baseVISION TI Report

Click, Paste and Compromise: When User's Trust Becomes Your Greatest Vulnerability

baseVISION

While the cyber threat landscape continues to evolve at an unprecedented pace, one constant remains: attackers' relentless focus on exploiting human behavior. One particularly insidious social engineering tactic has gained significant traction in recent years: ClickFix, a method that manipulates users into executing malicious commands through trusted interfaces.

Though the abuse of ClickFix tactics peaked in 2024, the concept traces back nearly a decade. This report provides a comprehensive examination of ClickFix and its recent variants, exploring its evolution from early tech support scams to more sophisticated forms. analyzing its operational mechanisms and offering recents IoCs for actionable defense strategies.

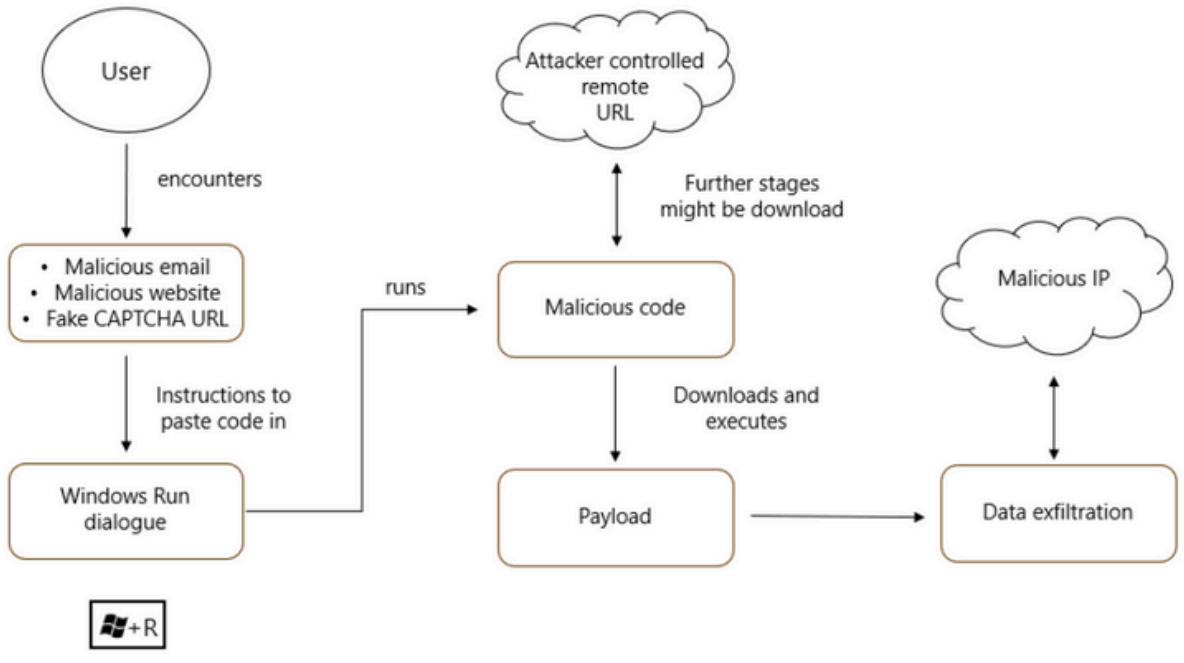
Understanding ClickFix: A "Not-So-New" Social Engineering Vector

ClickFix is a social engineering technique that deceives victims into manually executing harmful commands by exploiting their trust in familiar interfaces and common troubleshooting scenarios.

As the name suggests, the victim is often prompted to "fix a problem" with a system malfunction prompt, or prove they are "human" using fake CAPTCHA pages. These lures, appearing as simple fixes or benign tasks, are delivered via phishing emails, compromised websites or malvertising campaigns.

Victims are typically instructed to paste a pre-populated command (often obfuscated or base64-encoded) into the Windows Run dialog or a PowerShell terminal. Because these actions mimic routine system usage and don't trigger traditional red flags, less-savvy users may comply without suspicion.

Simplified ClickFix Attack Scenario

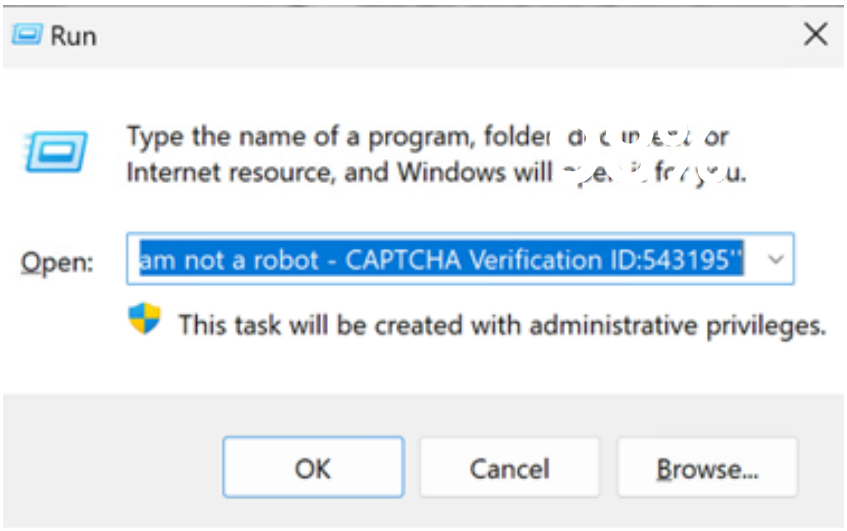


A wide range of payloads are delivered via ClickFix campaigns

- Lumma Stealer, Danabot, StealC, Vidar Stealer, NetSupport RAT, DarkGate and AsyncRAT have all been observed distributed through ClickFix attacks;
- Ransomware like Interlock (former Rhysida) has also surfaced within ClickFix scenarios, alongside post-exploitation frameworks including Havoc;

As an example, in one campaign deploying LummaStealer via ClickFix, attackers tricked users into opening the Windows Run dialog (Win + R) and pasting what appeared to be a benign "I am not a robot" verification. The prompt silently auto-copied a Base64-encoded PowerShell script to the clipboard. When users pressed Ctrl + V and Enter, it executed the hidden payload, first invoking the trusted Windows tool mshta to download a further secondary encoded script disguised as a legitimate file, and then deploying LummaStealer to exfiltrate credentials and system data.

Users are prompted to verify that "I am not a robot" by fulfilling these three verification steps



The user sees a "I am not a robot" verification in the run dialogue, and no malicious code is shown

How It All Started

Although ClickFix emerged as a recognized tactic in early 2024, its behavioral roots trace back nearly a decade to classic tech support scams. As early as 2016, attackers would contact victims via unsolicited phone calls posing as Microsoft or other trusted entities. Victims were commonly instructed to:

- Open the Windows Run dialog using Windows + R;
- Type or paste diagnostic commands such as eventvwr to reveal standard system logs (misrepresented as critical errors);
- Install remote access tools (RATs) like TeamViewer.

These early scams, which relied on live, voice-based social engineering, laid the foundation for today's clipboard-based attacks, which almost ten years later follow the same core principle: convincing the user to take a seemingly benign action that ultimately compromises their system. The difference today lies in scale and automation: modern ClickFix campaigns are executed entirely via web prompts, enabling attackers to reach thousands of victims at once, without the need for real-time interaction.

2024: the Golden Year for the Scam

The formalization of ClickFix as a named social engineering technique was first observed in widespread campaigns throughout 2024, documented by security vendors such as Proofpoint.

- In March 2024, a phishing campaign was conducted by TA571, a spam distributor threat actor delivering HTML attachment which were disguised as Microsoft Word documents. These documents displayed an error message, asking users to fix it by instructing them on copying and pasting base64-encoded PowerShell, leading to malware installation;
- In May 2024, the ClearFake cluster (unknown attribution) began compromising websites by injecting the ClickFix technique into fake-browser-alert pop-ups;
- Attackers diversified ClickFix delivery methods, such as fake CAPTCHA pages, and notably, fake Google Meet conference pages that mimicked microphone/headset error prompts. Clicking "Try Fix" deployed PowerShell code to install info-stealers (Rhadamanthys, AMOS) on Windows and macOS;
- By late 2024, the technique also appeared in state-sponsored campaigns: Kimsuky (North Korea), MuddyWater (Iran) and Russia-linked groups (APT28, UNK_RemoteRogue).

According to a report published by ESET regarding recent trends in the threat landscape, ClickFix usage surged by 517% between H2 2024 and H1 2025, becoming the second-most common initial access vector after phishing.

FileFix: The Next Evolution

Given the widespread success of ClickFix, the emergence of new variants was only a matter of time. One such variant is FileFix, which, as of July 2025, has only been demonstrated in proof-of-concept form by security researchers and has not yet been observed in-the-wild exploited by threat actors.

In June 2025, researcher mr.d0x introduced FileFix, showing how it abuses user trust in Windows File Explorer. The attack involves tricking users into pasting a malicious command, disguised as a file path, into the File Explorer address bar, triggering the execution of hidden PowerShell scripts without raising traditional security warnings.

FileFix attack flow:

- Visiting a fake "file shared" or upload prompt;
- Triggering a file-upload dialog to encourage interaction;
- Instructing the user to paste a fake path (actually a command) into the Windows File Explorer address bar.

FileFix exploits the familiarity and perceived safety of Windows File Explorer. Moreover, by avoiding traditional vectors like the Run dialog or web-based script downloads, it also bypasses Mark-of-the-Web (MOTW) restrictions and typical execution warnings, making detection significantly more challenging.

In a follow-up published in late June 2025, mr.d0x unveiled FileFix Part 2, further demonstrating how MOTW protections can be bypassed, this time with a different social engineering technique shifting from Explorer-based input to browser-based file handling. In fact, when a user saves a malicious HTML page (served as text/html) using the "Webpage, Complete" or "Single File" option and renames it to a .hta file as instructed, the resulting file executes with no MOTW warnings. By embedding script execution in the HTML, attackers can achieve code execution through simple social engineering and browser-native behavior. Like the original FileFix, this variant exploits users' trust in familiar interfaces, making detection harder and further blurring the line between user action and exploitation.

Conclusion

ClickFix and FileFix represent a significant evolution in social engineering. Attackers no longer need to directly bypass system defenses. Instead, they manipulate users into executing malicious commands themselves, often through trusted and familiar interface flows, converting users into insider threats.

The historical evolution of these tactics shows that they don't disappear: they evolve with the times, adopting new forms while preserving the same manipulation forms at their core. As defenders, we must keep pace and adapt as quickly, integrating threat intelligence, behavior-based detections and stricter endpoint controls into our security strategies.

What makes ClickFix and FileFix particularly dangerous is their accessibility: they target average users, with limited technical awareness and a tendency to rely on-screen prompts without questioning them. Their success lies not in technical sophistication, but in their ability to blend seamlessly into everyday interactions.

Proactive defense requires a layered approach, combining user training, endpoint hardening and real-time monitoring for indicators of compromise (IOCs). User awareness remains a critical element: employees should be regularly educated to never follow web-based instructions that involve copying and pasting commands into system interfaces like Run, PowerShell or File Explorer. Additionally, organizations should assess and limit which users require access to potentially risky features. Beyond awareness and access control, defenders must focus in behavioral detections, monitoring for anomalous use of system tools, clipboard manipulation and fake interface overlays. As a matter of fact, staying ahead of evolving threats like such requires a holistic approach, with human-aware security posture evolving as fast as the adversaries do.

Non-exhaustive list of Indicators of Compromise (IoCs) observed in recent campaigns, provided as a sample (to be completed)

ClickFix IOCs

188.34.195.44
27.102.138.169
193.36.38.237
103.149.98.247
34ff2f72c191434ce5f20ebc1a7e823794ac69bba9df70721829d66e7196b044
8daa6b20caf4bf384cc7912a73f243ce6e2f07a5cb3b3e95303db931c3fe339f

What you can do next

The findings in this report make one thing clear: users remain a prime target—and often the weakest link—in today's threat landscape. ClickFix and FileFix exploit trust, not technology. That's why your defense strategy must start with people.
Take action now:

- Educate your teams: Regularly train employees to recognize and resist social engineering tactics like ClickFix and FileFix.
- Review access policies: Limit the use of system tools like PowerShell and File Explorer to only those who truly need them.
- Implement behavior-based detection: Monitor for unusual clipboard activity, command execution, and fake interface overlays.

Need help getting started? Our team is here to support you with tailored awareness campaigns, technical assessments, and strategic guidance.
In case you have any questions or would like to discuss how to strengthen your organization's defenses, don't hesitate to reach out (info@baseVISION.ch)