

# STORM ⚡ WATCH

CYBERSECURITY NEWS

Deadline: 2024-02-13



LIKE



SUBSCRIBE

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://StormWatch.ing>



LEAVE A  
COMMENT



SHARE

# STORM ⚡ WATCH

CYBERSECURITY NEWS

# WHAT THE ...



**I have become death. Destroyer of worlds.  
What have I wrought on this world!**



<https://infosec.exchange/@Muddobbers/111904927734429527>

<https://www.tomshardware.com/networking/three-million-malware-infected-smart-toothbrushes-used-in-swiss-ddos-attacks-botnet-causes-millions-of-euros-in-damages>

# STORM ⚡ WATCH

CYBERSECURITY NEWS

# HIGH FIVE





[https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/Buying\\_Spying\\_-\\_Insights\\_into\\_Commercial\\_Surveillance\\_Vendors\\_-\\_TAG\\_report.pdf](https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/Buying_Spying_-_Insights_into_Commercial_Surveillance_Vendors_-_TAG_report.pdf)

# Buying Spying

Insights into Commercial Surveillance Vendors

## Executive Summary

The commercial surveillance industry has emerged to fill a lucrative market niche: selling cutting edge technology to governments around the world that exploit vulnerabilities in consumer devices and applications to surreptitiously install spyware on individuals' devices. By doing so, commercial surveillance vendors (CSVs) are enabling the proliferation of dangerous hacking tools.

The harm is not hypothetical. Spyware vendors point to their tools' legitimate use in law enforcement and counterterrorism. However, spyware deployed against journalists, human rights defenders, dissidents, and opposition party politicians — what Google refers to as 'high risk users' — has been well documented, both by analysis from Google, and by researchers from organizations like the University of Toronto's Citizen Lab and Amnesty International. While the number of users targeted by spyware is small compared to other types of cyber threat activity, the follow-on effects are much broader. This type of focused targeting threatens freedom of speech, a free press, and the integrity of elections worldwide.

As threat actors, CSVs pose a threat to Google users, as half of known 0-day exploits used against Google products, as well as Android ecosystem devices, can be attributed to CSVs. Google takes the security of our users very seriously, with dedicated teams in place to protect against attacks from a wide range of sources. Today, Google's Threat Analysis Group (TAG) actively tracks around 40 CSVs, with varying levels of sophistication and public exposure, selling exploits and surveillance capabilities to government customers.

In the appendix of this report, we have included an overview of a subset of the CSVs tracked by Google, their products, and the exploits they use against consumer devices and applications.



Spyware

Commercial Surveillance  
Vendors (CSVs)

0-Days

- Vulnerability researchers and exploit developers
- Exploit brokers and suppliers
- Commercial Surveillance Vendors (CSVs) or Private Sector Offensive Actors (PSOAs)
- Government customers

While prominent CSVs garner public attention and headlines, there are dozens of others that are less noticed, but play an important role in developing spyware



**The proliferation of spyware by  
CSVs causes real world harm.**

High-risk humans attested to the  
fear felt when these tools were  
used against them, the chilling  
effect on their professional  
relationships, and their  
determination to continue their  
important work

If governments ever claimed to have a monopoly on the most advanced cyber capabilities, that era is over. **The private sector is now responsible for a significant portion of the most sophisticated tools**

CSVs are behind half of known 0-day exploits targeting Google products as well as Android ecosystem devices

- **Cy4Gate and RCS Lab:** Italian firms known for the "Epeius" and "Hermit" spyware for Android and iOS. The former acquired the latter in 2022, but operate independently
- **Intellexa:** Alliance of spyware firms led by Tal Dilian since 2019. It combines technologies like Cytrox's "Predator" spyware and WiSpear's WiFi interception tools, offering integrated espionage solutions
- **Negg Group:** Italian CSV with international reach established in 2013. It is known for "Skygofree" malware and "VBiss" spyware, targeting mobile devices through exploit chains
- **NSO Group:** Israeli firm famous for Pegasus spyware and other sophisticated espionage tools. It continues operations despite sanctions and legal issues
- **Variston:** Spanish CSV providing tailored security solutions. It collaborates with other vendors for zero-day exploits and is linked to the Heliconia framework, expanding in the UAE.

CVE-2016-4655	CVE-2021-28664	CVE-2021-39793	CVE-2023-28206
CVE-2016-4656	CVE-2021-30551	CVE-2022-22047	CVE-2023-3079
CVE-2016-4657	CVE-2021-30554	CVE-2022-2294	CVE-2023-32409
CVE-2018-5002	CVE-2021-30860	CVE-2022-26485	CVE-2023-33063
CVE-2019-2215	CVE-2021-30883	CVE-2022-2856	CVE-2023-33106
CVE-2019-2215	CVE-2021-30983	CVE-2022-3075	CVE-2023-33107
CVE-2019-2215	CVE-2021-31010	CVE-2022-3723	CVE-2023-41061
CVE-2019-3568	CVE-2021-31199	CVE-2022-3723	CVE-2023-41064
CVE-2021-0920	CVE-2021-31201	CVE-2022-4135	CVE-2023-41991
CVE-2021-1048	CVE-2021-31979	CVE-2022-4262	CVE-2023-41992
CVE-2021-1905	CVE-2021-33742	CVE-2022-42856	CVE-2023-41993
CVE-2021-1906	CVE-2021-33771	CVE-2023-0266	CVE-2023-4211
CVE-2021-21166	CVE-2021-36948	CVE-2023-2033	CVE-2023-42916
CVE-2021-22600	CVE-2021-37973	CVE-2023-2136	CVE-2023-42917
CVE-2021-25394	CVE-2021-37976	CVE-2023-21492	CVE-2023-5217
CVE-2021-28550	CVE-2021-38000	CVE-2023-26083	CVE-2023-7024
CVE-2021-28663	CVE-2021-38003	CVE-2023-28205	

LINUX KERNEL

ANDROID

SAMSUNG MFC CHARGER DRIVER

ARM MALI GPU

WhatsApp

ANDROID KERNEL

WINDOWS

Chrome

SAMSUNG ANDROID

WEBKIT

ADOBE READER

SAFARI

INTERNET EXPLORER

iOS

QUALCOMM

IOS KERNEL

FLASH

FIREFOX



<https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/30/joint-statement-on-efforts-to-counter-the-proliferation-and-misuse-of-commercial-spyware/>

MARCH 30, 2023

# Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware



▶ BRIEFING ROOM



▶ STATEMENTS AND RELEASES

We, the governments of Australia, Canada, Costa Rica, Denmark, France, New Zealand, Norway, Sweden, Switzerland, the United Kingdom, and the United States, recognize the threat posed by the misuse of commercial spyware and the need for strict domestic and international controls on the proliferation and use of such technology.

# STORM ⚡ WATCH

CYBERSECURITY NEWS

# HEADS UP





# JOINT CYBERSECURITY ADVISORY

Co-Authored by:

TLP:CLEAR

Product ID: AA24-038A

February 7, 2024



**ASD** AUSTRALIAN  
SIGNALS  
DIRECTORATE  
ACSC Australian  
Cyber Security  
Centre



Communications  
Security Establishment

Centre de la sécurité  
des télécommunications

Canadian Centre  
for Cyber Security

Centre canadien  
pour la cybersécurité



National Cyber  
Security Centre  
PART OF THE GCSB



National Cyber  
Security Centre  
a part of GCHQ

# Volt Typhoon

# PRC State-Sponsored

# Actors Compromise

# and Maintain

# Persistent Access to

# U.S. Critical

# Infrastructure



PRC State-Sponsored Actors Compromise and  
Maintain Persistent Access to U.S. Critical  
Infrastructure

*This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see [cisa.gov/tlp](https://www.cisa.gov/tlp).*

TLP:CLEAR

[https://www.cisa.gov/sites/default/files/2024-02/aa24-038a-jcsa-prc-state-sponsored-actors-compromise-us-critical-infrastructure\\_1.pdf](https://www.cisa.gov/sites/default/files/2024-02/aa24-038a-jcsa-prc-state-sponsored-actors-compromise-us-critical-infrastructure_1.pdf)




LAWFARE

# **Volt Typhoon: Keep Calm and Carry On**

<https://www.lawfaremedia.org/article/volt-typhoon-keep-calm-and-carry-on-vpns-wounded-in-cyber-knife-fight>


 Chinese cyber group

 Compromised the IT environments of     

 Potential to disrupt critical infrastructure during geopolitical tensions or military conflicts

 Cyber knife fight involving UTA0178, a PRC cyber espionage group, and Ivanti

 KV botnet disruption

 FTC actions against data brokers, a U.S. law firm settling a hacking claim, and visa restrictions for commercial spyware peeps.

BLOGS

# Water ICS Exposures Highlight Vulnerabilities in Critical Infrastructure Security



<https://censys.com/water-ics-exposures-highlight-vulnerabilities-in-critical-infrastructure-security/>

S T O R M ⚡ W A T C H

CYBERSECURITY NEWS

# THREAT FOCUS





<https://www.securityweek.com/canon-patches-7-critical-vulnerabilities-in-small-office-printers/>

**VULNERABILITIES**

# Canon Patches 7 Critical Vulnerabilities in Small Office Printers

Canon announces patches for seven critical-severity remote code execution flaws impacting small office printer models.



By [Ionut Arghire](#)  
February 6, 2024



**Japanese electronics maker Canon on Monday announced software updates that patch seven critical-severity vulnerabilities impacting several small office printer models.**

S T O R M ⚡ W A T C H

CYBERSECURITY NEWS

# CYBER SPOTLIGHT





TLP:CLEAR



JOINT GUIDANCE:

# Identifying and Mitigating Living Off the Land Techniques

Publication: February 7, 2024

- U.S. Cybersecurity and Infrastructure Security Agency
- U.S. National Security Agency
- U.S. Federal Bureau of Investigation
- U.S. Department of Energy
- U.S. Environmental Protection Agency
- U.S. Transportation Security Administration
- Australian Signals Directorate's Australian Cyber Security Centre
- Canadian Centre for Cyber Security (Cyber Centre), a part of the Communications Security Establishment (CSE)
- United Kingdom National Cyber Security Centre
- New Zealand National Cyber Security Centre

This document is marked TLP:CLEAR. Recipients may share this information without restriction. Information is subject to standard copyright rules. For more information on the Traffic Light Protocol, see <https://www.cisa.gov/tlp>.

TLP:CLEAR

Guide for network defenders focuses on how to mitigate identified gaps and to detect and hunt for LotL activity

[https://www.cisa.gov/sites/default/files/2024-02/Joint-Guidance-Identifying-and-Mitigating-LOTL\\_V3508c.pdf](https://www.cisa.gov/sites/default/files/2024-02/Joint-Guidance-Identifying-and-Mitigating-LOTL_V3508c.pdf)



- Organizations lack effective security and network management practices that support detection of malicious LOTL activity
- General lack of conventional indicators of compromise (IOCs) associated with the activity,
- LotL enables cyber threat actors to avoid investing in developing and deploying custom tools

- Disabling or removing unnecessary protocols by default
- Limiting network reachability to the extent feasible
- Limiting processes and programs running with elevated privileges
- Enabling phishing-resistant MFA as a default feature
- Providing high-quality secure logging at no additional charge beyond processing and storage costs
- Eliminating default passwords and credentials when installing software
- Limiting or removing dynamic code execution

# STORM ⚡ WATCH

CYBERSECURITY NEWS

# TOOL TIME



## Living off the False Positive!

Living off the False Positive is an autogenerated collection of false positives sourced from some of the most popular rule sets. The information is categorized along with ATT&CK techniques, rule source, and data source. Entries include details from related rules along with their description and detection logic.

The goal is to enable both red and blue teams with this information. Red teams can use this information to blend in, whereas blue teams can use this information to assess weak spots in their detection logic. Interestingly, it can also assist during alert triage and investigation, by looking at common FPs around certain techniques and data sources.

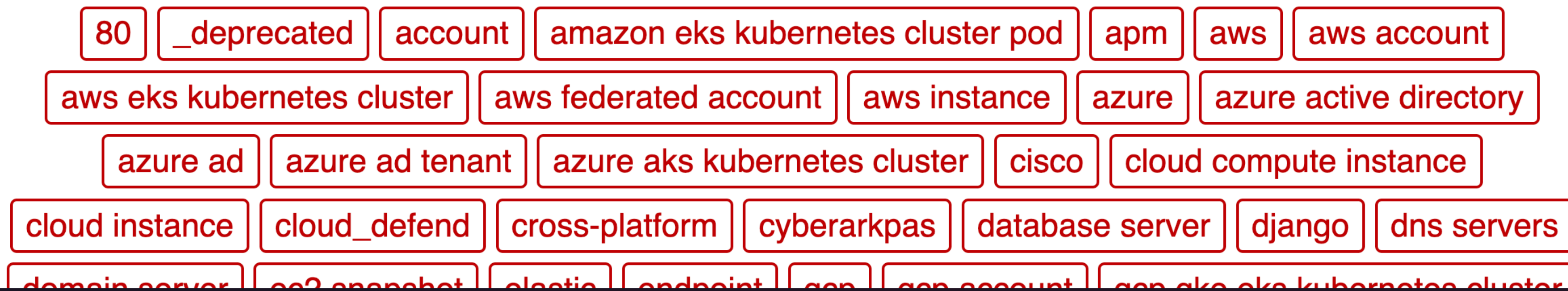


To maximize value, don't scroll – focus on searching for keywords in the false positives themselves (such as “python”, “powershell”, etc.), the techniques, rule source, or data source, then go from there!

A primary goal is to make this maintenance-free, so this data is automatically refreshed nightly.

For more details, checkout the release [blog](#).

If you are struggling with false positive management during rule creation, consider using the [Zen of Security Rules](#).



- Autogenerated collection of false positives sourced from popular rule sets
- Categorizes information along with ATT&CK techniques, rule source, and data source
- Includes details from related rules along with their description and detection logic
- Red teams can use it to blend in by mimicking or looking similar to the false positive activity
- Blue teams can assess weak spots in their detection logic and compare across rule sets
- Sourced from elastic detection rules, sigma rules, and splunk rules, and is refreshed nightly



# LoFP / a user may have multiple sessions open at the same time, such as on a mobile device and a laptop.

[t1550](#)[okta](#)[elastic](#)

## Techniques

- [T1550](#)

```
https://br0k3nlab.com/LoFP/a-user-may-have-multiple-sessions-open-at-the-same-time-such-as-on-a-mobile/
```

## Sample rules

### Multiple Okta Sessions Detected for a Single User

- source: [elastic](#)
- techniques:
  - T1550

## Description

Detects when a user has started multiple Okta sessions with the same user account and different session IDs. This may indicate that an attacker has stolen the user's session cookie and is using it to access the user's account from a different location.

# SHAMELESS SELF-PROMOTION



BLOGS

# A Beginner's Guide to Tracking Malware Infrastructure



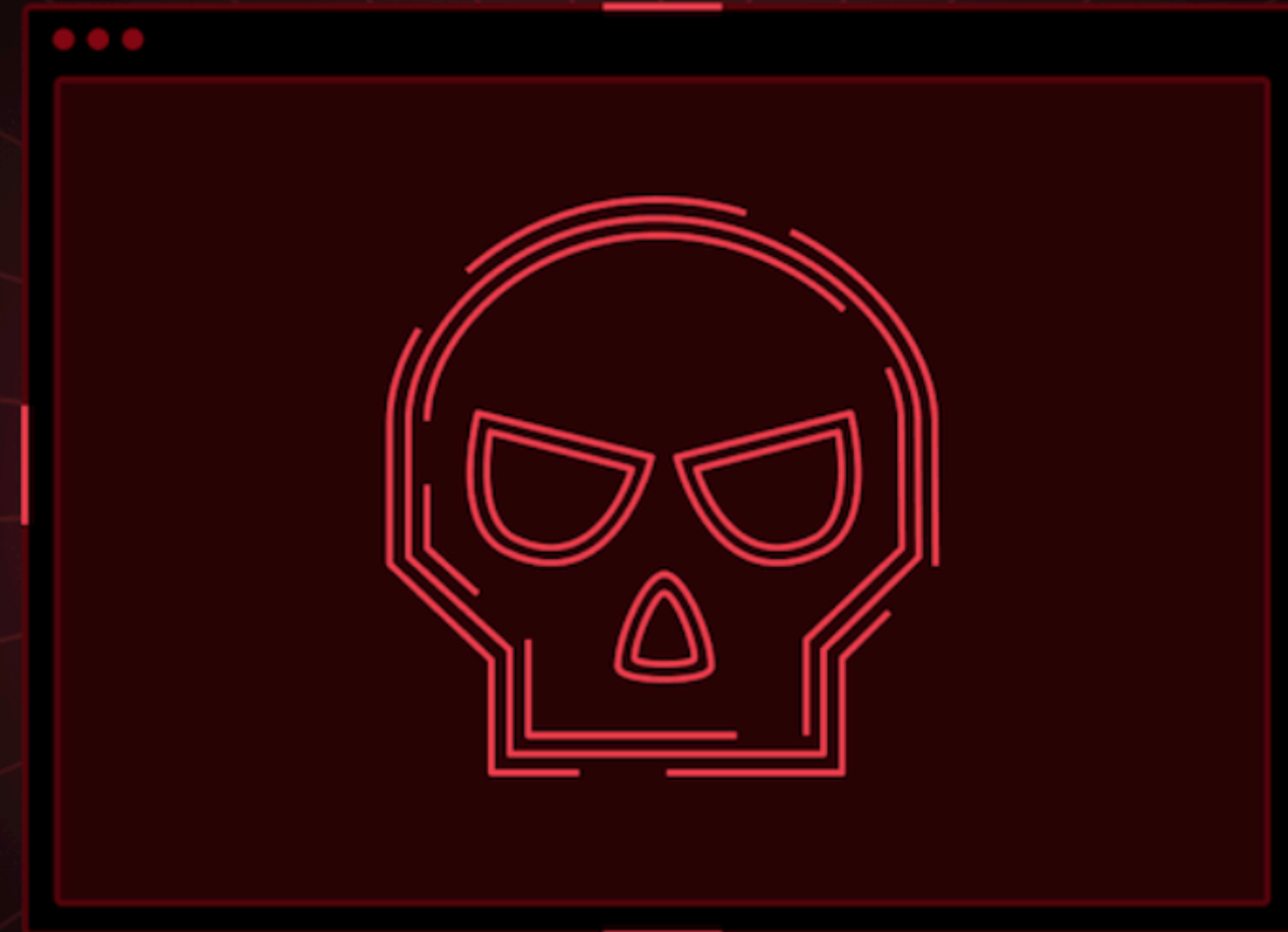
<https://censys.com/a-beginners-guide-to-tracking-malware-infrastructure/>



VULNERABILITIES PRODUCT

# Battling Ransomware One Tag At A Time

boB Rudis | February 8, 2024

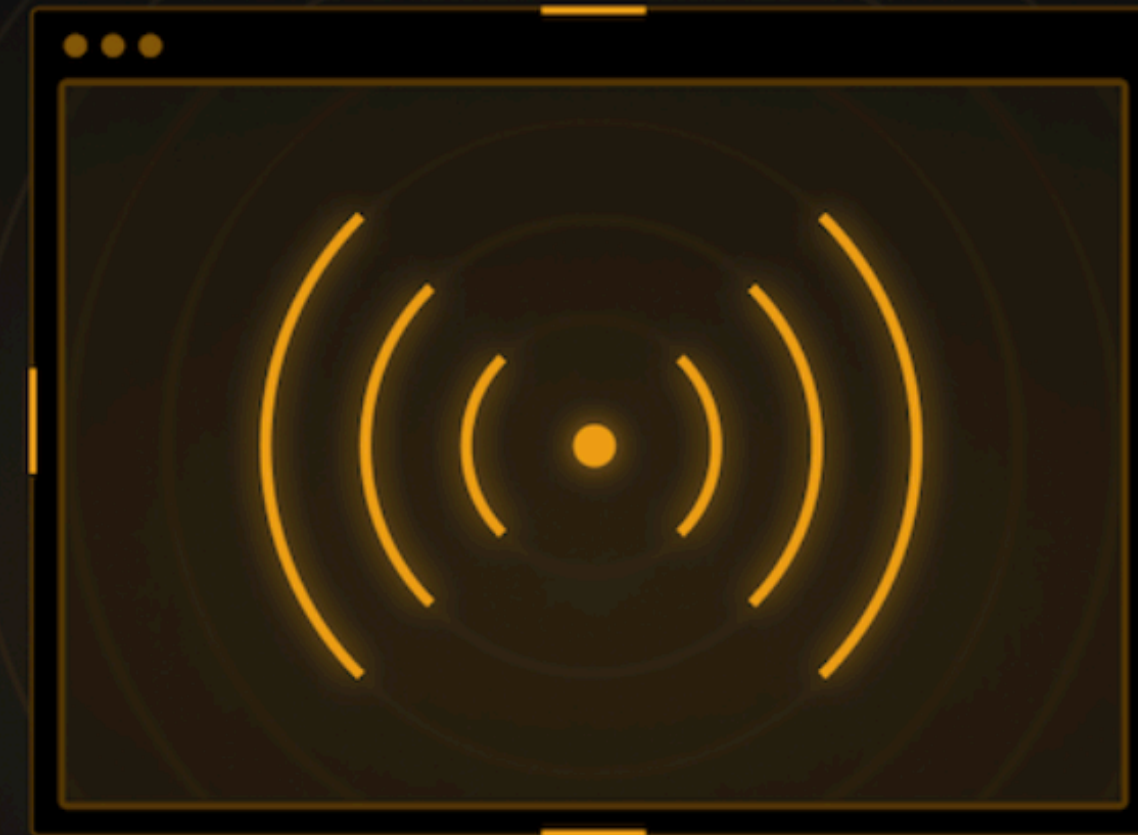


<https://www.greynoise.io/blog/battling-ransomware-one-tag-at-a-time>

INSIGHTS

# Governments Have Zero Reason To Be Flipping Mad About Open Source SDR Tech

The GreyNoise Team | February 12, 2024



<https://www.greynoise.io/blog/governments-have-zero-reason-to-be-flipping-mad-about-open-source-sdr-tech>



Valentines Day

<https://www.greynoise.io/events/greynoise-community-open-forum-vi>

## GreyNoise Community Open Forum VI

- **Date:** Thursday, February 15th
- **Time:** 1:30pm CT / 2:30pm ET
- **Duration:** 1 hour

Join us on February 15th for our next GreyNoise Open Forum, our townhall style event where the GreyNoise team shares what we've been up to lately and what's to come in the near future.

Here is a sneak peek into our agenda:

- Introduce our new head of the GreyNoise Community , Sam Houston!
- GreyNoise Labs' boB Rudis will take a deep dive into the results of our recent 2023 Internet Exploitation Retrospective Report
- GreyNoise Founder & CEO Andrew Morris will reveal what's coming up in 2024
- Plus the usual games, prizes, and general pandemonium!

<https://centripetal.registration.goldcast.io/events/faabb062-4f84-4591-8082-c8c6ad29a3c2>

# WHAT IS INTELLIGENCE POWERED **CYBERSECURITY?**



THURSDAY, FEBRUARY 15th  
11:00AM ET/8:00AM PT



**JESS PARNELL**  
CISO  
CENTRIPETAL



**GLENN THORPE**  
SR. DIRECTOR, SECURITY RESEARCH  
& DETECTION ENGINEERING  
GREYNOISE INTELLIGENCE



**DAVE AHN**  
VP, CHIEF ARCHITECT  
CENTRIPETAL



**KIMBER DUKE**  
PRODUCT MANAGER  
GREYNOISE INTELLIGENCE



CENTRIPETAL

S T O R M ⚡ W A T C H

CYBERSECURITY NEWS

# TAG ROUND-UP



- 🏷️ FCKeditor File Upload Scanning (CVE-2006-2529)
- 🏷️ Tongda OA RCE Attempt
- 🏷️ Parks Fiberlink 210 CVE-2023-33617 Attempt (CVE-2023-33617)
- 🏷️ Horde CVE-2012-0209 RCE Attempt (CVE-2012-0209)
- 🏷️ eXtplorer Authentication Bypass Attempt
- 🏷️ Jupyter Notebook Scanner
- 🏷️ Graphite Web CVE-2013-5093 RCE Attempt (CVE-2013-5093)
- 🏷️ MobileCartly RCE Attempt

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

**WE NEED  
TO TALK  
ABOUT  
KEY**



It Has Been

1

Days Since The  
Last KEV Release

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



**CVE-2023-4762:** Google Chromium V8 Type Confusion

**CVE-2024-21762:** Fortinet FortiOS Out-of-Bound Write

**CVE-2023-43770:** Roundcube Webmail Persistent Cross-Site Scripting (XSS)

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