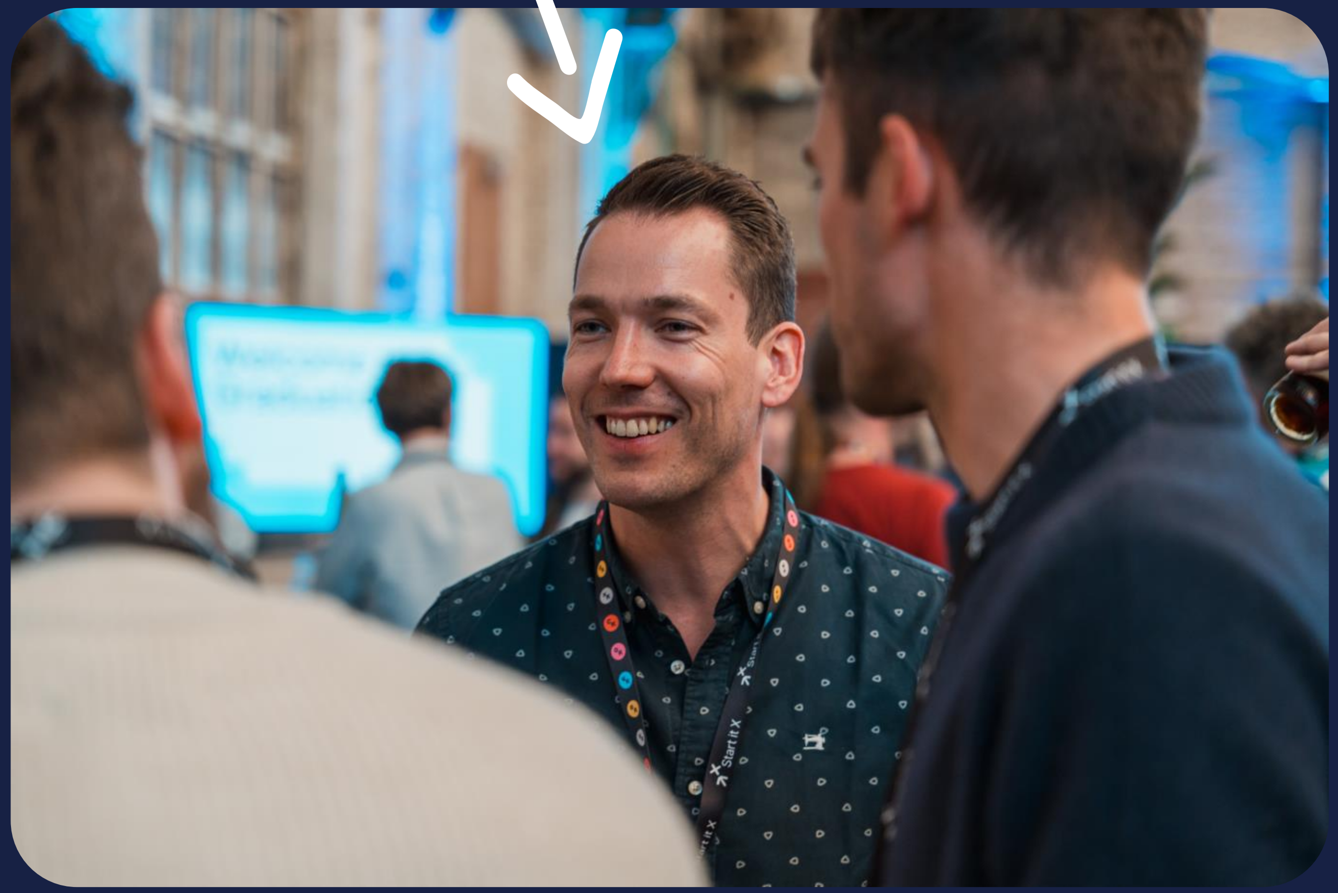
THE BEST OF 2023-2024:

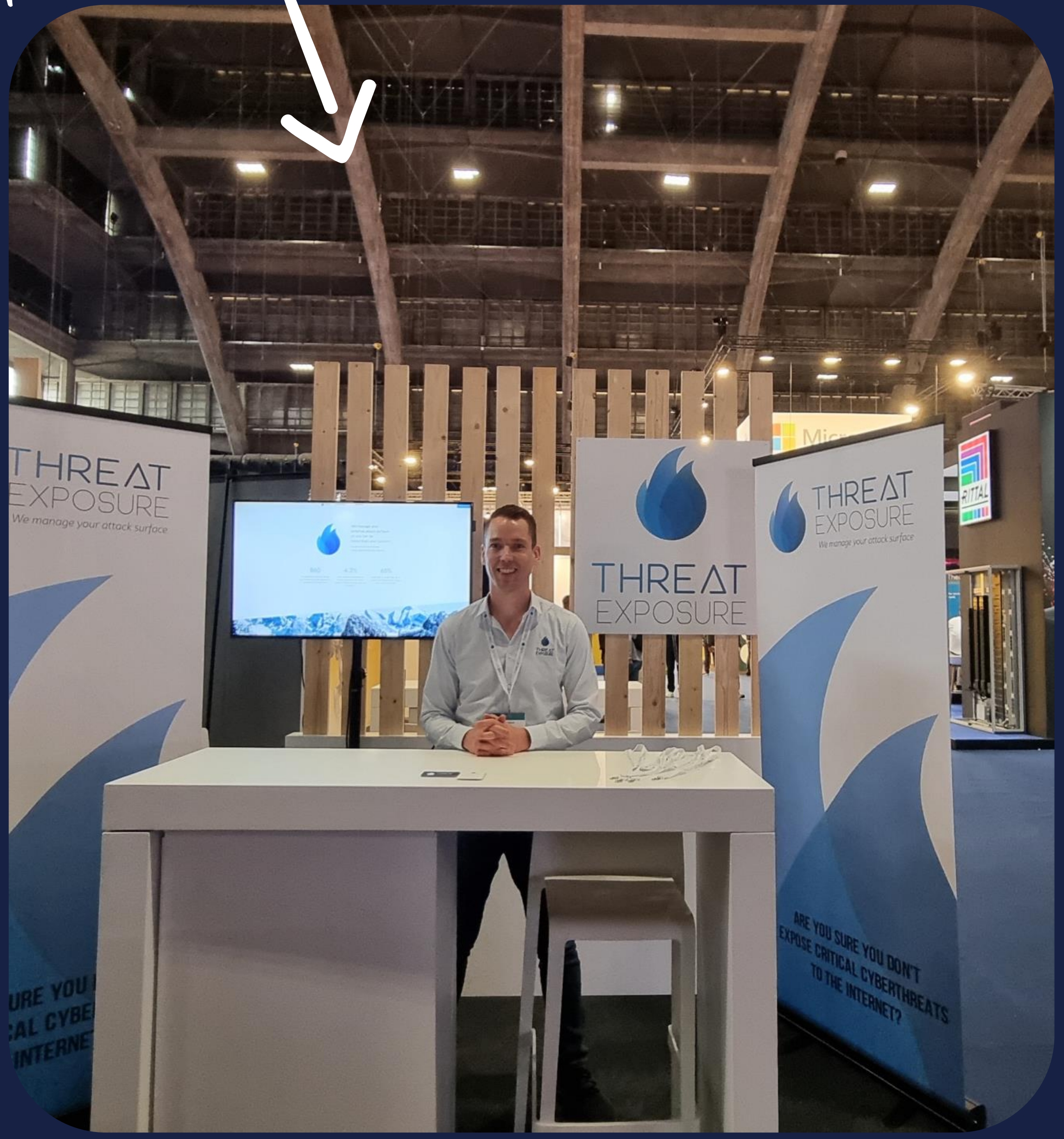
inside the biggest hacks and facts of the past year

Dieter Van Den Bosch



- Addicted to learning geeky stuff
  - All things technical, Sci-Fi, Science, Astronomy, Birds, Insects, ...
- Since 2009 in security
- Threat Intelligence analyst in group CERT
- International lead Attack Surface Management

Proud Dieter Van Den Bosch


THREAT EXPOSURE
We manage your attack surface
THREAT EXPOSURE
THREAT EXPOSURE
ARE YOU SURE YOU DON'T EXPOSE CRITICAL CYBERTHREATS TO THE INTERNET?

THREAT
EXPOSURE

We manage your attack surface

🌐 threatexposure.eu

✉ dieter@threatexposure.eu

in www.linkedin.com/in/vdbdieter/

BruCON 2023

START

Ransomware MGM

OCT
11

Sep 11: Scattered Spider gets in by calling MGM's helpdesk posing as an employee

Even key cards for rooms not functioning

Jan - June: 3 young adults from US & UK arrested

MGM doesn’t pay any ransom
Cyberattack costed $100 million

Ransomware Caesars

SEP 7

Days before MGM’s cyberattack,
Caesars paid a $15 million ransom

Ransomware MGM

OCT 11

Sep 11: Scattered Spider gets in by calling MGM's helpdesk posing as an employee

Even key cards for rooms not functioning

Jan - June: 3 young adults from US & UK arrested

MGM doesn’t pay any ransom
Cyberattack costed $100 million

Citrix Bleed

OCT
10

Steal authentication cookies from Citrix NetScaler ADC and Gateway appliances

Mandiant revealed that the flaw was abused months before the patch came out

Victims:
Boeing
Allen & Overy
DP World
Industrial and Commercial Bank of China

MULTI-MILLION CORPORATE CYBERSECURITY SPENDING
FORGOT TO PATCH THE CITRIX SERVER

OCT
10

HTTP/2 ‘Rapid Reset’ DDoS attack

New DDoS record: 400 million requests per second. Many times bigger than the last record.

A primary design goal of HTTP/2 was efficiency, and unfortunately the features that make HTTP/2 more efficient for legitimate clients can also be used to make DDoS attacks more efficient.

DEC
5

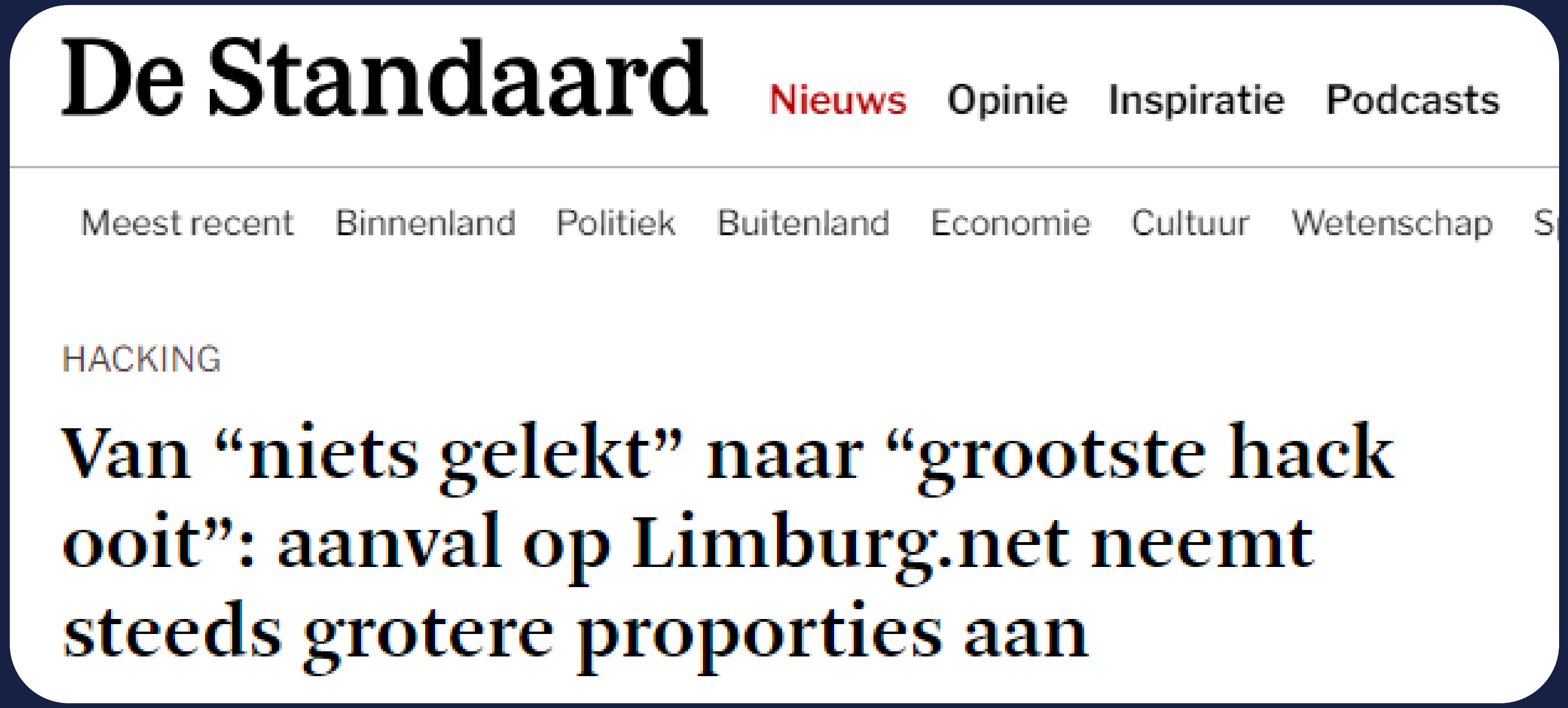
23andMe hack finally clear

23andMe spent months downplaying it and blaming their customers

DNA related data of 6.9 million, about half of customers, in the hands of hackers

The names, addresses belonging to 1 million 23andMe customers with Jewish heritage on BreachForums

Lacking MFA



HACKING

Van “niets gelekt” naar “grootste hack ooit”: aanval op Limburg.net neemt steeds grotere proporties aan

DEC
13

Ransomware attack Limburg.net

By Medusa

One server hacked with data of 311.000 families. Also leaked: data of 61 people in debt mediation etc.

RDP server exposed to the internet lacking MFA.
Source: Belang van Limburg

> “Ransom payments to ransomware gangs
> are
> tax-deductible as
> business expenses”

- Minister of Finances Vincent Van Peteghem -

> By paying ransom, you are financing cybercrime. Cybercriminals use their profit from ransomware attacks to launch new attacks on other companies.

- Simen Van Der Perre (Orange Cyberdefense), de Tijd -

> Ransom payments to ransomware gangs are tax-deductible as business expenses

- Minister of Finances Vincent Van Peteghem -

The toothbrush DDoS attack

FEB
6

Reported by Swiss newspaper
after an interview with Fortinet.

The DDoS knocked out a Swiss company
for several hours, costing millions of euros

The news quickly went viral around the world.

Except… it wasn't true.
Fortinet said it was just a hypothetical story.

Did we all think it was indeed plausible?

FEB
18

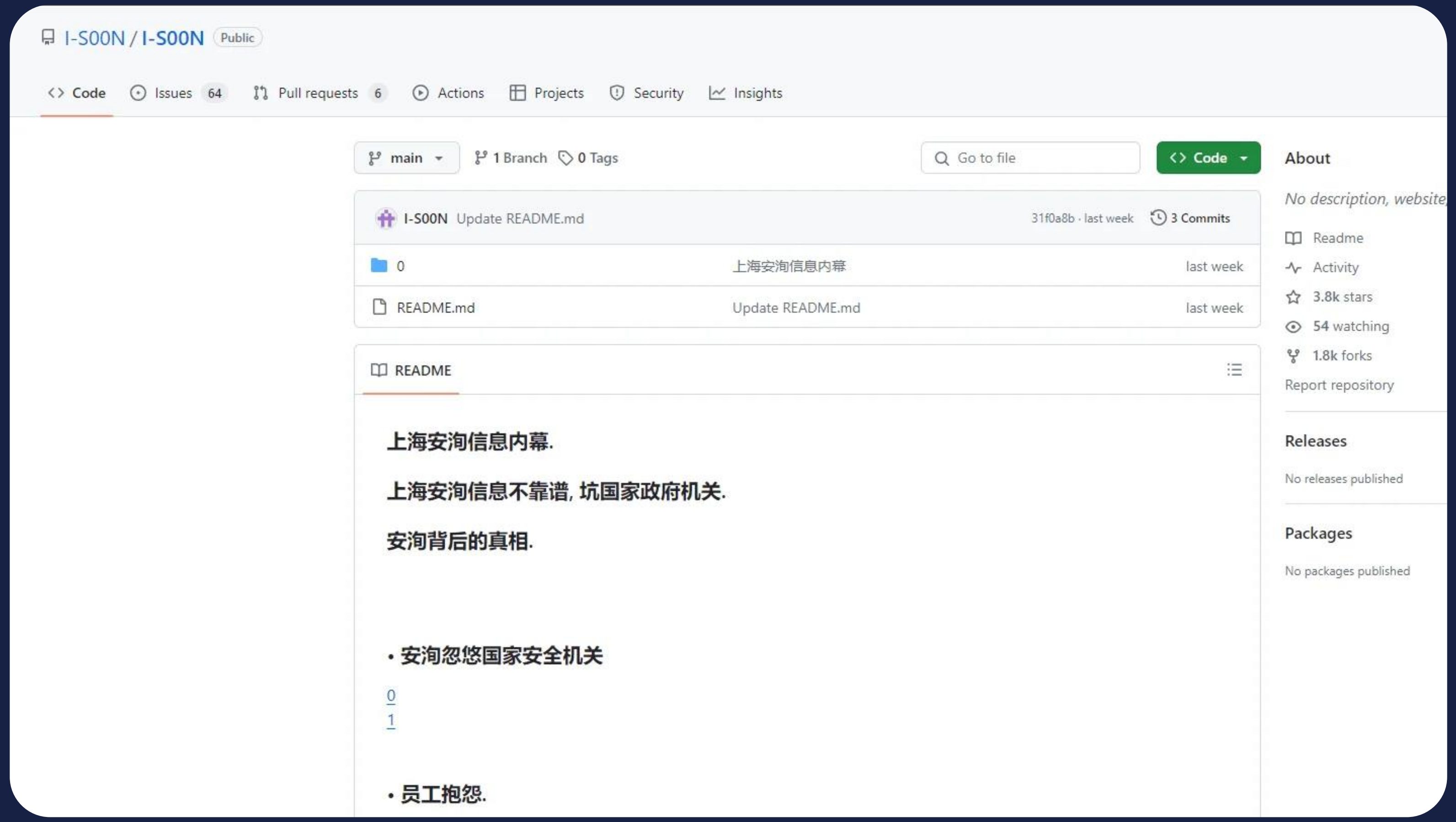
i-Soon leak

APT-for-hire for multiple Chinese authorities

It got quickly deleted

80 targets: government of India, Thailand, Vietnam, South Korea, Pakistan, Afghanistan…

Chat logs reveal:
A: we've got stuff from their chairman Jens Stoltenberg
B: they are not interested
A: what about making it cheaper? I'm running low on money



I-SOON / I-SOON Public

I-SOON Update README.md 31f0a8b · last week 3 Commits

0 上海安洵信息内幕 last week
README.md Update README.md last week

README

上海安洵信息内幕.

上海安洵信息不靠谱, 坑国家政府机关.

安洵背后的真相.

- 安洵忽悠国家安全机关

0
1

- 员工抱怨.

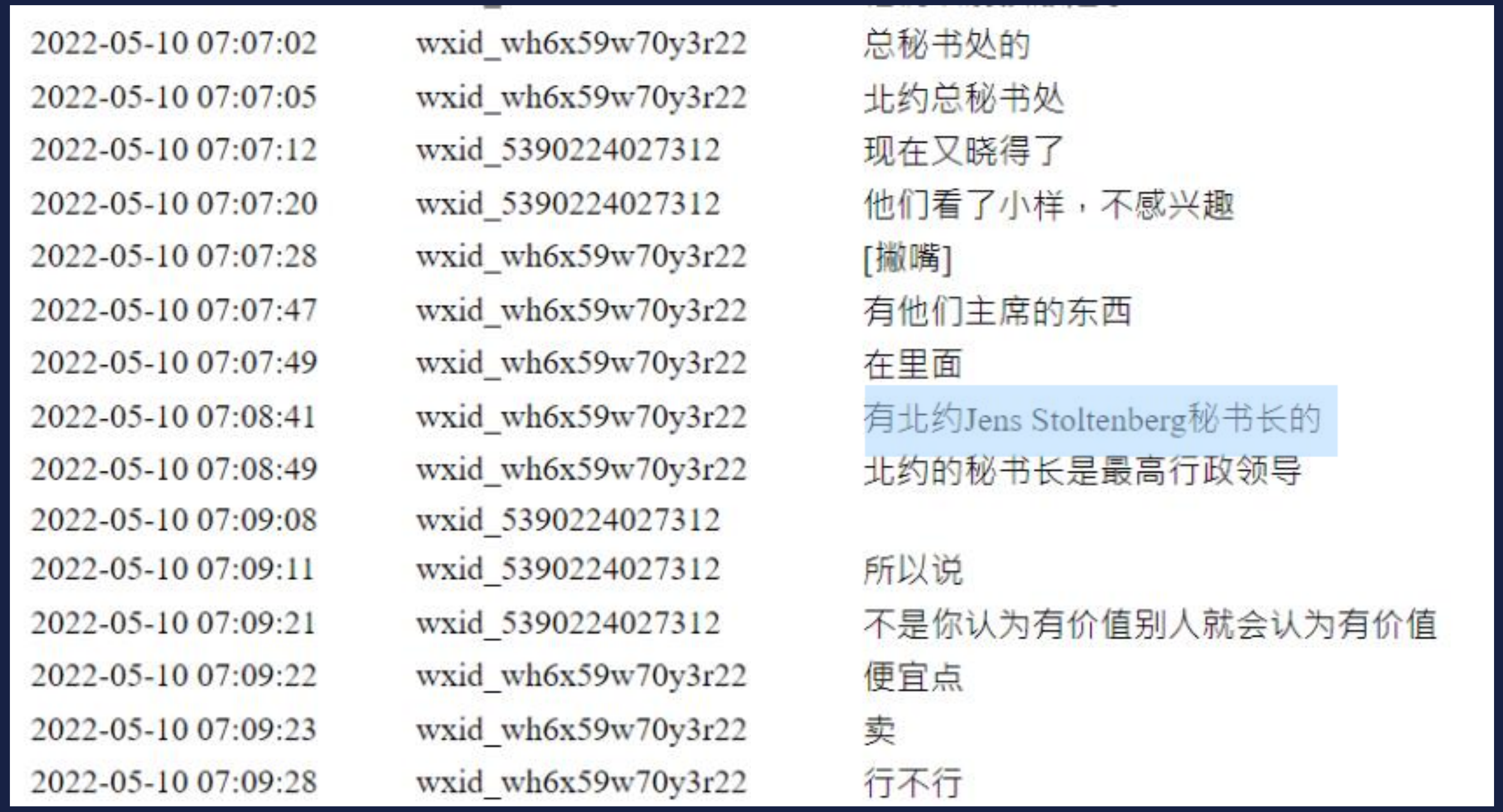
No description, website

3.8k stars
54 watching
1.8k forks

No releases published

No packages published

1800 forks



```
2022-05-10 07:07:02    wxid_wh6x59w70y3r22    总秘书处的
2022-05-10 07:07:05    wxid_wh6x59w70y3r22    北约总秘书处
2022-05-10 07:07:12    wxid_5390224027312     现在又晓得了
2022-05-10 07:07:20    wxid_5390224027312     他们看了小样，不感兴趣
2022-05-10 07:07:28    wxid_wh6x59w70y3r22    [撇嘴]
2022-05-10 07:07:47    wxid_wh6x59w70y3r22    有他们主席的东西
2022-05-10 07:07:49    wxid_wh6x59w70y3r22    在里面
2022-05-10 07:08:41    wxid_wh6x59w70y3r22    有北约Jens Stoltenberg秘书长的
2022-05-10 07:08:49    wxid_wh6x59w70y3r22    北约的秘书长是最高行政领导
2022-05-10 07:09:08    wxid_5390224027312
2022-05-10 07:09:11    wxid_5390224027312     所以说
2022-05-10 07:09:21    wxid_5390224027312     不是你认为有价值别人就会认为有价值
2022-05-10 07:09:22    wxid_wh6x59w70y3r22    便宜点
2022-05-10 07:09:23    wxid_wh6x59w70y3r22    卖
2022-05-10 07:09:28    wxid_wh6x59w70y3r22    行不行
```

FEB
20

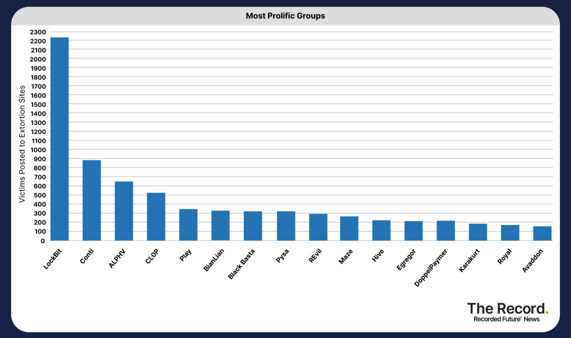
LockBit hackers hacked

Led by British National Crime Agency

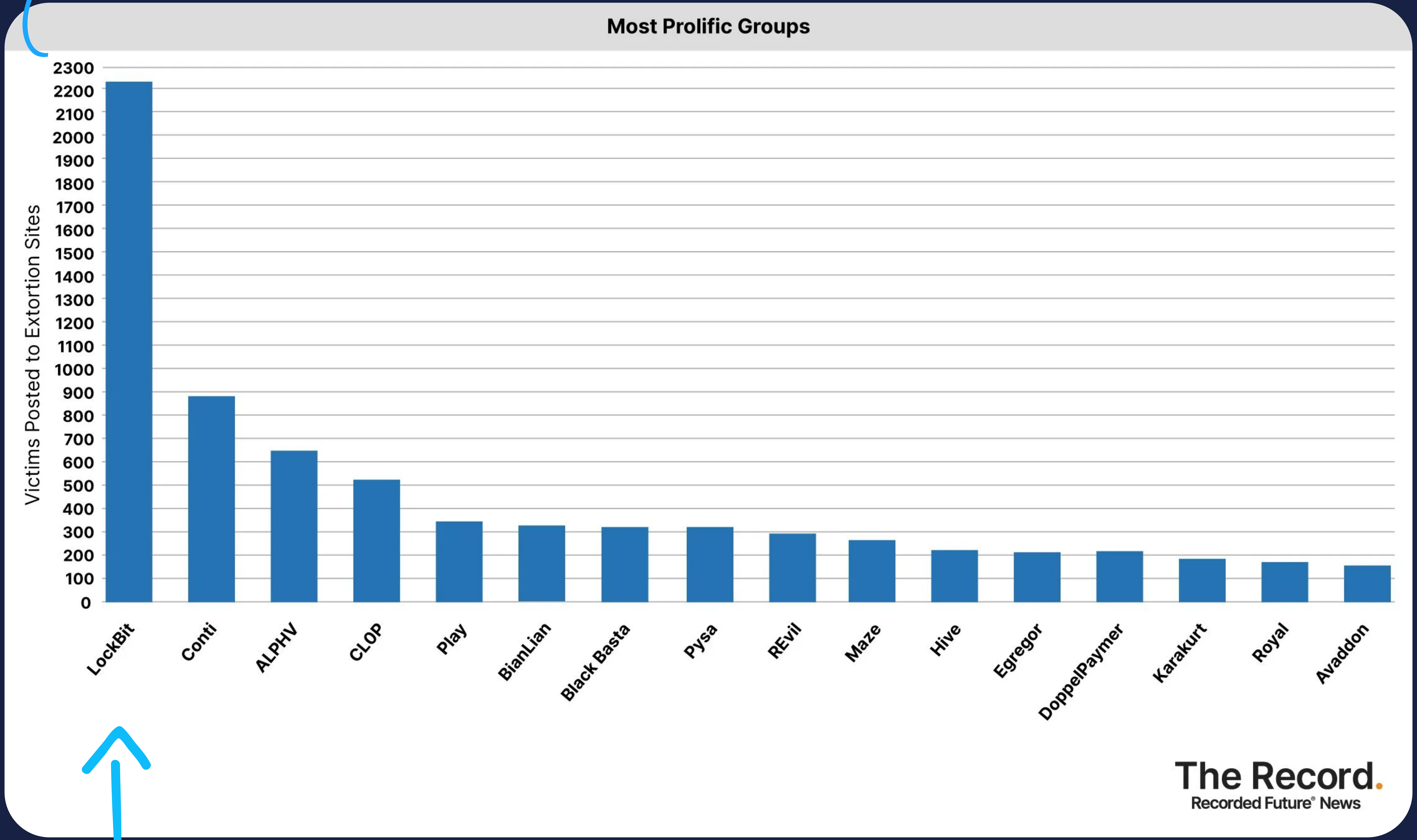
Victims: Accenture, British Royal Mail, City of Geraardsbergen, Maldegem, province Namur, French Ministry of Justice, Canada's largest pediatric hospital, …

2500 victims. More than $500 million in ransom

194 affiliates (the ones that do the actual hacking)
80% off ransom goes to affiliate



Number of victims is 50% -60% higher,
because not all victims reach the leak site.
Source: Orange Cyber Defense



FEB
20

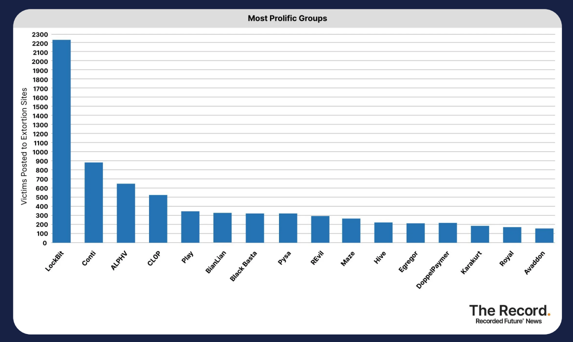
LockBit hackers hacked

Led by British National Crime Agency

Victims: Accenture, British Royal Mail, City of Geraardsbergen, Maldegem, province Namur, French Ministry of Justice, Canada’s largest pediatric hospital, …

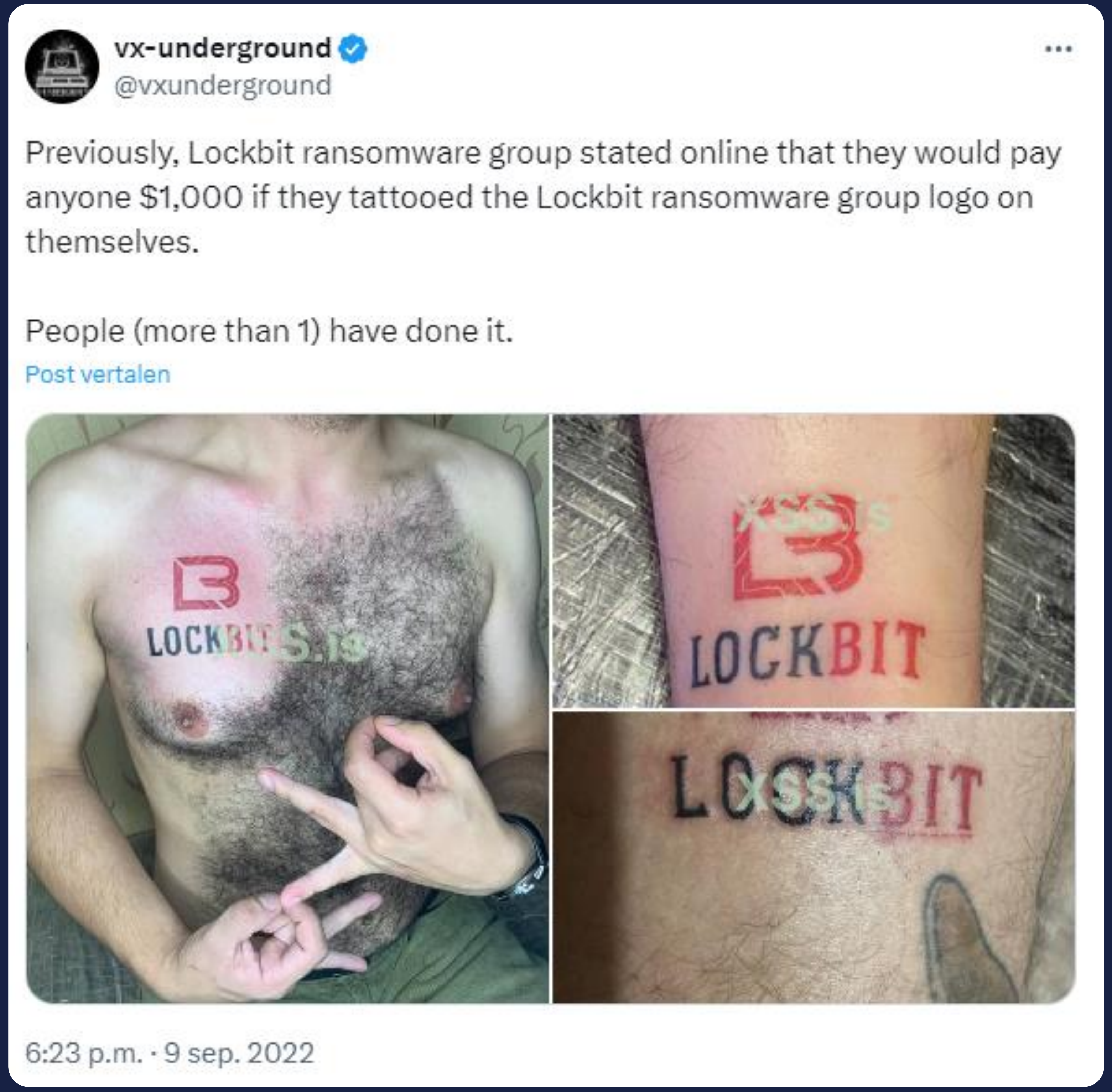
2500 victims. More than $500 million in ransom

194 affiliates (the ones that do the actual hacking)
80% off ransom goes to affiliate



In 2021 LockBit said jokingly they would give money to anyone who would get a tattoo.

And some were crazy enough to do it!



vx-underground
@vxunderground

Previously, Lockbit ransomware group stated online that they would pay anyone $1,000 if they tattooed the Lockbit ransomware group logo on themselves.

People (more than 1) have done it.

Post vertalen

6:23 p.m. · 9 sep. 2022

LOCKBIT
XSS.is

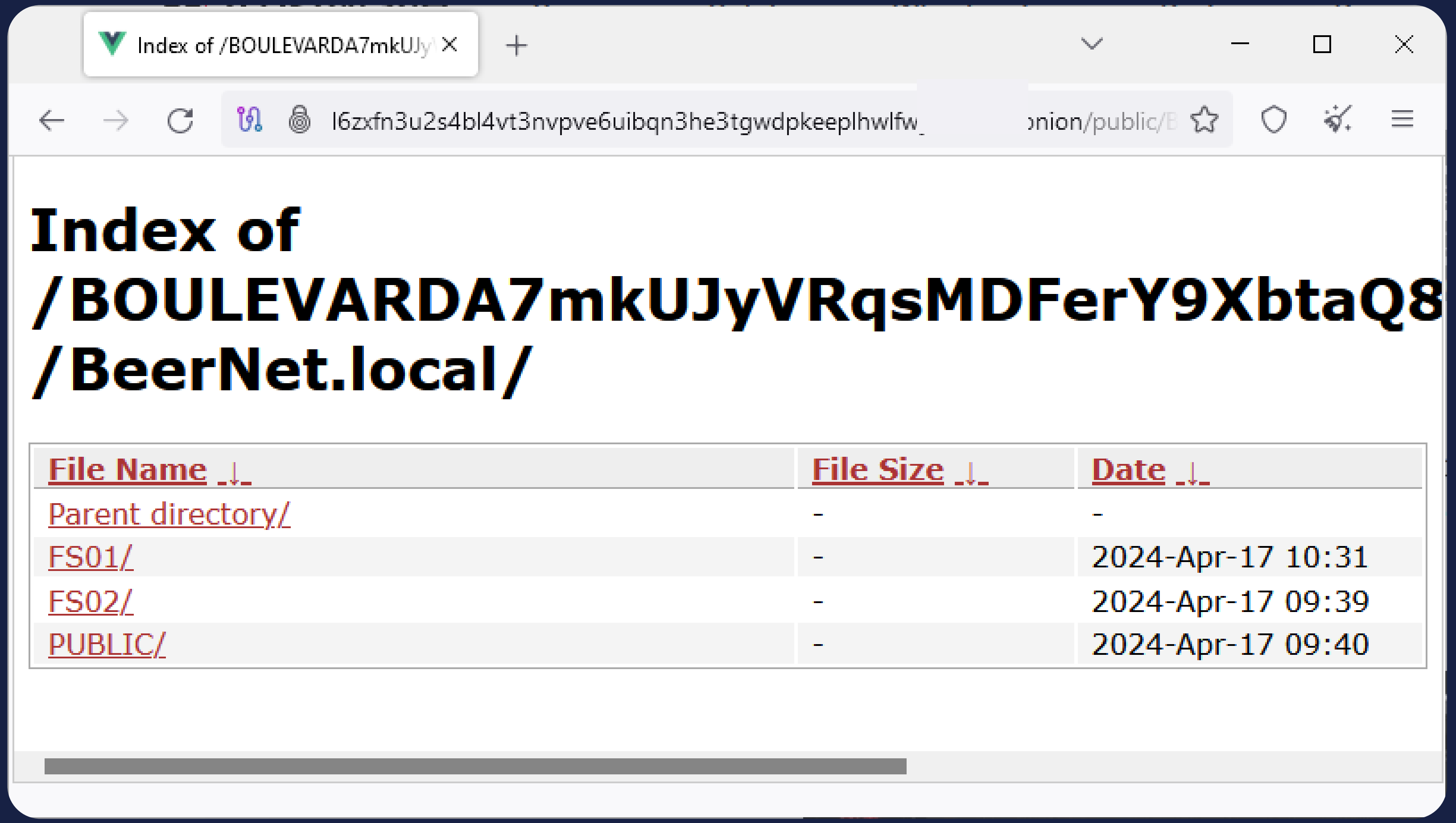
MAR
6

Ransomware attack Duvel Moortgat

Ransomware Gang Stormous…
or Black Basta? Conti?

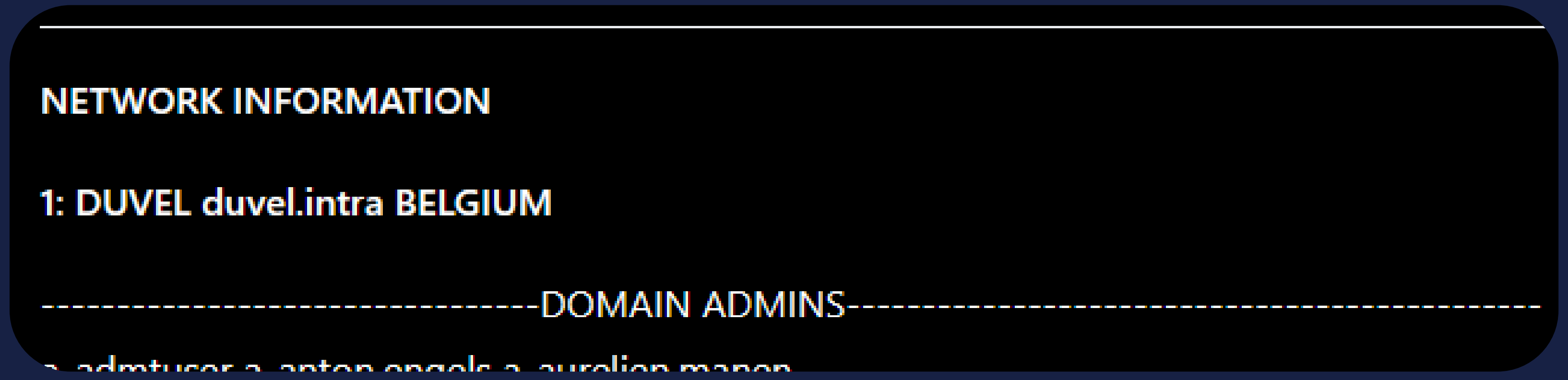
2 fileservers from American daughter

But also access to Belgian DC
e.g. domain admins with passwords
1 day later main brewery of Duvel was back in action


Index of /BOULEVARDA7mkUJy
l6zxfn3u2s4bl4vt3nvpve6uibqn3he3tgwdpkeeplhwlfw_ .onion/public/

Index of /BOULEVARDA7mkUJyVRqsMDFerY9XbtaQ8 /BeerNet.local/

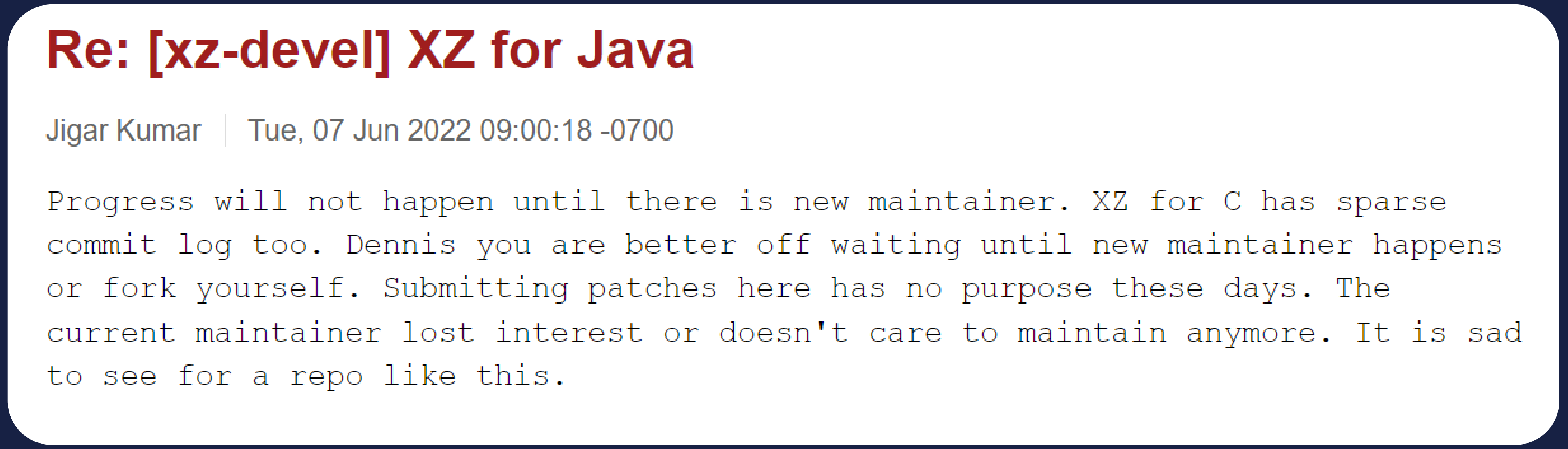
File Name ↓	File Size ↓	Date ↓
Parent directory/	-	-
FS01/	-	2024-Apr-17 10:31
FS02/	-	2024-Apr-17 09:39
PUBLIC/	-	2024-Apr-17 09:40



```
NETWORK INFORMATION

1: DUVEL duvel.intra BELGIUM

--------------------------------DOMAIN ADMINS--------------------------------------------
a-admtuser a-anton.engels a-aurelien.manon
```



Re: [xz-devel] XZ for Java

Jigar Kumar | Tue, 07 Jun 2022 09:00:18 -0700

```
Progress will not happen until there is new maintainer. XZ for C has sparse
commit log too. Dennis you are better off waiting until new maintainer happens
or fork yourself. Submitting patches here has no purpose these days. The
current maintainer lost interest or doesn't care to maintain anymore. It is sad
to see for a repo like this.
```

MAR
29

XZ Utils backdoor

XZ = a compression tool e.g. used in sshd

Three years in the making

Found by Andres Freund from Berlin, Postgres developer working at Microsoft, who thought his CPU levels were suspicious

THE MICROSOFT NERD BENCHMARKING HIS SSH CONNECTIONS
THE ENTIRE INFOSEC COMMUNITY

MAR
20

Microsoft hacked

Again.

May and June, 2023

Chinese cyber-espionage group Storm-0558 compromised the Microsoft Exchange Online mailboxes of 22 organizations around the world.

From 10 State Department e-mail boxes alone, 60 000 emails were stolen.

🇨🇳

“Cascade of security failures at Microsoft” caused hack

1) Found a key from 2016. These ‘keys to their kingdom’ were still valid after 7 years.

2) In September: the hackers found the key in a crash dump.

In March: we have not found a crash dump containing the impacted key material. It was just a ‘theory’.

May and June, 2023

Chinese cyber-espionage group Storm-0558 compromised the Microsoft Exchange Online mailboxes of 22 organizations around the world.

From 10 State Department e-mail boxes alone, 60 000 emails were stolen.

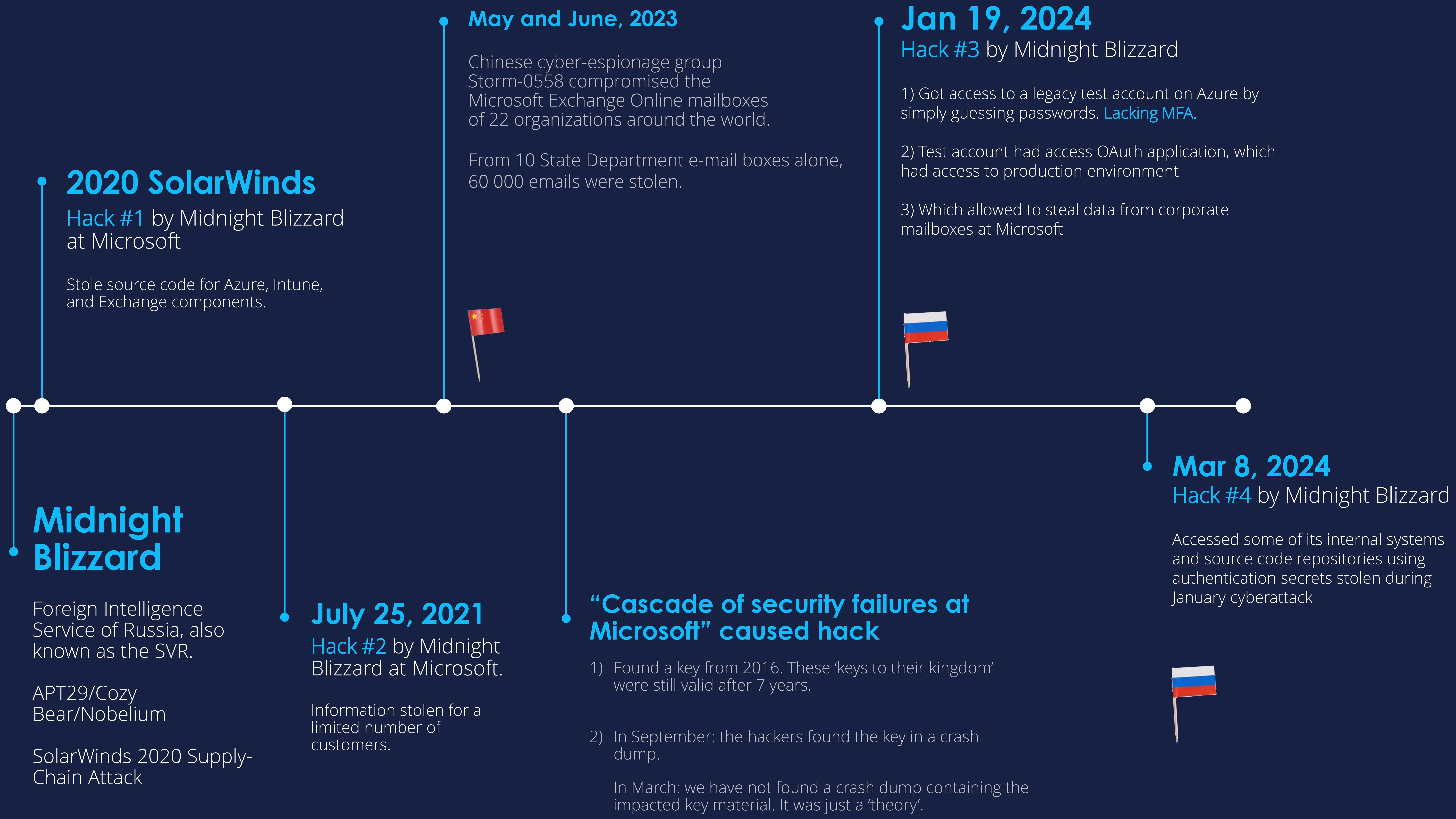
🇨🇳

“Cascade of security failures at Microsoft” caused hack

1) Found a key from 2016. These ‘keys to their kingdom’ were still valid after 7 years.

2) In September: the hackers found the key in a crash dump.

   In March: we have not found a crash dump containing the impacted key material. It was just a ‘theory’.



Midnight Blizzard

Foreign Intelligence Service of Russia, also known as the SVR.

APT29/Cozy Bear/Nobelium

SolarWinds 2020 Supply-Chain Attack

2020 SolarWinds

Hack #1 by Midnight Blizzard at Microsoft

Stole source code for Azure, Intune, and Exchange components.

July 25, 2021

Hack #2 by Midnight Blizzard at Microsoft.

Information stolen for a limited number of customers.

May and June, 2023

Chinese cyber-espionage group Storm-0558 compromised the Microsoft Exchange Online mailboxes of 22 organizations around the world.

From 10 State Department e-mail boxes alone, 60 000 emails were stolen.

“Cascade of security failures at Microsoft” caused hack

1) Found a key from 2016. These ‘keys to their kingdom’ were still valid after 7 years.

2) In September: the hackers found the key in a crash dump.

   In March: we have not found a crash dump containing the impacted key material. It was just a ‘theory’.

Jan 19, 2024

Hack #3 by Midnight Blizzard

1) Got access to a legacy test account on Azure by simply guessing passwords. Lacking MFA.

2) Test account had access OAuth application, which had access to production environment

3) Which allowed to steal data from corporate mailboxes at Microsoft

Mar 8, 2024

Hack #4 by Midnight Blizzard

Accessed some of its internal systems and source code repositories using authentication secrets stolen during January cyberattack

> We are making security our top priority at Microsoft, above all else, above all features

- Charlie Bell, Executive Vice President, Microsoft Security -

MAY
20

Microsoft announces Recall

~~Photographic memory of your PC life~~
Built-in information stealer/password grabber

~~Only admins can read the database~~ Nope!

~~Users on the same device can not access the database~~ Nope!

June 14: Recall got… ~~recalled~~ delayed to Ocober!
Windows Insiders with Copilot+ PCs

Snowflake

May
30

April 14

Data stolen of 109 million, nearly all of its mobile customers

Months worth of call and text records

Paid $370,000 to delete the data

'ShinyHunters' hacked them in 2021 as well

AT&T

May 14

Data stolen of 30 million customers and employees

'ShinyHunters' claims it contains 28 million credit card numbers

Santander

May 20

'ShinyHunters' claims data from 560 million customers

One of the largest data breaches ever

ticketmaster®

May 30

Leading cloud-based data storage and analytics provider

Compromised customer credentials lacking MFA

snowflake

June 10

UNC5537,
"A teen crimeware group"

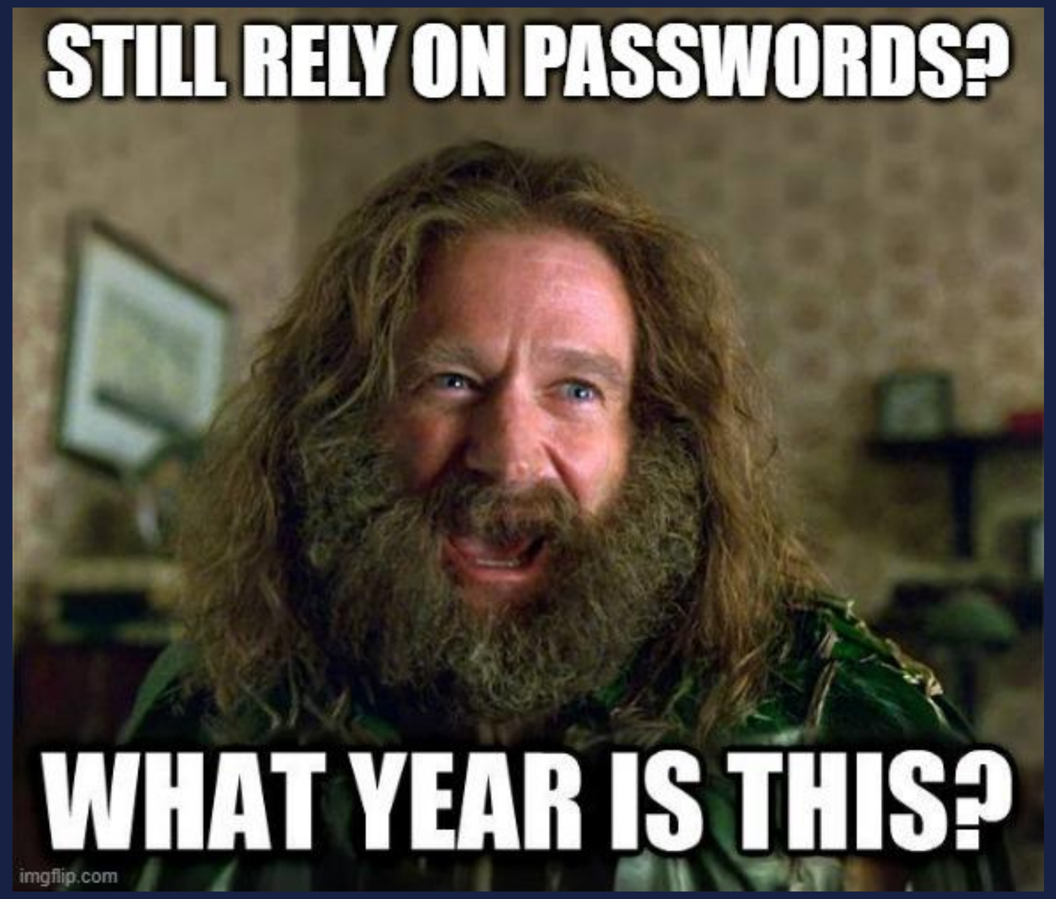
165 potentially impacted organizations, mostly under the radar

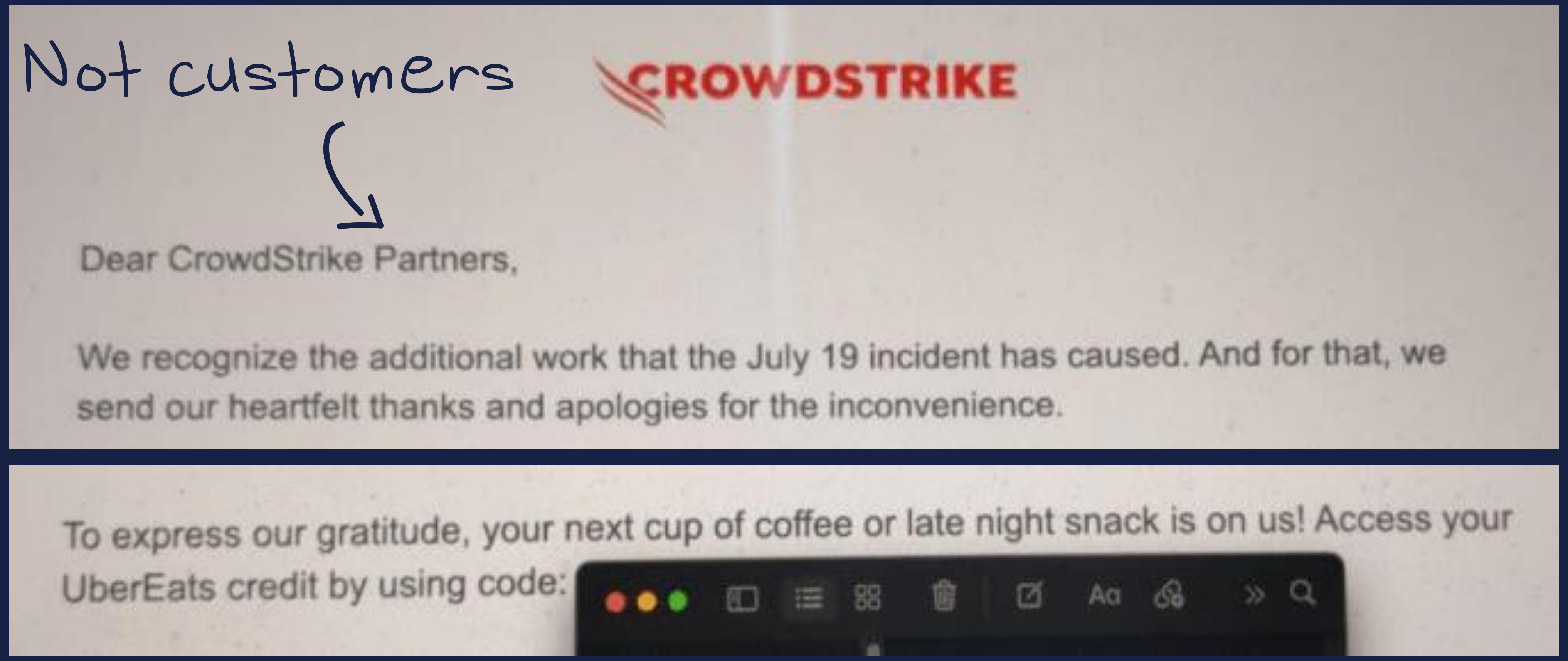
Threat actor claims: Anheuser-Busch, Mitsubishi, …

Future prediction

This kind of attack will continue, as long as there are sites relying on passwords only

Infostealer malware





Not customers

CROWDSTRIKE

Dear CrowdStrike Partners,

We recognize the additional work that the July 19 incident has caused. And for that, we send our heartfelt thanks and apologies for the inconvenience.

To express our gratitude, your next cup of coffee or late night snack is on us! Access your UberEats credit by using code:

July
19

Largest IT outage ever

Caused the exact thing that companies pay them to protect them from

8.5 million systems impacted with this CrowdStrike flu

Every single Windows machine that got the update got a blue screen of death. This means they didn't test it on a single Windows machine

So one lazy bastard??
They did test it on their own systems

To express their gratitude CrowdStrike gave a $10 Uber Eats voucher. Not kidding.

McAfee also 'pulled a CrowdStrike' in 2010 with svchost.exe
Guess who was the CTO?

BruCON 2024

The End

Conclusion

1. Teenage hackers with new skills will keep popping up
2. Days are over to rely on passwords without MFA
3. This will not stop. Next year will not be boring…

THREAT
EXPOSURE

We manage your attack surface

Presentation of today

🌐 threatexposure.eu/**brucon2024.pdf**

✉ dieter.vandenbosch@threatexposure.eu

in www.linkedin.com/in/vdbdieter/