Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

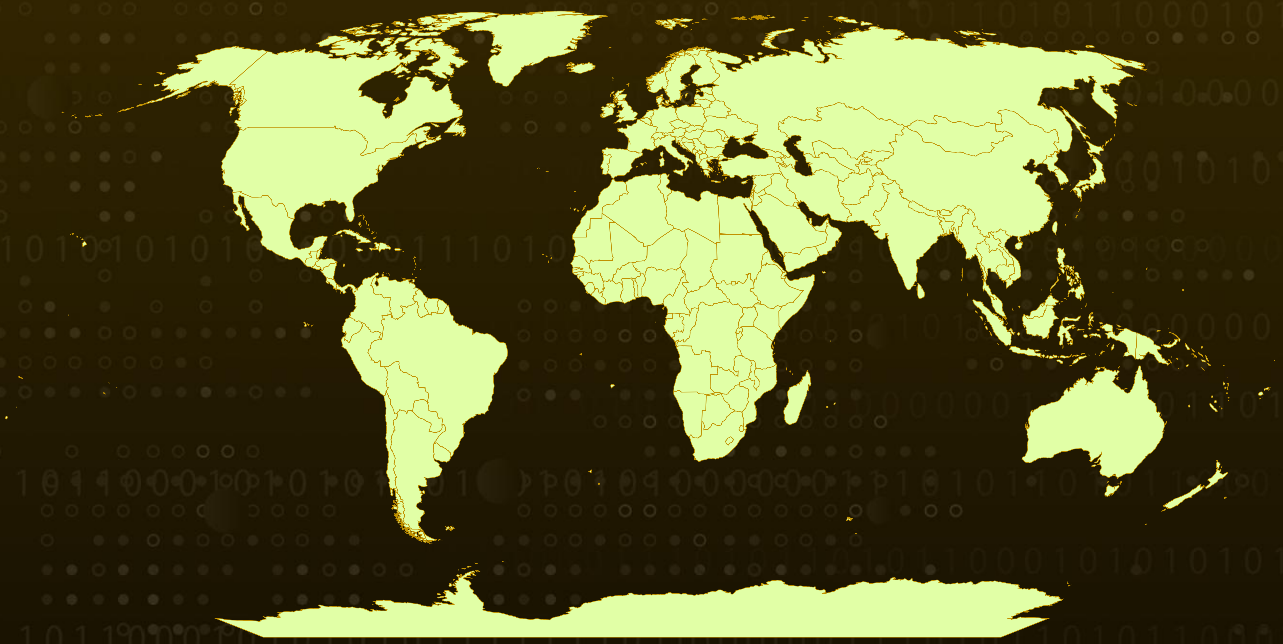
ClearFake: Blockchain-Powered Malware Lures Thousands with Fake Security Prompts

Date of Publication	Admiralty Code	TA Number
March 20, 2025	A1	TA2025087

Summary

Attack Discovered: July 2023
Targeted Countries: Worldwide
Affected Platforms: Windows and Mac
Malware: ClearFake, Emmenhtal Loader, Lumma Stealer, Vidar Stealer
Attack: ClearFake, a malicious JavaScript framework, continues to evolve, using fake reCAPTCHA and Cloudflare Turnstile verifications to lure users into downloading malware. Initially tricking victims with fake browser updates in 2023, it later adopted the ClickFix tactic, displaying deceptive error messages to convince users to execute malicious PowerShell commands. The latest variant now integrates with the Binance Smart Chain, a blockchain network, leveraging smart contract Application Binary Interfaces (ABIs) to load JavaScript, fingerprint victims' systems, and execute its payload.

Attack Regions



Powered by Bing

© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, Overture Maps Fundation, TomTom, Zenrin

Attack Details

#1 ClearFake is an evolving JavaScript-based malware framework that uses drive-by downloads to infect victims. First detected in July 2023, it quickly adopted a deceptive technique called ClickFix, which displayed fake error messages to trick users into downloading malicious PowerShell scripts.

#2 By December 2024, ClearFake introduced a more sophisticated approach, leveraging fake reCAPTCHA and Cloudflare Turnstile verifications to convince victims they needed to resolve a technical issue. This latest variant interacts with the Binance Smart Chain (BSC), dynamically retrieving JavaScript code to fingerprint victims' systems before launching an attack.

#3 In its early stages, ClearFake delivered fake browser updates to distribute malware. By October 2023, it had evolved to incorporate EtherHiding, a technique that stored obfuscated JavaScript within smart contracts on the Binance Smart Chain.

#4 A major update in December 2024 expanded ClearFake's Web3 capabilities, enhancing persistence. The ClickFix HTML code was encrypted and hosted on Cloudflare Pages, while its JavaScript execution chain leveraged smart contracts to fetch and execute obfuscated code dynamically. The malware also introduced an improved fingerprinting mechanism, collecting system details via User-Agent values to refine its targeting.

#5 By early 2025, ClearFake's ClickFix lures had evolved into highly convincing fake security challenges. Victims were presented with either a Cloudflare Turnstile verification or a reCAPTCHA prompt. If they attempted to solve the fake challenge, a malicious PowerShell command was automatically copied to their clipboard, infecting their system upon execution. These scripts, distributed via BscScan9 and monitored Ethereum addresses, deployed Vidar Stealer, Lumma Stealer, and Emmental Loader. With an estimated 200,000 unique users exposed, ClearFake remains a persistent and widespread threat, reinforcing the need for continuous monitoring and mitigation efforts.

Recommendations

Blocking Malicious Execution: Prevent unauthorized script execution by blocking JavaScript on untrusted websites through web content filtering, reducing the risk of malicious injections. Additionally, enforce Group Policy restrictions to allow only signed PowerShell scripts, mitigating the threat of unauthorized command execution.

Detecting Suspicious Blockchain Activity: Monitor network traffic for unusual interactions with Binance Smart Chain and Ethereum-based APIs, as these connections could signal attempts to retrieve malicious scripts or execute unauthorized transactions.

User Awareness: Educate employees on identifying fake security alerts, deceptive reCAPTCHA prompts, and misleading pop-ups designed to trick users into downloading malware. Regular training can help prevent accidental infections and enhance overall cybersecurity awareness.

Enhance Endpoint Protection: Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0005 Defense Evasion	TA0007 Discovery
TA0010 Exfiltration	TA0011 Command and Control	TA0040 Impact	T1189 Drive-by Compromise
T1566 Phishing	T1059 Command and Scripting Interpreter	T1059.001 PowerShell	T1059.007 JavaScript
T1078 Valid Accounts	T1027 Obfuscated Files or Information	T1071 Application Layer Protocol	T1486 Data Encrypted for Impact
T1132 Data Encoding	T1132.001 Standard Encoding	T1218 System Binary Proxy Execution	T1218.005 Mshta

T1140 Deobfuscate/Decode Files or Information	T1217 Browser Information Discovery	T1041 Exfiltration Over C2 Channel

Indicators of Compromise (IOCs)

TYPE	VALUE
URLs	hxxps[:]//ert67-o9.pages[.]dev/data, hxxps[:]//f003[.]backblazeb2[.]com/file/skippp/uu[.]html, hxxps[:]//f003[.]backblazeb2[.]com/file/skippp/index[.]html, hxxps[:]//hostme[.]pages[.]dev/host, hxxps[:]//ghost-name[.]pages[.]dev/website, hxxps[:]//gdfg-23rwe[.]pages[.]dev/index[.]html, hxxps[:]//sha-11x[.]pages[.]dev/, hxxps[:]//b1-c1-k8[.]pages[.]dev/, hxxps[:]//1a-a1[.]pages[.]dev/, hxxps[:]//sdfwefwg[.]pages[.]dev/, hxxps[:]//niopg[.]pages[.]dev/, hxxps[:]//sdfwefwg[.]pages[.]dev/, hxxps[:]//cleaning-devices-k[.]pages[.]dev/, hxxps[:]//tour-agency-media[.]pages[.]dev/, hxxps[:]//fresh-orange-juice[.]pages[.]dev/, hxxps[:]//you-insk-bad[.]pages[.]dev/, hxxps[:]//human-verify-7u[.]pages[.]dev/, hxxps[:]//recaptcha-verify-me-1c[.]pages[.]dev/, hxxps[:]//macos-browser-update-9n[.]pages[.]dev/, hxxps[:]//macos-browser-update-5i[.]pages[.]dev/, hxxps[:]//recaptcha-verify-2e[.]pages[.]dev/, hxxps[:]//recaptcha-verify-7z[.]pages[.]dev/, hxxps[:]//recaptcha-verify-1t[.]pages[.]dev/, hxxps[:]//recaptcha-verify-9m[.]pages[.]dev/, hxxps[:]//disable-data-collect-ai[.]pages[.]dev/, hxxps[:]//recaptcha-verify-1r[.]pages[.]dev/, hxxps[:]//recaptha-verify-5q[.]pages[.]dev/, hxxps[:]//note1[.]nz7bn[.]pro/nnp[.]mp4, hxxps[:]//ai[.]fdswgw[.]shop/one[.]mp4, hxxps[:]//mnjk-jk[.]bsdfg-zmp-q-n[.]shop/1[.]mp4, hxxps[:]//nbhg-v[.]iuksdfb-f[.]shop/ajax[.]mp3, hxxps[:]//hur[.]bweqlkjr[.]shop/m41[.]mp4, hxxps[:]//hur[.]bweqlkjr[.]shop/1a[.]m4a, hxxps[:]//yob[.]yrwebsdf[.]shop/1a[.]m4a, hxxps[:]//yob[.]yrwebsdf[.]shop/3t[.]mp4, hxxps[:]//start[.]cleaning-room-device[.]shop/sha589[.]m4a,

TYPE	VALUE
URLs	hxxps[:]//discover-travel-agency[.]pro/joke[.]m4a, hxxps[:]//discover-travel-agency[.]pro/walking[.]mp3, hxxps[:]//discover-travel-agency[.]pro/1[.]m4a, hxxps[:]//travel[.]image-gene-saver[.]it[.]com/1[.]m4a, hxxps[:]//ads[.]green-pickle-jo[.]shop/1[.]m4a, hxxps[:]//recaptcha-verify-4h[.]pro/kangarooing[.]m4a, hxxps[:]//recaptcha-manual[.]shop/kangarooing[.]m4a, hxxps[:]//recaptcha-verify-4h[.]pro/xfiles/kangarooing[.]vsdx, hxxps[:]//recaptcha-verify-4h[.]pro/xfiles/verify[.]mp4, hxxps[:]//human-verify[.]shop/xfiles/verify[.]mp4, hxxps[:]//human-verify-4r[.]pro/xfiles/verify[.]mp4, hxxps[:]//human-verify-4r[.]pro/xfiles/human[.]cpp, hxxps[:]//dns-verify-me[.]pro/xfiles/train[.]mp4, hxxp[:]//83[.]217[.]208[.]130/xfiles/Ohio[.]mp4, hxxp[:]//83[.]217[.]208[.]130/xfiles/VIDA[.]mp3, hxxp[:]//83[.]217[.]208[.]130/xfiles/VIDA[.]mp4, hxxp[:]//83[.]217[.]208[.]130/xfiles/trip[.]mp4, hxxp[:]//83[.]217[.]208[.]130/xfiles/trip[.]psd, hxxp[:]//80[.]64[.]30[.]238/trip[.]psd, hxxp[:]//80[.]64[.]30[.]238/evix[.]xll, hxxps[:]//raw[.]githubusercontent[.]com/fuad686337/tyu/refs/heads/main/BEGIMOT[.]xll, hxxps[:]//domain[.]com/BEGIMOT[.]xll, hxxps[:]//disable-data-ai-agent[.]pages[.]dev, hxxps[:]//tumbl[.]design-x[.]xyz/glass[.]mp3, hxxps[:]//f003[.]backblazeb2[.]com/file/skippp/glass[.]mp3, hxxps[:]//sandbox[.]yunqof[.]shop/macan[.]mp3, hxxps[:]//microsoft-dns-reload-1r[.]pages[.]dev, hxxps[:]//microsoft-dns-reload-5q[.]pages[.]dev

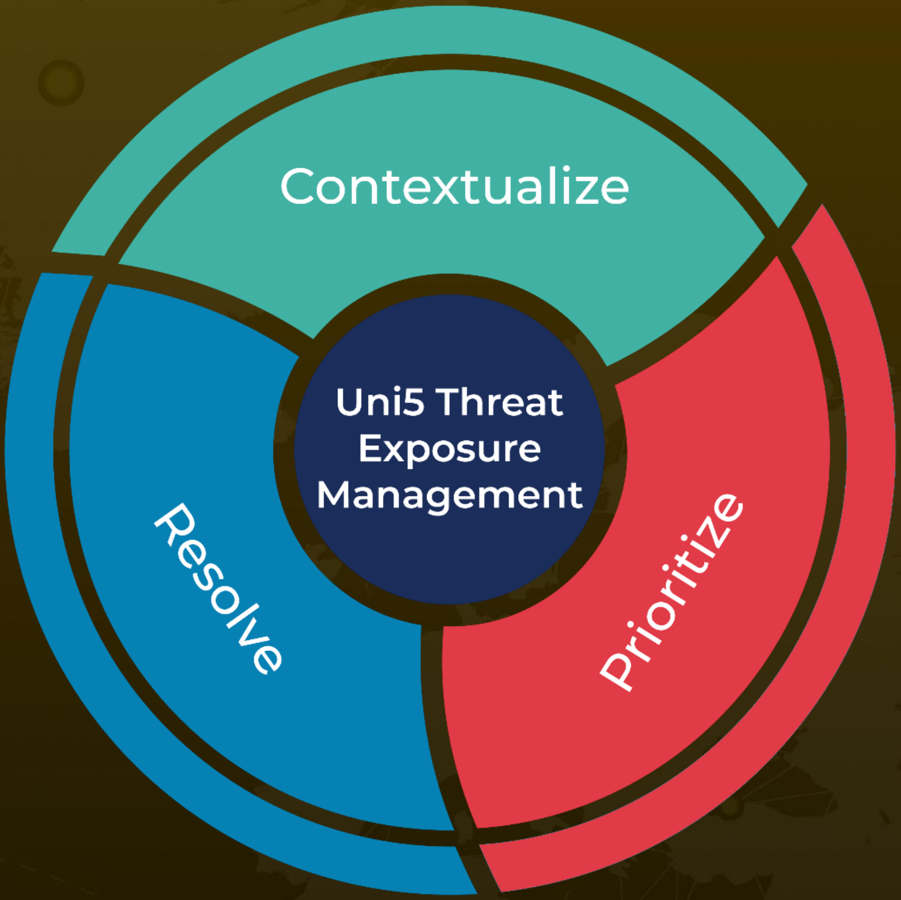
References

https://blog.sekoia.io/clearfakes-new-widespread-variant-increased-web3-exploitation-for-malware-delivery/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

March 20, 2025 • 5:20 AM

More at www.hivepro.com