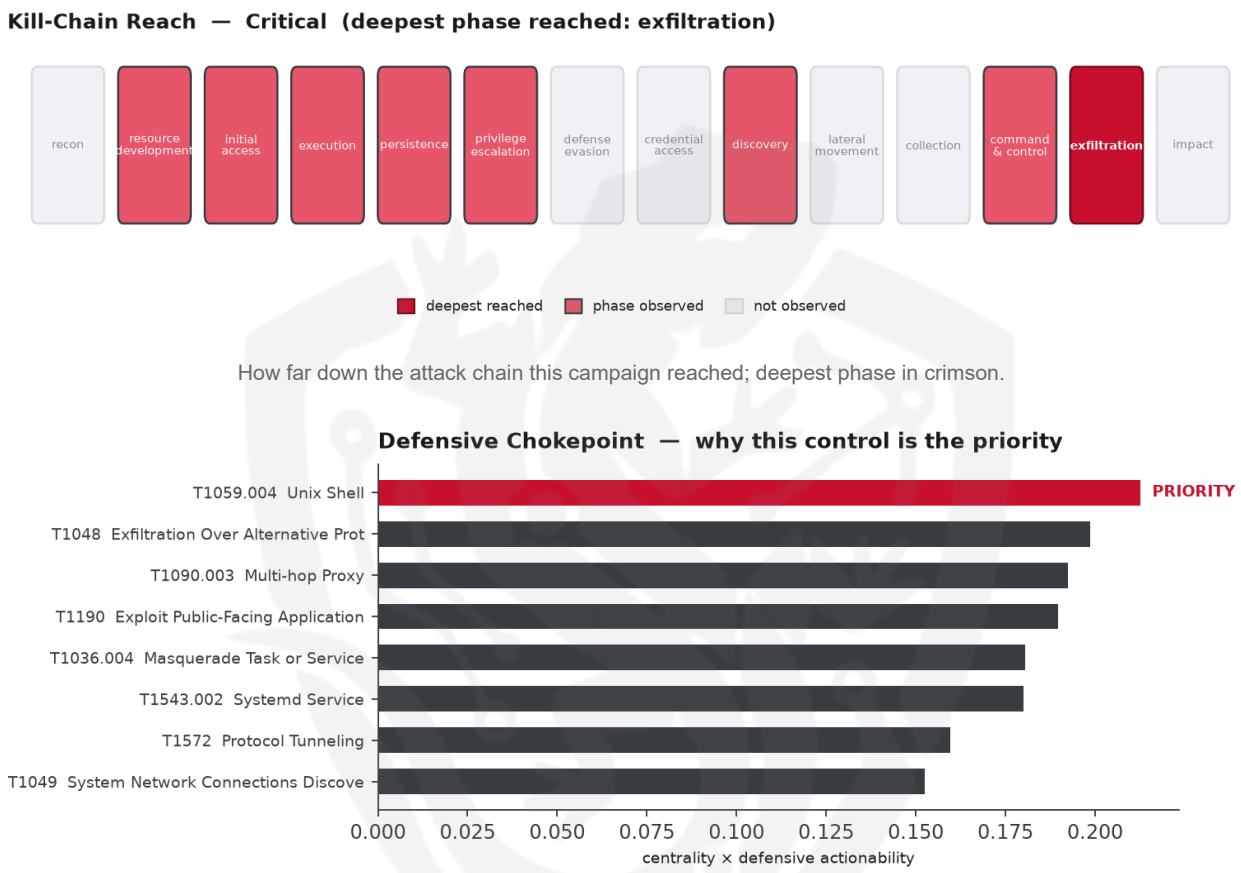
THREAT REPORT: PCPJACK

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 PCPJack, a threat actor who has hijacked over 230 cloud servers across AWS, GCP, and Azure to operate a hidden SMTP relay network. The actor utilizes various malware families, including Sliver and Chisel, to carry out their operations. Priority should be given to constraining PowerShell for unprivileged users and enabling script-block logging to mitigate the threat. The targeted country and sectors remain unknown due to insufficient data.

Threat Overview

The threat actor, PCPJack, employs a range of techniques, including exploiting public-facing applications and utilizing protocol tunneling, to achieve their goals. The malware families used, Sliver and Chisel, play a crucial role in the actor's operations. Although the central CVE is unknown, the actor's techniques, such as masquerading tasks and services, and exfiltrating data over alternative protocols, pose a significant threat.

Attack Chain and Priority Control

The observed techniques used by PCPJack form a complex attack chain, involving cron jobs, exploit of public-facing applications, and protocol tunneling, among others. The priority technique is T1059.004 Unix Shell, which serves as a critical chokepoint in the attack chain. To counter this, the priority control is to Constrain PowerShell for unprivileged users (Constrained Language Mode + AppLocker); enable script-block logging; block wscript/cscript where unneeded.

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, 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)

- T1053.003 Cron
- T1190 Exploit Public-Facing Application
- T1572 Protocol Tunneling
- T1583.003 Virtual Private Server
- T1036.004 Masquerade Task or Service
- T1049 System Network Connections Discovery
- T1057 Process Discovery
- T1048 Exfiltration Over Alternative Protocol
- T1090.003 Multi-hop Proxy
- T1059.004 Unix Shell
- T1543.002 Systemd Service
- T1564.001 Hidden Files and Directories

Analytical Scores

- Priority technique (graph chokepoint): T1059.004 Unix Shell (centrality 0.2659).
- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.3569; 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	0.3569
APT5	0.2832
Poseidon Group	0.2767
Winter Vivern	0.2677
FIN13	0.2649

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.

Indicators of Compromise (defanged — non-clickable)

No indicators were attached to this pulse.

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:** T1059.004 Unix Shell (execution)
- **Observed here:** PCPJack used T1053.003 Cron here as an alternative execution technique.
- **Projected pivot:** T1053.003 Cron (execution)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

PCPJack could pivot to utilizing T1053.003 Cron to maintain persistence and execute malicious commands at scheduled intervals, potentially evading detection by blending in with legitimate system tasks. This technique may allow PCPJack to adapt to the blocked Unix Shell control by leveraging the cron utility to schedule and run malicious jobs. To counter this, the defensive control would involve alerting on new scheduled tasks and restricting access to task scheduling utilities, as mandated by alerting on new scheduled tasks (Event ID 4698); restrict schtasks/at to admins; baseline legitimate task creators.

Detection and hardening for the pivot (T1053.003 Scheduled Task/Job)

- **Telemetry:** Windows Security (Object Access audit); Microsoft-Windows-TaskScheduler/Operational; Sysmon
- **Detect:**
  - Security 4698 (task created), 4702 (updated), 4700/4701 (enabled/disabled), 4699 (deleted)
  - TaskScheduler/Operational 106 (registered), 140 (updated), 141 (deleted)

    - Sysmon 1 for schtasks.exe and at.exe; Sysmon 11 for writes under C:\Windows\System32\Tasks\
- **Harden:**
    - Restrict schtasks/at to administrators; disable the legacy at.exe
    - Baseline the legitimate task creators and alert on anything outside it
- **MITRE:** M1047 Audit, M1028 Operating System Configuration, M1026 Privileged Account Management · DS0003 Scheduled Job, DS0009 Process, DS0022 File