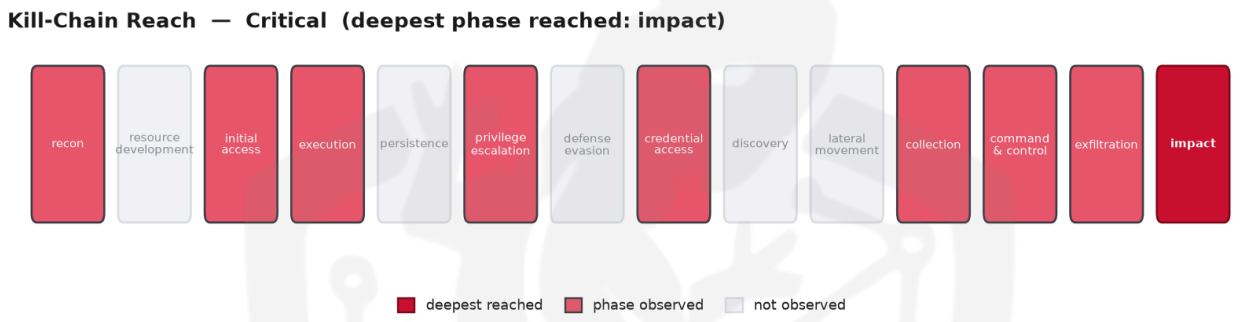
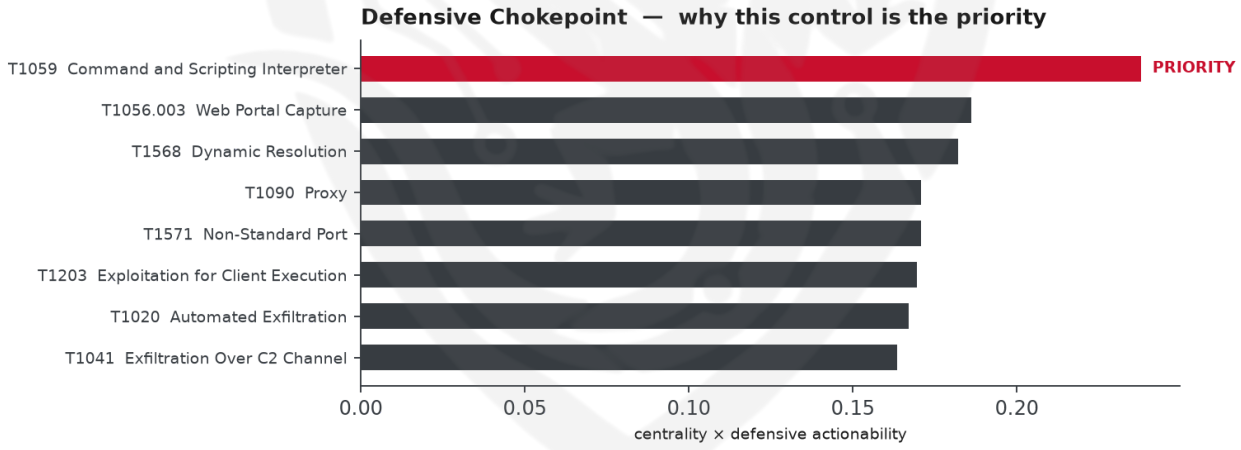
THREAT REPORT: UNATTRIBUTED MALWARE CAMPAIGN TARGETS EDUCATION, GOVERNMENT, AND TRANSPORTATION SECTORS

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 involves the use of various malware families, including Phorpiex, Mozi, SectopRAT, Mirai, and Boatnet, to target the education, government, and transportation sectors. The threat actor's identity and motivations are unknown. Priority should be given to constraining PowerShell for unprivileged users and enabling script-block logging to mitigate the threat. The campaign's impact is considered critical, reaching the operational risk band.

Threat Overview

The threat actor, whose identity is unknown, is utilizing a range of malware families to exploit public-facing applications and steal web session cookies. The targeted sectors include education, government, and

transportation, although the specific countries targeted are unknown. The malware families used include Phorpiex, Mozi, SectopRAT, Mirai, and Boatnet.

Attack Chain and Priority Control

The observed techniques used by the threat actor include stealing web session cookies, exploiting public-facing applications, and using remote access tools. The priority technique is T1059 Command and Scripting Interpreter, which is the graph chokepoint. To mitigate this threat, 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

The malicious infrastructure is hosted on various providers, including Omegatech LTD, Interdigi Joint Stock Company, Yisu Cloud Ltd, and Servinga GmbH. Abuse.ch has corroborated the presence of malware families such as CoinMiner, Phorpiex, SectopRAT, Socks5Systemz, Stealc, and Unknown malware. However, AbuseIPDB has only reported a highest confidence level of 14% for the indicators, with no indicators reaching an 80% confidence level.

Technical Appendix

Ground-truth telemetry from the source pulse; analytical scores are secondary and clearly labelled.

Observed Techniques (ATT&CK, expert-tagged by source)

- T1539 Steal Web Session Cookie
- T1071 Application Layer Protocol
- T1190 Exploit Public-Facing Application
- T1219 Remote Access Tools
- T1055 Process Injection
- T1595 Active Scanning
- T1056.003 Web Portal Capture
- T1090 Proxy
- T1059 Command and Scripting Interpreter
- T1020 Automated Exfiltration
- T1568 Dynamic Resolution
- T1041 Exfiltration Over C2 Channel
- T1571 Non-Standard Port
- T1027 Obfuscated Files or Information
- T1573 Encrypted Channel
- T1203 Exploitation for Client Execution
- T1095 Non-Application Layer Protocol
- T1498 Network Denial of Service
- T1027.002 Software Packing

- T1105 Ingress Tool Transfer

Analytical Scores

- Priority technique (graph chokepoint): T1059 Command and Scripting Interpreter (centrality 0.2974).
- Operational risk: Critical (score 1.0, reaches impact).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.3273; 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	0.3273
RedEcho	0.3086
BITTER	0.2996
Metador	0.2817
Sandworm Team	0.2717

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 14%.
- Malware families corroborated by abuse.ch: CoinMiner, Phorpiex, SectopRAT, Socks5Systemz, Stealc, Unknown malware.
- Note: enrichment raises the severity signal (an IOC at or above 80% AbuseIPDB confidence, or a confirmed malware-family hit). This is context, not a change to the source assessment.

Indicators of Compromise (defanged — non-clickable)

The network and file indicators observed in this activity are listed below for blocklisting:

Type	Indicator	Context
IP	103[.]245[.]236[.]146	AbuseIPDB 0% (VN) · AS151858 Interdigi Joint Stock Company
IP	154[.]92[.]19[.]71	AbuseIPDB 0% (HK) · AS142403 Yisu Cloud Ltd

Type	Indicator	Context
IP	178[.]16[.]54[.]109	AbuseIPDB 14% (NL) · Unknown malware · AS202412 Omegatech LTD
IP	91[.]92[.]243[.]29	AbuseIPDB 0% (NL) · Phorpiex · AS202412 Omegatech LTD
IP	194[.]76[.]227[.]94	AbuseIPDB 0% (EE) · AS207408 Servinga GmbH
IP	178[.]16[.]54[.]31	AbuseIPDB 0% (NL) · Socks5Systemz · AS202412 Omegatech LTD
IP	87[.]120[.]107[.]33	AbuseIPDB 0% (FI) · SectopRAT · AS215428 Mykyta Skorobohatko
IP	2[.]26[.]98[.]67	AbuseIPDB 0% (DE) · AS215439 Play2Go International Limited
IP	62[.]60[.]179[.]230	AbuseIPDB 0% (US) · AS15611 Iranian Research Organization for Science & Technology
Hash	083d5895283755a910b5c59d60a5348b	CoinMiner
Hash	0d94bf4d0418061907ff7977e3f25a463cb25188	CoinMiner
Hash	9639f7ebc6a6d69d7bf5b8bc869e7783a1406088f192868624ad8919e9bfd1d4	CoinMiner
Hash	e3513922666c202c1ae5c06eea277ba10477868d6d89ce2819f4f8ff9070bc85	Phorpiex
Hash	01a96eeafb72042b3f69afd21b4c9155dbfe7f97ab3dca392972ad531a075ac2	
Hash	bf24277400cc453d530e4277d3bd24e96c5e409adef6970518bdc59205aa0241	Stealc
Hash	946a9cc6b501d993a108c90ef7d0930d	Stealc
Hash	c98aa812a271c9c78017c2c90b60a97ae13df9cf	Stealc
Hash	04d20417bb04779c8762032b8c6942be	Phorpiex

Type	Indicator	Context
Hash	0783237785d65621d1e887f24cc2103b	
Hash	1fec4103f40b6432e45d67fc87b504e024962376	Phorpiex
Hash	7f6f4b3b341818b6db89fac39efb6c257addde95	
Hash	cc43cdbe8eb9874f55fffbe23b560b673eb9f31fb9a953926bba29464fd2dd07	
Hash	e310476c41ae4f6e3c4ed9bb88303ee6e5e1455bd7afe51cf48965ea7599e6e5	
Hash	e5715e6611ef6bcb233f5d2098510dab3db408abbb728b00e1821bb255829373	

Reputation by AbuseIPDB · malware attribution by abuse.ch · Geo/ASN data by IP2Location LITE.

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 and evade detection. This technique may be particularly appealing as it allows the actor to execute tasks without requiring an interactive login session, which could be useful if the actor's initial command and scripting interpreter access has been blocked. To counter this potential move, the defensive control would be to alert on new scheduled tasks (Event ID 4698); restrict schtasks/at to admins; 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