Breaching Bad

Unpacking the Root Causes of recent Incidents

Petar 'Hetti' Kosic

11.10.24 – IT-SECX 2024

Classification: Public

whoami

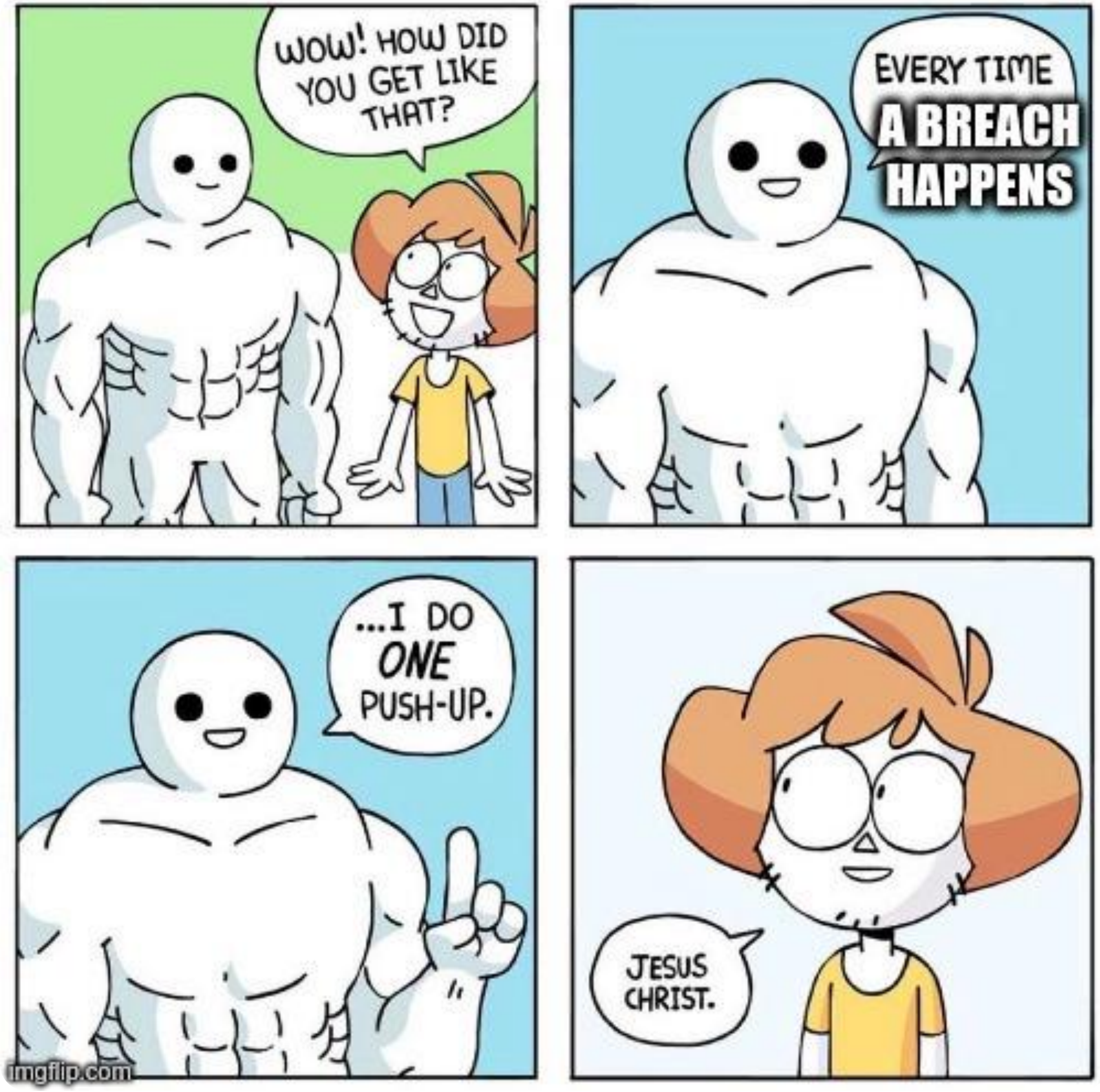
```
~ $ cat work.txt
    Offensive Security @ Erste Digital GmbH
~ $ cat freetime.txt
    Capture the Flag with We 0wn Y0u (TU Vienna)
    Hacking coffee machines
    Speaking at community conferences and camps
    hunTU - Scavenger hunt organisation
```

Another Day
Another Breach

News about breaches pop up regularly in the news.

Why do breaches happen?

A journey through four real life cases & lessons learned



Breach implication for companies

- Data loss
- Losing customers and reputation
- Business fraud
- GDPR and/or regulatory fines
- Rebuilding the complete infrastructure
- Downtime of production systems and/or manufacturing

CASE #1

Okta

Okta

Cloud-based access and identity management service provider

Well-known companies like 1Password and Cloudflare rely on them

Multiple IT security incidents occurred in the last years

Fact Box (2024)

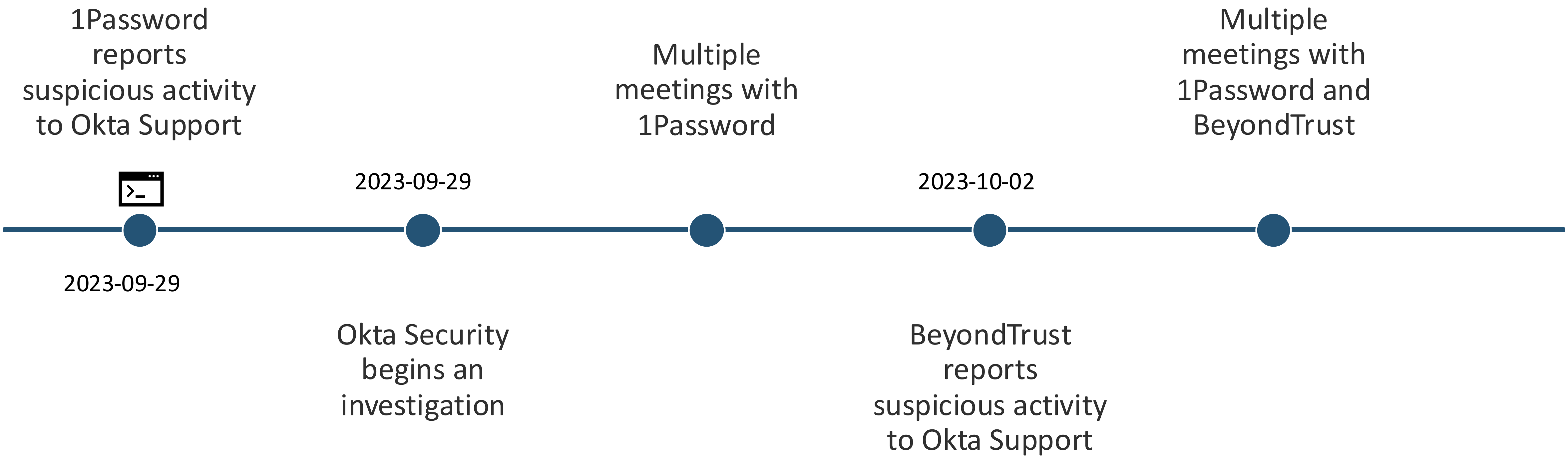
- San Francisco, US
- 6000
- $2,6 billion revenue

29 September 2023

1Password reports suspicious activity to Okta Support

Source: https://sec.okta.com/articles/2023/11/unauthorized-access-oktas-support-case-management-system-root-cause

Breach Timeline



1Password reports suspicious activity to Okta Support

2023-09-29

2023-09-29

Okta Security begins an investigation

Multiple meetings with 1Password

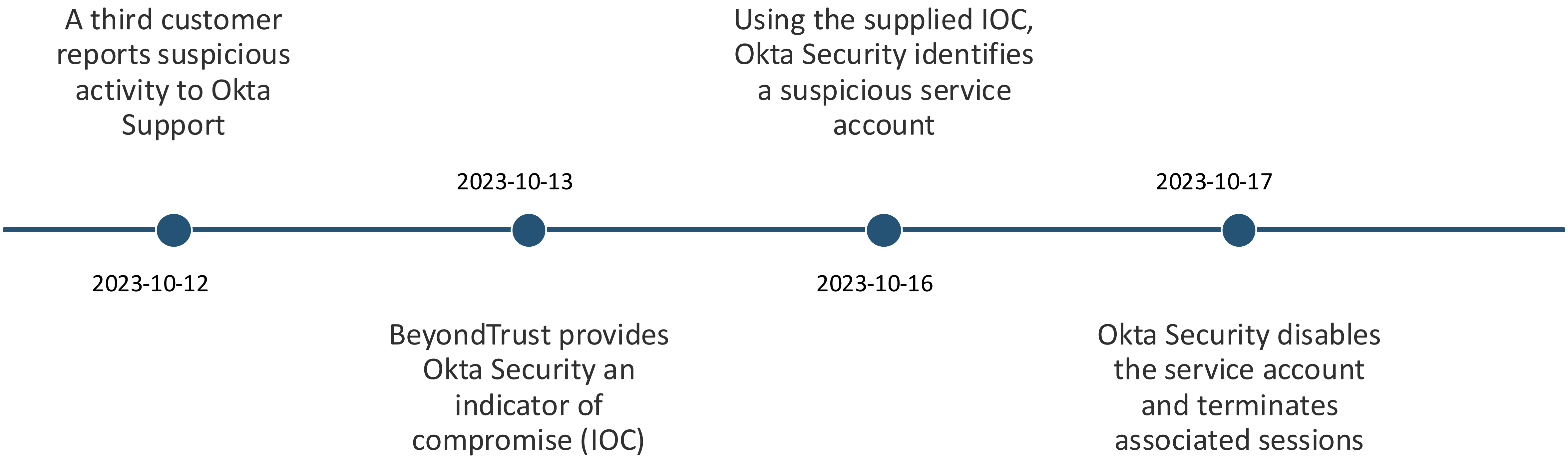
2023-10-02

BeyondTrust reports suspicious activity to Okta Support

Multiple meetings with 1Password and BeyondTrust

Source: https://sec.okta.com/articles/2023/11/unauthorized-access-oktas-support-case-management-system-root-cause

Breach Timeline



2023-10-12

A third customer reports suspicious activity to Okta Support

2023-10-13

BeyondTrust provides Okta Security an indicator of compromise (IOC)

2023-10-16

Using the supplied IOC, Okta Security identifies a suspicious service account

2023-10-17

Okta Security disables the service account and terminates associated sessions

Source: https://sec.okta.com/articles/2023/11/unauthorized-access-oktas-support-case-management-system-root-cause

What was breached?

Okta's customer support system

Customers provide HTTP Archive (HAR) files within support cases

HAR files can contain session tokens

Source: https://sec.okta.com/articles/2023/11/unauthorized-access-oktas-support-case-management-system-root-cause

How was it breached?

Access via internal service account

Employee had signed-in to their personal Google profile on the Chrome browser of their Okta-managed laptop

Credentials of service account saved in personal Google account

Assumption: Employees Google account or private computer compromised

Source: https://sec.okta.com/articles/2023/11/unauthorized-access-oktas-support-case-management-system-root-cause

Lessons Learned: Root Causes

Insufficient device management

➡️ Prevent technically the usage of private accounts

Missing awareness regarding private and personal account separation

➡️ Awareness trainings for employees

CASE #2

Cloudflare

Cloudflare

Provides various security products
(Cloud, DDoS Protection, CDN)

Releases excellent post-mortem analysis blog posts

Was breached due to Okta breach

Fact Box (2023)

California, US

3700

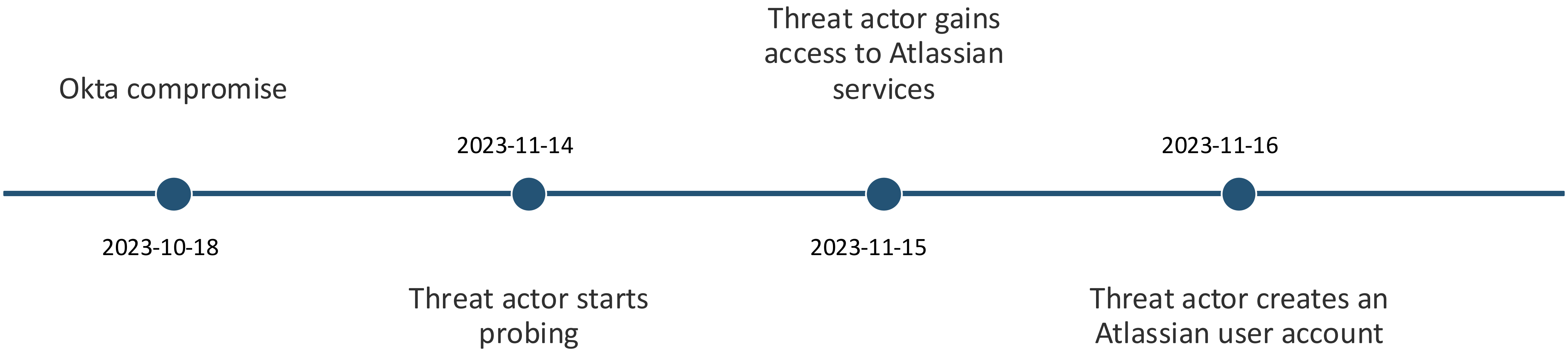
$1,3 billion revenue

23 November 2023

The Cloudflare security team receives an automated alert about a change at 15:58

Source: https://blog.cloudflare.com/thanksgiving-2023-security-incident

Breach Timeline



Okta compromise

2023-10-18

2023-11-14

Threat actor starts probing

Threat actor gains access to Atlassian services

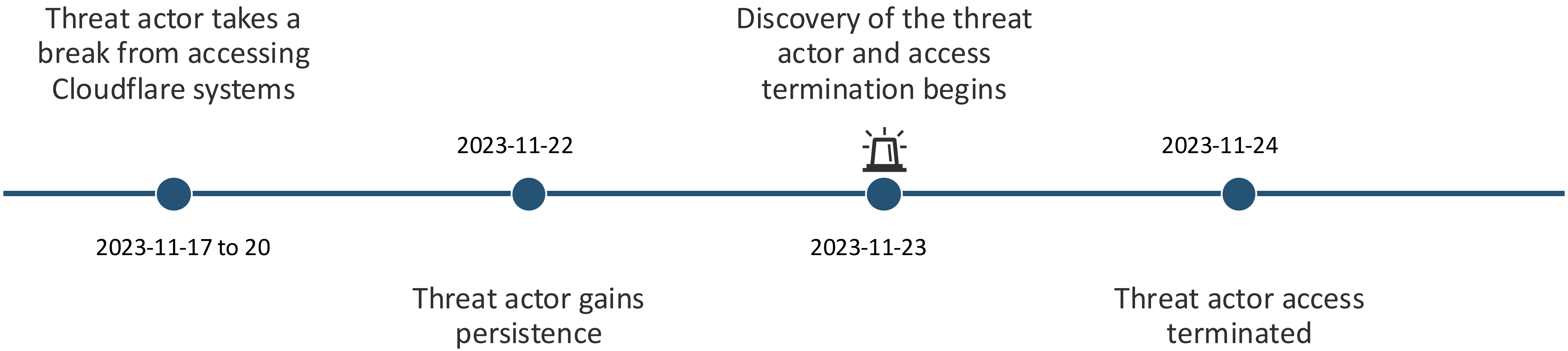
2023-11-15

2023-11-16

Threat actor creates an Atlassian user account

Source: https://blog.cloudflare.com/thanksgiving-2023-security-incident

Breach Timeline



2023-11-17 to 20

Threat actor takes a break from accessing Cloudflare systems

2023-11-22

Threat actor gains persistence

🚨 2023-11-23

Discovery of the threat actor and access termination begins

2023-11-24

Threat actor access terminated

Source: https://blog.cloudflare.com/thanksgiving-2023-security-incident

Why was this breach possible?

Cloudflare failed to rotate 1 service token and 3 service accounts after Okta breach

- AWS service account
- Bitbucket service account
- Jira service account
- Confluence service token

It was mistakenly believed that those accounts were unused

Source: https://blog.cloudflare.com/thanksgiving-2023-security-incident

Lesson Learned: Root Causes

Assumptions instead of verification

➡ Always verify assumptions and provided information

Failure of complete credential rotation after 3rd party breach

➡ Credential documentation + full credential rotation after breaches

Aftermath

Rotation of over 5000 individual credentials

Performed forensic triages on 4893 systems

Reimaged (!) and rebooted every machine in their global network

Source: https://blog.cloudflare.com/thanksgiving-2023-security-incident

Supply Chain Attacks are the new normal

CASE #3

LockBit

LockBit

Ransomware group

Ransomware as a Service (RaaS)

Leaking data of conducted breaches

Fact Box (2020-2023)

🌐 Unknown

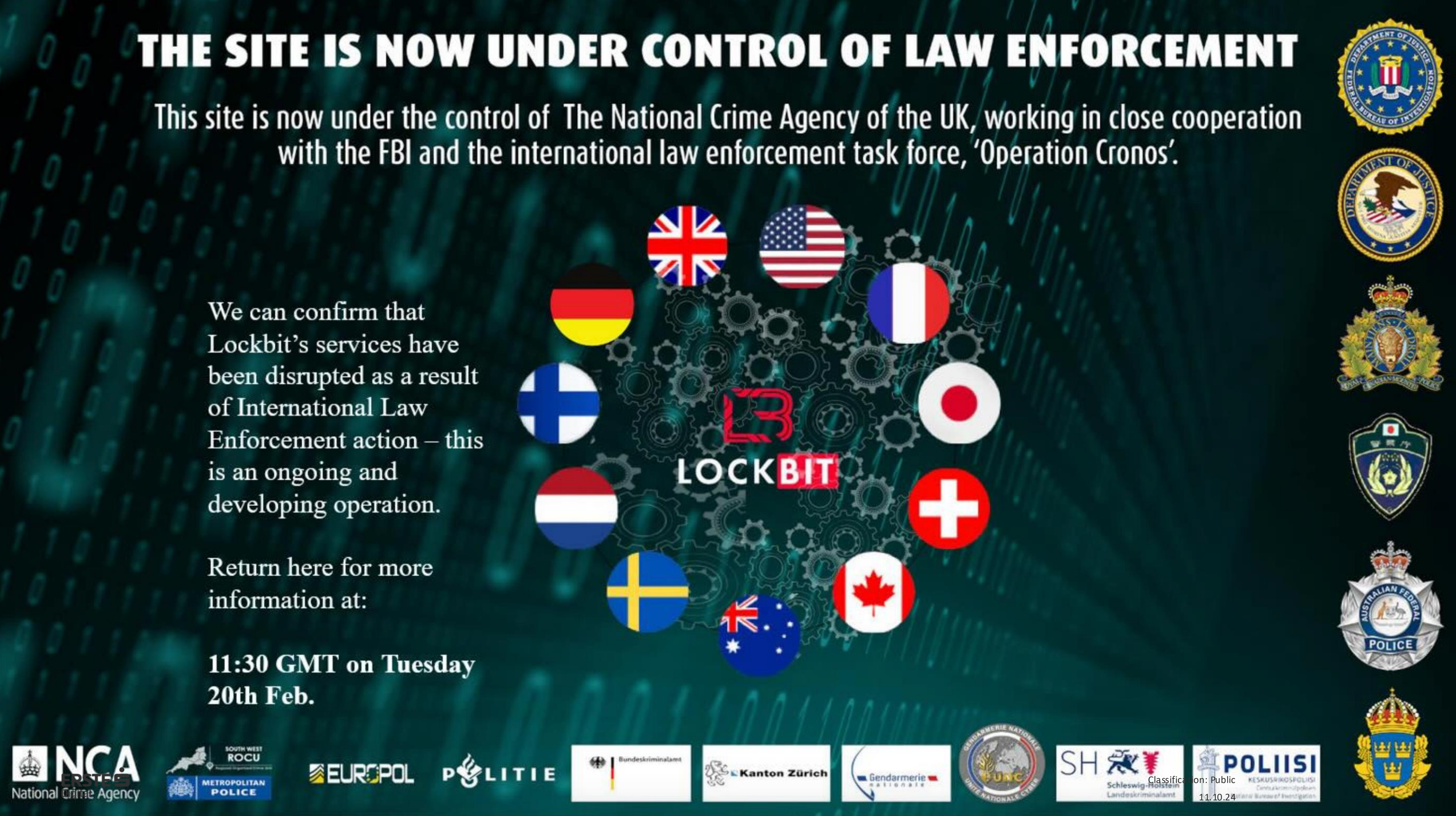
👥 Unknown

💰 $91 million revenue (US)

Source: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a

2024-02-19 16:00 ET

Operation Cronos



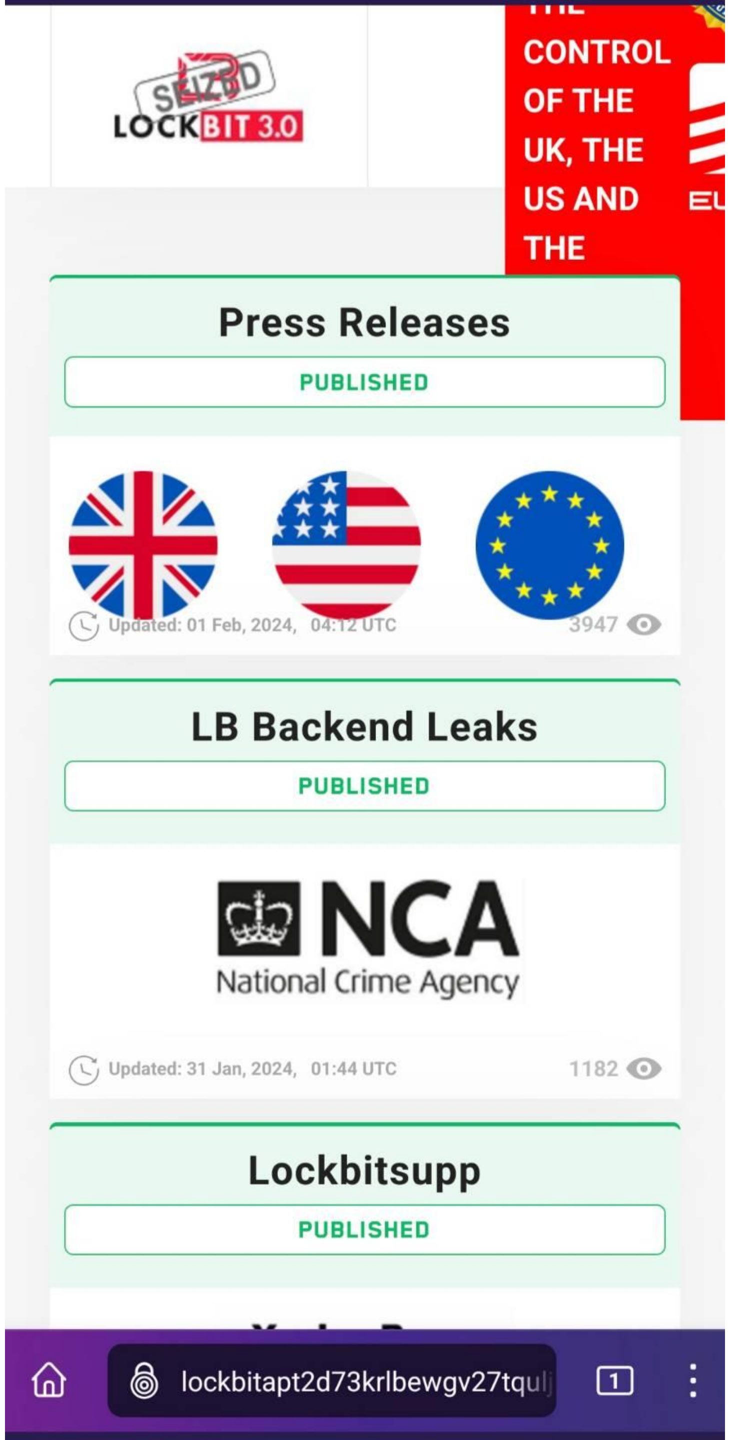
THE SITE IS NOW UNDER CONTROL OF LAW ENFORCEMENT

This site is now under the control of The National Crime Agency of the UK, working in close cooperation with the FBI and the international law enforcement task force, 'Operation Cronos'.

We can confirm that Lockbit's services have been disrupted as a result of International Law Enforcement action – this is an ongoing and developing operation.

Return here for more information at:

11:30 GMT on Tuesday 20th Feb.



THE CONTROL OF THE UK, THE US AND THE

Press Releases

PUBLISHED

Updated: 01 Feb, 2024, 04:12 UTC 3947

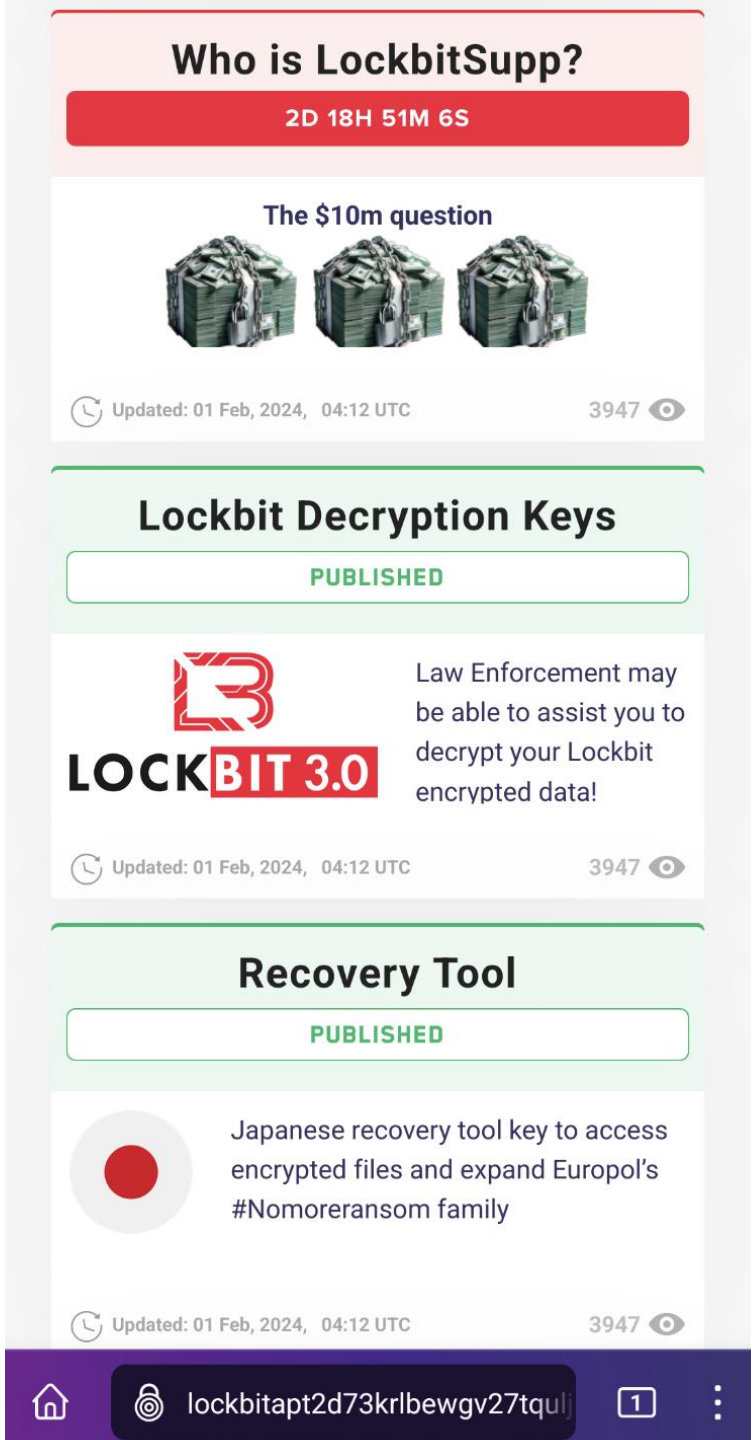
LB Backend Leaks

PUBLISHED

Updated: 31 Jan, 2024, 01:44 UTC 1182

Lockbitsupp

PUBLISHED



Who is LockbitSupp?

2D 18H 51M 6S

The $10m question

Updated: 01 Feb, 2024, 04:12 UTC 3947

Lockbit Decryption Keys

PUBLISHED

Law Enforcement may be able to assist you to decrypt your Lockbit encrypted data!

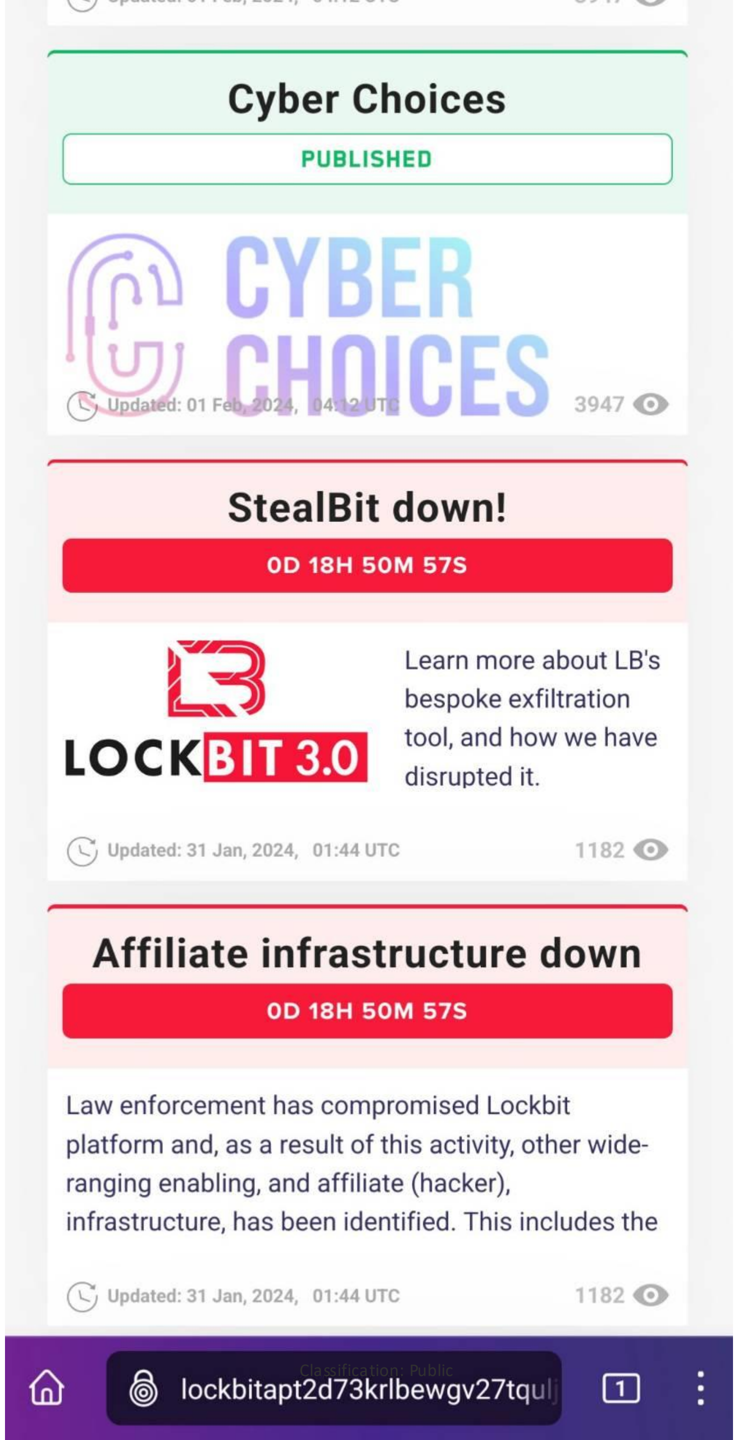
Updated: 01 Feb, 2024, 04:12 UTC 3947

Recovery Tool

PUBLISHED

Japanese recovery tool key to access encrypted files and expand Europol's #Nomoreransom family

Updated: 01 Feb, 2024, 04:12 UTC 3947



Cyber Choices

PUBLISHED

Updated: 01 Feb, 2024, 04:12 UTC 3947

StealBit down!

0D 18H 50M 57S

Learn more about LB's bespoke exfiltration tool, and how we have disrupted it.

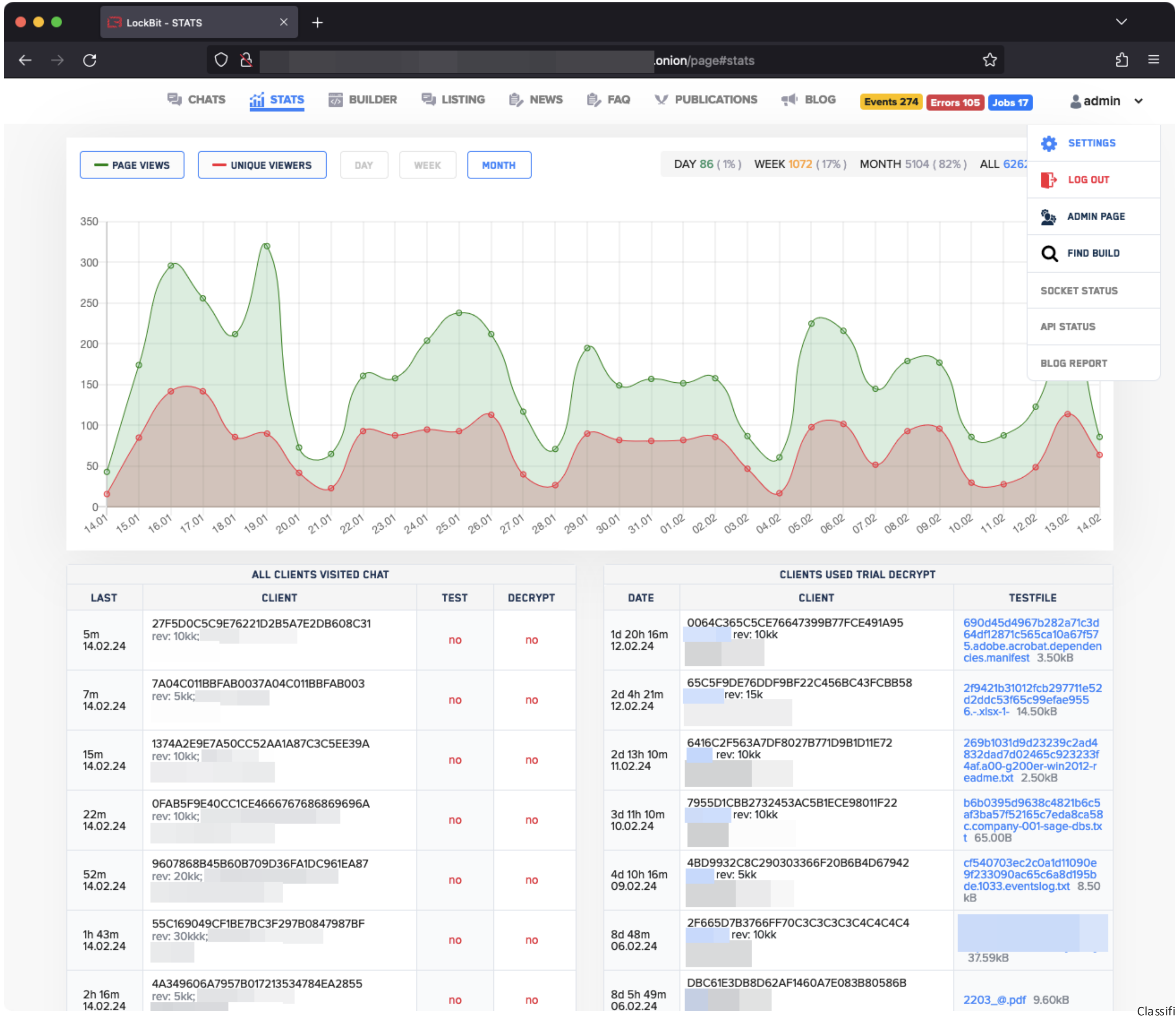
Updated: 31 Jan, 2024, 01:44 UTC 1182

Affiliate infrastructure down

0D 18H 50M 57S

Law enforcement has compromised Lockbit platform and, as a result of this activity, other wide-ranging enabling, and affiliate (hacker), infrastructure, has been identified. This includes the

Updated: 31 Jan, 2024, 01:44 UTC 1182



DAY 86 (1%) WEEK 1072 (17%) MONTH 5104 (82%) ALL 626

ALL CLIENTS VISITED CHAT

LAST	CLIENT	TEST	DECRYPT
5m 14.02.24	27F5D0C5C9E76221D2B5A7E2DB608C31 rev: 10kk; [redacted]	no	no
7m 14.02.24	7A04C011BBFAB0037A04C011BBFAB003 rev: 5kk; [redacted]	no	no
15m 14.02.24	1374A2E9E7A50CC52AA1A87C3C5EE39A rev: 10kk; [redacted]	no	no
22m 14.02.24	0FAB5F9E40CC1CE46667676868669696A rev: 10kk; [redacted]	no	no
52m 14.02.24	9607868B45B60B709D36FA1DC961EA87 rev: 20kk; [redacted]	no	no
1h 43m 14.02.24	55C169049CF1BE7BC3F297B0847987BF rev: 30kkk; [redacted]	no	no
2h 16m 14.02.24	4A349606A7957B017213534784EA2855 rev: 5kk; [redacted]	no	no

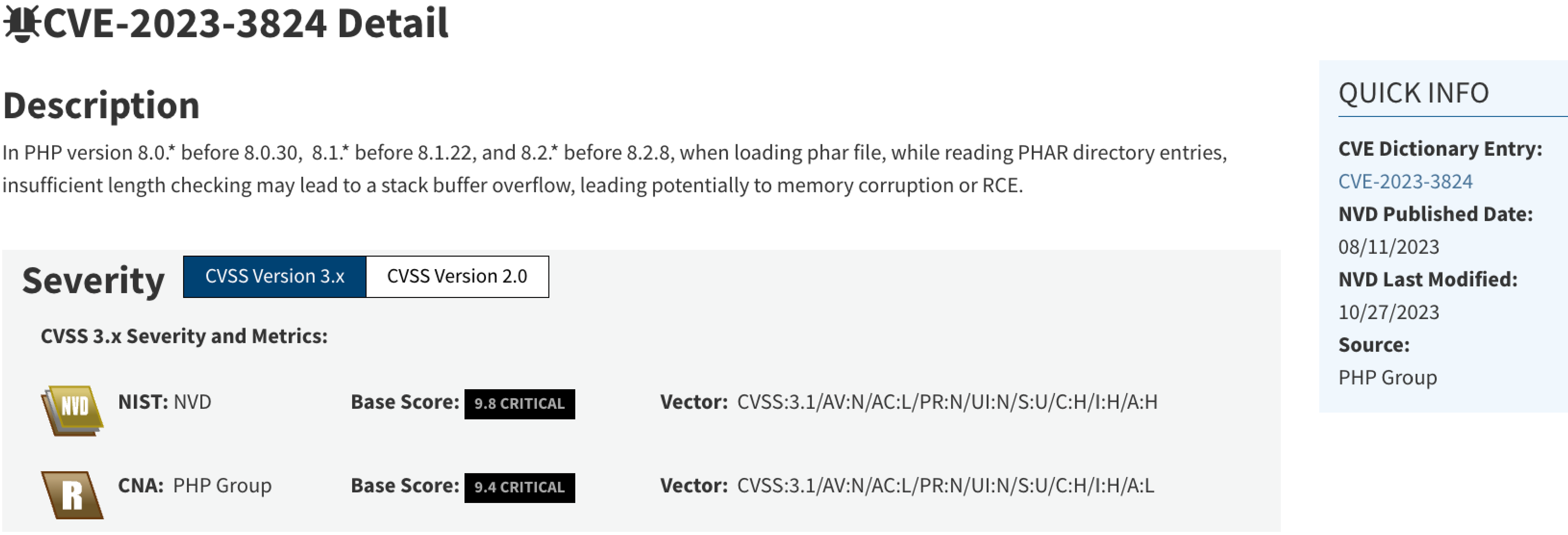
CLIENTS USED TRIAL DECRYPT

DATE	CLIENT	TESTFILE
1d 20h 16m 12.02.24	0064C365C5CE76647399B77FCE491A95 [redacted] rev: 10kk	690d45d4967b282a71c3d64df12871c565ca10a67f575.adobe.acrobat.dependencies.manifest 3.50kB
2d 4h 21m 12.02.24	65C5F9DE76DDF9BF22C456BC43FCBB58 [redacted] rev: 15k	2f9421b31012fcb297711e52d2ddc53f65c99efae9556.-.xlsx-1- 14.50kB
2d 13h 10m 11.02.24	6416C2F563A7DF8027B771D9B1D11E72 [redacted] rev: 10kk	269b1031d9d23239c2ad4832dad7d02465c923233f4af.a00-g200er-win2012-readme.txt 2.50kB
3d 11h 10m 10.02.24	7955D1CBB2732453AC5B1ECE98011F22 [redacted] rev: 10kk	b6b0395d9638c4821b6c5af3ba57f52165c7eda8ca58c.company-001-sage-dbs.txt 65.00B
4d 10h 16m 09.02.24	4BD9932C8C290303366F20B6B4D67942 [redacted] rev: 5kk	cf540703ec2c0a1d11090e9f233090ac65c6a8d195bde.1033.eventslog.txt 8.50 kB
8d 48m 06.02.24	2F665D7B3766FF70C3C3C3C3C4C4C4C4 [redacted] rev: 10kk	[redacted] 37.59kB
8d 5h 49m 06.02.24	DBC61E3DB8D62AF1460A7E083B80586B [redacted]	2203_@.pdf 9.60kB

Picture Source: NCA / Europol

How did LockBit get breached?

Might be due to:



CVE-2023-3824 Detail

Description

In PHP version 8.0.* before 8.0.30, 8.1.* before 8.1.22, and 8.2.* before 8.2.8, when loading phar file, while reading PHAR directory entries, insufficient length checking may lead to a stack buffer overflow, leading potentially to memory corruption or RCE.

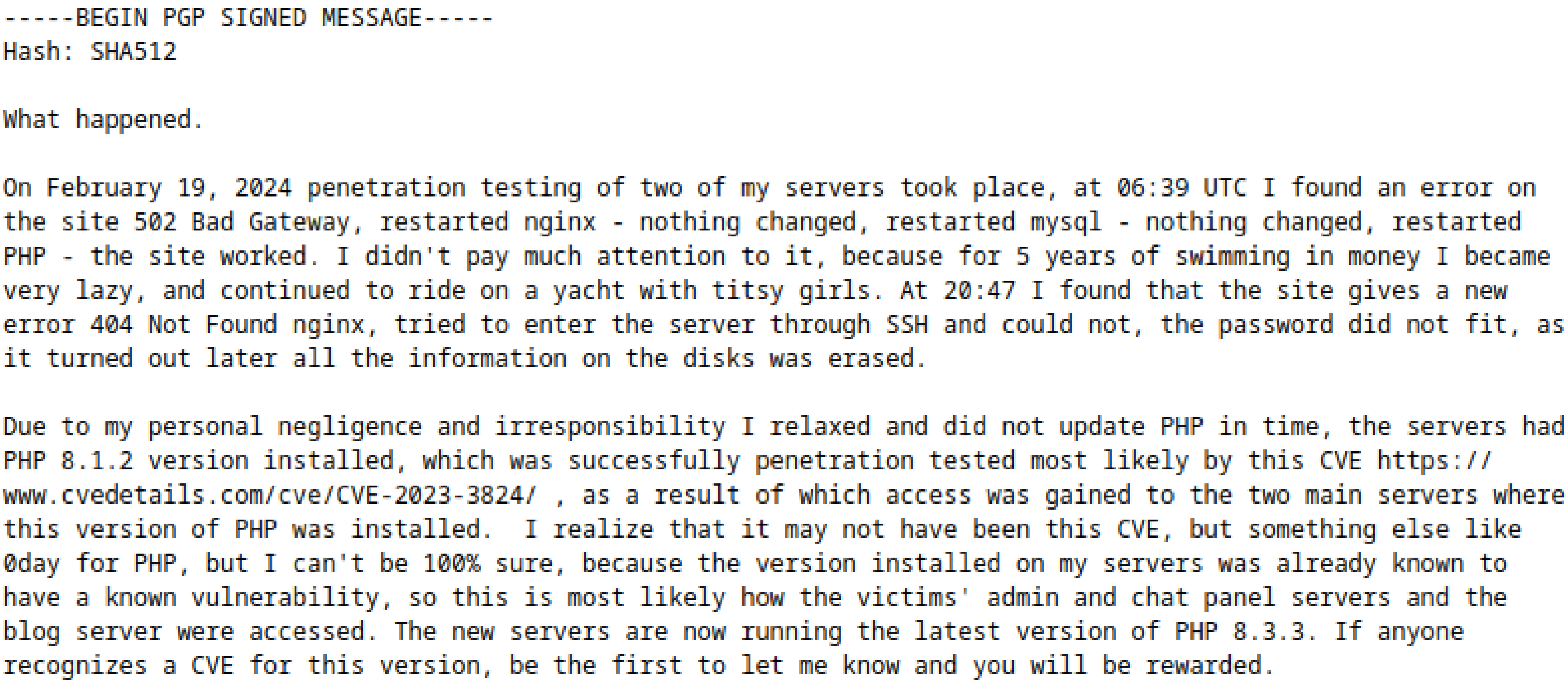
Severity

CVSS 3.x Severity and Metrics:

NIST: NVD	**Base Score:** 9.8 CRITICAL	**Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CNA: PHP Group	**Base Score:** 9.4 CRITICAL	**Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L

QUICK INFO

CVE Dictionary Entry:
CVE-2023-3824
NVD Published Date:
08/11/2023
NVD Last Modified:
10/27/2023
Source:
PHP Group



-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

What happened.

On February 19, 2024 penetration testing of two of my servers took place, at 06:39 UTC I found an error on the site 502 Bad Gateway, restarted nginx - nothing changed, restarted mysql - nothing changed, restarted PHP - the site worked. I didn't pay much attention to it, because for 5 years of swimming in money I became very lazy, and continued to ride on a yacht with titsy girls. At 20:47 I found that the site gives a new error 404 Not Found nginx, tried to enter the server through SSH and could not, the password did not fit, as it turned out later all the information on the disks was erased.

Due to my personal negligence and irresponsibility I relaxed and did not update PHP in time, the servers had PHP 8.1.2 version installed, which was successfully penetration tested most likely by this CVE https://www.cvedetails.com/cve/CVE-2023-3824/ , as a result of which access was gained to the two main servers where this version of PHP was installed. I realize that it may not have been this CVE, but something else like 0day for PHP, but I can't be 100% sure, because the version installed on my servers was already known to have a known vulnerability, so this is most likely how the victims' admin and chat panel servers and the blog server were accessed. The new servers are now running the latest version of PHP 8.3.3. If anyone recognizes a CVE for this version, be the first to let me know and you will be rewarded.

Lesson Learned: Root Causes

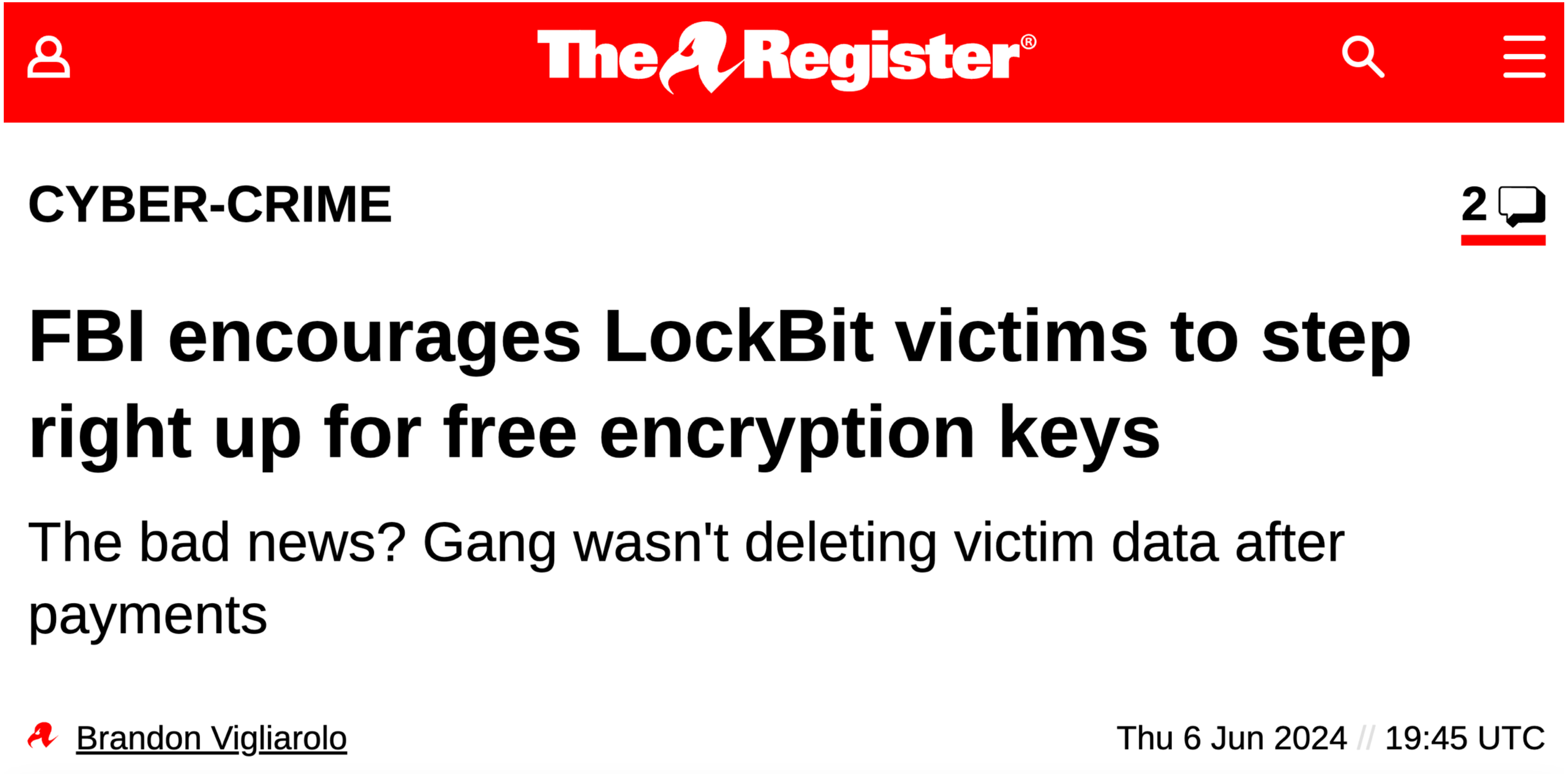
Being criminal

➡️ Don't be criminal – stay legal; companies are searching for talents

Critical software patches missing

➡️ Implement patch management

Fast forward to June



CYBER-CRIME

2

FBI encourages LockBit victims to step right up for free encryption keys

The bad news? Gang wasn't deleting victim data after payments

Brandon Vigliarolo

Thu 6 Jun 2024 // 19:45 UTC

Source: https://www.theregister.com/2024/06/06/lockbit_fbi_decryption_key/

Investing in #Security beforehand will be cheaper in the long run

CASE #4

Microsoft

Microsoft

Offers cloud infrastructure and security services

Customers:
consumers, enterprises and governments

Very valuable target for criminals and nation state actors

Fact Box (2023)

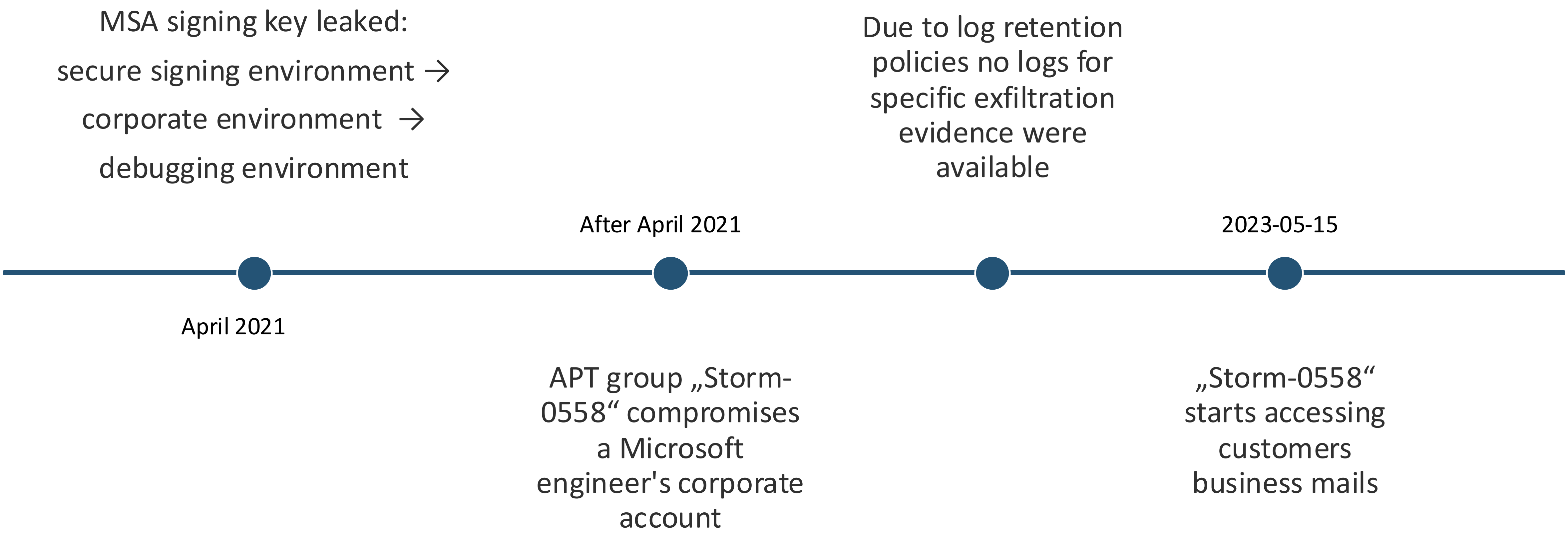
- Washington, US
- 221.000
- $212 billion revenue

16 June 2023

A customer notified Microsoft about anomalous Exchange Online data access

Source: https://www.microsoft.com/en-us/security/blog/2023/07/14/analysis-of-storm-0558-techniques-for-unauthorized-email-access/

Breach Timeline



April 2021

MSA signing key leaked:

secure signing environment →

corporate environment →

debugging environment

After April 2021

APT group „Storm-0558“ compromises a Microsoft engineer's corporate account

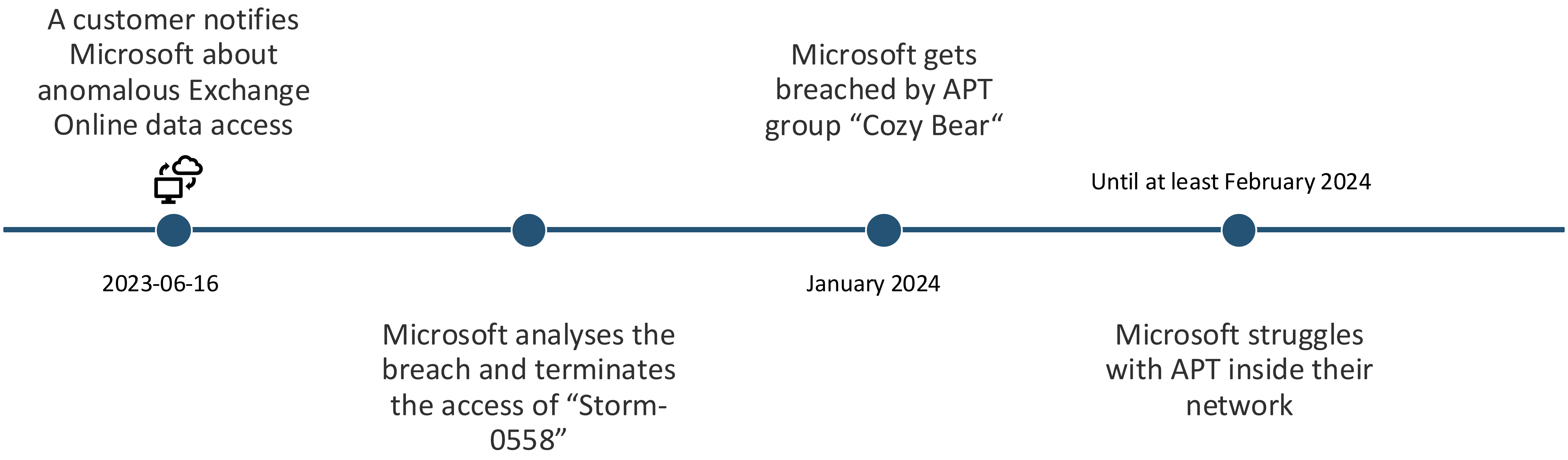
Due to log retention policies no logs for specific exfiltration evidence were available

2023-05-15

„Storm-0558“ starts accessing customers business mails

Source: https://msrc.microsoft.com/blog/2023/09/results-of-major-technical-investigations-for-storm-0558-key-acquisition/

Breach Timeline



A customer notifies Microsoft about anomalous Exchange Online data access

2023-06-16

Microsoft analyses the breach and terminates the access of “Storm-0558”

Microsoft gets breached by APT group “Cozy Bear“

January 2024

Until at least February 2024

Microsoft struggles with APT inside their network

Source: https://www.microsoft.com/en-us/security/blog/2023/07/14/analysis-of-storm-0558-techniques-for-unauthorized-email-access/

Signing keys and access with forged tokens

Key types:

- Microsoft account (MSA) consumer signing key
- Azure AD (enterprise) signing keys

Authentication tokens were forged with MSA keys

Enterprise mails were successfully accessed with those forged tokens

Source: https://msrc.microsoft.com/blog/2023/07/microsoft-mitigates-china-based-threat-actor-storm-0558-targeting-of-customer-email/

WHY DOES A CONSUMER KEY
HAVE ACCESS TO ENTERPRISE MAILS
imgflip.com

”

> Developers in the mail system incorrectly assumed libraries performed complete validation and did not add the required issuer/scope validation. Thus, the mail system would accept a request for enterprise email using a security token signed with the consumer key.

“

Microsoft Security Response Center (MSRC)

Source: https://msrc.microsoft.com/blog/2023/09/results-of-major-technical-investigations-for-storm-0558-key-acquisition/

Lesson Learned: Root Causes

Insufficient secret filters on critical paths

➡️ Prevent secret leakage with proper filtering

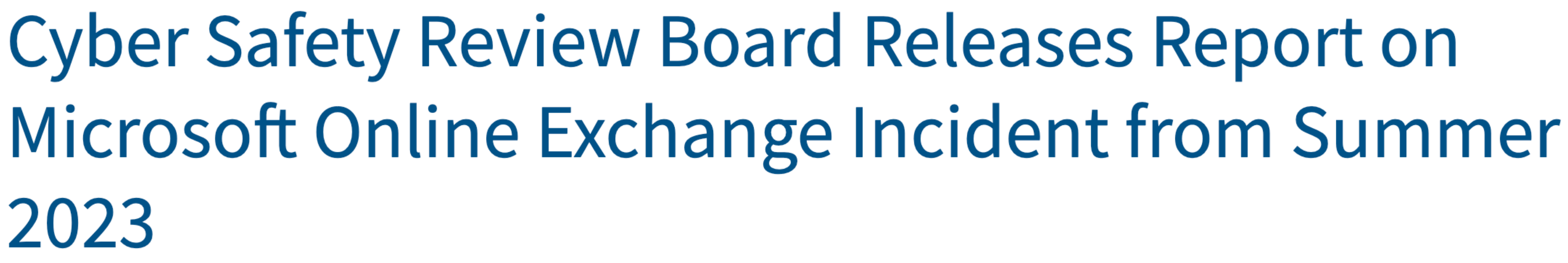
Assumptions instead of verification (again)

➡️ Always verify assumptions and provided information

Missing validation of authentication data

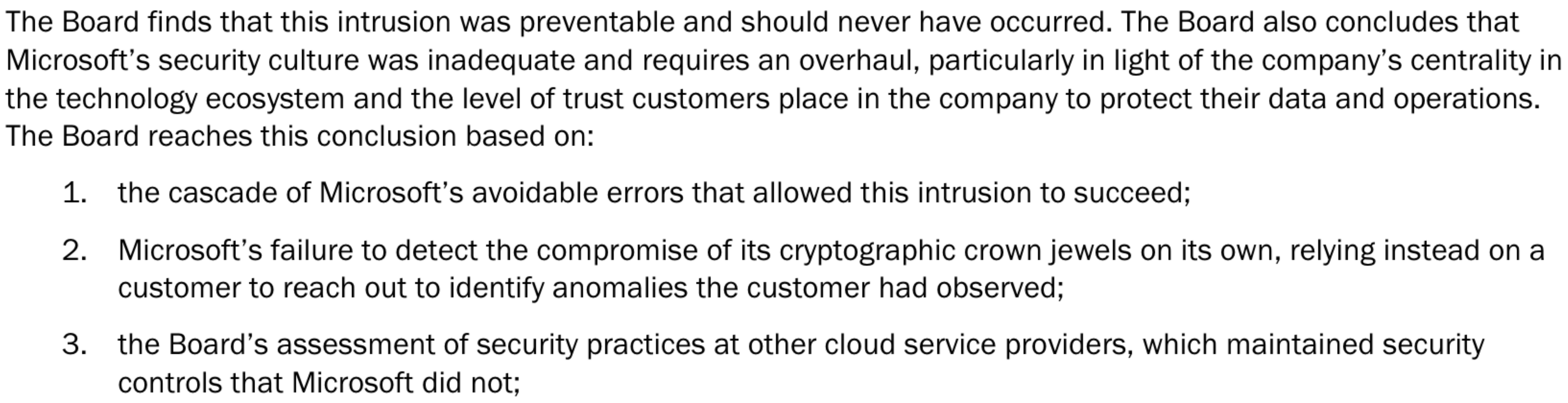
➡️ Stringent validation of authentication & authorization data at every stage

Aftermath



Cyber Safety Review Board Releases Report on Microsoft Online Exchange Incident from Summer 2023

Excerpt:



The Board finds that this intrusion was preventable and should never have occurred. The Board also concludes that Microsoft's security culture was inadequate and requires an overhaul, particularly in light of the company's centrality in the technology ecosystem and the level of trust customers place in the company to protect their data and operations. The Board reaches this conclusion based on:

1. the cascade of Microsoft's avoidable errors that allowed this intrusion to succeed;
2. Microsoft's failure to detect the compromise of its cryptographic crown jewels on its own, relying instead on a customer to reach out to identify anomalies the customer had observed;
3. the Board's assessment of security practices at other cloud service providers, which maintained security controls that Microsoft did not;

Sources: https://www.cisa.gov/sites/default/files/2024-04/CSRB_Review_of_the_Summer_2023_MEO_Intrusion_Final_508c.pdf
https://www.cisa.gov/resources-tools/resources/cyber-safety-review-board-releases-report-microsoft-online-exchange-incident-summer-2023
Microsoft Statement: https://blogs.microsoft.com/on-the-issues/2024/06/13/microsofts-work-to-strengthen-cybersecurity-protection/

RECAP

Lessons learned

Recap - Lessons Learned

- Never assume; always verify
- Patch your systems regularly
- Regularly conduct awareness trainings for employees
- Implement a comprehensive device management
- Rotate **all** credentials after breaches
- Analyse supply chain dependencies and their possible impacts
- Implement **Multi-Factor-Authentication** (MFA), for **everything** that is **externally reachable**

We are hiring!

Visit us at our booth for more information

Questions?

> „If it‘s reachable
> It‘s breachable“

Petar 'Hetti' Kosic
Offensive Security Expert

Thank You