

STORMWATCH

CYBERSECURITY NEWS

Dateline: 2024-06-04



LIKE



SUBSCRIBE

S T O R M ⚡ W A T C H



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://StormWatch.ing>



LEAVE A
COMMENT



SHARE

S T O R M ⚡ W A T C H

CYBERSECURITY NEWS

CYBERSIDE CHAT



How would you know if someone stole your mind?

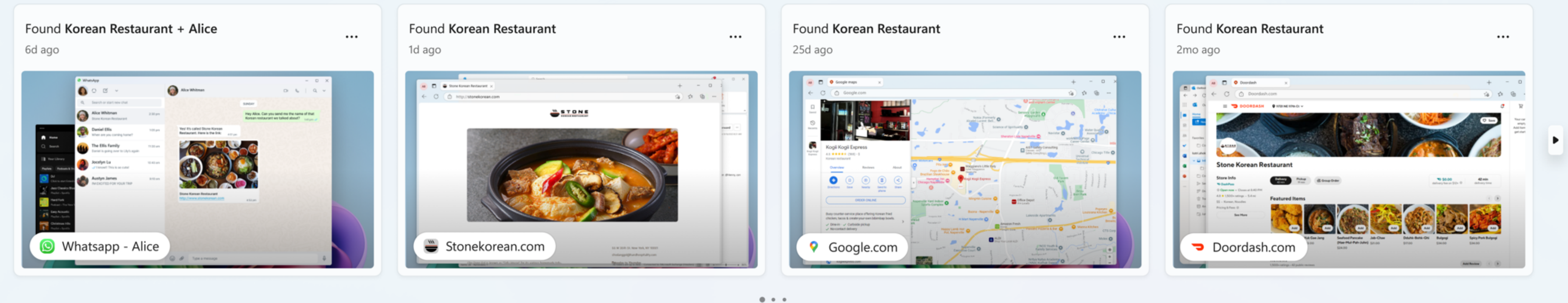
THINK
BETTER

<https://support.microsoft.com/en-us/windows/retrace-your-steps-with-recall-aa03f8a0-a78b-4b3e-b0a1-2eb8ac48701c>

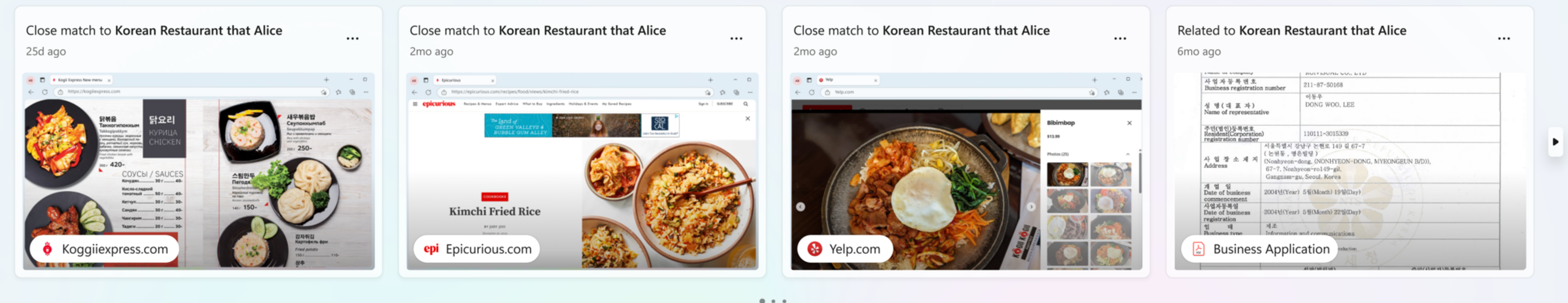
Results

[All](#)
[Word](#)
[Edge](#)
[PowerPoint](#)
[Outlook](#)
[View File Explorer results](#)

Text matches >



Visual matches >



Search across time to find the content you need. Then, re-engage with it. With Recall, you have an explorable timeline of your PC's past. Just describe how you remember it and Recall will retrieve the moment you saw it. Any photo, link, or message can be a fresh point to continue from. As you use your PC, Recall takes snapshots of your screen. Snapshots are taken every five seconds while content on the screen is different from the previous snapshot. Your snapshots are then locally stored and locally analyzed on your PC. Recall's analysis allows you to search for content, including both images and text, using natural language. Trying to remember the name of the Korean restaurant your friend Alice mentioned? Just ask Recall and it retrieves both text and visual matches for your search, automatically sorted by how closely the results match your search. Recall can even take you back to the exact location of the item you saw.

- A Copilot+ PC
- 16 GB RAM
- 8 logical processors
- 256 GB storage capacity
 - To enable Recall, you'll need at least 50 GB of storage space free
 - Saving screenshots automatically pauses once the device has less than 25 GB of storage space

<https://doublepulsar.com/recall-stealing-everything-youve-ever-typed-or-viewed-on-your-own-windows-pc-is-now-possible-da3e12e9465e>

Stealing everything you've ever typed or viewed on your own Windows PC is now possible with two lines of code — inside the Copilot+ Recall disaster.



Kevin Beaumont · [Follow](#)

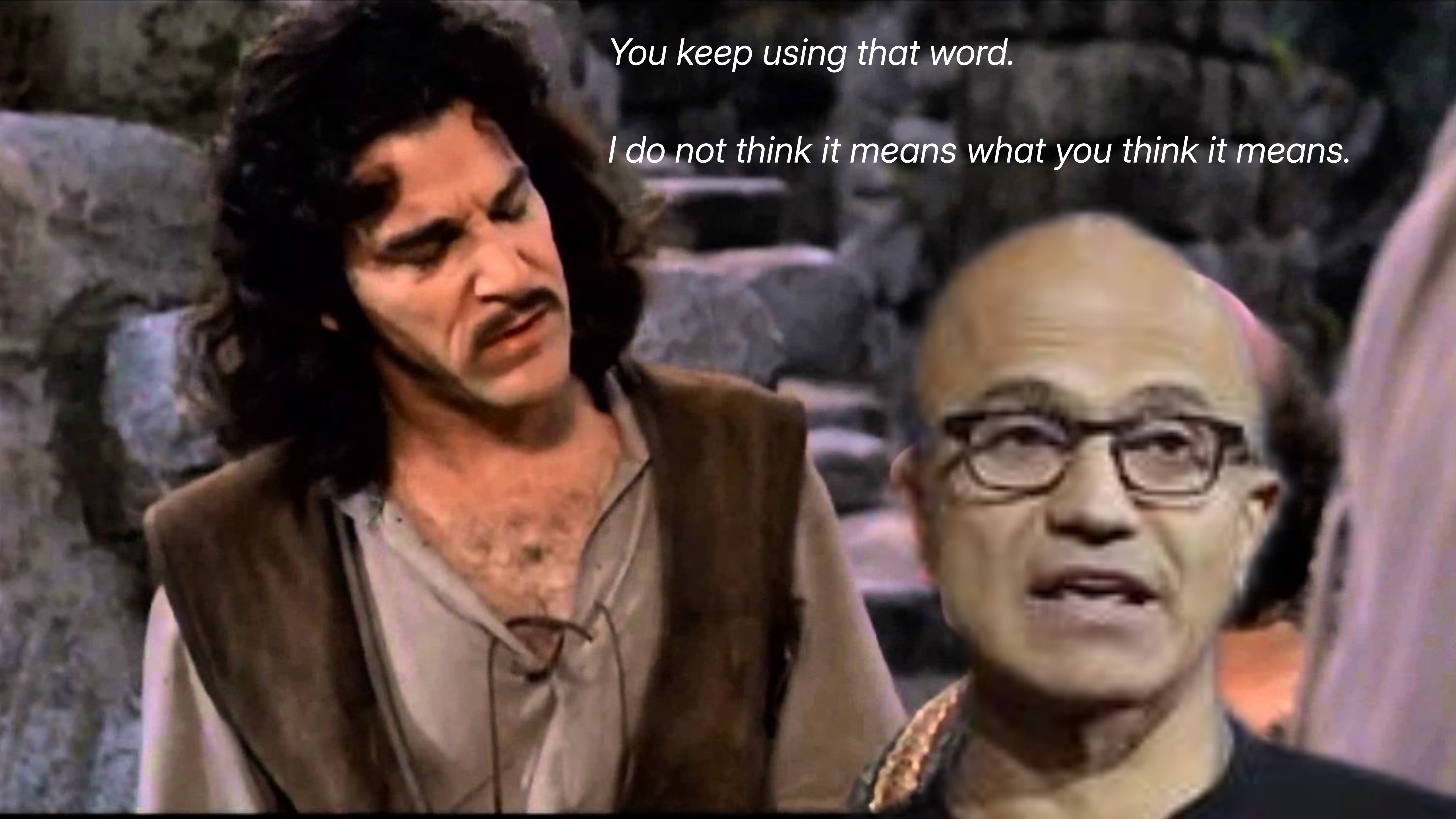
Published in DoublePulsar · 9 min read

%APPDATA%

*If you're faced with the
tradeoff between **security**
and another priority, your
answer is clear: Do **security**.*

— May 3, 2024





You keep using that word.

I do not think it means what you think it means.

A still from the movie The Lord of the Rings: The Two Towers showing Gollum crouching in a cave. He has a determined and slightly angry expression on his face, with wide eyes and a small, open mouth showing his teeth. He is wearing a simple, dark, loincloth-like garment. The background is a dark, rocky cave with some moss and a small opening in the distance.

They stole it from us!



Introducing Limitless

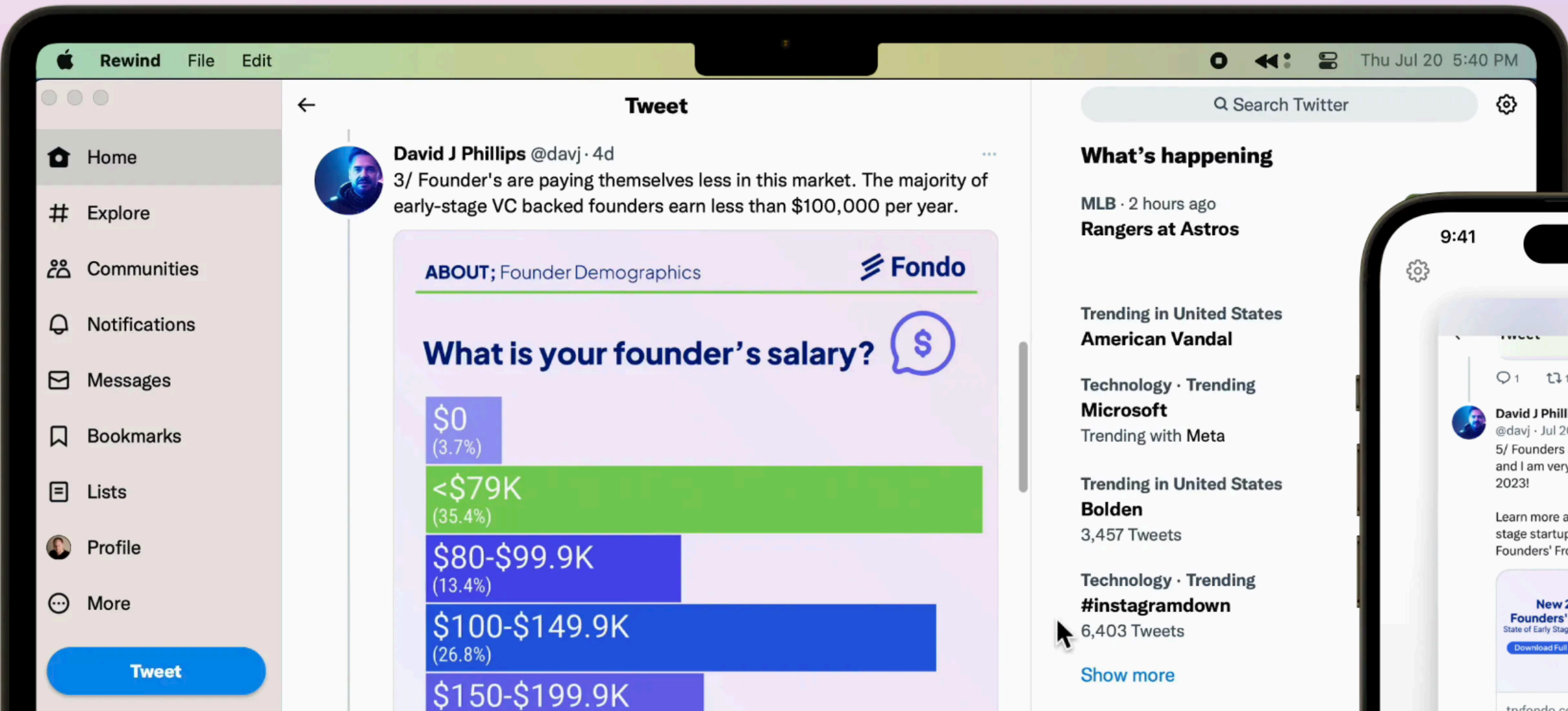
A web app, Mac app, Windows app, and wearable.



<https://www.rewind.ai/>

Your AI assistant that has all the context

Rewind is a personalized AI powered by everything
you've seen, said, or heard. Your colleagues will
wonder how you do it all.



PRODUCT HUNT

#1 Product of the Week

“ I’m very optimistic about Rewind’s approach to personalized AI.



Sam Altman CEO, OpenAI

“ Rewind is a great example of how AI can augment human intelligence.



Marc Andreessen Cofounder, a16z

S T O R M ⚡ W A T C H

CYBERSECURITY NEWS

CYBER SPOTLIGHT





I'm having a moment here.



- 🎃 Over 600,000 small office/home office (SOHO) routers belonging to a single internet service provider (ISP) were taken offline in a destructive event between October 25-27, 2024.
- 🎃 The routers were rendered permanently inoperable, requiring hardware replacement.
- 🎃 Public scan data confirmed a 49% sudden drop in modems from the impacted ISP's network during this period.

- 🎃 The "Chalubo" remote access trojan (RAT) was identified as the primary malware payload responsible for the attack.
- 🎃 Chalubo employed techniques to obfuscate its activity, like running in-memory, using random process names, and encrypting communications.
- 🎃 While used in this destructive attack, Chalubo was not specifically written for destructive purposes based on its widespread activity observed by Lumen in late 2023 and early 2024

- 🎃 The attack involved a multi-stage infection mechanism that installed the Chalubo RAT botnet targeting SOHO gateways and IoT devices globally.
- 🎃 Lumen's Black Lotus Labs has shared indicators of compromise (IoCs) related to the Chalubo malware family to help detect and prevent such attacks.



STORM ⚡ WATCH

CYBERSECURITY NEWS

TOOL TIME























<https://cybersectools.com/>

The Largest Curated Directory of Cybersecurity Tools and Resources

2631 tools and resources curated by Nikoloz. Follow on **X** and **LinkedIn**.

Tools Tags Searching for tools

-  AI Security
-  Application Security
-  Blogs and News
-  Cloud and Container Security
-  Data Protection and Cryptography
-  Digital Forensics
-  Endpoint Security
-  Governance, Risk, and Compliance
-  Guides and eBooks
-  Honeypots
-  Identity, Access, and Credential Management
-  Malware Analysis
-  Network Security
-  Offensive Security
-  Security Operations
-  SIEM and Log Management
-  Specialized Security
-  Threat Management
-  Training and Resources
-  Vulnerability Management
-  Miscellaneous

FEATURED



Mandos Brief Newsletter

Stay ahead in cybersecurity. Get the week's top cybersecurity news and insights in 8 minutes or less.



Mandos Way

Mandos Way provides strategic cybersecurity insights, particularly in AI implementation and leadership.



Feature Your Cybersecurity Product

Showcase your innovative cybersecurity solution to our dedicated audience of security professionals. [Reach out to explore collaboration opportunities!](#)

Home > Tools > Censys



Censys

Report Issue

Visit Website

Censys is a search engine for the Internet of Things (IoT) that provides real-time information about devices connected to the internet. It allows users to search for specific devices, such as webcams, routers, and servers, and provides information about their IP addresses, open ports, and other details.

Vulnerability Management Free iot search-engine device-discovery port-scanning

ALTERNATIVES



CakeFuzzer

Automated vulnerability discovery tool for Cake PHP framework with limited false positives.



Sysreptor

A fully customizable, offensive security reporting solution for pentesters, red teamers, and other security professionals.

Acunetix Web

◆ Vulnerability Scanner Demonstration Site

A demonstration site for the Acunetix Web Vulnerability Scanner, intentionally vulnerable to various web-based attacks.

Vulnerability Management Free

SHAMELESS SELF-PROMOTION



BLOGS

<https://censys.com/cve-2024-24919/>

May 31, 2024: Arbitrary File Read in Check Point VPN Gateways [CVE-2024-24919]

S T O R M ⚡ W A T C H

CYBERSECURITY NEWS

TAG ROUND-UP



Check Point Quantum Gateway CVE-2024-24919 Information
Disclosure Attempt

Linksys EA7500 CVE-2023-46012 Buffer Overflow RCE Attempt

Zyxel NAS326 CVE-2023-4473 Auth Bypass Attempt

Zyxel NAS326 CVE-2023-4474 Shell Injection Attempt

INTENTION

CATEGORY

CVES

MALICIOUS

Activity

No associated CVEs

IP addresses with this tag have exhibited behavior that indicates they are infected with Dridex banking malware.

24 HOURS

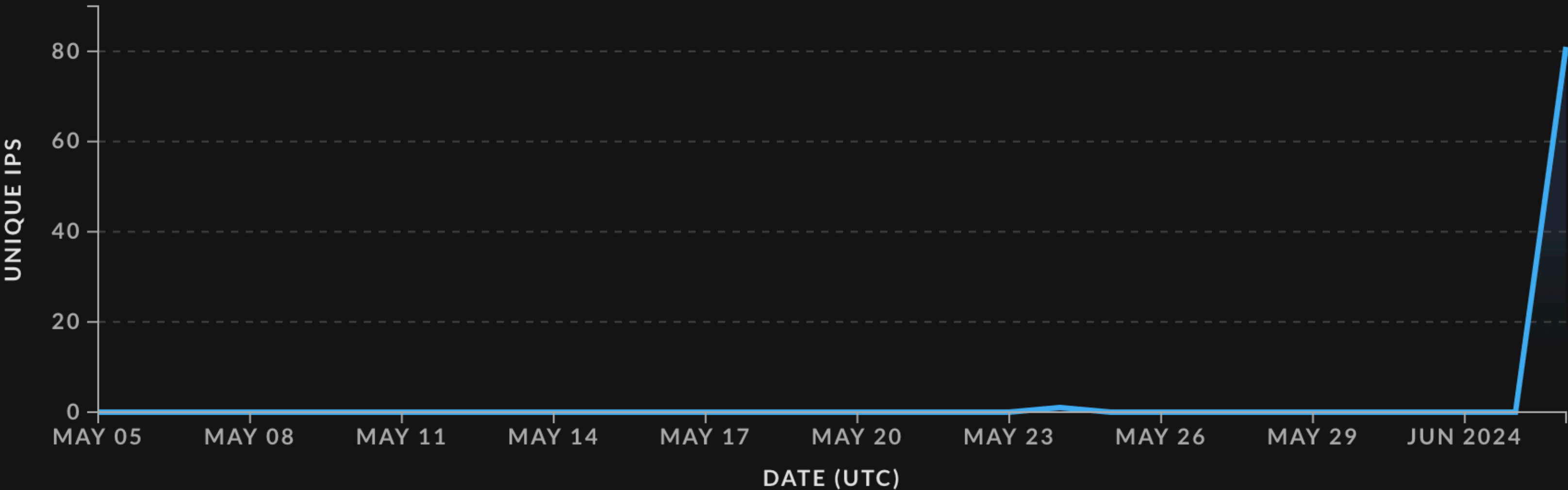
10 DAYS

30 DAYS

May 05, 2024 - June 03, 2024 (UTC)

Unique IPs Observed

Last 30 days



Timeline

Sequence of recorded events

> GreyNoise Created Tag

2020-04-07 00:00 UTC



INTENTION

CATEGORY

CVES

MALICIOUS

Worm

No associated CVEs

IP addresses with this tag exhibit behavior that indicates they are infected with the banking malware TrickBot.

24 HOURS

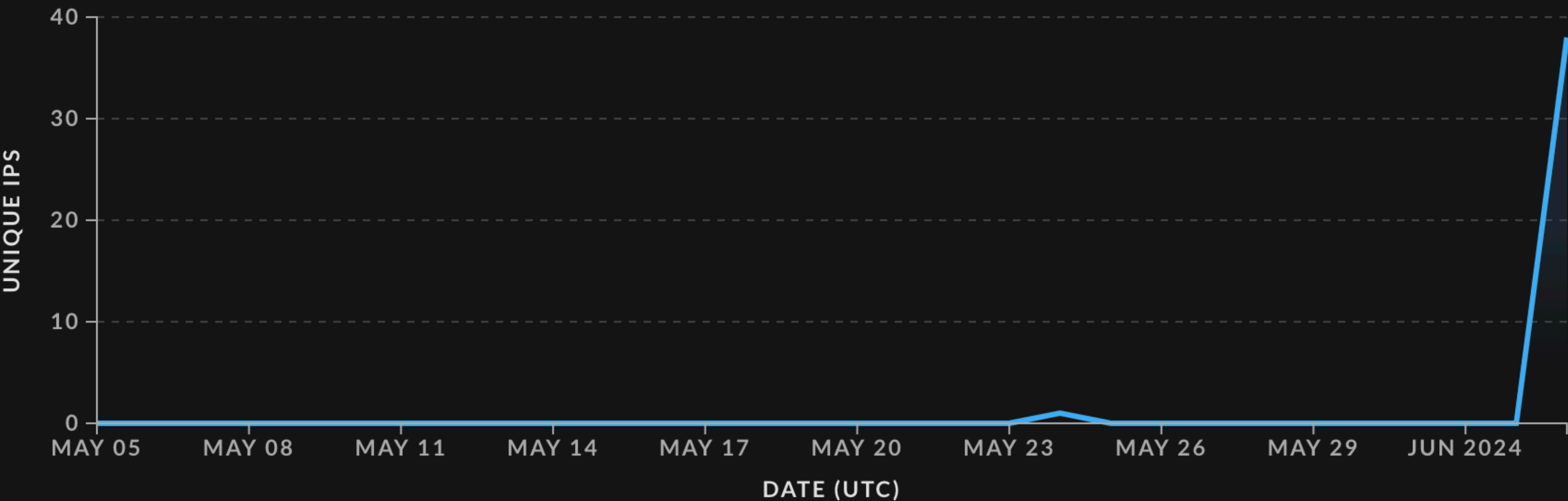
10 DAYS

30 DAYS

May 05, 2024 - June 03, 2024 (UTC)

Unique IPs Observed

Last 30 days



Timeline

Sequence of recorded events

> + GreyNoise Created Tag

2020-04-07 00:00 UTC

CHECK POINT QUANTUM GATEWAY CVE-2024-24919 INFORMATION DISCLOSURE ATTEMPT

INTENTION
MALICIOUS

CATEGORY
Activity

CVES
CVE-2024-24919

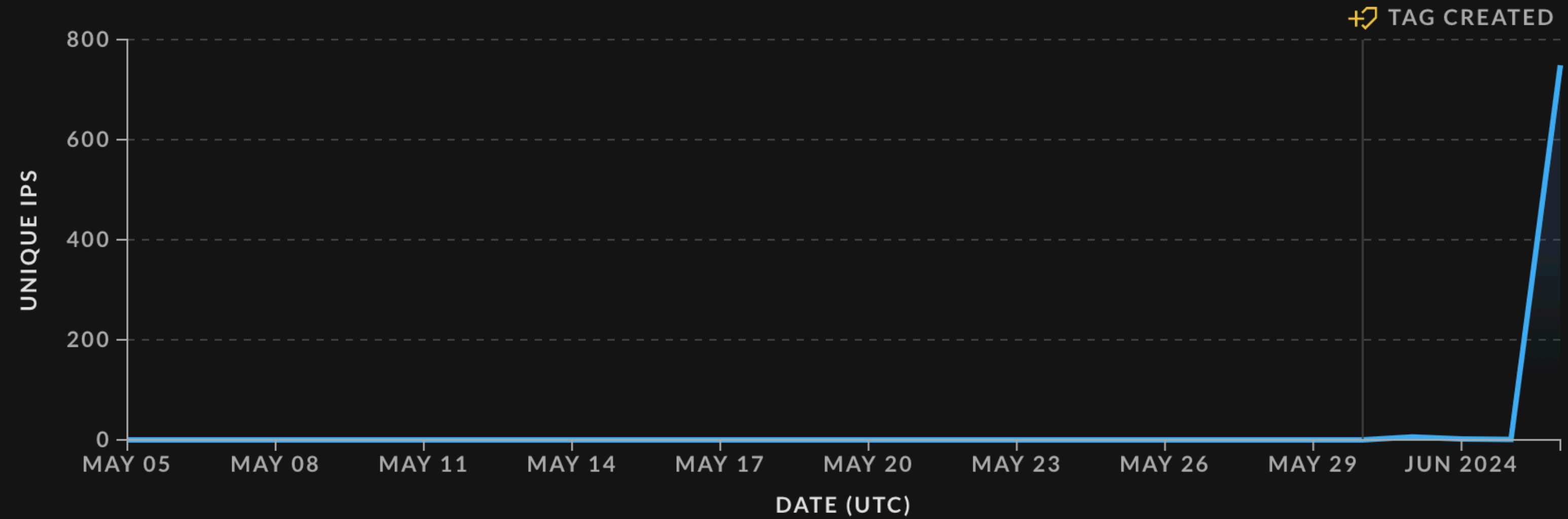
IP addresses with this tag have been observed attempting to exploit CVE-2024-24919, an unauthenticated information disclosure vulnerability in multiple Check Point products.

24 HOURS 10 DAYS 30 DAYS

May 05, 2024 - June 03, 2024 (UTC)

Unique IPs Observed

Last 30 days



<https://viz.greynoise.io/tags/check-point-quantum-gateway-cve-2024-24919-information-disclosure-attempt?days=30>

Timeline

Sequence of recorded events

- > + GreyNoise Created Tag 2024-05-30 00:00 UTC
- > CVE-2024-24919 Published 2024-05-28 19:15 UTC



**WE NEED
TO TALK
ABOUT
KEY**



S T O R M ⚡ W A T C H

It Has Been 1 Days Since The Last KEV Release

<https://kev.hrbrmstr.app>

CVE-2024-5274:
Google Chromium V8 Type Confusion

CVE-2024-4978:
Justice AV Solutions (JAVS) Viewer Installer Embedded Malicious Code

CVE-2024-1086
Linux Kernel Use-After-Free

CVE-2024-24919
Check Point Quantum Security Gateways Information Disclosure

CVE-2017-3506
Oracle WebLogic Server OS Command Injection