STORMWATCH

CYBERSECURITY NEWS

Dateline: 2024-04-16

LIKE

SUBSCRIBE

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

Erick Galinkin

AI Security Researcher

NVIDIA

STORM WATCH

CYBERSECURITY NEWS

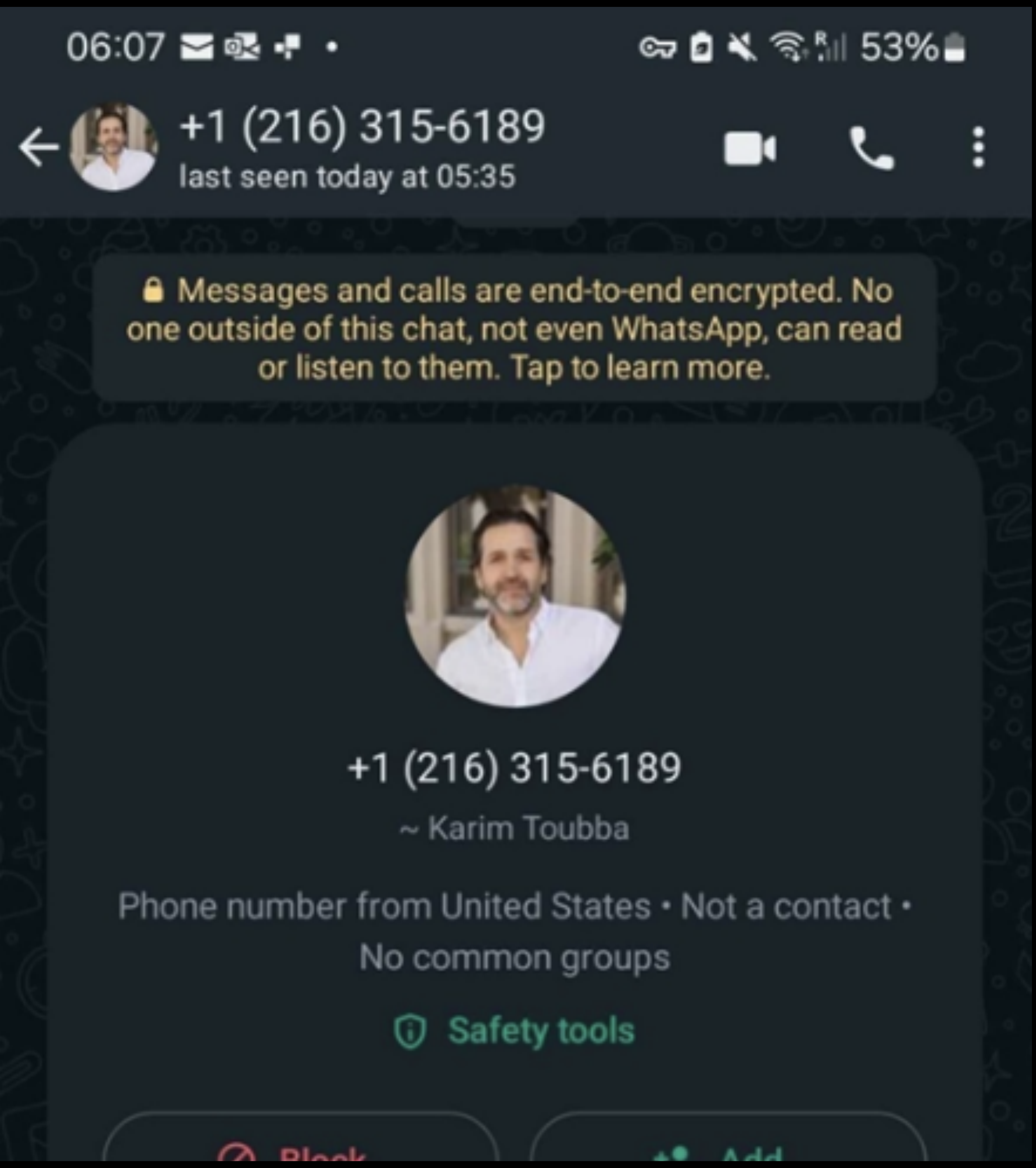
CYBERSIDE CHAT

LASTPASS LABS

Attempted Audio Deepfake Call Targets LastPass Employee

Mike Kosak • April 10, 2024

https://blog.lastpass.com/posts/2024/04/attempted-audio-deepfake-call-targets-lastpass-employee



+1 (216) 315-6189

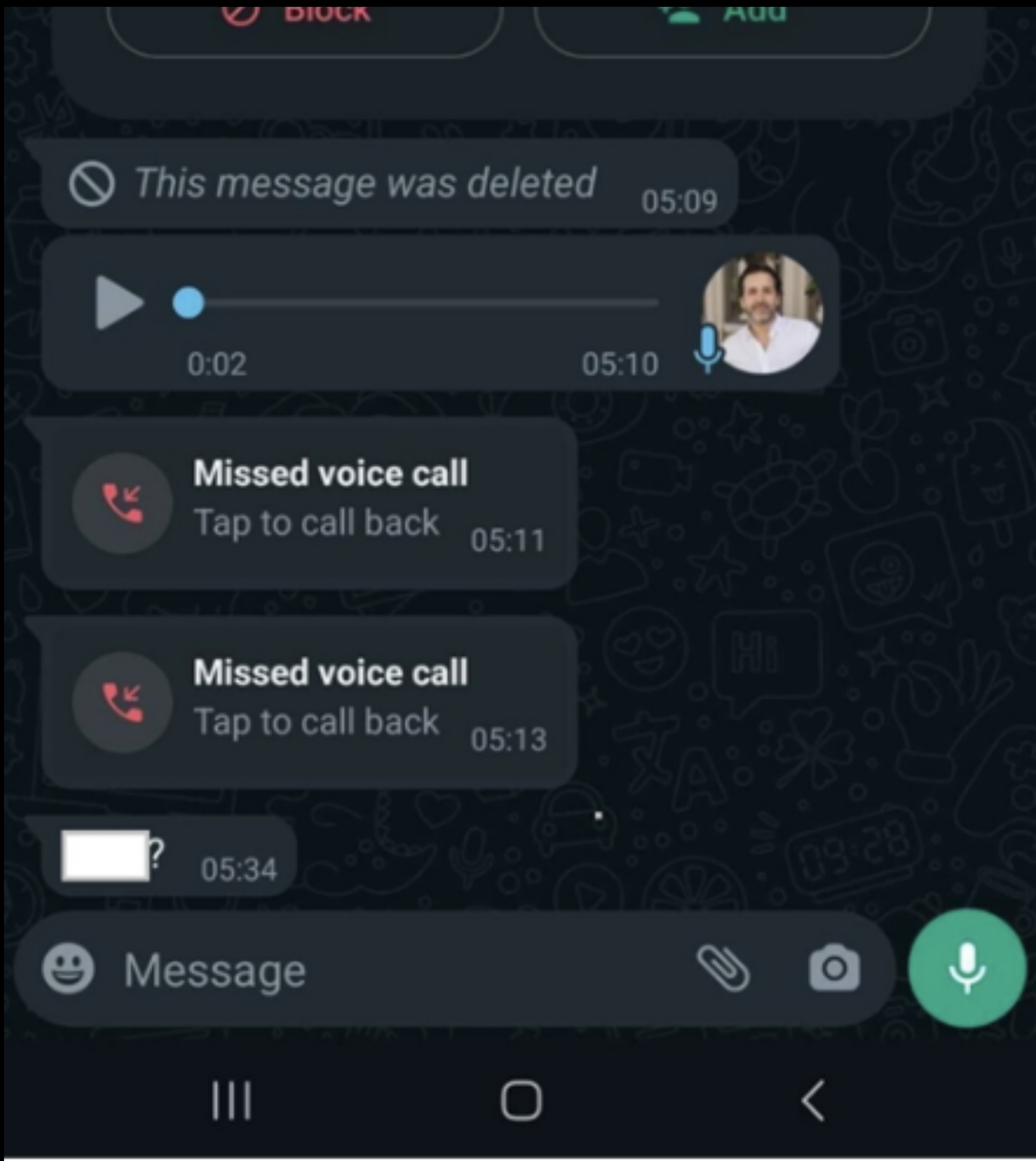
last seen today at 05:35

Messages and calls are end-to-end encrypted. No one outside of this chat, not even WhatsApp, can read or listen to them. Tap to learn more.

+1 (216) 315-6189

~ Karim Toubba

Phone number from United States • Not a contact • No common groups



This message was deleted 05:09

0:02 05:10

Missed voice call
Tap to call back 05:11

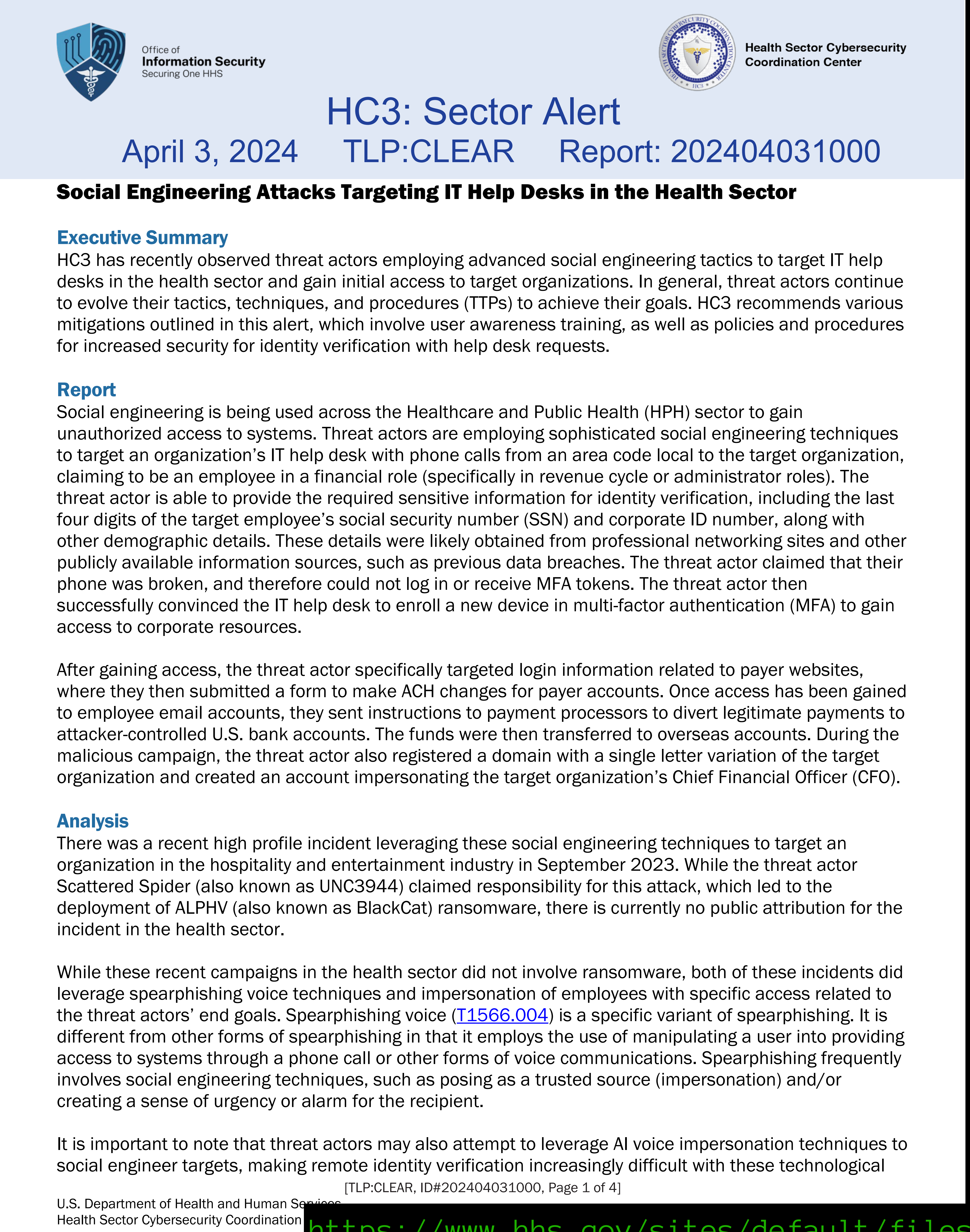
Missed voice call
Tap to call back 05:13

[redacted]? 05:34

Deepfake technology, which uses AI to create fabricated audio/visual recordings, has become more accessible and is being used for fraud and disinformation campaigns. This includes cases of deepfake audio being used to impersonate company executives and trick employees into transferring funds.

LastPass recently experienced an attempted deepfake attack, where an employee received calls, texts, and a voicemail from a threat actor impersonating the LastPass CEO using deepfake audio. The employee recognized the signs of a social engineering attempt and reported it to the security team.

While there was no impact to LastPass, the company is sharing this incident to raise awareness that deepfake attacks are becoming more common, even targeting private companies, and organizations should verify suspicious contacts through established internal channels.[1]



Office of
Information Security
Securing One HHS

Health Sector Cybersecurity
Coordination Center

HC3: Sector Alert

April 3, 2024 TLP:CLEAR Report: 202404031000

Social Engineering Attacks Targeting IT Help Desks in the Health Sector

Executive Summary

HC3 has recently observed threat actors employing advanced social engineering tactics to target IT help desks in the health sector and gain initial access to target organizations. In general, threat actors continue to evolve their tactics, techniques, and procedures (TTPs) to achieve their goals. HC3 recommends various mitigations outlined in this alert, which involve user awareness training, as well as policies and procedures for increased security for identity verification with help desk requests.

Report

Social engineering is being used across the Healthcare and Public Health (HPH) sector to gain unauthorized access to systems. Threat actors are employing sophisticated social engineering techniques to target an organization's IT help desk with phone calls from an area code local to the target organization, claiming to be an employee in a financial role (specifically in revenue cycle or administrator roles). The threat actor is able to provide the required sensitive information for identity verification, including the last four digits of the target employee's social security number (SSN) and corporate ID number, along with other demographic details. These details were likely obtained from professional networking sites and other publicly available information sources, such as previous data breaches. The threat actor claimed that their phone was broken, and therefore could not log in or receive MFA tokens. The threat actor then successfully convinced the IT help desk to enroll a new device in multi-factor authentication (MFA) to gain access to corporate resources.

After gaining access, the threat actor specifically targeted login information related to payer websites, where they then submitted a form to make ACH changes for payer accounts. Once access has been gained to employee email accounts, they sent instructions to payment processors to divert legitimate payments to attacker-controlled U.S. bank accounts. The funds were then transferred to overseas accounts. During the malicious campaign, the threat actor also registered a domain with a single letter variation of the target organization and created an account impersonating the target organization's Chief Financial Officer (CFO).

Analysis

There was a recent high profile incident leveraging these social engineering techniques to target an organization in the hospitality and entertainment industry in September 2023. While the threat actor Scattered Spider (also known as UNC3944) claimed responsibility for this attack, which led to the deployment of ALPHV (also known as BlackCat) ransomware, there is currently no public attribution for the incident in the health sector.

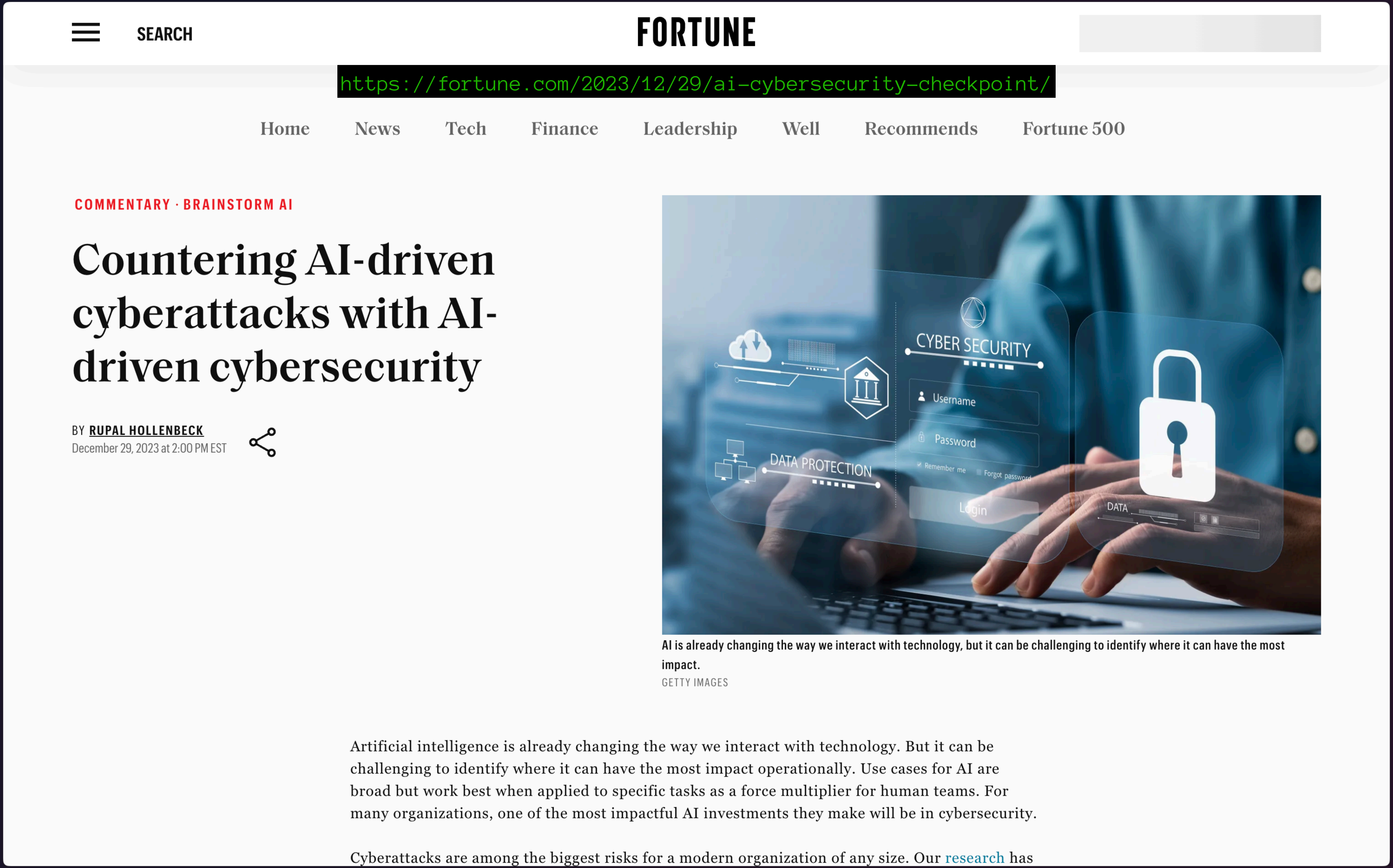
While these recent campaigns in the health sector did not involve ransomware, both of these incidents did leverage spearphishing voice techniques and impersonation of employees with specific access related to the threat actors' end goals. Spearphishing voice (T1566.004) is a specific variant of spearphishing. It is different from other forms of spearphishing in that it employs the use of manipulating a user into providing access to systems through a phone call or other forms of voice communications. Spearphishing frequently involves social engineering techniques, such as posing as a trusted source (impersonation) and/or creating a sense of urgency or alarm for the recipient.

It is important to note that threat actors may also attempt to leverage AI voice impersonation techniques to social engineer targets, making remote identity verification increasingly difficult with these technological

While these recent campaigns in the health sector did not involve ransomware, both of these incidents did leverage spearphishing voice techniques and impersonation of employees with specific access related to the threat actors' end goals. Spearphishing voice (T1566.004) is a specific variant of spearphishing. It is different from other forms of spearphishing in that it employs the use of manipulating a user into providing access to systems through a phone call or other forms of voice communications. Spearphishing frequently involves social engineering techniques, such as posing as a trusted source (impersonation) and/or creating a sense of urgency or alarm for the recipient.

It is important to note that threat actors may also attempt to leverage AI voice impersonation techniques to social engineer targets, making remote identity verification increasingly difficult with these technological advancements. A recent global study found that out of 7,000 people surveyed, one in four said that they had experienced an AI voice cloning scam or knew someone who had.

https://www.hhs.gov/sites/default/files/help-desk-social-engineering-sector-alert-tlpclear.pdf



SEARCH

FORTUNE

https://fortune.com/2023/12/29/ai-cybersecurity-checkpoint/

COMMENTARY · BRAINSTORM AI

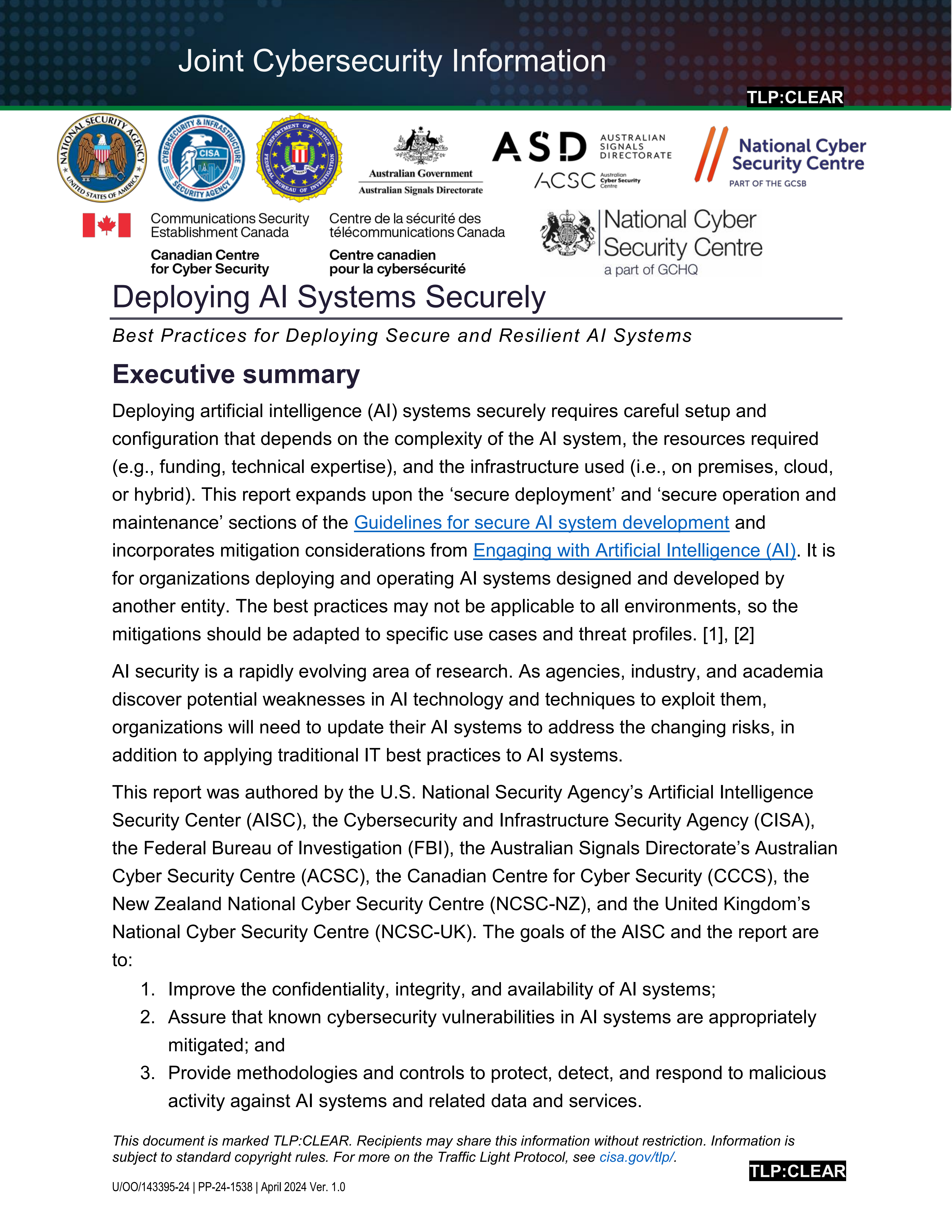
Countering AI-driven cyberattacks with AI-driven cybersecurity

BY RUPAL HOLLENBECK
December 29, 2023 at 2:00 PM EST

AI is already changing the way we interact with technology, but it can be challenging to identify where it can have the most impact.
GETTY IMAGES

Artificial intelligence is already changing the way we interact with technology. But it can be challenging to identify where it can have the most impact operationally. Use cases for AI are broad but work best when applied to specific tasks as a force multiplier for human teams. For many organizations, one of the most impactful AI investments they make will be in cybersecurity.

Cyberattacks are among the biggest risks for a modern organization of any size. Our research has



Joint Cybersecurity Information

TLP:CLEAR

Australian Government
Australian Signals Directorate

ASD Australian Signals Directorate
ACSC Australian Cyber Security Centre

National Cyber Security Centre
PART OF THE GCSB

Communications Security Establishment Canada
Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications Canada
Centre canadien pour la cybersécurité

National Cyber Security Centre
a part of GCHQ

Deploying AI Systems Securely

Best Practices for Deploying Secure and Resilient AI Systems

Executive summary

Deploying artificial intelligence (AI) systems securely requires careful setup and configuration that depends on the complexity of the AI system, the resources required (e.g., funding, technical expertise), and the infrastructure used (i.e., on premises, cloud, or hybrid). This report expands upon the 'secure deployment' and 'secure operation and maintenance' sections of the Guidelines for secure AI system development and incorporates mitigation considerations from Engaging with Artificial Intelligence (AI). It is for organizations deploying and operating AI systems designed and developed by another entity. The best practices may not be applicable to all environments, so the mitigations should be adapted to specific use cases and threat profiles. [1], [2]

AI security is a rapidly evolving area of research. As agencies, industry, and academia discover potential weaknesses in AI technology and techniques to exploit them, organizations will need to update their AI systems to address the changing risks, in addition to applying traditional IT best practices to AI systems.

This report was authored by the U.S. National Security Agency's Artificial Intelligence Security Center (AISC), the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), the Australian Signals Directorate's Australian Cyber Security Centre (ACSC), the Canadian Centre for Cyber Security (CCCS), the New Zealand National Cyber Security Centre (NCSC-NZ), and the United Kingdom's National Cyber Security Centre (NCSC-UK). The goals of the AISC and the report are to:

1. Improve the confidentiality, integrity, and availability of AI systems;
2. Assure that known cybersecurity vulnerabilities in AI systems are appropriately mitigated; and
3. Provide methodologies and controls to protect, detect, and respond to malicious activity against AI systems and related data and services.

This document is marked TLP:CLEAR. Recipients may share this information without restriction. Information is subject to standard copyright rules. For more on the Traffic Light Protocol, see cisa.gov/tlp/.

TLP:CLEAR

U/OO/143395-24 | PP-24-1538 | April 2024 Ver. 1.0

https://media.defense.gov/2024/Apr/15/2003439257/-1/-1/0/CSI-DEPLOYING-AI-SYSTEMS-SECURELY.PDF

Secure the deployment environment

- Establish robust governance over the AI system deployment, including understanding risks, defining roles/responsibilities, and collaborating across teams.
- Ensure a secure and well-designed architecture for the deployment environment, applying zero trust principles and protecting data sources.
- Harden configurations by applying security best practices like encryption, authentication, and vulnerability management.
- Protect the deployment networks using detection and response capabilities.

Continuously protect the AI system

- Validate the AI system before and during use through testing, integrity checks, and supply chain security.
- Secure exposed APIs and actively monitor model behavior for anomalies.
- Implement strong protections for the AI model weights and parameters.

Securely operate and maintain the AI system

- Enforce strict access controls and user awareness/training.
- Conduct regular audits, penetration testing, and monitoring.
- Maintain a rigorous patch and update management process.

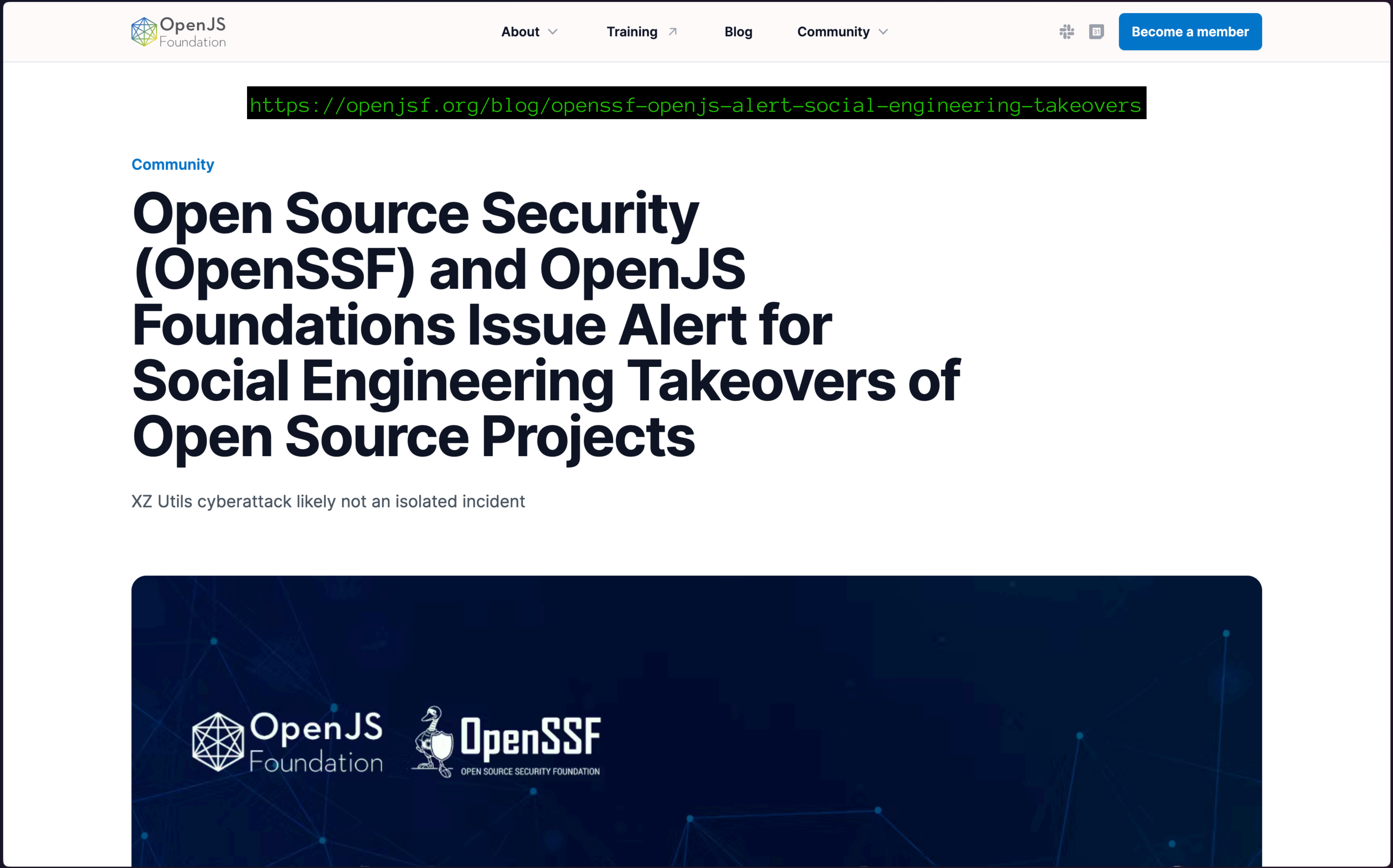
Threat actors are experts at finding malicious applications for technology advances, and ChatGPT is no exception. They discovered that despite its safeguards, they could easily use the tool to write malicious emails for phishing campaigns. Prior to this, many phishing emails contained obvious red flags: poor grammar, abnormal word choice, typos, and other deviations that raised questions. This fortunate last line of defense has disappeared as threat actors use generative AI to draft phishing lures that are formally perfect and often personalized. These engines typically feature a natural speech-to-code function, which can be used to build malicious files to deploy.

Generative AI lowers the barrier to entry across the entire attack life cycle. The generative AI boom may be having an impact already: Our research shows that email-delivered attacks have spiked in 2023, representing 86% of all file-based attacks we recorded. Other types of AI also amplify threat actors' capacity by automating attacks, finding vulnerabilities, managing botnets, and more. They use artificial intelligence as a force multiplier.

STORMWATCH

CYBERSECURITY NEWS

CYBER SPOTLIGHT

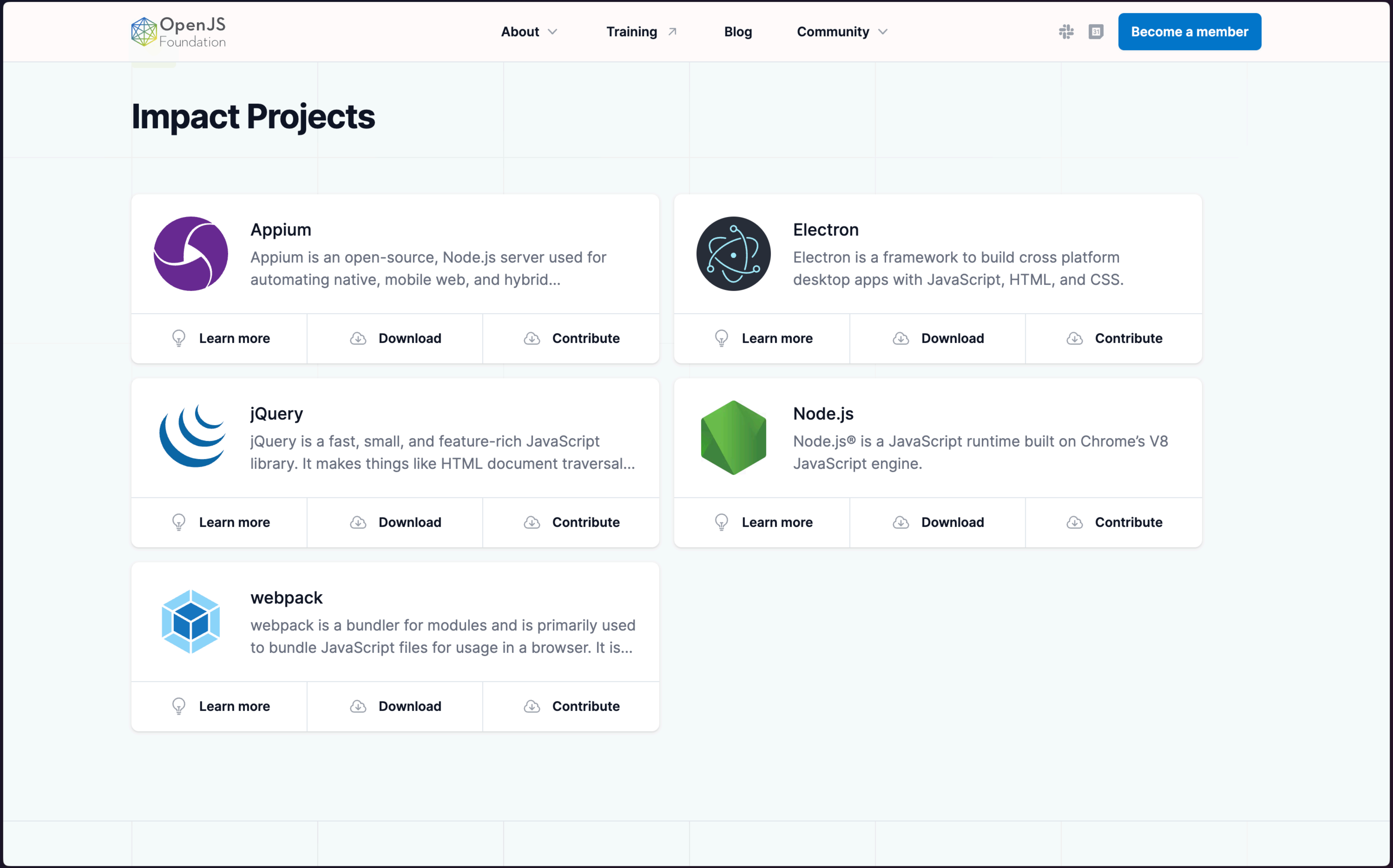


https://openjsf.org/blog/openssf-openjs-alert-social-engineering-takeovers

Community

Open Source Security (OpenSSF) and OpenJS Foundations Issue Alert for Social Engineering Takeovers of Open Source Projects

XZ Utils cyberattack likely not an isolated incident



Impact Projects

Appium

Appium is an open-source, Node.js server used for automating native, mobile web, and hybrid...

Learn more | Download | Contribute

Electron

Electron is a framework to build cross platform desktop apps with JavaScript, HTML, and CSS.

Learn more | Download | Contribute

jQuery

jQuery is a fast, small, and feature-rich JavaScript library. It makes things like HTML document traversal...

Learn more | Download | Contribute

Node.js

Node.js® is a JavaScript runtime built on Chrome's V8 JavaScript engine.

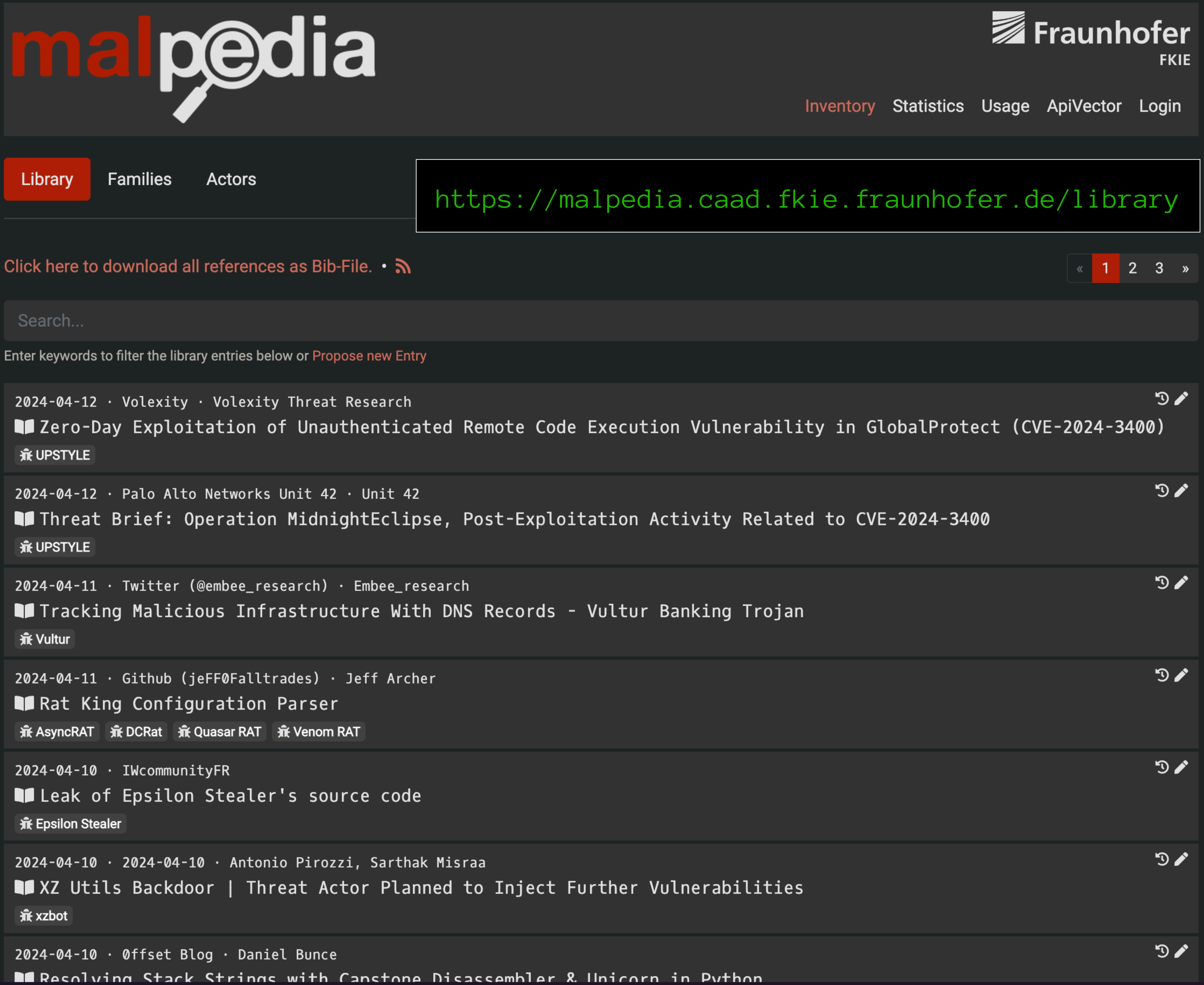
Learn more | Download | Contribute

webpack

webpack is a bundler for modules and is primarily used to bundle JavaScript files for usage in a browser. It is...

Learn more | Download | Contribute

TOOL TIME



https://malpedia.caad.fkie.fraunhofer.de/library

Click here to download all references as Bib-File. •

Enter keywords to filter the library entries below or Propose new Entry

2024-04-12 · Volexity · Volexity Threat Research
Zero-Day Exploitation of Unauthenticated Remote Code Execution Vulnerability in GlobalProtect (CVE-2024-3400)
UPSTYLE

2024-04-12 · Palo Alto Networks Unit 42 · Unit 42
Threat Brief: Operation MidnightEclipse, Post-Exploitation Activity Related to CVE-2024-3400
UPSTYLE

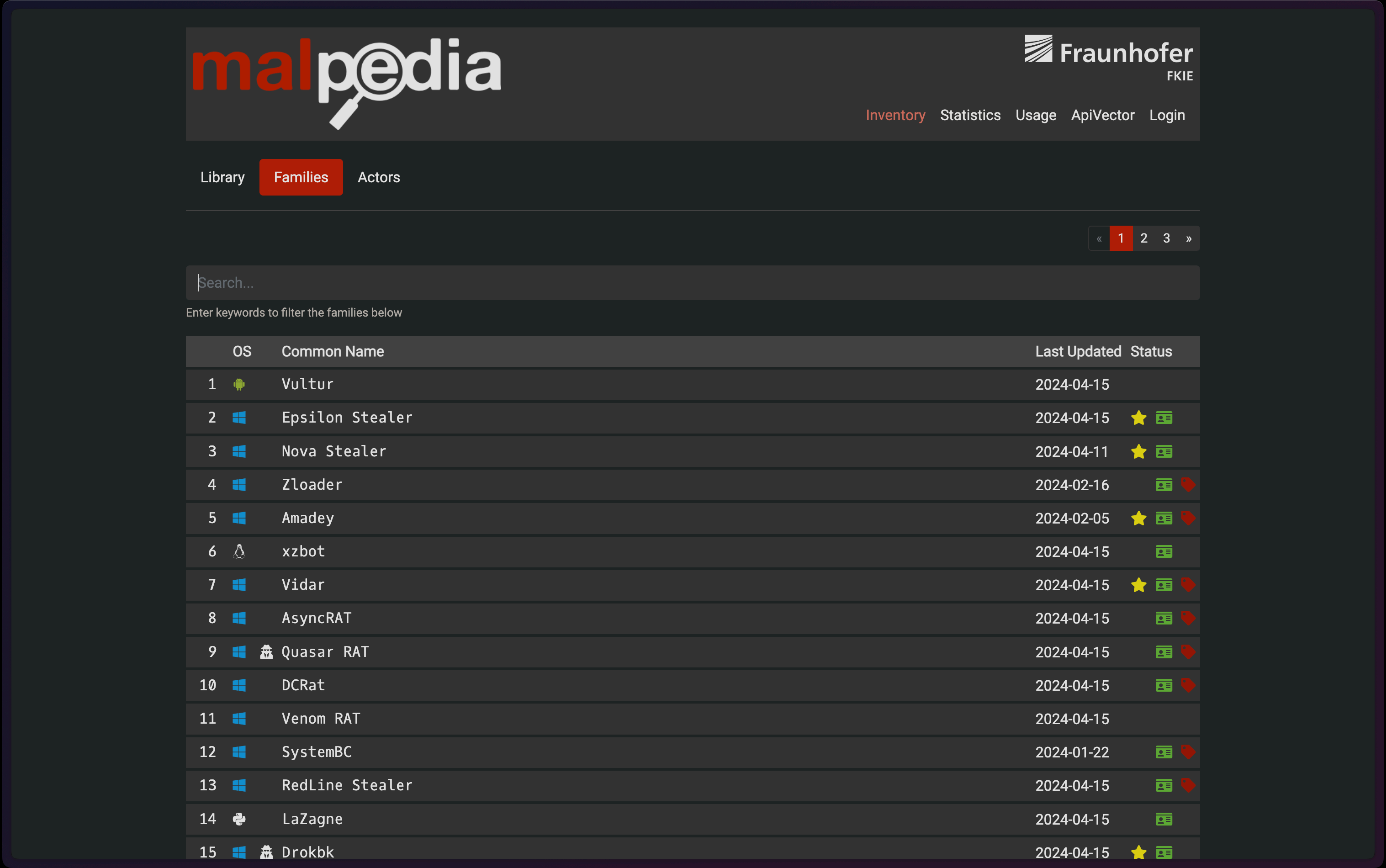
2024-04-11 · Twitter (@embee_research) · Embee_research
Tracking Malicious Infrastructure With DNS Records - Vultur Banking Trojan
Vultur

2024-04-11 · Github (jeFF0Falltrades) · Jeff Archer
Rat King Configuration Parser
AsyncRAT DCRat Quasar RAT Venom RAT

2024-04-10 · IWcommunityFR
Leak of Epsilon Stealer's source code
Epsilon Stealer

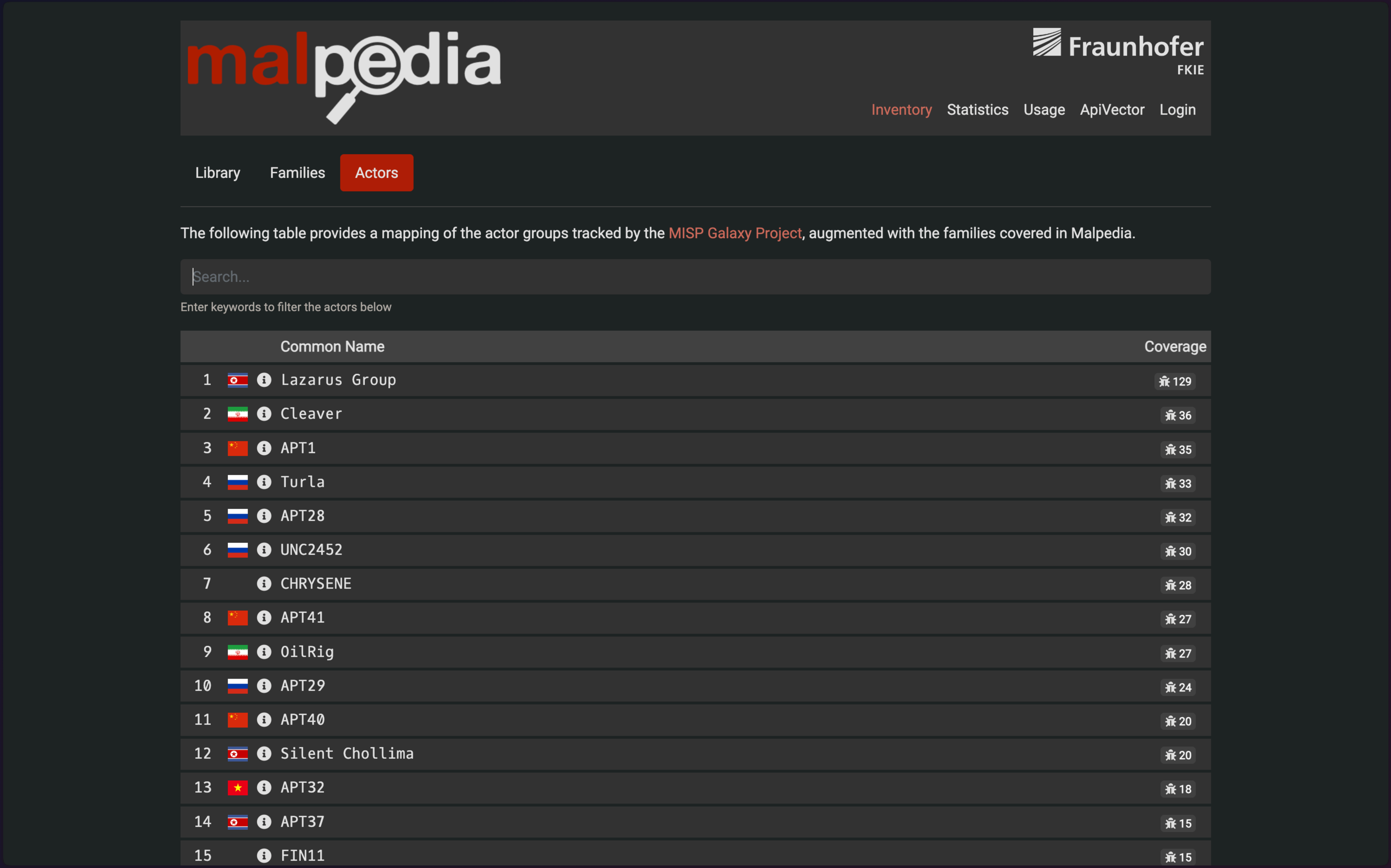
2024-04-10 · 2024-04-10 · Antonio Pirozzi, Sarthak Misraa
XZ Utils Backdoor | Threat Actor Planned to Inject Further Vulnerabilities
xzbot

2024-04-10 · 0ffset Blog · Daniel Bunce
Resolving Stack Strings with Capstone Disassembler & Unicorn in Python



Enter keywords to filter the families below

	OS		Common Name	Last Updated	Status
1	🤖		Vultur	2024-04-15	
2	⊞		Epsilon Stealer	2024-04-15	★ 🪪
3	⊞		Nova Stealer	2024-04-11	★ 🪪
4	⊞		Zloader	2024-02-16	🪪 🏷
5	⊞		Amadey	2024-02-05	★ 🪪 🏷
6	🐧		xzbot	2024-04-15	🪪
7	⊞		Vidar	2024-04-15	★ 🪪 🏷
8	⊞		AsyncRAT	2024-04-15	🪪 🏷
9	⊞	🕵	Quasar RAT	2024-04-15	🪪 🏷
10	⊞		DCRat	2024-04-15	🪪 🏷
11	⊞		Venom RAT	2024-04-15	
12	⊞		SystemBC	2024-01-22	🪪 🏷
13	⊞		RedLine Stealer	2024-04-15	🪪 🏷
14	🐍		LaZagne	2024-04-15	🪪
15	⊞	🕵	Drokbk	2024-04-15	★ 🪪



malpedia

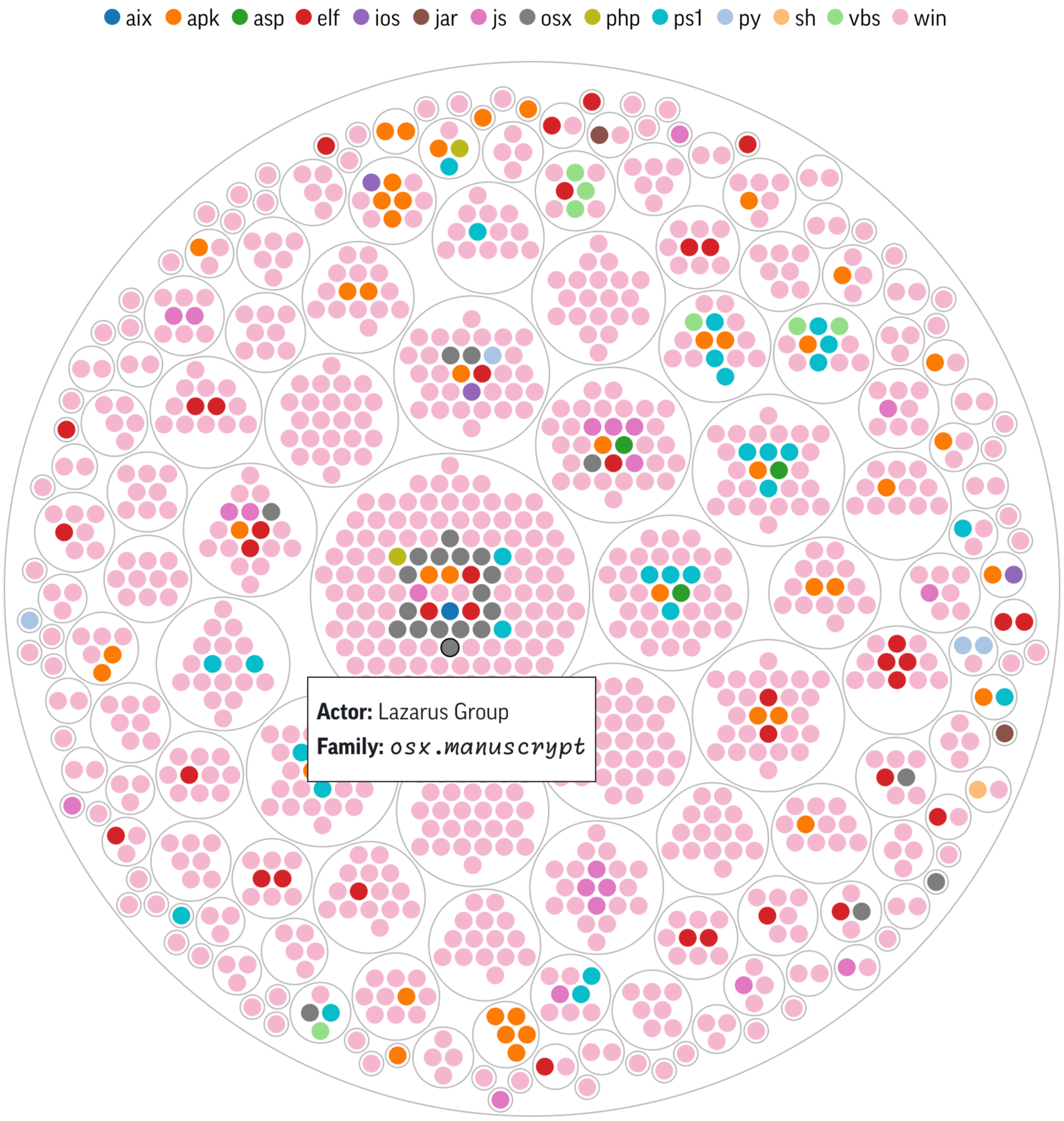
Fraunhofer
FKIE

The following table provides a mapping of the actor groups tracked by the MISP Galaxy Project, augmented with the families covered in Malpedia.

Enter keywords to filter the actors below

			Common Name	Coverage
1	🇰🇵	ℹ	Lazarus Group	129
2	🇮🇷	ℹ	Cleaver	36
3	🇨🇳	ℹ	APT1	35
4	🇷🇺	ℹ	Turla	33
5	🇷🇺	ℹ	APT28	32
6	🇷🇺	ℹ	UNC2452	30
7		ℹ	CHRYSENE	28
8	🇨🇳	ℹ	APT41	27
9	🇮🇷	ℹ	OilRig	27
10	🇷🇺	ℹ	APT29	24
11	🇨🇳	ℹ	APT40	20
12	🇰🇵	ℹ	Silent Chollima	20
13	🇻🇳	ℹ	APT32	18
14	🇰🇵	ℹ	APT37	15
15		ℹ	FIN11	15

https://observablehq.com/
@hrbrmstr/2024-30-day-map-
challenge-day-12-
relationships-family



SHAMELESS SELF-PROMOTION

censys

Join Censys for a Thrunting Workshop & Happy Hour!

```
https://go.censys.com/threat-hunting-workshop-philadelphia-2024.html
```

April 17, 2024 | City Winery | Philadelphia

Lunch | 12 - 1:30 p.m.
Thrunting Workshop | 1:30 - 4:30 p.m. (see below for 'who should attend')
Happy Hour to follow | 4:30 p.m. (everyone welcome!)

BLOGS

CVE-2024-3272 & CVE-2024-3273: D-Link NAS

https://censys.com/cve-2024-3272-and-2024-3273/

censys
Products
Solutions
Federal
Resources
Company
Search Now
Request a Demo

BLOGS

Sisense: A Look at Industry and Geography

https://censys.com/sisense-a-look-at-industry-and-geography/

https://www.greynoise.io/blog/netnoisecon-amplifying-the-future-of-infosec

COMPANY

NetNoiseCon: Amplifying the Future of InfoSec

Sam Houston | April 2, 2024

VULNERABILITIES LABS

CVE-2024-3400: Command Injection Vulnerability in Palo Alto Networks PAN-OS

The GreyNoise Labs Team | April 15, 2024

ZERO
DAY
Palo Alto Networks PAN-OS
CVE-2024-3400

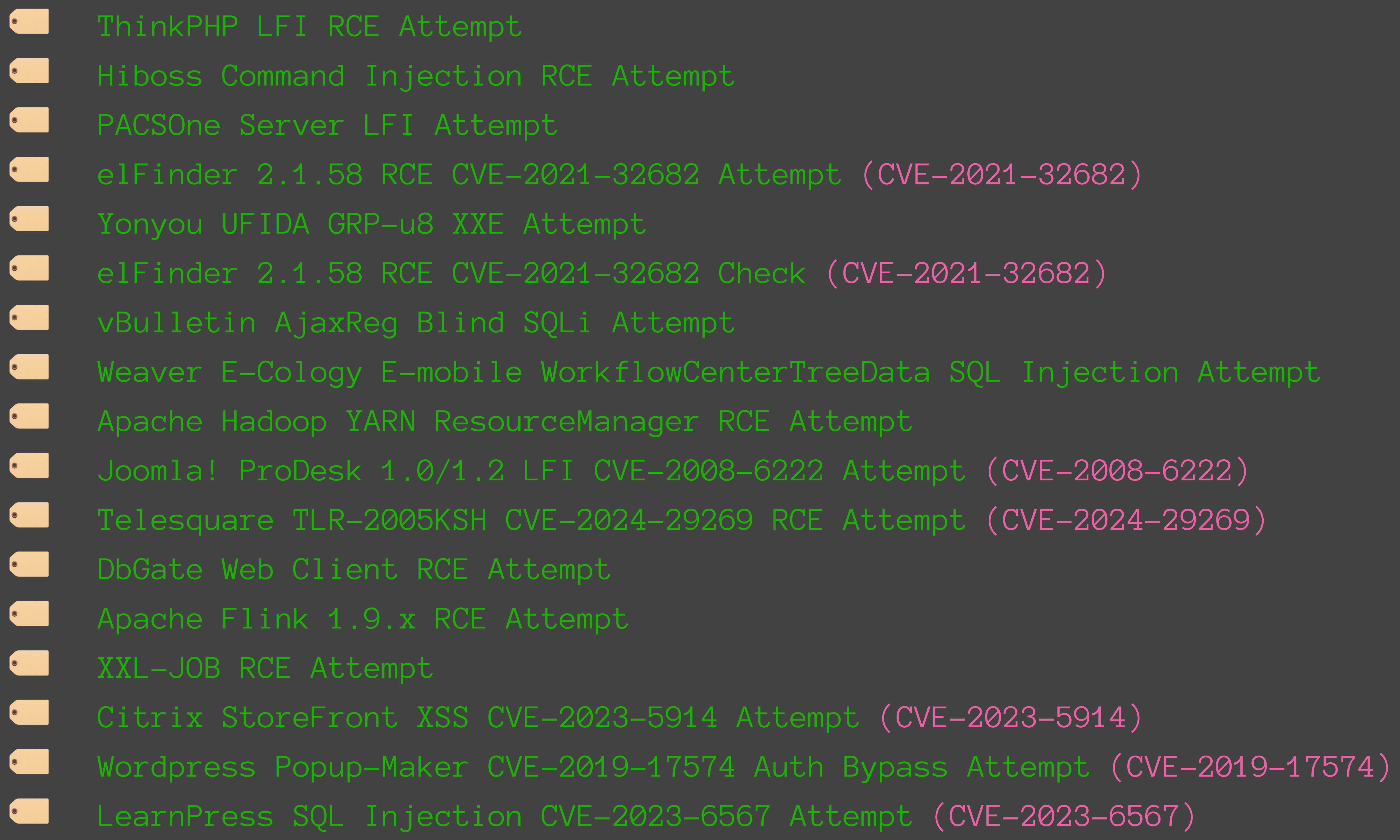
https://www.greynoise.io/blog/cve-2024-3400-command-injection-vulnerability-palo-alto-networks-pan-os

https://viz.greynoise.io/tags/palo-alto-pan-os-cve-2024-3400-rce-attempt?days=30

STORMWATCH

CYBERSECURITY NEWS

TAG ROUND-UP

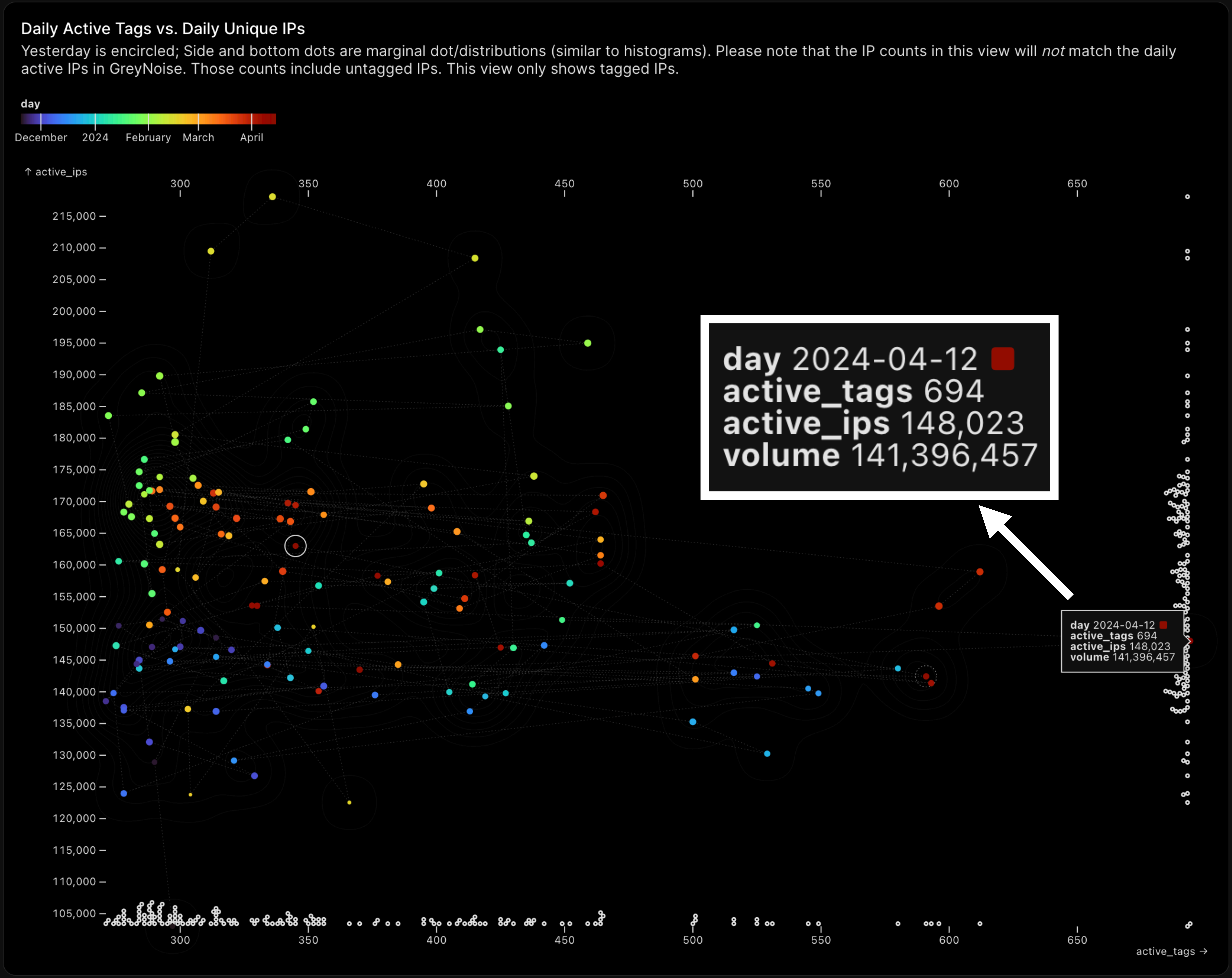


- ThinkPHP LFI RCE Attempt
- Hiboss Command Injection RCE Attempt
- PACSOne Server LFI Attempt
- elFinder 2.1.58 RCE CVE-2021-32682 Attempt (CVE-2021-32682)
- Yonyou UFIDA GRP-u8 XXE Attempt
- elFinder 2.1.58 RCE CVE-2021-32682 Check (CVE-2021-32682)
- vBulletin AjaxReg Blind SQLi Attempt
- Weaver E-Cology E-mobile WorkflowCenterTreeData SQL Injection Attempt
- Apache Hadoop YARN ResourceManager RCE Attempt
- Joomla! ProDesk 1.0/1.2 LFI CVE-2008-6222 Attempt (CVE-2008-6222)
- Telesquare TLR-2005KSH CVE-2024-29269 RCE Attempt (CVE-2024-29269)
- DbGate Web Client RCE Attempt
- Apache Flink 1.9.x RCE Attempt
- XXL-JOB RCE Attempt
- Citrix StoreFront XSS CVE-2023-5914 Attempt (CVE-2023-5914)
- Wordpress Popup-Maker CVE-2019-17574 Auth Bypass Attempt (CVE-2019-17574)
- LearnPress SQL Injection CVE-2023-6567 Attempt (CVE-2023-6567)

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

- Duplicator Unauthenticated Data Exposure CVE-2023-6114 Attempt (CVE-2023-6114)
- ColumbiaSoft DocumentLocator SSRF CVE-2023-5830 Attempt (CVE-2023-5830)
- ZZZCMD zzzphp CVE-2019-9041 RCE Attempt (CVE-2019-9041)
- WordPress Automatic Plugin CVE-2024-27954 Attempt (CVE-2024-27354)
- Adobe ColdFusion Arbitrary File Read CVE-2024-20767 Attempt (CVE-2024-20767)
- ESAFENET CDG Arbitrary File Download CVE-2019-9632 Attempt (CVE-2019-9632)
- Nexus Repository Manager CVE-2020-10199 RCE Attempt (CVE-2020-10199)
- NotificationX SQL Injection CVE-2024-1698 Attempt (CVE-2024-1698)
- Apache Tika CVE-2018-1335 Command Injection RCE Attempt (CVE-2018-1335)
- Qi An Xin Wang Kang Firewall RCE Attempt
- PrestaShop AtributeWizardPro CVE-2018-10942 Arbitrary File Upload Attempt (CVE-2018-10942)
- Joomla! Component RWCards 3.0.11 LFI CVE-2008-6172 Attempt (CVE-2008-6172)
- Palo Alto PAN-OS CVE-2024-3400 RCE Attempt (CVE-2024-3400)
- Zabbix Default Credential Attempt
- EC2 IAM Credential Access Attempt
- Samsung WLAN AP RCE Attempt
- Tongda OA Login Bypass Attempt
- Inspur ClusterEngine CVE-2020-21224 RCE Attempt (CVE-2020-21224)
- ThinkPHP PHP Code Injection RCE Attempt

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



Daily Active Tags vs. Daily Unique IPs

Yesterday is encircled; Side and bottom dots are marginal dot/distributions (similar to histograms). Please note that the IP counts in this view will *not* match the daily active IPs in GreyNoise. Those counts include untagged IPs. This view only shows tagged IPs.

day 2024-04-12 🟥
active_tags 694
active_ips 148,023
volume 141,396,457

day 2024-04-12 🟥
active_tags 694
active_ips 148,023
volume 141,396,457

WE NEED

TO TALK

ABOUT

KEV

STORM WATCH

It Has Been

5

Days Since The Last KEV Release

https://kev.hrbrmstr.app

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

CVE-2024-3273: D-Link Multiple NAS Devices Command Injection

CVE-2024-3272: D-Link Multiple NAS Devices Use of Hard-Coded Credentials

CVE-2024-3400: Palo Alto Networks PAN-OS Command Injection