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

- DECTECTION
- 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

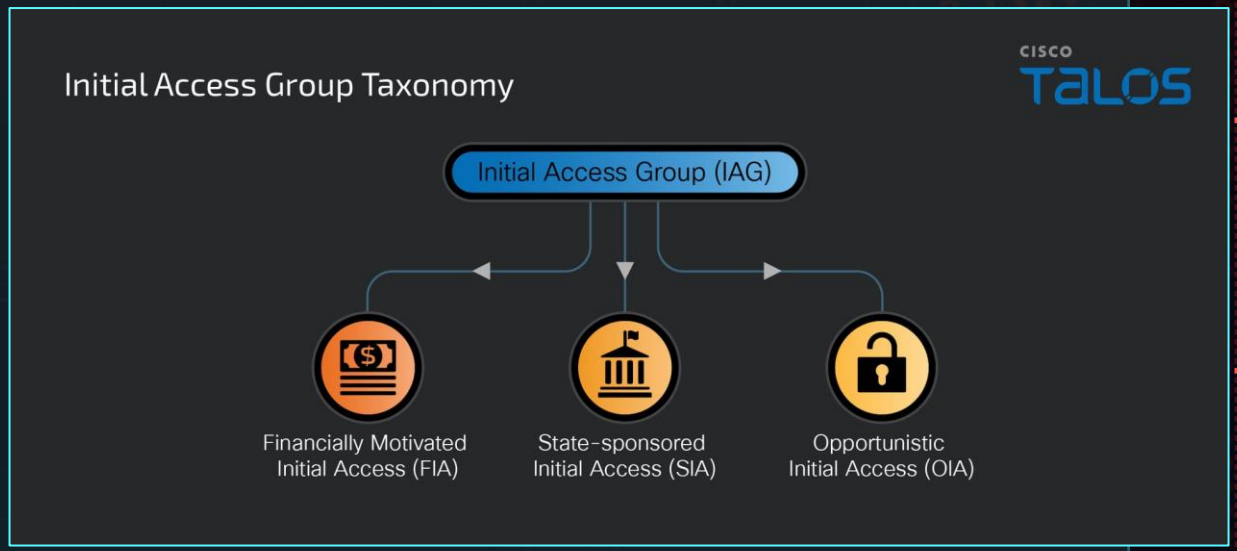
- (T1566) Phishing
- (T1189) Drive-by Downloads
- (T1133) Exposed RDP
- (T1190) Exploiting Public-Facing Applications

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



ANALYSIS CLICK FIX

OVERVIEW
STATICS
ANALYSIS
CLICK FIX IN THE WILD

CLICK FIX - OVERVIEW

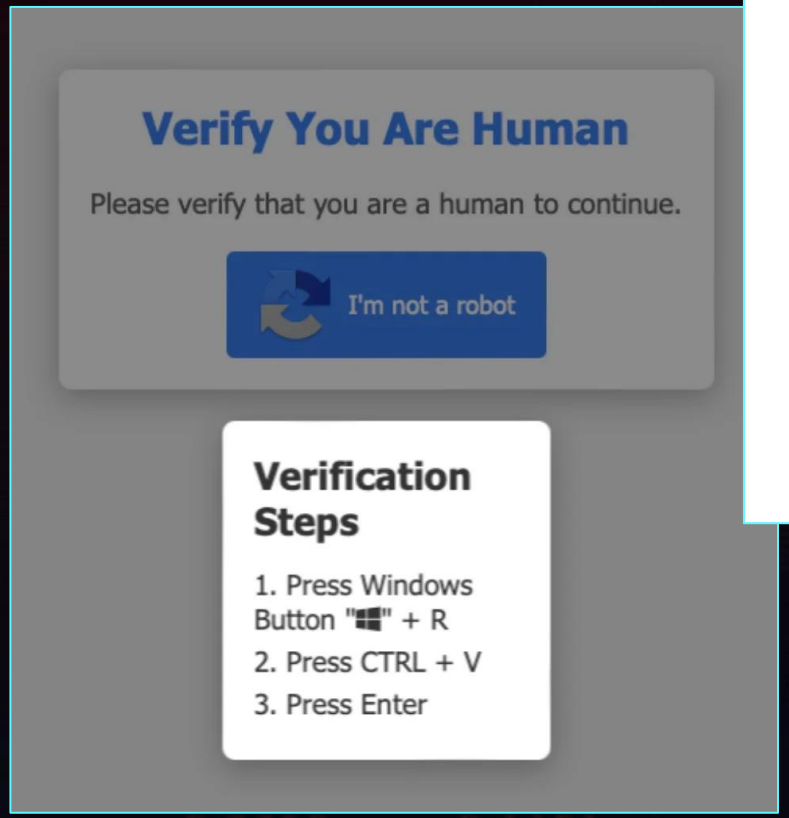
- ClickFix is an **emerging social engineering** tactic
- First identified by Proofpoint in 03/2024
- Emerged and become one of the fastest rising and most effective threats in H2-2024 & H1-2025

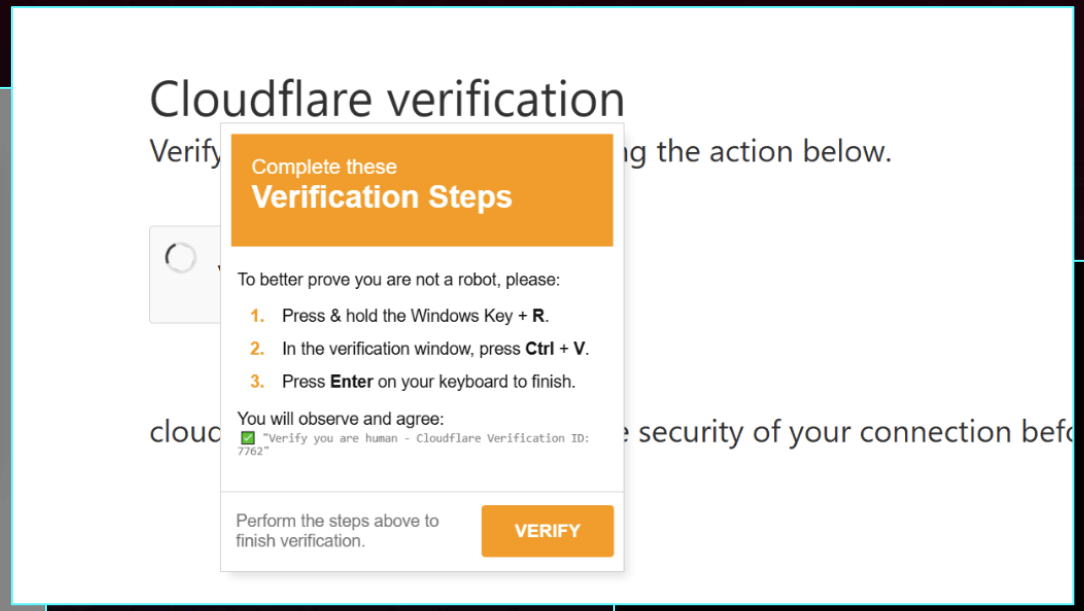
CLICK FIX - OVERVIEW

- 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**!

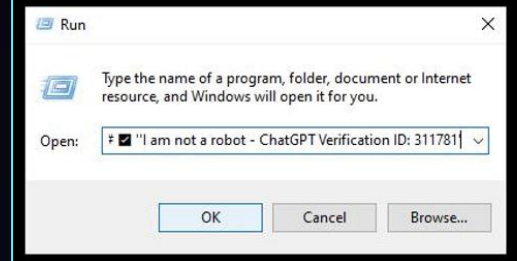
- Once executed, the adversary will typically be able to establish a foothold on the victim's machine.

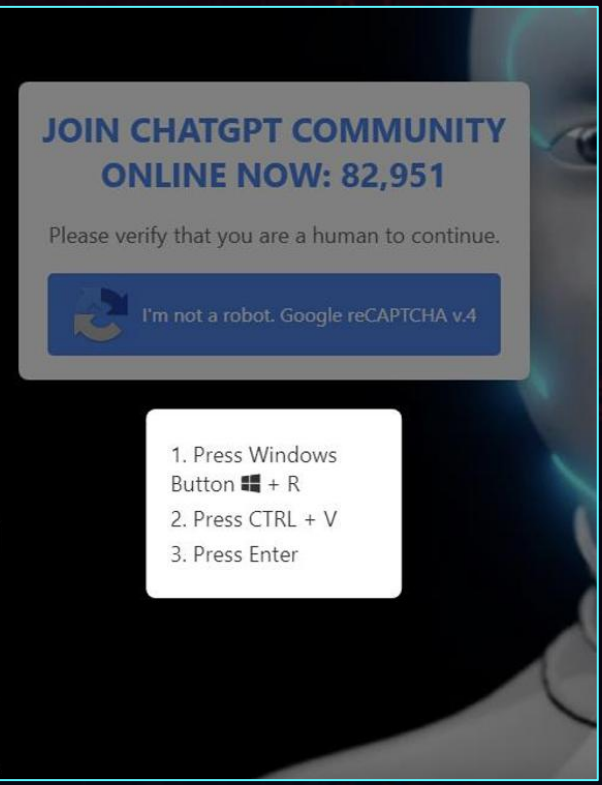
CLICK FIX - OVERVIEW



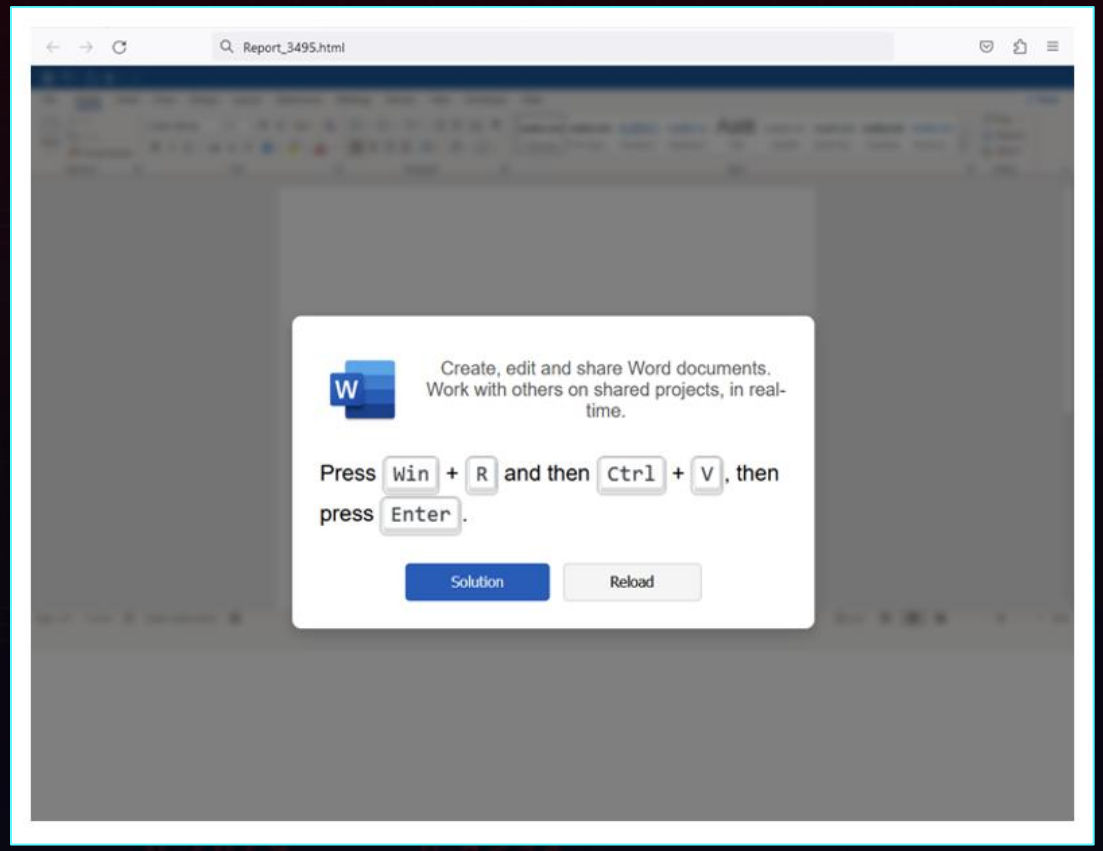


Fake captcha

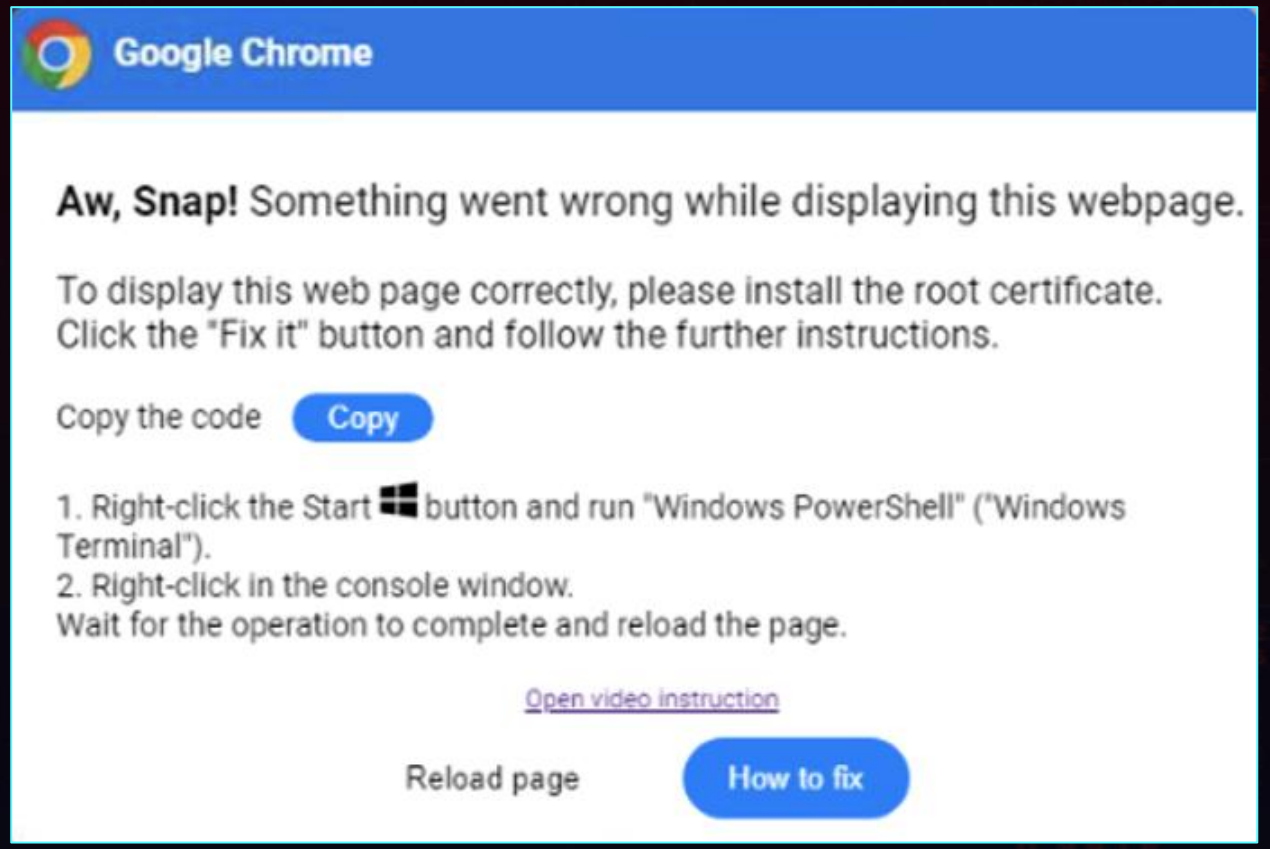




CLICK FIX - OVERVIEW



Fake Word error



Fake Browser error

CLICK FIX - STATICS

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

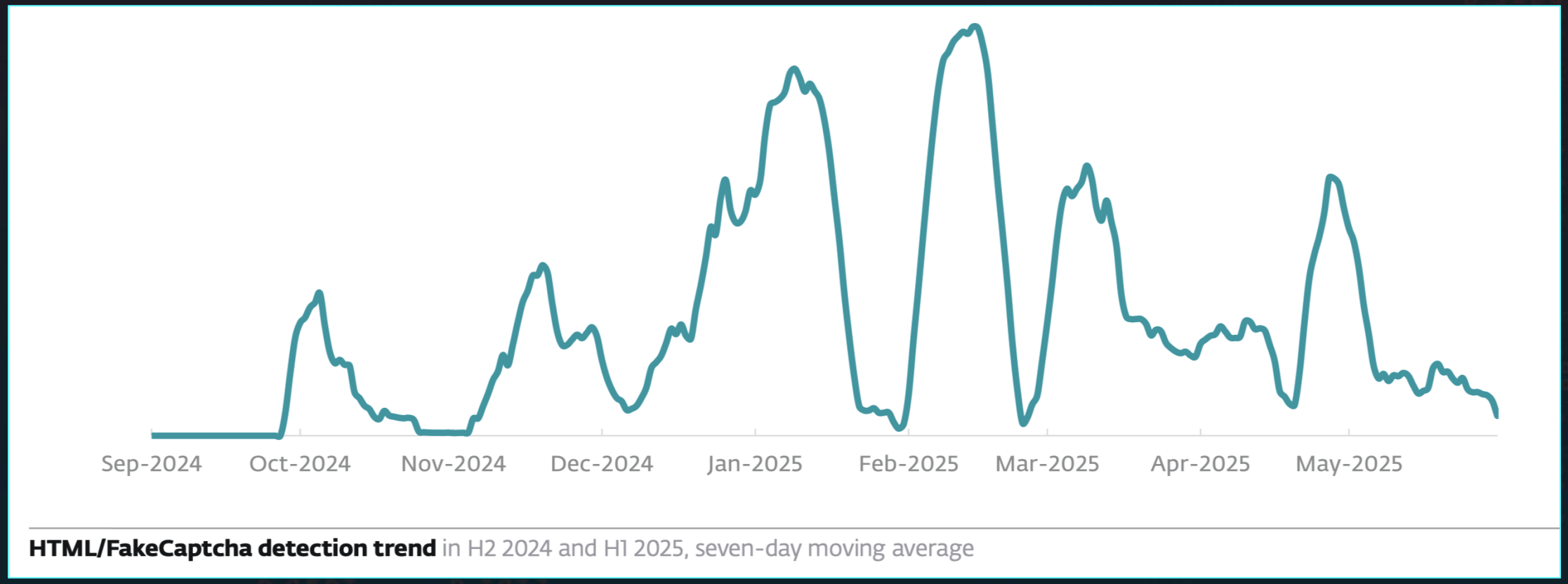
https://redcanary.com/threat-detection-report/trends/initial-access/

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



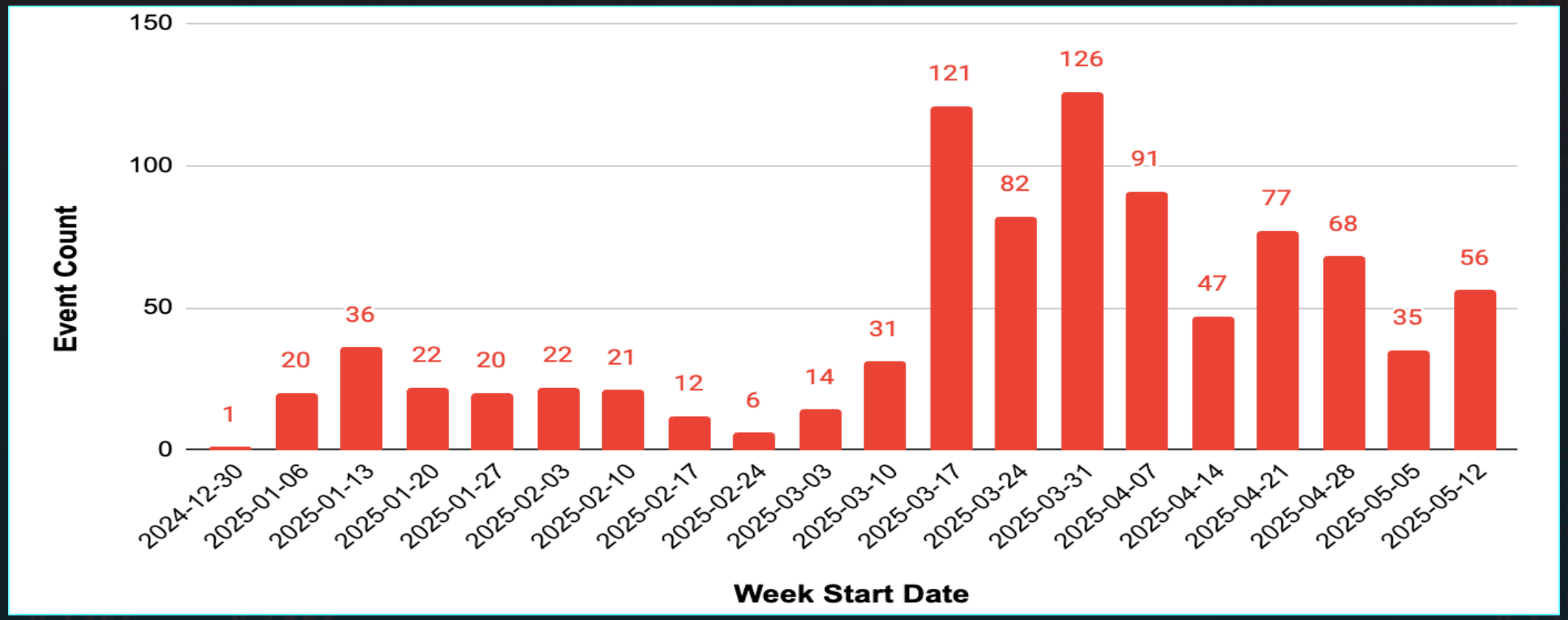
HTML/FakeCaptcha detection trend in H2 2024 and H1 2025, seven-day moving average

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



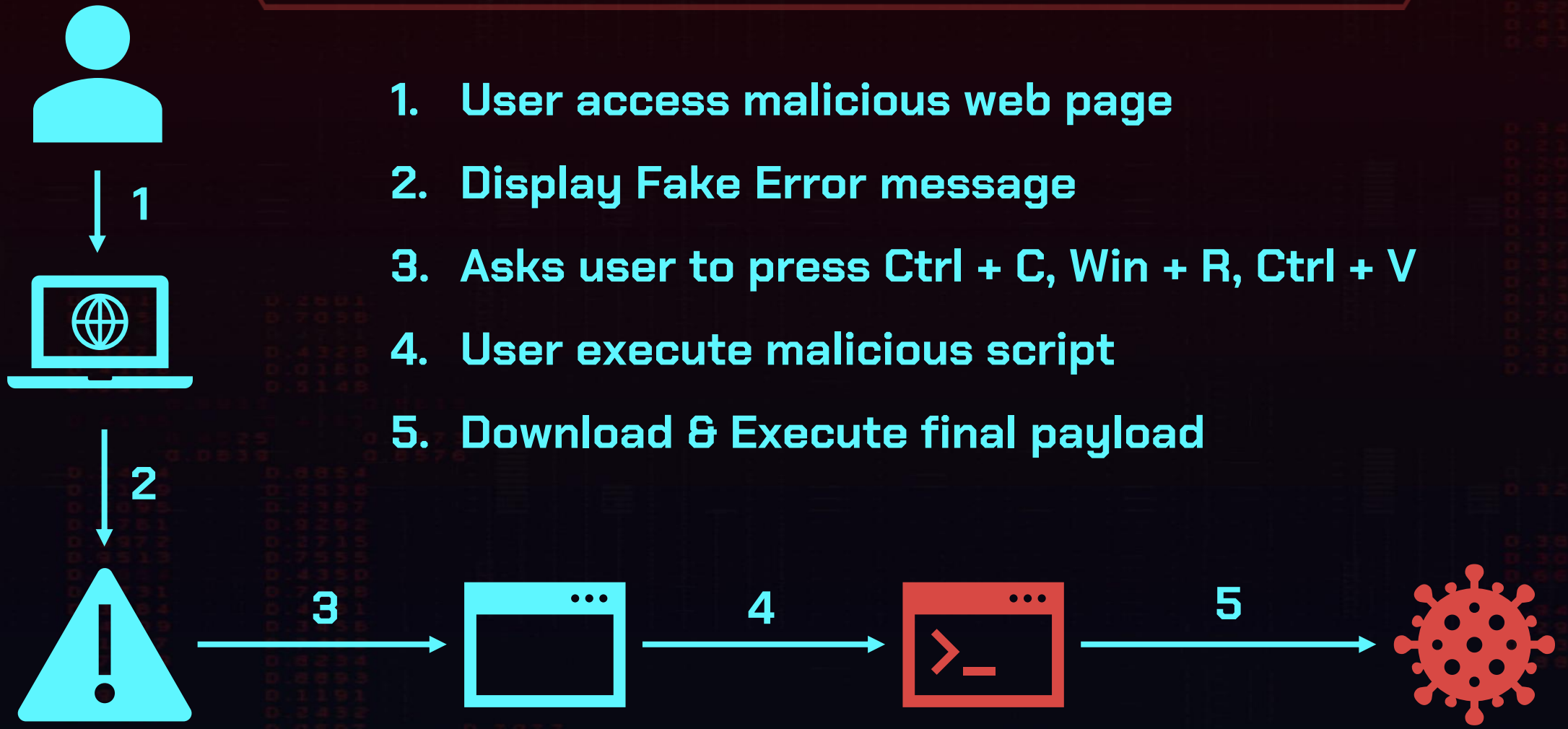
ClickFix distribution of cases per week by Unit42 @ Paloato

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

CLICK FIX - STATICS

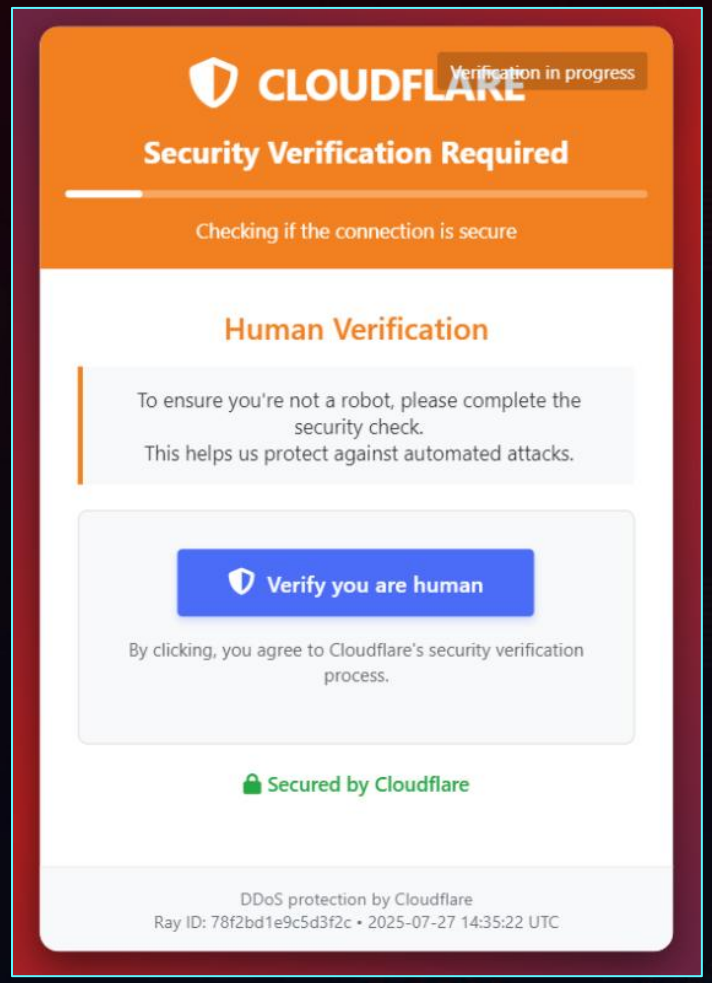
https://x.com/TheDFIRReport/status/1898005073289986369

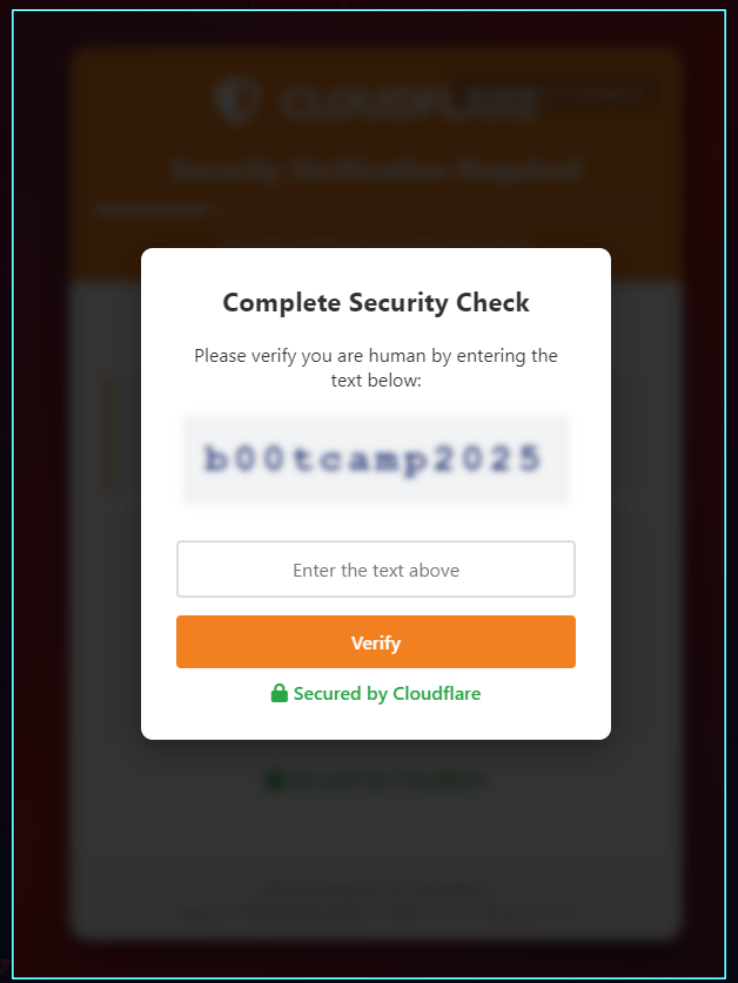
CLICK FIX - ANALYSIS

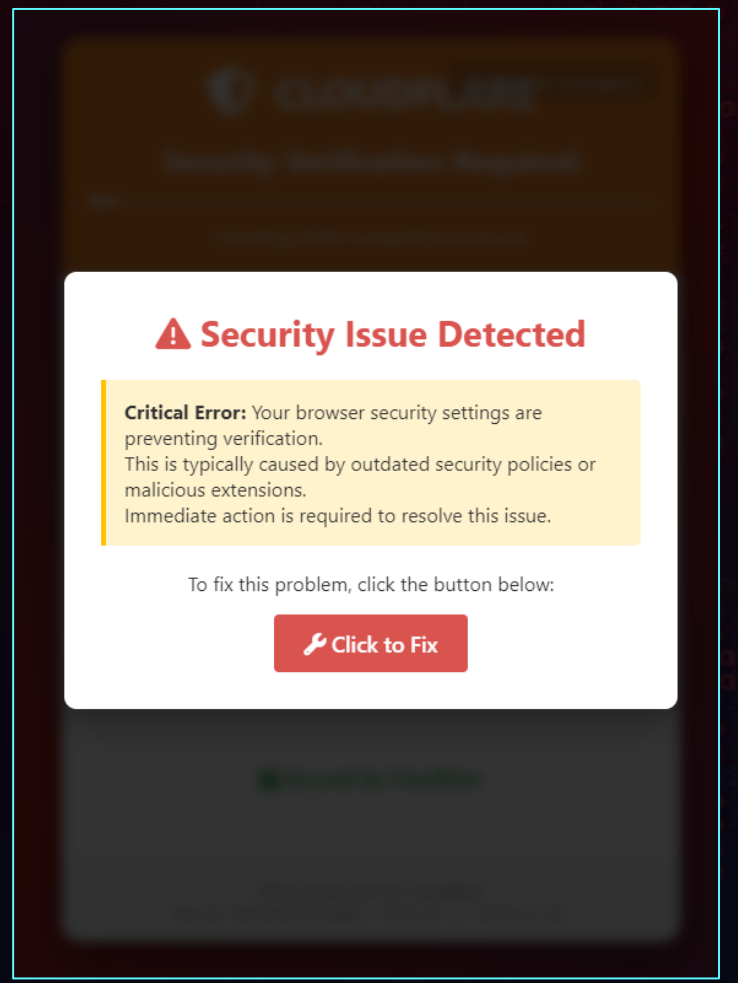


1. User access malicious web page
2. Display Fake Error message
3. Asks user to press Ctrl + C, Win + R, Ctrl + V
4. User execute malicious script
5. Download & Execute final payload

CLICK FIX - ANALYSIS

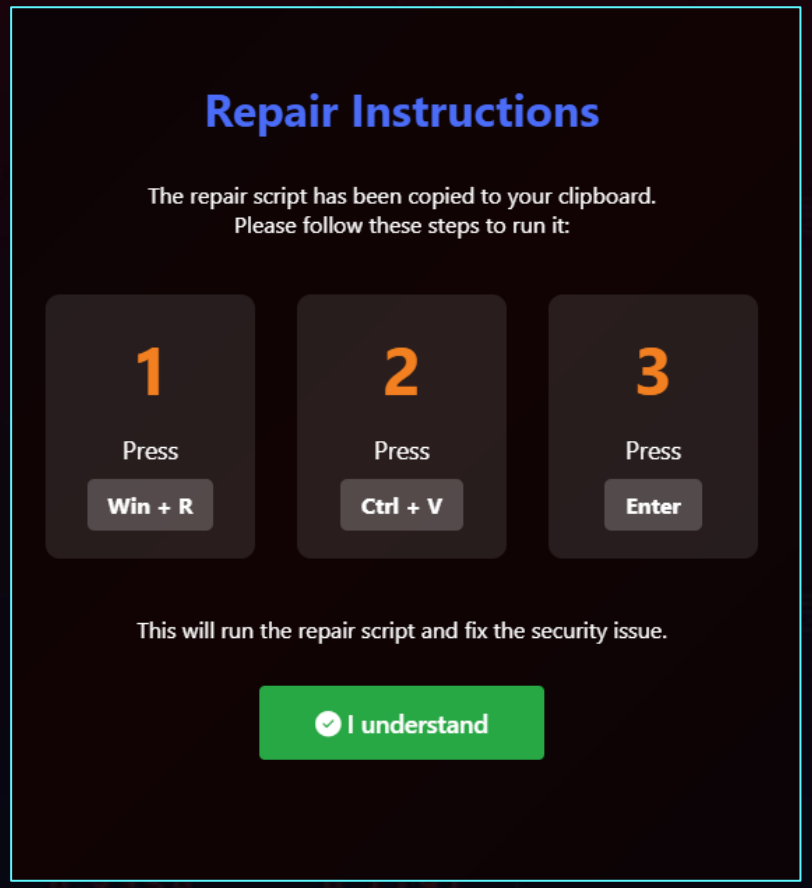


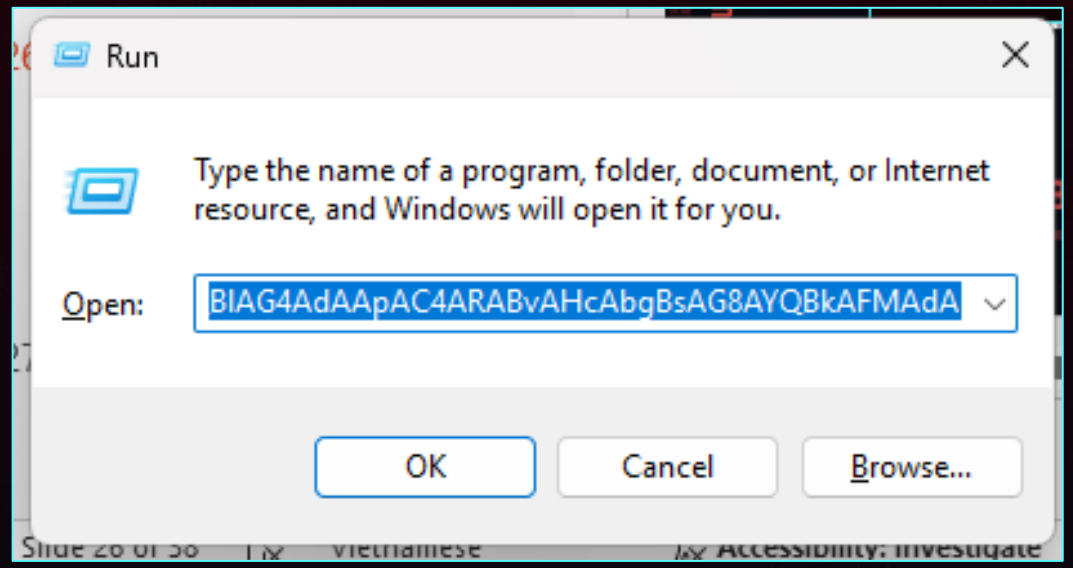


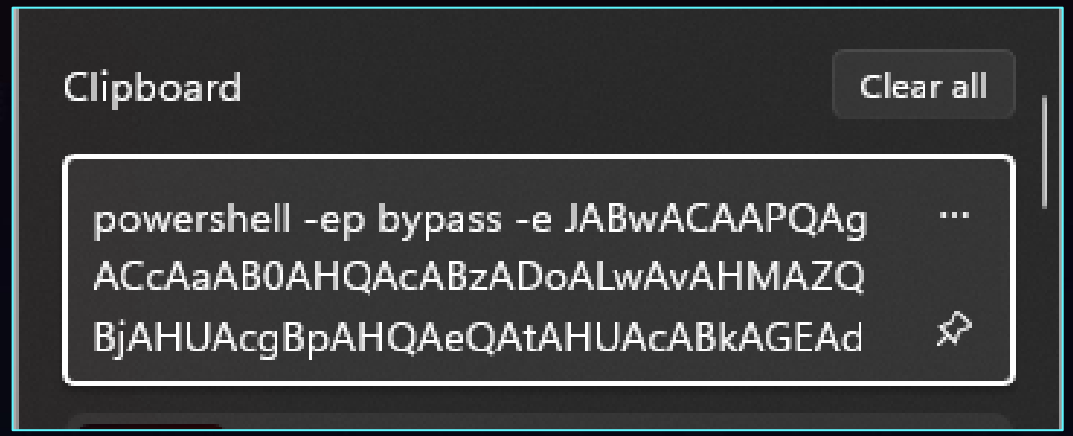


Click Fix generated by AI

CLICK FIX - ANALYSIS





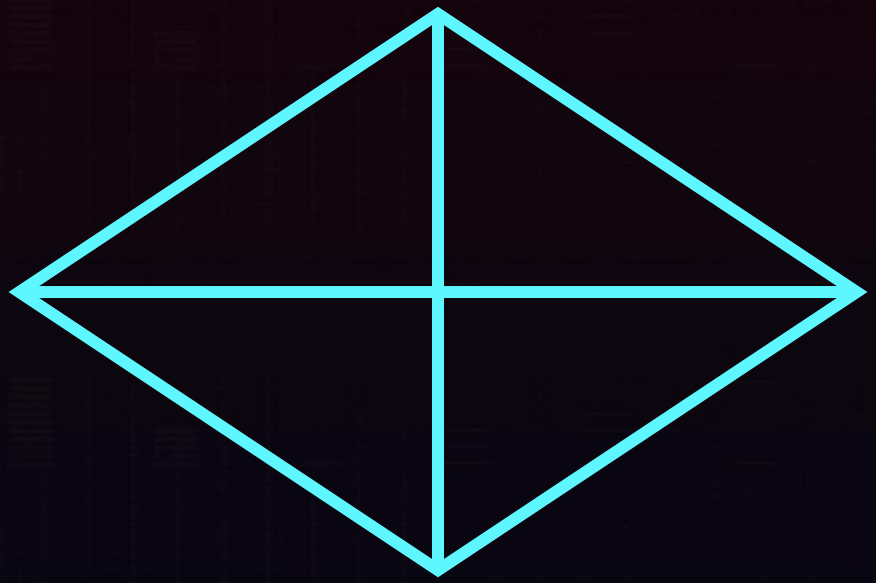


Click Fix generated by AI

CLICK FIX IN THE WILD

Adversary
TA571

Infrastructure
Vidar Stealer



Capability
Injected Website
ClearFake
ClickFix

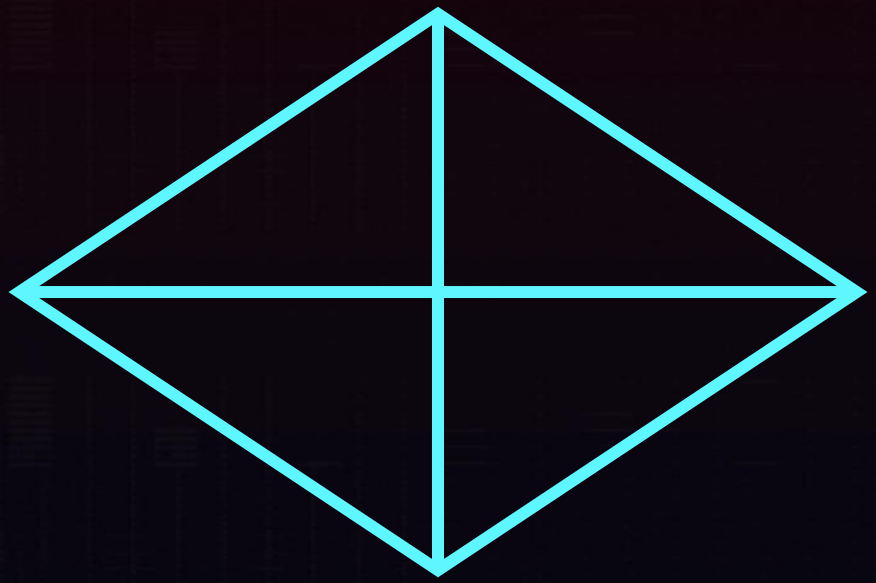
Victim
Global

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

CLICK FIX IN THE WILD

Adversary
N/A

Infrastructure
Lumma Stealer, StealC, NetSupport



Capability
ClickFix

Victim
Transport & logistic in North America

Source by proofpoint.com

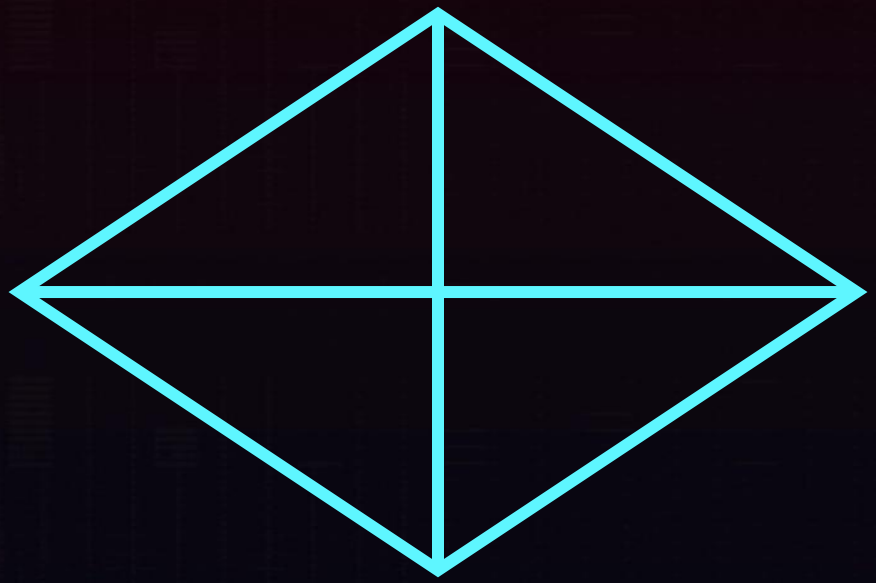
CLICK FIX IN THE WILD

Adversary

Storm-2477

Infrastructure

Lumma Stealer



Capability

Github issues
ClickFix

Victim

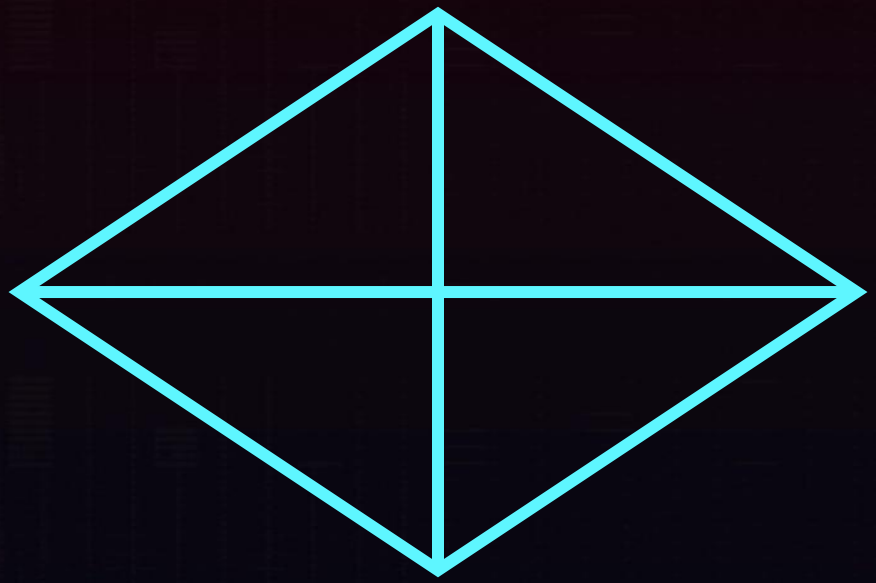
organizations in Canada

MS lumma-stealer-breaking-down

CLICK FIX IN THE WILD

Adversary
APT28

Infrastructure
Metasploit,
Lucky Volunteer,
AresLoader



Capability
Phishing Email
ClickFix

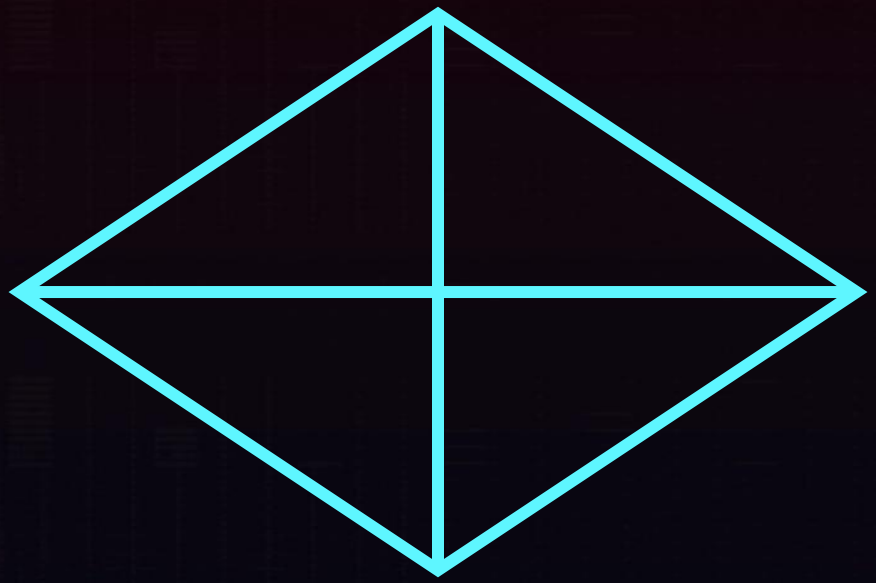
Victim
Ukrainian government

https://cert.gov.ua/article/6281123 , Or source by proofpoint

CLICK FIX IN THE WILD

Adversary
Lazarus

Infrastructure
GolangGhost

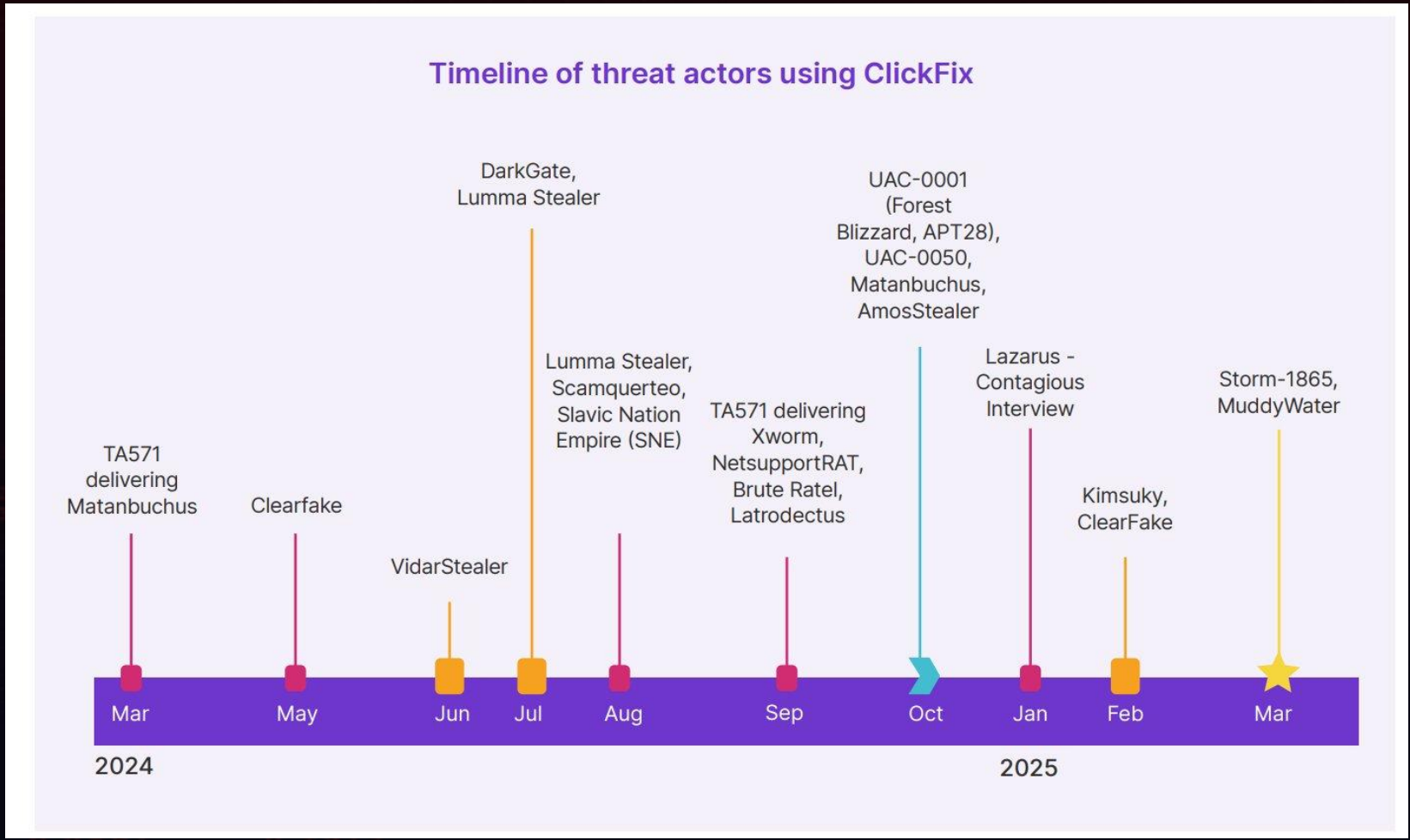


Capability
ClickFix
ClickFake Interview

Victim
Financial, Cryptocurrency

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

CLICK FIX IN THE WILD



BrideWell Cyber%20Threat%20Intelligence%20Report%202025%202.pdf

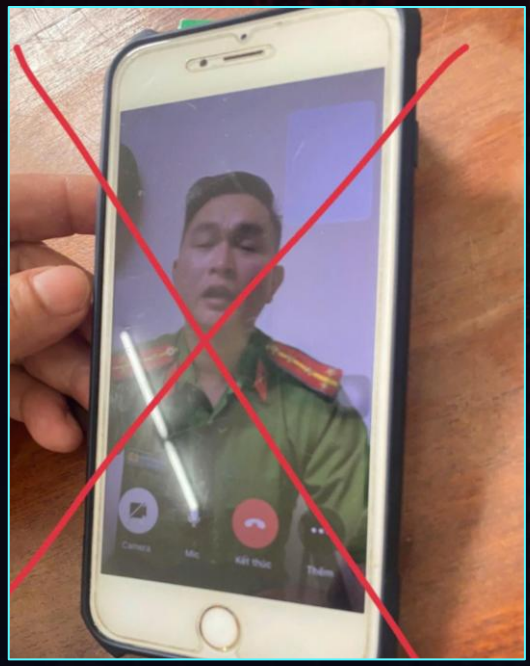
CLICK FIX IN VIET NAM?

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



DETECT & HUNTING

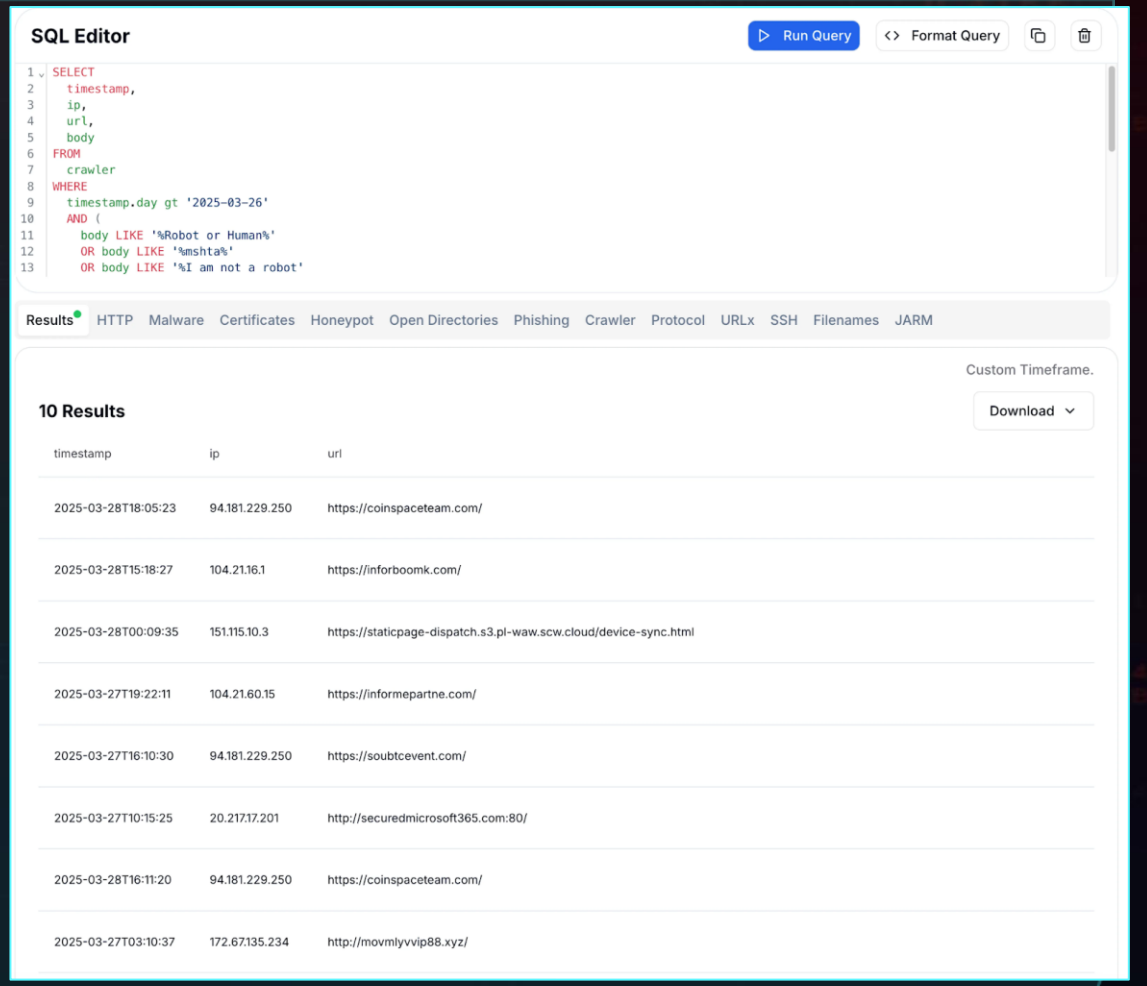
DECTECTION

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



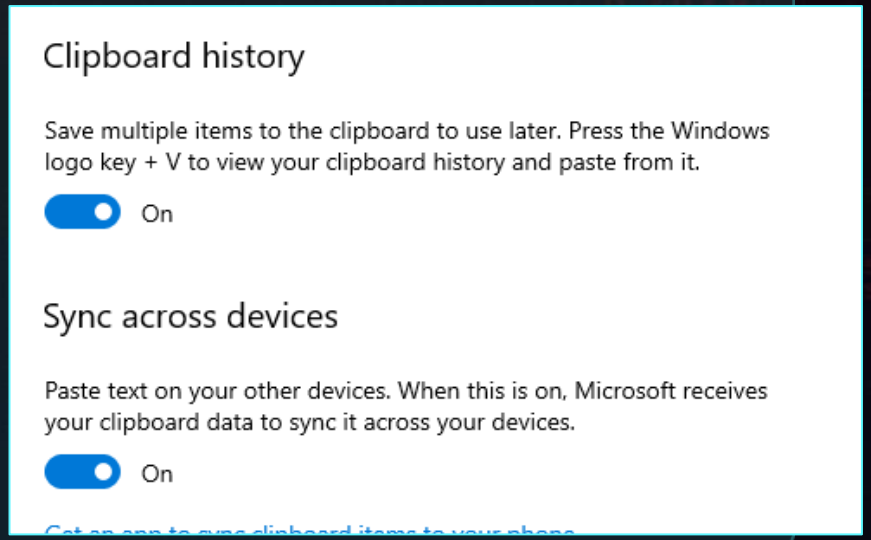
https://x.com/silentpush/status/1950897893159600158

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

HUNTING CLICKFIX

Hunt clipboard for what has been copied

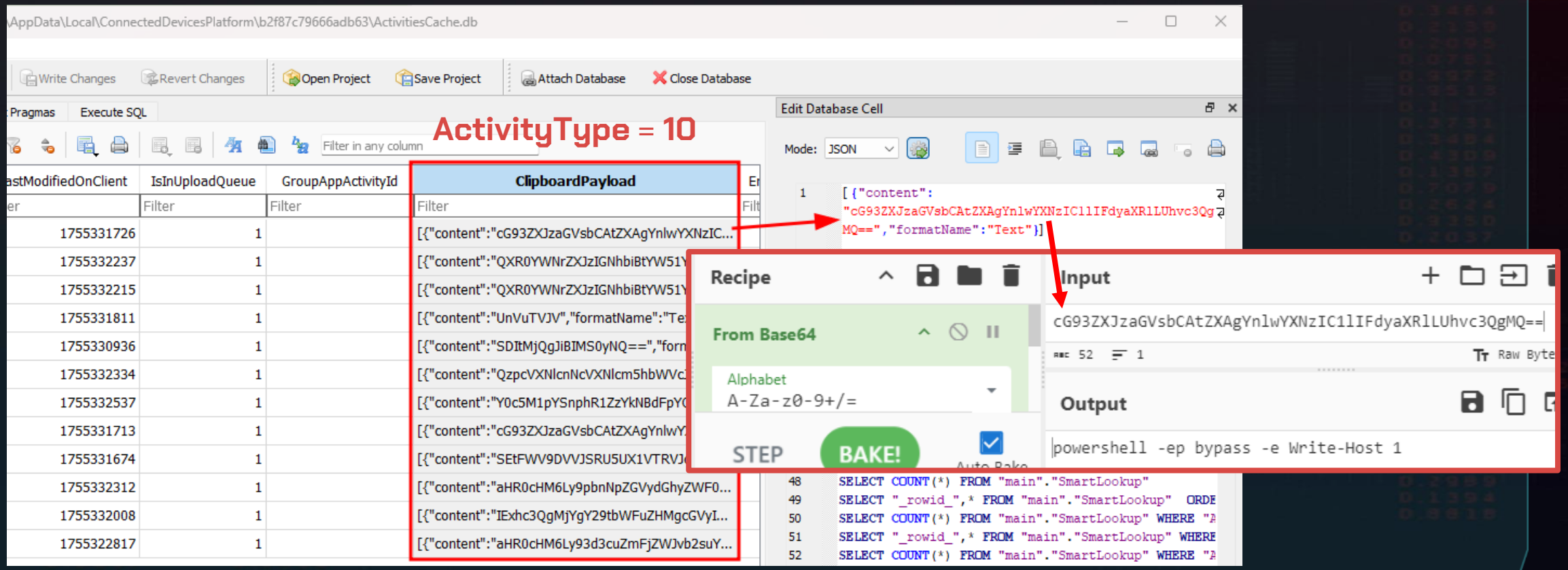
- ActivitiesCache.db
  - %AppData%\Local\ConnectedDevicesPlatform\<UserProfile>
  - Filter ActivityType
    - 10 – what data in clipboard
    - 16 – where data was copied/pasted
- Clipboard History & Sync across devices **must be Enabled**



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

HUNTING CLICKFIX

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

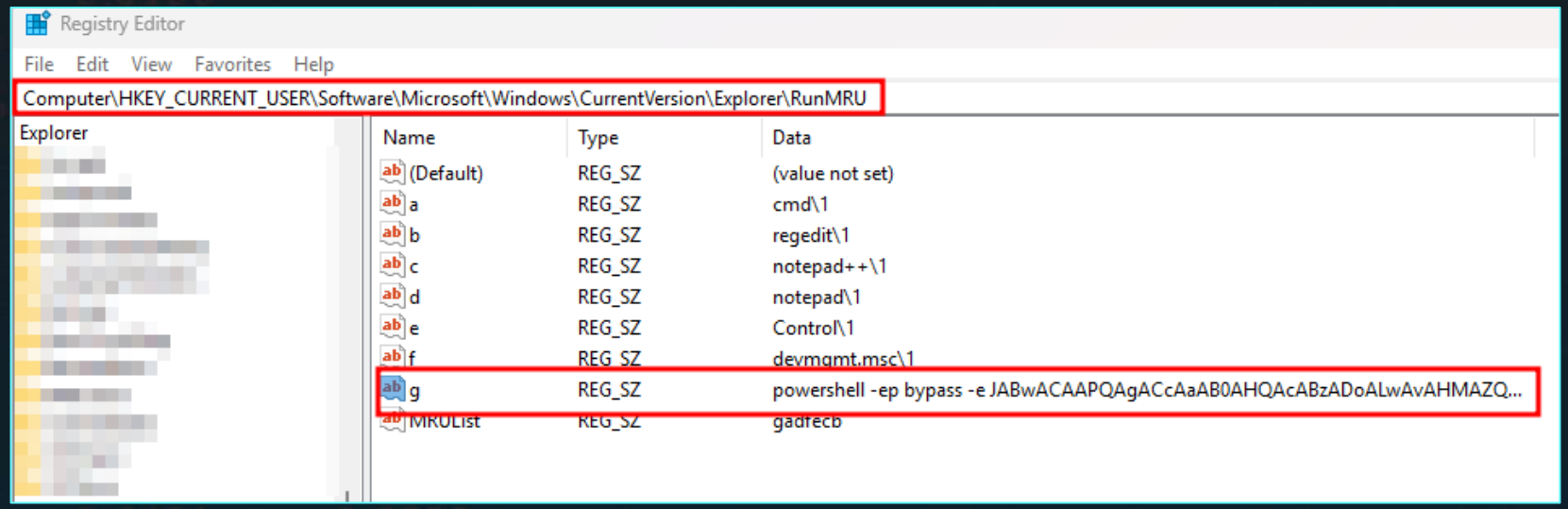


https://insiderthreatmatrix.org/detections/DT090

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:

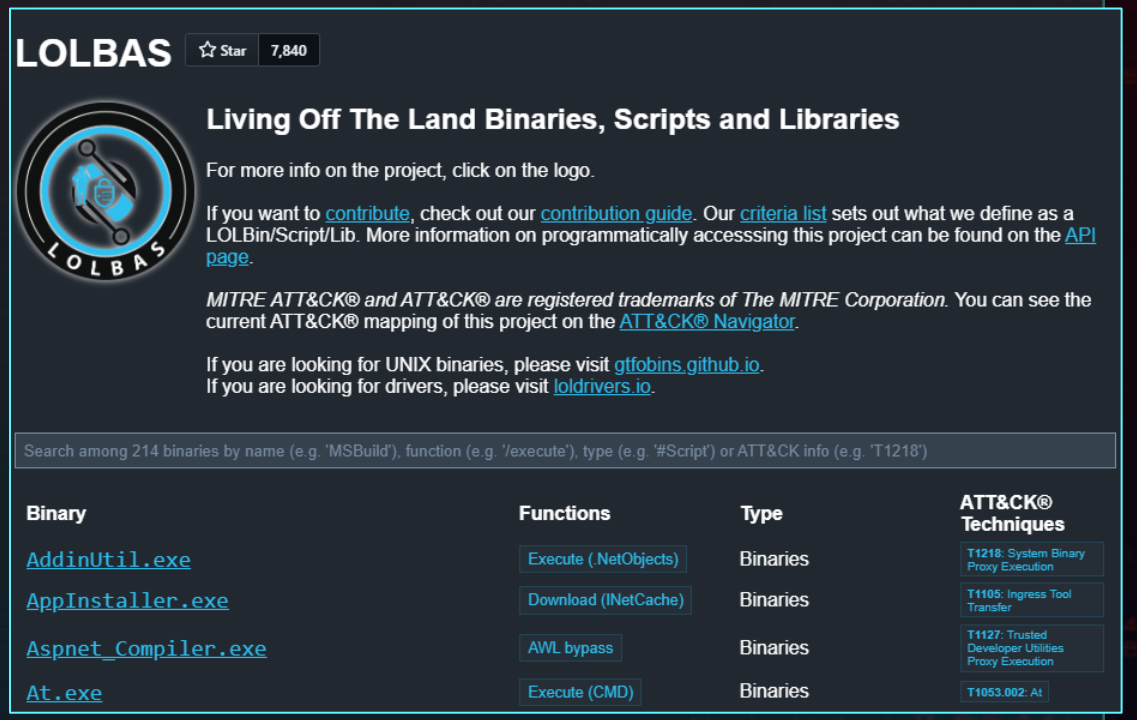
- Powershell, Mshta, Curl, ...
- https://lolbas-project.github.io

As a child of **Explore.exe**

RegSetValue **RunMRU** key

Execute **Encoded command**

Connect/download **Suspicious URL**



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

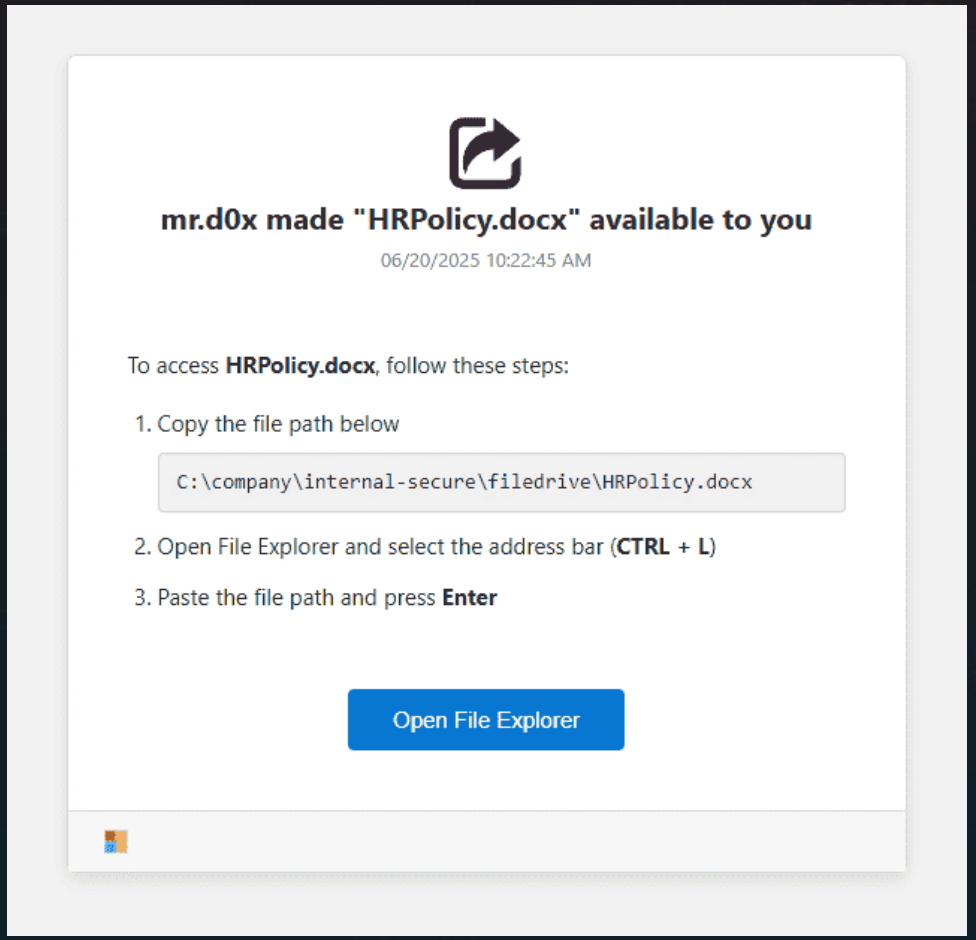
- ClickFix **is not** malware sophistication, its just **simple** but
  - precision delivery
  - legitimate-looking prompts
  - high-trust delivery paths
  - and low-friction execution
- Threat actors are quickly adopting new techniques
  - once they prove to yield results (ex: File Fix)

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!

tuept

@tuedenn

hi@goDefend.work