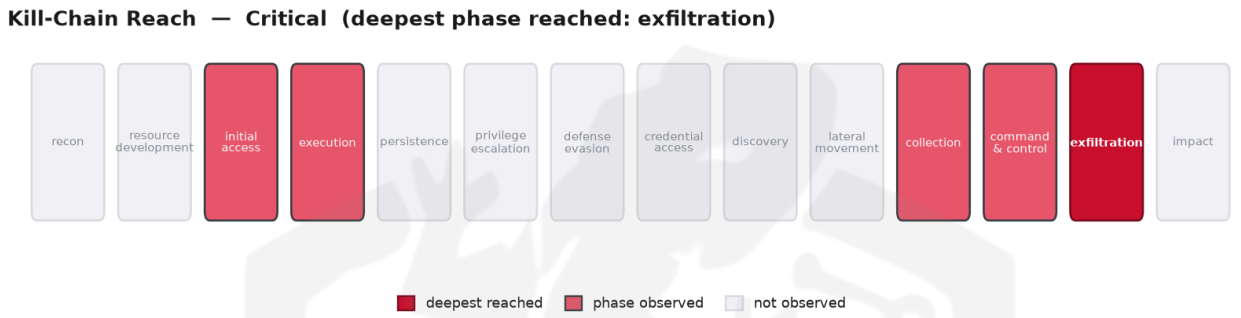
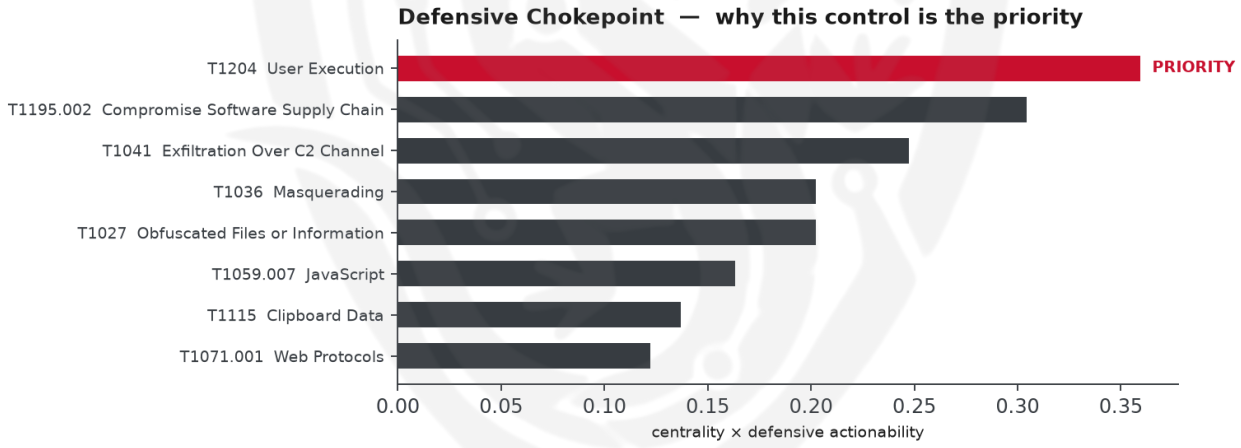
THREAT REPORT: UNKNOWN_ADVERSARY MALICIOUS BROWSER EXTENSIONS

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 malicious browser extensions posing as free VPNs, which install clipboard stealers via updates. These extensions, including "VPN Go: Free VPN" and "Free VPN by VPN GO", are the primary malware families involved. The targeted countries and sectors are unknown, but priority should be given to blocking the execution of malicious files and raising user awareness about potential lures. The threat actor's identity remains insufficient to determine.

Threat Overview

The threat actor, referred to here as the observed cluster of activity, utilizes malware families such as "VPN Go: Free VPN" and "Free VPN by VPN GO" to exploit unsuspecting users. The central vulnerability exploited is insufficient to determine, but the techniques used include masquerading, user execution, and

exfiltration over command and control channels. The victimology of this campaign is also insufficient to determine.

Attack Chain and Priority Control

The attack chain involves a series of techniques, including JavaScript execution, clipboard data theft, and masquerading, ultimately leading to exfiltration over a command and control channel. The priority technique in this chain is T1204 User Execution, which serves as a critical chokepoint. To mitigate this threat, the priority control is to "Block execution of downloaded HTA/JS/LNK; enforce mark-of-the-web; disable Office macros from the internet; user awareness on lures."

Infrastructure and Corroboration

The malicious infrastructure associated with this activity is hosted by providers such as Aeza Group LLC and Local NCC Ltd. However, there are no corroborated malware families from abuse.ch, and no indicators have reached an 80% confidence level on AbuseIPDB, with the highest confidence seen being 0%. These findings are based on third-party enrichment and do not override the primary source assessment.

Technical Appendix

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

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

- T1059.007 JavaScript
- T1115 Clipboard Data
- T1036 Masquerading
- T1204 User Execution
- T1041 Exfiltration Over C2 Channel
- T1027 Obfuscated Files or Information
- T1195.002 Compromise Software Supply Chain
- T1071.001 Web Protocols

Analytical Scores

- Priority technique (graph chokepoint): T1204 User Execution (centrality 0.4495).
- Operational risk: Critical (score 0.885, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.3853; 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
Daggerfly	0.3853
TA551	0.3772
Higaisa	0.3767
Windshift	0.3693
TA577	0.3636

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	Context
IP	77[.]91[.]123[.]187	AbuseIPDB 0% (NL) · AS212171 Local NCC Ltd.
IP	178[.]236[.]252[.]133	AbuseIPDB 0% (NL) · AS210644 Aeza Group LLC
IP	178[.]236[.]252[.]161	AbuseIPDB 0% (NL) · AS210644 Aeza Group LLC
Domain	gecko[.]id	
Domain	vpngogmail[.]com	
Domain	vpngo[.]com	
URL	hxxp://178[.]236[.]252[.]133/html/continue[.]php	
URL	hxxp://77[.]91[.]123[.]187/html/continue[.]php	
URL	hxxp://178[.]236[.]252[.]161/html/continue[.]php	

Type	Indicator	Context
URL	hxxp://77[.]91[.]123[.]187/html/continue[.]php[.]	
Hash	43dc5b1d4c73d5ed9f4f7f561830079896eeb533a7c21bc577e4e267d5a3aa56	
Hash	b3b63970833b3379ecec2d3ef8fea328fef8dd1c1574b1bcdfebad5bdce9280c	
Hash	72fc06a8b03720f4a64744eecd5b3f658ad880bdb327c0c465c7bdc66b14a8d2	
Hash	fbbdf4bc490ad7b28953630c1707aa68b89d319b9b735f3d8563320b81b21a97	
Hash	2fe9c41901045013ba28ccb9af5870f9aef4f1ffd1e717cd5e0189ffdbe7fca2	
Hash	11f01e8296a074e6e3b23e9413c51f205d4b6a14146fb4d95bec291d768a9071	
Hash	638636692e3eef6c83dbca784a40fb7b6ac95b76d6551a2fbdfebc11588ad8ff	
Hash	7386252b9a86e5357e6aa884326720abf015465a2567e75717830b6688ef05cc	
Hash	d7d43e8e8f03afdcaaba85622daf24ced944e7ca4d03ac124fc325d0bb6e3d66	

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:** T1204 User Execution (execution)
- **Observed here:** the threat actor used T1059.007 JavaScript here as an alternative execution technique.
- **Projected pivot:** T1059.007 JavaScript (execution)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

The actor could pivot to using JavaScript (T1059.007) to maintain their objective, potentially leveraging it to execute malicious code or scripts in a way that evades the blocked User Execution control. This technique may allow the actor to continue their campaign, possibly by using JavaScript to interact with the

system in an unauthorized manner. To counter this potential move, the mandated defensive control of constraining PowerShell for unprivileged users, enabling script-block logging, and blocking wscript/cscript where unneeded should be implemented.

Detection and hardening for the pivot (T1059.007 Command and Scripting Interpreter)

- **Telemetry:** Sysmon / EDR process + command line; PowerShell Script Block Logging (4104); AMSI
- **Detect:**
  - Security 4688 / Sysmon 1 with full command lines; encoded or obfuscated PowerShell
  - PowerShell 4104 script-block content; suspicious cmdlets and download cradles
  - Office or browser processes spawning powershell/cmd/wscript
- **Harden:**
  - Enable Script Block Logging + AMSI; Constrained Language Mode
  - Application control (WDAC/AppLocker); remove/limit unused interpreters
- **MITRE:** M1049 Antivirus/Antimalware, M1038 Execution Prevention, M1042 Disable or Remove Feature, M1045 Code Signing · DS0009 Process, DS0012 Script, DS0017 Command