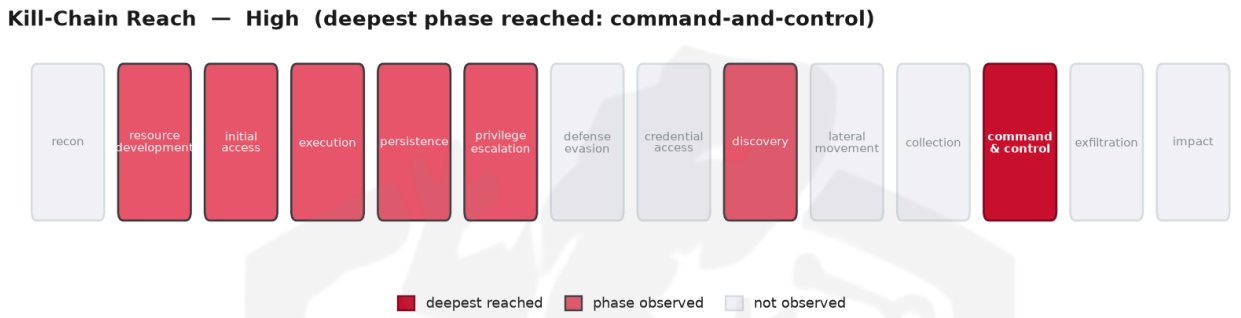
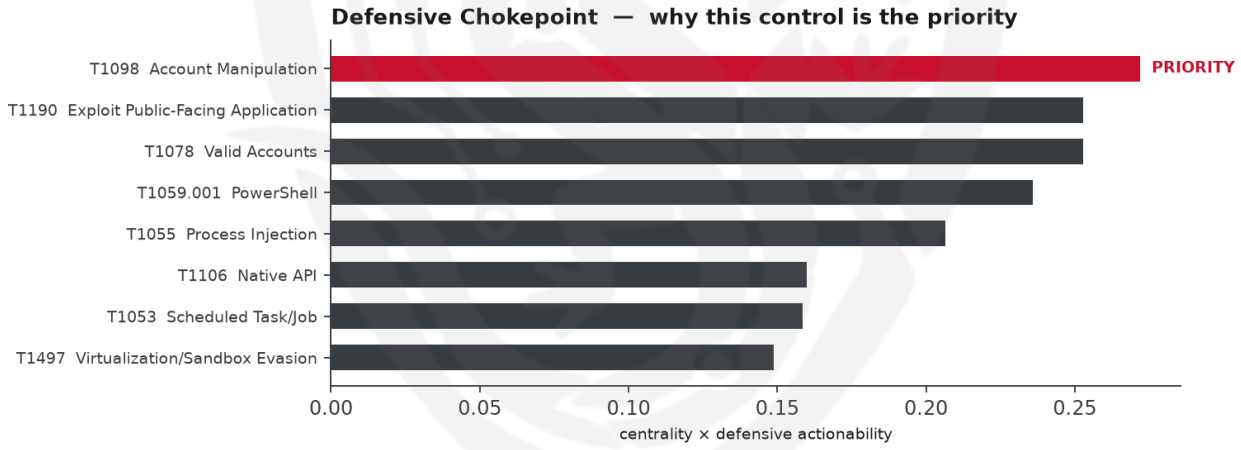
THREAT REPORT: EAGLE WEREWOLF, ENERGETIC BEAR, VELVET TEMPEST, APT28, GRAYCHARLIE

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 Eagle Werewolf, ENERGETIC BEAR, Velvet Tempest, APT28, and GrayCharlie, who have been observed exploiting the CVE-2025-11953 vulnerability, primarily targeting the energy and government sectors. The threat actor has utilized various malware families, including Phorpiex, Twizt, and XMRig, among others. Priority should be given to patching the CVE-2025-11953 vulnerability on all affected systems to prevent further exploitation. The threat actor's activities pose a significant risk, and defensive measures should be taken to alert on privilege and group changes.

Threat Overview

The observed cluster of activity, attributed to Eagle Werewolf, ENERGETIC BEAR, Velvet Tempest, APT28, and GrayCharlie, involves the exploitation of the CVE-2025-11953 vulnerability using malware

families such as Phorpiex, Twizt, and XMRig. The victimology indicates that the energy and government sectors are the primary targets. The threat actor's techniques include creating or modifying system processes, spearphishing, and exploiting public-facing applications.

Attack Chain and Priority Control

The attack chain involves a series of techniques, including creating or modifying system processes, spearphishing, and exploiting public-facing applications, ultimately leading to the exploitation of the CVE-2025-11953 vulnerability. The priority technique is T1098 Account Manipulation, which serves as a chokepoint in the attack chain. To mitigate this threat, the priority control is to: Patch CVE-2025-11953 on all affected systems as the top priority, then: Alert on privilege/group changes and credential additions to accounts (Event ID 4738/4670); review conditional-access changes.

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 an AbuseIPDB confidence 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)

- T1543 Create or Modify System Process
- T1071.004 DNS
- T1566.001 Spearphishing Attachment
- T1053 Scheduled Task/Job
- T1106 Native API
- T1140 Deobfuscate/Decode Files or Information
- T1190 Exploit Public-Facing Application
- T1583.001 Domains
- T1036 Masquerading
- T1055 Process Injection
- T1497 Virtualization/Sandbox Evasion
- T1059.001 PowerShell
- T1098 Account Manipulation
- T1562.001 Impair Defenses: Disable or Modify Tools
- T1078 Valid Accounts
- T1027 Obfuscated Files or Information
- T1573 Encrypted Channel
- T1071.001 Web Protocols
- T1136 Create Account

- T1105 Ingress Tool Transfer
- T1204.001 Malicious Link

Analytical Scores

- Priority technique (graph chokepoint): T1098 Account Manipulation (centrality 0.2863).
- 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 0.5; 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
Winter Vivern	0.5
WIRTE	0.4938
LazyScripter	0.4747
BITTER	0.4707
TA505	0.4481

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.

Indicators of Compromise (defanged — non-clickable)

No indicators were attached to this pulse.