

Forum:[Hack Forums](#)

Thread: [New ClearFake Variant Uses Fake reCAPTCHA and Deploy Malicious PowerShell Code](#)

JoseMar - March 20, 2025, 3:05 am

New ClearFake Variant Uses Fake reCAPTCHA to Deceive Users and Deploy Malicious PowerShell Code

ClearFake, a noxious JavaScript system recognized in July 2023, has advanced with advanced unused social building tactics.

Originally planned to show fake browser overhaul pages, the system has experienced critical improvements, joining more progressed duplicity procedures to convey malware through compromised websites.

The most recent variation, found in December 2024, utilizes fake reCAPTCHA or Cloudflare Gate confirmation challenges to trap clients into executing noxious PowerShell code.

This speaks to a critical advancement from prior forms that depended on fake browser updates.

Sekoia examiners found that this unused variation utilizes the “EtherHiding” strategy but has presented extra intelligence with the Binance Shrewd Chain.

The system sends different JavaScript codes and assets that uniquely finger impression victims’ frameworks, which have recently been downloading, decoding, and showing beguiling lures.

When clients visit a compromised site, they experience a starting script that loads Web3 libraries and starts communication with the Binance Shrewd Chain.

The pernicious code is concealed inside keen contracts, making the investigation more troublesome and expulsion incomprehensible due to the unchanging nature of blockchain data.

Installation stream

The disease stream starts with infused JavaScript on compromised websites, which recovers noxious code from blockchain-savvy contracts, eventually driving the show of fake security challenges.

Attack Analysis

The assault begins with a brief JavaScript code infused into compromised websites (generally WordPress destinations), which loads genuine conditions like web3, pako, and crypto-js.

This beginning script interatomic with shrewd contracts at wallet addresses like 0x9179dda8B285040Bf381AABb8a1f4a1b8c37Ed53 to recover and execute extra code segments.

The malware employs compressed and base64-encoded information that must have been unscrambled in recent execution.

The ClickFix draws displayed to clients incorporate a fake Cloudflare Entryway confirmation that claims to distinguish “unusual web traffic” or a fake reCAPTCHA challenge near a DNS mistake message.

Both draw educated clients to open the Run command (Win+R) and execute a PowerShell command naturally replicated to their clipboard.

ClickFix baits utilized

The fake reCAPTCHA asks clients to select pictures of cars, whereas the fake Cloudflare Entryway presents clients with a confirmation challenge, eventually driving them to social building attempts.

The PowerShell commands execute mshta.exe with scripts that provide payloads counting Emmenhtal Loader and eventually Lumma Stealer or Vidar Stealer.

Sekoia analysts are famous for the ClearFake framework, which incorporates over 9,300 compromised websites, with thousands of clients possibly uncovered to these malevolent draws daily.

Utilizing blockchain innovation for malware conveyance speaks to a rising risk that makes conventional relief and blocking more challenging.

Don't forget to update and stay safe!?

Additional sources to explore: You can also search directly by CVE on Google for more information:
<https://blog.sekoia.io/clearfakes-new-widespread-variant-increased-web3-exploitation-for-malware-delivery/>
<https://thehackernews.com/2025/03/clearfake-infests-9300-sites-uses-fake.html>
<https://cyberpress.org/clearfake-variant-exploits-fake-recaptcha/>

Bastille - March 20, 2025, 3:36 am

Didn't know the ClearFake framework and this technique, thanks for the share [JoseMar](#) , your threads are really useful and improve our knowledge everyday ?

JoseMar - March 20, 2025, 3:41 am

(Mar 20, 2025 03:36 AM)Bastille Wrote: [\[CITE\]](#) Didn't know the ClearFake framework and this technique, thanks for the share [JoseMar](#) , your threads are really useful and improve our knowledge everyday ?

The truth is, this comment truly makes me happy, especially coming from you. Really appreciate it, mate!?

DramaKing - March 20, 2025, 4:43 am

The DNS error and fox is a nice touch. I remember a HF member sending me a link to a fake CAPTCHA that required downloading and executing a RAT stager in Command Prompt.

0x503cad - April 5, 2025, 12:35 pm

(Mar 20, 2025 04:43 AM)DramaKing Wrote: [\[CITE\]](#) The DNS error and fox is a nice touch. I remember a HF member sending me a link to a fake CAPTCHA that required downloading and executing a RAT stager in Command Prompt.

Lol, it's a recent trend

alexvenutelli7 - September 9, 2025, 12:11 am

I am interested in purchase this, can anyone help me ?

Andy Walker - September 10, 2025, 8:28 pm

Thanks for this. I'm going to have to study more about this clear fake system. Your breakdown gives me a good idea of how it works.

ScarT0k3n - *September 11, 2025, 7:06 am*

Lmao thanks for this