

S T O R M ⚡ W A T C H

GREYNOISE



**Dateline: 2023-09-26**

[Store](#)[Mac](#)[iPad](#)[iPhone](#)[Watch](#)[AirPods](#)[TV & Home](#)[Entertainment](#)[Accessories](#)[Support](#)

## Apple Podcasts Preview

<https://stormwatch.libsyn.com/>



16 episodes

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 boB Rudis, Kimber Duke, Glenn Thorpe, and other guests discussing various cybersecurity topics and internet exploitation trends. The goal of the show is to provide insights and updates on cybersecurity issues, helping viewers stay informed about the latest threats and developments in the field.

## Storm ⚡ Watch by GreyNoise Intelligence

GreyNoise Intelligence

Technology

★★★★★ 5.0 • 3 Ratings

[Listen on Apple Podcasts ↗](#)



SEP 19, 2023

### Storm ⚡ Watch - 9/19/23



In this episode of Storm Watch, the hosts discuss a recent noise storm, which is an event where a capable attacker group sends out massive amounts of TCP packets without three-way handshakes. These noise storms can cause problems for data processing pipelines and are sometimes used to...

[▶ PLAY](#) 57 min

SEP 12, 2023

### Storm ⚡ Watch - 9/12/23



In the Storm Watch podcast episode from September 12, 2023, the host discusses the value of private group chats and the resurgence of IRC. They mention the creation of a new Discord server for their community and express concerns about Salesforce's ownership of Slack. The conversation the...

[▶ PLAY](#) 47 min

SEP 5, 2023

### Storm ⚡ Watch - 9/5/23



In this episode of Storm Watch, the hosts discuss various topics related to cybersecurity and the internet. They begin by comparing the unpredictability of weather patterns to the challenges of predicting internet activity and cyber threats. The hosts suggest that perhaps they should consider...

<https://www.labscon.io/>

# LABSCON 2023

Security Research in Real Time | September 20-23, 2023

LABScon is an intimate event for the world's top cybersecurity minds to gather, share cutting-edge research, and push the envelope of threat landscape understanding.

Presented by SentinelOne.

REQUEST AN INVITE >



Presented by:



<https://www.cyberkendra.com/2023/09/moveit-transfersql-injection.html>



**⚠ WARNING**

**SQLi**

Progress  
MOVEit

**MOVEit**  
New SQL  
Injection

CVE-2023-40043  
CVE-2023-42660



CVE-2023-42660 • CVSS: 8.8  
MOVEit Transfer Machine  
Interface (Auth'd) SQL  
Injection

CVE-2023-40043 • CVSS: 7.2  
MOVEit Transfer  
\*\*SysAdmin\*\* SQL Injection

<https://community.progress.com/s/article/MOVEit-Transfer-Service-Pack-September-2023>

# Hackers who breached casino giants MGM, Caesars also hit 3 other firms, Okta says

By Zeba Siddiqui

September 19, 2023 4:17 PM EDT · Updated 5 days ago

<https://www.reuters.com/technology/hackers-who-breached-casino-giants-mgm-caesars-also-hit-3-other-firms-okta-says-2023-09-19/>

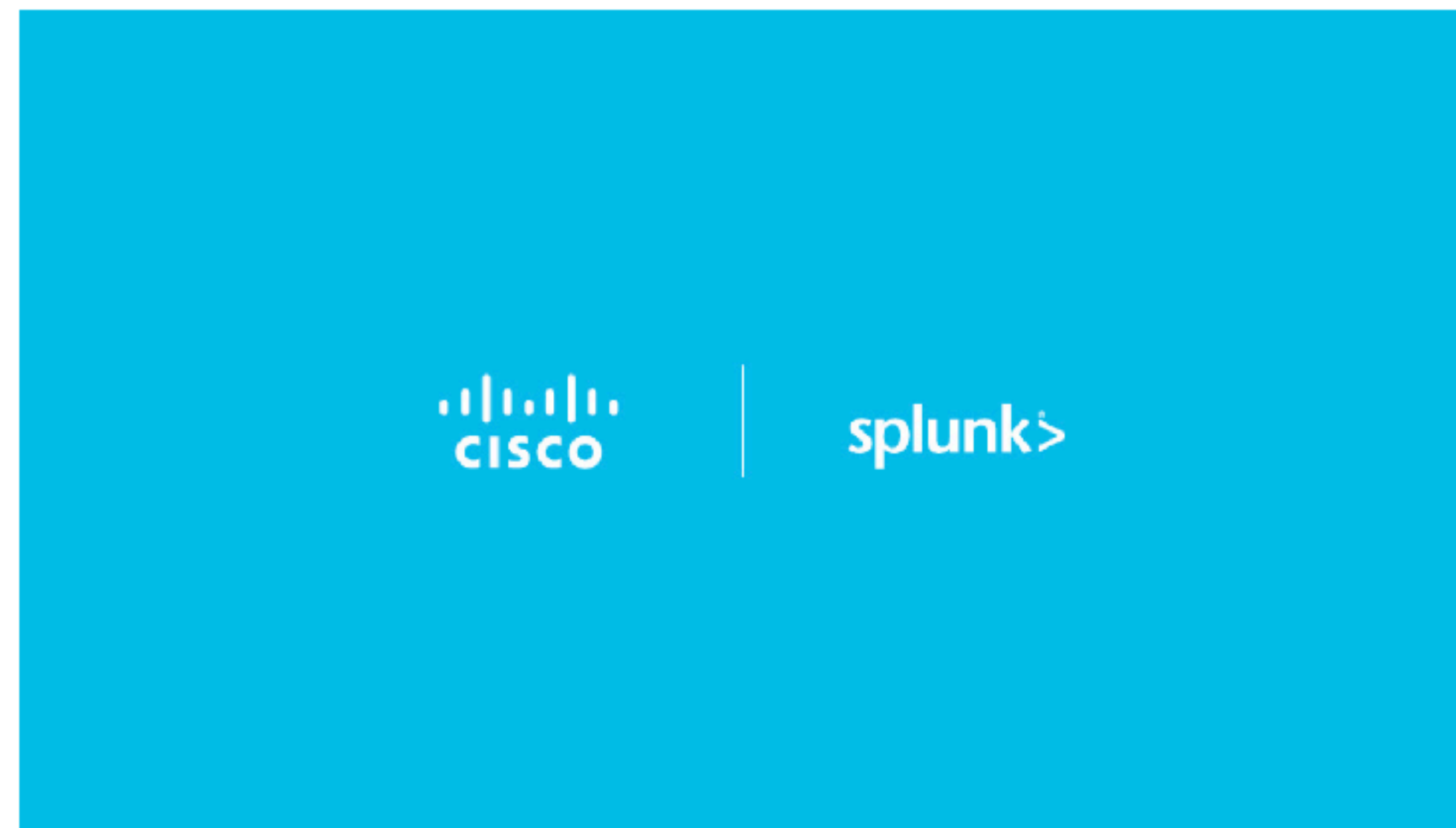




<https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2023/m09/cisco-to-acquire-splunk-to-help-make-organizations-more-secure-and-resilient-in-an-ai-powered-world.html>

Press Release

# Cisco to Acquire Splunk, to Help Make Organizations More Secure and Resilient in an AI-Powered World



Sep 21, 2023



[LinkedIn](#)



[Twitter](#)



[Facebook](#)

## News Summary

- Together, Cisco and Splunk will help move organizations from threat detection and response to threat prediction and prevention
- Combined, Cisco and Splunk will become one of the world's largest software companies and will accelerate Cisco's business transformation to more recurring revenue
- Expected to be cash flow positive and gross margin accretive in first fiscal year post close, and non-GAAP EPS accretive in year 2. Will accelerate revenue growth and gross margin expansion
- Unites two "Great Places to Work" with similar values, strong cultures, and talented teams
- The combination of these two innovative leaders makes them well positioned to lead in security and observability in the age of AI

**San Jose and San Francisco, Calif., September 21, 2023** – Cisco (NASDAQ: CSCO) and Splunk

WHOOPS—

# Incomplete disclosures by Apple and Google create “huge blindspot” for 0-day hunters

No one mentioned that libwebp, a library found in millions of apps, was a 0-day origin.

DAN GOODIN - 9/21/2023, 6:19 PM

<https://arstechnica.com/security/2023/09/incomplete-disclosures-by-apple-and-google-create-huge-blindspot-for-0-day-hunters/>



Getty Images

Enlarge

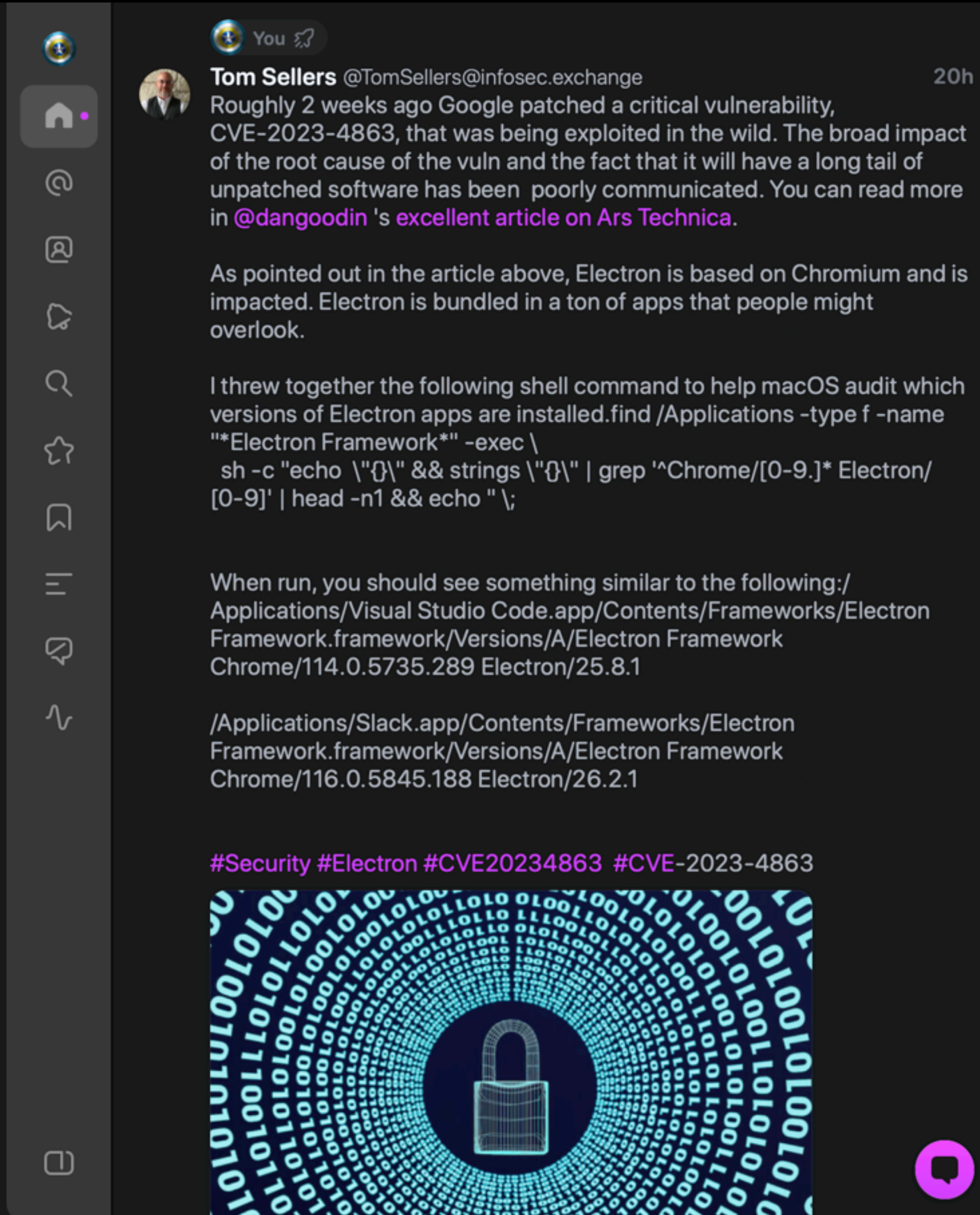
1Password  
balenaEtcher  
Basecamp 3  
Beaker (web  
browser)  
Bitwarden  
CrashPlan  
Cryptocat  
(discontinued)  
Discord  
Eclipse Theia  
FreeTube  
GitHub Desktop  
GitKraken  
Joplin

Keybase  
Lbry  
Light Table  
Logitech Options+  
LosslessCut  
Mattermost  
Microsoft Teams  
MongoDB Compass  
Mullvad  
Notion  
Obsidian  
QQ (for macOS)  
Quasar Framework  
Shift  
Signal

Skype  
Slack  
Symphony Chat  
Tabby  
Termius  
TIDAL  
Twitch  
Visual Studio Code  
WebTorrent  
Wire  
Yammer



https://infosec.exchange/@TomSellers/111126352647377681



**You**

**Tom Sellers** @TomSellers@infosec.exchange 20h

Roughly 2 weeks ago Google patched a critical vulnerability, CVE-2023-4863, that was being exploited in the wild. The broad impact of the root cause of the vuln and the fact that it will have a long tail of unpatched software has been poorly communicated. You can read more in [@dangoodin](#)'s excellent article on Ars Technica.

As pointed out in the article above, Electron is based on Chromium and is impacted. Electron is bundled in a ton of apps that people might overlook.

I threw together the following shell command to help macOS audit which versions of Electron apps are installed.


```
find /Applications -type f -name "*Electron Framework*" -exec \
  sh -c "echo \"{}\" && strings \"{}\" | grep '^Chrome/[0-9.]* Electron/[0-9]' | head -n1 && echo \" \";
```

When run, you should see something similar to the following:

```
Applications/Visual Studio Code.app/Contents/Frameworks/Electron Framework.framework/Versions/A/Electron Framework
Chrome/114.0.5735.289 Electron/25.8.1
```

```
/Applications/Slack.app/Contents/Frameworks/Electron Framework.framework/Versions/A/Electron Framework
Chrome/116.0.5845.188 Electron/26.2.1
```

[#Security](#) [#Electron](#) [#CVE20234863](#) [#CVE-2023-4863](#)



I threw together the following shell command to help macOS audit which versions of Electron apps are installed.

```
find /Applications -type f -name "*Electron Framework*" -exec \
  sh -c "echo \"{}\" && strings \"{}\" | grep '^Chrome/[0-9.]* Electron/[0-9]' | head -n1 && echo \" \";
```

When run, you should see something similar to the following:

```
/Applications/Visual Studio Code.app/Contents/
Frameworks/Electron Framework.framework/
Versions/A/Electron Framework
Chrome/114.0.5735.289 Electron/25.8.1
```

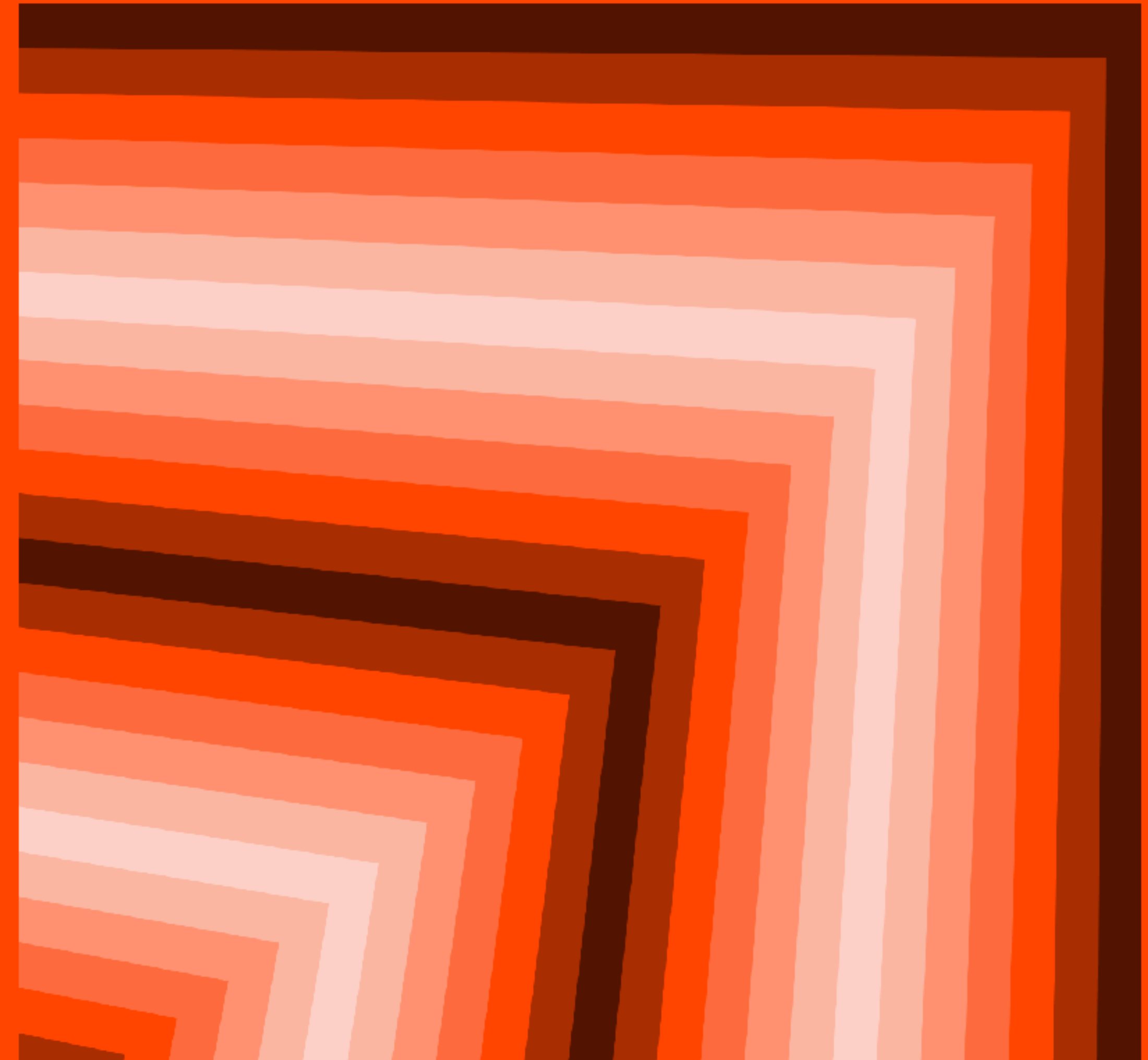
```
/Applications/Slack.app/Contents/Frameworks/
Electron Framework.framework/Versions/A/
Electron Framework
Chrome/116.0.5845.188 Electron/26.2.1
```

<https://openai.com/blog/red-teaming-network>

# OpenAI Red Teaming Network

We're announcing an open call for the OpenAI Red Teaming Network and invite domain experts interested in improving the safety of OpenAI's models to join our efforts.

[Apply to join](#)





# STATE SERVICE OF SPECIAL COMMUNICATIONS AND INFORMATION PROTECTION OF UKRAINE

<https://cip.gov.ua/en/news/yak-zminyuyutsya-taktiki-cili-i-spromozhnosti-khakerskikh-grup-uryadu-rf-ta-kontrolovanikh-nim-ugrupovan-zvit>



## How russian government-controlled hacking groups shift their tactics, objectives and capacities – report

News

25.09.2023 09:08

The SSSCIP has prepared an analytical report *Russia's Cyber Tactics H1 2023*. We have analyzed and explored cyber threats by russian hacking groups in 2022 and the first half of 2023 as well as shifts in the cybercriminals' behavior.

The report contains information that may be helpful to Ukrainian cybersecurity specialists as well as to our international partners. Specifically, it will be useful for:

- understanding russian hackers' motives, capabilities to carry out cyber operations as well as their choice of targets;
- anticipating the extent of cyber capacities that may be employed by the enemy in the current and future geopolitical conflicts;
- seeking new tools and methods to counter hostile cyberattacks, etc.

The new trends of 2023 include increased focus of the enemy hackers on Ukrainian law enforcement. It is about intelligence operations aimed at accessing the data on the evidence of russia's war crimes, collected and submitted materials for trials and prosecution, arrest warrants for suspected agents, etc.

Energy and media sectors remain among the major targets of the enemy hackers.

Besides, the SSSCIP specialists have revealed an indicative trend of recurring attacks. Hackers revisit their prior targets that own and operate critical data, required by the russian military. This approach enables the perpetrators to strategically plan their future operations and forecast our responses. Early knowledge of the target entity's network infrastructure, protection measures, key personnel and communication modalities offers the attackers a substantial advantage when it comes to exploiting the earlier compromised organizations.

Read more in [the Russia's Cyber Tactics H1 2023 analytical report](#).

Please be reminded that for better understanding of the changes in the objectives faced by russian government-controlled hacking groups and other teams directly engaged in the

2X Growth In The Number Of Incidents Where  
Cert Ua Was Involved In Investigations &  
Forensics

The Civic & Law-Enforcement Sector Is  
Dominating Across Espionage Targets

Once A Victim – Always A Victim!

Focus On Immediate Data Exfiltration

The Media Sector Is Under Constant Attack  
During First Six Months Of 2023

Growing On Usage “Living Off The Land”

Hacking And Exploiting Open-Source Mail  
Systems

The Energy Sector Continues To Be Under Attack

# RUSSIA'S CYBER TACTICS H1'2023

## Lessons Learned:

Shift in the Patterns, Goals, and Capacity  
of the Russian Government and  
Government-Controlled Groups

Threat Research Report

September 2023



State Service of Special Communications  
and Information Protection of Ukraine

Russian threat actors now have limited time for lateral movement, prompting them to place even greater emphasis on a particular tactic: dumping documents, sometimes as many as 21,000 office documents in certain cases, along with browser credentials. They execute this tactic within the first 30 minutes of successfully infiltrating a compromised system. Subsequently, they commence disseminating their malware through various channels, such as email, to other high-profile targets, taking advantage of established trust relationships.

We've observed a shift in tactics that involve infecting systems, prioritizing victims, and gaining access to more valuable assets by replacing compromised Command and Control servers (C2s). The primary payloads still consist of office documents and HTML/ JS-based malware packaged in archives, which remain the most prevalent and favored formats.

<https://gothamist.com/news/the-nypd-is-deploying-a-420-pound-robot-to-roam-times-squares-subway-station>

# The NYPD is deploying a 420-pound robot to roam Times Square subway station



By Jessy Edwards  
Published Sep 22, 2023  
[90 comments](#)

Share    

## Never miss a story

Email address



By submitting your information, you're agreeing to receive communications from New York Public Radio in accordance with our [Terms](#).

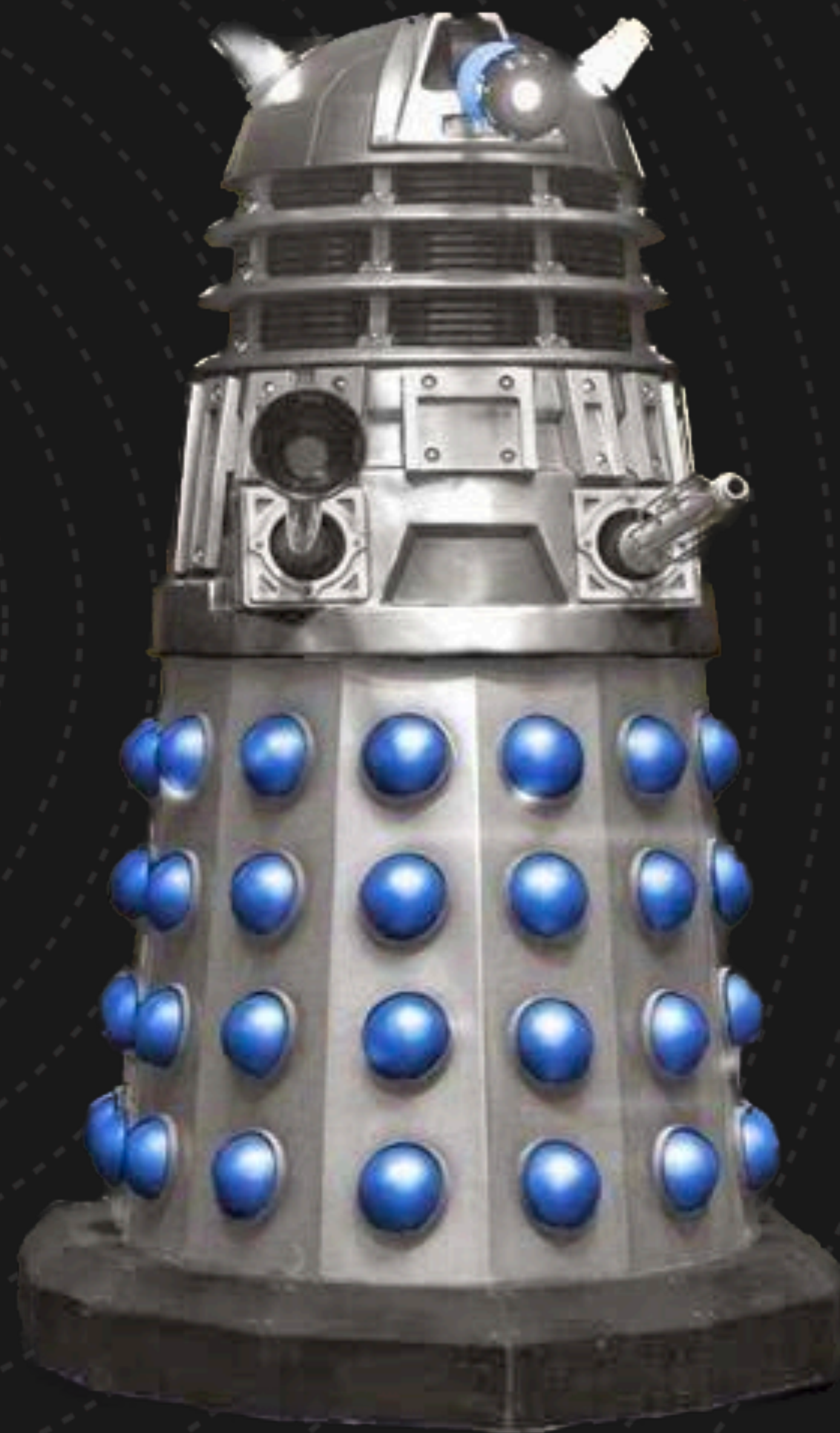


Screenshot: NYC Mayor's Office YouTube page

Gothamist is funded by sponsors and member donations

S T O R M ⚡ W A T C H

GREYNOISE



- 🏷️ Cisco CVE-2020-3187 Scanner
- 🏷️ Apache Roller OGNL Injection Attempt
- 🏷️ jQuery-File-Upload Attempt
- 🏷️ phpThumb fltr RCE Attempt
- 🏷️ Horde Path Traversal Attempt

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



It Has Been

1

Days Since The  
Last KEV Release

\$ shutdown -r now



MinIO Security Feature Bypass Vulnerability

Trend Micro Apex One and Worry-Free Business Security Remote Code Execution Vulnerability

Apple Multiple Products WebKit Code Execution Vulnerability

Apple Multiple Products Kernel Privilege Escalation Vulnerability

Apple Multiple Products Improper Certificate Validation Vulnerability

S T O R M ⚡ W A T C H

GREYNOISE



**Dateline: 2023-09-26**