

STORM ⚡ WATCH



Dateline
2024-01-16

S T O R M ⚡ W A T C H

Bangor Daily News

Statewide edition

BDN bangordailynews.com

Saturday/Sunday, January 13-14, 2024 \$3.00

'A perfect storm of everything horrible'



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

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

S T O R M ⚡ W A T C H

GREY OISE

It's all good



ДО ЗАВДАНЬ КІБЕРПОЛІЦІЇ ВХОДЯТЬ:

Реалізація державної політики в сфері протидії кіберзлочинності
Завчасне інформування населення про появу нових кіберзлочинців
Впровадження програмних засобів для систематизації кіберінцидентів
Реагування на запити зарубіжних партнерів, які будуть надходити по каналах Національної Цілодобової мережі контактних пунктів



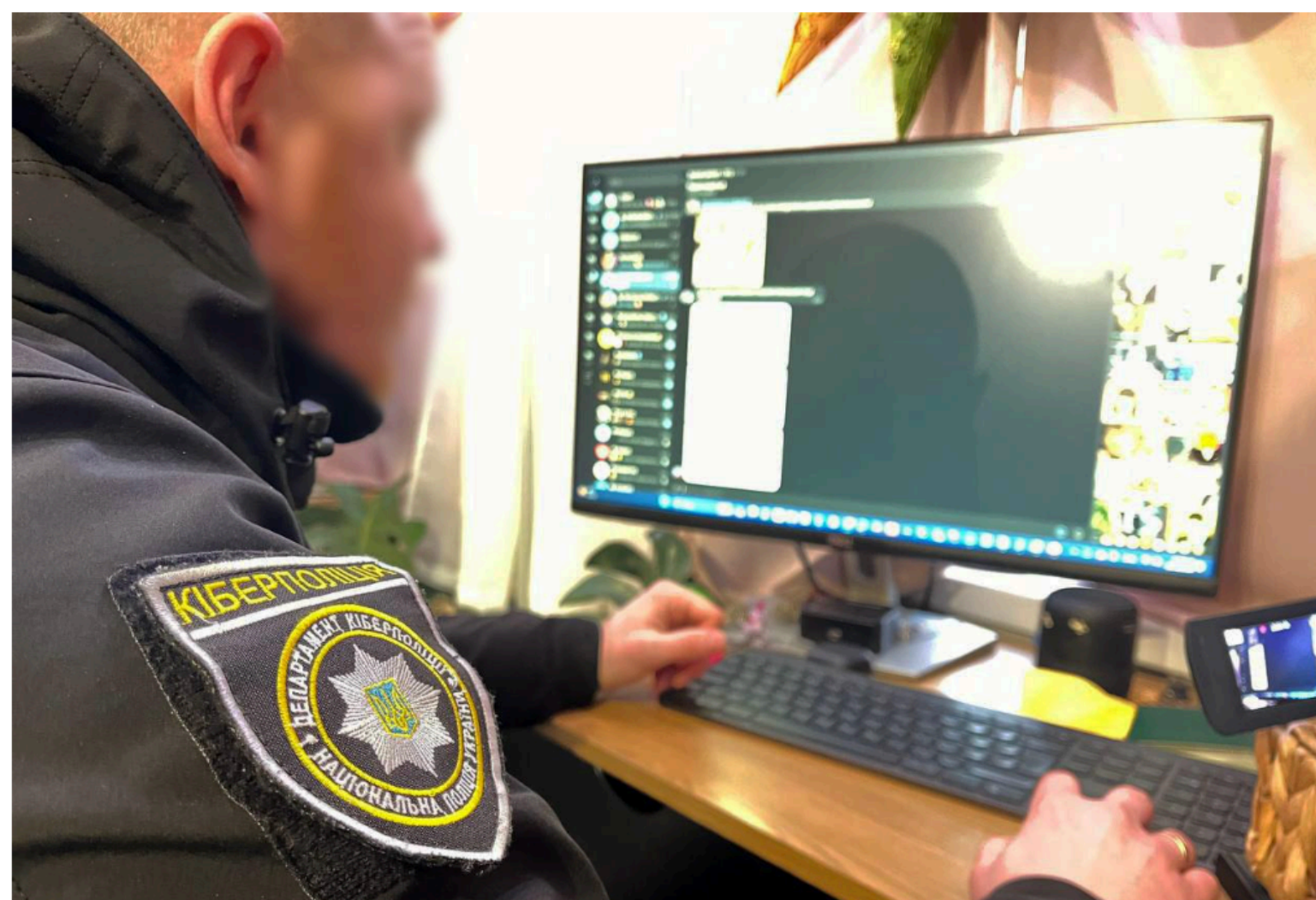
[Зворотний зв'язок](#) [Новини](#) [Рекомендації](#) [No more ransom](#) [Контакти](#) [Вакансії](#) [Запобігання корупції](#) [Очищення влади](#)

Завдав провідній світовій компанії сотні мільйонів збитків: кіберполіція та слідчі Нацполучи викрили хакера

12 січня 2024 р. 15:45

Мешканець Миколаєва інфікував сервера відомої американської компанії вірусом-майнером. У ході міжнародної поліцейської операції правоохоронці провели обшуки та припинили діяльність хакера.

Оперативники Департаменту кіберполіції та слідчі Головного слідчого управління Нацполучи під процесуальним керівництвом Офісу Генерального прокурора спільно з колегами з Європолу (установа правопорядку ЄС з протидії міжнародній організованій злочинності) викрили 29-річного хакера.



Hacker spins up 1 million virtual servers to illegally mine crypto

By **Bill Toulas**

January 13, 2024 10:09 AM 4

A 29-year-old man in Ukraine was arrested this week for using hacked accounts to create 1 million virtual servers used to mine \$2 million in cryptocurrency.

As announced today by **Europol**, the suspect is believed to be the mastermind behind a large-scale cryptojacking scheme that involves hijacking cloud computing resources for crypto-mining.

By using the computing resources of others' servers to mine cryptocurrency, the cybercriminals can profit at the expense of the compromised organizations, whose CPU and GPU performance is degraded by the mining.

For on-premise compromises, the damage extends to having to pay for increased power usage, commonly generated by miners.

A 2022 report from **Sysdig** estimated the damage from cryptojacking to be about \$53 for every \$1 worth of Monero (XMR) the cybercriminals mine on hijacked devices.

Europol says they first learned of the cryptojacking attack in January 2023 from a cloud service provider who was investigating compromised cloud accounts on their platform.

Europol, the Ukrainian police, and the cloud provider worked together to develop operation intelligence that could be used to track down and identify the hacker.

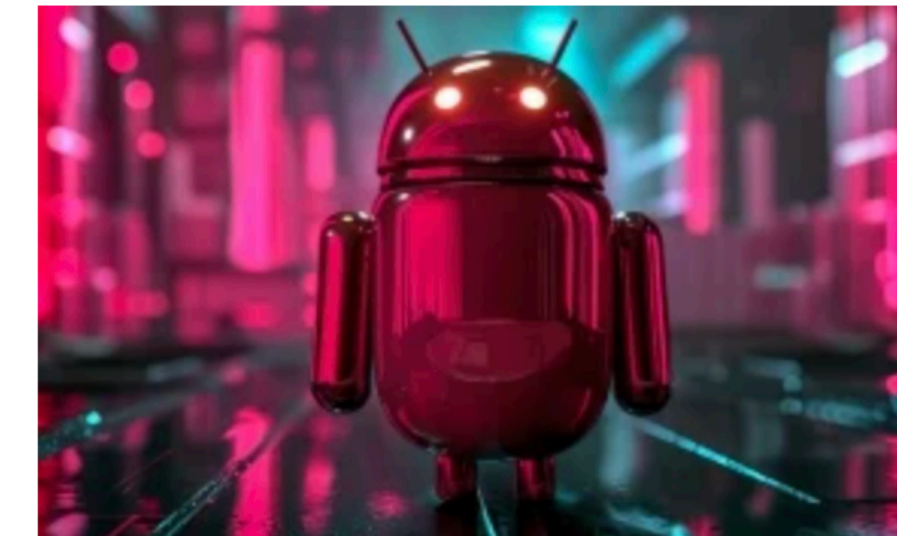
The police say they arrested the hacker on January 9th, when they seized computer equipment, bank and SIM cards, electronic media, and other evidence of illegal activity.



POPULAR STORIES






The new Windows 11 features coming in 2024



GrapheneOS: Frequent Android auto-reboots block firmware exploits

LATEST DOWNLOADS

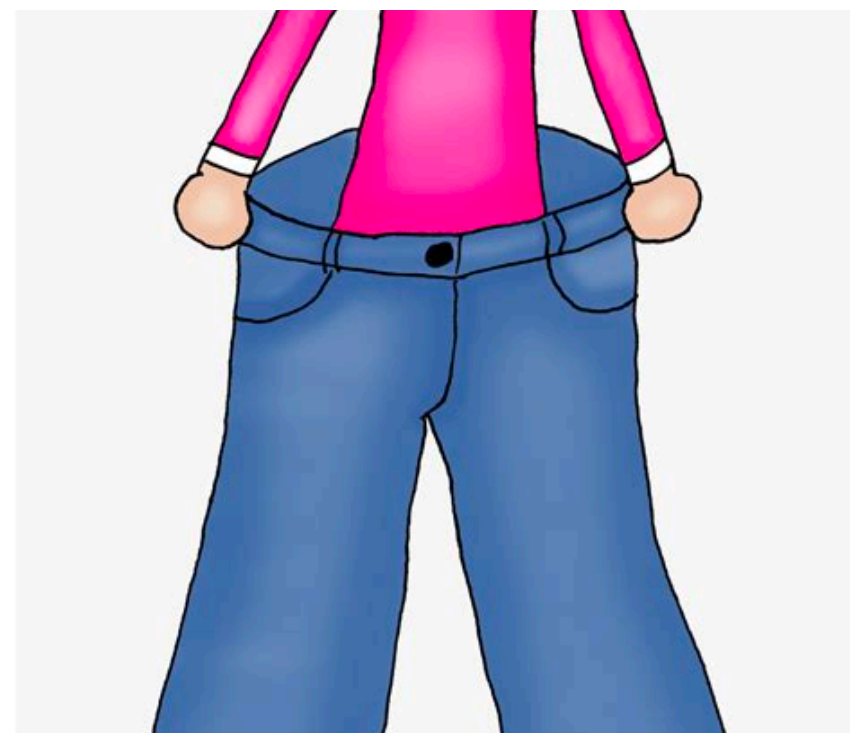
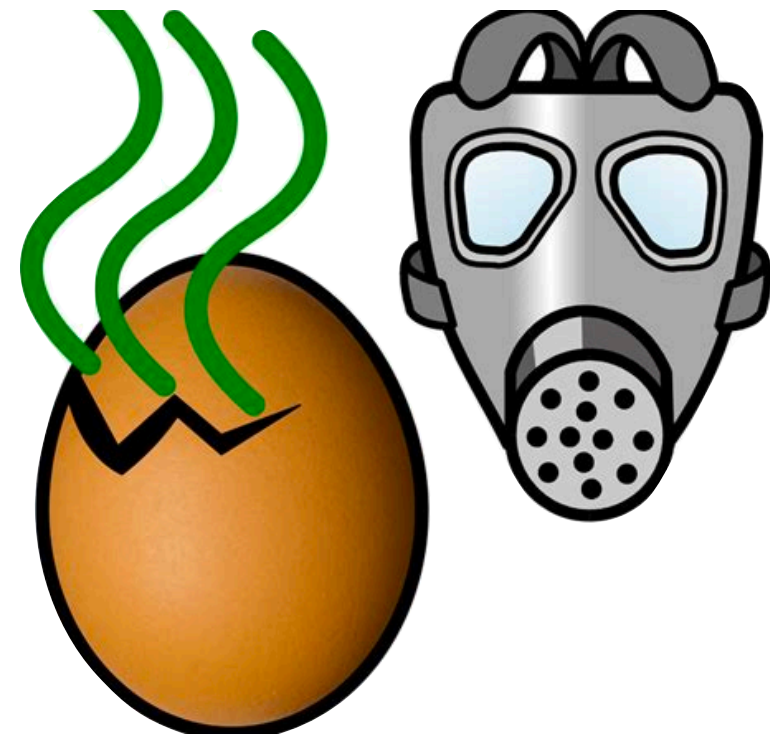
	Malwarebytes Anti-Malware Version: 4.6.8.311	5M+ DOWNLOADS
	Windows Repair (All In One) Version: 4.14.1	2M+ DOWNLOADS
	McAfee Consumer Products Removal tool Version: NA	440,787 DOWNLOADS

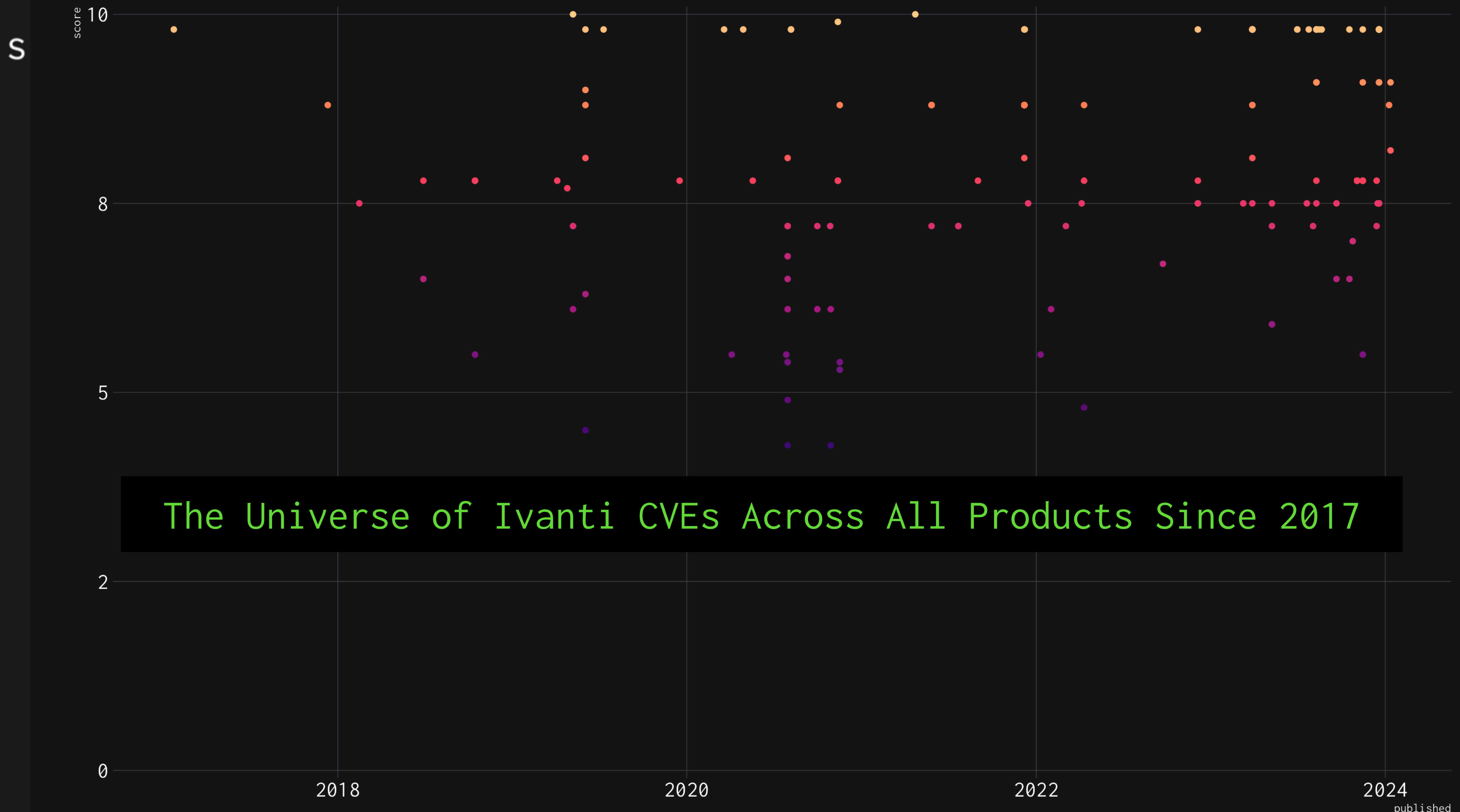


NEWS IN



Select all images containing
things you need to throw out





The Universe of Ivanti CVEs Across All Products Since 2017

S

cn

Cumulative Sum Of Weekly Ivanti CVE Releases Since 2017

150
100
50
0

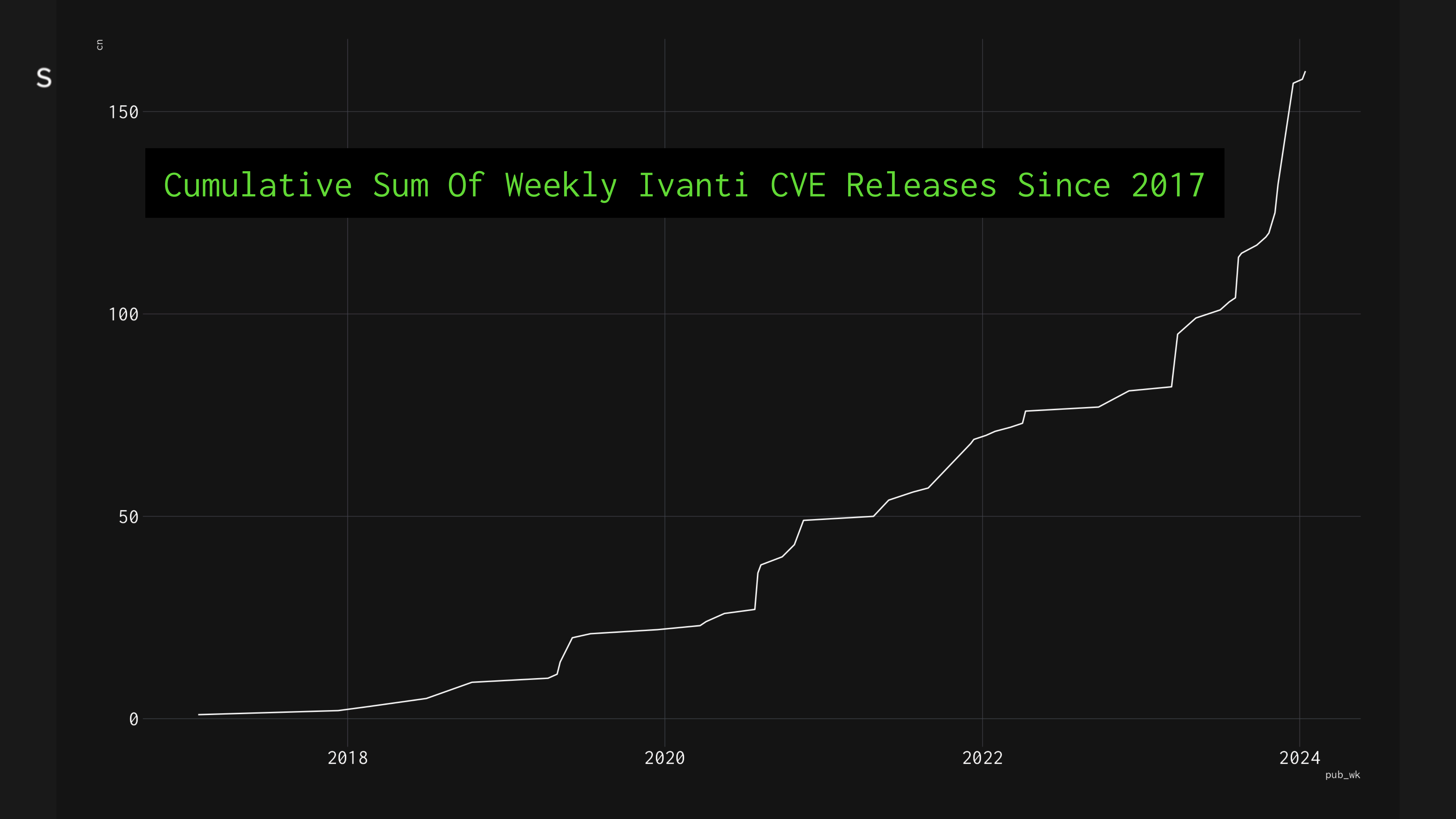
2018

2020

2022

2024

pub_wk



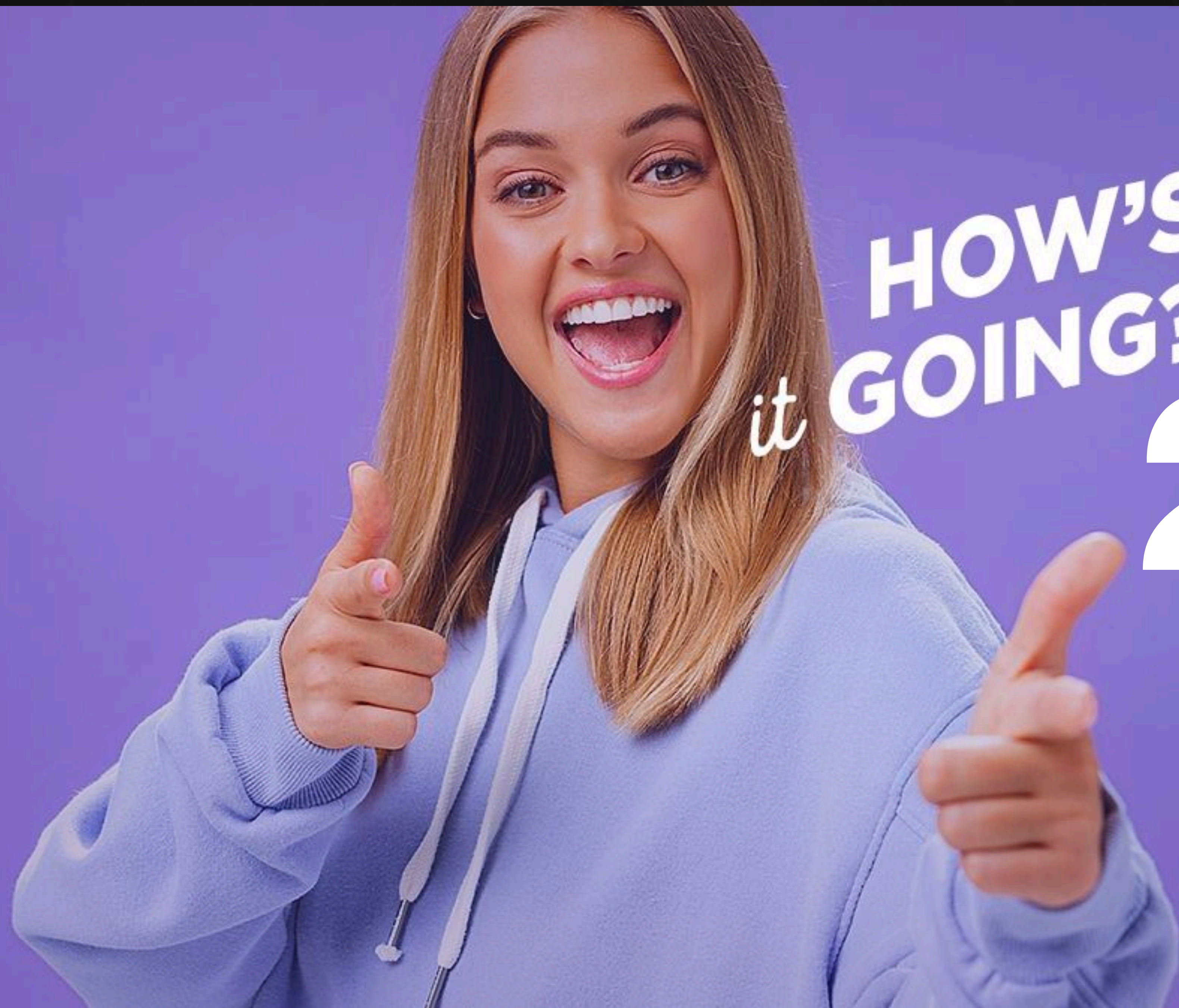
KEV'd Ivanti CVEs

Pulse Connect Secure	7
Connect Secure and Policy Secure	2
Endpoint Manager Mobile (EPMM)	2
MobileIron Multiple Products	1
Pulse Connect Secure and Pulse Policy Secure	1
Sentry	1

Ivanti Connect Secure VPN Exploitation Goes Global

- Volexity identifies over 1,700 compromised Ivanti Connect Secure VPN devices worldwide
- Victims spread across nearly all verticals, including military, defense, government, financial & technology
- Webshell with unique key per victim observed
- Vulnerabilities exploited by multiple threat actors

**NOW BACK TO OUR
REGULARLY SCHEDULED
PROGRAMMING**



HOW'S
GOING?

it

2024



M



https://www.theregister.com/2024/01/09/sec_bitcoin_etf_hacked/
<https://securityaffairs.com/157296/cyber-crime/mandiant-x-account-hacked-2.html>



ARTIFICIAL INTELLIGENCE

NSA official warns of hackers using AI to perfect their English in phishing schemes

NSA Cybersecurity Director Rob Joyce said the language used in hacking and phishing schemes was becoming more sophisticated and convincing.

<https://www.nbcnews.com/tech/security/nsa-hacker-ai-bot-chat-chatgpt-bard-english-google-openai-rcna133086>



Create your free profile or log in to save this article

Jan. 9, 2024, 7:08 PM UTC

By Kevin Collier

Hackers and propagandists are turning to generative artificial intelligence chatbots like [ChatGPT](#) to make their operations seem more convincing to native English speakers, a senior official at the National Security Agency said Tuesday.

Speaking at the International Conference on Cyber Security at Fordham University in New York, NSA Cybersecurity Director Rob Joyce said the spy agency has seen both cybercriminals and hackers who work for foreign intelligence agencies using such chatbots to seem more like native English speakers.

“We already see criminal and nation-state elements utilizing AI,” he



cR0w

@cR0w@infosec.exchange

I can't believe that this is still a thing, but if your risk model is noticeably impacted by the adversarial capability of `_writing an email in the English language_` then I'm pretty sure your threat model is already broken.

<https://infosec.exchange/@cR0w/111732515111789725>

Stuxnet: The malware that cost a billion dollars to develop?

Media report claims that Dutch man played key role in attack on Iranian nuclear facility.



Graham Cluley @ 2:47 pm, January 8, 2024

@gcluley@mastodon.green

@gcluley



<https://grahamcluley.com/stuxnet-the-malware-that-cost-a-billion-dollars/>

A report from the Netherlands claims that a Dutch man played a key role in the notorious Stuxnet worm attack against an Iranian nuclear facility, which then accidentally escaped into the wider world.

Law Firm Orrick Reveals Extensive Data Breach, Over Half a Million Affected

Global law firm Orrick, Herrington & Sutcliffe disclosed a data breach that affects a roughly 600,000 individuals.



By [Ionut Arghire](#)
January 5, 2024



Orrick, Herrington & Sutcliffe, a law firm that specializes in cyberattacks, last week disclosed that more than 600,000 individuals were impacted by a data breach that happened in early 2023.

Between February 28 and March 13, 2023, the company said attackers had unauthorized access to a portion of its network, including a file share storing files related to Orrick's clients.

"Orrick has identified no evidence of further unauthorized activity since detecting the security incident on March 13," the company said.

Orrick said its analysis of the exposed files determined that personal information pertaining to the customers of its clients was compromised in the attack, and that notification letters were sent to the impacted individuals starting June 2023.

Some of these individuals, the law firm said, were customers of companies that suffered data breaches. Their information was shared with Orrick to facilitate the

TRENDING

- 1 [GitLab Patches Critical Password Reset Vulnerability](#)
- 2 [New Class of CI/CD Attacks Could Have Led to PyTorch Supply Chain Compromise](#)
- 3 [Mr. Cooper Data Breach Impacts 14.7 Million Individuals](#)
- 4 [Russian Hackers Likely Not Involved in Attacks on Denmark's Critical Infrastructure](#)
- 5 [CISA Urges Patching of Exploited SharePoint Server Vulnerability](#)
- 6 [Volexity Catches Chinese Hackers Exploiting Ivanti VPN Zero-Days](#)



Between February 28 and March 13, 2023, the company said attackers had unauthorized access to a portion of its network, including a file share storing files related to Orrick's clients.

"Orrick has identified no evidence of further unauthorized activity since detecting the security incident on March 13," the company said.

Orrick said its analysis of the exposed files determined that personal information pertaining to the customers of its clients was compromised in the attack, and that notification letters were sent to the impacted individuals starting June 2023.

Some of these individuals, the law firm said, were customers of companies that suffered data breaches. Their information was shared with Orrick to facilitate the provision of legal counseling to those companies.

S T O R M ⚡ W A T C H

TOOL TIME





Casualtek / Cyberwatch



<> Code

Issues 3

Pull requests

Actions

Projects

Security



<https://github.com/Casualtek/Cyberwatch>

Building a consolidated RSS feed for articles about cyberattacks

Unlicense license

39 stars

11 forks

4 watching

1 Branch

0 Tags

Activity

Public repository

main



Go to file

+

<> Code



Casualtek and github-actions[bot] Apply automatic changes

38 minutes ago



.github/workflows

Create flux_rss.yml

12 hours ago

Cyberwatch is a project that aims to build a consolidated RSS feed for articles about cyberattacks. The feed consolidates information from various sources, making it easier for defenders to stay updated on the latest cybersecurity news and trends.

Now, what's in the individual records? You'll find there the name of the victim, the country, the date, a short description of the situation, and a link to the original news story ... extracted from the original news story with the help of ChatGPT (the output is checked manually).

S T O R M ⚡ W A T C H



Shameless Self-Promotion

BLOGS

CVE-2024-21591 – Juniper J-Web OOB Write vulnerability

<https://censys.com/cve-2024-21591-juniper-j-web-oob-write-vulnerability/>



JANUARY 12, 2024

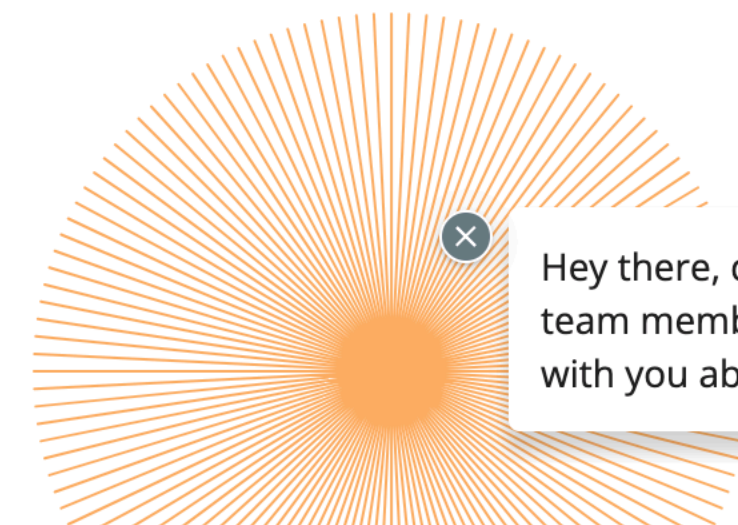
Tags:



Summary:

- Juniper Networks recently patched a critical pre-authentication Remote Code Execution (RCE) vulnerability in the J-Web configuration interface across all versions of Junos OS on

ABOUT THE AUTHOR



Hey there, down here! One of our team members wants to chat with you about your business! 😊



Fuzzy Matching to Find Phish-y Domains: A Censys Lunch and Learn

https://go.censys.com/JanuaryLunchandLearn_Registration.html

January 18, 2024 at 1:00pm ET

In this exclusive Censys Lunch and Learn webinar we will unravel the complexities of the vast digital landscape. In an era where the internet is both a treasure trove and a potential minefield, distinguishing between legitimate and malicious web pages has never been more challenging. The prevalence of technology has empowered cyber adversaries to swiftly deploy deceptive websites, posing a significant threat to organizations. Navigating this perilous terrain demands a proactive approach in identifying fake websites as they emerge and safeguarding your employees from potential cyber threats.

Join us as we delve into the intricacies of fuzzy matching where knowledge becomes your greatest defense. Learn how leveraging BigQuery's user-defined functions can empower you to identify phishing domains by finding websites that cunningly resemble your own. We will demonstrate the effectiveness of combining the capabilities of BigQuery with Censys' data, providing you with a powerful toolkit to proactively protect your organization. Through insightful queries and data analysis, discover how to stay one step ahead in the relentless battle against cyber threats. Don't miss this opportunity to fortify your defenses and secure your organization's digital presence!

Presenters:

Register Now

First Name:

Last Name:

Email:

Company:

Country:

Phone Number:

<https://www.greynoise.io/events/webinar-series-greynoise-tags-deep-dive>

GREYNOISE

WEBINAR SERIES

GreyNoise Tags Deep Dive

101, 201, 301

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





D E C O D I N G
2 0 2 3

A GREYNOISE
RETROSPECTIVE ON
INTERNET EXPLOITATION

<https://www.greynoise.io/resources/2023-greynoise-retrospective-internet-exploitation-report>

S T O R M ⚡ W A T C H

- **Critical 2023 Exploits:** Explore detailed information on three notable vulnerabilities: Progress MOVEit Transfer, Citrix NetScaler ADC/NetScaler Gateway, and PaperCut MF/NG, understanding their impact, exploitation methods, and affected sectors.
- **Key Statistics:** Discover key statistics on GreyNoise tags, covering 290 new tags and 242 Common Vulnerabilities and Exposures (CVEs) in 2023, highlighting their proactive role in identifying and responding to internet probes and attacks.
- **Active Defense and Incident Response:** Understand how GreyNoise's tag taxonomies, enriched with modern defender frameworks like MITRE ATT&CK, CAPEC, and CWE, empower organizations to respond proactively to emerging threats and exploits.

S T O R M ⚡ W A T C H

- 🏷️ Jboss Application Server Check (CVE-2017-12149)
- 🏷️ Ivanti Connect Secure (ICS) Scanner
- 🏷️ GitLab Account Takeover Attempt (CVE-2023-7028)
- 🏷️ ThinkPHP RCE Attempt

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

24 HOURS

10 DAYS

• 30 DAYS

December 17, 2023 - January 15, 2024 (UTC)

Unique IPs Observed

Last 30 days

GREYNOISE TRENDS

THINKPHP RCE ATTEMPT

TAG INTENT

Malicious

TAG CATEGORY

Activity

IP addresses with this tag have been observed attempting to exploit ThinkPHP to achieve remote code execution (RCE).

UNIQUE IPS



24 HOURS

10 DAYS

• 30 DAYS

December 17, 2023 - January 15, 2024 (UTC)

Unique IPs Observed

Last 30 days



Chart	Tag	Category
	Apache ActiveMQ RCE Attempt	trending
	Citrix ADC Netscaler CVE-2023-4966 Information Disclosure Attempt	trending
	D-Link Hardcoded Telnet Attempt	trending
	HTTP PUT Uploader	trending
	Looks Like RDP Worm	trending
	Mailbox Bruteforcer	trending
	QNX Qconn Exploit	trending
	RouterOS Bruteforcer	trending
	ThinkPHP RCE Attempt	trending
	Zyxel USG SSH Backdoor Attempt	trending
	Drupal CVE-2018-7600 Worm	anomalies
	Fortinet SSL VPN Bruteforcer	anomalies
	Jboss Application Server CVE-2017-12149 Check	anomalies
	Mikrotik CVE-2018-14847 Worm	anomalies
	TP-Link Authenticated RCE Attempt	anomalies
	Zyxel Router Worm	anomalies
	Generic IoT Brute Force Attempt	active
	Huawei HG532 UPnP CVE-2017-17215 Worm	active
	Looks Like Conficker	active
	Mirai	active
	MSSQL Bruteforcer	active
	Open Proxy Scanner	active
	SSH Bruteforcer	active
	SSH Worm	active
	Telnet Bruteforcer	active
	X Server Connection Attempt	active

WE NEED

TO TALK

ABOUT

KEY



It Has Been

6

Days Since The
Last KEV Release

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

CVE-2023-29357: Microsoft SharePoint Server Privilege Escalation

CVE-2023-46805: Ivanti Connect Secure & Policy Secure Authentication Bypass

CVE-2024-21887: Ivanti Connect Secure & Policy Secure Command Injection

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