Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

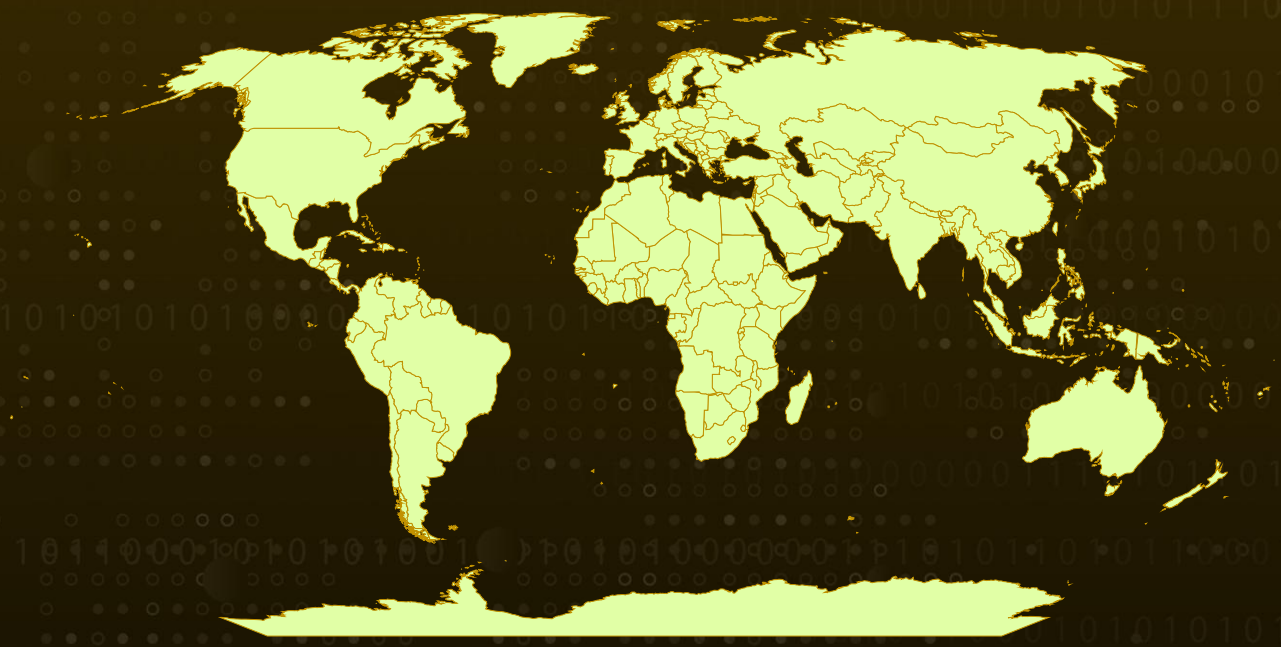
TerminalFix: Fake Cloudflare Checks Open a Reverse Tunnel

Date of Publication	Admiralty Code	TA Number
August 31, 2026	A1	TA2026254

Summary

First Seen: 2026
Targeted Regions: Worldwide
Targeted Platform: Windows
Campaign: TerminalFix (a ClickFix variant)
Attack: TerminalFix is a ClickFix-style social engineering campaign that uses compromised websites to display a fake Cloudflare Turnstile CAPTCHA. Victims are guided to paste a PowerShell command into Windows Terminal or PowerShell, which downloads a ZIP archive and sideloads a malicious DLL through a legitimate signed binary. The chain then pulls further payloads hidden inside PNG images, sets up registry and scheduled-task persistence, runs deep Active Directory reconnaissance, and finally drops a Python reverse-tunnel implant that hands the attacker encrypted, network-level proxy access into the environment.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, Overture Maps Fundation, TomTom, Zenrin

Targeted Non-Targeted

Attack Details

#1

TerminalFix is a fresh spin on the ClickFix playbook, built to lure people into pasting a malicious command into Windows Terminal or PowerShell. It starts on a compromised website that swaps its real content for a fake Cloudflare Turnstile overlay, logo, "Verify you are human" checkbox, and spinner, which copies a PowerShell command to the clipboard and tells the user to paste it into the terminal. Steering victims there instead of the Run dialog is the key twist: it makes long, multi-line scripts run cleanly. Once pasted, the command prints reassuring Cloudflare-themed messages while it downloads a ZIP from attacker infrastructure, unpacks it to C:\ProgramData, and silently launches a batch file.

#2

The batch file launches LockScreenContentServer.exe, a legitimate signed binary that normally loads dui70.dll. Because Windows checks the application folder before System32, a malicious dui70.dll planted alongside it loads instead, DLL sideloading that runs attacker code inside a trusted, signed process. That DLL decodes an obfuscated payload in memory without touching disk, then runs PowerShell that pulls three PNG images from attacker domains and uses steganography to rebuild an executable and a DLL hidden in their pixels before deleting the images. For persistence, it adds an HKCU Run key and a scheduled task that fires every 60 minutes, and hides its working folder with system and hidden attributes.

#3

Next comes heavy reconnaissance that looks like groundwork for hands-on-keyboard activity. The malware gathers system details using English, Spanish, and German locale filters, maps domain trusts, checks domain admin membership, and searches Active Directory for users and computers, even scraping user description fields, which sometimes leak passwords or role hints. It then pings servers named for common roles such as domain controllers, databases, backup, gateways, and mail to chart the internal network, and runs a PowerShell file-watch loop that executes commands dropped into a text file and writes results to another, a simple asynchronous shell. Microsoft did not see the follow-on hands-on actions here, but the recon and access clearly set up privilege escalation and lateral movement.

#4

The finale is a custom Python reverse-tunnel implant. The attacker ships an unmodified, signed Python 3.14.5 runtime from python.org and keeps all malicious logic in client.py, launched through pythonw.exe so no window appears. It dials out over TLS on port 443 to gitnow[.]dev, upgrades to a WebSocket, and relays arbitrary TCP traffic, with certificate checks disabled and browser User-Agent strings rotating; its SOCKS5-style addressing lets the C2 reach any host the victim can see, turning the machine into a full network pivot. Because it all looks like ordinary encrypted web traffic to one site, the channel is hard to spot; while Microsoft did not observe data theft here, it warns that the same access typically leads to exfiltration and ransomware.

Recommendations

- **Restrict PowerShell and Run Dialog Execution:** Use AppLocker, Application Control for Windows, or Group Policy to limit PowerShell for standard users, and block or audit the Win+R Run dialog where it is not needed for daily work.
- **Warn on Multi-Line Terminal Pastes:** Configure Windows Terminal to warn users when pasted text spans multiple lines, since TerminalFix relies on users pasting a long script into the terminal without noticing what it does.
- **Hunt for LockScreenContentServer.exe Sideloading:** Alert whenever LockScreenContentServer.exe loads dui70.dll from any path other than C:\Windows\SystemApps, and run Microsoft's published hunting query to surface this activity across the estate.
- **Rotate Credentials on Affected Hosts:** Treat any host showing these indicators as a network pivot point and rotate every credential reachable from it, prioritizing domain admin accounts if the machine was domain-joined.
- **Enable PowerShell Script Block Logging:** Turn on script block logging to capture and analyze obfuscated or encoded commands, giving visibility into the disguised Cloudflare-themed script and the stages that follow it.
- **Train Users to Recognize ClickFix Lures:** Teach employees that no legitimate CAPTCHA ever asks them to paste a command into Terminal or the Run dialog, and give them a fast way to report such prompts.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1189: Drive-by Compromise	
Execution	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
	T1204: User Execution	T1204.002: Malicious File
Persistence	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
Defense Evasion	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
	T1027: Obfuscated Files or Information	T1027.003: Steganography
	T1564: Hide Artifacts	T1564.001: Hidden Files and Directories
	T1036: Masquerading	T1036.005: Match Legitimate Name or Location
Discovery	T1018: Remote System Discovery	
	T1069: Permission Groups Discovery	T1069.002: Domain Groups
	T1482: Domain Trust Discovery	

Tactic	Technique	Sub-technique
Discovery	T1087: Account Discovery	T1087.002: Domain Account
	T1082: System Information Discovery	
Command and Control	T1572: Protocol Tunneling	
	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1105: Ingress Tool Transfer	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	18c2090e8a0ae0568af9b87e59eaf8270f23d2909600ed9db91a9444fd8b278f, b8d107800403b9197e5b7609ceacd8e4cac1b0f9a1d156e6dacd6c3f7794b36a, ba77feed86bcda49308746421bdc684a432dd5d68c363975b2a3c6831bda3f07, 026478003fe354134c03acf6890e7d3b153ba08a836eca42350db48f213872ab, 032b529fac61e550f5dc9489686f519b82d64625fa05a8d9ecf8ba8be9b2ad22, df8221a933b38284ebdcb8bffc2df62123c9f5b5f421dd0b070e13e668b3eabf, eb1b4be34d05b394fb74efdeb95faecd1d1963be6ecc1b9db2b4757b491f01f0, 5d43abf5c36ea203176d3300ff14af27b4be81810ad2679b3a62b255e3d6e1c8, 9a7b4dcd51d9251c177d323d6aaecdfc86674f69bc1af048dc872926d22aaa24, 342df92235c9dec81203b837addaa38bb85b64b4a48fe71b5303ca86d991991e, edededeacf30e493dd632d477fe770ba419aa2848f685ea049381a0a8d2cc3e84d
Domains	gitnow[.]dev, bestsocialmedianewspapper[.]com, offlineupdater[.]com, linked-log[.]com

References

https://www.microsoft.com/en-us/security/blog/2026/08/28/terminalfix-campaign-deploys-reverse-tunnel-through-multistage-intrusion/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

August 31, 2026 • 09:00 AM

© 2026 All Rights are Reserved by Hive Pro

More at www.hivepro.com