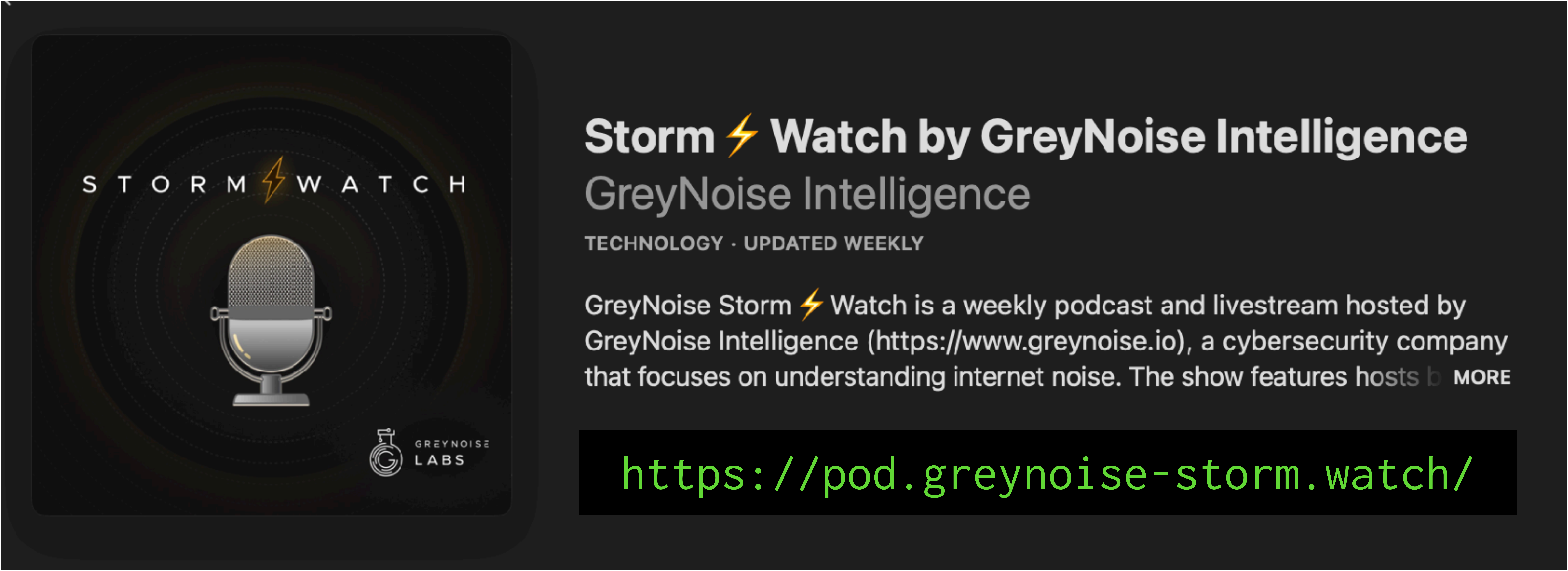
STORM⚡WATCH

Dateline: 2023-12-05

GREYNOISE
LABS



Storm ⚡ Watch by GreyNoise Intelligence

GreyNoise Intelligence

TECHNOLOGY · UPDATED WEEKLY

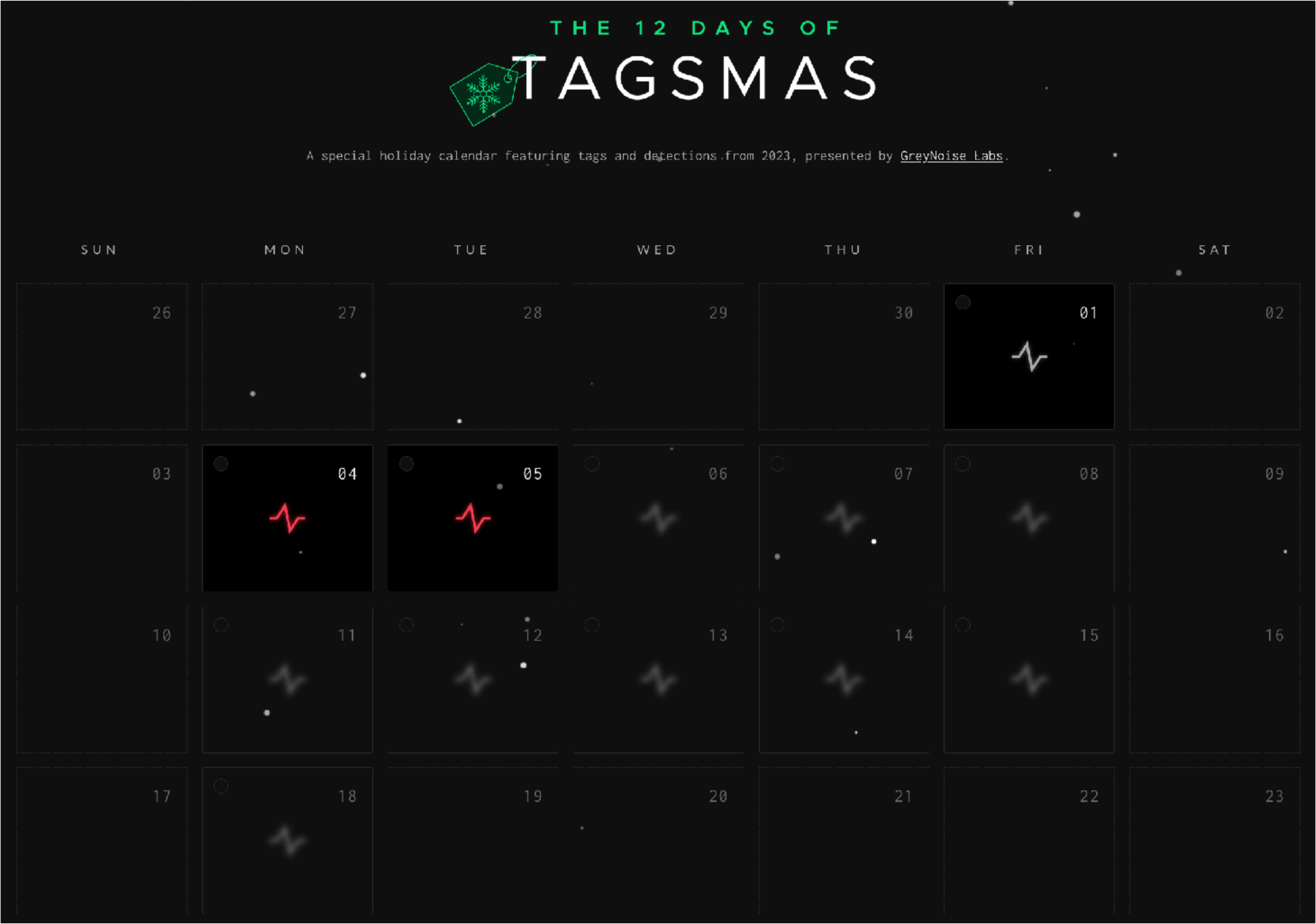
GreyNoise Storm ⚡ Watch is a weekly podcast and livestream hosted by GreyNoise Intelligence (https://www.greynoise.io), a cybersecurity company that focuses on understanding internet noise. The show features hosts b MORE

https://pod.greynoise-storm.watch/

https://show.greynoise-storm.watch/

TAGSMAS IS **HERE!**

https://www.greynoise.io/12-days-of-tagsmas



THE 12 DAYS OF

TAGSMAS

A special holiday calendar featuring tags and detections from 2023, presented by GreyNoise Labs.

SUN	MON	TUE	WED	THU	FRI	SAT
26	27	28	29	30	01	02
03	04	05	06	07	08	09
10	11	12	13	14	15	16
17	18	19	20	21	22	23

About Trinity Cyber

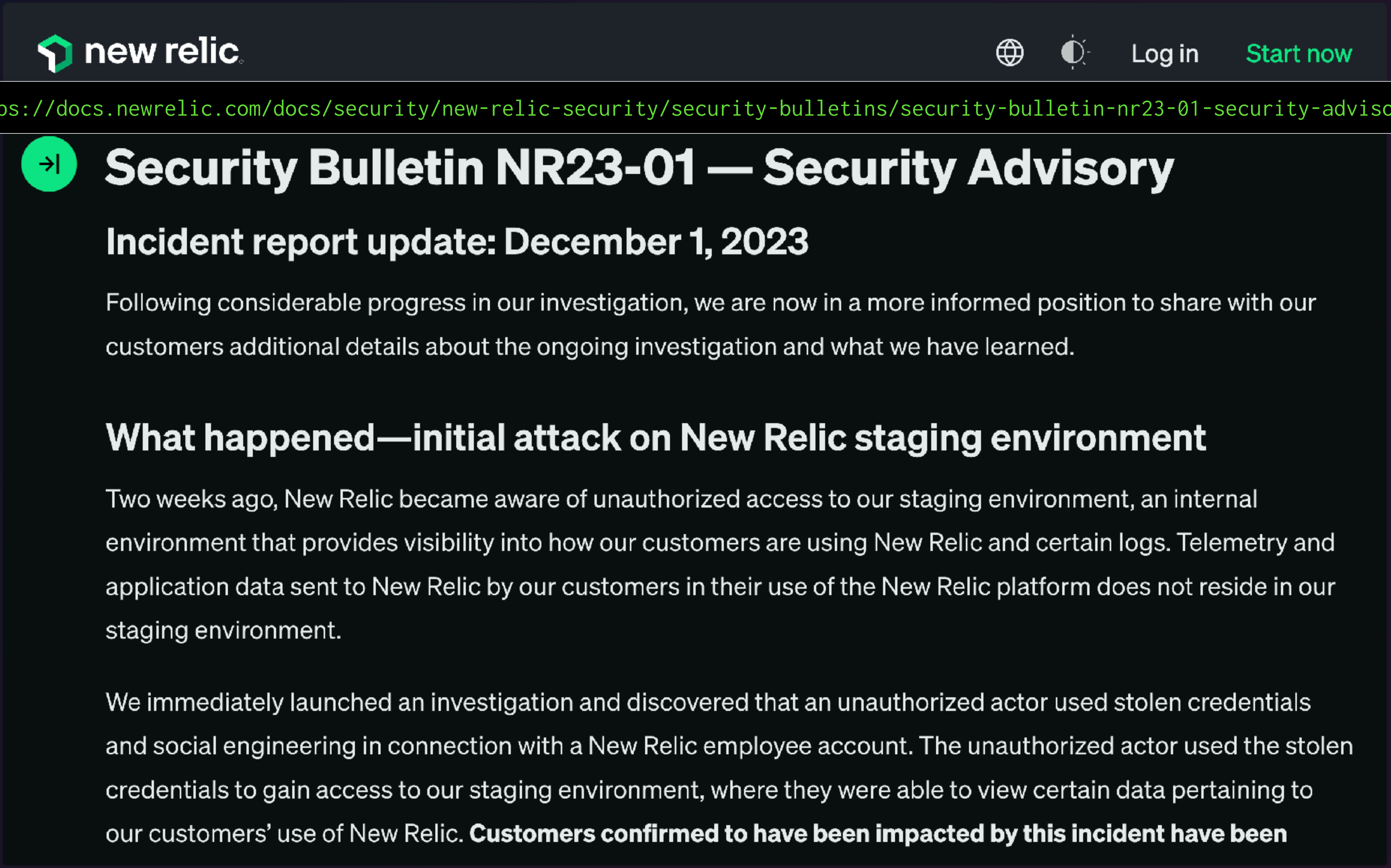
https://www.trinitycyber.com/

The Future of Cybersecurity

At Trinity Cyber, our mission is to stop the bad guys. We invented and patented a groundbreaking new approach to cybersecurity that identifies, stops and prevents threats others miss. Our technology is the first in the industry that can deeply inspect full session Internet traffic in both directions to expose and mitigate threat content inline. We are solving the four biggest challenges for customers today with better security, automated vulnerability mitigation, reduced alert fatigue and fewer false positives.

BREAKING NEWS

`https://docs.newrelic.com/docs/security/new-relic-security/security-bulletins/security-bulletin-nr23-01-security-advisory/`



Security Bulletin NR23-01 — Security Advisory

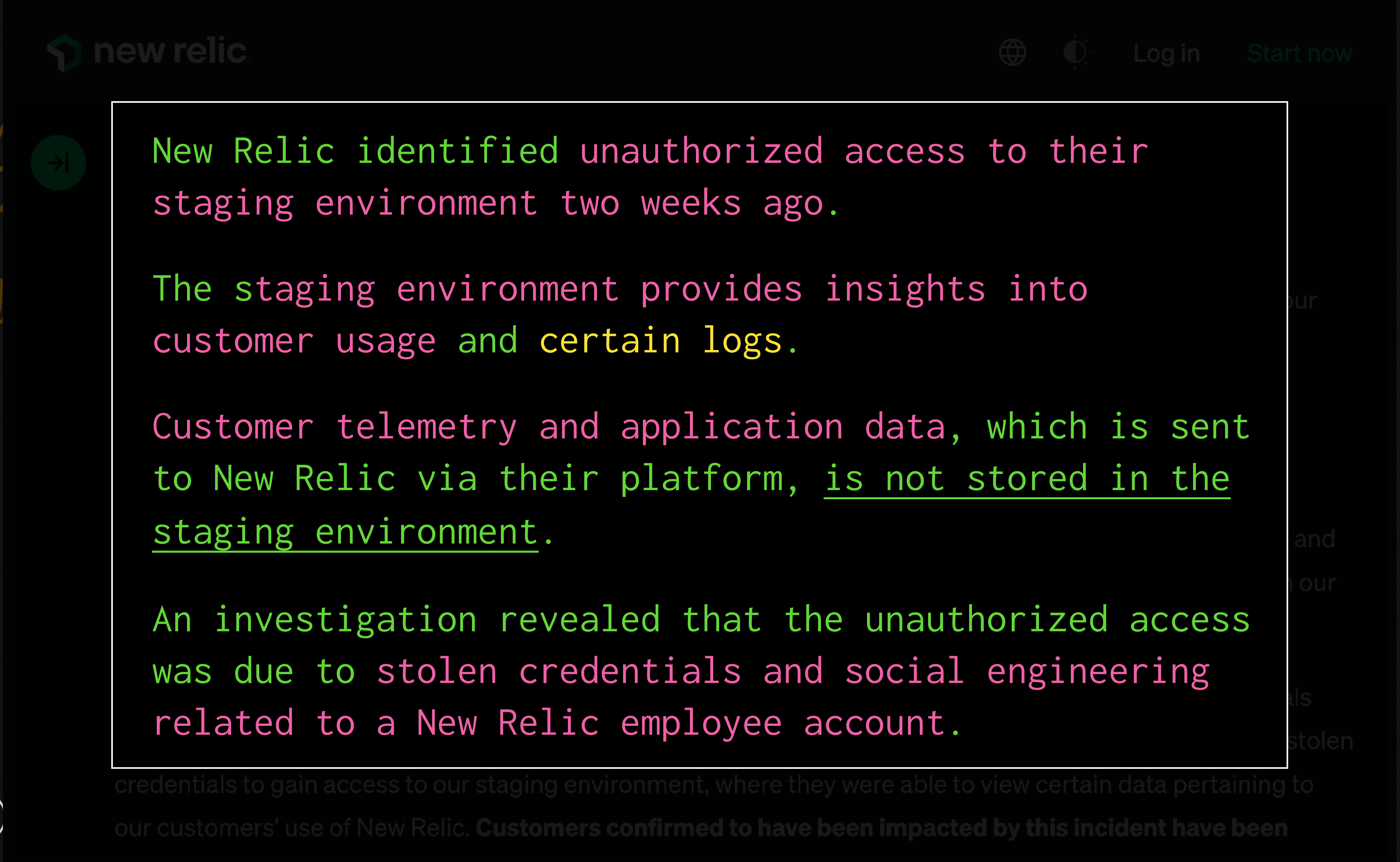
Incident report update: December 1, 2023

Following considerable progress in our investigation, we are now in a more informed position to share with our customers additional details about the ongoing investigation and what we have learned.

What happened—initial attack on New Relic staging environment

Two weeks ago, New Relic became aware of unauthorized access to our staging environment, an internal environment that provides visibility into how our customers are using New Relic and certain logs. Telemetry and application data sent to New Relic by our customers in their use of the New Relic platform does not reside in our staging environment.

We immediately launched an investigation and discovered that an unauthorized actor used stolen credentials and social engineering in connection with a New Relic employee account. The unauthorized actor used the stolen credentials to gain access to our staging environment, where they were able to view certain data pertaining to our customers' use of New Relic. **Customers confirmed to have been impacted by this incident have been**



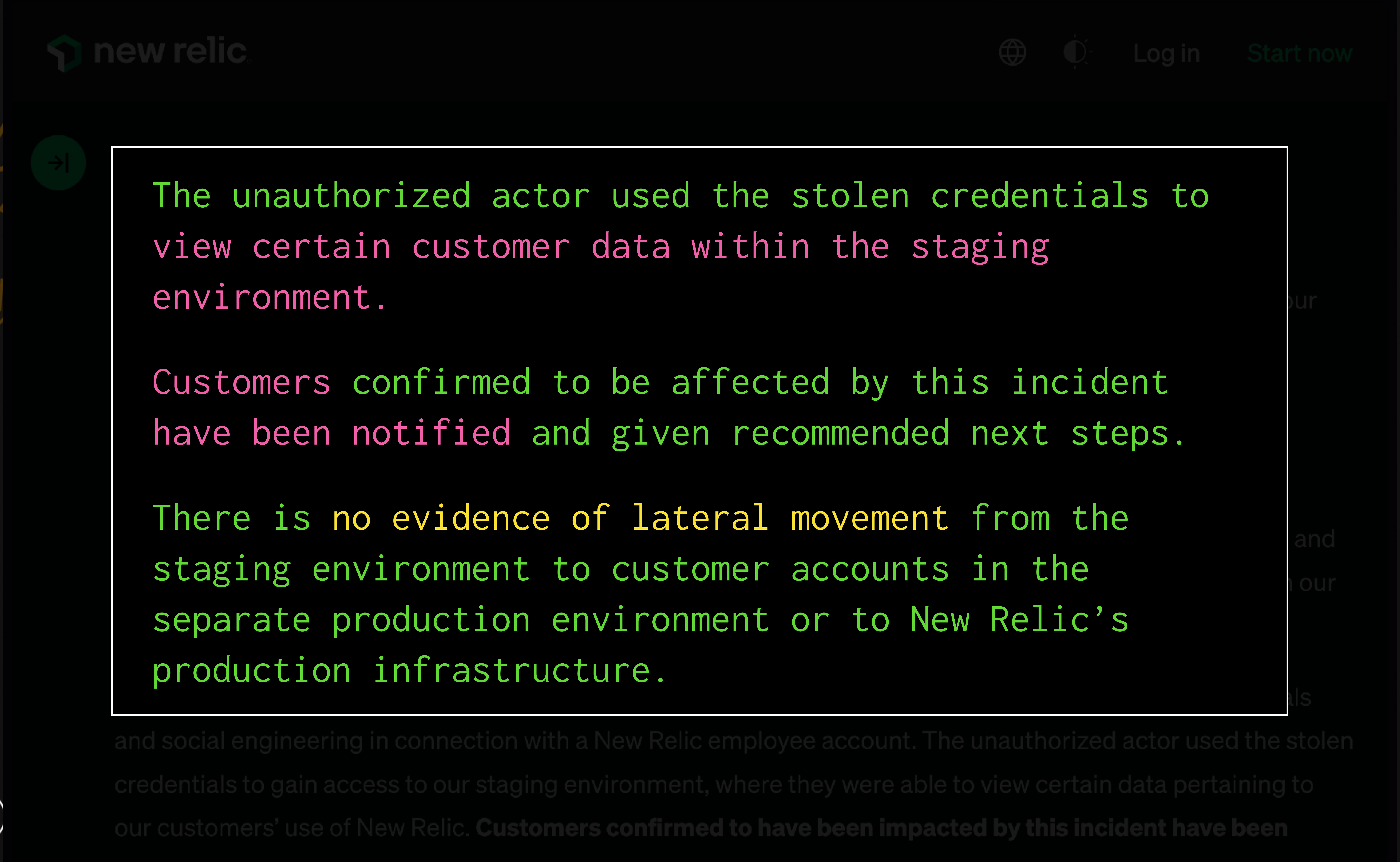
New Relic identified unauthorized access to their staging environment two weeks ago.

The staging environment provides insights into customer usage and certain logs.

Customer telemetry and application data, which is sent to New Relic via their platform, is not stored in the staging environment.

An investigation revealed that the unauthorized access was due to stolen credentials and social engineering related to a New Relic employee account.

credentials to gain access to our staging environment, where they were able to view certain data pertaining to our customers' use of New Relic. **Customers confirmed to have been impacted by this incident have been**



The unauthorized actor used the stolen credentials to view certain customer data within the staging environment.

Customers confirmed to be affected by this incident have been notified and given recommended next steps.

There is no evidence of lateral movement from the staging environment to customer accounts in the separate production environment or to New Relic’s production infrastructure.

ur

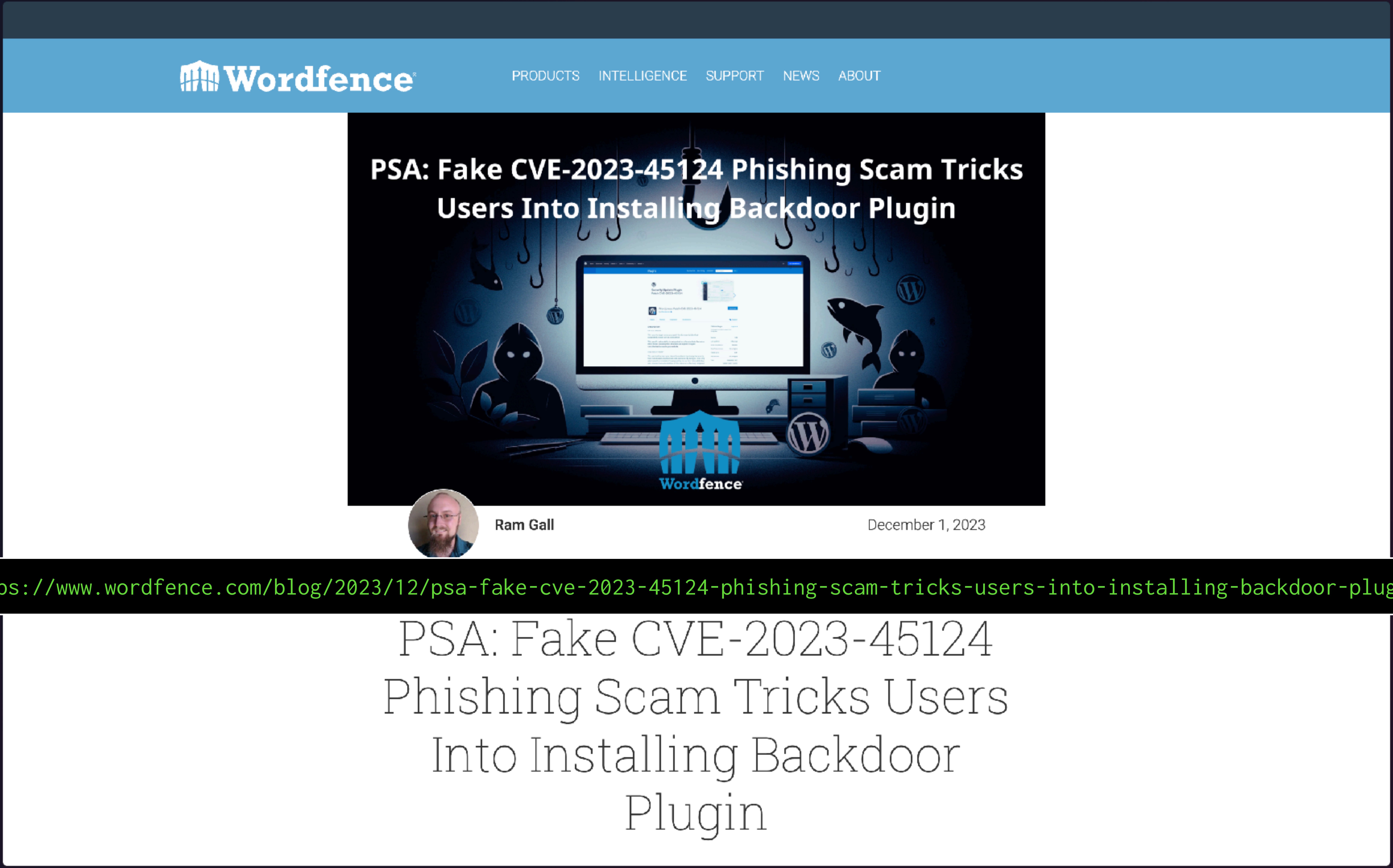
and

our

als

and social engineering in connection with a New Relic employee account. The unauthorized actor used the stolen credentials to gain access to our staging environment, where they were able to view certain data pertaining to our customers’ use of New Relic. **Customers confirmed to have been impacted by this incident have been**

NOW BACK TO OUR REGULARLY SCHEDULED PROGRAMMING



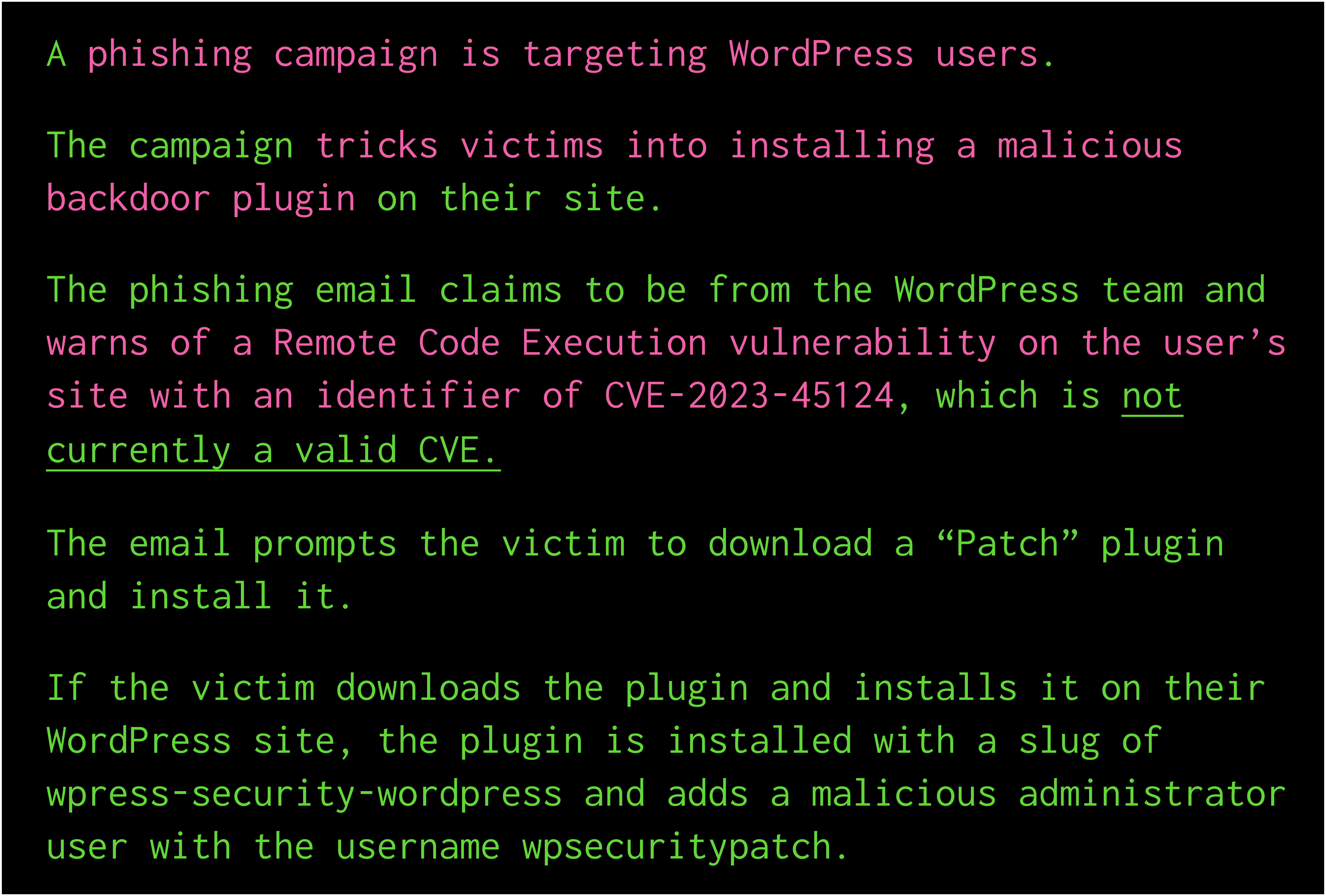
PSA: Fake CVE-2023-45124 Phishing Scam Tricks Users Into Installing Backdoor Plugin

Ram Gall

December 1, 2023

https://www.wordfence.com/blog/2023/12/psa-fake-cve-2023-45124-phishing-scam-tricks-users-into-installing-backdoor-plugin/

PSA: Fake CVE-2023-45124 Phishing Scam Tricks Users Into Installing Backdoor Plugin



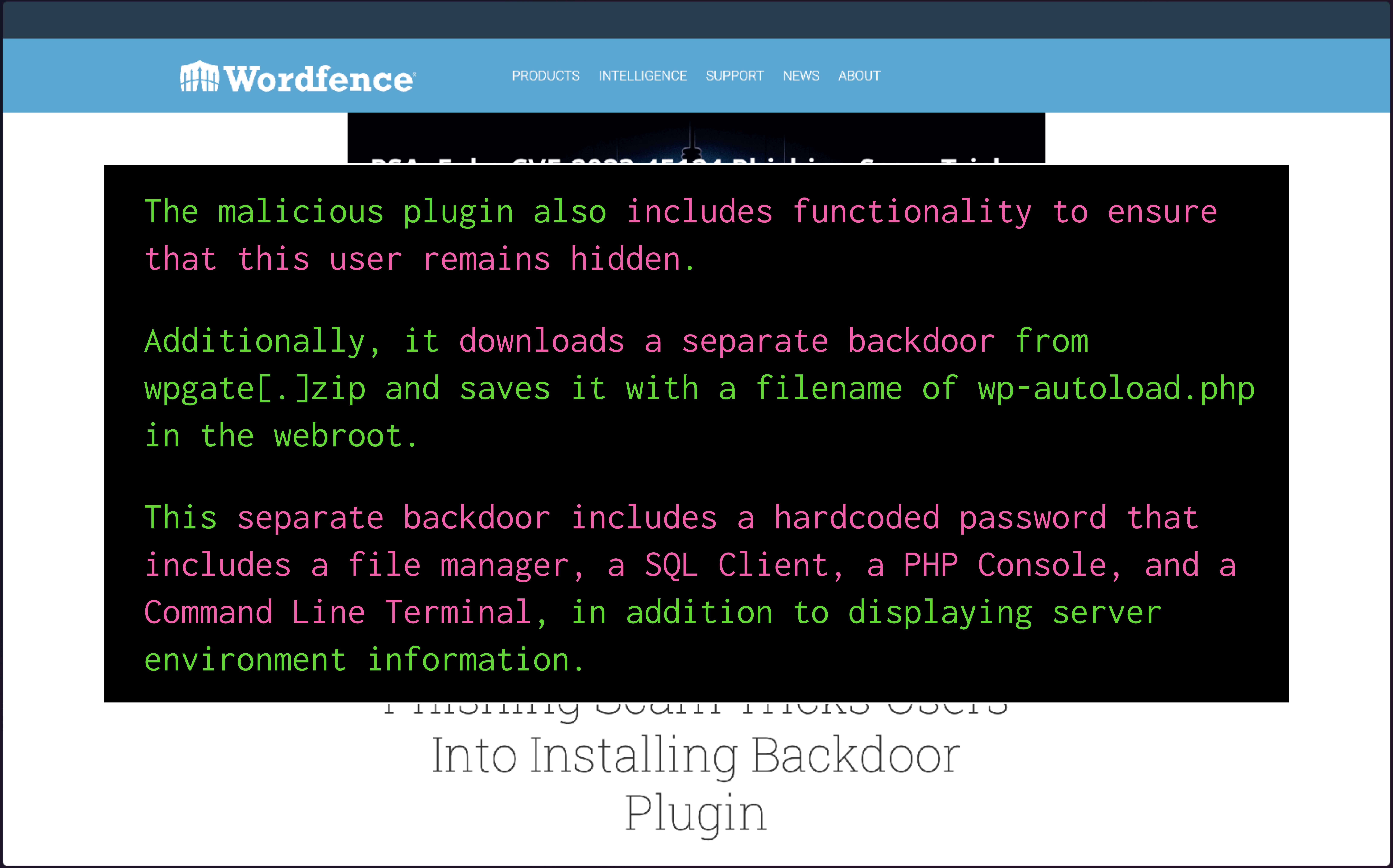
A phishing campaign is targeting WordPress users.

The campaign tricks victims into installing a malicious backdoor plugin on their site.

The phishing email claims to be from the WordPress team and warns of a Remote Code Execution vulnerability on the user's site with an identifier of CVE-2023-45124, which is not currently a valid CVE.

The email prompts the victim to download a "Patch" plugin and install it.

If the victim downloads the plugin and installs it on their WordPress site, the plugin is installed with a slug of wpress-security-wordpress and adds a malicious administrator user with the username wpsecuritypatch.



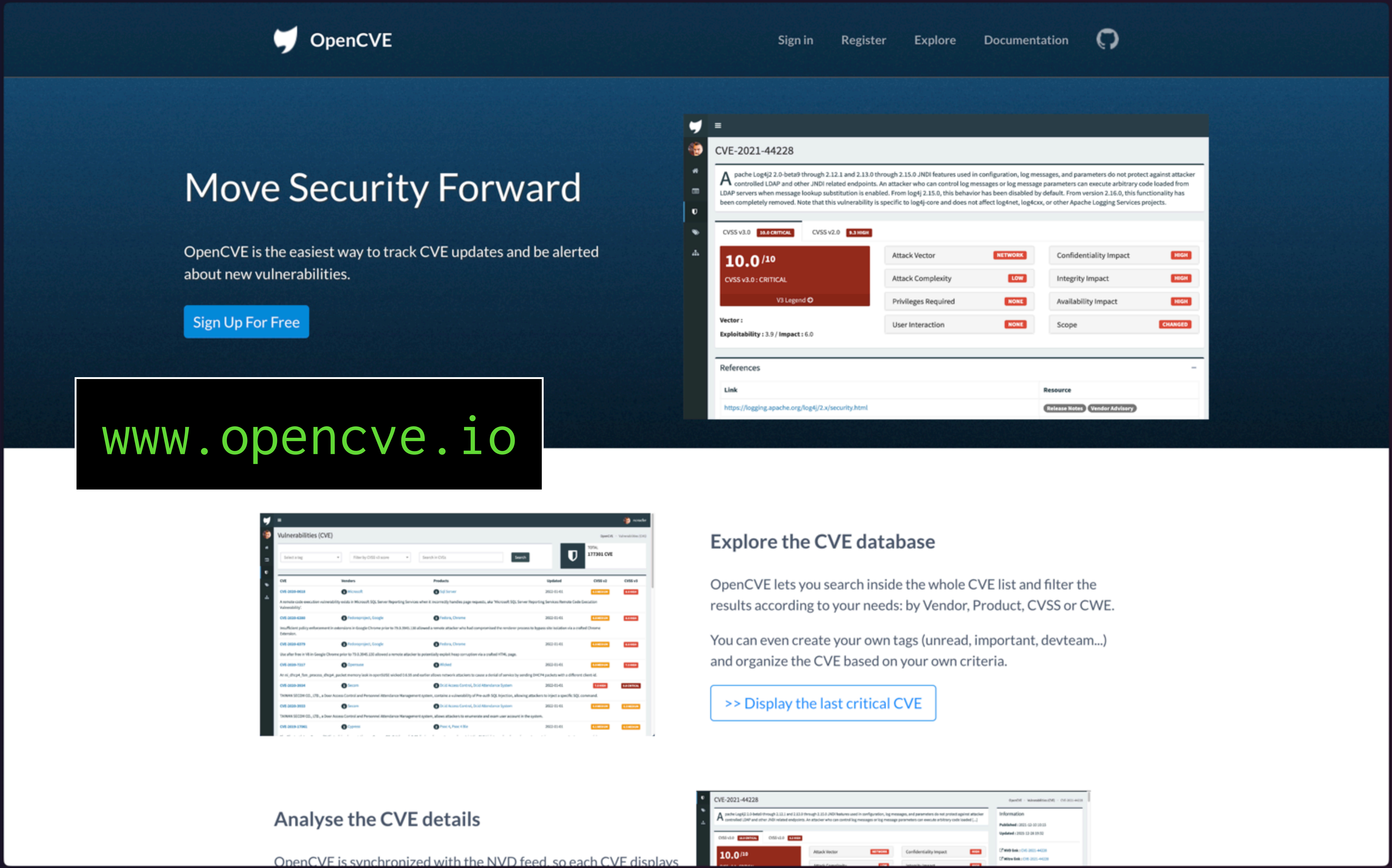
```
The malicious plugin also includes functionality to ensure
that this user remains hidden.

Additionally, it downloads a separate backdoor from
wpgate[.]zip and saves it with a filename of wp-autoload.php
in the webroot.

This separate backdoor includes a hardcoded password that
includes a file manager, a SQL Client, a PHP Console, and a
Command Line Terminal, in addition to displaying server
environment information.
```

Into Installing Backdoor Plugin

TOOL TIME



Move Security Forward

OpenCVE is the easiest way to track CVE updates and be alerted about new vulnerabilities.

Sign Up For Free

CVE-2021-44228

Apache Log4j2 2.0-beta9 through 2.12.1 and 2.13.0 through 2.15.0 JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by default. From version 2.16.0, this functionality has been completely removed. Note that this vulnerability is specific to log4j-core and does not affect log4net, log4cxx, or other Apache Logging Services projects.

CVSS v3.0 10.0 CRITICAL | CVSS v2.0 9.3 HIGH

10.0 /10
CVSS v3.0 : CRITICAL
V3 Legend

Attack Vector	NETWORK	Confidentiality Impact	HIGH
Attack Complexity	LOW	Integrity Impact	HIGH
Privileges Required	NONE	Availability Impact	HIGH
User Interaction	NONE	Scope	CHANGED

Vector :

Exploitability : 3.9 / **Impact :** 6.0

References

Link	Resource
https://logging.apache.org/log4j/2.x/security.html	Release Notes Vendor Advisory

www.opencve.io

Vulnerabilities (CVE)

177301 CVE

Explore the CVE database

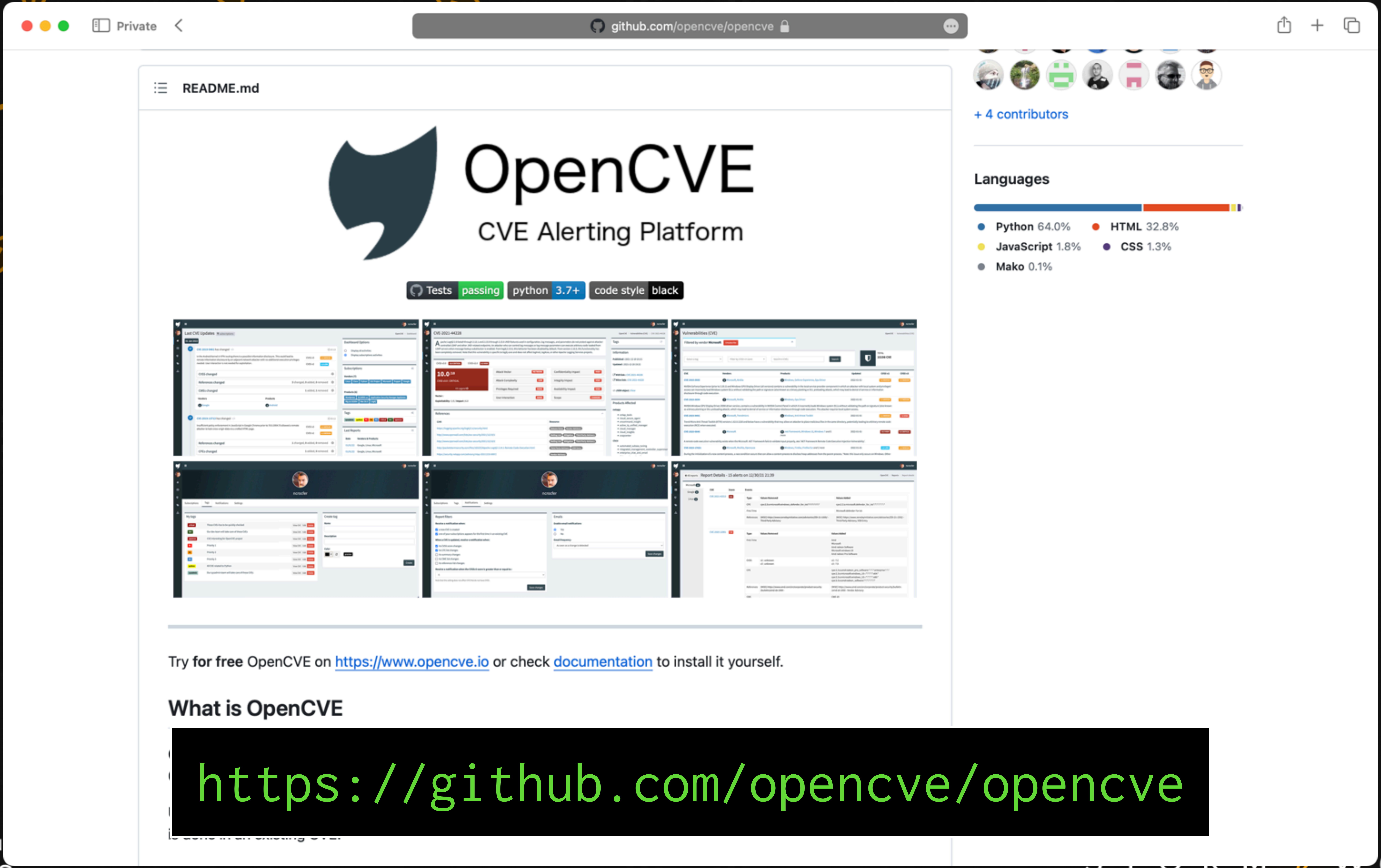
OpenCVE lets you search inside the whole CVE list and filter the results according to your needs: by Vendor, Product, CVSS or CWE.

You can even create your own tags (unread, important, devteam...) and organize the CVE based on your own criteria.

>> Display the last critical CVE

Analyse the CVE details

OpenCVE is synchronized with the NVD feed, so each CVE displays



README.md

OpenCVE

CVE Alerting Platform

Tests passing | python 3.7+ | code style black

Try **for free** OpenCVE on https://www.opencve.io or check documentation to install it yourself.

What is OpenCVE

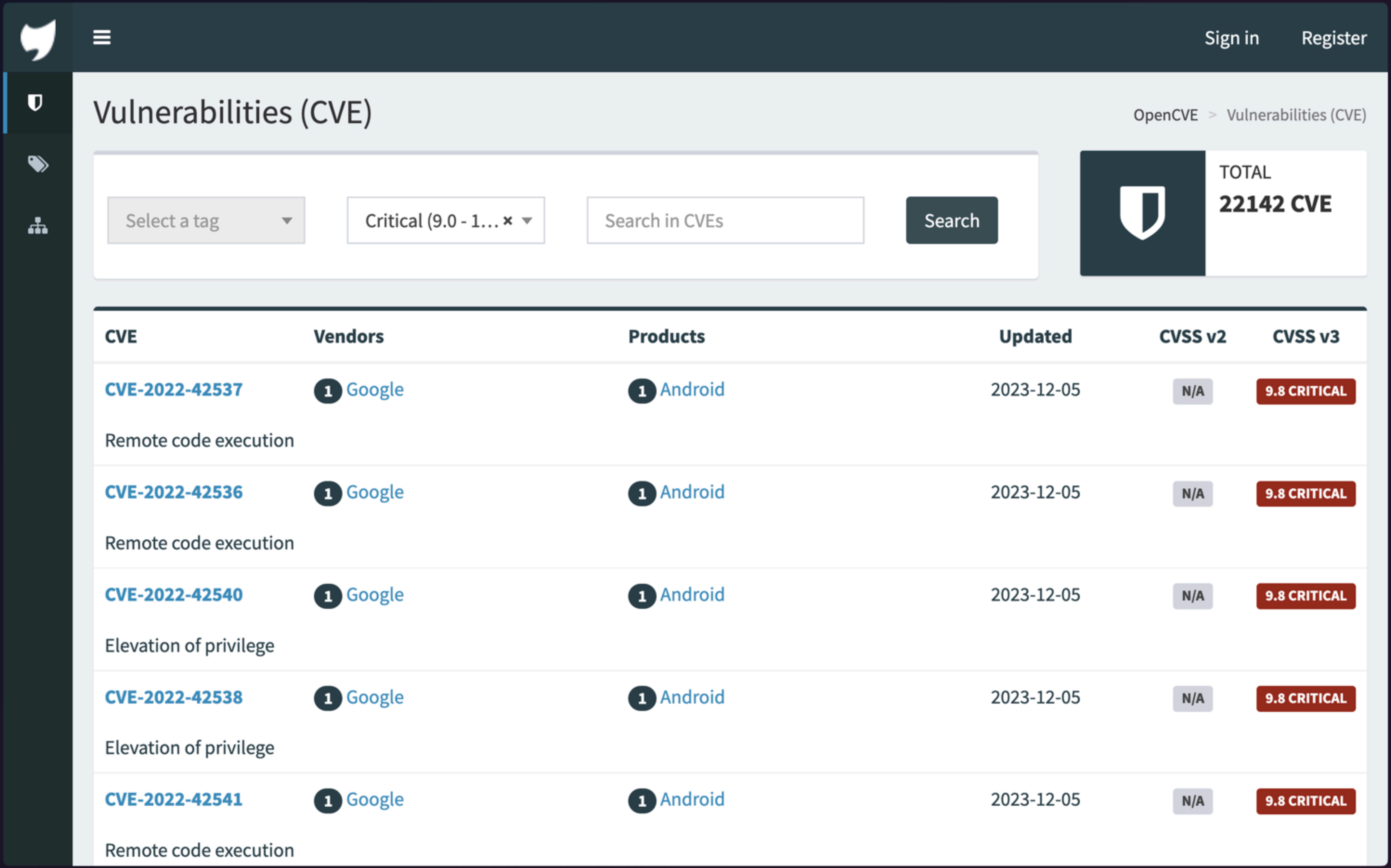
is done in an existing CVE.

+ 4 contributors

Languages

- Python 64.0%
- HTML 32.8%
- JavaScript 1.8%
- CSS 1.3%
- Mako 0.1%

https://github.com/opencve/opencve



Vulnerabilities (CVE)

OpenCVE > Vulnerabilities (CVE)

Select a tag ▾ | Critical (9.0 - 1… × ▾ | Search in CVEs | Search

TOTAL
22142 CVE

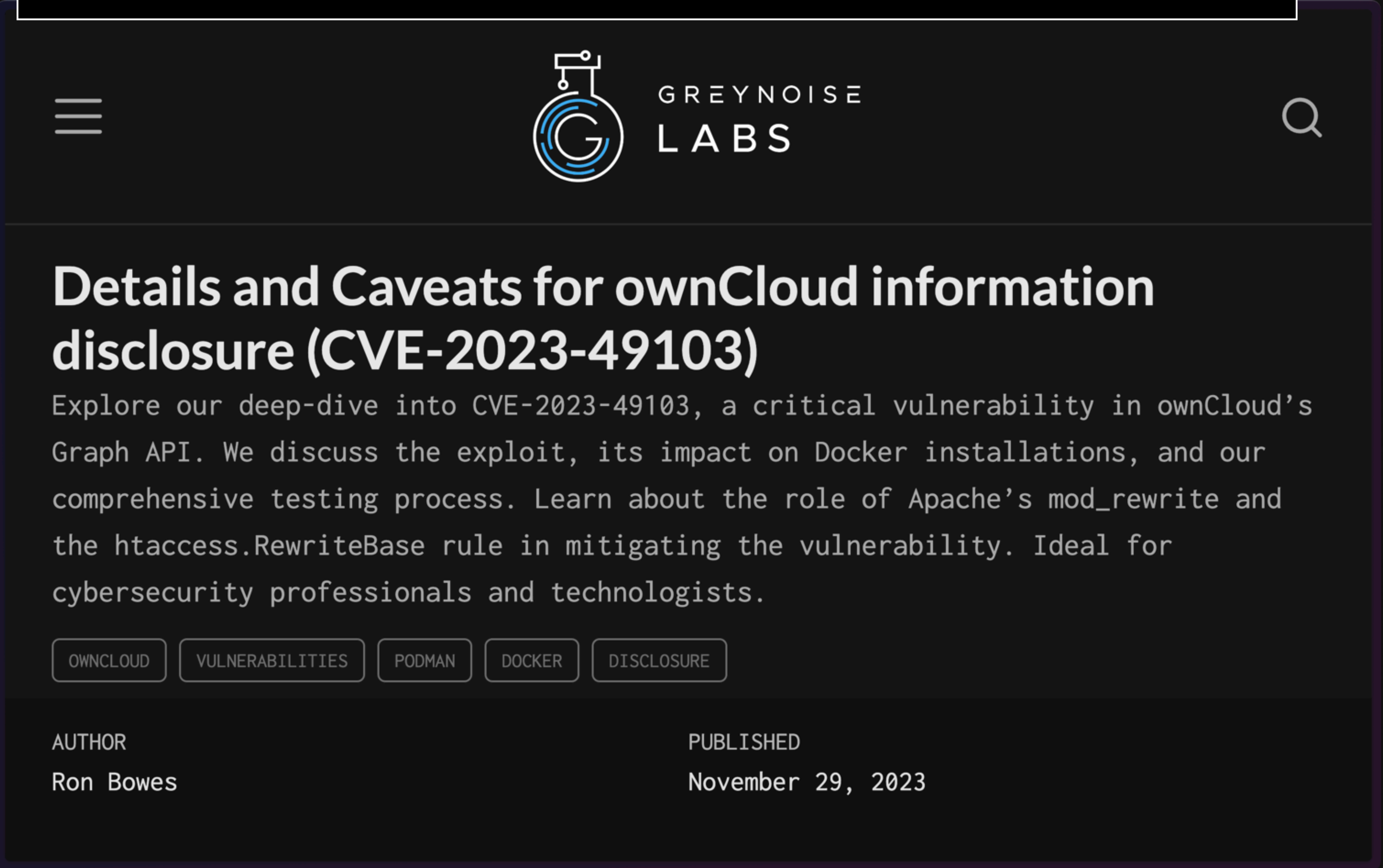
CVE	Vendors	Products	Updated	CVSS v2	CVSS v3
CVE-2022-42537 Remote code execution	1 Google	1 Android	2023-12-05	N/A	9.8 CRITICAL
CVE-2022-42536 Remote code execution	1 Google	1 Android	2023-12-05	N/A	9.8 CRITICAL
CVE-2022-42540 Elevation of privilege	1 Google	1 Android	2023-12-05	N/A	9.8 CRITICAL
CVE-2022-42538 Elevation of privilege	1 Google	1 Android	2023-12-05	N/A	9.8 CRITICAL
CVE-2022-42541 Remote code execution	1 Google	1 Android	2023-12-05	N/A	9.8 CRITICAL

Shameless Self-Promotion

GREYNOISE LABS

STORM⚡WATCH

https://www.labs.greynoise.io//grimoire/2023-11-29-owncloud-redux/



GREYNOISE LABS

Details and Caveats for ownCloud information disclosure (CVE-2023-49103)

Explore our deep-dive into CVE-2023-49103, a critical vulnerability in ownCloud’s Graph API. We discuss the exploit, its impact on Docker installations, and our comprehensive testing process. Learn about the role of Apache’s mod_rewrite and the htaccess.RewriteBase rule in mitigating the vulnerability. Ideal for cybersecurity professionals and technologists.

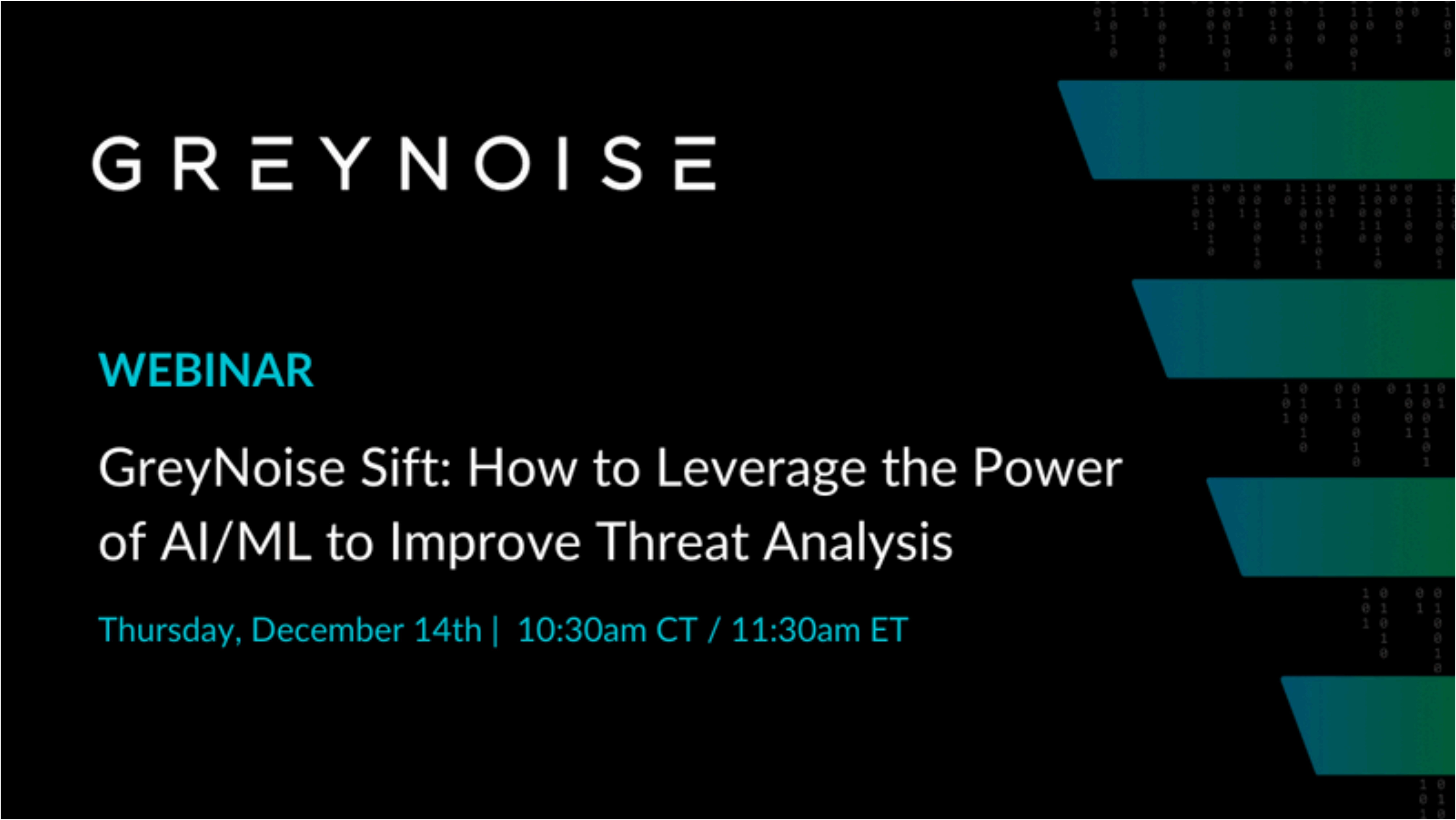
AUTHOR
Ron Bowes

PUBLISHED
November 29, 2023

NOISELETTER

NOVEMBER 2023

https://www.greynoise.io/resources/noiseletter-november-2023 http://www.greynoise.io/events/webinar-greynoise-sift-how-to-leverage-the-power-of-ai-ml-to-improve-threat-analysis

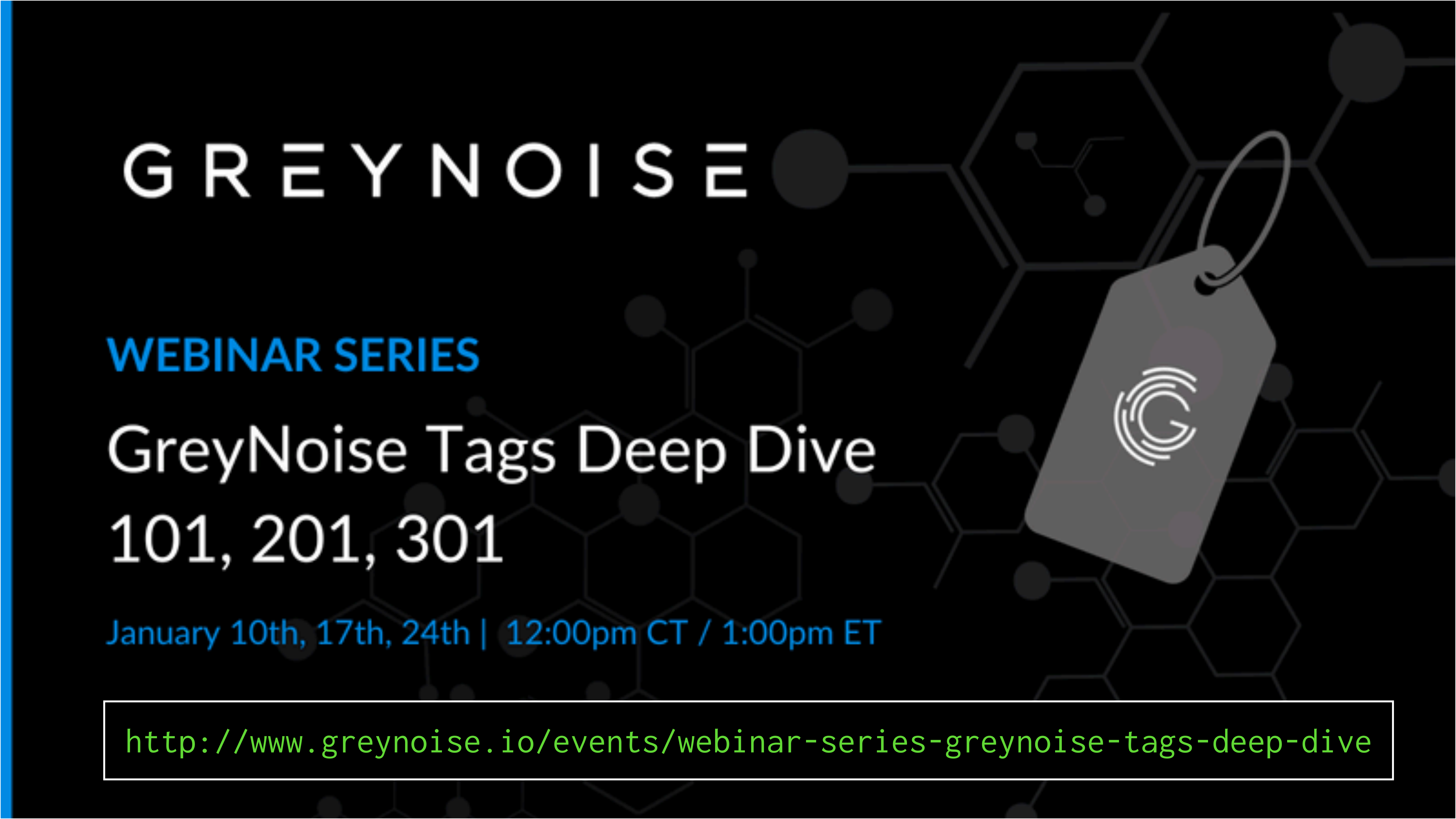


GREYNOISE

WEBINAR

GreyNoise Sift: How to Leverage the Power of AI/ML to Improve Threat Analysis

Thursday, December 14th | 10:30am CT / 11:30am ET



GREYNOISE

WEBINAR SERIES

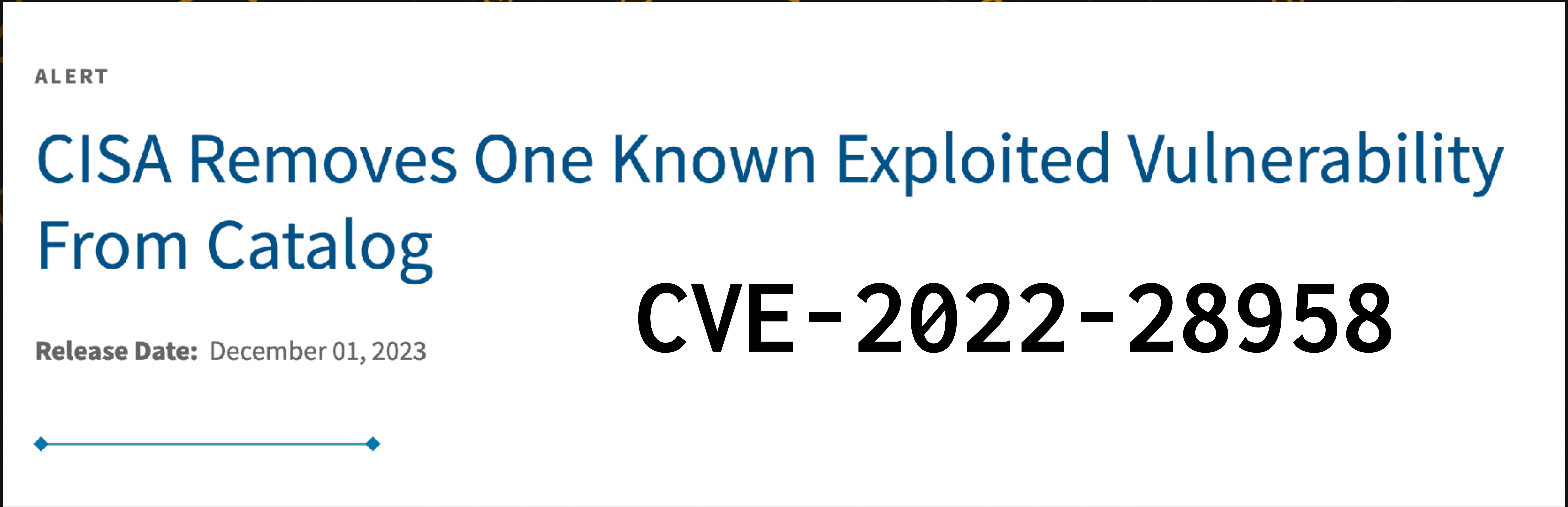
GreyNoise Tags Deep Dive 101, 201, 301

January 10th, 17th, 24th | 12:00pm CT / 1:00pm ET

```
http://www.greynoise.io/events/webinar-series-greynoise-tags-deep-dive
```

- Apache Struts2 includeParams RCE Attempt
- China Chopper Webshell
- PHP Utility Belt RCE Attempt

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



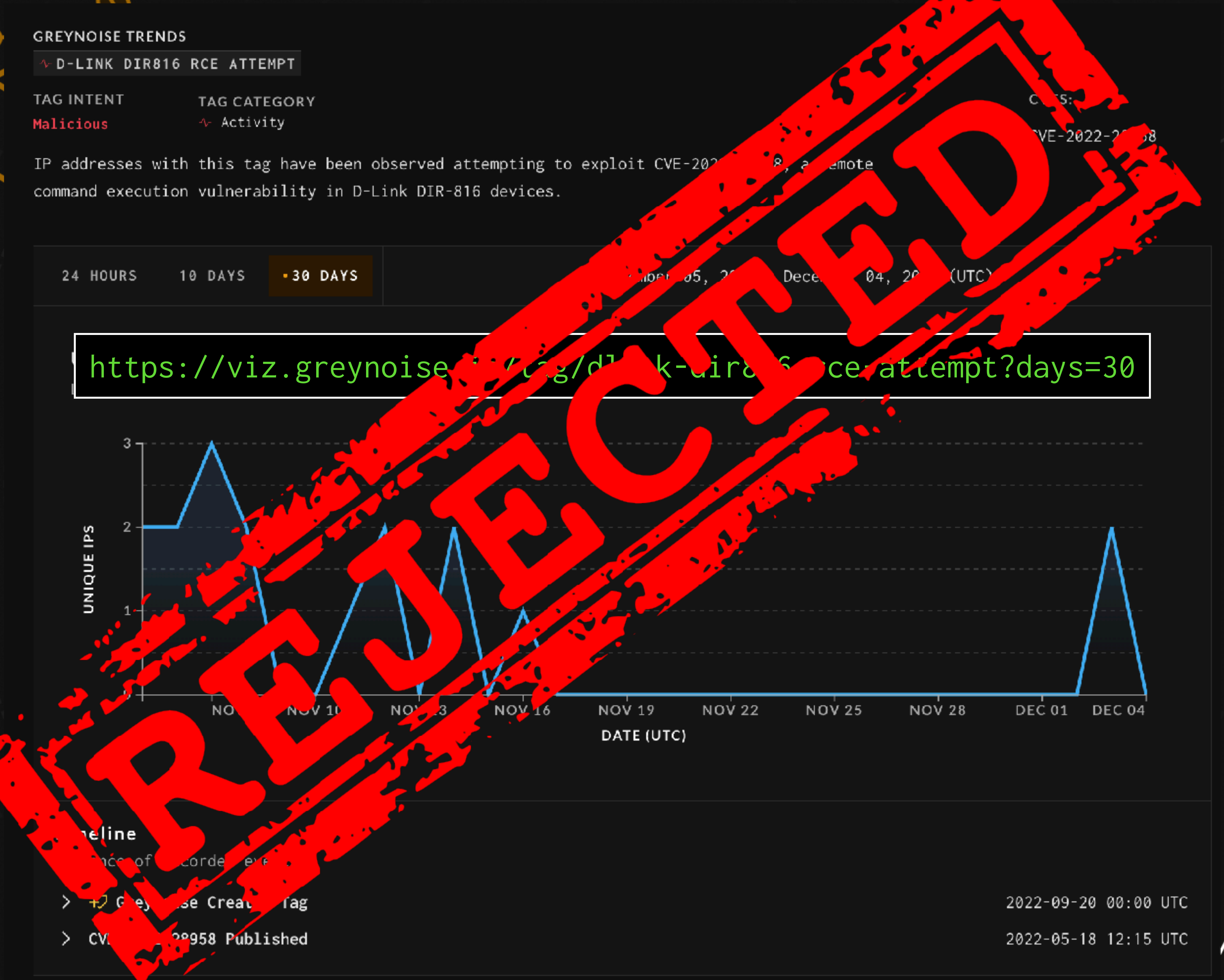
ALERT

CISA Removes One Known Exploited Vulnerability From Catalog

Release Date: December 01, 2023

CVE-2022-28958

https://www.cisa.gov/news-events/alerts/2023/12/01/cisa-removes-one-known-exploited-vulnerability-catalog



GREYNOISE TRENDS

D-LINK DIR816 RCE ATTEMPT

TAG INTENT
Malicious

TAG CATEGORY
Activity

CVES:
CVE-2022-28958

IP addresses with this tag have been observed attempting to exploit CVE-2022-28958, a remote command execution vulnerability in D-Link DIR-816 devices.

24 HOURS 10 DAYS 30 DAYS November 05, 2022 – December 04, 2022 (UTC)

https://viz.greynoise.io/tag/dlink-dir816-rce-attempt?days=30

Timeline

Sequence of recorded events

GreyNoise Created Tag 2022-09-20 00:00 UTC

CVE-2022-28958 Published 2022-05-18 12:15 UTC

REJECTED

GREYNOISE LABS

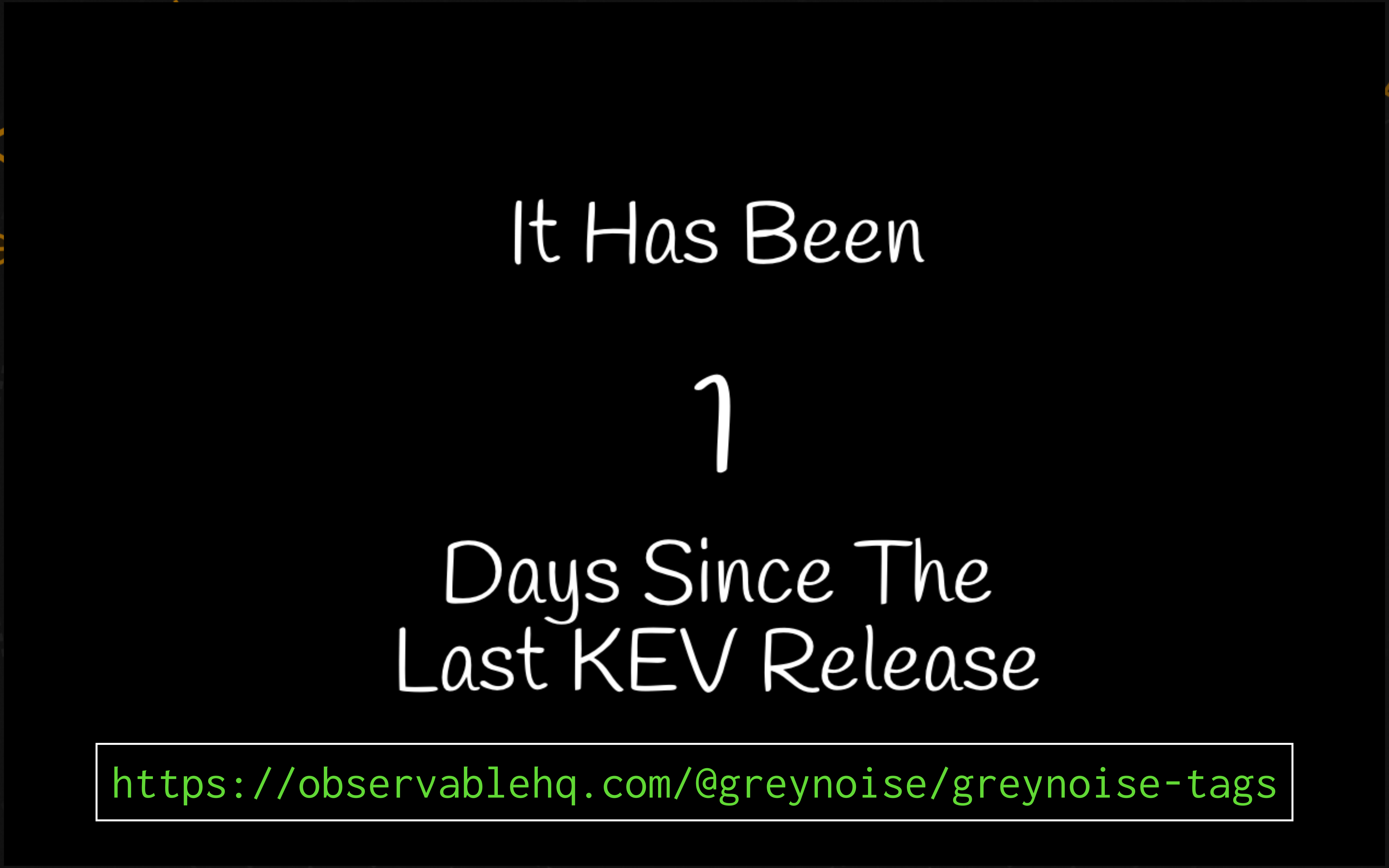
M WØTCH

WE NEED

TO TALK

ABOUT

KEV



It Has Been

1

Days Since The
Last KEV Release

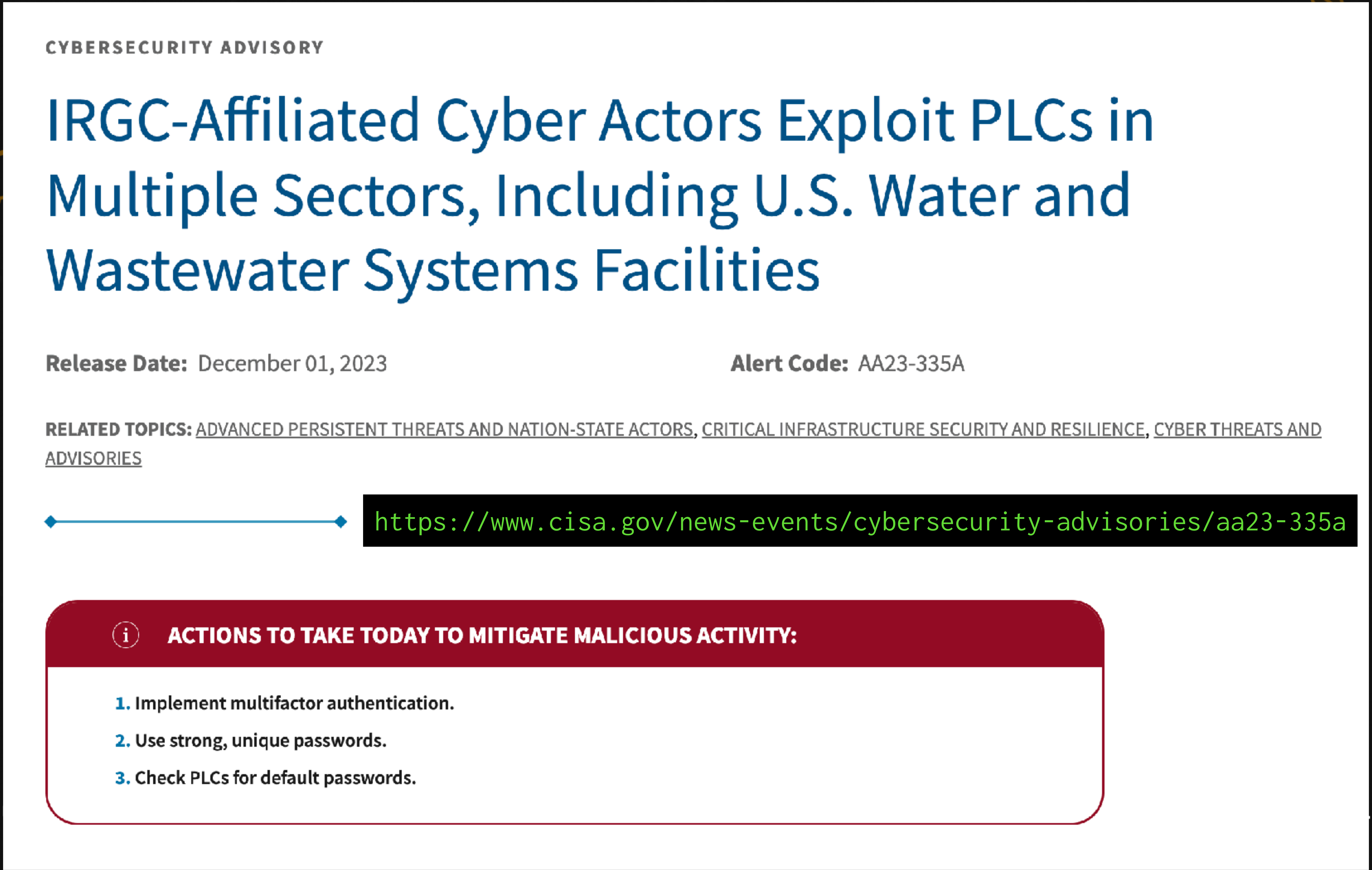
https://observablehq.com/@greynoise/greynoise-tags

- Google Skia Integer Overflow Vulnerability (CVE-2023-6345)
- ownCloud graphapi Information Disclosure Vulnerability (CVE-2023-49103)
- Apple Multiple Products WebKit Memory Corruption Vulnerability (CVE-2023-42917)
- Apple Multiple Products WebKit Out-of-Bounds Read Vulnerability (CVE-2023-42916)

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

CVE-2022-28958 was rejected from the CVE list because further investigation showed that it was not a security issue. This CVE was initially reported as a remote code execution (RCE) vulnerability in the D-Link DIR816L_FW206b01 firmware, specifically via the value parameter at shareport.php. However, this claim was disputed by a third party.

A detailed analysis by VulnCheck found that CVE-2022-28958 is not a real vulnerability and at-scale exploitation has never occurred. The vulnerability was initially reported to be exploited by Moobot, a Mirai-like botnet, but this was found to be incorrect. The report also pointed out that without a working bypass, an attacker would need to be authenticated to the device, a detail that was overlooked when assigning CVE-2022-28958 a CVSSv3 score of 9.8.



CYBERSECURITY ADVISORY

IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities

Release Date: December 01, 2023

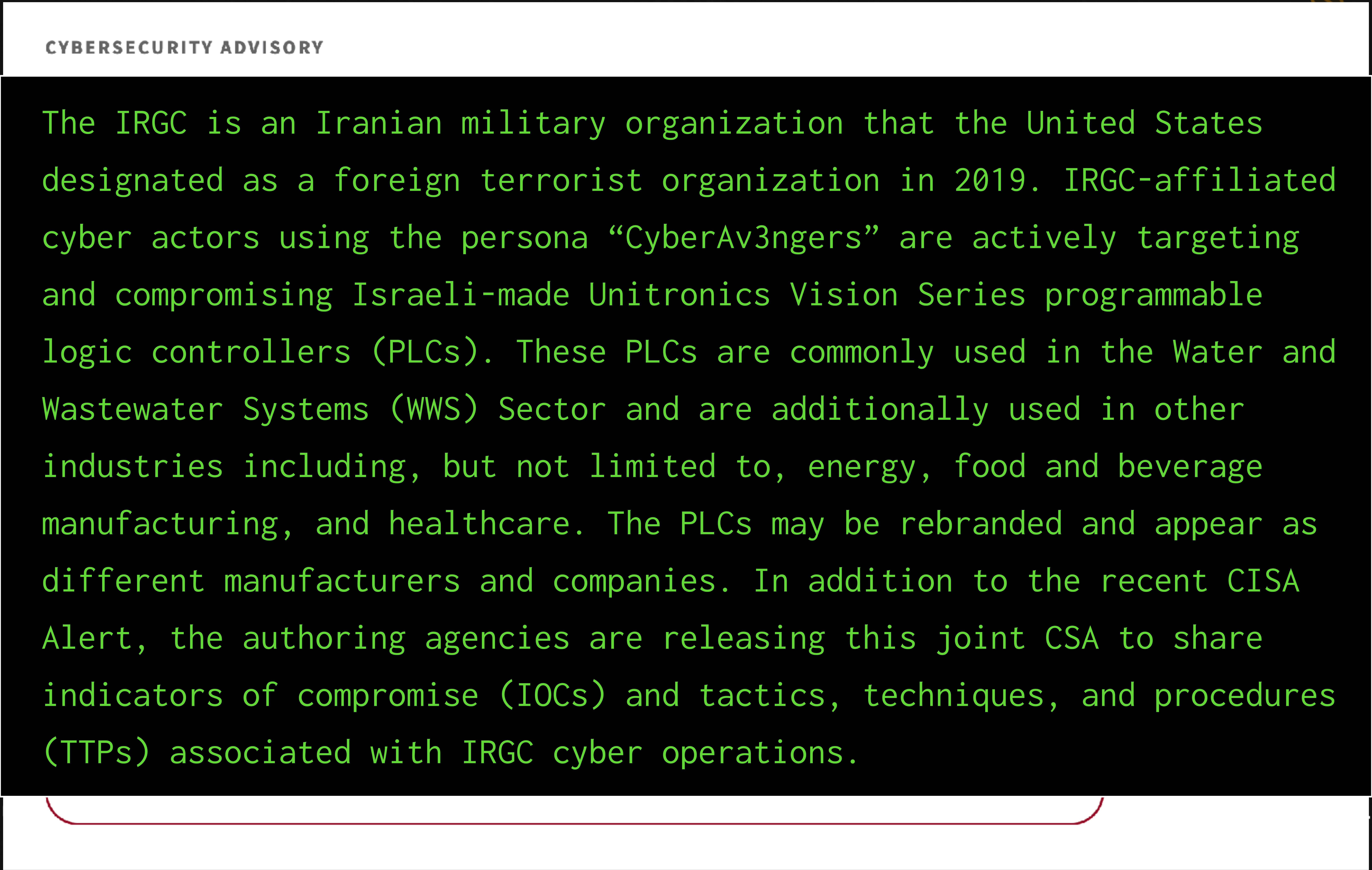
Alert Code: AA23-335A

RELATED TOPICS: ADVANCED PERSISTENT THREATS AND NATION-STATE ACTORS, CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE, CYBER THREATS AND ADVISORIES

https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a

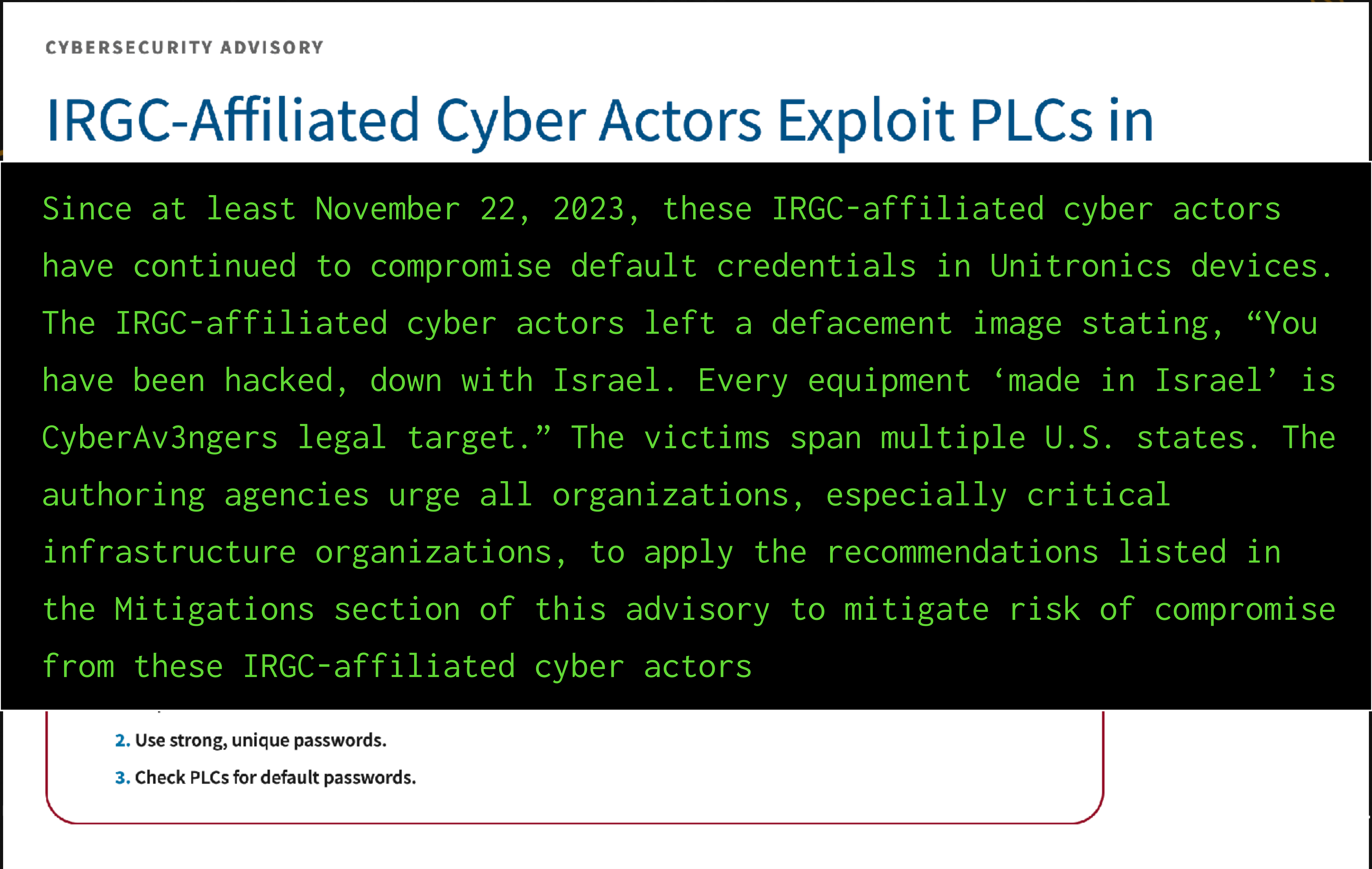
ACTIONS TO TAKE TODAY TO MITIGATE MALICIOUS ACTIVITY:

1. Implement multifactor authentication.
2. Use strong, unique passwords.
3. Check PLCs for default passwords.



CYBERSECURITY ADVISORY

The IRGC is an Iranian military organization that the United States designated as a foreign terrorist organization in 2019. IRGC-affiliated cyber actors using the persona “CyberAv3ngers” are actively targeting and compromising Israeli-made Unitronics Vision Series programmable logic controllers (PLCs). These PLCs are commonly used in the Water and Wastewater Systems (WWS) Sector and are additionally used in other industries including, but not limited to, energy, food and beverage manufacturing, and healthcare. The PLCs may be rebranded and appear as different manufacturers and companies. In addition to the recent CISA Alert, the authoring agencies are releasing this joint CSA to share indicators of compromise (IOCs) and tactics, techniques, and procedures (TTPs) associated with IRGC cyber operations.



CYBERSECURITY ADVISORY

IRGC-Affiliated Cyber Actors Exploit PLCs in

Since at least November 22, 2023, these IRGC-affiliated cyber actors have continued to compromise default credentials in Unitronics devices. The IRGC-affiliated cyber actors left a defacement image stating, “You have been hacked, down with Israel. Every equipment ‘made in Israel’ is CyberAv3ngers legal target.” The victims span multiple U.S. states. The authoring agencies urge all organizations, especially critical infrastructure organizations, to apply the recommendations listed in the Mitigations section of this advisory to mitigate risk of compromise from these IRGC-affiliated cyber actors

2. Use strong, unique passwords.
3. Check PLCs for default passwords.

Storm⚡Watch

GREYNOISE LABS

STORM⚡WATCH