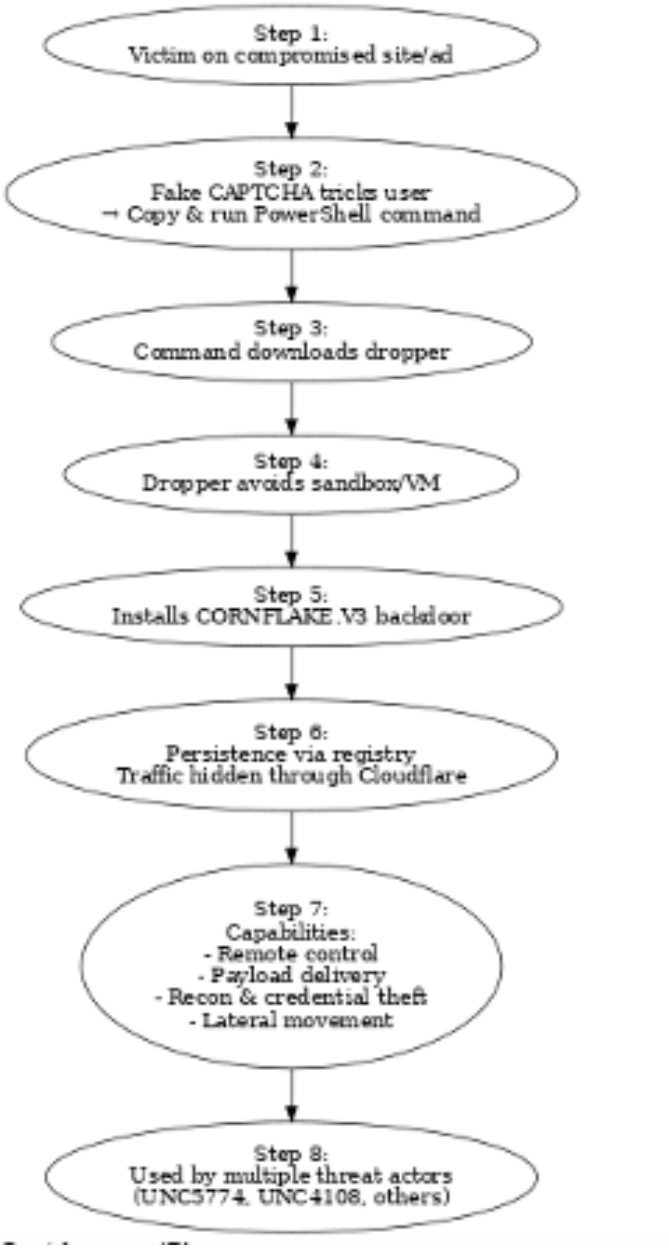

# Criminal Tactic CLICKFIX and Fake CAPTCHA pages to deploy CORNFLAKE V3 Backdoor

August 22, 2025

**Over the past year, cyber threat actors have refined their focus on low-cost, high-impact techniques that rely on human error and physical media. Instead of exploiting complex software flaws, they turn to tactics that convince users to run malicious commands or unknowingly spread infections through removable devices. Two major campaigns illustrate this trend. The first, known as ClickFix, leverages fake verification pages and social engineering to trick victims into installing a persistent backdoor called CORNFLAKE.V3. The second uses infected USB drives to deliver multi-stage payloads that culminate in the deployment of cryptocurrency miners. Both methods show how attackers bypass automated defenses, monetize access, and expand control across networks.**

**ClickFix: Social Engineering as Initial Access**

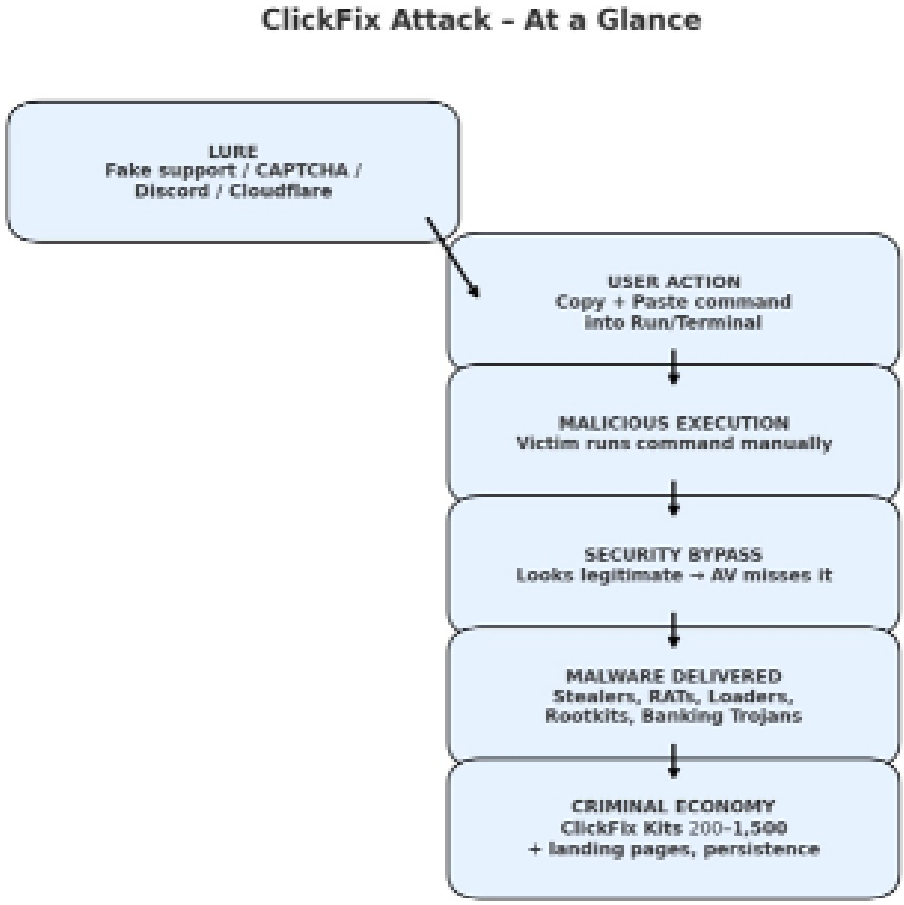
Threat actors have increasingly shifted toward low-cost, high-impact infection vectors that rely on social engineering and physical media, blending persistence, obfuscation, and commoditization in ways that bypass traditional security controls. One example is the ClickFix tactic, a deceptively simple but highly effective method that tricks users into launching malicious commands themselves. The attack often starts with a fake CAPTCHA page hosted on a compromised website or delivered through poisoned search results and malicious ads. Victims are told to copy and run a PowerShell command through the Windows Run dialog, or on macOS through the Terminal, under the pretext of verifying identity or solving a minor technical issue. Once executed, the command pulls a dropper script from a remote server, which checks for signs of virtualization before delivering CORNFLAKE.V3, a backdoor with broad functionality. CORNFLAKE.V3 can download and execute multiple payload types, gather system data, establish persistence via registry Run keys, and proxy its traffic through Cloudflare tunnels to evade detection.



**Commoditization of ClickFix: A Service Economy for Access**

The popularity of ClickFix has grown rapidly because of its flexibility and its ability to evade security tools. Threat actors have broadened the lures: fake Cloudflare Turnstile pages, Discord server verifications, even supposed technical fixes. In each case, the victim is manipulated into copying and running commands in Windows PowerShell, Windows Terminal, or macOS Terminal. Because the action is initiated by the user rather than an automated exploit, traditional defenses often do not flag the behavior. Microsoft notes that this is why ClickFix consistently slips past automated detection. It is distributed through common channels—phishing, malvertising, drive-by compromises—while impersonating legitimate brands to reduce suspicion. Once the foothold is established, a wide range of malware families can be delivered: information stealers like Lumma, RATs including Xworm, AsyncRAT, NetSupport RAT, and SectopRAT, loaders such as Latrodectus and MintsLoader, rootkits like r77, and banking trojans including Lampion.

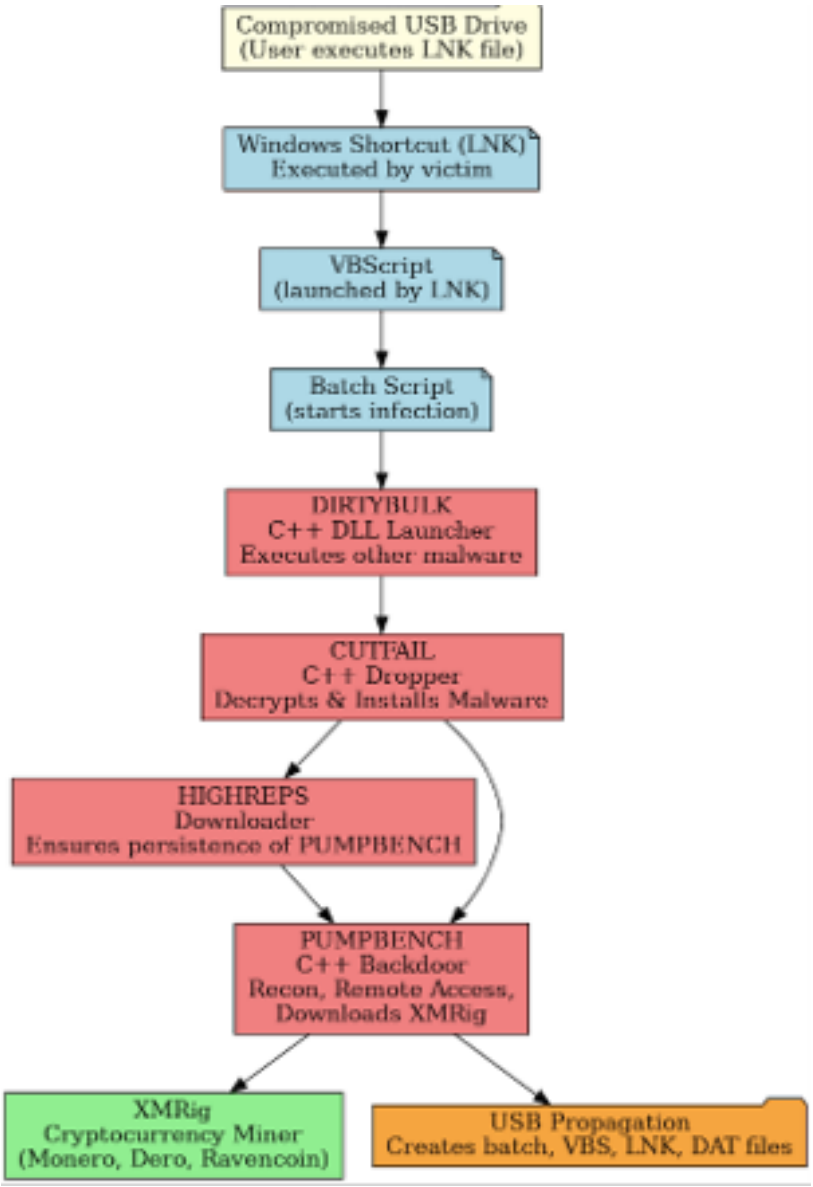
The rise of an underground market for ClickFix tools shows how this technique has become industrialized. Since late 2024, configurable “Win + R” builders have been sold on cybercrime forums for $200 to $1,500 per month. Cheaper one-time purchases exist for $200 to $500, covering things like source code, landing pages, or even the exact command line needed to kick off infection. Sellers bundle these builders with existing kits that generate LNK, JavaScript, or SVG malware files, offering pre-made landing pages with Cloudflare-themed lures and malicious commands ready to paste into Windows Run. Some even advertise antivirus and SmartScreen bypasses and claim to guarantee persistence of payloads. This commercialization lowers the entry barrier for less skilled actors and increases the number of campaigns leveraging the tactic.




**USB Infections: Old Vectors, New Payloads**

Parallel to this, physical vectors like USB drives remain a persistent threat, demonstrating that traditional methods of spreading malware continue to succeed when carefully integrated into multi-stage toolchains. Since September 2024, Mandiant has tracked a campaign using infected USB drives to spread cryptocurrency miners. The attack begins when the victim clicks on a malicious shortcut (LNK file) on the compromised USB. That shortcut executes a Visual Basic script, which in turn launches a batch file that sets off the infection chain. At the core is DIRTYBULK, a DLL launcher written in C++, which loads other components such as CUTFAIL, a dropper designed to decrypt and install malware. CUTFAIL then delivers HIGHREPS, a downloader that maintains persistence of subsequent payloads, and PUMPBENCH, a backdoor written in C++. PUMPBENCH enables reconnaissance, communicates with a PostgreSQL server for remote access, and downloads the XMRig miner. XMRig itself is open-source and used to mine Monero, Dero, and Ravencoin.

PUMPBENCH also functions as the propagation mechanism. It scans the system for any connected USB drives and replicates itself by creating a batch script, a VBScript, a shortcut file, and a DAT file, ensuring the infection spreads every time the drive is plugged into another machine. This campaign highlights the enduring value of USB as an infection vector: it bypasses network-based protections, requires little cost, and exploits human behavior in environments where removable media is common.




- 🟨 **Infection vector (USB + scripts)**
- 🟥 **Malware components**
- 🟩 **Cryptominer (XMRig)**
- 🟧 **Propagation mechanism**

**Conclusion**

650Taken together, these operations illustrate a broader trend in attacker tradecraft: exploiting human trust and behavior to launch malicious code, monetizing access by reselling or re-using it across multiple groups, and using modular toolchains that combine persistence, obfuscation, and payload flexibility. Whether through the sleek social engineering of ClickFix or the tried-and-tested simplicity of infected USB drives, threat actors continue to rely on the weakest link—the user—to achieve initial access and establish long-term control.