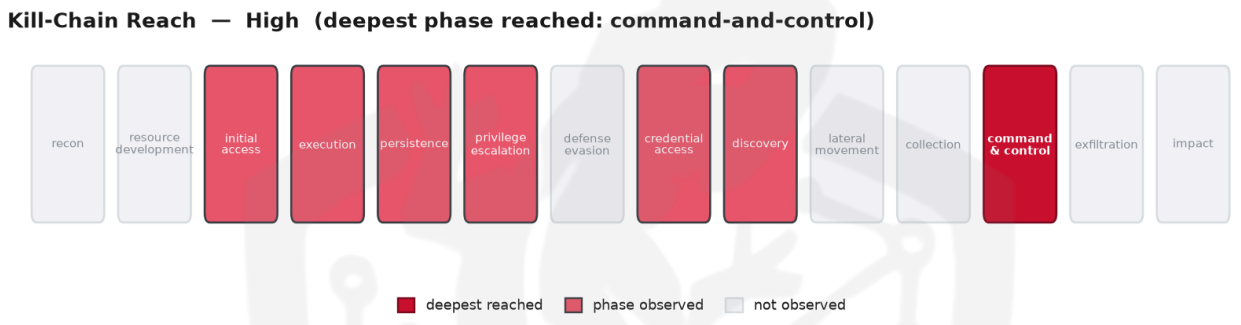
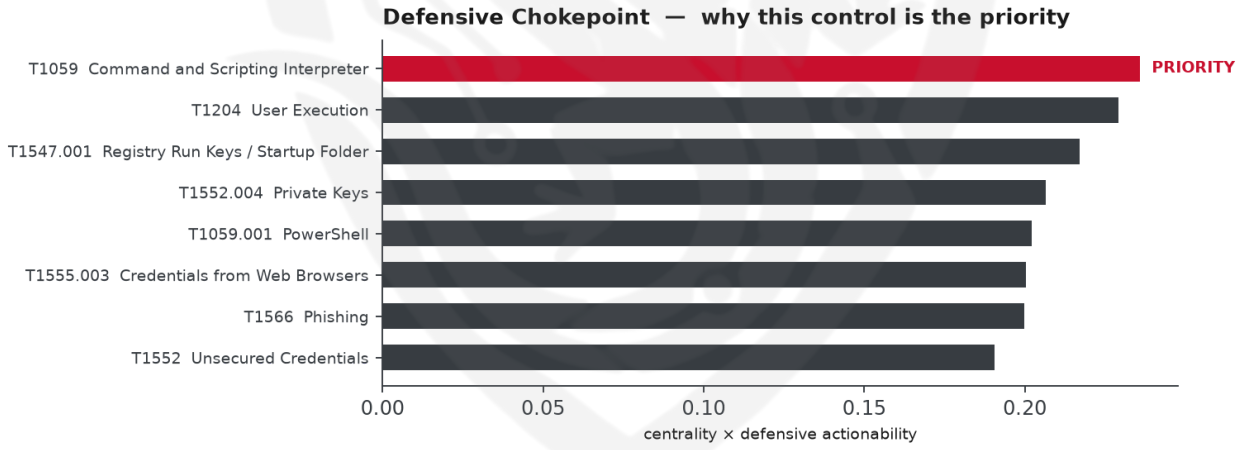
THREAT REPORT: FAKE COREPACK SITE TARGETS DEVELOPERS WITH INFOSTEALER AND PROXYWARE

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 is distributing OpenShield and Apprunner malware to developers in the technology sector, although the specific countries targeted are not known. The threat actor is exploiting various techniques to gain access to sensitive information. Priority should be given to constraining scripting interpreters to prevent further exploitation. The lack of specific attribution and central CVE information highlights the need for vigilance in defending against this threat.

Threat Overview

The threat actor, whose identity is not specified, is utilizing OpenShield and Apprunner malware families to target developers. The exploited vulnerability is not identified, but the actor is employing various

techniques, including masquerading, spearphishing, and system information discovery, to compromise their targets. The technology sector is the primary target of this campaign.

Attack Chain and Priority Control

The observed techniques form a complex chain, starting with masquerading and spearphishing, followed by system information discovery, and ultimately leading to command and scripting interpreter exploitation. The priority technique in this chain is T1059 Command and Scripting Interpreter, which serves as a critical chokepoint. To mitigate this threat, the recommended priority control is: Constrain PowerShell for unprivileged users (Constrained Language Mode + AppLocker); enable script-block logging; block wscript/cscript where unneeded.

Infrastructure and Corroboration

There is no specific information available on the hosting providers or ASNs observed in this campaign. 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, expert-tagged by source)

- T1036.005 Match Legitimate Resource Name or Location
- T1547 Boot or Logon Autostart Execution
- T1204.002 Malicious File
- T1566.002 Spearphishing Link
- T1082 System Information Discovery
- T1555 Credentials from Password Stores
- T1036 Masquerading
- T1552 Unsecured Credentials
- T1555.003 Credentials from Web Browsers
- T1552.004 Private Keys
- T1090 Proxy
- T1059 Command and Scripting Interpreter
- T1204 User Execution
- T1057 Process Discovery
- T1059.001 PowerShell
- T1547.001 Registry Run Keys / Startup Folder
- T1566 Phishing
- T1090.003 Multi-hop Proxy
- T1203 Exploitation for Client Execution
- T1059.003 Windows Command Shell

- T1189 Drive-by Compromise

Analytical Scores

- Priority technique (graph chokepoint): T1059 Command and Scripting Interpreter (centrality 0.2949).
- 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 0.5239; 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
Inception	0.5239
Windshift	0.49
Darkhotel	0.4865
APT37	0.483
Molerats	0.4801

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	corepack[.]org
Domain	yakteam[.]xyz
URL	hxxp://freevpn[.]win/lps/gbox-lp/index[.]html
URL	hxxp://openshield[.]canatrace[.]com/download-free-can/

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 Command and Scripting Interpreter (execution)
- **Observed here:** T1059 Command and Scripting Interpreter was the only execution technique observed in this campaign, so the pivot is projected from cross-actor behaviour.
- **Projected pivot:** T1053 Scheduled Task/Job (execution)
- **Basis:** of the 54+ groups that use Command and Scripting Interpreter, this pairing runs 1.3x above base rate, a disproportionately-coupled move rather than the obvious one.

The actor could pivot to T1053 Scheduled Task/Job to maintain persistence and execute malicious commands at a later time, potentially leveraging the Windows Task Scheduler to blend in with legitimate system activity, which may allow them to bypass the blocked command and scripting interpreter control. This technique in particular could be appealing to the actor because it enables them to schedule tasks to run under the context of a specific user or system account, which may provide the necessary privileges to achieve their objectives. To counter this potential move, the defensive control would be to alert on new scheduled tasks (Event ID 4698), restrict schtasks/at to admins, and baseline legitimate task creators.

Also plausible (same tactic): T1047 Windows Management Instrumentation (n=40, lift 1.3), T1574 Hijack Execution Flow (n=32, lift 1.2)

Detection and hardening for the pivot (T1053 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