 4688 / Sysmon 1 with full command lines; encoded or obfuscated PowerShell
  - PowerShell 4104 script-block content; suspicious cmdlets and download cradles
  - Office or browser processes spawning powershell/cmd/wscript
- **Harden:**
  - Enable Script Block Logging + AMSI; Constrained Language Mode
  - Application control (WDAC/AppLocker); remove/limit unused interpreters
- **MITRE:** M1049 Antivirus/Antimalware, M1038 Execution Prevention, M1042 Disable or Remove Feature, M1045 Code Signing · DS0009 Process, DS0012 Script, DS0017 Command