CSE508 Network Security

Stony Brook University

2024-01-23

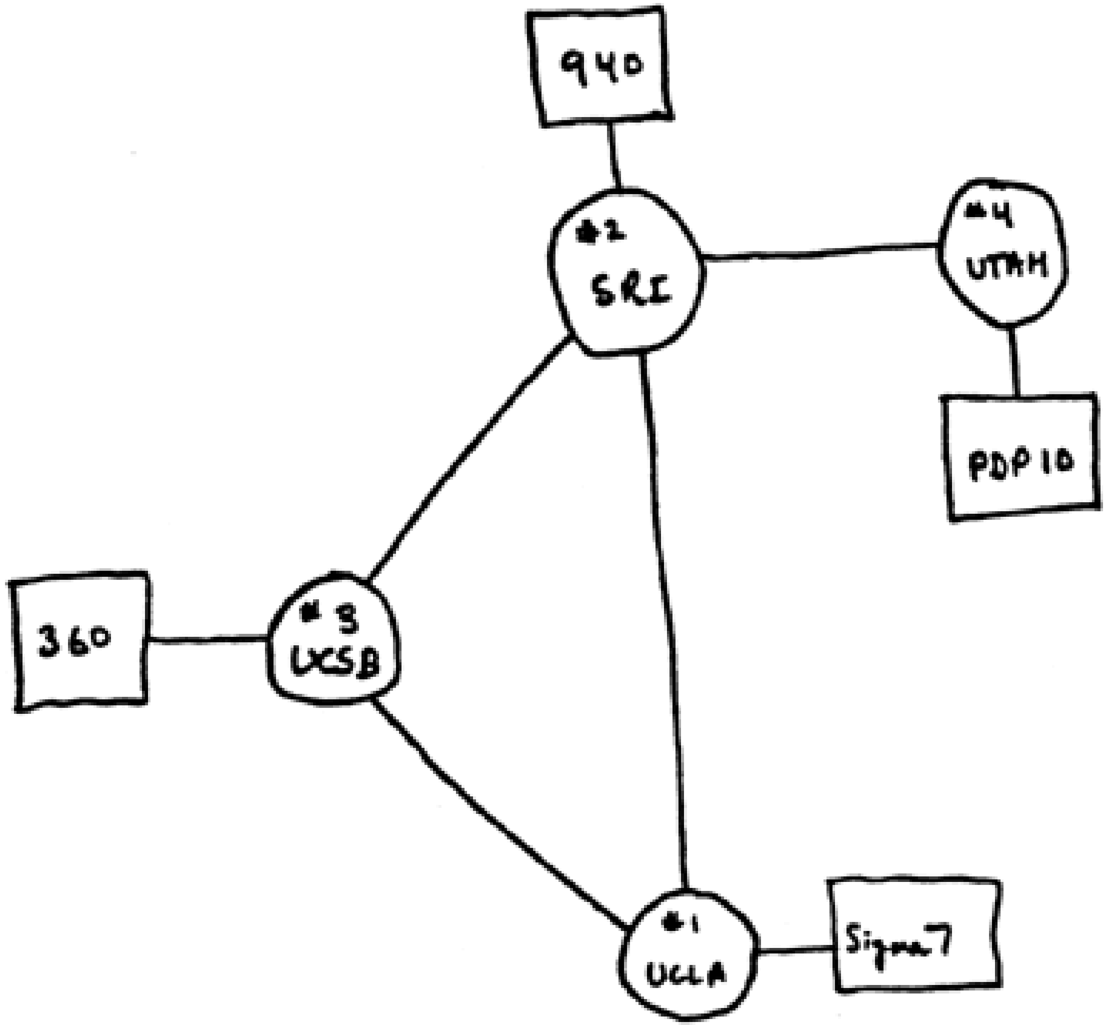
Introduction and Basic Concepts

Michalis Polychronakis

Stony Brook University

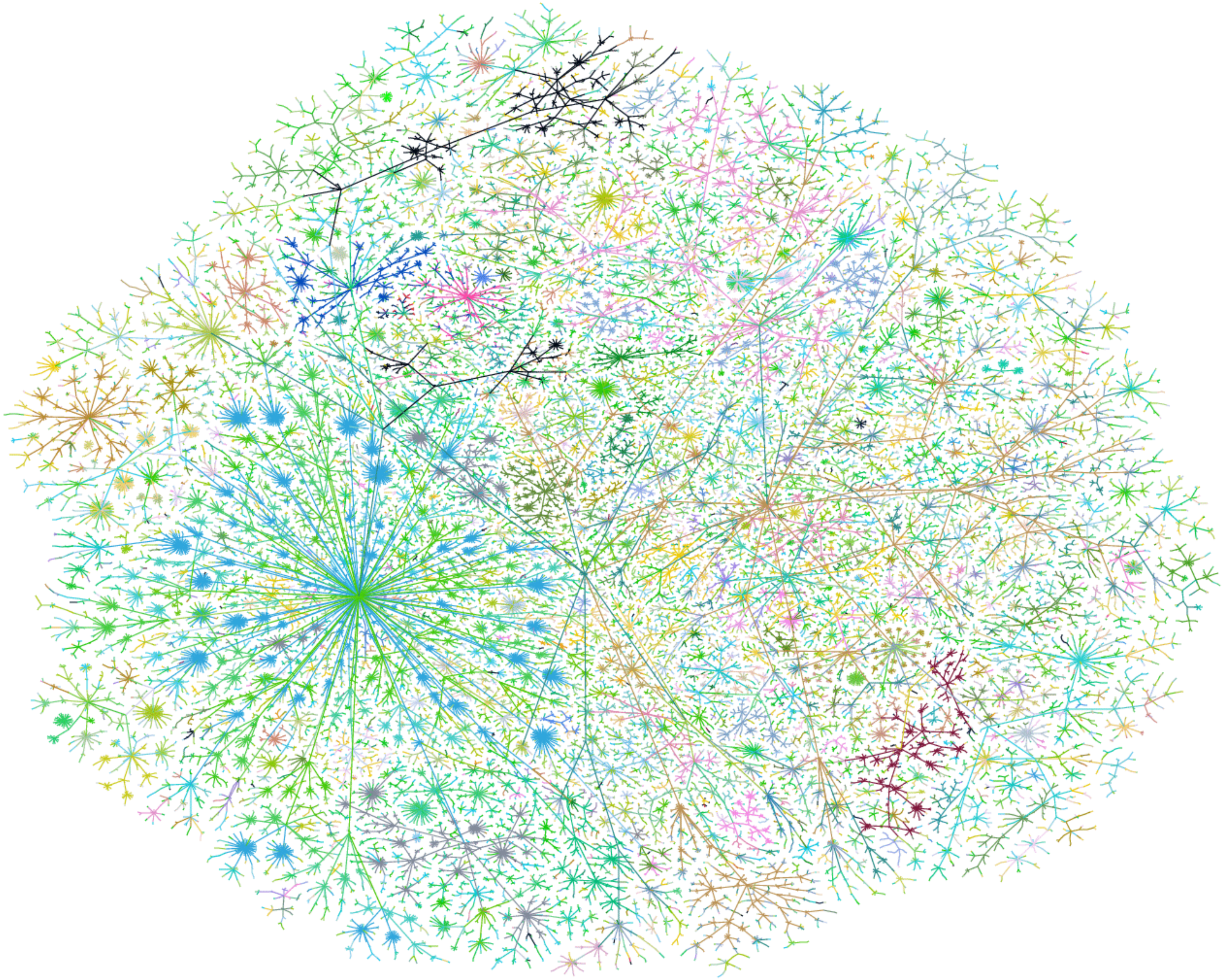
Why care about network security?

1969



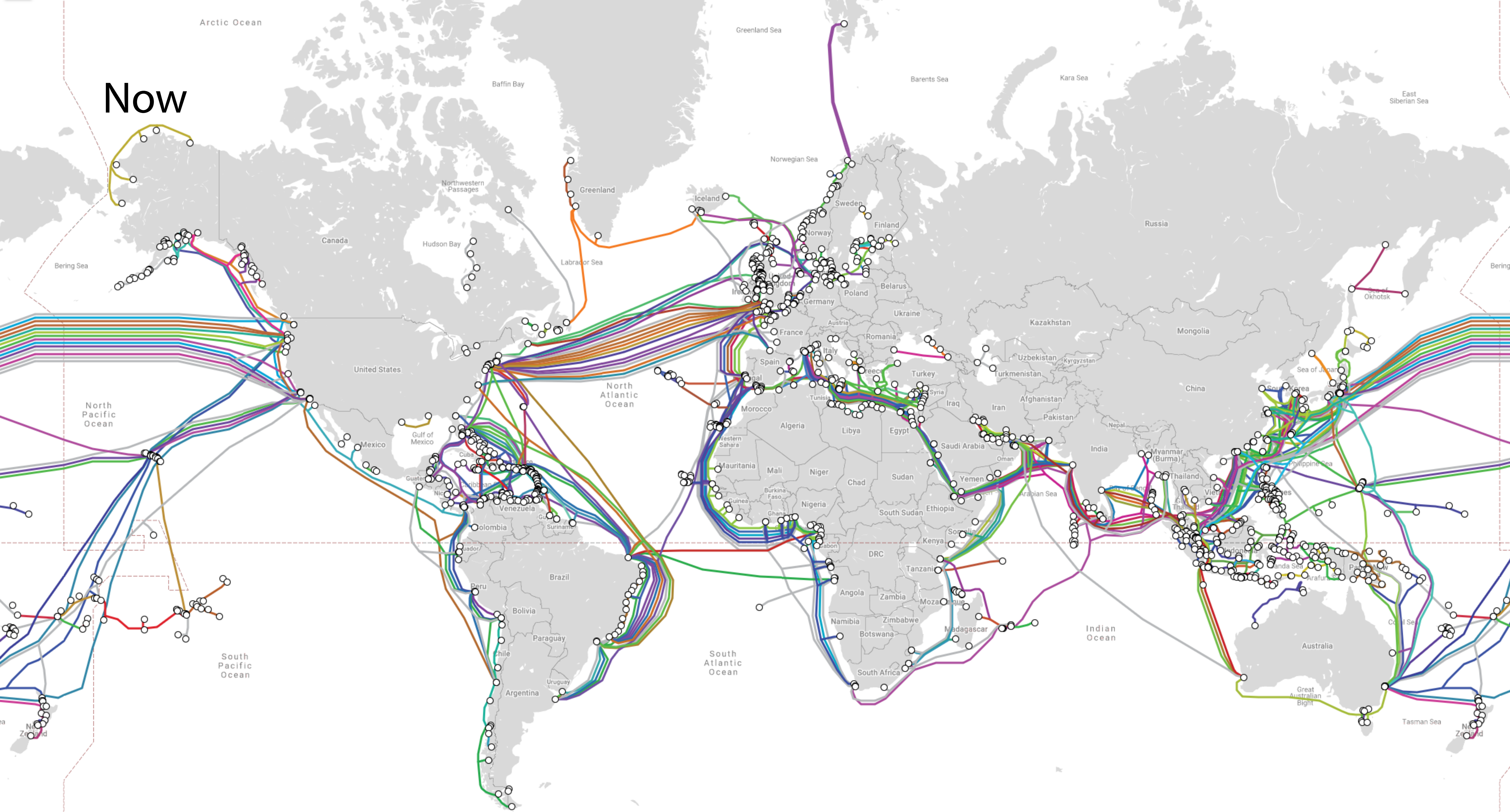
© 2004 Computer History Museum - http://www.computerhistory.org/internet_history/

1998



© Bill Cheswick - http://www.cheswick.com/ches/map/gallery/index.html

Now



© Submarine Cable Map – https://www.submarinecablemap.com/

Cisco Annual Internet Report -
https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html
Executive summary
Table of Contents
Executive summary
Trends
Appendices
For more information

Cisco Annual Internet Report (2018–2023) White Paper

Updated: March 9, 2020

Global Internet adoption and devices and connection

Internet users

Nearly two-thirds of the global population will have Internet access by 2023. There will be 5.3 billion total Internet users (66 percent of global population) by 2023, up from 3.9 billion (51 percent of global population) in 2018.

Devices and connections

The number of devices connected to IP networks will be more than three times the global population by 2023. There will be 3.6 networked devices per capita by 2023, up from 2.4 networked devices per capita in 2018. There will be 29.3 billion networked devices by 2023, up from 18.4 billion in 2018.

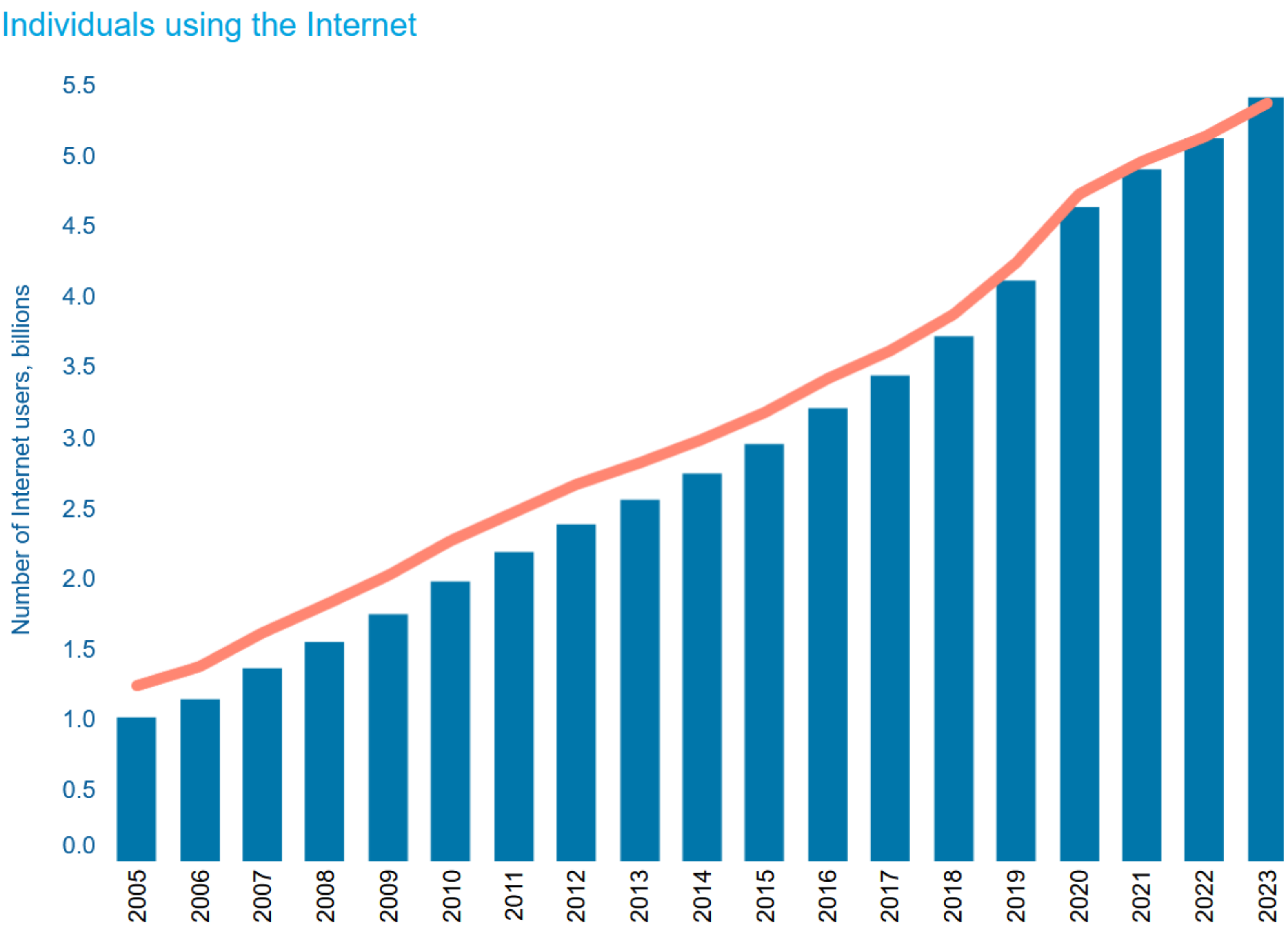
M2M connections will be half of the global connected devices and connections by 2023. The share of Machine-To-Machine (M2M) connections will grow from 33 percent in 2018 to 50 percent by 2023. There will be 14.7 billion M2M connections by 2023.

The consumer segment will have nearly three-fourths share of total devices and connections by 2023. Globally, consumer segment's share of total devices and connections will be 74 percent, with the business segment claiming the remaining 26 percent.

Internet of Things (IoT) by application

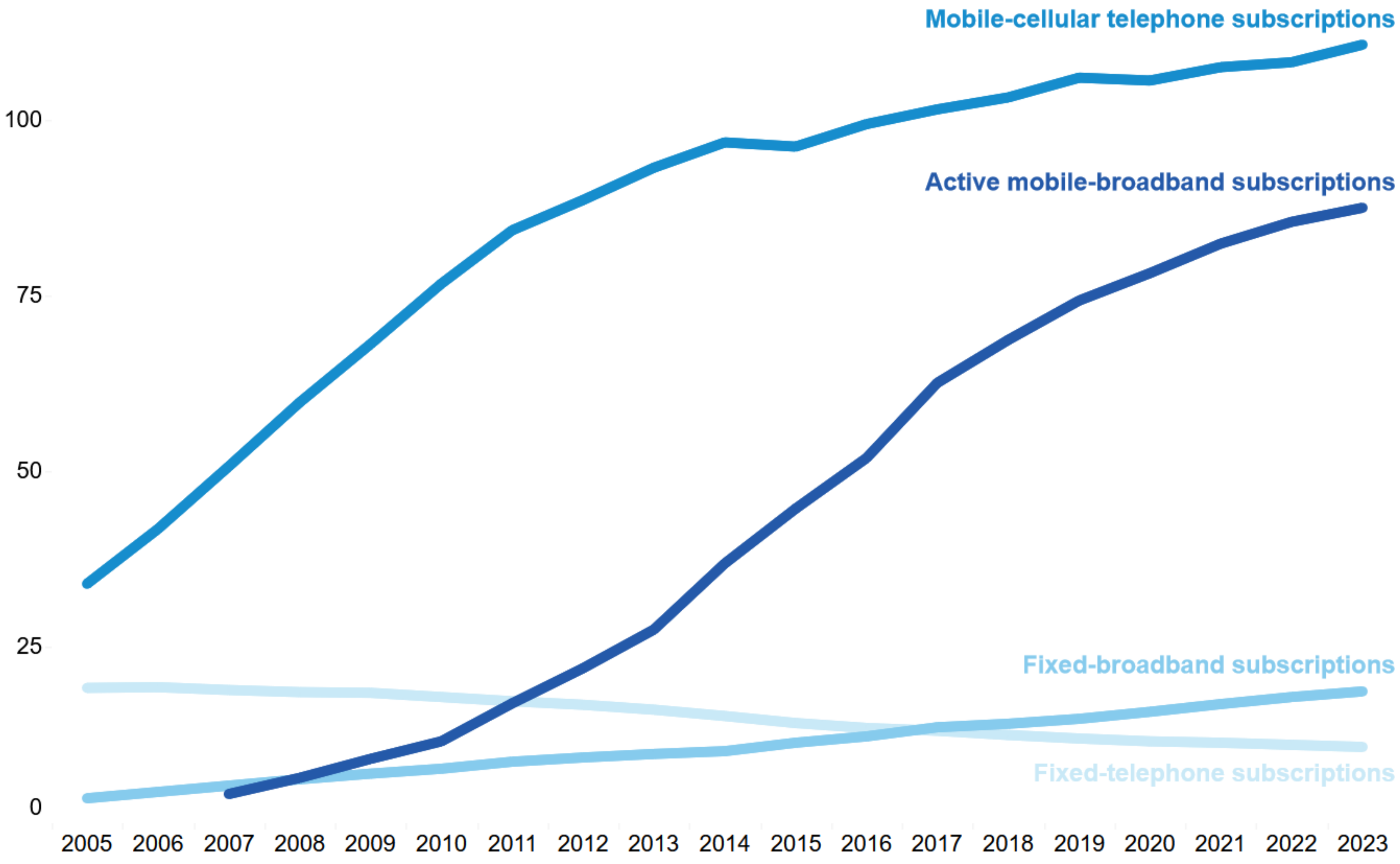
Within the M2M connections category (which is also referred to as IoT), **connected home applications will have the largest share and connected car will be the fastest growing application type**. Connected home applications will have nearly half or 48 percent of M2M share by 2023 and Connected car applications will grow the fastest at 30 percent CAGR over the forecast period (2018–2023).

Mobility growth

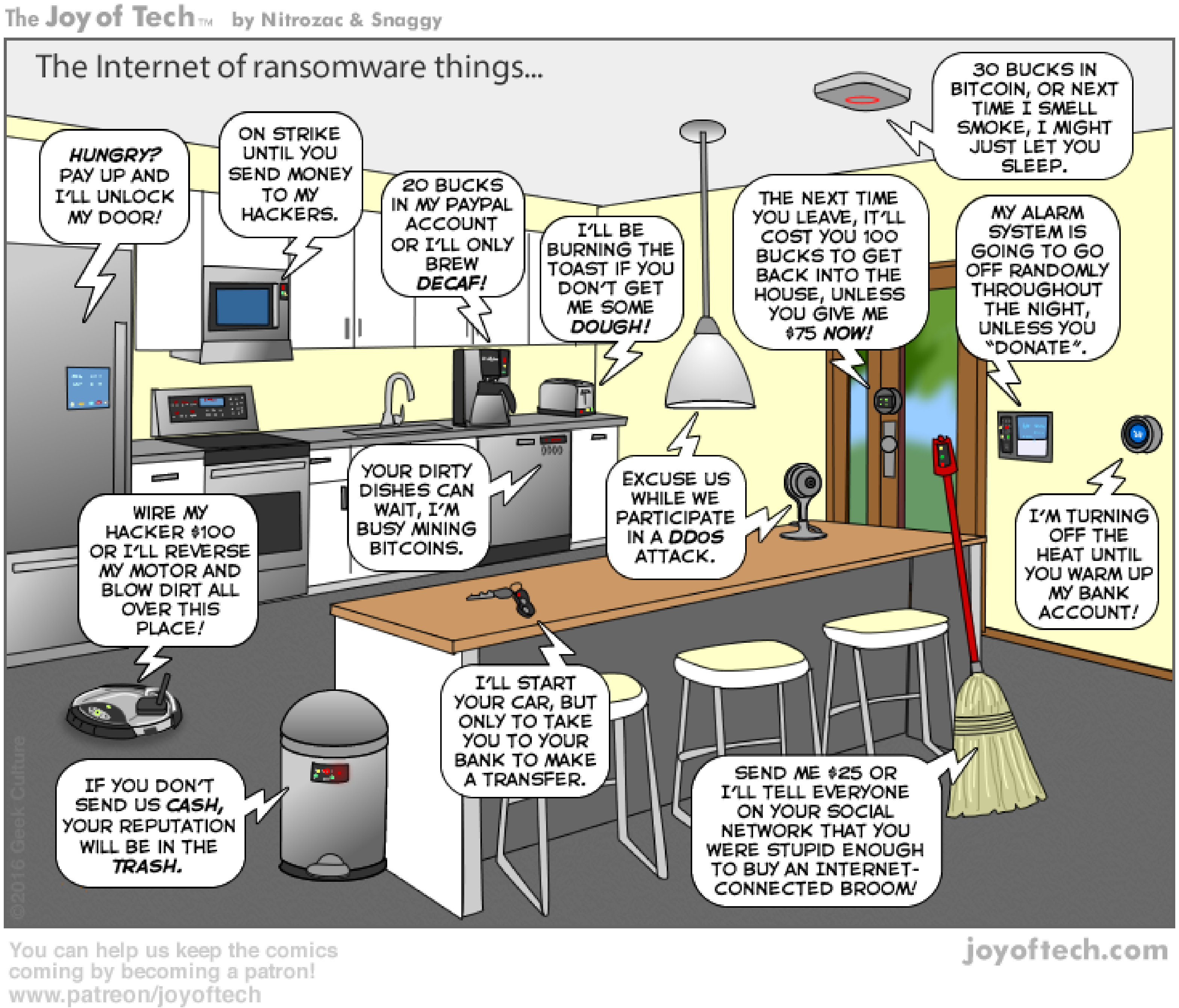


© ITU – https://www.itu.int/itu-d/reports/statistics/2023/10/10/ff23-internet-use/

Subscriptions per 100 inhabitants, world



© ITU – https://www.itu.int/itu-d/reports/statistics/2023/10/10/ff23-subscriptions/


The Joy of Tech™ by Nitrozac & Snaggy
The Internet of ransomware things...
HUNGRY? PAY UP AND I'LL UNLOCK MY DOOR!
ON STRIKE UNTIL YOU SEND MONEY TO MY HACKERS.
20 BUCKS IN MY PAYPAL ACCOUNT OR I'LL ONLY BREW DECAF!
I'LL BE BURNING THE TOAST IF YOU DON'T GET ME SOME DOUGH!
THE NEXT TIME YOU LEAVE, IT'LL COST YOU 100 BUCKS TO GET BACK INTO THE HOUSE, UNLESS YOU GIVE ME $75 NOW!
30 BUCKS IN BITCOIN, OR NEXT TIME I SMELL SMOKE, I MIGHT JUST LET YOU SLEEP.
MY ALARM SYSTEM IS GOING TO GO OFF RANDOMLY THROUGHOUT THE NIGHT, UNLESS YOU "DONATE".
YOUR DIRTY DISHES CAN WAIT, I'M BUSY MINING BITCOINS.
EXCUSE US WHILE WE PARTICIPATE IN A DDoS ATTACK.
I'M TURNING OFF THE HEAT UNTIL YOU WARM UP MY BANK ACCOUNT!
WIRE MY HACKER $100 OR I'LL REVERSE MY MOTOR AND BLOW DIRT ALL OVER THIS PLACE!
I'LL START YOUR CAR, BUT ONLY TO TAKE YOU TO YOUR BANK TO MAKE A TRANSFER.
IF YOU DON'T SEND US CASH, YOUR REPUTATION WILL BE IN THE TRASH.
SEND ME $25 OR I'LL TELL EVERYONE ON YOUR SOCIAL NETWORK THAT YOU WERE STUPID ENOUGH TO BUY AN INTERNET-CONNECTED BROOM!
©2016 Geek Culture
You can help us keep the comics coming by becoming a patron! www.patreon/joyoftech
joyoftech.com

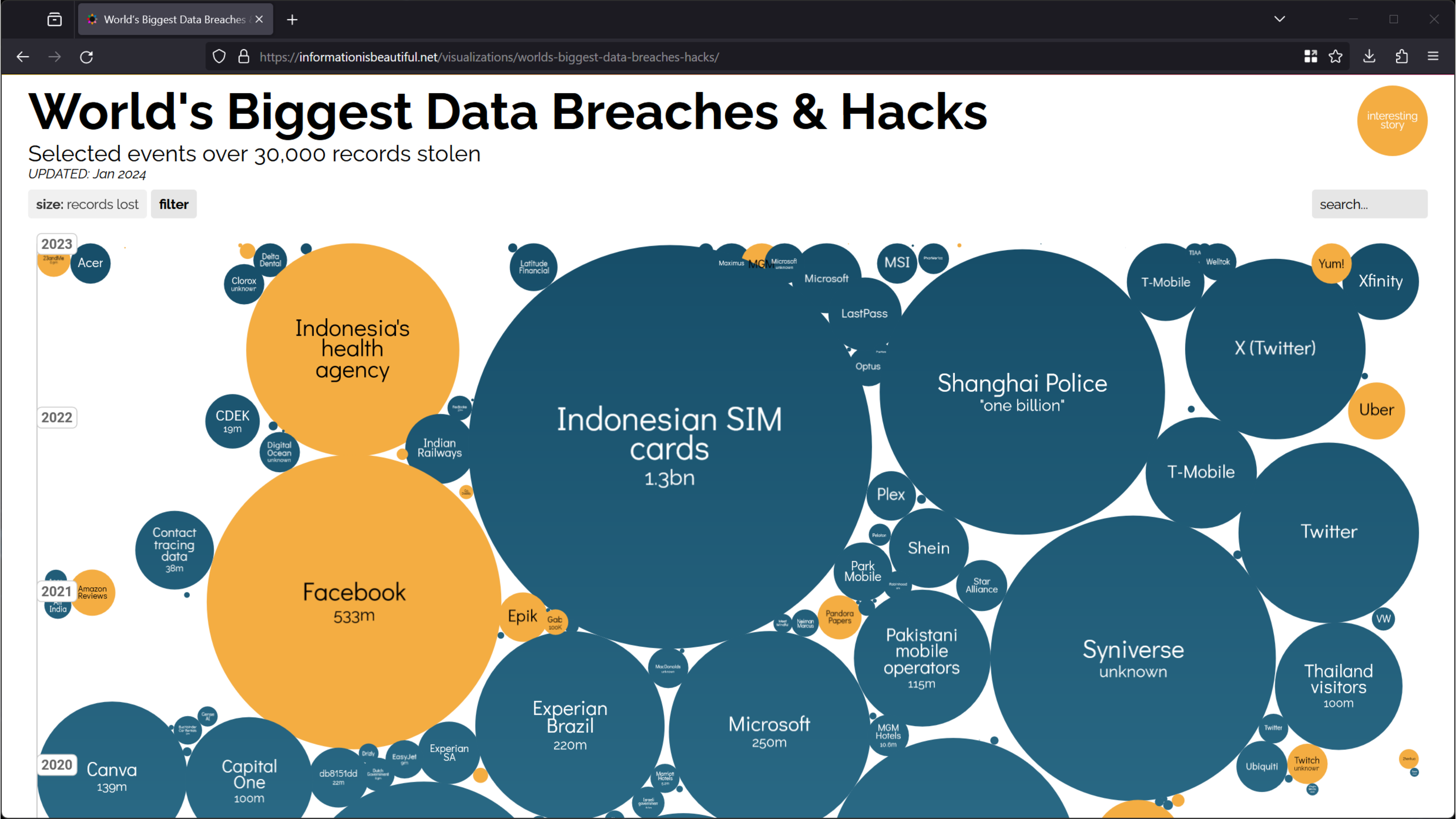
An increasing part of our business, social, and personal life involves Internet-connected computer systems

Mobile computing, Internet of things, wearable devices, vehicles, cyber-physical systems, …

Web, email, IM, videoconferencing, business operations, cloud services, social networks, entertainment, …

Protecting the security and privacy of our digital interactions is more critical than ever

Most of them involve networked systems and applications



World's Biggest Data Breaches

https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

World's Biggest Data Breaches & Hacks

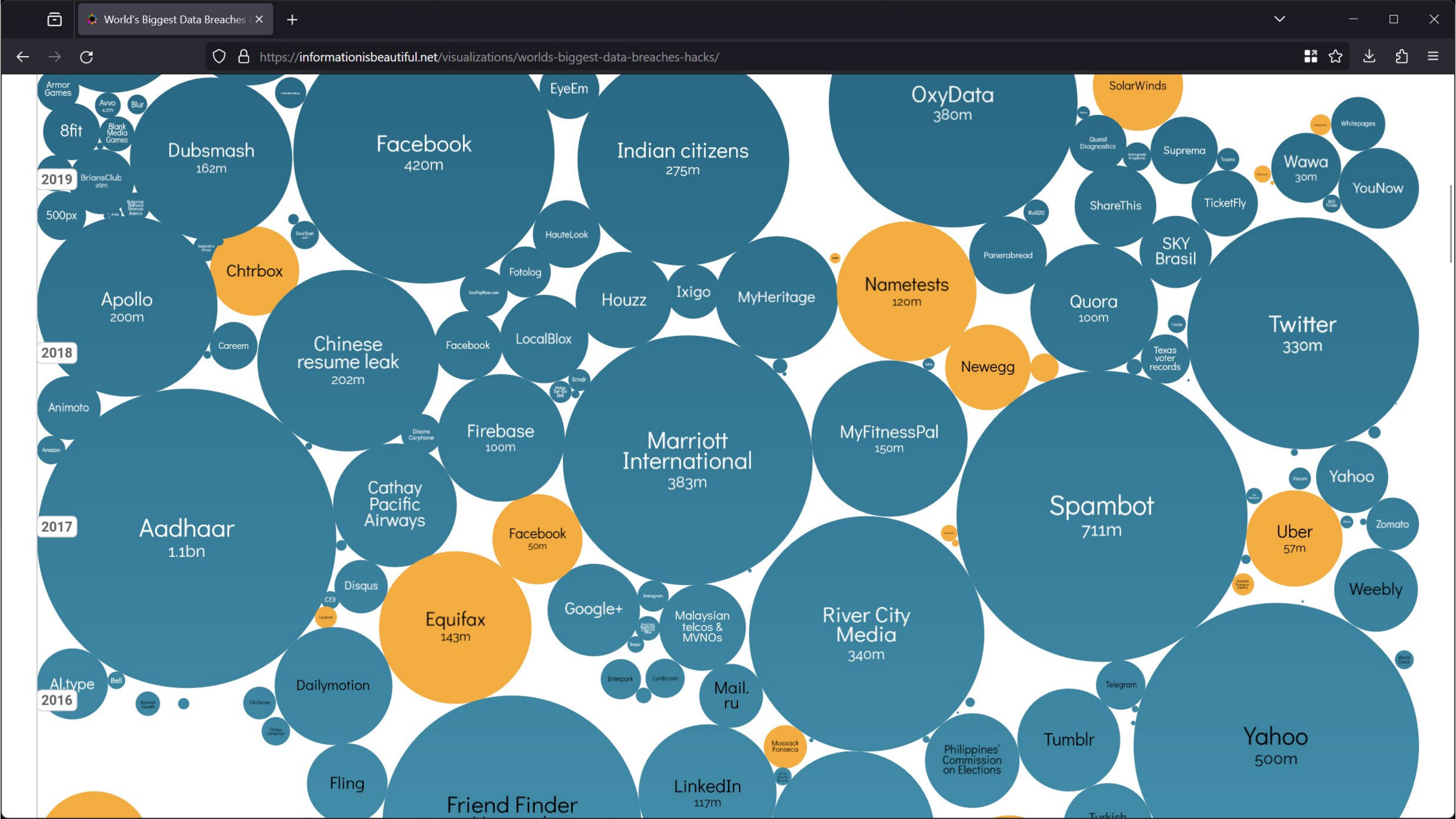
Selected events over 30,000 records stolen

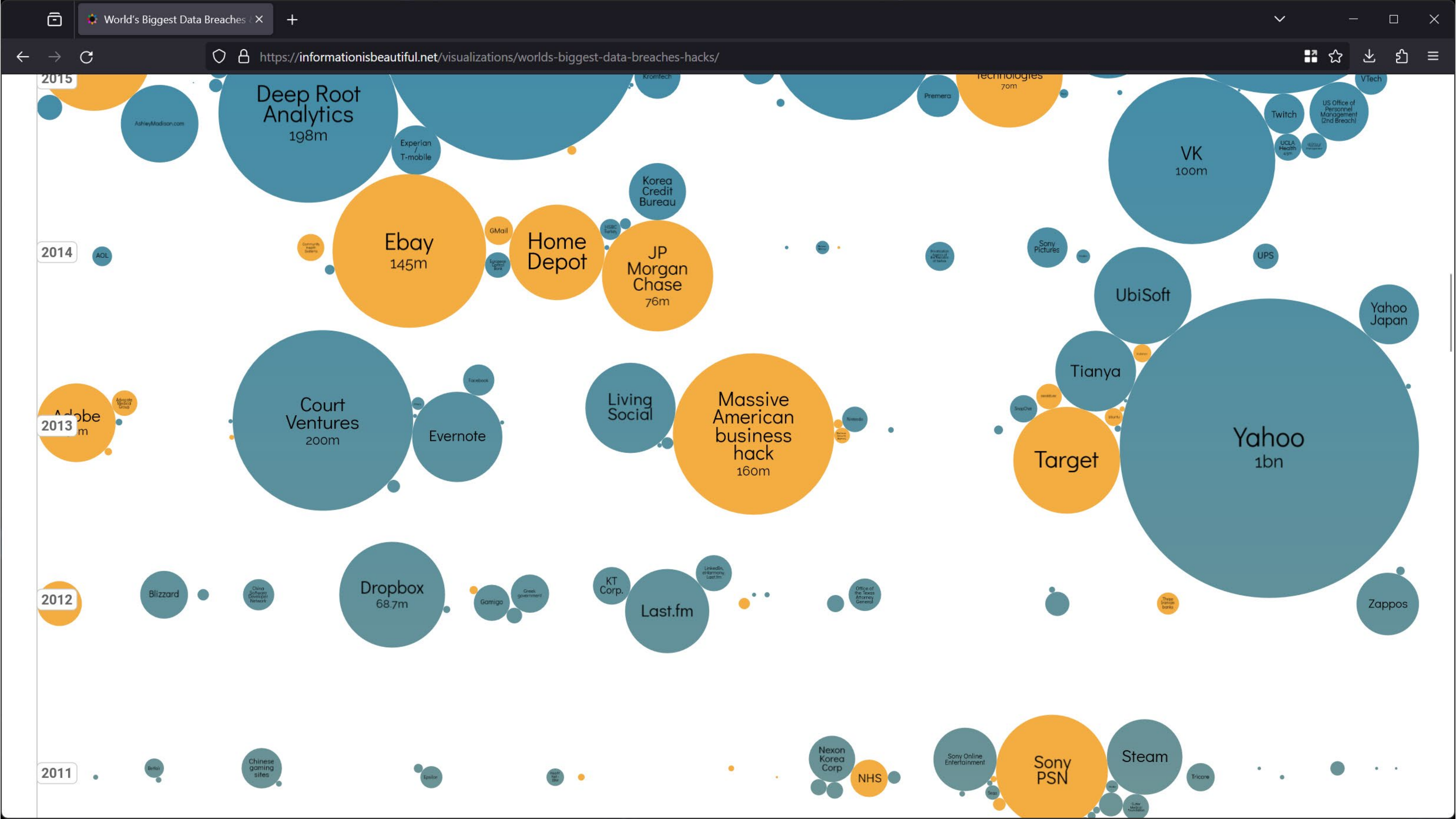
UPDATED: Jan 2024

size: records lost **filter**

search...

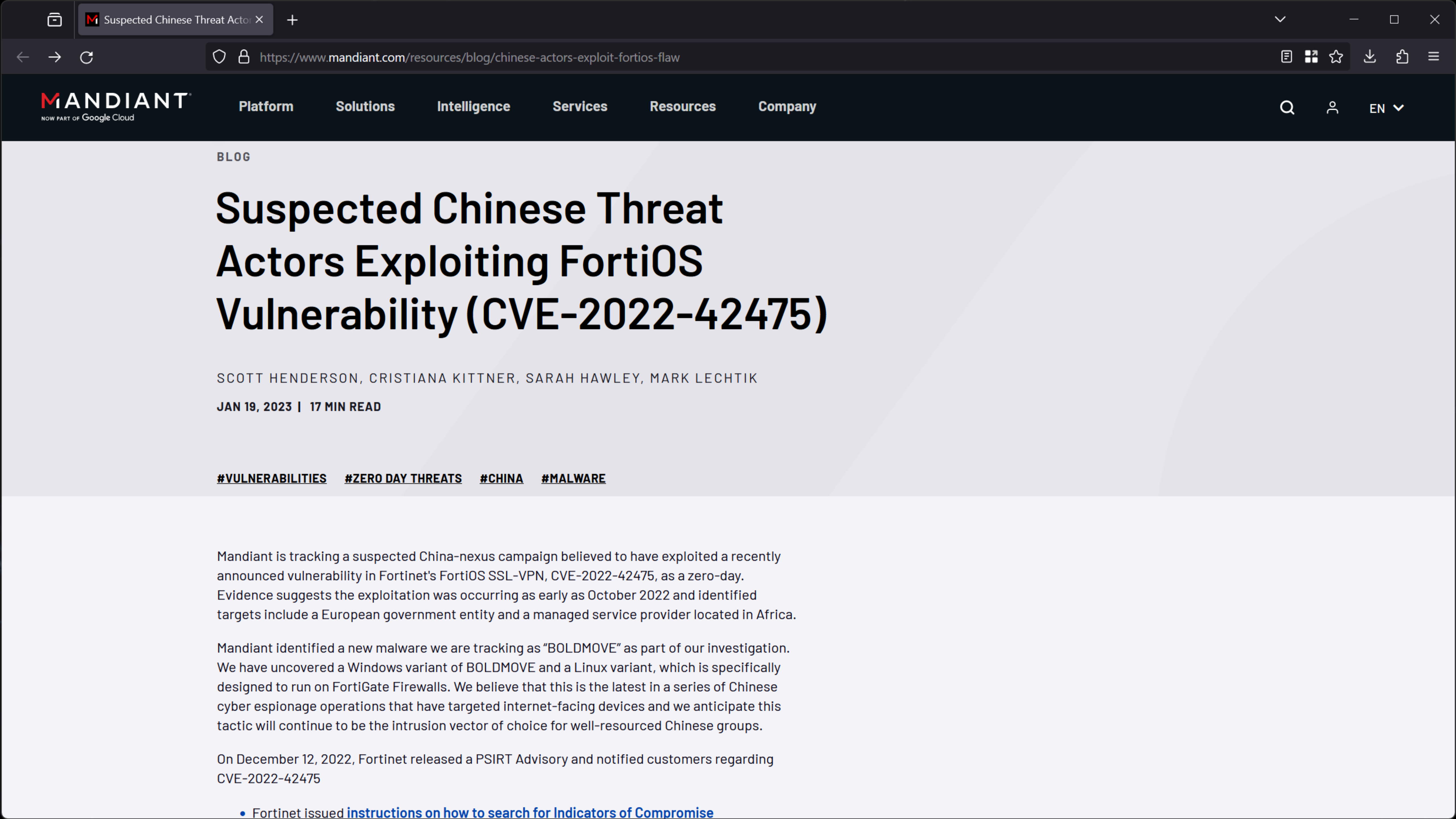
interesting story


World's Biggest Data Breaches
https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
2019
2018
2017
2016
Armor Games
Avvo 4.1m
Blur
8fit
Blank Media Games
Dubsmash 162m
BriansClub 26m
Bulgarian National Revenue Agency
Artsy
500px
DoorDash
Desjardins Group
Facebook 420m
EyeEm
Indian citizens 275m
OxyData 380m
SolarWinds
Quest Diagnostics
Stronghold Kingdoms
Suprema
Toyota
Whitepages
Wawa 30m
YouNow
Wifi Finder
ShareThis
TicketFly
SKY Brasil
Roll20
Panerabread
Chtrbox
Apollo 200m
Careem
HauteLook
Fotolog
GovPayNow.com
Houzz
Ixigo
MyHeritage
Nametests 120m
Quora 100m
Twitter 330m
Texas voter records
Chinese resume leak 202m
Facebook
LocalBlox
Grindr
Newegg
Animoto
Amazon
Firebase 100m
Dixons Carphone
Marriott International 383m
MyFitnessPal 150m
Spambot 711m
Yahoo
Viacom
Uber 57m
Zomato
Aadhaar 1.1bn
Cathay Pacific Airways
Facebook 50m
Disqus
CEX
Equifax 143m
Google+
Instagram
Malaysian telcos & MVNOs
Imgur
River City Media 340m
Weebly
Telegram
AI.type
Bell
Banner Health
ClixSense
Dailymotion
Interpark
Lynda.com
Mail.ru
Mossack Fonseca
Tumblr
Philippines' Commission on Elections
Yahoo 500m
Fling
Friend Finder
LinkedIn 117m
Turkish


World's Biggest Data Breaches &

https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Just a sample of incidents in the *past year*…


Suspected Chinese Threat Acto
https://www.mandiant.com/resources/blog/chinese-actors-exploit-fortios-flaw
MANDIANT
NOW PART OF Google Cloud
Platform
Solutions
Intelligence
Services
Resources
Company
EN

BLOG

Suspected Chinese Threat Actors Exploiting FortiOS Vulnerability (CVE-2022-42475)

SCOTT HENDERSON, CRISTIANA KITTNER, SARAH HAWLEY, MARK LECHTIK

JAN 19, 2023 | 17 MIN READ

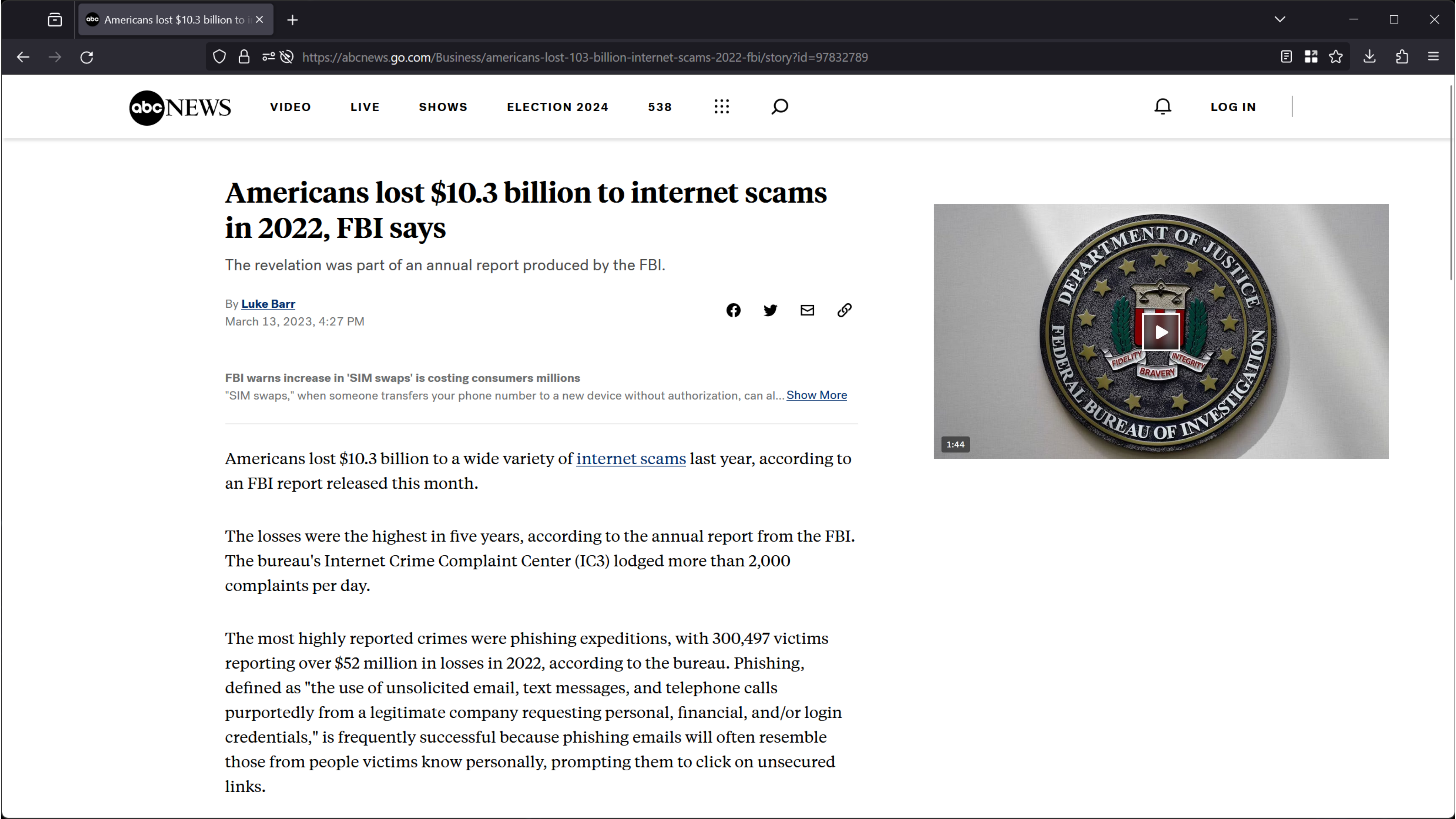
#VULNERABILITIES **#ZERO DAY THREATS** **#CHINA** **#MALWARE**

Mandiant is tracking a suspected China-nexus campaign believed to have exploited a recently announced vulnerability in Fortinet's FortiOS SSL-VPN, CVE-2022-42475, as a zero-day. Evidence suggests the exploitation was occurring as early as October 2022 and identified targets include a European government entity and a managed service provider located in Africa.

Mandiant identified a new malware we are tracking as “BOLDMOVE” as part of our investigation. We have uncovered a Windows variant of BOLDMOVE and a Linux variant, which is specifically designed to run on FortiGate Firewalls. We believe that this is the latest in a series of Chinese cyber espionage operations that have targeted internet-facing devices and we anticipate this tactic will continue to be the intrusion vector of choice for well-resourced Chinese groups.

On December 12, 2022, Fortinet released a PSIRT Advisory and notified customers regarding CVE-2022-42475

- Fortinet issued instructions on how to search for Indicators of Compromise


Americans lost $10.3 billion to i
https://abcnews.go.com/Business/americans-lost-103-billion-internet-scams-2022-fbi/story?id=97832789
abc NEWS
VIDEO
LIVE
SHOWS
ELECTION 2024
538
LOG IN
1:44

Americans lost $10.3 billion to internet scams in 2022, FBI says

The revelation was part of an annual report produced by the FBI.

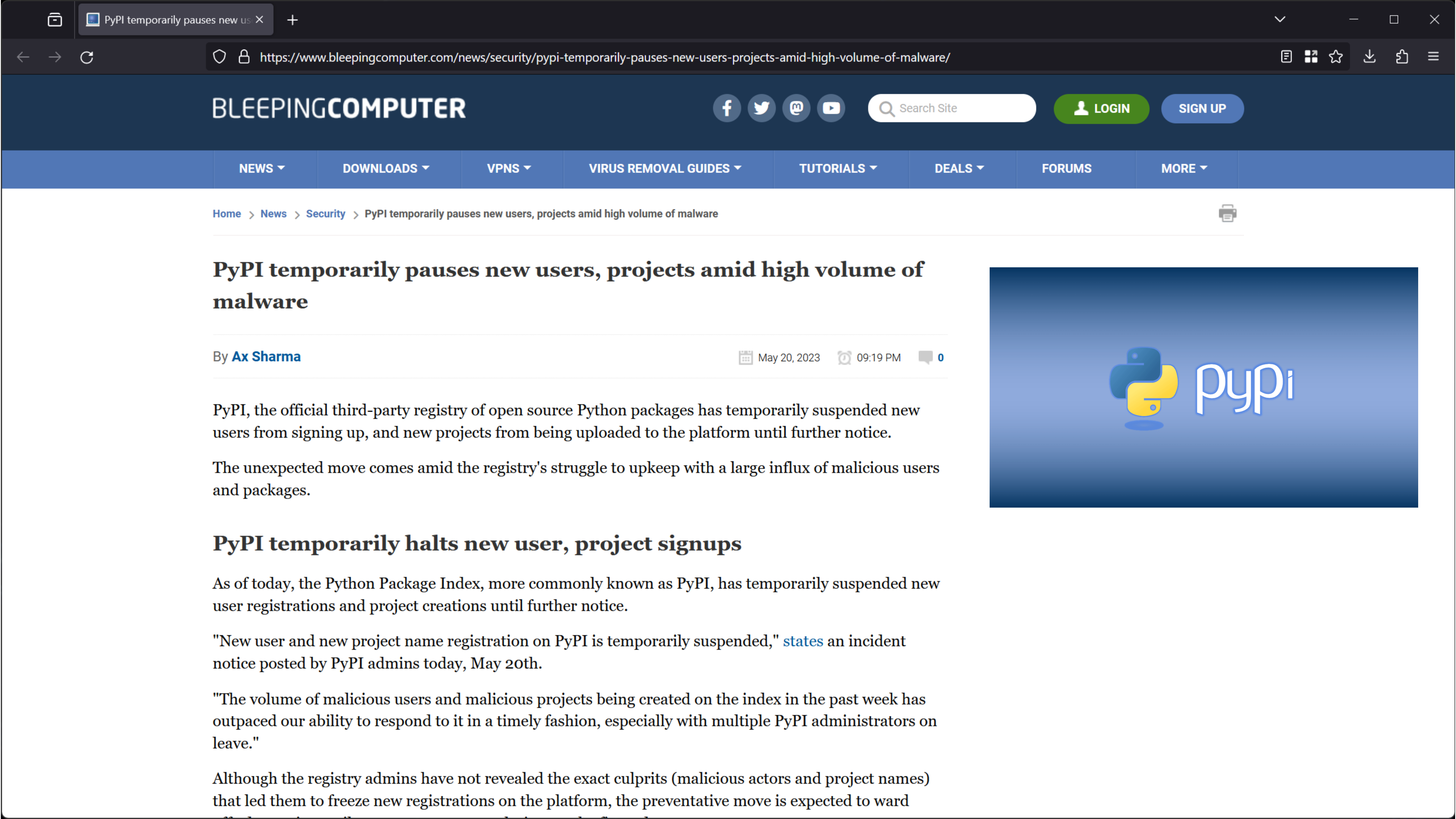
By Luke Barr
March 13, 2023, 4:27 PM

FBI warns increase in 'SIM swaps' is costing consumers millions
"SIM swaps," when someone transfers your phone number to a new device without authorization, can al... Show More

Americans lost $10.3 billion to a wide variety of internet scams last year, according to an FBI report released this month.

The losses were the highest in five years, according to the annual report from the FBI. The bureau's Internet Crime Complaint Center (IC3) lodged more than 2,000 complaints per day.

The most highly reported crimes were phishing expeditions, with 300,497 victims reporting over $52 million in losses in 2022, according to the bureau. Phishing, defined as "the use of unsolicited email, text messages, and telephone calls purportedly from a legitimate company requesting personal, financial, and/or login credentials," is frequently successful because phishing emails will often resemble those from people victims know personally, prompting them to click on unsecured links.



PyPI temporarily pauses new us
https://www.bleepingcomputer.com/news/security/pypi-temporarily-pauses-new-users-projects-amid-high-volume-of-malware/
BLEEPINGCOMPUTER
Search Site
LOGIN
SIGN UP
NEWS
DOWNLOADS
VPNS
VIRUS REMOVAL GUIDES
TUTORIALS
DEALS
FORUMS
MORE
pypi

Home > News > Security > PyPI temporarily pauses new users, projects amid high volume of malware

PyPI temporarily pauses new users, projects amid high volume of malware

By **Ax Sharma** May 20, 2023 09:19 PM 0

PyPI, the official third-party registry of open source Python packages has temporarily suspended new users from signing up, and new projects from being uploaded to the platform until further notice.

The unexpected move comes amid the registry's struggle to upkeep with a large influx of malicious users and packages.

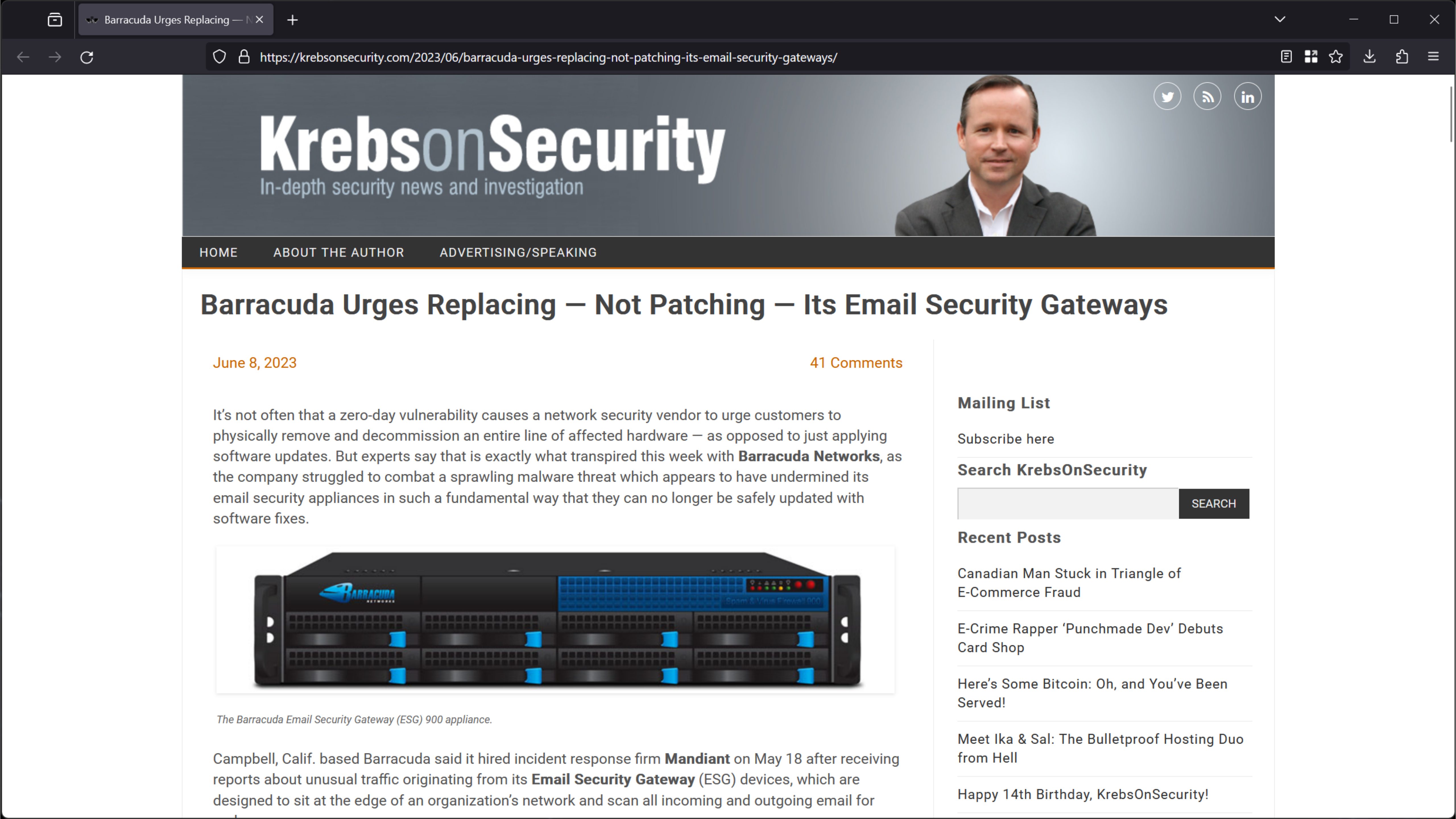
PyPI temporarily halts new user, project signups

As of today, the Python Package Index, more commonly known as PyPI, has temporarily suspended new user registrations and project creations until further notice.

"New user and new project name registration on PyPI is temporarily suspended," states an incident notice posted by PyPI admins today, May 20th.

"The volume of malicious users and malicious projects being created on the index in the past week has outpaced our ability to respond to it in a timely fashion, especially with multiple PyPI administrators on leave."

Although the registry admins have not revealed the exact culprits (malicious actors and project names) that led them to freeze new registrations on the platform, the preventative move is expected to ward


Barracuda Urges Replacing — N
https://krebsonsecurity.com/2023/06/barracuda-urges-replacing-not-patching-its-email-security-gateways/

KrebsonSecurity
In-depth security news and investigation

Barracuda Urges Replacing — Not Patching — Its Email Security Gateways

June 8, 2023 41 Comments

It's not often that a zero-day vulnerability causes a network security vendor to urge customers to physically remove and decommission an entire line of affected hardware — as opposed to just applying software updates. But experts say that is exactly what transpired this week with **Barracuda Networks**, as the company struggled to combat a sprawling malware threat which appears to have undermined its email security appliances in such a fundamental way that they can no longer be safely updated with software fixes.

The Barracuda Email Security Gateway (ESG) 900 appliance.

Campbell, Calif. based Barracuda said it hired incident response firm **Mandiant** on May 18 after receiving reports about unusual traffic originating from its **Email Security Gateway** (ESG) devices, which are designed to sit at the edge of an organization's network and scan all incoming and outgoing email for

Mailing List

Subscribe here

Search KrebsOnSecurity

SEARCH

Recent Posts

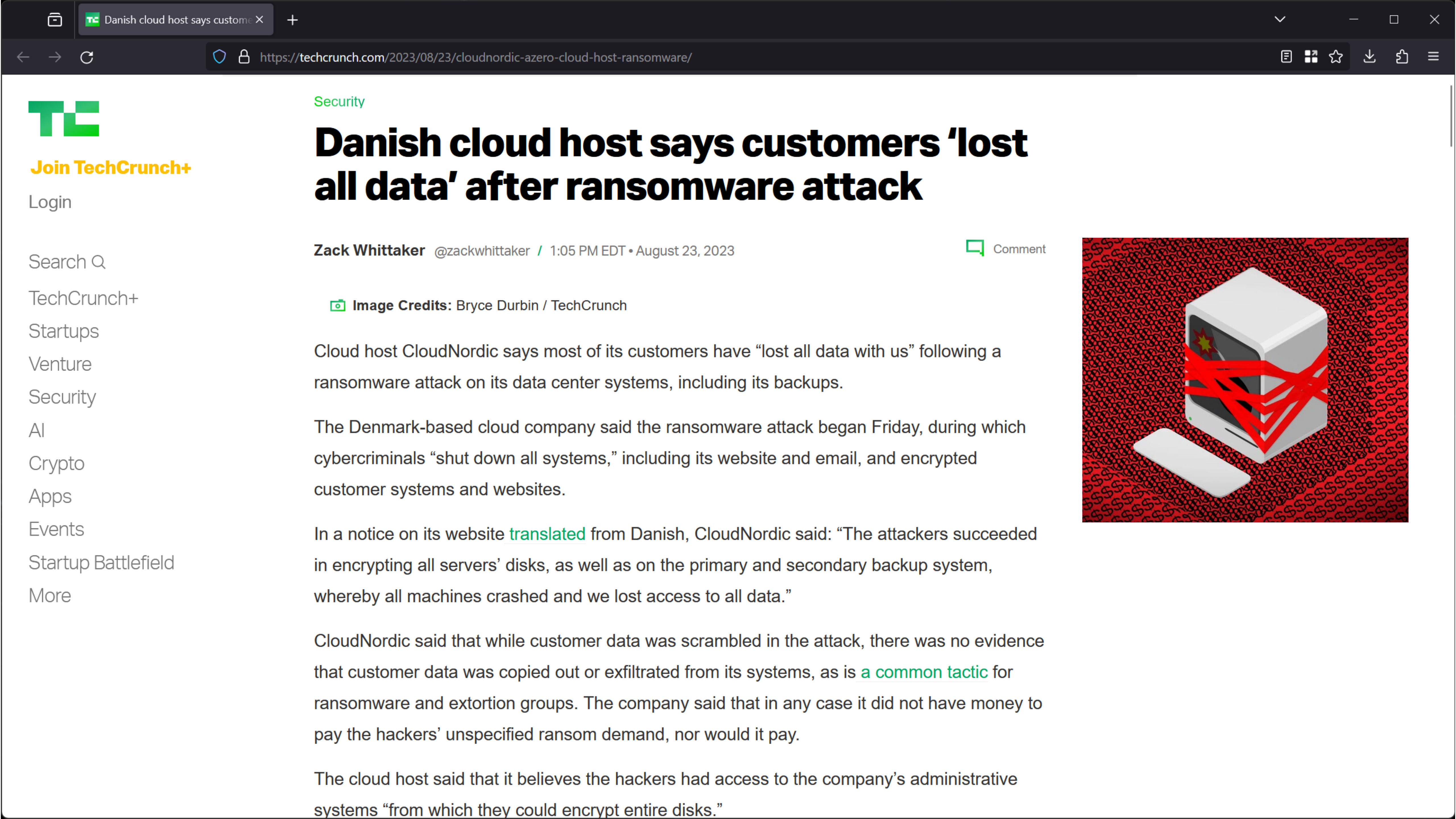
Canadian Man Stuck in Triangle of E-Commerce Fraud

E-Crime Rapper 'Punchmade Dev' Debuts Card Shop

Here's Some Bitcoin: Oh, and You've Been Served!

Meet Ika & Sal: The Bulletproof Hosting Duo from Hell

Happy 14th Birthday, KrebsOnSecurity!



Danish cloud host says custome
https://techcrunch.com/2023/08/23/cloudnordic-azero-cloud-host-ransomware/

Security

Danish cloud host says customers 'lost all data' after ransomware attack

Zack Whittaker @zackwhittaker / 1:05 PM EDT • August 23, 2023

Comment

Image Credits: Bryce Durbin / TechCrunch

Cloud host CloudNordic says most of its customers have "lost all data with us" following a ransomware attack on its data center systems, including its backups.

The Denmark-based cloud company said the ransomware attack began Friday, during which cybercriminals "shut down all systems," including its website and email, and encrypted customer systems and websites.

In a notice on its website translated from Danish, CloudNordic said: "The attackers succeeded in encrypting all servers' disks, as well as on the primary and secondary backup system, whereby all machines crashed and we lost access to all data."

CloudNordic said that while customer data was scrambled in the attack, there was no evidence that customer data was copied out or exfiltrated from its systems, as is a common tactic for ransomware and extortion groups. The company said that in any case it did not have money to pay the hackers' unspecified ransom demand, nor would it pay.

The cloud host said that it believes the hackers had access to the company's administrative systems "from which they could encrypt entire disks."

#1 Trusted Cybersecurity News Platform

Followed by 4.50+ million

The Hacker News

WinRAR Security Flaw Exploited in Zero-Day Attacks to Target Traders

Aug 24, 2023 Newsroom Endpoint Security / Zero-Day

A recently patched security flaw in the popular WinRAR archiving software has been exploited as a zero-day since April 2023, new findings from Group-IB reveal.

The vulnerability, cataloged as CVE-2023-38831, allows threat actors to spoof file extensions, thereby making it possible to launch malicious scripts contained within an archive that masquerades as seemingly innocuous image or text files. It was addressed in version 6.23 released on August 2, 2023, alongside CVE-2023-40477.

In attacks discovered by the Singapore-based firm in July 2023, specially crafted ZIP or RAR archive files distributed via trading-related forums such as Forex Station have been used to deliver a variety of malware families such as DarkMe, GuLoader, and Remcos RAT.

"After infecting devices, the cybercriminals withdraw money from broker accounts," Group-IB malware analyst Andrey Polovinkin said, adding as many as 130 traders' devices have been compromised as part of the campaign. The total number of victims and financial losses stemming from this activity are currently not clear.

The booby-trapped archive file is created such that it contains an image file as well as a folder with the

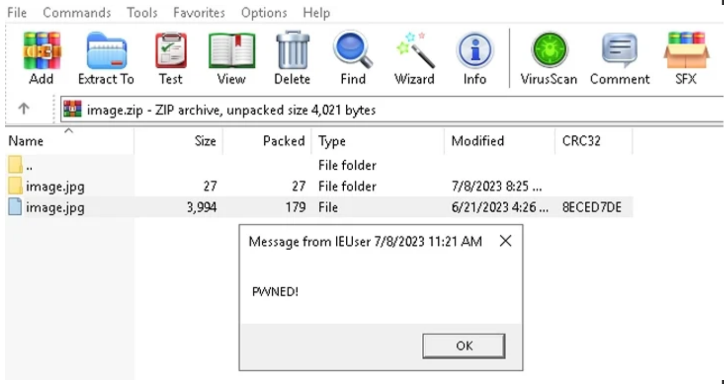


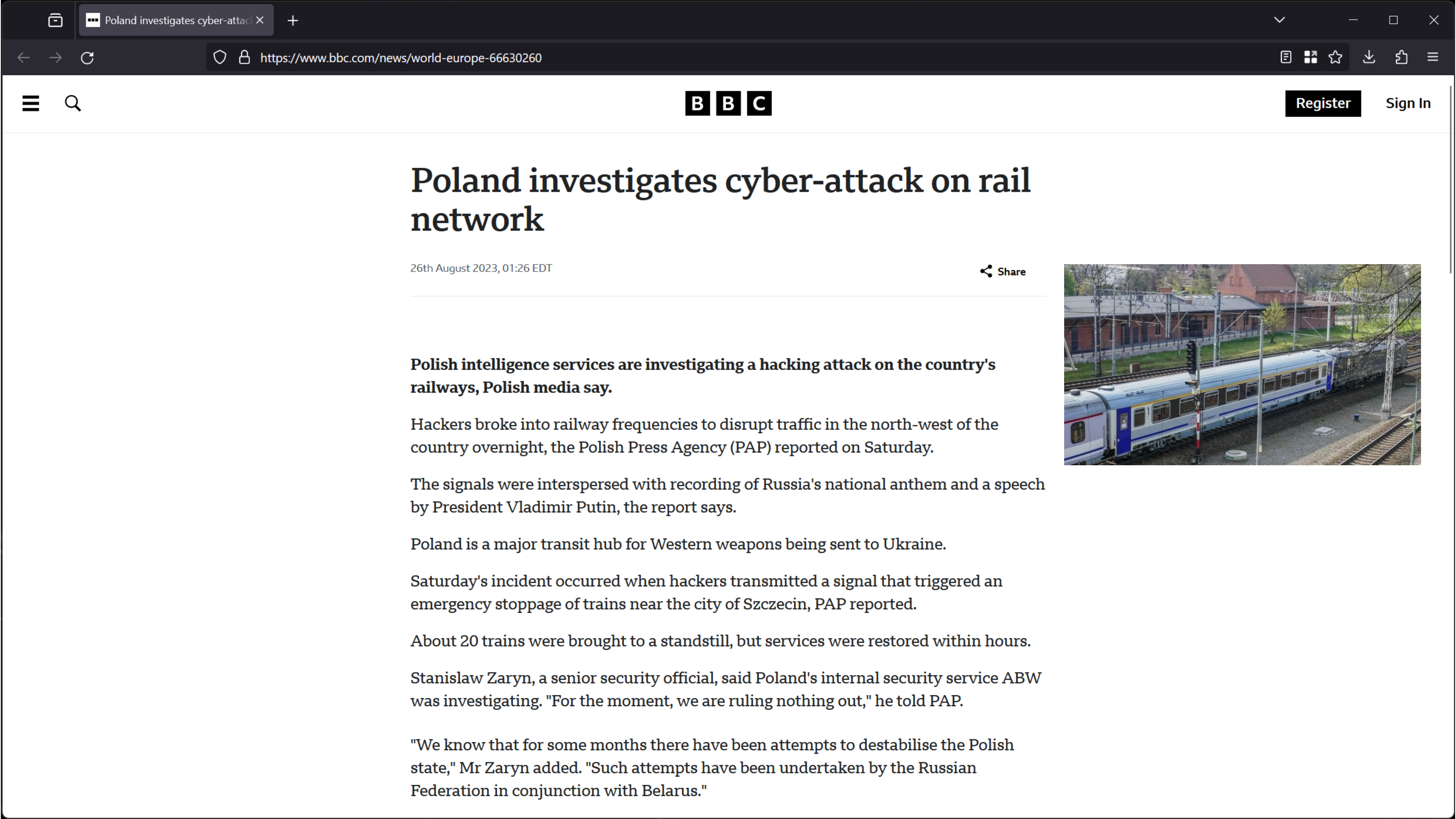
image.zip - ZIP archive, unpacked size 4,021 bytes

Name	Size	Packed	Type	Modified	CRC32
..			File folder		
image.jpg	27	27	File folder	7/8/2023 8:25 ...	
image.jpg	3,994	179	File	6/21/2023 4:26 ...	8ECED7DE

Message from IEUser 7/8/2023 11:21 AM

PWNED!

OK


Poland investigates cyber-attac
https://www.bbc.com/news/world-europe-66630260
BBC
Register
Sign In
Share

Poland investigates cyber-attack on rail network

26th August 2023, 01:26 EDT

Polish intelligence services are investigating a hacking attack on the country's railways, Polish media say.

Hackers broke into railway frequencies to disrupt traffic in the north-west of the country overnight, the Polish Press Agency (PAP) reported on Saturday.

The signals were interspersed with recording of Russia's national anthem and a speech by President Vladimir Putin, the report says.

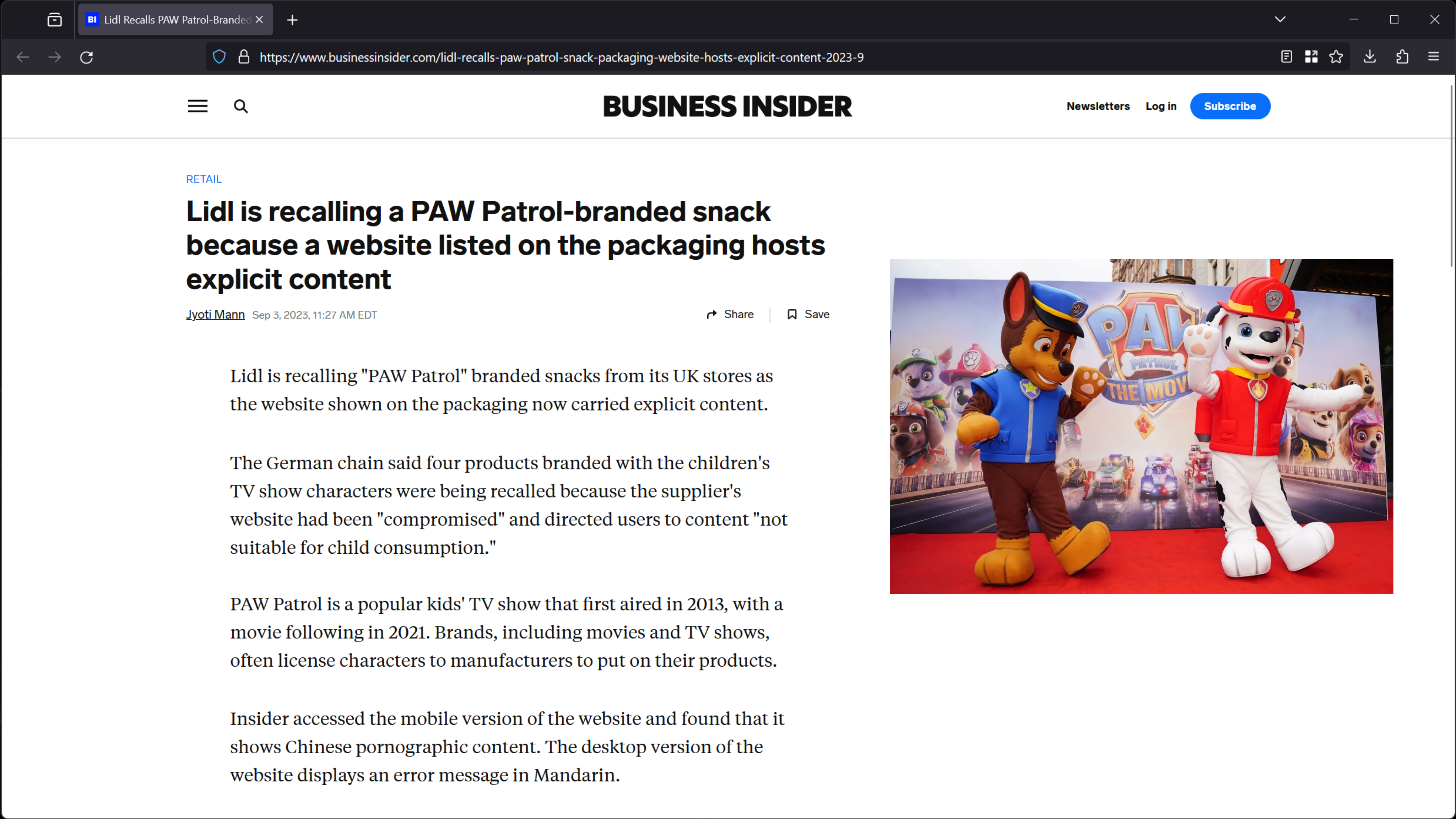
Poland is a major transit hub for Western weapons being sent to Ukraine.

Saturday's incident occurred when hackers transmitted a signal that triggered an emergency stoppage of trains near the city of Szczecin, PAP reported.

About 20 trains were brought to a standstill, but services were restored within hours.

Stanislaw Zaryn, a senior security official, said Poland's internal security service ABW was investigating. "For the moment, we are ruling nothing out," he told PAP.

"We know that for some months there have been attempts to destabilise the Polish state," Mr Zaryn added. "Such attempts have been undertaken by the Russian Federation in conjunction with Belarus."


Lidl Recalls PAW Patrol-Branded
https://www.businessinsider.com/lidl-recalls-paw-patrol-snack-packaging-website-hosts-explicit-content-2023-9
BUSINESS INSIDER
Newsletters
Log in
Subscribe
Share
Save
PAW PATROL
THE MOV

RETAIL

Lidl is recalling a PAW Patrol-branded snack because a website listed on the packaging hosts explicit content

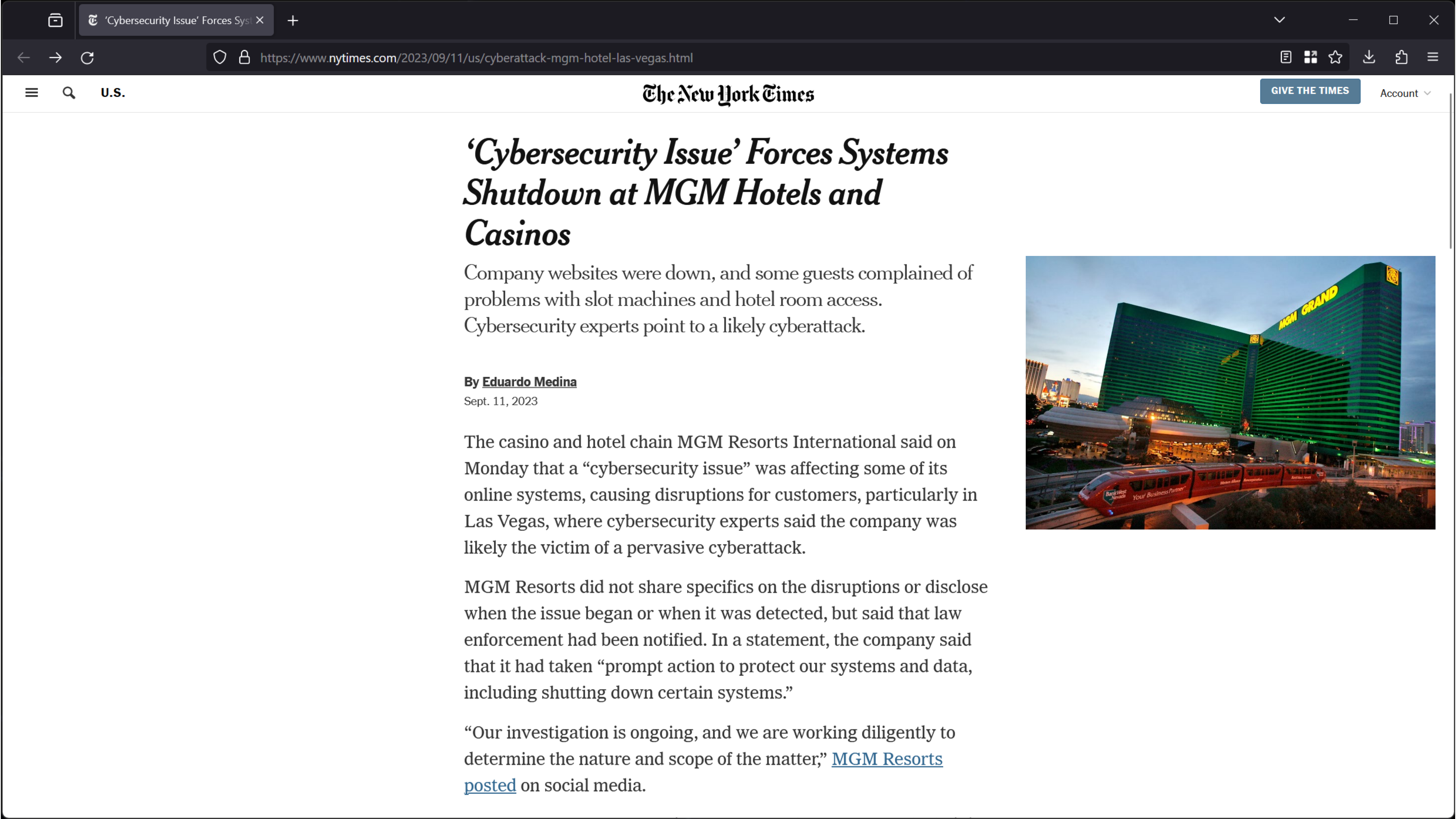
Jyoti Mann Sep 3, 2023, 11:27 AM EDT

Lidl is recalling "PAW Patrol" branded snacks from its UK stores as the website shown on the packaging now carried explicit content.

The German chain said four products branded with the children's TV show characters were being recalled because the supplier's website had been "compromised" and directed users to content "not suitable for child consumption."

PAW Patrol is a popular kids' TV show that first aired in 2013, with a movie following in 2021. Brands, including movies and TV shows, often license characters to manufacturers to put on their products.

Insider accessed the mobile version of the website and found that it shows Chinese pornographic content. The desktop version of the website displays an error message in Mandarin.


'Cybersecurity Issue' Forces Syst
https://www.nytimes.com/2023/09/11/us/cyberattack-mgm-hotel-las-vegas.html
U.S.
The New York Times
GIVE THE TIMES
Account
MGM GRAND
Your Business Partner

‘Cybersecurity Issue’ Forces Systems Shutdown at MGM Hotels and Casinos

Company websites were down, and some guests complained of problems with slot machines and hotel room access. Cybersecurity experts point to a likely cyberattack.

By Eduardo Medina

Sept. 11, 2023

The casino and hotel chain MGM Resorts International said on Monday that a “cybersecurity issue” was affecting some of its online systems, causing disruptions for customers, particularly in Las Vegas, where cybersecurity experts said the company was likely the victim of a pervasive cyberattack.

MGM Resorts did not share specifics on the disruptions or disclose when the issue began or when it was detected, but said that law enforcement had been notified. In a statement, the company said that it had taken “prompt action to protect our systems and data, including shutting down certain systems.”

“Our investigation is ongoing, and we are working diligently to determine the nature and scope of the matter,” MGM Resorts posted on social media.

The Record.
Recorded Future® News

Catalin Cimpanu

July 30th, 2021

News

Technology News

Privacy News

Hackers leak full EA data after failed extortion attempt

The hackers who breached Electronic Arts last month have released the entire cache of stolen data after failing to extort the company and later sell the stolen files to a third-party buyer.

The data, dumped on an underground cybercrime forum on Monday, July 26, is now being widely distributed on torrent sites.

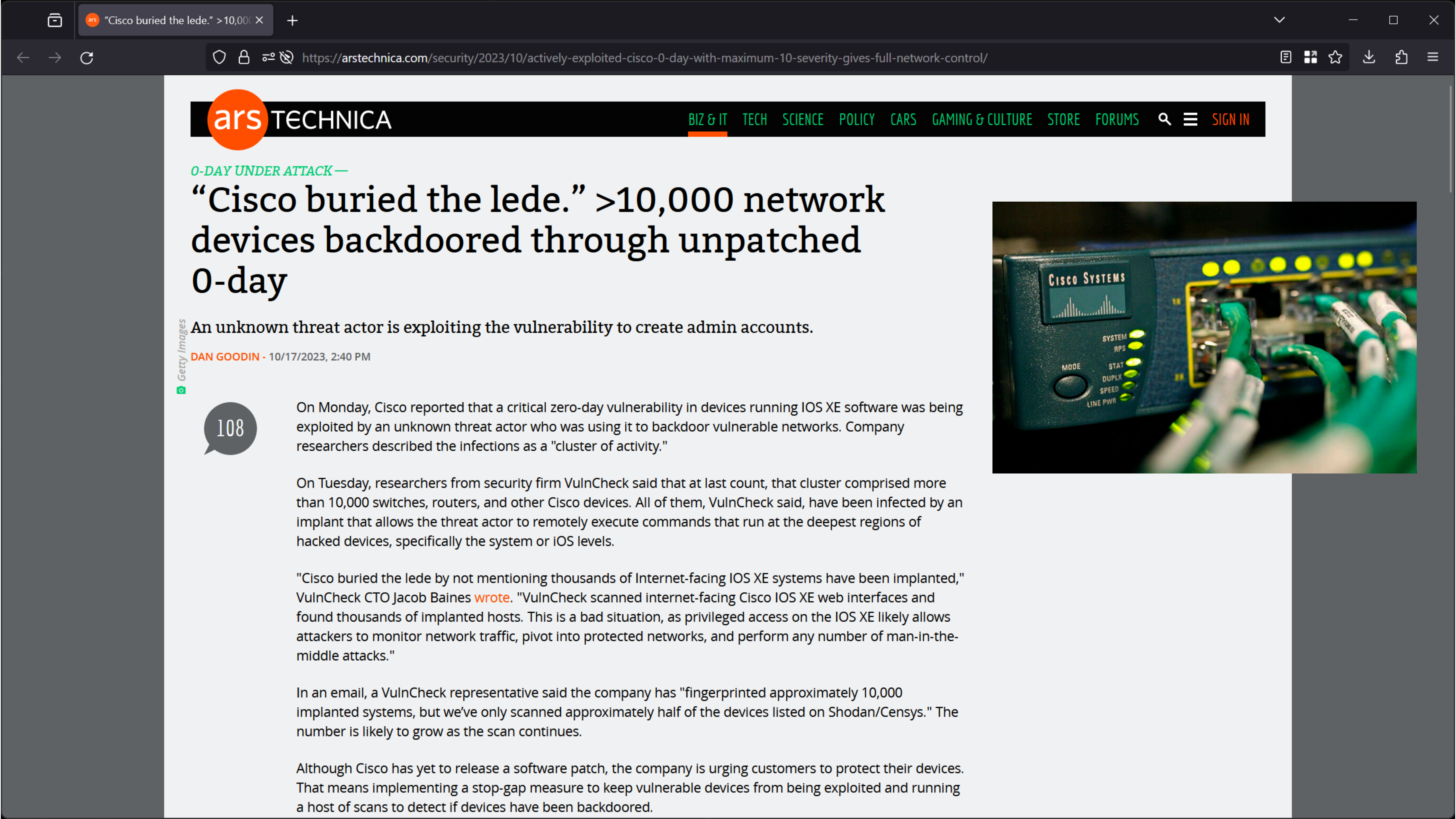
According to a copy of the dump obtained by *The Record*, the leaked files contain the source code of the FIFA 21 soccer game, including tools to support the company's server-side services.

How the EA breach took place

The existence of this leak was initially disclosed on June 10, when the hackers posted a thread on an underground hacking forum claiming to be in possession of EA data, which they were willing to sell for $28 million.

In an interview with Motherboard, the hackers claimed to have gained access to the data after buying authentication cookies for an EA internal Slack channel from a dark web marketplace called Genesis.

The hackers said they used the authentication cookies to mimick an


“Cisco buried the lede.” >10,00
https://arstechnica.com/security/2023/10/actively-exploited-cisco-0-day-with-maximum-10-severity-gives-full-network-control/
ars TECHNICA
BIZ & IT
TECH
SCIENCE
POLICY
CARS
GAMING & CULTURE
STORE
FORUMS
SIGN IN
108
Getty Images
Cisco Systems
SYSTEM
RPS
STAT
DUPLX
SPEED
LINE PWR
MODE

0-DAY UNDER ATTACK —

“Cisco buried the lede.” >10,000 network devices backdoored through unpatched 0-day

An unknown threat actor is exploiting the vulnerability to create admin accounts.

DAN GOODIN - 10/17/2023, 2:40 PM

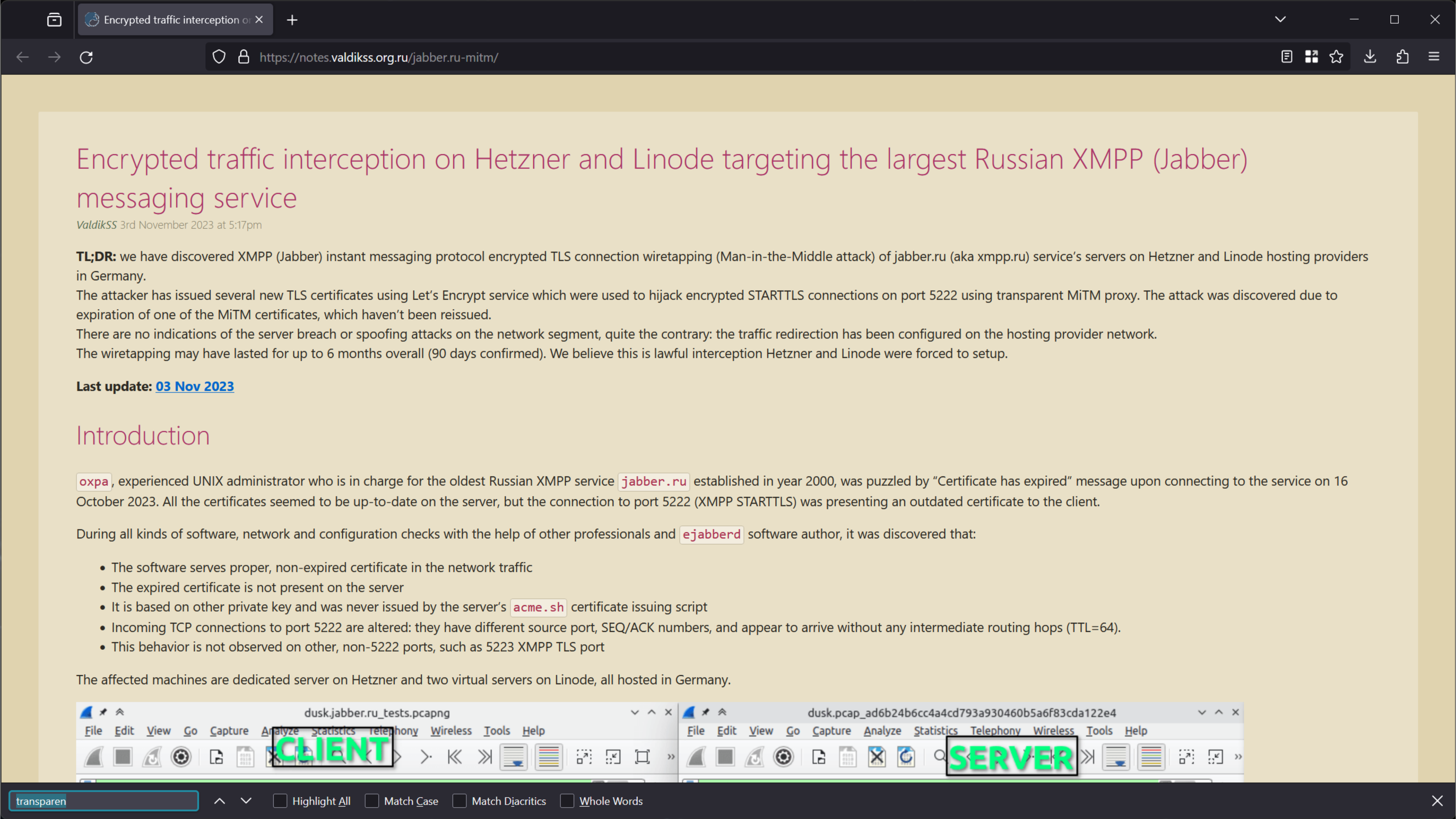
On Monday, Cisco reported that a critical zero-day vulnerability in devices running IOS XE software was being exploited by an unknown threat actor who was using it to backdoor vulnerable networks. Company researchers described the infections as a "cluster of activity."

On Tuesday, researchers from security firm VulnCheck said that at last count, that cluster comprised more than 10,000 switches, routers, and other Cisco devices. All of them, VulnCheck said, have been infected by an implant that allows the threat actor to remotely execute commands that run at the deepest regions of hacked devices, specifically the system or iOS levels.

"Cisco buried the lede by not mentioning thousands of Internet-facing IOS XE systems have been implanted," VulnCheck CTO Jacob Baines wrote. "VulnCheck scanned internet-facing Cisco IOS XE web interfaces and found thousands of implanted hosts. This is a bad situation, as privileged access on the IOS XE likely allows attackers to monitor network traffic, pivot into protected networks, and perform any number of man-in-the-middle attacks."

In an email, a VulnCheck representative said the company has "fingerprinted approximately 10,000 implanted systems, but we’ve only scanned approximately half of the devices listed on Shodan/Censys." The number is likely to grow as the scan continues.

Although Cisco has yet to release a software patch, the company is urging customers to protect their devices. That means implementing a stop-gap measure to keep vulnerable devices from being exploited and running a host of scans to detect if devices have been backdoored.



Encrypted traffic interception o
https://notes.valdikss.org.ru/jabber.ru-mitm/

Encrypted traffic interception on Hetzner and Linode targeting the largest Russian XMPP (Jabber) messaging service

ValdikSS 3rd November 2023 at 5:17pm

TL;DR: we have discovered XMPP (Jabber) instant messaging protocol encrypted TLS connection wiretapping (Man-in-the-Middle attack) of jabber.ru (aka xmpp.ru) service's servers on Hetzner and Linode hosting providers in Germany.
The attacker has issued several new TLS certificates using Let's Encrypt service which were used to hijack encrypted STARTTLS connections on port 5222 using transparent MiTM proxy. The attack was discovered due to expiration of one of the MiTM certificates, which haven't been reissued.
There are no indications of the server breach or spoofing attacks on the network segment, quite the contrary: the traffic redirection has been configured on the hosting provider network.
The wiretapping may have lasted for up to 6 months overall (90 days confirmed). We believe this is lawful interception Hetzner and Linode were forced to setup.

Last update: 03 Nov 2023

Introduction

`oxpa`, experienced UNIX administrator who is in charge for the oldest Russian XMPP service `jabber.ru` established in year 2000, was puzzled by "Certificate has expired" message upon connecting to the service on 16 October 2023. All the certificates seemed to be up-to-date on the server, but the connection to port 5222 (XMPP STARTTLS) was presenting an outdated certificate to the client.

During all kinds of software, network and configuration checks with the help of other professionals and `ejabberd` software author, it was discovered that:

- The software serves proper, non-expired certificate in the network traffic
- The expired certificate is not present on the server
- It is based on other private key and was never issued by the server's `acme.sh` certificate issuing script
- Incoming TCP connections to port 5222 are altered: they have different source port, SEQ/ACK numbers, and appear to arrive without any intermediate routing hops (TTL=64).
- This behavior is not observed on other, non-5222 ports, such as 5223 XMPP TLS port

The affected machines are dedicated server on Hetzner and two virtual servers on Linode, all hosted in Germany.

dusk.jabber.ru_tests.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
CLIENT
dusk.pcap_ad6b24b6cc4a4cd793a930460b5a6f83cda122e4
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
SERVER
transparen
Highlight All
Match Case
Match Diacritics
Whole Words

BREAKING

Russian Hackers Breached 632,000 DOJ And Pentagon Email Addresses In Massive MOVEit Cyberattack, Report Says

Ty Roush Forbes Staff

I cover breaking news.

Oct 30, 2023, 01:43pm EDT

TOPLINE The email addresses of about 632,000 employees from the Justice and Defense departments were accessed in a hack earlier this year, Bloomberg reported Monday, adding to the number of organizations—including airlines, universities and other U.S. agencies—impacted by a series of data breaches largely blamed on a Russian-speaking criminal group.

KEY FACTS

- The accessed email addresses, links to government employee surveys administered by the agency and internal agency tracking codes, according to a report by the Office of Personnel Management obtained by Bloomberg.
- Hackers obtained access through a file transfer program called MOVEit used by the data firm Westat, which OPM uses to administer employee surveys, according to the Bloomberg report.

The Record.
Recorded Future® News

Daryna Antoniuk
November 1st, 2023

News

Government News

Cybercrime News

Massive ransomware attack hinders services in 70 German municipalities

A ransomware attack this week has paralyzed local government services in multiple cities and districts in western Germany.

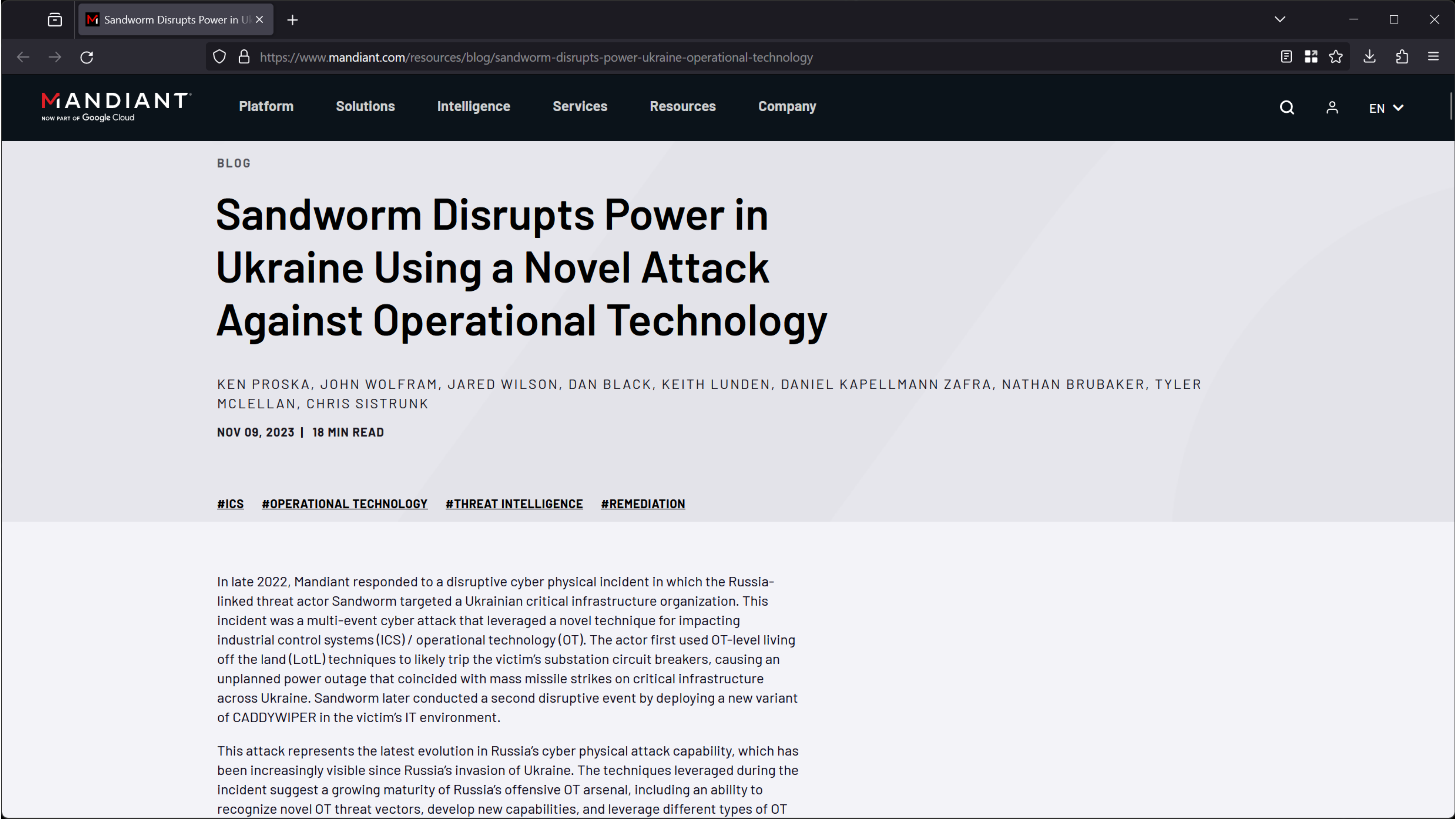
Early on Monday, an unknown hacker group encrypted the servers of the local municipal service provider Südwestfalen IT. To prevent the malware from spreading, the company restricted access to its infrastructure for over 70 municipalities, primarily in the western German state of North Rhine-Westphalia.

The attack left local government services “severely limited,” the company said in a statement posted on a temporary website, as its main site is inaccessible following the incident.

Nearly all town halls in the region were impacted by the hack.

TKG Südwestfalen mbH
@tkgswf · Follow

Cyberangriff auf die @SuedwestfalenIT. Die Kreisverwaltungen unserer Gesellschafter #Hochsauerlandkreis, @KreisSoest, @Kreis_SiWi, @Kreis_Olpe und #MärkischerKreis und Rathäuser in #Südwestfalen sind betroffen.


Sandworm Disrupts Power in Uk
https://www.mandiant.com/resources/blog/sandworm-disrupts-power-ukraine-operational-technology
MANDIANT
NOW PART OF Google Cloud
Platform
Solutions
Intelligence
Services
Resources
Company
EN

BLOG

Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology

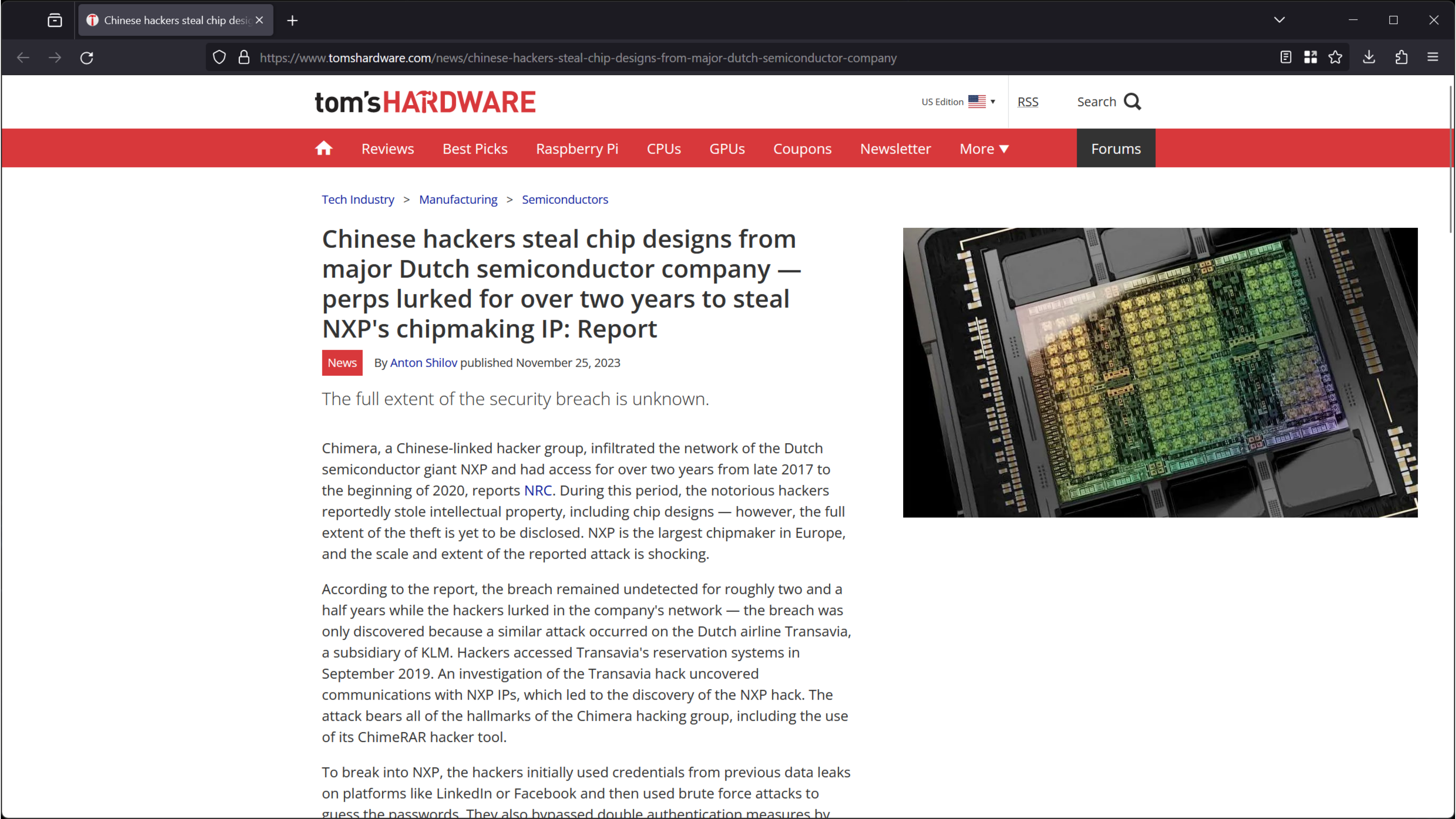
KEN PROSKA, JOHN WOLFRAM, JARED WILSON, DAN BLACK, KEITH LUNDEN, DANIEL KAPELLMANN ZAFRA, NATHAN BRUBAKER, TYLER MCLELLAN, CHRIS SISTRUNK

NOV 09, 2023 | 18 MIN READ

#ICS **#OPERATIONAL TECHNOLOGY** **#THREAT INTELLIGENCE** **#REMEDIATION**

In late 2022, Mandiant responded to a disruptive cyber physical incident in which the Russia-linked threat actor Sandworm targeted a Ukrainian critical infrastructure organization. This incident was a multi-event cyber attack that leveraged a novel technique for impacting industrial control systems (ICS) / operational technology (OT). The actor first used OT-level living off the land (LotL) techniques to likely trip the victim's substation circuit breakers, causing an unplanned power outage that coincided with mass missile strikes on critical infrastructure across Ukraine. Sandworm later conducted a second disruptive event by deploying a new variant of CADDYWIPER in the victim's IT environment.

This attack represents the latest evolution in Russia's cyber physical attack capability, which has been increasingly visible since Russia's invasion of Ukraine. The techniques leveraged during the incident suggest a growing maturity of Russia's offensive OT arsenal, including an ability to recognize novel OT threat vectors, develop new capabilities, and leverage different types of OT


Chinese hackers steal chip desig
https://www.tomshardware.com/news/chinese-hackers-steal-chip-designs-from-major-dutch-semiconductor-company
tom's HARDWARE
US Edition
RSS
Search
Reviews
Best Picks
Raspberry Pi
CPUs
GPUs
Coupons
Newsletter
More
Forums
Tech Industry > Manufacturing > Semiconductors

Chinese hackers steal chip designs from major Dutch semiconductor company — perps lurked for over two years to steal NXP's chipmaking IP: Report

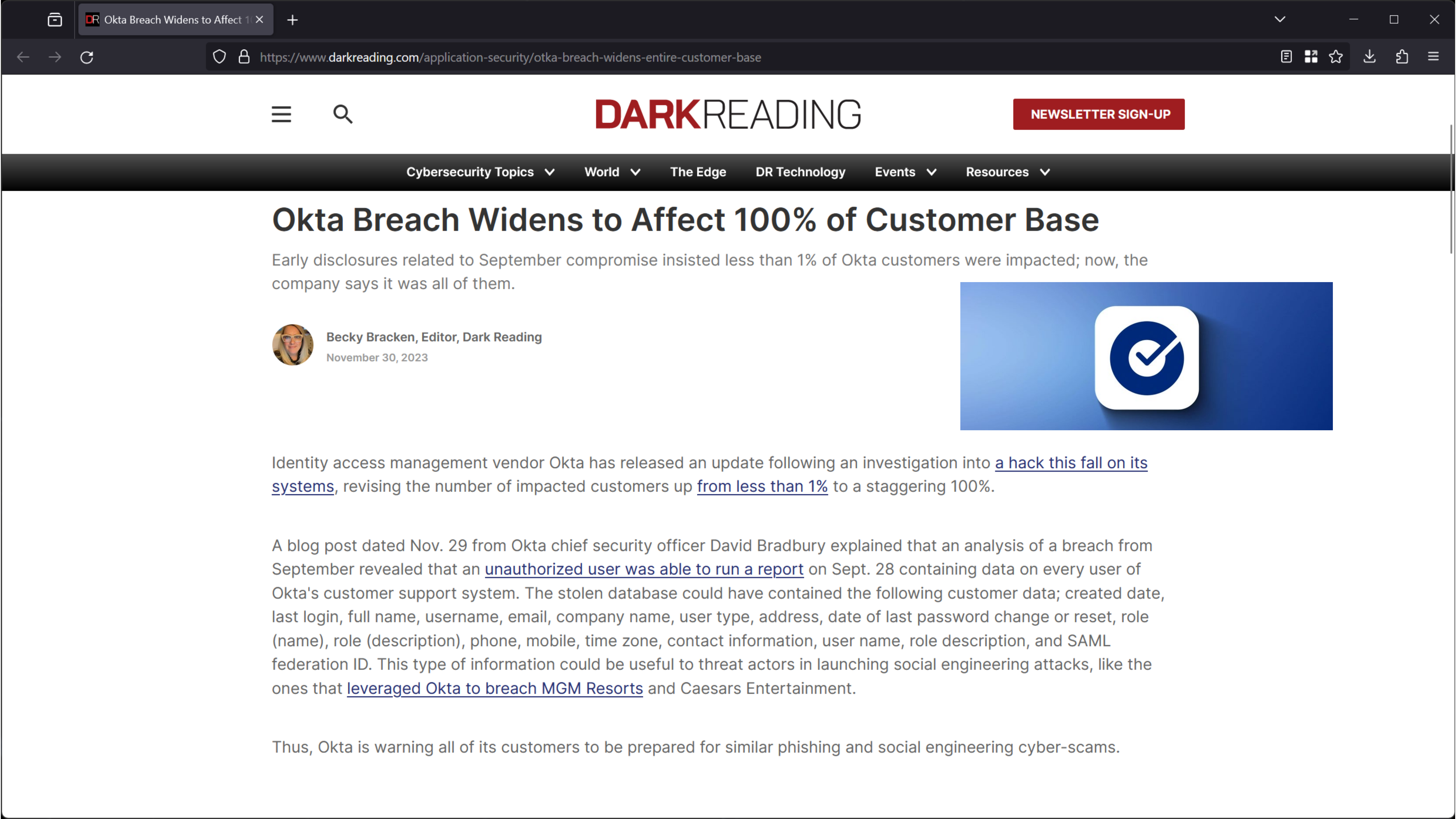
News By Anton Shilov published November 25, 2023

The full extent of the security breach is unknown.

Chimera, a Chinese-linked hacker group, infiltrated the network of the Dutch semiconductor giant NXP and had access for over two years from late 2017 to the beginning of 2020, reports NRC. During this period, the notorious hackers reportedly stole intellectual property, including chip designs — however, the full extent of the theft is yet to be disclosed. NXP is the largest chipmaker in Europe, and the scale and extent of the reported attack is shocking.

According to the report, the breach remained undetected for roughly two and a half years while the hackers lurked in the company's network — the breach was only discovered because a similar attack occurred on the Dutch airline Transavia, a subsidiary of KLM. Hackers accessed Transavia's reservation systems in September 2019. An investigation of the Transavia hack uncovered communications with NXP IPs, which led to the discovery of the NXP hack. The attack bears all of the hallmarks of the Chimera hacking group, including the use of its ChimeRAR hacker tool.

To break into NXP, the hackers initially used credentials from previous data leaks on platforms like LinkedIn or Facebook and then used brute force attacks to guess the passwords. They also bypassed double authentication measures by


Okta Breach Widens to Affect 1
https://www.darkreading.com/application-security/otka-breach-widens-entire-customer-base
DARKREADING
NEWSLETTER SIGN-UP
Cybersecurity Topics
World
The Edge
DR Technology
Events
Resources

Okta Breach Widens to Affect 100% of Customer Base

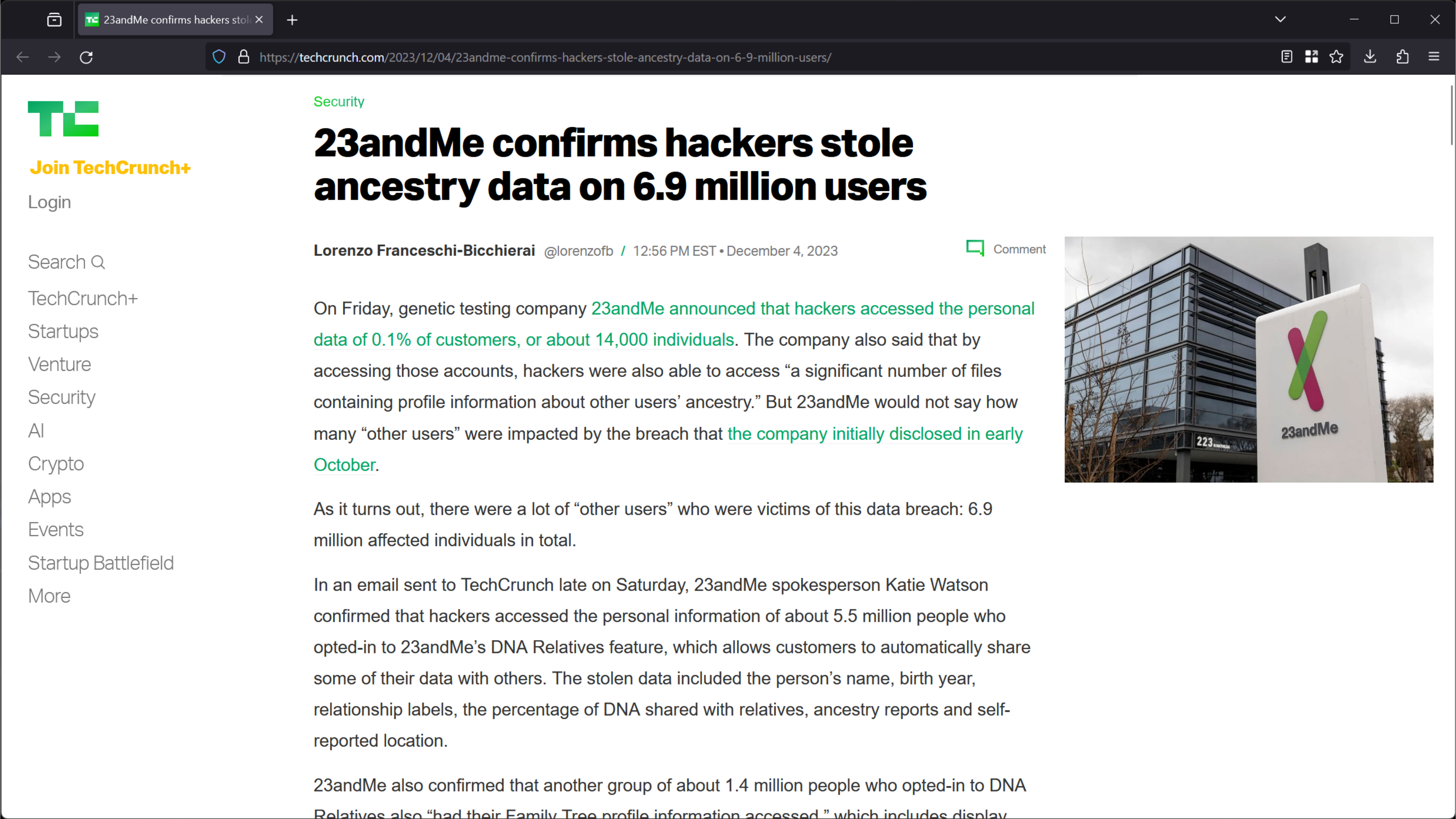
Early disclosures related to September compromise insisted less than 1% of Okta customers were impacted; now, the company says it was all of them.

Becky Bracken, Editor, Dark Reading
November 30, 2023

Identity access management vendor Okta has released an update following an investigation into a hack this fall on its systems, revising the number of impacted customers up from less than 1% to a staggering 100%.

A blog post dated Nov. 29 from Okta chief security officer David Bradbury explained that an analysis of a breach from September revealed that an unauthorized user was able to run a report on Sept. 28 containing data on every user of Okta's customer support system. The stolen database could have contained the following customer data; created date, last login, full name, username, email, company name, user type, address, date of last password change or reset, role (name), role (description), phone, mobile, time zone, contact information, user name, role description, and SAML federation ID. This type of information could be useful to threat actors in launching social engineering attacks, like the ones that leveraged Okta to breach MGM Resorts and Caesars Entertainment.

Thus, Okta is warning all of its customers to be prepared for similar phishing and social engineering cyber-scams.


23andMe confirms hackers stol
https://techcrunch.com/2023/12/04/23andme-confirms-hackers-stole-ancestry-data-on-6-9-million-users/
Join TechCrunch+
Login
Search
TechCrunch+
Startups
Venture
Security
AI
Crypto
Apps
Events
Startup Battlefield
More
Comment
223
23andMe

Security

23andMe confirms hackers stole ancestry data on 6.9 million users

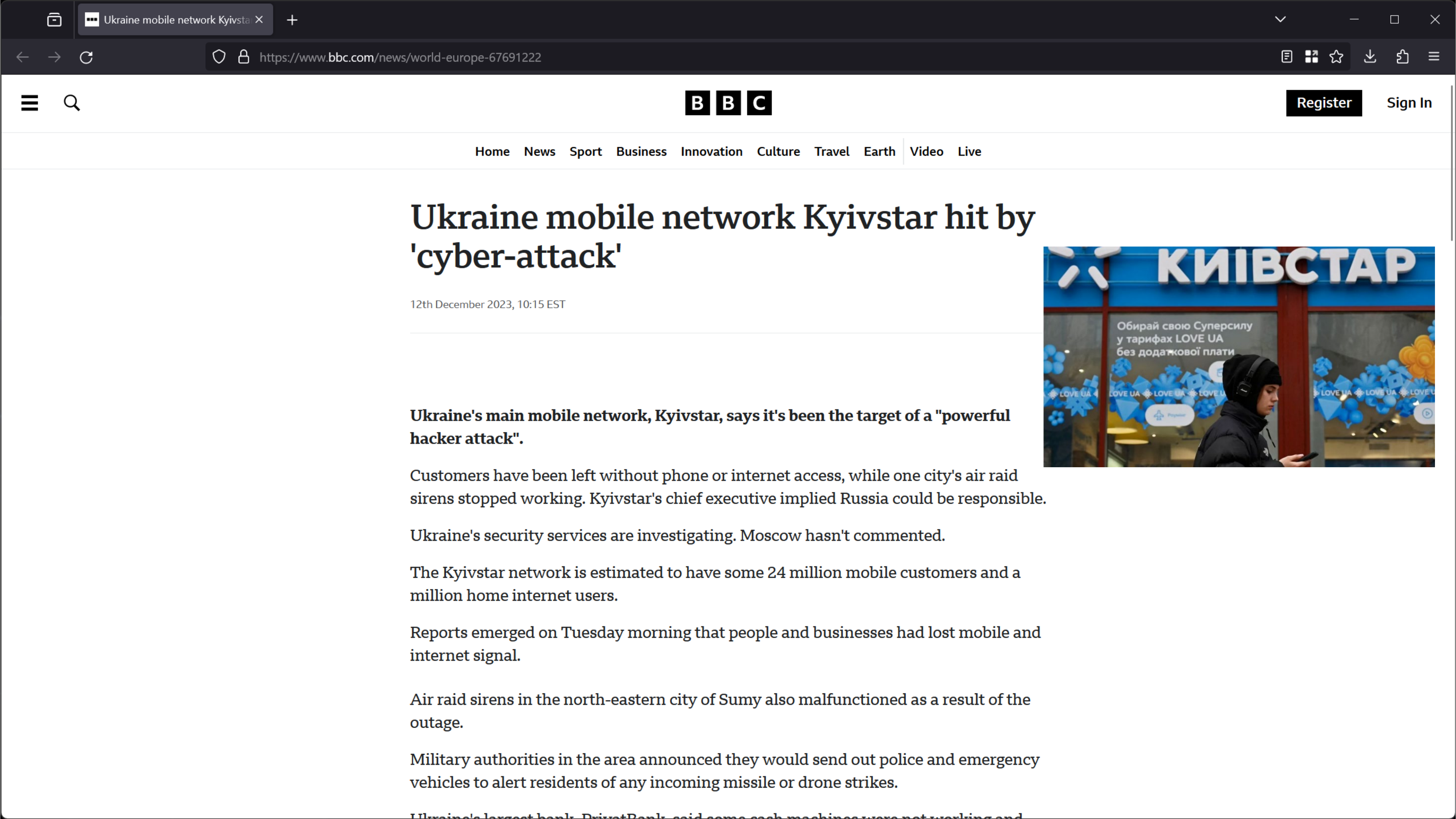
Lorenzo Franceschi-Bicchierai @lorenzofb / 12:56 PM EST • December 4, 2023

On Friday, genetic testing company 23andMe announced that hackers accessed the personal data of 0.1% of customers, or about 14,000 individuals. The company also said that by accessing those accounts, hackers were also able to access “a significant number of files containing profile information about other users’ ancestry.” But 23andMe would not say how many “other users” were impacted by the breach that the company initially disclosed in early October.

As it turns out, there were a lot of “other users” who were victims of this data breach: 6.9 million affected individuals in total.

In an email sent to TechCrunch late on Saturday, 23andMe spokesperson Katie Watson confirmed that hackers accessed the personal information of about 5.5 million people who opted-in to 23andMe’s DNA Relatives feature, which allows customers to automatically share some of their data with others. The stolen data included the person’s name, birth year, relationship labels, the percentage of DNA shared with relatives, ancestry reports and self-reported location.

23andMe also confirmed that another group of about 1.4 million people who opted-in to DNA Relatives also “had their Family Tree profile information accessed,” which includes display



Ukraine mobile network Kyivstar hit by 'cyber-attack'

12th December 2023, 10:15 EST

Ukraine's main mobile network, Kyivstar, says it's been the target of a "powerful hacker attack".

Customers have been left without phone or internet access, while one city's air raid sirens stopped working. Kyivstar's chief executive implied Russia could be responsible.

Ukraine's security services are investigating. Moscow hasn't commented.

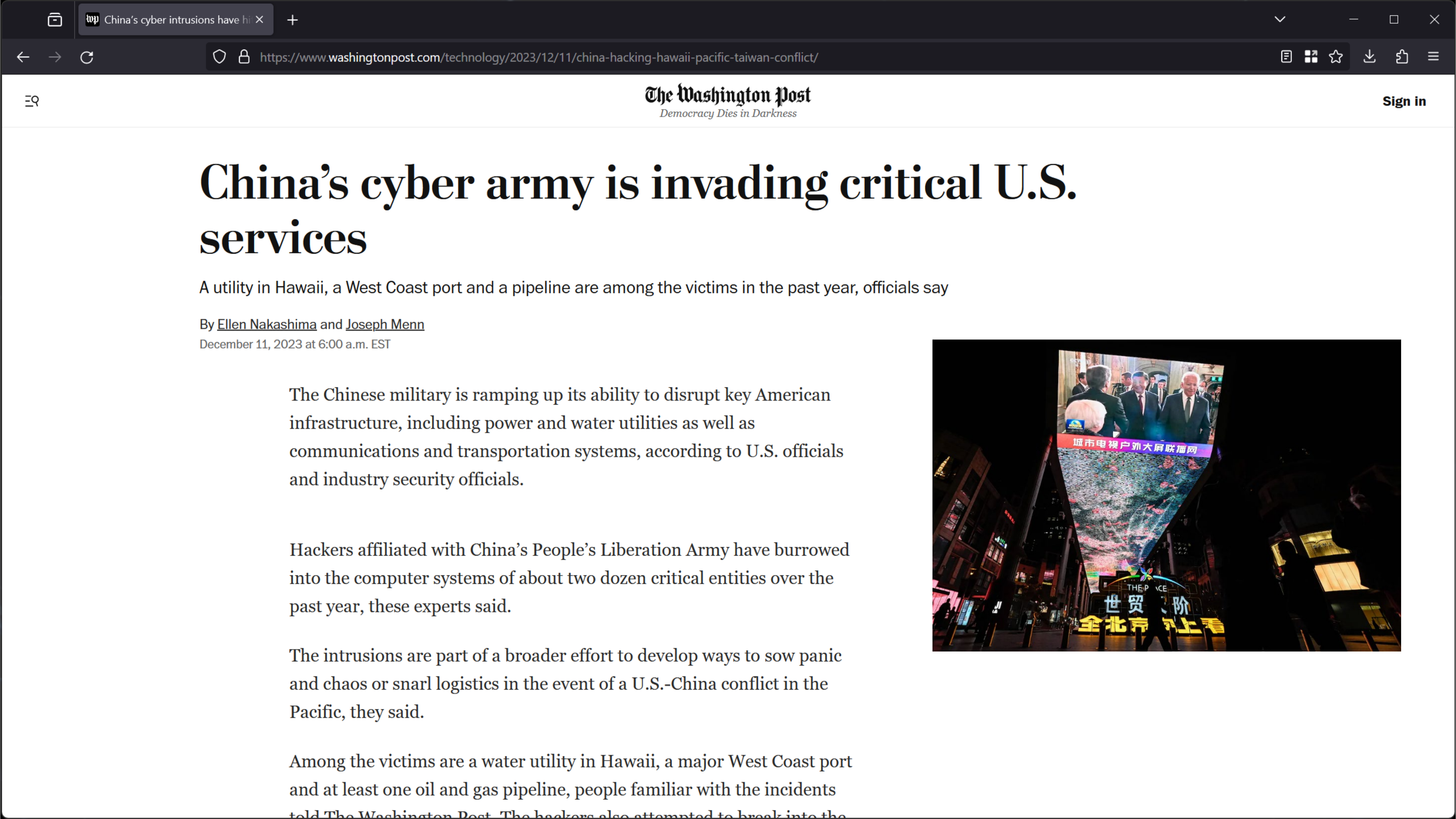
The Kyivstar network is estimated to have some 24 million mobile customers and a million home internet users.

Reports emerged on Tuesday morning that people and businesses had lost mobile and internet signal.

Air raid sirens in the north-eastern city of Sumy also malfunctioned as a result of the outage.

Military authorities in the area announced they would send out police and emergency vehicles to alert residents of any incoming missile or drone strikes.

Ukraine's largest bank, PrivatBank, said some cash machines were not working and


China's cyber intrusions have hi
https://www.washingtonpost.com/technology/2023/12/11/china-hacking-hawaii-pacific-taiwan-conflict/
Sign in

The Washington Post
Democracy Dies in Darkness

China's cyber army is invading critical U.S. services

A utility in Hawaii, a West Coast port and a pipeline are among the victims in the past year, officials say

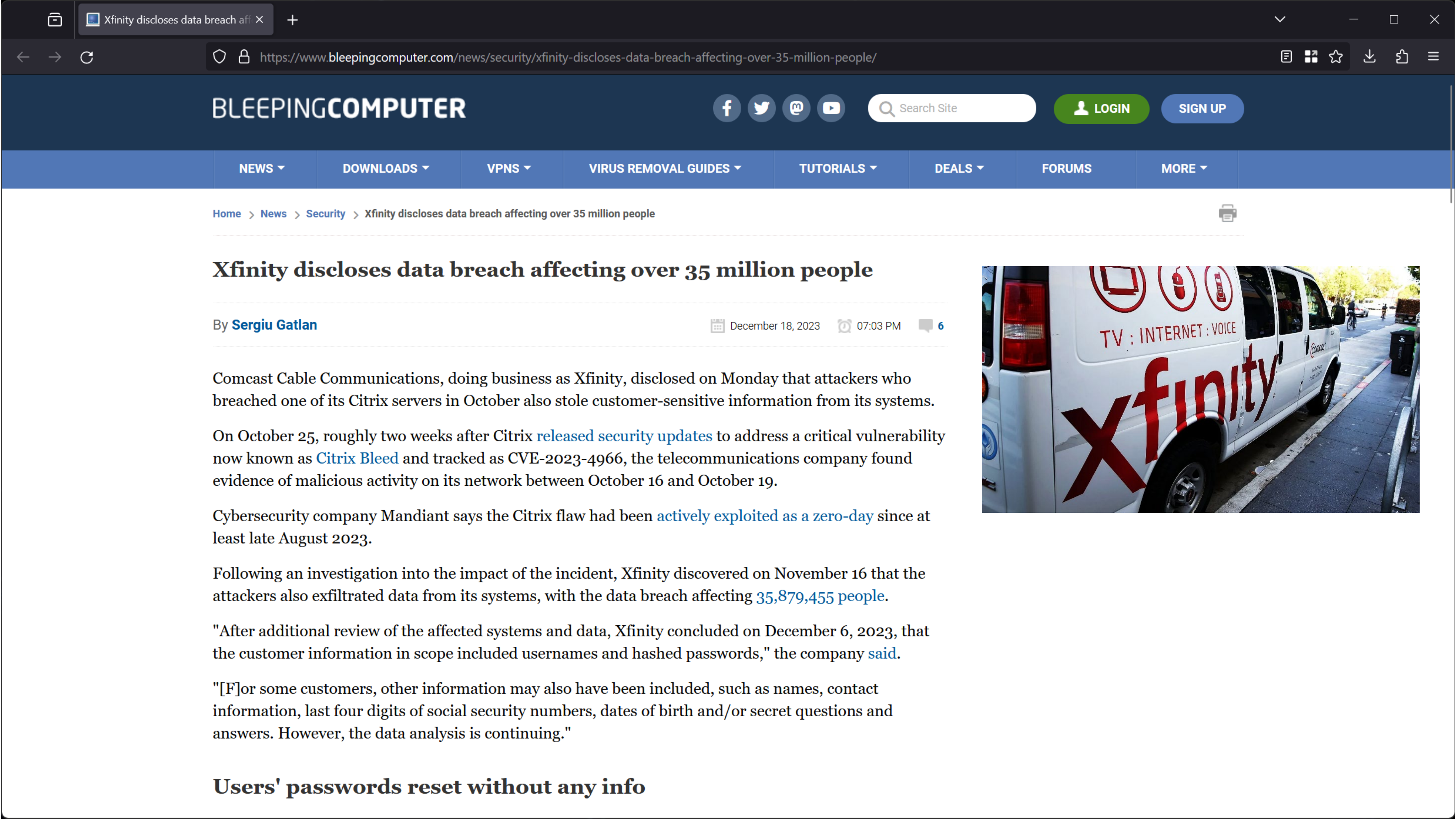
By Ellen Nakashima and Joseph Menn
December 11, 2023 at 6:00 a.m. EST

The Chinese military is ramping up its ability to disrupt key American infrastructure, including power and water utilities as well as communications and transportation systems, according to U.S. officials and industry security officials.

Hackers affiliated with China's People's Liberation Army have burrowed into the computer systems of about two dozen critical entities over the past year, these experts said.

The intrusions are part of a broader effort to develop ways to sow panic and chaos or snarl logistics in the event of a U.S.-China conflict in the Pacific, they said.

Among the victims are a water utility in Hawaii, a major West Coast port and at least one oil and gas pipeline, people familiar with the incidents told The Washington Post. The hackers also attempted to break into the


Xfinity discloses data breach aff
https://www.bleepingcomputer.com/news/security/xfinity-discloses-data-breach-affecting-over-35-million-people/
BLEEPINGCOMPUTER
Search Site
LOGIN
SIGN UP
NEWS
DOWNLOADS
VPNS
VIRUS REMOVAL GUIDES
TUTORIALS
DEALS
FORUMS
MORE
TV : INTERNET : VOICE
xfinity
Comcast

Home > News > Security > Xfinity discloses data breach affecting over 35 million people

Xfinity discloses data breach affecting over 35 million people

By **Sergiu Gatlan**　December 18, 2023　07:03 PM　6

Comcast Cable Communications, doing business as Xfinity, disclosed on Monday that attackers who breached one of its Citrix servers in October also stole customer-sensitive information from its systems.

On October 25, roughly two weeks after Citrix released security updates to address a critical vulnerability now known as Citrix Bleed and tracked as CVE-2023-4966, the telecommunications company found evidence of malicious activity on its network between October 16 and October 19.

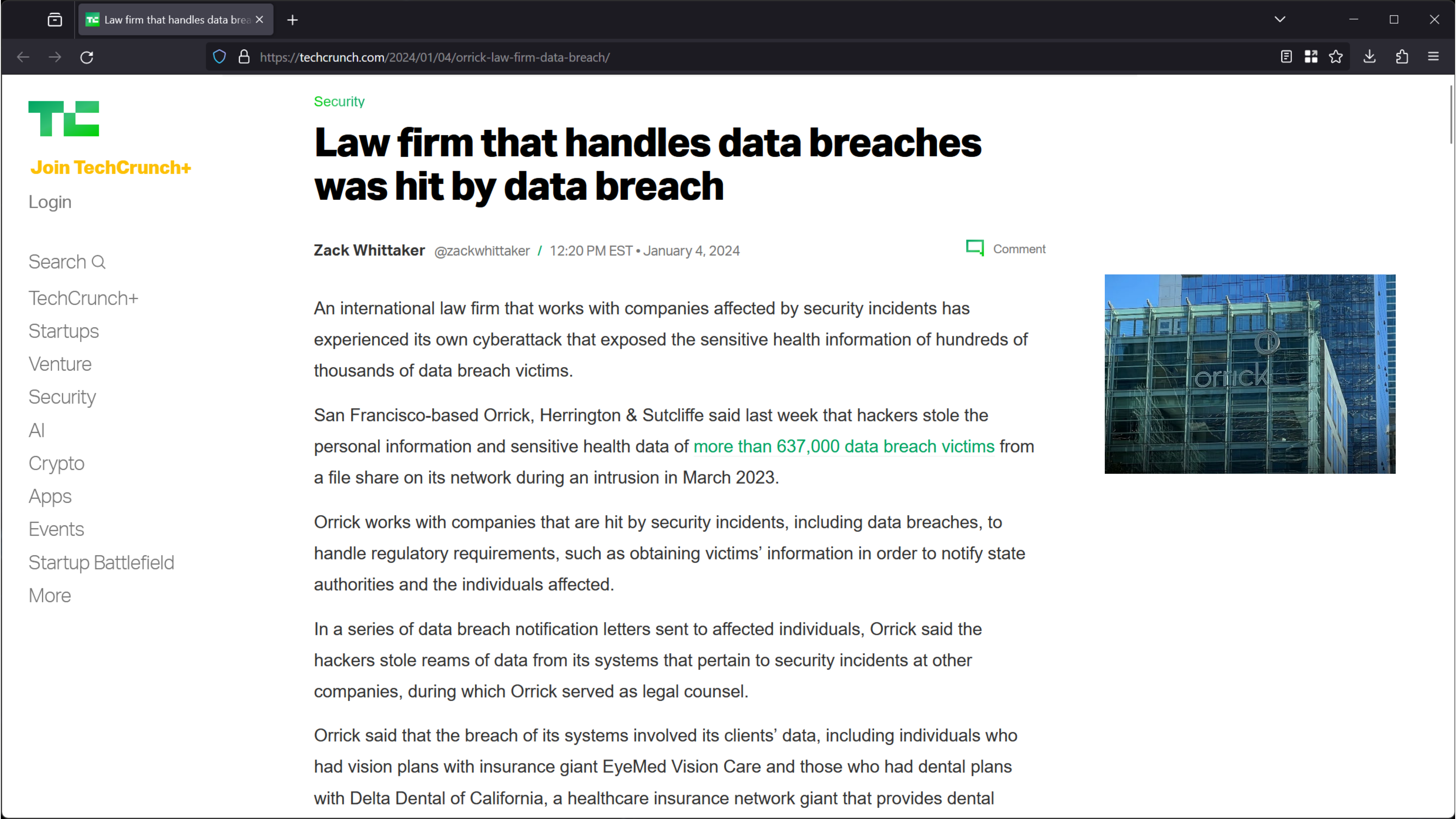
Cybersecurity company Mandiant says the Citrix flaw had been actively exploited as a zero-day since at least late August 2023.

Following an investigation into the impact of the incident, Xfinity discovered on November 16 that the attackers also exfiltrated data from its systems, with the data breach affecting 35,879,455 people.

"After additional review of the affected systems and data, Xfinity concluded on December 6, 2023, that the customer information in scope included usernames and hashed passwords," the company said.

"[F]or some customers, other information may also have been included, such as names, contact information, last four digits of social security numbers, dates of birth and/or secret questions and answers. However, the data analysis is continuing."

Users' passwords reset without any info



Security

Law firm that handles data breaches was hit by data breach

Zack Whittaker @zackwhittaker / 12:20 PM EST • January 4, 2024

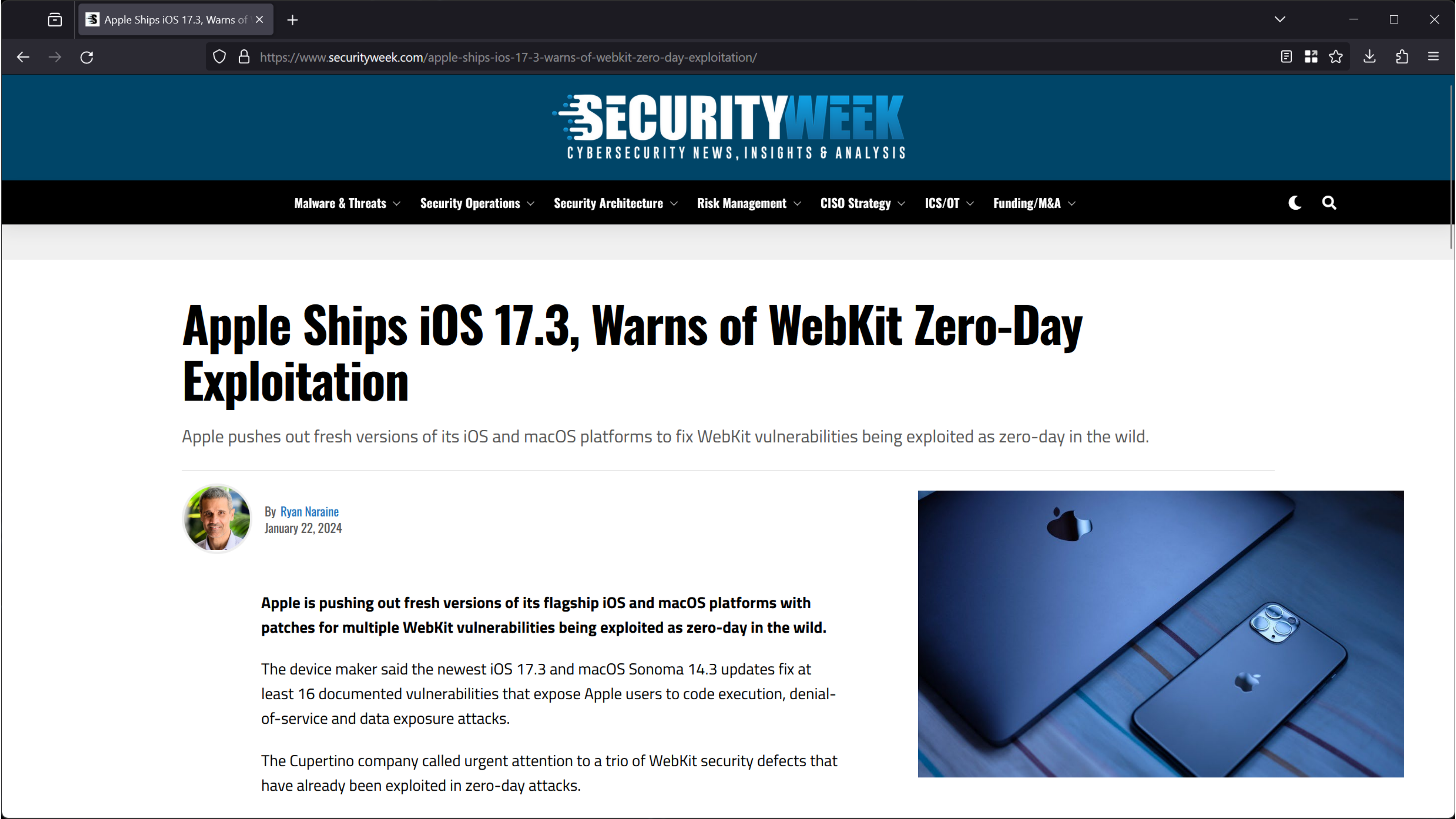
An international law firm that works with companies affected by security incidents has experienced its own cyberattack that exposed the sensitive health information of hundreds of thousands of data breach victims.

San Francisco-based Orrick, Herrington & Sutcliffe said last week that hackers stole the personal information and sensitive health data of more than 637,000 data breach victims from a file share on its network during an intrusion in March 2023.

Orrick works with companies that are hit by security incidents, including data breaches, to handle regulatory requirements, such as obtaining victims' information in order to notify state authorities and the individuals affected.

In a series of data breach notification letters sent to affected individuals, Orrick said the hackers stole reams of data from its systems that pertain to security incidents at other companies, during which Orrick served as legal counsel.

Orrick said that the breach of its systems involved its clients' data, including individuals who had vision plans with insurance giant EyeMed Vision Care and those who had dental plans with Delta Dental of California, a healthcare insurance network giant that provides dental


Apple Ships iOS 17.3, Warns of
https://www.securityweek.com/apple-ships-ios-17-3-warns-of-webkit-zero-day-exploitation/
SECURITYWEEK
CYBERSECURITY NEWS, INSIGHTS & ANALYSIS
Malware & Threats
Security Operations
Security Architecture
Risk Management
CISO Strategy
ICS/OT
Funding/M&A

Apple Ships iOS 17.3, Warns of WebKit Zero-Day Exploitation

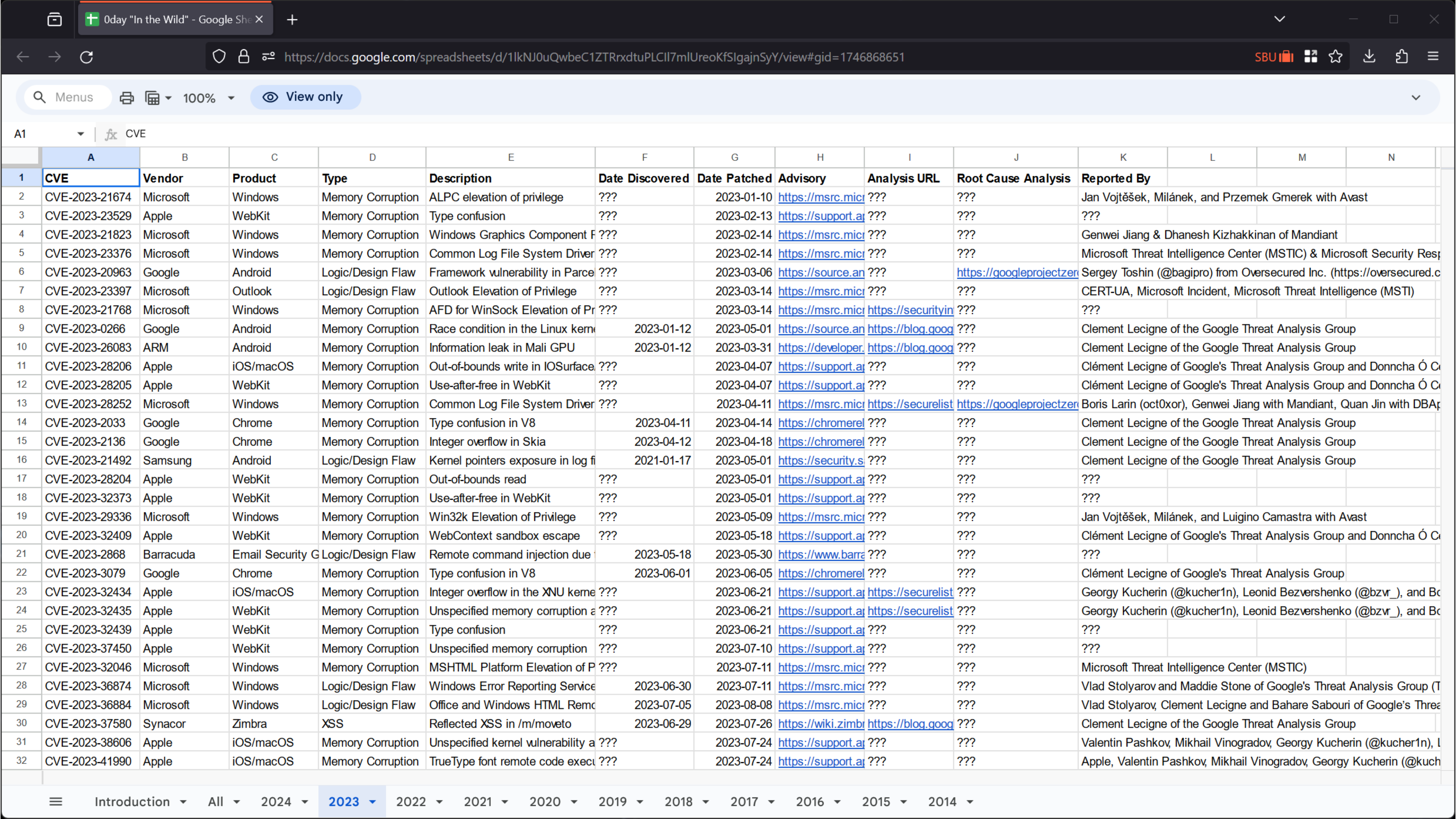
Apple pushes out fresh versions of its iOS and macOS platforms to fix WebKit vulnerabilities being exploited as zero-day in the wild.

By Ryan Naraine
January 22, 2024

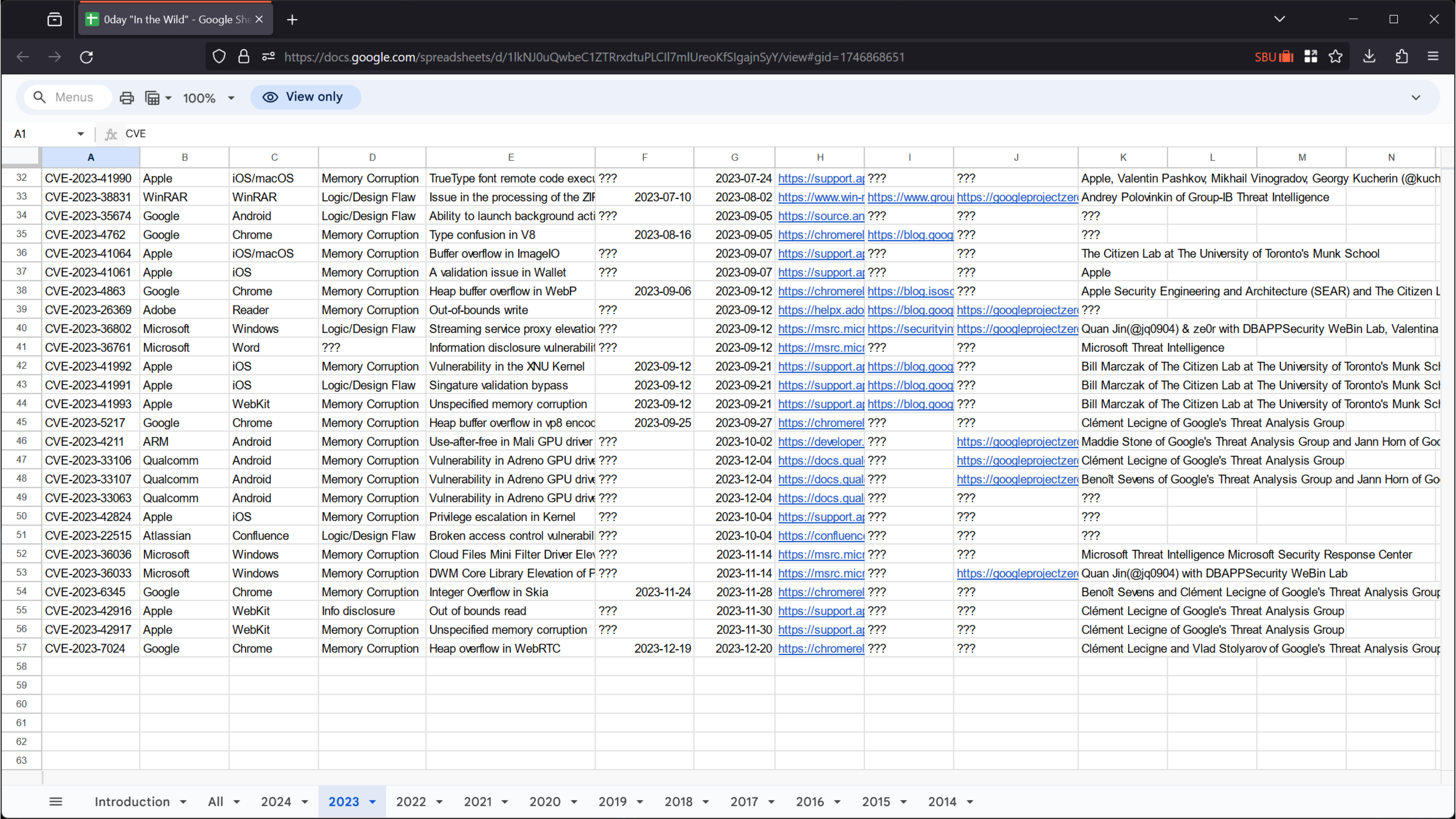
Apple is pushing out fresh versions of its flagship iOS and macOS platforms with patches for multiple WebKit vulnerabilities being exploited as zero-day in the wild.

The device maker said the newest iOS 17.3 and macOS Sonoma 14.3 updates fix at least 16 documented vulnerabilities that expose Apple users to code execution, denial-of-service and data exposure attacks.

The Cupertino company called urgent attention to a trio of WebKit security defects that have already been exploited in zero-day attacks.

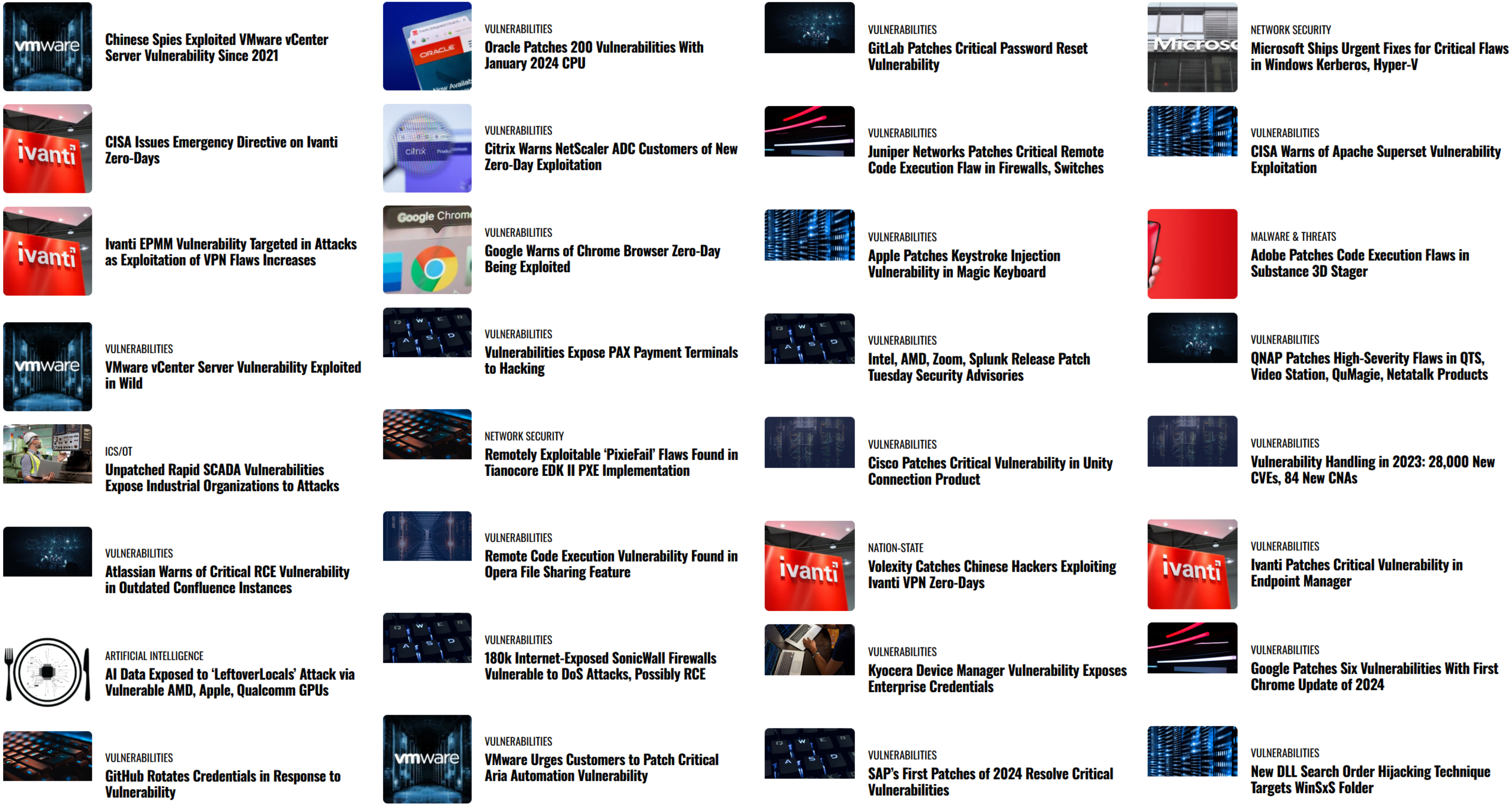

0day "In the Wild" - Google She
https://docs.google.com/spreadsheets/d/1lkNJ0uQwbeC1ZTRrxdtuPLCll7mlUreoKfSIgajnSyY/view#gid=1746868651
SBU
Menus
100%
View only
A1
fx
CVE
Introduction
All
2024
2023
2022
2021
2020
2019
2018
2017
2016
2015
2014

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	**CVE**	**Vendor**	**Product**	**Type**	**Description**	**Date Discovered**	**Date Patched**	**Advisory**	**Analysis URL**	**Root Cause Analysis**	**Reported By**			
2	CVE-2023-21674	Microsoft	Windows	Memory Corruption	ALPC elevation of privilege	???	2023-01-10	https://msrc.micr	???	???	Jan Vojtěšek, Milánek, and Przemek Gmerek with Avast			
3	CVE-2023-23529	Apple	WebKit	Memory Corruption	Type confusion	???	2023-02-13	https://support.ap	???	???	???			
4	CVE-2023-21823	Microsoft	Windows	Memory Corruption	Windows Graphics Component F	???	2023-02-14	https://msrc.micr	???	???	Genwei Jiang & Dhanesh Kizhakkinan of Mandiant			
5	CVE-2023-23376	Microsoft	Windows	Memory Corruption	Common Log File System Driver	???	2023-02-14	https://msrc.micr	???	???	Microsoft Threat Intelligence Center (MSTIC) & Microsoft Security Resp			
6	CVE-2023-20963	Google	Android	Logic/Design Flaw	Framework vulnerability in Parcel	???	2023-03-06	https://source.an	???	https://googleprojectzer	Sergey Toshin (@bagipro) from Oversecured Inc. (https://oversecured.c			
7	CVE-2023-23397	Microsoft	Outlook	Logic/Design Flaw	Outlook Elevation of Privilege	???	2023-03-14	https://msrc.micr	???	???	CERT-UA, Microsoft Incident, Microsoft Threat Intelligence (MSTI)			
8	CVE-2023-21768	Microsoft	Windows	Memory Corruption	AFD for WinSock Elevation of Pr	???	2023-03-14	https://msrc.micr	https://securityin	???	???			
9	CVE-2023-0266	Google	Android	Memory Corruption	Race condition in the Linux kern	2023-01-12	2023-05-01	https://source.an	https://blog.goog	???	Clement Lecigne of the Google Threat Analysis Group			
10	CVE-2023-26083	ARM	Android	Memory Corruption	Information leak in Mali GPU	2023-01-12	2023-03-31	https://developer.	https://blog.goog	???	Clement Lecigne of the Google Threat Analysis Group			
11	CVE-2023-28206	Apple	iOS/macOS	Memory Corruption	Out-of-bounds write in IOSurface.	???	2023-04-07	https://support.ap	???	???	Clément Lecigne of Google's Threat Analysis Group and Donncha Ó C			
12	CVE-2023-28205	Apple	WebKit	Memory Corruption	Use-after-free in WebKit	???	2023-04-07	https://support.ap	???	???	Clément Lecigne of Google's Threat Analysis Group and Donncha Ó C			
13	CVE-2023-28252	Microsoft	Windows	Memory Corruption	Common Log File System Driver	???	2023-04-11	https://msrc.micr	https://securelist	https://googleprojectzer	Boris Larin (oct0xor), Genwei Jiang with Mandiant, Quan Jin with DBAp			
14	CVE-2023-2033	Google	Chrome	Memory Corruption	Type confusion in V8	2023-04-11	2023-04-14	https://chromerel	???	???	Clement Lecigne of the Google Threat Analysis Group			
15	CVE-2023-2136	Google	Chrome	Memory Corruption	Integer overflow in Skia	2023-04-12	2023-04-18	https://chromerel	???	???	Clement Lecigne of the Google Threat Analysis Group			
16	CVE-2023-21492	Samsung	Android	Logic/Design Flaw	Kernel pointers exposure in log fi	2021-01-17	2023-05-01	https://security.s	???	???	Clement Lecigne of the Google Threat Analysis Group			
17	CVE-2023-28204	Apple	WebKit	Memory Corruption	Out-of-bounds read	???	2023-05-01	https://support.ap	???	???	???			
18	CVE-2023-32373	Apple	WebKit	Memory Corruption	Use-after-free in WebKit	???	2023-05-01	https://support.ap	???	???	???			
19	CVE-2023-29336	Microsoft	Windows	Memory Corruption	Win32k Elevation of Privilege	???	2023-05-09	https://msrc.micr	???	???	Jan Vojtěšek, Milánek, and Luigino Camastra with Avast			
20	CVE-2023-32409	Apple	WebKit	Memory Corruption	WebContext sandbox escape	???	2023-05-18	https://support.ap	???	???	Clément Lecigne of Google's Threat Analysis Group and Donncha Ó C			
21	CVE-2023-2868	Barracuda	Email Security G	Logic/Design Flaw	Remote command injection due	2023-05-18	2023-05-30	https://www.barra	???	???	???			
22	CVE-2023-3079	Google	Chrome	Memory Corruption	Type confusion in V8	2023-06-01	2023-06-05	https://chromerel	???	???	Clément Lecigne of Google's Threat Analysis Group			
23	CVE-2023-32434	Apple	iOS/macOS	Memory Corruption	Integer overflow in the XNU kerne	???	2023-06-21	https://support.ap	https://securelist	???	Georgy Kucherin (@kucher1n), Leonid Bezvershenko (@bzvr_), and Bo			
24	CVE-2023-32435	Apple	WebKit	Memory Corruption	Unspecified memory corruption a	???	2023-06-21	https://support.ap	https://securelist	???	Georgy Kucherin (@kucher1n), Leonid Bezvershenko (@bzvr_), and Bo			
25	CVE-2023-32439	Apple	WebKit	Memory Corruption	Type confusion	???	2023-06-21	https://support.ap	???	???	???			
26	CVE-2023-37450	Apple	WebKit	Memory Corruption	Unspecified memory corruption	???	2023-07-10	https://support.ap	???	???	???			
27	CVE-2023-32046	Microsoft	Windows	Memory Corruption	MSHTML Platform Elevation of P	???	2023-07-11	https://msrc.micr	???	???	Microsoft Threat Intelligence Center (MSTIC)			
28	CVE-2023-36874	Microsoft	Windows	Logic/Design Flaw	Windows Error Reporting Service	2023-06-30	2023-07-11	https://msrc.micr	???	???	Vlad Stolyarov and Maddie Stone of Google's Threat Analysis Group (T			
29	CVE-2023-36884	Microsoft	Windows	Logic/Design Flaw	Office and Windows HTML Remo	2023-07-05	2023-08-08	https://msrc.micr	???	???	Vlad Stolyarov, Clement Lecigne and Bahare Sabouri of Google's Threa			
30	CVE-2023-37580	Synacor	Zimbra	XSS	Reflected XSS in /m/moveto	2023-06-29	2023-07-26	https://wiki.zimbr	https://blog.goog	???	Clement Lecigne of the Google Threat Analysis Group			
31	CVE-2023-38606	Apple	iOS/macOS	Memory Corruption	Unspecified kernel vulnerability a	???	2023-07-24	https://support.ap	???	???	Valentin Pashkov, Mikhail Vinogradov, Georgy Kucherin (@kucher1n), L			
32	CVE-2023-41990	Apple	iOS/macOS	Memory Corruption	TrueType font remote code execu	???	2023-07-24	https://support.ap	???	???	Apple, Valentin Pashkov, Mikhail Vinogradov, Georgy Kucherin (@kuch			


0day "In the Wild" - Google She
https://docs.google.com/spreadsheets/d/1lkNJ0uQwbeC1ZTRrxdtuPLCIl7mlUreoKfSIgajnSyY/view#gid=1746868651
SBU
Menus
100%
View only
A1
CVE
Introduction
All
2024
2023
2022
2021
2020
2019
2018
2017
2016
2015
2014

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
32	CVE-2023-41990	Apple	iOS/macOS	Memory Corruption	TrueType font remote code execu	???	2023-07-24	https://support.a	???	???	Apple, Valentin Pashkov, Mikhail Vinogradov, Georgy Kucherin (@kuch			
33	CVE-2023-38831	WinRAR	WinRAR	Logic/Design Flaw	Issue in the processing of the ZIF	2023-07-10	2023-08-02	https://www.win-r	https://www.grou	https://googleprojectzer	Andrey Polovinkin of Group-IB Threat Intelligence			
34	CVE-2023-35674	Google	Android	Logic/Design Flaw	Ability to launch background acti	???	2023-09-05	https://source.an	???	???	???			
35	CVE-2023-4762	Google	Chrome	Memory Corruption	Type confusion in V8	2023-08-16	2023-09-05	https://chromerel	https://blog.goog	???	???			
36	CVE-2023-41064	Apple	iOS/macOS	Memory Corruption	Buffer overflow in ImageIO	???	2023-09-07	https://support.a	???	???	The Citizen Lab at The University of Toronto's Munk School			
37	CVE-2023-41061	Apple	iOS	Memory Corruption	A validation issue in Wallet	???	2023-09-07	https://support.a	???	???	Apple			
38	CVE-2023-4863	Google	Chrome	Memory Corruption	Heap buffer overflow in WebP	2023-09-06	2023-09-12	https://chromerel	https://blog.isosc	???	Apple Security Engineering and Architecture (SEAR) and The Citizen L			
39	CVE-2023-26369	Adobe	Reader	Memory Corruption	Out-of-bounds write	???	2023-09-12	https://helpx.ado	https://blog.goog	https://googleprojectzer	???			
40	CVE-2023-36802	Microsoft	Windows	Logic/Design Flaw	Streaming service proxy elevatio	???	2023-09-12	https://msrc.micr	https://securityin	https://googleprojectzer	Quan Jin(@jq0904) & ze0r with DBAPPSecurity WeBin Lab, Valentina			
41	CVE-2023-36761	Microsoft	Word	???	Information disclosure vulnerabili	???	2023-09-12	https://msrc.micr	???	???	Microsoft Threat Intelligence			
42	CVE-2023-41992	Apple	iOS	Memory Corruption	Vulnerability in the XNU Kernel	2023-09-12	2023-09-21	https://support.a	https://blog.goog	???	Bill Marczak of The Citizen Lab at The University of Toronto's Munk Sch			
43	CVE-2023-41991	Apple	iOS	Logic/Design Flaw	Singature validation bypass	2023-09-12	2023-09-21	https://support.a	https://blog.goog	???	Bill Marczak of The Citizen Lab at The University of Toronto's Munk Sch			
44	CVE-2023-41993	Apple	WebKit	Memory Corruption	Unspecified memory corruption	2023-09-12	2023-09-21	https://support.a	https://blog.goog	???	Bill Marczak of The Citizen Lab at The University of Toronto's Munk Sch			
45	CVE-2023-5217	Google	Chrome	Memory Corruption	Heap buffer overflow in vp8 encoc	2023-09-25	2023-09-27	https://chromerel	???	???	Clément Lecigne of Google's Threat Analysis Group			
46	CVE-2023-4211	ARM	Android	Memory Corruption	Use-after-free in Mali GPU driver	???	2023-10-02	https://developer.	???	https://googleprojectzer	Maddie Stone of Google's Threat Analysis Group and Jann Horn of Goo			
47	CVE-2023-33106	Qualcomm	Android	Memory Corruption	Vulnerability in Adreno GPU driv	???	2023-12-04	https://docs.qual	???	https://googleprojectzer	Clément Lecigne of Google's Threat Analysis Group			
48	CVE-2023-33107	Qualcomm	Android	Memory Corruption	Vulnerability in Adreno GPU driv	???	2023-12-04	https://docs.qual	???	https://googleprojectzer	Benoît Sevens of Google's Threat Analysis Group and Jann Horn of Goo			
49	CVE-2023-33063	Qualcomm	Android	Memory Corruption	Vulnerability in Adreno GPU driv	???	2023-12-04	https://docs.qual	???	???	???			
50	CVE-2023-42824	Apple	iOS	Memory Corruption	Privilege escalation in Kernel	???	2023-10-04	https://support.a	???	???	???			
51	CVE-2023-22515	Atlassian	Confluence	Logic/Design Flaw	Broken access control vulnerabil	???	2023-10-04	https://confluenc	???	???	???			
52	CVE-2023-36036	Microsoft	Windows	Memory Corruption	Cloud Files Mini Filter Driver Elev	???	2023-11-14	https://msrc.micr	???	???	Microsoft Threat Intelligence Microsoft Security Response Center			
53	CVE-2023-36033	Microsoft	Windows	Memory Corruption	DWM Core Library Elevation of P	???	2023-11-14	https://msrc.micr	???	https://googleprojectzer	Quan Jin(@jq0904) with DBAPPSecurity WeBin Lab			
54	CVE-2023-6345	Google	Chrome	Memory Corruption	Integer Overflow in Skia	2023-11-24	2023-11-28	https://chromerel	???	???	Benoît Sevens and Clément Lecigne of Google's Threat Analysis Grour			
55	CVE-2023-42916	Apple	WebKit	Info disclosure	Out of bounds read	???	2023-11-30	https://support.a	???	???	Clément Lecigne of Google's Threat Analysis Group			
56	CVE-2023-42917	Apple	WebKit	Memory Corruption	Unspecified memory corruption	???	2023-11-30	https://support.a	???	???	Clément Lecigne of Google's Threat Analysis Group			
57	CVE-2023-7024	Google	Chrome	Memory Corruption	Heap overflow in WebRTC	2023-12-19	2023-12-20	https://chromerel	???	???	Clément Lecigne and Vlad Stolyarov of Google's Threat Analysis Group			
58														
59														
60														
61														
62														
63														

Just a sample of vulnerabilities in the past *three weeks*…



Chinese Spies Exploited VMware vCenter Server Vulnerability Since 2021

CISA Issues Emergency Directive on Ivanti Zero-Days

Ivanti EPMM Vulnerability Targeted in Attacks as Exploitation of VPN Flaws Increases

VULNERABILITIES
VMware vCenter Server Vulnerability Exploited in Wild

ICS/OT
Unpatched Rapid SCADA Vulnerabilities Expose Industrial Organizations to Attacks

VULNERABILITIES
Atlassian Warns of Critical RCE Vulnerability in Outdated Confluence Instances

ARTIFICIAL INTELLIGENCE
AI Data Exposed to 'LeftoverLocals' Attack via Vulnerable AMD, Apple, Qualcomm GPUs

VULNERABILITIES
GitHub Rotates Credentials in Response to Vulnerability

VULNERABILITIES
Oracle Patches 200 Vulnerabilities With January 2024 CPU

VULNERABILITIES
Citrix Warns NetScaler ADC Customers of New Zero-Day Exploitation

VULNERABILITIES
Google Warns of Chrome Browser Zero-Day Being Exploited

VULNERABILITIES
Vulnerabilities Expose PAX Payment Terminals to Hacking

NETWORK SECURITY
Remotely Exploitable 'PixieFail' Flaws Found in Tianocore EDK II PXE Implementation

VULNERABILITIES
Remote Code Execution Vulnerability Found in Opera File Sharing Feature

VULNERABILITIES
180k Internet-Exposed SonicWall Firewalls Vulnerable to DoS Attacks, Possibly RCE

VULNERABILITIES
VMware Urges Customers to Patch Critical Aria Automation Vulnerability

VULNERABILITIES
GitLab Patches Critical Password Reset Vulnerability

VULNERABILITIES
Juniper Networks Patches Critical Remote Code Execution Flaw in Firewalls, Switches

VULNERABILITIES
Apple Patches Keystroke Injection Vulnerability in Magic Keyboard

VULNERABILITIES
Intel, AMD, Zoom, Splunk Release Patch Tuesday Security Advisories

VULNERABILITIES
Cisco Patches Critical Vulnerability in Unity Connection Product

NATION-STATE
Volexity Catches Chinese Hackers Exploiting Ivanti VPN Zero-Days

VULNERABILITIES
Kyocera Device Manager Vulnerability Exposes Enterprise Credentials

VULNERABILITIES
SAP's First Patches of 2024 Resolve Critical Vulnerabilities

NETWORK SECURITY
Microsoft Ships Urgent Fixes for Critical Flaws in Windows Kerberos, Hyper-V

VULNERABILITIES
CISA Warns of Apache Superset Vulnerability Exploitation

MALWARE & THREATS
Adobe Patches Code Execution Flaws in Substance 3D Stager

VULNERABILITIES
QNAP Patches High-Severity Flaws in QTS, Video Station, QuMagie, Netatalk Products

VULNERABILITIES
Vulnerability Handling in 2023: 28,000 New CVEs, 84 New CNAs

VULNERABILITIES
Ivanti Patches Critical Vulnerability in Endpoint Manager

VULNERABILITIES
Google Patches Six Vulnerabilities With First Chrome Update of 2024

VULNERABILITIES
New DLL Search Order Hijacking Technique Targets WinSxS Folder

https://www.securityweek.com/category/vulnerabilities/

Network vs. System vs. Computer vs. Information Security

Not always a clear distinction

- PCs, servers, mobile/wearable devices, IoT, …
- Routers, switches, access points, SCADA, CPS, …
- Operating systems, software, plugins, …
- Protocols, workflows, configurations, …

Complex interactions

- Core internet protocols/services
- Distributed/web/cloud applications
- Third-party integrations

There is more

- People
- Physical security

Threats span all these areas

Network Security Arsenal

Cryptography: wide range of techniques for enabling secure, confidential, and anonymous communication

Access Control: authentication and authorization, firewalls, …

Monitoring: audit logs, network monitoring, intrusion detection, …

Rigorous protocol and system design, implementation, and testing: account for both benign failures and malicious actions

- Data corruption, timeouts, dead hosts, routing problems, …
- Eavesdropping, modification, injection, deletion, replay, …
- Software/hardware/protocol flaws: may turn into **vulnerabilities**

Threats

Exposure of data

Tampering with data

Denial of service

Impersonation

Forbidden access

Exposure of personal information

Identification of individuals

Threats	**Goals**
Exposure of data	Confidentiality
Tampering with data	Integrity
Denial of service	Availability
Impersonation	Authentication
Forbidden access	Authorization
Exposure of personal information	Privacy
Identification of individuals	Anonymity

Confidentiality

"The property that information is not made available or disclosed to unauthorized individuals, entities, or processes [i.e., to any unauthorized system entity]." [RFC2828]

Sensitive data must be protected

- In transit: network packets, network connections, messages, documents, …
- At rest: main memory (buffers, message queues), flash/disk storage, backups, …

Cryptography is a tool to achieve confidentiality

- Not the only one: access control, steganography, …

Content protection is often *not* enough

- Data vs. *metadata* (e.g., phone call content vs. phone call records)

Data Integrity

"The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner." [RFC2828]

Cryptography is a tool to achieve data integrity

Intentional or accidental data changes should be detectable

System integrity

"Attribute of an information system when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system." [CNSSI No. 4009]

Fragile: weak authentication, vulnerable software, social engineering, physical access, supply chain attacks, …

Availability

“The property of being accessible and useable upon demand by an authorized entity.” [CNSSI No. 4009]

Denial of Service (DoS) attacks are the most common way of affecting system availability

- Saturation of resources (bandwidth, CPU, memory, …)
- Disruption of configuration or state (routing, DNS, …)
- Data corruption, jamming, interference, physical damage, …

Malware can do more harm

- Ransomware: encrypt user files and then demand a ransom (Gpcode, Cryptolocker, WannaCry, Bad Rabbit, Petya, Ryuk, REvil, LockBit, …)
- Just wipe out data ➔ brick the system (Wiper, NotPetya, …)

Authentication

"The process of verifying an identity claimed by or for a system entity." [RFC2828]

Different approaches ("factors")

- Something you know (password, pin, …)
- Something you have (phone, token, …)
- Something you are (fingerprint, face, …)

Multi-factor authentication is a must

Cryptography is a tool to perform authentication

Password theft/leakage is a huge problem

Authorization

“Access privileges granted to a user, program, or process or the act of granting those privileges.” [CNSSI No. 4009]

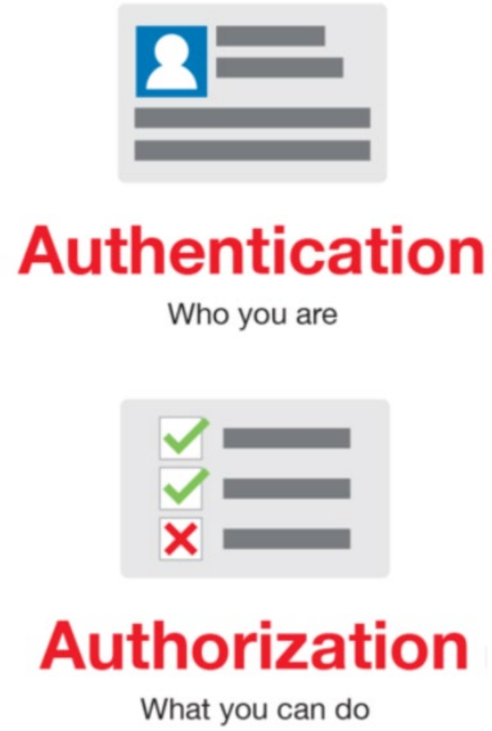
Authorization verifies that a user has the proper privileges to access a resource (presumes successful authentication)

Related term: *access control*

Access restriction based on various properties: identity, role, labels, date/time, IP address, domain, access frequency, …

One of the core goals of network and system security:

Keep unauthorized parties from gaining access to resources



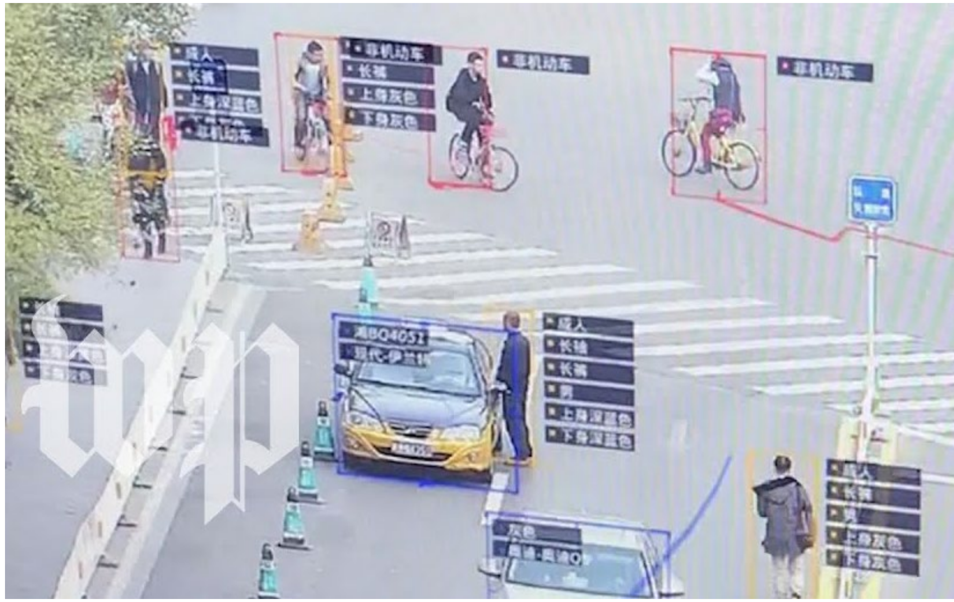
Privacy

"The right of an entity (normally a person), acting in its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share information about itself with others." [RFC2828]

Beyond private data (messages/files):

- Activities (browsing history, voice commands, …)
- Location (3/4/5G, GPS, WiFi, cameras, …)
- Preferences ("likes," Amazon, Netflix, …)
- Health (Fitbit, iWatch, …)
- …

Metadata is equally important!



Anonymity

"The state of being not identifiable within a set of subjects, the anonymity set." [Pfitzmann and Köhntopp]

The larger the anonymity set, the stronger the anonymity

Very different from privacy:

An anonymous action may be public, but the actor's identity remains unknown (e.g., vote in free elections)

Anonymous communication

Sender anonymity	(unknown sender, known receiver)
Receiver anonymity	(known sender, unknown receiver)
Unlinkability of sender and receiver	(unknown sender, unknown receiver)

Course Focus (you get the idea…)

Internet, technologies, protocols, applications, attacks, and defenses, from a highly practical perspective

Indicative topics

- Network protocols, eavesdropping, scanning, DoS attacks, firewalls, VPNs, proxies, intrusion detection, forensics, honeypots, encrypted communication, authentication, cloud services and applications, botnets, targeted attacks, privacy, anonymity, …

Goal: cultivate the "security mindset"

- Understand the tactics, techniques, and procedures (TTPs) of attackers
- Find vulnerabilities, subvert protections, bypass all the things
- Think sideways
- How to secure a system – know what to defend against

Play Fair

Cannot teach defense without offense, but:

Breaking into systems is illegal!

Unauthorized data access is illegal!

Computer Fraud and Abuse Act (CFAA)

http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf

Practice only on your own systems or controlled environment

Scanning/penetration testing of third-party systems may be allowed only after getting *written* permission by their owner

Course Information

Mixed format

- Lectures, hands-on sessions, research paper discussions, online discussion

Requirements

- Four programming assignments
- Midterm and final exams

Grading

- Assignments: 45% (split: 8%, 11%, 15%, 11%)
- Midterm: 15%
- Final: 40%

Late Policy

You are allowed **five** “late days” throughout the semester

- To be used at your discretion for any homework or project deliverables
- No prior communication is necessary
  (we will keep track of used late days)
- Each day (24h) is indivisible, and can be used only as a whole
  (even if a submission is just a few minutes late, this still counts as a whole day)
- Submission through Brightspace

Once all late days are used, late submissions will receive zero credit

Schedule (Tentative)

Ethics

Threat Landscape

Lower Layers

Core Protocols

Denial of Service

Firewalls and Gateways

Encrypted Communication

Authentication

SSL/TLS

Reconnaissance and Scanning

Intrusion Detection

Malware and Botnets

Honeypots and Deception

Email

Spam and Phishing

Web/Cloud

Tracking/Privacy

Anonymity/Online Freedom

Course web page

https://www.cs.stonybrook.edu/~mikepo/CSE508/

All slides will be posted on the public Schedule page

Please sign up on Piazza

https://piazza.com/stonybrook/spring2024/cse508

Q&A, discussion, homework descriptions, and additional resources

- Piazza supports private messages: please use that functionality (instead of email to the instructor or TAs) for any private questions
- You may want to install the Piazza app on your mobile device
- Sign up with your SBU email address