

STORM ⚡ WATCH

CYBERSECURITY NEWS

DateLine: 2024-02-27



LIKE



SUBSCRIBE

S T O R M ⚡ W A T C H



Storm ⚡ Watch by GreyNoise Intelligence

GreyNoise Intelligence

TECHNOLOGY · UPDATED WEEKLY

GreyNoise Storm ⚡ Watch is a weekly podcast and livestream hosted by GreyNoise Intelligence (<https://www.greynoise.io>), a cybersecurity company that focuses on understanding internet noise. The show features hosts b MORE

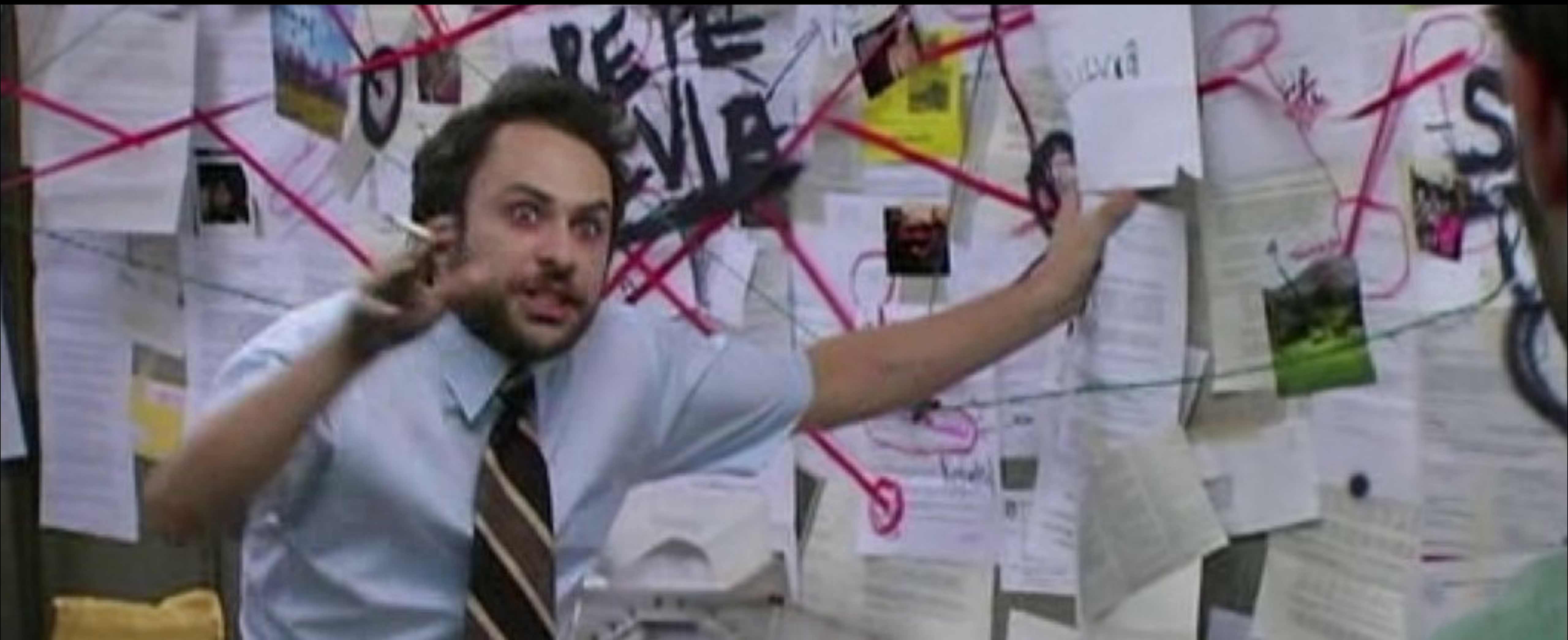
<https://StormWatch.ing>



LEAVE A
COMMENT



SHARE



LOCKBIT LOWDOWN





LOCK **BIT** **3.0**



LEAKED DATA

THIS SITE IS NOW UNDER THE CONTROL OF THE UK, THE US AND THE CRONOS TASK FORCE



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

You've Been Banned From LOCKBIT 3.0

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

Who is LockbitSupp?

2D 17H 25M 18S



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

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

US Indictments

PUBLISHED



FBI Investigation Leads to a Total of 5 LockBit Affiliates Charged By the Department of Justice. Two of Those Indictments Released Today.

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

Sanctions

0D 1H 55M 18S



United States Sanctions for Threat Actors Engaged in Significant Malicious Cyber Related Activity

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

Arrest in Poland

PUBLISHED

On 20/02/2024 a suspected LockBit actor was arrested in Poland on the request of the French judicial authorities.

Activity in Ukraine

PUBLISHED

On 20/02/2024 a suspected Lockbit actor was arrested in Ternopil (UA) by the local authorities.

Report Cyber Attacks!

PUBLISHED

Please report your Cyber Incident. To enable Law Enforcement to take protective and disruptive action, it is vital that victims report attacks and

Cyber Choices

PUBLISHED



CYBER CHOICES

Activate Windows Go to Settings to activate



<https://www.npu.gov.ua/news/slidchi-natspolitsii-prypynyly-dialnist-transnatsionalnoho-khakerskoho-uhropovannia-lockbit-v-ukraini>

The investigators of the National Police stopped the activities of the transnational hacking group "LockBit" in Ukraine

Posted on February 21, 2024 at 2:00 pm

This criminal cyber organization is considered the most authoritative in the world of extortionists and since 2019 has carried out more than three thousand cyber attacks on the infrastructure of the private sector in the United States and Europe with losses of billions of euros.

At the national level, the special operation took place with the participation of investigators of the Main Investigative Department of the National Police, cyber specialists of the Security Service of Ukraine under the procedural guidance of the Prosecutor General's Office, at the international level - under the coordination of Europol.

Hackers provided their virus software and infrastructure as a service to affiliates in Western Europe who encrypted victims' data, threatened them with information leaks, and demanded ransom. After receiving the funds, they were distributed between the main team of "LockBit" and affiliated persons, who received up to 75% of the criminal profits.

In Ukraine, the criminals were represented by a father and son, whose actions affected individuals, enterprises, state institutions and health care institutions in France.



-----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.

The problem doesn't just affect me. Anyone who has used a vulnerable version of PHP keep in mind that your server may have been compromised, I'm sure many competitors may have been hacked in the same way, but they didn't even realize how it happened. I'm sure the forums I know are also hacked in the same way via PHP, there are good reasons to be sure, not only because of my hack but also because of information from whistleblowers. I noticed the PHP problem by accident, and I'm the only one with a decentralized infrastructure with different servers, so I was able to quickly figure out how the attack happened, if I didn't have backup servers that didn't have PHP on them, I probably wouldn't have figured out how the hack happened.

The FBI decided to hack now for one reason only, because they didn't want to leak information from <https://fultoncountyga.gov/> the stolen documents contain a lot of interesting things and Donald Trump's court cases that could affect the upcoming US election. Personally I will vote for Trump because the situation on the border with Mexico is some kind of nightmare, Biden should retire, he is a puppet. If it wasn't for the FBI attack, the documents would have been released the same day, because the negotiations stalled, right after the partner posted the press release to the blog, the FBI really didn't like the public finding out the true reasons for the failure of all the systems of this city. Had it not been for the election situation, the FBI would have continued to sit on my server waiting for any leads to arrest me and my associates, but all you need to do to not get caught is just quality cryptocurrency laundering. The FBI can sit on your resources and also collect information useful for the FBI, but do not show the whole world that you are hacked, because you do not cause any critical damage, you bring only benefit. What conclusions can be drawn from this situation? Very simple, that I need to attack the .gov sector more often and more, it is after such attacks that the FBI will be forced to show me weaknesses and vulnerabilities and make me

“Due to my personal negligence and irresponsibility I relaxed and did not update PHP in time”

“I always have an active bug bounty program and I pay money for bugs found”

http://lockbit7z2jwcskxpbokpemdxmltipntwlkmidc1l2qirbu7ykg46eyd.onion/fbi.gov/fbi.gov_en.txt

- LockBit initially set a release date for the data on February 16 but removed the countdown after Fulton County refused to negotiate a ransom.
- The data allegedly includes documents related to former President Trump's prosecution and could jeopardize other criminal trials.
- The FBI and U.K.'s National Crime Agency seized LockBit's websites and released a free decryption tool as part of "Operation Cronos."
- LockBit is regrouping, claims to have retained copies of stolen data despite the law enforcement action, has set up new dark web sites, and threatens to release the data on March 2 unless a ransom is paid.
- LockBitSupp has placed a bounty on his own identity and denies that the FBI knows his real-life identity.
- Fulton County is still recovering from the ransomware attack and working to restore services.

<https://krebsonsecurity.com/2024/02/fbis-lockbit-takedown-postponed-a-ticking-time-bomb-in-fulton-county-ga/>

Deadline: 02 Mar, 2024 04:27:14 UTC

[no logo]

fultoncountyga.gov

Fulton County is governed by a seven-member Board of Commissioners who are elected to four-year terms. Six of the members are district commissioners, and the Chairman is At-Large, representing all of Fulton County. The Board of Commissioners meets on the first and third Wednesday of each month at 10

You can contact the main system administrator on the contacts below, waiting for an answer can take some time from 1 minute to several days depending on the workload.

Contact Us

Tox

<https://tox.chat/download.html>

3085B89A0C515D2FB124D645906F5D3DA5CB97CEBEA975959AE4F95302A04E1D709C3C4AE9B7

UPLOADED: 24 FEB, 2024 21:27 UTC

UPDATED: 24 FEB, 2024 21:27 UTC

Until the files will be available left

5D 08h 31m 12s



<https://fultoncountyga.gov/news/2024/02/22/fulton-county-cyber-incident-response-update-february-22>

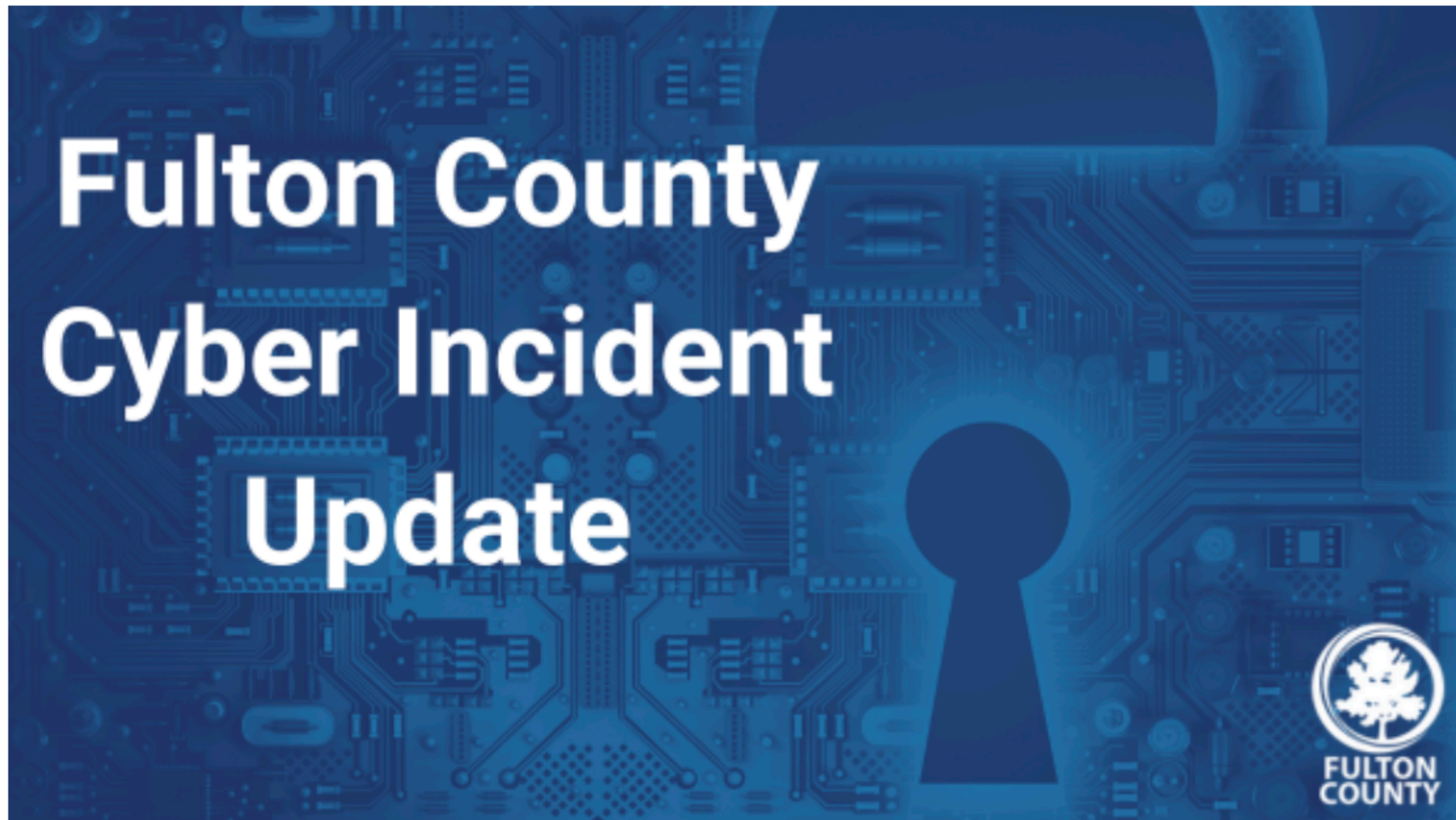
SYSTEM OUTAGE

Fulton County is experiencing an unexpected IT outage currently affecting multiple systems. To read the latest update on the outage, **CLICK HERE**. For additional contact information, please **CLICK HERE**.



<https://fultoncountyga.gov/cyberresponse>

Fulton Home > News > **Fulton County Cyber Incident Response Update for February 22, 2024**



FULTON COUNTY CYBER INCIDENT RESPONSE UPDATE FOR FEBRUARY 22, 2024

February 22, 2024

SHARE THIS STORY

Fulton County continues to make substantial progress in restoring its systems following the recent ransomware incident resulting in service outages. Since the start of this incident, our team has been working

- Individuals involved in ongoing criminal trials, including jurors, witnesses, and defendants, due to potential exposure of confidential information.
- Victims of crimes, such as the child abuse case mentioned, whose sensitive records could be made public.
- Fulton County government employees and officials, whose personal data may be compromised.
- The integrity of the criminal justice system in Fulton County, as the release of sealed documents could undermine legal proceedings.
- The security of the county's IT infrastructure, which could be further compromised by the exposure of sensitive data.
- The privacy of Fulton County residents, if their personal data is included in the leaked documents.
- The reputation and operational stability of Fulton County, which could face public distrust and administrative challenges.
- The safety of confidential informants, whose identities might be revealed, putting their lives at risk.
- Any businesses or individuals mentioned in the leaked data, who may face reputational damage, legal consequences, or financial loss.

S T O R M ⚡ W A T C H

CYBERSECURITY NEWS

TRUSTWORTHY COMPUTING



Community Alert: Ongoing Malicious Campaign Impacting Azure Cloud Environments

SHARE WITH YOUR NETWORK!

FEBRUARY 12, 2024 | THE PROOFPOINT CLOUD SECURITY RESPONSE TEAM



Over the past weeks, Proofpoint researchers have been monitoring an ongoing cloud account takeover campaign impacting dozens of Microsoft Azure environments and compromising hundreds of user accounts, including senior executives. This post serves as a community warning regarding the attack and offers suggestions that affected organizations can implement to protect themselves from it.

What are we seeing?

In late November 2023, Proofpoint researchers detected a new malicious campaign, integrating credential phishing and cloud account takeover (ATO) techniques. As part of this campaign, which is still active, threat actors target users with individualized phishing lures within shared documents. For example, some weaponized documents include embedded links to “View document” which, in turn, redirect users to a malicious phishing webpage upon clicking the URL.

Threat actors seemingly direct their focus toward a wide range of individuals holding diverse titles across different organizations, impacting hundreds of users globally. The affected user base encompasses a wide spectrum of positions, with frequent targets including Sales Directors, Account Managers, and Finance Managers. Individuals holding executive positions such as “Vice President, Operations”, "Chief Financial Officer & Treasurer" and "President & CEO" were also among those targeted. The varied selection of targeted roles indicates a practical strategy by threat actors, aiming to compromise accounts with various levels of access to valuable

- Proofpoint researchers have identified an ongoing cloud account takeover campaign targeting Microsoft Azure environments and compromising hundreds of user accounts, including those of senior executives.
- The campaign, active since late November 2023, uses credential phishing and cloud account takeover techniques, with phishing lures in shared documents.
- Targets include a diverse range of roles, such as Sales Directors, Account Managers, Finance Managers, and high-level executives.
- Attackers use a specific Linux user-agent to access Microsoft365 apps and manipulate multi-factor authentication (MFA).
- Post-compromise activities include MFA manipulation, data exfiltration, internal and external phishing, financial fraud, and the creation of mailbox rules to hide malicious activities.
- The attackers' operational infrastructure includes proxies, data hosting services, and hijacked domains, with some non-proxy sources pointing to Russian and Nigerian ISPs.
- Proofpoint has not attributed the campaign to any known threat actor but suggests possible Russian and Nigerian involvement.
- Indicators of compromise (IOCs) include specific user-agent strings and several domains and ISPs used as malicious infrastructure.
- Recommendations for organizations include monitoring for specific IOCs, enforcing credential changes, identifying account takeovers, detecting initial threat vectors, and employing auto-remediation policies.

RON WYDEN
OREGON

CHAIRMAN OF COMMITTEE ON
FINANCE

221 DIRKSEN SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-5244

United States Senate
WASHINGTON, DC 20510-3703

COMMITTEES:
COMMITTEE ON FINANCE
COMMITTEE ON THE BUDGET
COMMITTEE ON ENERGY AND NATURAL RESOURCES
SELECT COMMITTEE ON INTELLIGENCE
JOINT COMMITTEE ON TAXATION

July 27, 2023

The Honorable Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency
245 Murray Lane SW
Washington, D.C. 20528-0075

The Honorable Merrick B. Garland
Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530-0001

The Honorable Lina Khan
Chair
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Dear Director Easterly, Attorney General Garland and Chair Khan:

I write to request that your agencies take action to hold Microsoft responsible for its negligent cybersecurity practices, which enabled a successful Chinese espionage campaign against the United States government.

On July 12, the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation published a joint advisory about a hacking campaign targeting organizations, including government agencies, that were Microsoft customers. According to press reports, “at least hundreds of thousands of individual U.S. government emails” were stolen, and the email accounts compromised include the Secretary of Commerce, the U.S. Ambassador to China, and the Assistant Secretary of State for East Asia. Rob Joyce, the director of cybersecurity at the National Security Agency, has publicly described this hacking campaign as “China doing espionage.”

Microsoft revealed in a July 14 blog post that the hack occurred because hackers had stolen an encryption key that Microsoft had generated for its identity service, Microsoft Account (MSA). MSA validates that a user is who they claim to be – for example, by verifying the password for a @hotmail.com account – and issues “authentication tokens” that confirm that a user has been validated. Consumer-facing Microsoft products, such as Outlook, verify that a token is valid by checking that a token is digitally signed using an MSA encryption key.

911 NE 11TH AVENUE
SUITE 630
PORTLAND, OR 97232
(503) 326-7525

405 EAST 8TH AVE
SUITE 2020
EUGENE, OR 97401
(541) 431-0229

SAC ANNEX BUILDING
105 FIR ST
SUITE 201
LA GRANDE, OR 97850
(541) 962-7691

U.S. COURTHOUSE
310 WEST 6TH ST
ROOM 118
MEDFORD, OR 97501
(541) 858-5122

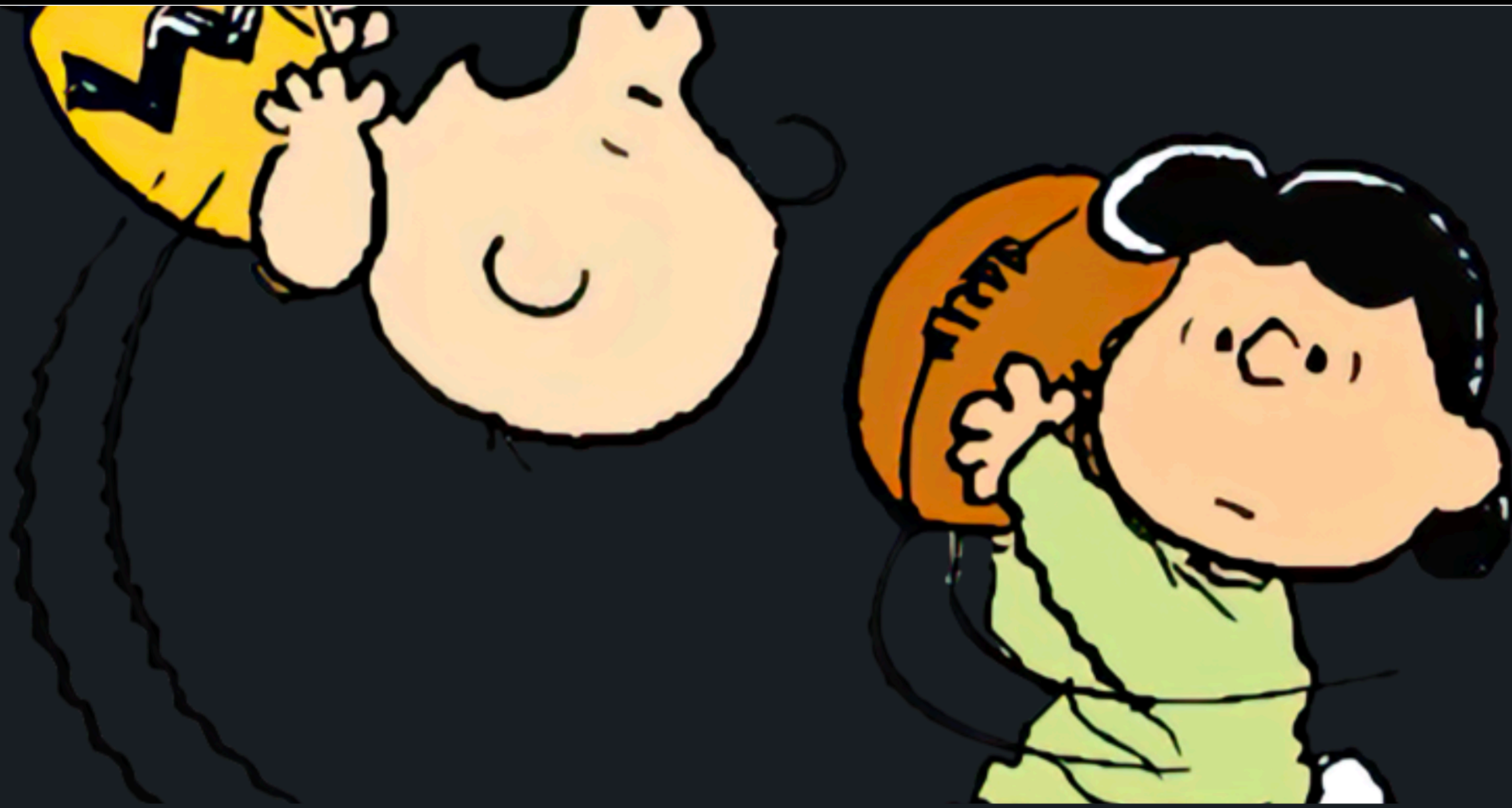
THE JAMISON BUILDING
131 NW HAWTHORNE AVE
SUITE 107
BEND, OR 97701
(541) 330-9142

707 13TH ST, SE
SUITE 285
SALEM, OR 97301
(503) 589-4555

[HTTPS://WYDEN.SENATE.GOV](https://wyden.senate.gov)
PRINTED ON RECYCLED PAPER

“I write to request that your agencies take action to hold Microsoft responsible for its negligent cybersecurity practices”

https://www.wyden.senate.gov/imo/media/doc/wyden_letter_to_cisa_doj_ftc_re_2023_microsoft_breach.pdf



Microsoft...The Truth Is Even Worse Than You Think



Amit Yoran

Chairman and CEO, Tenable (TENB)

6 articles

+ Follow

"Microsoft products have accounted for an aggregate 42.5% of all zero days discovered since 2014."

"Microsoft's lack of transparency applies to breaches, irresponsible security practices and to vulnerabilities, all of which expose their customers to risks they are deliberately kept in the dark about."

"What you hear from Microsoft is 'just trust us,' but what you get back is very little transparency and a culture of toxic obfuscation."

Microsoft expands free logging capabilities after May breach

By [Sergiu Gatlan](#)

February 21, 2024 05:31 PM 4



Microsoft has expanded free logging capabilities for all Purview Audit standard customers, including U.S. federal agencies, six months after disclosing that Chinese hackers stole U.S. government emails undetected in an Exchange Online breach between May and June 2023.

The company has been working with CISA, the Office of Management and Budget (OMB), and the Office of the National Cyber Director (ONCD) since it disclosed the incident to ensure that federal agencies now have access to all logging data needed to detect similar attacks in the future.

"Beginning this month, expanded logging will be available to all agencies using Microsoft Purview Audit regardless of license tier," a press release issued today reads.

POPULAR STORIES






White House urges devs to switch to memory-safe programming languages



LockBit ransomware returns, restores servers after police disruption

LATEST DOWNLOADS

	Malwarebytes Anti-Malware Version: 4.6.8.311	5M+ DOWNLOADS
	Windows Repair (All In One) Version: 4.14.1	2M+ DOWNLOADS
	McAfee Consumer	442,016



S T O R M ⚡ W A T C H

CYBERSECURITY NEWS

ABANDON ALL

HOPE



SUBSCRIBE SIGN IN

WSJ PRO

Hospitals and Pharmacies Reeling After Change Healthcare Cyberattack

Healthcare organizations forced to revert to manual procedures after Change Healthcare, part of Optum, disconnects services

By *James Rundle and Catherine Stupp*

Updated Feb. 23, 2024 12:19 pm ET | WSJ PRO

Share icon Font size icon (AA) Headphones icon



CYBER-CRIME 8

Cyberattack downs pharmacies across America

Prescription orders hit after IT supplier Change Healthcare pulls plug on systems

By *Jessica Lyons*

Thu 22 Feb 2024 // 21:13 UTC

UPDATED IT provider Change Healthcare has confirmed it shut down some of its systems following a cyberattack, disrupting prescription orders and other services at pharmacies across the US.

The technology outfit is one of the largest in the country of its kind, and is used by pharmacists to check patients' eligibility for treatments and process orders for medication given their insurance situation, among many other things. Pulling the plug on its backend services has hit pharmacies relying on its tech, including CVS, and forced some folks to pay for their medication at full price in cash.

"Change Healthcare is experiencing a cyber security issue, and our experts are working to address the matter," the biz, which is owned by UnitedHealth and claims to handle 15 billion healthcare transactions annually, said earlier today.

The trouble appears to have started on Wednesday, and at the time Change said it was "experiencing enterprise-wide connectivity issues." That evening it confirmed it was "experiencing a network interruption related to a cyber security issue."

The IT supplier added: "Once we became aware of the outside threat, in the interest of protecting our partners and patients, we took immediate action to disconnect our systems to prevent further impact. At this time, we believe the issue is specific to Change Healthcare and all other systems across UnitedHealth Group are operational."

The healthcare biz said it expects the disruption to last throughout the day and into Friday, if not longer, and promised to provide updates as additional information becomes available.

*“It’s a mess, and I believe
it’s our Colonial Pipeline
moment in healthcare”*

Optum supplies technology
services to
67,000 pharmacies
and care to
129 million individual customers

“I'm trying to get my daughter's antibiotics filled, and was like, ‘no biggie, I'll just pay for it because I don't want to wait to start the medication. How much?’ ... \$745! Still over \$700 with the discount cards. For a 5 day course of antibiotics.”

“Hopefully this gets fixed soon, what a disaster.”

BlackCat/ALPHV

*ScreenConnect auth bypass flaw
(CVE-2024-1709)*

<https://www.reuters.com/technology/cybersecurity/cyber-security-outage-change-healthcare-continues-sixth-straight-day-2024-02-26/>

<https://www.bleepingcomputer.com/news/security/unitedhealth-subsubsidiary-optum-hack-linked-to-blackcat-ransomware/>

iSoon's Secret APT Status Exposes China's Foreign Hacking Machinations

Chinese government agencies are paying an APT, masked as a legitimate company, to spy on foreign and domestic targets of political interest.



Nate Nelson, Contributing Writer

February 22, 2024

🕒 4 Min Read



SOURCE: ROKAS TENYS VIA SHUTTERSTOCK

Editor's Choice



ConnectWise ScreenConnect Mass Exploitation Delivers Ransomware

by Tara Seals, Managing Editor, News, Dark Reading

FEB 23, 2024

4 MIN READ

“The key lesson is: if they can go after a government ministry for \$55,000, what do you think your price is?”

STORM ⚡ WATCH

CYBERSECURITY NEWS

TOOL TIME





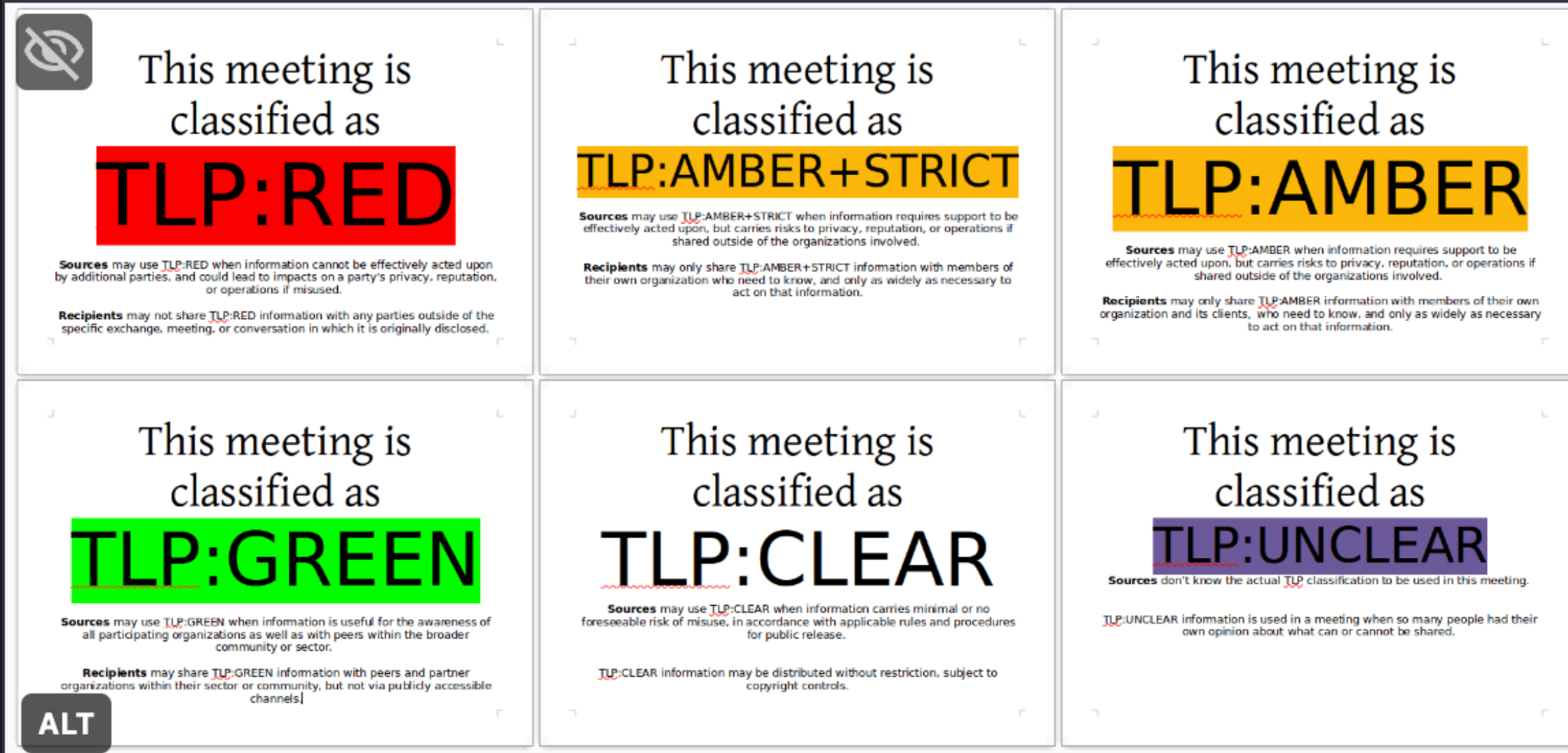
Alexandre Dulaunoy

@adulau@infosec.exchange

Good news for everyone involved in meetings where TLP classifications play a crucial role! I've just updated my repository with the latest, second edition of the TLP Classification Meeting Posters. These are handy tools to explicitly display the TLP classification in use during your meetings.

Grab the PDF and ODT versions here - git.foo.be/adulau/tlp-meeting

Updates are welcome, like better design, translation or alike.



ALT

<https://infosec.exchange/@adulau/111993806919797575>



Copied Current URL

adulau / tlp-meeting

Watch 1 Star 0 Fork 0

Code Issues Pull Requests Packages Projects Releases Wiki

Traffic Light Protocol - meeting classification

4 Commits 2 Branches 0 Tags

master Go to file HTTPS https://git.foo.be/adulau/tlp-me

- Alexandre... 04bbd53d37 2 days ago
- image 2 days ago
- README.md 2 days ago
- TLP-Classification-a4.pdf 2 days ago
- TLP-Classification.odt 2 days ago

README.md

Traffic Light Protocol - Meeting Classification

The Traffic Light Protocol (TLP) is a well-known set of classifications for sensitive information.

The TLP classification is regularly used by the CSIRT community and other organizations around the

<https://git.foo.be/adulau/tlp-meeting>

I was looking for...

SHAMELESS SELF-PROMOTION





[Request a Demo](#)

BLOGS

New Research Demonstrates Censys' Unmatched Internet Intelligence

<https://censys.com/new-research-demonstrates-censys-unmatched-internet-intelligence/>



FEBRUARY 26, 2024

Tags:

- Censys Internet Map
- Censys Search
- Research



BLOGS

Ivanti Connect (in)Secure – Revisited

<https://censys.com/ivanti-connect-insecure-revisited/>



FEBRUARY 21, 2024

ABOUT THE AUTHOR

Executive Summary

- As of Monday, Feb 19, 2024, Censys observes **24,590** exposed Ivanti Connect Secure gateways
- **Over 6,000** (nearly **24.7%** of the total exposed) gateways show indications of running a version vulnerable to one or more of the five recently disclosed vulnerabilities (CVE-2023-46805, CVE-2024-21887, CVE-2024-21888, CVE-2024-21893, and CVE-2024-22024)



STORM ⚡ WATCH

CYBERSECURITY NEWS

TAG ROUND-UP



<https://viz.greynoise.io/trends?view=recent>

- 🏷️ pypider unauthorized access rce attempt
- 🏷️ ConnectWise ScreenConnect Auth Bypass Check (CVE-2024-1708)
- 🏷️ Spring OAuth Template Injection RCE Attempt (CVE-2016-4977)
- 🏷️ WordPress InPost Local File Inclusion Attempt (CVE-2022-4063)
- 🏷️ Nmap phpMyAdmin Local File Inclusion Attempt (CVE-2005-3299)
- 🏷️ WordPress Bricks Builder RCE Attempt (CVE-2024-25600)
- 🏷️ Sugar CRM Crawler
- 🏷️ jeecg-boot SQL Injection Attempt (CVE-2023-1454)
- 🏷️ ConnectWise ScreenConnect Auth Bypass RCE Attempt (CVE-2024-1708)
- 🏷️ MagnusBilling Command Injection RCE Attempt (CVE-2023-30258)
- 🏷️ WordPress WP Visitor Statistics SQL Injection Attempt (CVE-2023-0600)
- 🏷️ Common Gateway Interface /cgi-bin/ crawler

GreyNoise Trends

COMMON GATEWAY INTERFACE /CGI-BIN/ CRAWLER

<https://viz.greynoise.io/tags/cgi-bin-crawler?days=1>

INTENTION

CATEGORY

UNKNOWN

Activity

No associated CVEs

IP addresses with this tag have been observed crawling for /cgi-bin/ URIs

• 24 HOURS

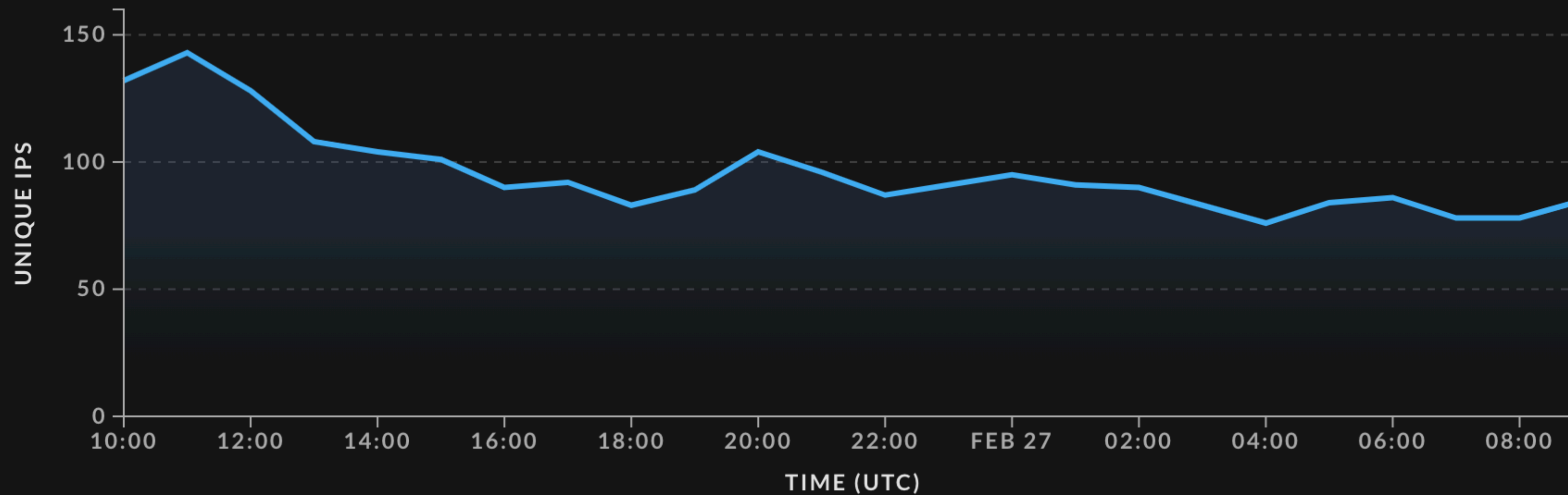
10 DAYS

30 DAYS

February 26, 2024 10:00 UTC - February 27, 2024 09:00 UTC

Unique IPs Observed

Last 24 hours



Timeline

Sequence of recorded events

> + GreyNoise Created Tag

2024-02-23 00:00 UTC

INTENTION: UNKNOWN
CATEGORY: Activity

CVE-2024-1708

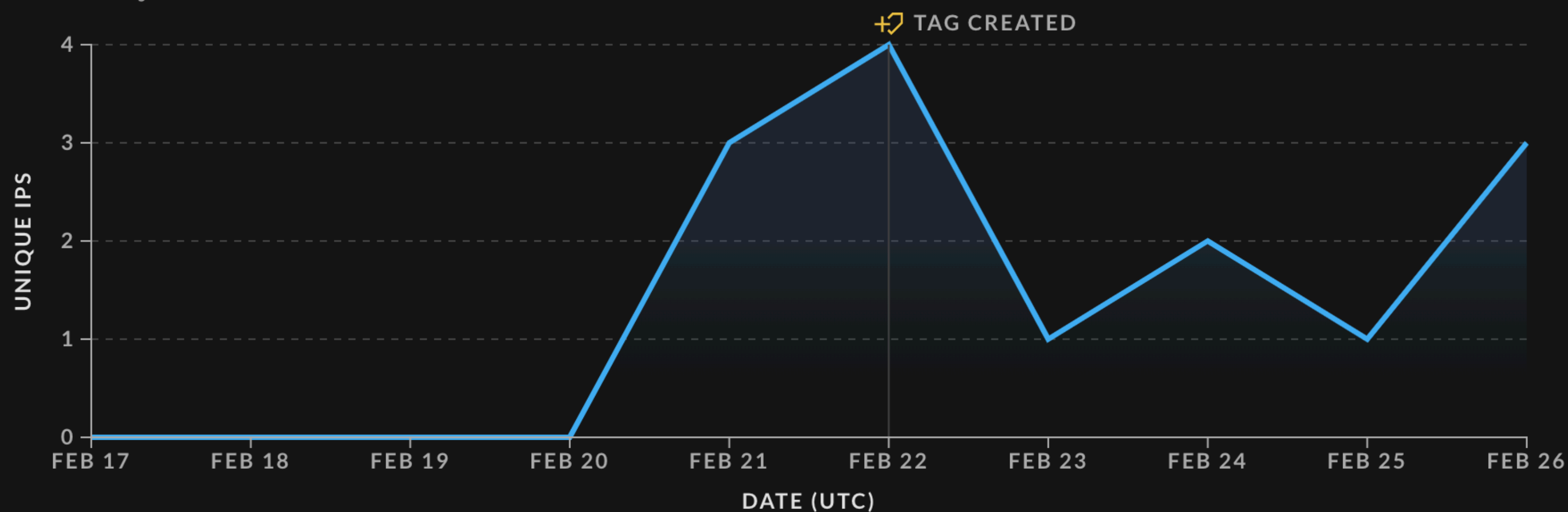
IP addresses with this tag have been observed attempting to access the endpoint associated with CVE-2024-1708 - an authentication bypass vulnerability in ConnectWise ScreenConnect versions prior to version 23.9.8.

24 HOURS • 10 DAYS 30 DAYS

February 17, 2024 - February 26, 2024 (UTC)

Unique IPs Observed

Last 10 days



Timeline

Sequence of recorded events

- > GreyNoise Created Tag 2024-02-22 00:00 UTC
- > CVE-2024-1708 Published 2024-02-21 16:15 UTC

**WE NEED
TO TALK
ABOUT
KEY**



It Has Been 5 Days Since The Last KEV Release

<https://observablehq.com/@greynoise/greynoise-tags>

CVE-2024-1709: ConnectWise ScreenConnect Authentication Bypass

<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>