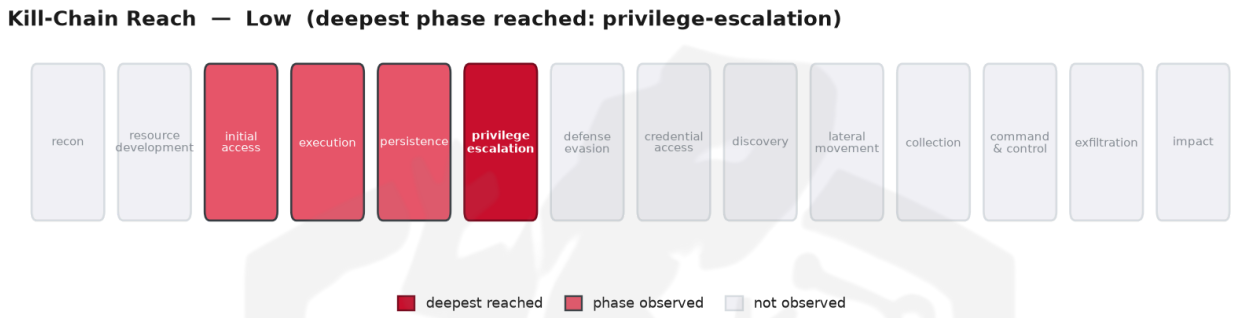
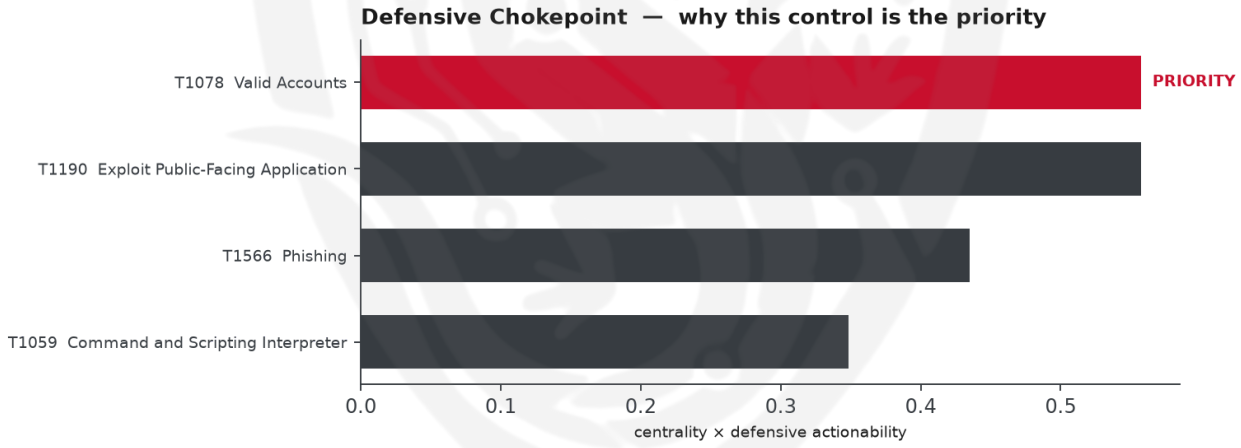
THREAT REPORT: REDHOOK TARGETS INDONESIA'S FINANCE AND GOVERNMENT SECTORS

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 RedHook malware family, targeting Indonesia's finance and government sectors. The reporting indicates techniques such as command and scripting interpreter, valid accounts, exploit public-facing application, and phishing are being used. Priority should be given to enforcing multi-factor authentication and disabling dormant accounts to mitigate the threat. The threat actor's identity remains insufficiently determined.

Threat Overview

The threat actor, linked to the RedHook malware family, is targeting Indonesia's finance and government sectors. The reporting indicates the use of various techniques, including command and scripting

interpreter, valid accounts, exploit public-facing application, and phishing. The victimology suggests a focus on Indonesian financial and government institutions.

Attack Chain and Priority Control

The observed techniques suggest a chain of activity that includes exploiting public-facing applications, using valid accounts, and employing phishing tactics. The priority technique is T1078 Valid Accounts, which serves as a chokepoint in the attack chain. To counter this, the lead control is: Enforce MFA on all accounts; disable dormant and over-privileged accounts; alert on impossible-travel and anomalous logons.

Infrastructure and Corroboration

There is no observed hosting provider or ASN associated with this activity. Additionally, no malware families have been corroborated by abuse.ch, and 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, machine-extracted from report text — reduced confidence)

The source pulse carried no expert ATT&CK tags, so these techniques were inferred from its narrative by a self-consensus LLM extractor and validated against the ATT&CK catalogue. Treat this technique set, and the chokepoint, kill-chain and risk scores derived from it, as lower-confidence than an expert-tagged brief. - T1059 Command and Scripting Interpreter - T1078 Valid Accounts - T1190 Exploit Public-Facing Application - T1566 Phishing

Analytical Scores

- Priority technique (graph chokepoint): T1078 Valid Accounts (centrality 0.5573).
- Operational risk: Low (score 0.276, reaches privilege-escalation).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.433; 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
GOLD SOUTHFIELD	0.433
Suckfly	0.378
Threat Group-1314	0.378
TA459	0.3536
AppleJeus	0.3536

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	api[.]3n7wj[.]com
Domain	skt[.]3n7wj[.]com
Domain	sktv[.]3n7wj[.]com
URL	hxxp://sktv[.]3n7wj[.]com/ws/device?menberId=
URL	hxxps://api[.]3n7wj[.]com
Hash	453333bffdd1850ea2e0647f7c805530b578919978a01b1e2be52d6eb2add946

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:** T1047 Windows Management Instrumentation (execution)
- **Basis:** of the 29+ groups that use Valid Accounts, this pairing runs 1.8x above base rate, a disproportionately-coupled move rather than the obvious one.

The actor could pivot to T1047 Windows Management Instrumentation to maintain access and evade detection, as this technique allows them to leverage the existing Windows management infrastructure to execute commands and gather information, potentially exploiting the same level of access that was previously obtained through T1078 Valid Accounts. This technique may be particularly appealing to the actor because it enables them to interact with the system in a way that blends in with normal administrative activity, making it harder to detect. The defensive countermeasure to mitigate this potential pivot is to monitor wmiprvse.exe child-process creation; restrict remote WMI (DCOM) at the host firewall; enable WMI-Activity operational logging.

Also plausible (same tactic): T1569 System Services (n=13, lift 2.0), T1053 Scheduled Task/Job (n=31, lift 1.4)

Detection and hardening for the pivot (T1047 Windows Management Instrumentation)

- **Telemetry:** Sysmon (WMI events); Microsoft-Windows-WMI-Activity/Operational
- **Detect:**
  - Sysmon 19/20/21 (WMI event filter/consumer/binding) for persistence
  - wmic.exe / WmiPrvSE.exe spawning shells; remote WMI process creation
  - WMI-Activity/Operational operations from unusual users/hosts
- **Harden:**
  - Restrict WMI remote access; monitor permanent WMI subscriptions
  - Least-privilege; segment management protocols
- **MITRE:** M1040 Behavior Prevention, M1038 Execution Prevention, M1026 Privileged Account Management · DS0009 Process, DS0005 WMI, DS0017 Command