halcyon | Ransomware Research Center

Clipboard to Encryption: The Critical Role of ClickFix in Ransomware Campaigns

Since March 2026, Halcyon has observed a surge across our customer networks in the use of a technique known as "ClickFix", with most activity occurring in the Americas. Dubbed by Proofpoint researchers in June 2024, ClickFix started as a social engineering campaign wherein webpages presented fake errors and prompted a victim to *click* (or take actions) to *fix* the fake problems. Today, ClickFix has transitioned from a single campaign to an overall technique adopted by initial access brokers (IABs), advanced persistent threat (APTs), and ransomware groups for initial access.

The Halcyon Ransomware Operations Center (ROC) detected the recent surge in ClickFix activity and notified Halcyon clients on over 10 pre-ransomware instances in March and April 2026. In all cases, ClickFix evaded all other security solutions except Halcyon, and the ROC was able to prevent ransomware deployment by Qilin, Termite, Interlock, and LeakNet. ROC notified each customer immediately, and customers implemented various additional domain blocks, such as malicious domains presenting ClickFix, and ensured there were no other infections in the respective environments.

Background

ClickFix is a social engineering attack technique that has become increasingly prevalent in cybersecurity threat landscapes since 2024. One cybersecurity firm reported that ClickFix usage skyrocketed by over 500% during the technique's first six months, becoming the second most common attack vector after phishing. Payloads vary widely from infostealers to ransomware and even nation-state malware.

Multiple threat actor groups from state-sponsored to financially motivated ransomware groups have adopted ClickFix. Notable users of ClickFix include: Kimsuky/TA427 (North Korea), MuddyWater (Iran), APT28 (Russia), UNK_RemoteRogue (Russia), Qilin, Interlock, Termite, and LeakNet. It has also been distributed via malvertising, search engine optimization (SEO) poisoning, and phishing emails.

The attack typically follows this pattern regardless of threat actor group:

1. A user visits a compromised or malicious website or opens a malicious document/email.
2. The user is presented with a fake error message, often mimicking something familiar such as a CAPTCHA, a Microsoft Word error, a browser update prompt, or a reCAPTCHA verification.

3. The fake prompt instructs the user to "fix" the problem by copying a command to their clipboard and pasting it into the Windows Run dialog (Win+R), PowerShell, or a terminal.
4. The command, which the user pastes and executes themselves, downloads and runs the malicious payload.

ClickFix is effective because:

- It bypasses many traditional endpoint security controls because the user is the one executing the command, not an automated process.
- It exploits trust where the fake user interface (UI) looks legitimate and the "fix" or "request for actions" seems reasonable.
- It sidesteps browser sandboxes, email attachment scanning, and traditional endpoint security that typically catch direct file downloads.
- It abuses built-in operating system tools (e.g., PowerShell, mshta, curl, rundll32.exe), so-called "living off the land" (LotL) techniques, making detection harder.

Common lures seen for ClickFix include:

- Fake browser update pages
- Fake CAPTCHA or "Verify you are human" prompts
- Fake Microsoft Office/Word document errors ("Enable editing to view content")
- Fake GitHub issues or error pages
- Fake Cloudflare DDoS protection screens
- Fake "Complete these Verification Steps"

ClickFix has been used to deliver a wide variety of payloads, including:

- Information Stealers (Infostealers) (e.g., Lumma Stealer, Vidar)
- Remote Access Trojans (RATs) (e.g., NetSupport RAT, CastleRAT)
- Ransomware (e.g., LeakNet, Qilin)
- Cryptocurrency miners
- Initial access for further attacks (e.g., Cobalt Strike beacons)

ClickFix primarily targets Windows; however, there are variants targeting macOS that use Terminal commands rather than Windows Run/Terminal/PowerShell.

Halcyon Ransomware Attack Chain

The Halcyon Anti-Ransomware Platform protects against the ClickFix campaign tools, which are used by Initial Access Brokers (IABs), Advanced Persistent Threats (APTs), and ransomware groups. For situational awareness, the following is an example infection chain if a user falls for ClickFix without protection:

Initial Access

Fake error messages, CAPTCHA prompts, or verification screens lure victims to open the Windows Run dialog (Win+R) or Terminal (Win+X → I) and execute a pre-loaded clipboard command. The malicious command is silently injected via JavaScript, bypassing browser download protections entirely as no file is directly downloaded. As of April 2026, this is automated via rundll32.exe, removing even the manual paste step.

Remote Access

C2 traffic is routed over HTTPS using Cloudflare Workers and CDN infrastructure to blend with normal web traffic. EtherHiding stores C2 configuration and payload URLs in Binance Smart Chain smart contracts, making infrastructure takedowns ineffective. Steam Community profile pages are used as dead-drop resolvers to retrieve C2 addresses. Remote Access Trojans (RATs) deployed include MIMICRAT/AstarionRAT, CastleRAT, QuasarRAT, and NetSupport RAT.

Environment Enumeration

Native Windows utilities (reg.exe, findstr.exe) enumerate installed security software and extract system identifiers including MachineGuid. Depending on the operator's objective, this reconnaissance phase informs the selection of follow-on payloads. Hardware specifications are profiled to optimize cryptocurrency miner yield and avoid resource thresholds that would trigger user or security team attention.

Credential Harvesting

Commodity infostealers are deployed as secondary payloads, including Lumma Stealer, Vidar, StealC, and AMOS (macOS-focused). Cobalt Strike beacons enable persistent hands-on-keyboard credential access. Loaders such as Matanbuchus 3.0, DonutLoader, and Latrodectus stage further harvesting tooling.

Lateral Movement

Cobalt Strike beacons, deployed via ClickFix-enabled initial access brokers, establish persistent footholds for hands-on-keyboard activity, lateral movement, and pre-ransomware reconnaissance across the victim environment.

Security Bypass

Living-off-the-land binaries (LOLBins) including curl.exe, mshta.exe, finger.exe, reg.exe, and findstr.exe blend into normal administrative activity. Payloads are injected directly into memory using the Deno runtime, leaving minimal on-disk forensic evidence. Windows Event Tracing (ETW) is patched and AMSI is disabled to blind endpoint detection before staging further payloads. JavaScript clipboard injection bypasses browser-based download protections entirely.

Data Exfiltration

Ransomware groups operating double-extortion campaigns (Interlock, Termite/Velvet Tempest, LeakNet, Qilin) exfiltrate victim data over encrypted C2 channels prior to encryption, using the stolen data as additional extortion leverage.

Data Encryption

Ransomware groups including Interlock, Termite (via Velvet Tempest/DEV-0504), LeakNet, and Qilin use ClickFix as the entry point for ransomware deployment. MachineGuid is used to bind encryption keys to individual victim machines, ensuring decryption is impossible without attacker cooperation even if the ransomware binary is captured.

Mitigations

- **Deploy Dedicated Anti-Ransomware Solution:** Deploy dedicated anti-ransomware defenses capable of detecting and stopping threats before encryption begins. Halcyon focuses on various detections based on the use of Windows Run dialog or rundll32 functions, WebDAV-enabled payload delivery, and in-memory execution of loaders. Given ClickFix's use of living-off-the-land binaries, solutions should additionally alert on anomalous execution of `curl.exe, mshta.exe, finger.exe, reg.exe,and csc.exe` when spawned from user-initiated processes or the Run dialog [M1038] [M1040].
- **User Awareness Training:** The user interview is both a root cause finding exercise and the natural entry point into this mitigation. User Awareness Training involves educating employees and contractors on recognizing, reporting, and preventing cyber threats that rely on human interaction by creating a human firewall and empowering users to be active components of the organization's cybersecurity defenses. The interview reveals how the user encountered the lure (search result, malvertising, links in documents or emails, fake CAPTCHA, or spoofed software update page) and informs what training gaps need to be addressed. Training should specifically reinforce that no legitimate website, CAPTCHA service, browser, or Windows Update process will ever instruct a user to paste commands into a Run dialog or terminal window [M1017].

- **Restricting PowerShell and the Run Dialog:** For non-admin users, this is very powerful as it reduces the attack vector to administrators for most ClickFix activity. Preventing non-admin users from running commands or launching via the Windows Run dialog (`Win+R`) significantly reduces the risk of a successful ClickFix execution. Organizations should enforce PowerShell Constrained Language Mode, apply Software Restriction Policies or AppLocker rules to block execution of `mshta.exe` and `wscript.exe` from user-writable directories, and use Group Policy Objects (GPOs) to disable or restrict clipboard-based execution pathways [M1026] [M1038].
- **Endpoint Detection and Behavioral Analytics:** Configure EDR solutions to alert on the specific behavioral chain associated with ClickFix: a user-interactive process (Run dialog or terminal) spawning `cmd.exe` or `powershell.exe`, followed by outbound connections and secondary payload staging. Monitor the `RunMRU` registry key, which stores a history of commands executed via the Run dialog and can confirm whether a ClickFix command was executed during incident response. Alert on anomalous DLL sideloading from `C:\ProgramData` and unexpected use of legitimate signed runtimes (e.g., Deno) to execute encoded JavaScript payloads in memory [M1049] [M1057].
- **Web Filtering and Malvertising Protection:** Deploy URL filtering and DNS security solutions to block access to known malicious domains and newly registered domains (under 90 days old), which are frequently used in ClickFix infrastructure. Organizations should additionally block or monitor traffic to dynamic DNS providers (e.g., FreeDNS, No-IP) and TryCloudflare tunnel endpoints, which have been widely abused as C2 relay infrastructure in ClickFix campaigns. Blocking malvertising at the network layer reduces the likelihood of users ever reaching a ClickFix lure page [M1021] [M1031].
- **macOS-Specific Controls:** ClickFix has increasingly targeted macOS users, pivoting from Terminal-based execution to abusing the applescript:// URL scheme to auto-open Script Editor and execute malicious AppleScript payloads, a technique that bypasses Apple's macOS 26.4 Terminal paste-scanning protections. Organizations managing macOS endpoints should deploy MDM policies to block execution of unsigned scripts, restrict the applescript:// URL scheme in browsers, monitor for outbound WebSocket connections from developer endpoints, and deploy behavioral detections tuned to AMOS Stealer patterns including bulk Keychain access and credential file reads [M1038] [M1042].

References

- ESET's H1 2025 Threat Report
- From Clipboard to Compromise: A PowerShell Self-Pwn
- I am not a robot: ClickFix used to deploy StealC and Qilin
- Interlock's ClickFix Trick: One Click, Total Data Compromise

- LeakNet ransomware uses ClickFix, Deno runtime in stealthy attacks
- Termite ransomware breaches linked to ClickFix CastleRAT attacks
- The ClickFix Evolution: New Variant Replaces PowerShell with Rundll32 and WebDAV

Source Summary

This research is based on Halcyon observations, open-source information, and ongoing research. Findings reflect our current understanding of threat actor activity and may be updated as new evidence emerges. Assessments may be revised as additional evidence becomes available.

The Halcyon Ransomware Research Center unites experts, drives smart policies, and delivers actionable intelligence to detect, disrupt, and defeat ransomware. Explore the Center's latest reports, analysis, and resources *here*.