STORM WATCH

Dateline: 2024-01-23

STORM WATCH

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/


CYBER
SPOTLIGHT

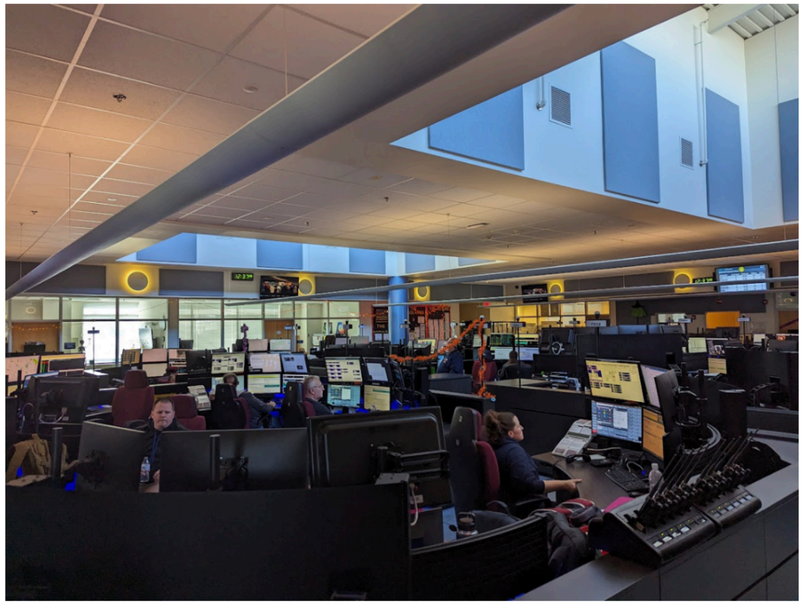
https://www.newhopefreepress.com/2024/01/22/bucks-county-computer-aided-dispatch-system-out-of-service/

Cops, Courts and Fire · Government

UPDATE: Bucks County Computer-Aided Dispatch System Crippled By Cyberattack

13 hours ago · by Tom Sofield

Bucks County's computer-aided dispatch (CAD) system stopped working on Sunday.

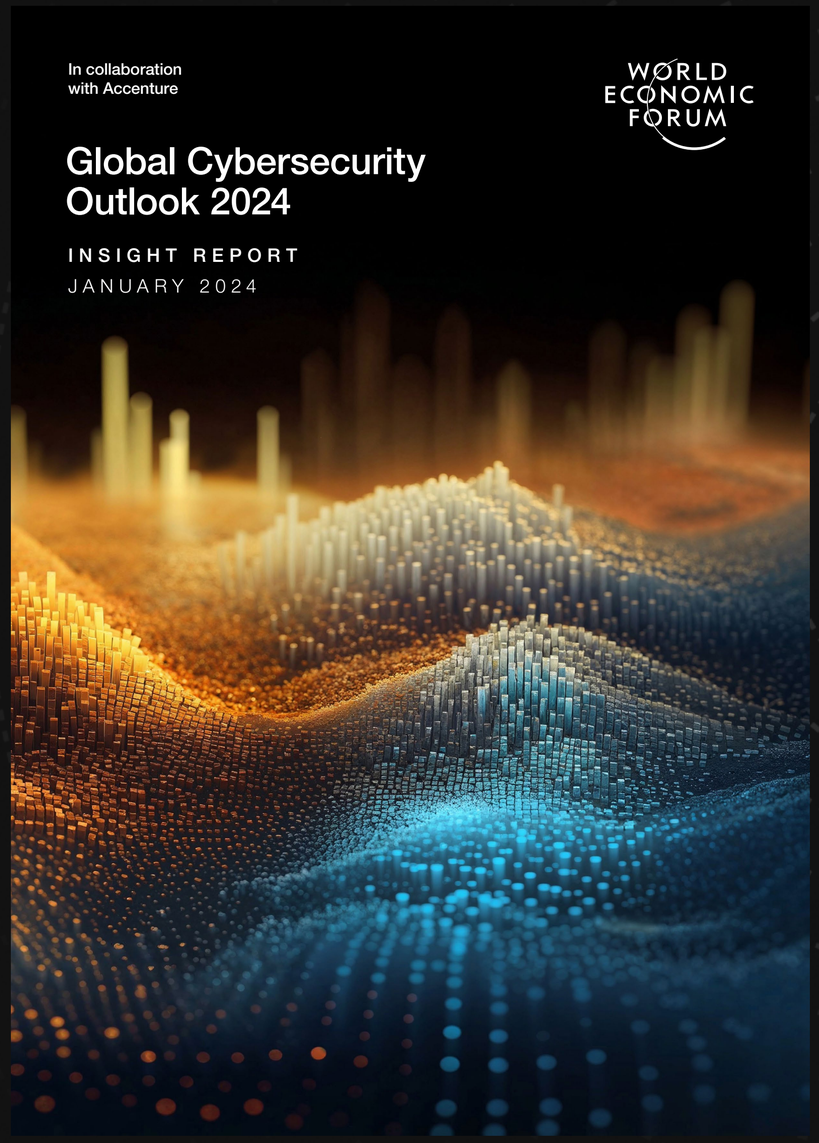


The Bucks County 9-1-1 Center. File photo

STORMWATCH

Bucks County's computer-aided dispatch (CAD) system experienced an outage, which authorities believe was caused by a cyberattack. The CAD system is used by dispatchers, 9-1-1 call-takers, and responders to input and broadcast addresses and developing information on incidents. The outage impacted local law enforcement agencies, fire companies, and ambulance squads. The 9-1-1 center remained operational and continued to receive calls and dispatch local crews as necessary. County officials are working to restore the CAD service, and incident documentation is being kept on a backup system. Due to the incident, the county's access to statewide and federal law enforcement databases was disabled.

STORM WATCH



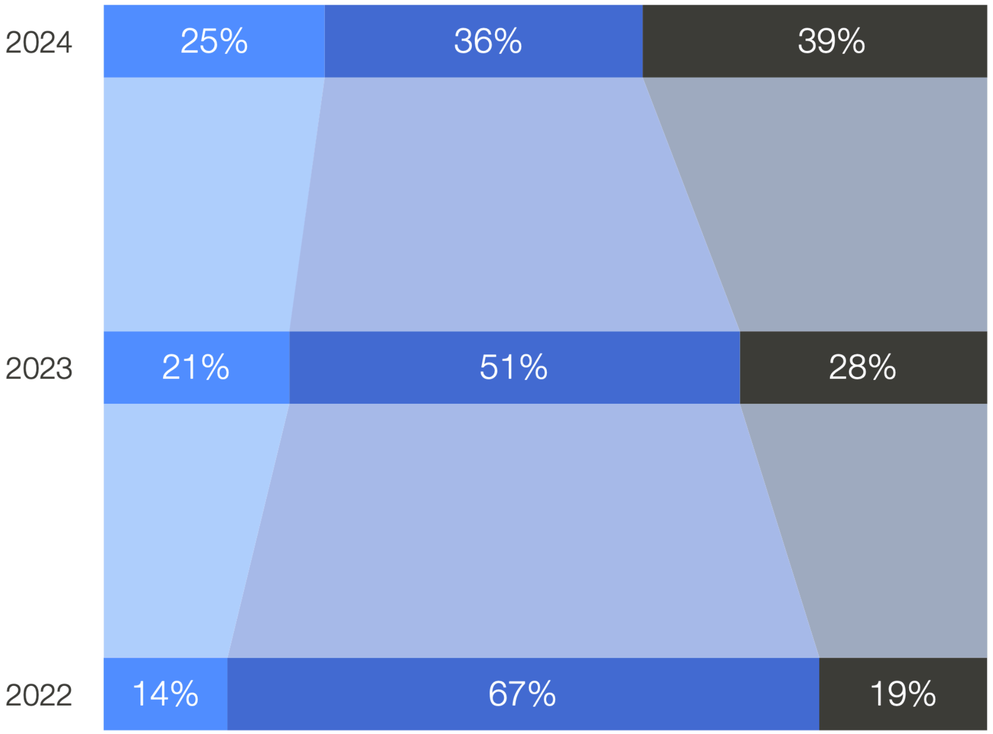
https://www.weforum.org/publications/global-cybersecurity-outlook-2024/

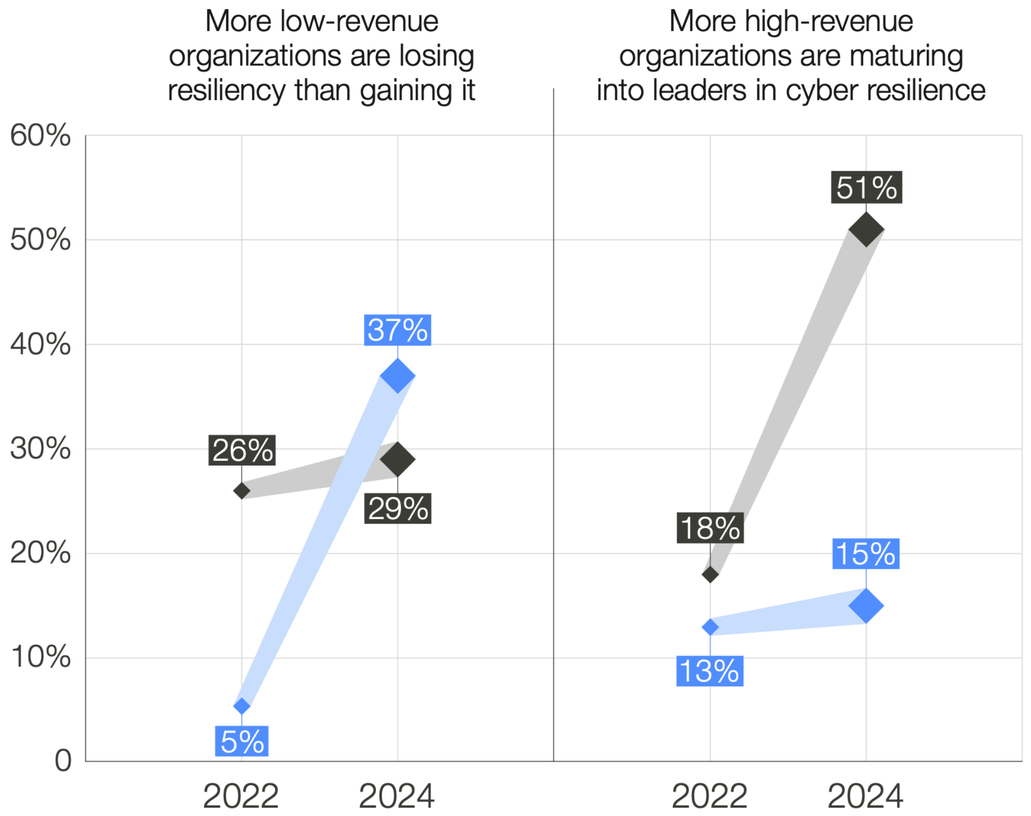
https://commercial.allianz.com/news-and-insights/expert-risk-articles/allianz-risk-barometer-2024-cyber-incidents.html

STORMWATCH

There is growing cyber inequity between organizations that are cyber resilient and those that are not

What is the state of your organization's cyber resilience this year?

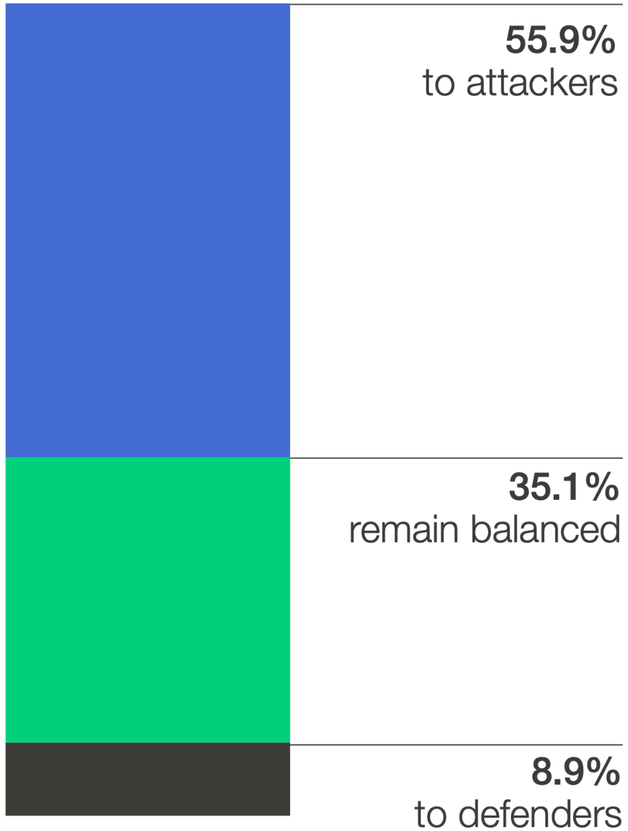




Our cyber resilience is **insufficient** | Our cyber resilience meets **minimum requirements** | Our cyber resilience **exceeds** our requirements

Emerging technologies will exacerbate long-standing challenges related to cyber resilience

In the next two years, will generative AI provide overall cyber advantage to attackers or defenders?



What are you most concerned about in regards to generative AI's impact on cyber?

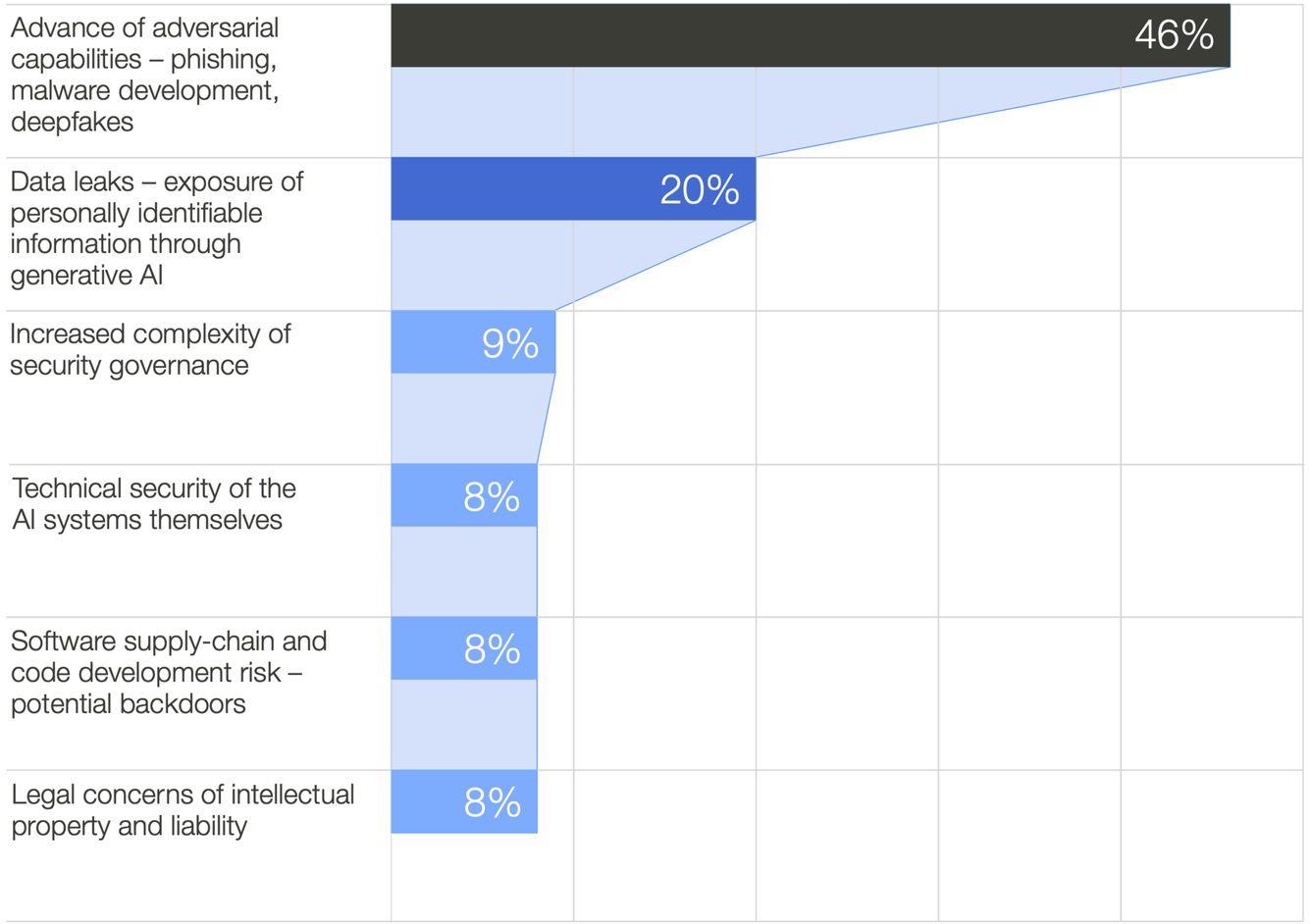


FIGURE 5 | **Do you have the skills needed to achieve your cybersecurity objectives?**

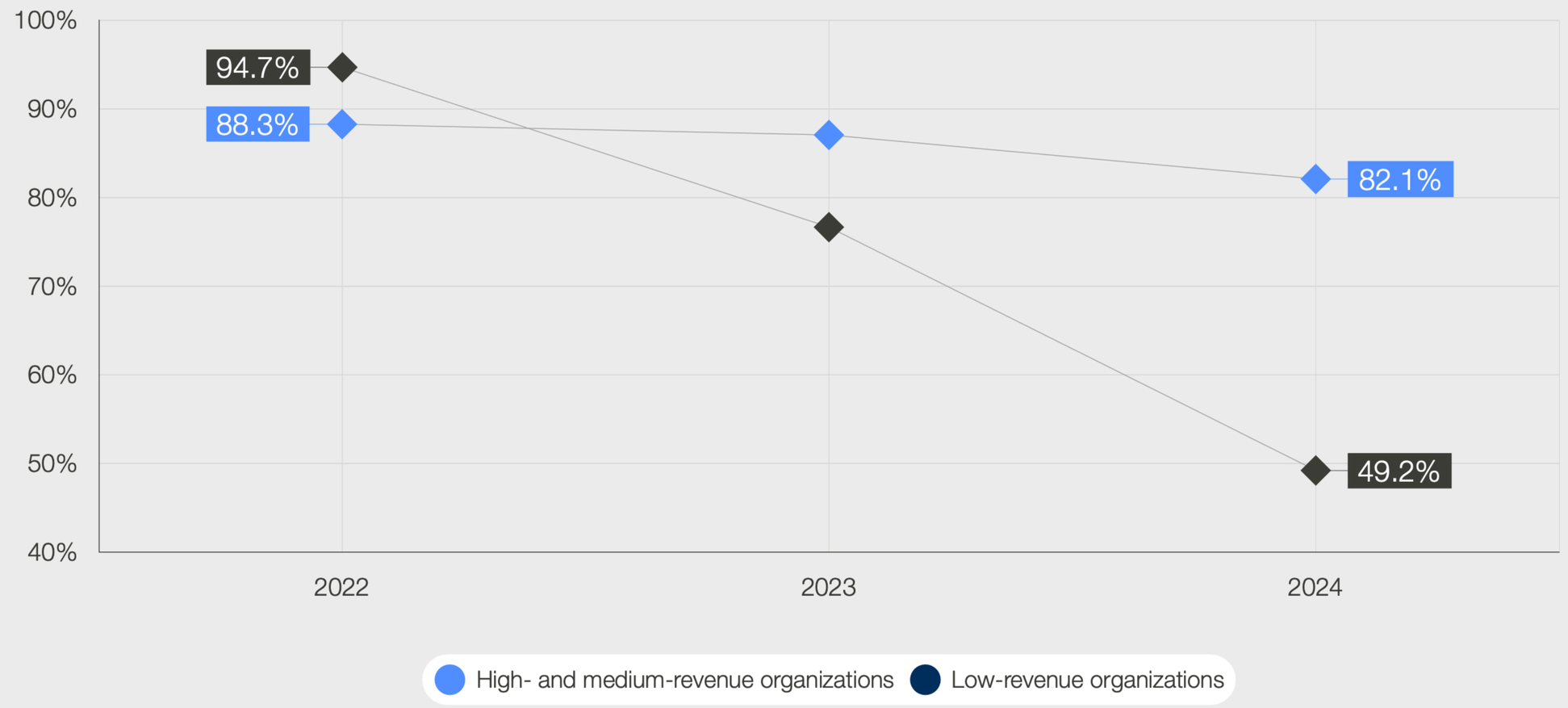
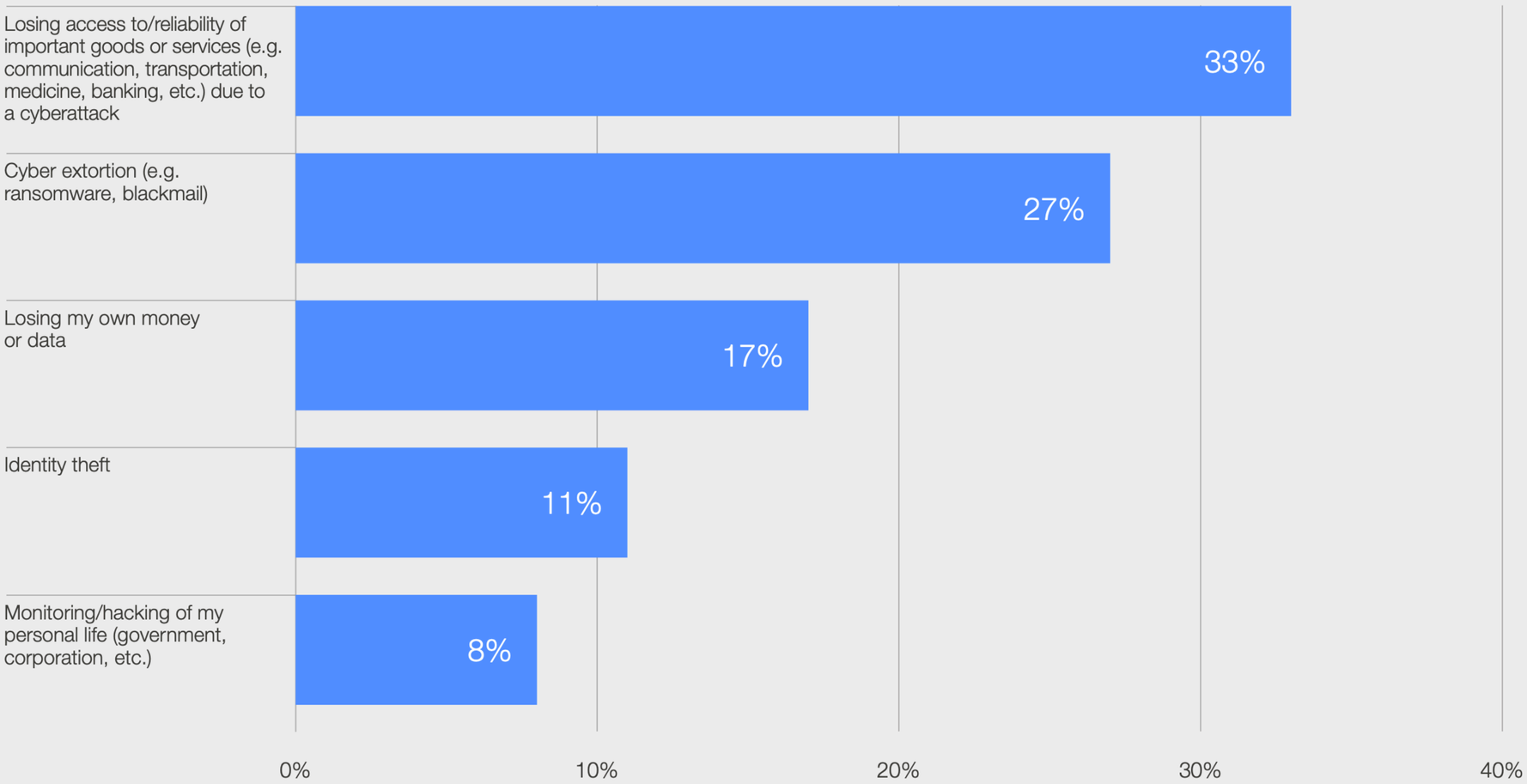


FIGURE 7 | **What keeps you up at night?**



STORMWATCH

ALLIANZ RISK BAROMETER 2024 | ALLIANZ COMMERCIAL

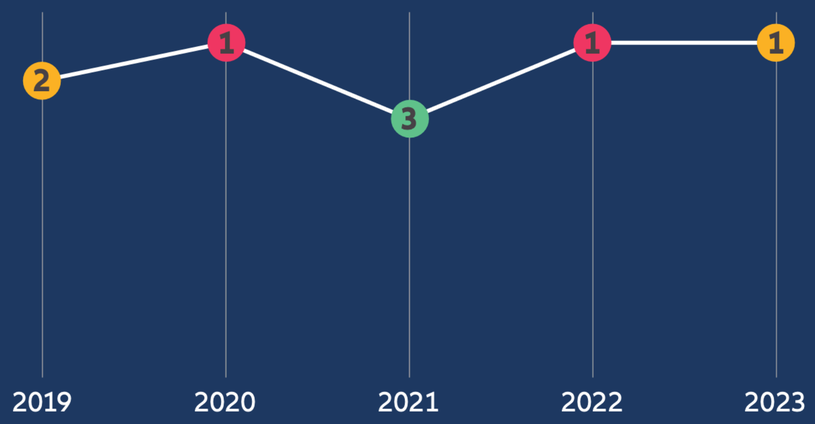
1 2 3 4 5 6 7 8 9 10

Cyber incidents

36% →

Ranking history:

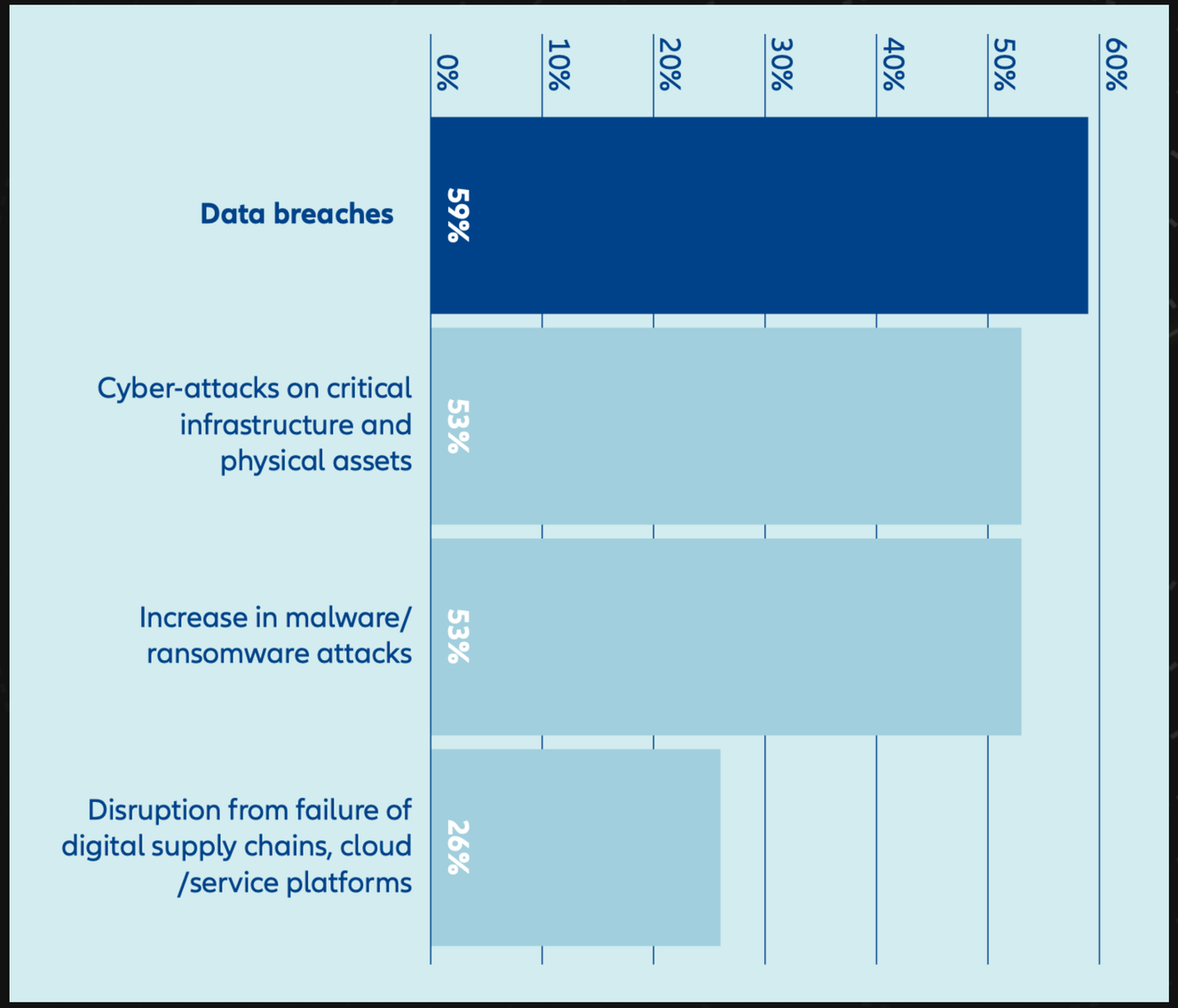
Up on previous year · No change · Down on previous year



Top risk in:

- Argentina
- Australia
- Austria
- Belgium
- France
- Germany
- India
- Italy
- Japan
- Kenya
- Mauritius
- Nigeria
- Portugal
- Switzerland
- Uganda
- UK
- USA

STORM WATCH



Which cyber exposures concern your company most?

STORMWATCH

The lion’s share of IT security budgets is currently spent on prevention with around 35% directed to detection and response.

“However, if undetected an intrusion can quickly escalate, and once data is encrypted and / or stolen, the costs snowball – as much as 1,000 times higher than if an incident is detected and contained early.

*The difference between a €20,000 loss turning into a **€20mn** one,”*

explains Michael Daum, Global Head of Cyber Claims at Allianz Commercial.

STORM WATCH

joeavanzato / LogBoost

Type / to search

Code Issues Pull requests Actions Projects Wiki Security Insights

LogBoost Public

https://github.com/joeavanzato/LogBoost

Fork 0 Star 60

main 1 Branch 3 Tags Go to file t Code

README MIT license

LogBoost

What is it?

LogBoost is a command-line utility originally designed to enrich IP addresses in CSV files with ASN, Country and City information provided by the freely available MaxMind GeoLite2 DBs.

LogBoost can parse and convert a variety of structured and semi-structured log formats to CSV while simultaneously enriching detected IP addresses, including JSON, IIS, W3C, ELF, CLF, CEF, KV, SYSLOG.

About

Convert a variety of log formats to CSV while enriching detected IPs with Geolocation, Domain, ASN, DNS and Threat Indicator matches.

osint geolocation incident-response dfir concurrent log-parser threat-intelligence log-parsing log-process log-enrich

Readme
MIT license
Activity
60 stars
2 watching
0 forks
Report repository

Releases 3

v1.2.0 Latest
last month

+ 2 releases

Packages

No packages published

STORMWATCH

Shameless Self-Promotion

CVE-2023-34048: VMWare vCenter

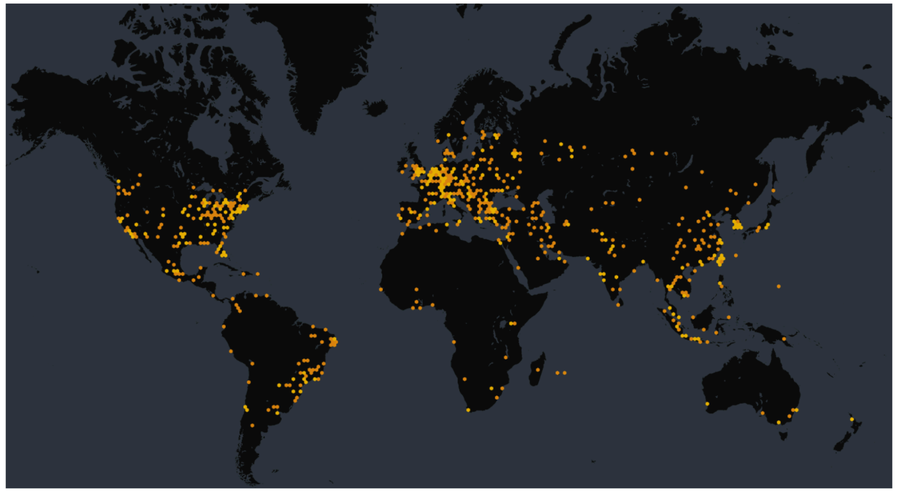
https://censys.com/cve-2023-34048-vmware-vcenter/

SHARE

JANUARY 22, 2024

Tags:

Rapid Response | Research



VMWare vCenter (web-ui) hosts on the Internet

Summary

- Mandiant recently reported that an advanced espionage hacking group had been observed exploiting CVE-2023-34048 (a vulnerability in vCenter's DCERPC implementation) in the wild since 2021.
- Censys has observed approximately 3,541 hosts with the vCenter web administration service running; of those, only 293 hosts (8.2%) had the DCERPC service running on the same public network interface on the default port (TCP/135).
- VMWare has released several new versions to address this issue.

ABOUT THE AUTHOR

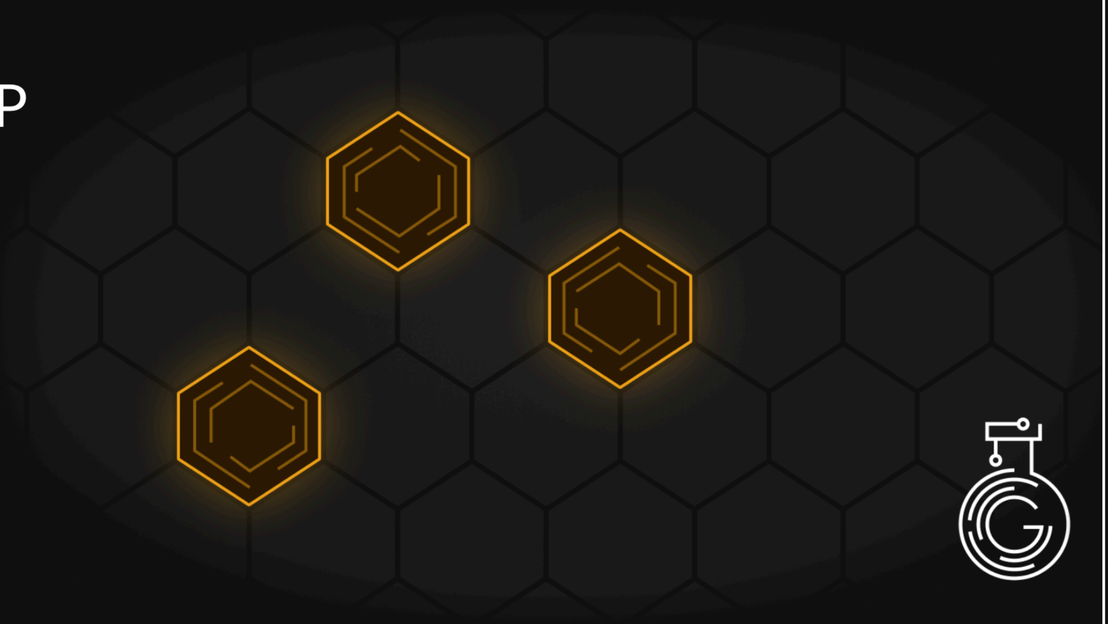
The Censys Research Team

STORMWATCH

LABS

The Confusing History of F5 BIG-IP RCE Vulnerabilities

The GreyNoise Team | January 22, 2024



https://www.greynoise.io/blog/the-confusing-history-of-f5-big-ip-rce-vulnerabilities

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

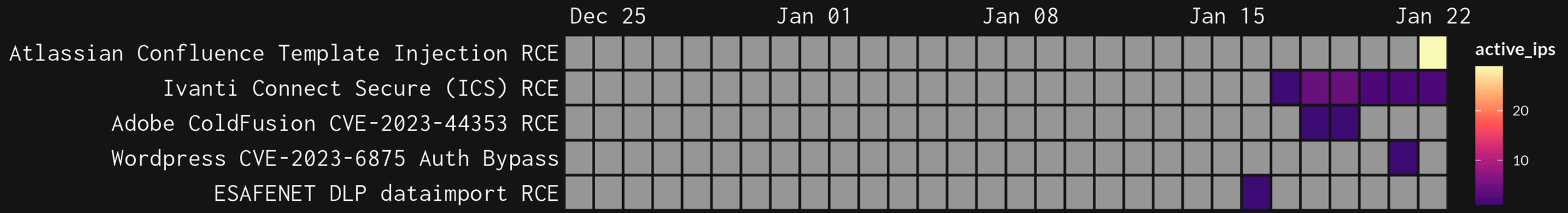
https://www.greynoise.io/resources/2023-greynoise-retrospective-internet-exploitation-report

STORMWATCH

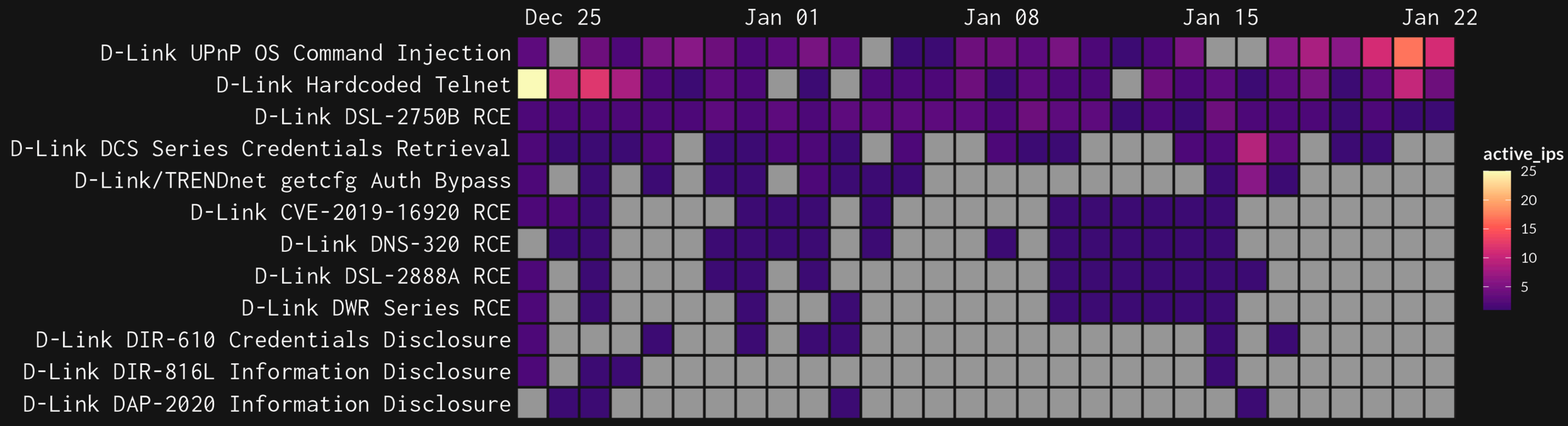
- Adobe ColdFusion CVE-2023-38203 RCE Attempt (CVE-2023-38203)
- TikiWiki Sirius jhot.php RCE Attempt (CVE-2006-4602)
- Narcissus Image Configuration RCE Attempt
- Adobe ColdFusion CVE-2023-44353 RCE Attempt (CVE-2023-44353)
- JetNexus/EdgeNexus RCE Attempt (CVE-2022-37718)
- MajorDoMo RCE attempt (CVE-2023-50917)
- WordPress LearnPress RCE Attempt (CVE-2023-6634)
- Ivanti Connect Secure (ICS) RCE Attempt (CVE-2023-46805, CVE-2024-21887)
- Atlassian Confluence Template Injection RCE Attempt (CVE-2023-22527)
- SonicOS RCE Attempt (CVE-2022-22274, CVE-2023-0656)
- ESAFENET DLP dataimport RCE
- Wordpress CVE-2023-6875 Auth Bypass Attempt (CVE-2023-6875)

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

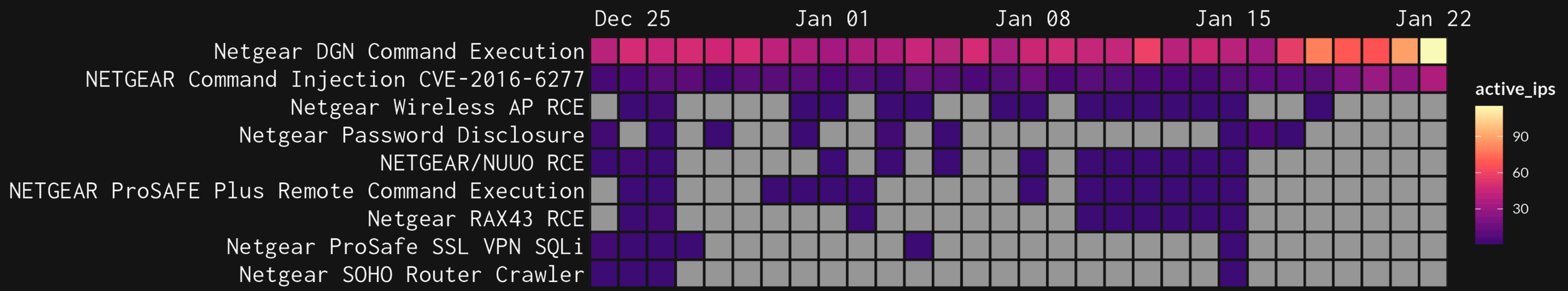
STORMWATCH


Dec 25
Jan 01
Jan 08
Jan 15
Jan 22
Atlassian Confluence Template Injection RCE
Ivanti Connect Secure (ICS) RCE
Adobe ColdFusion CVE-2023-44353 RCE
Wordpress CVE-2023-6875 Auth Bypass
ESAFENET DLP dataimport RCE
active_ips
20
10

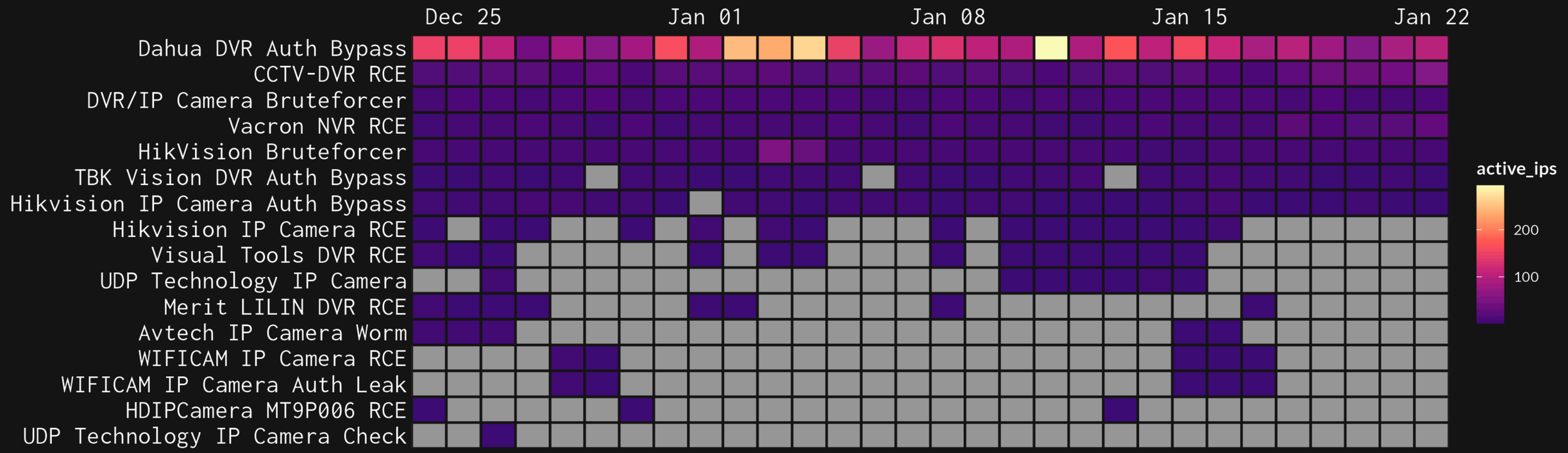
STORM WATCH


Dec 25
Jan 01
Jan 08
Jan 15
Jan 22
D-Link UPnP OS Command Injection
D-Link Hardcoded Telnet
D-Link DSL-2750B RCE
D-Link DCS Series Credentials Retrieval
D-Link/TRENDnet getcfg Auth Bypass
D-Link CVE-2019-16920 RCE
D-Link DNS-320 RCE
D-Link DSL-2888A RCE
D-Link DWR Series RCE
D-Link DIR-610 Credentials Disclosure
D-Link DIR-816L Information Disclosure
D-Link DAP-2020 Information Disclosure
active_ips
25
20
15
10
5

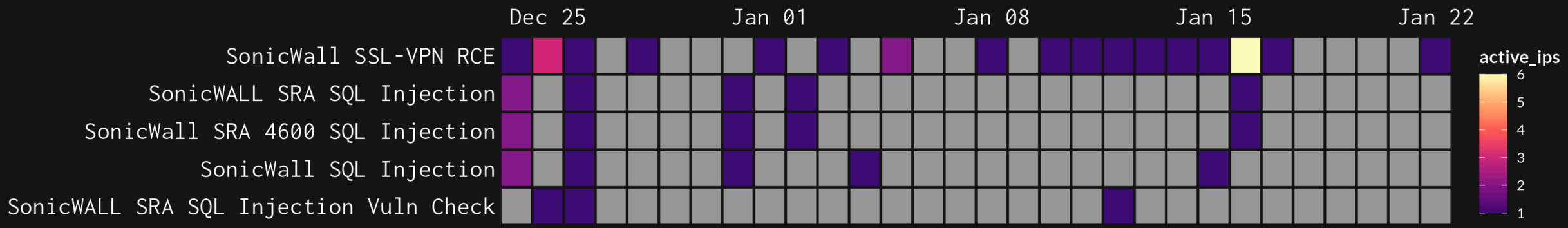
STORM WATCH


Dec 25
Jan 01
Jan 08
Jan 15
Jan 22
Netgear DGN Command Execution
NETGEAR Command Injection CVE-2016-6277
Netgear Wireless AP RCE
Netgear Password Disclosure
NETGEAR/NUUO RCE
NETGEAR ProSAFE Plus Remote Command Execution
Netgear RAX43 RCE
Netgear ProSafe SSL VPN SQLi
Netgear SOHO Router Crawler
active_ips
90
60
30

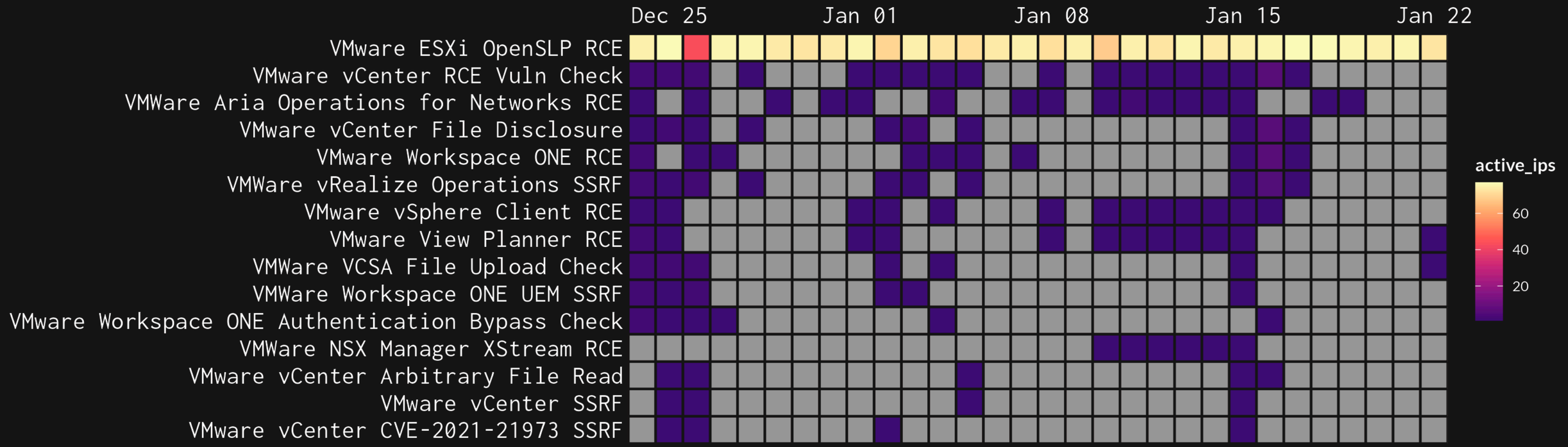
STORMWATCH


Dec 25
Jan 01
Jan 08
Jan 15
Jan 22
Dahua DVR Auth Bypass
CCTV-DVR RCE
DVR/IP Camera Bruteforcer
Vacron NVR RCE
HikVision Bruteforcer
TBK Vision DVR Auth Bypass
Hikvision IP Camera Auth Bypass
Hikvision IP Camera RCE
Visual Tools DVR RCE
UDP Technology IP Camera
Merit LILIN DVR RCE
Avtech IP Camera Worm
WIFICAM IP Camera RCE
WIFICAM IP Camera Auth Leak
HDIPCamera MT9P006 RCE
UDP Technology IP Camera Check
active_ips
200
100

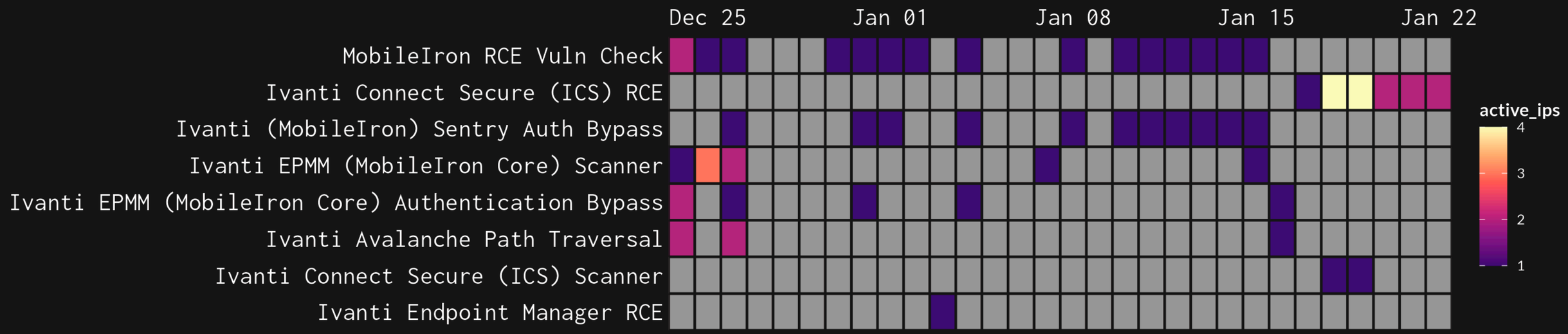
STORM WATCH


Dec 25
Jan 01
Jan 08
Jan 15
Jan 22
SonicWall SSL-VPN RCE
SonicWALL SRA SQL Injection
SonicWall SRA 4600 SQL Injection
SonicWall SQL Injection
SonicWALL SRA SQL Injection Vuln Check
active_ips
6
5
4
3
2
1

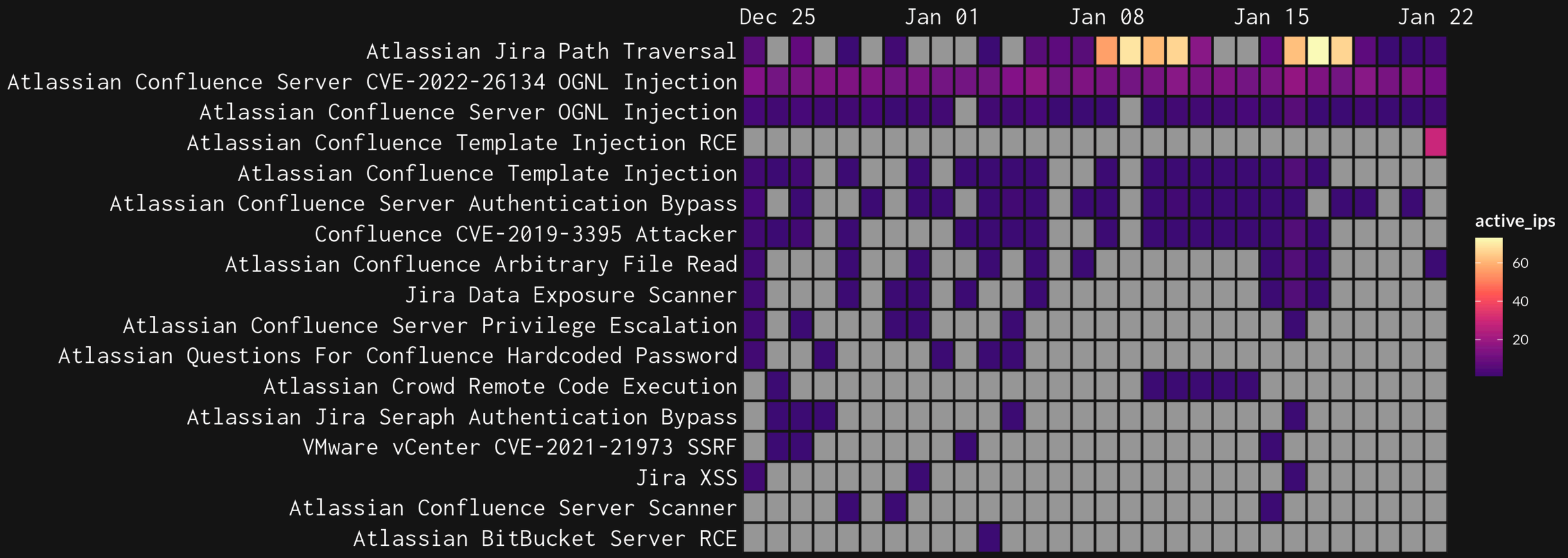
STORM WATCH


Dec 25
Jan 01
Jan 08
Jan 15
Jan 22
VMware ESXi OpenSLP RCE
VMware vCenter RCE Vuln Check
VMWare Aria Operations for Networks RCE
VMware vCenter File Disclosure
VMware Workspace ONE RCE
VMWare vRealize Operations SSRF
VMware vSphere Client RCE
VMware View Planner RCE
VMWare VCSA File Upload Check
VMWare Workspace ONE UEM SSRF
VMware Workspace ONE Authentication Bypass Check
VMWare NSX Manager XStream RCE
VMware vCenter Arbitrary File Read
VMware vCenter SSRF
VMware vCenter CVE-2021-21973 SSRF
active_ips
60
40
20

STORM WATCH


Dec 25
Jan 01
Jan 08
Jan 15
Jan 22
MobileIron RCE Vuln Check
Ivanti Connect Secure (ICS) RCE
Ivanti (MobileIron) Sentry Auth Bypass
Ivanti EPMM (MobileIron Core) Scanner
Ivanti EPMM (MobileIron Core) Authentication Bypass
Ivanti Avalanche Path Traversal
Ivanti Connect Secure (ICS) Scanner
Ivanti Endpoint Manager RCE
active_ips
4
3
2
1

STORMWATCH


Dec 25
Jan 01
Jan 08
Jan 15
Jan 22
Atlassian Jira Path Traversal
Atlassian Confluence Server CVE-2022-26134 OGNL Injection
Atlassian Confluence Server OGNL Injection
Atlassian Confluence Template Injection RCE
Atlassian Confluence Template Injection
Atlassian Confluence Server Authentication Bypass
Confluence CVE-2019-3395 Attacker
Atlassian Confluence Arbitrary File Read
Jira Data Exposure Scanner
Atlassian Confluence Server Privilege Escalation
Atlassian Questions For Confluence Hardcoded Password
Atlassian Crowd Remote Code Execution
Atlassian Jira Seraph Authentication Bypass
VMware vCenter CVE-2021-21973 SSRF
Jira XSS
Atlassian Confluence Server Scanner
Atlassian BitBucket Server RCE
active_ips
60
40
20

It Has Been

1

Days Since The
Last KEV Release

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

STORM WATCH

CVE-2018-15133: Laravel Deserialization of Untrusted Dat

CVE-2024-0519: Google Chromium V8 Out-of-Bounds Memory Access

CVE-2023-6549: Citrix NetScaler ADC and NetScaler Gateway Buffer Overflow

CVE-2023-6548: Citrix NetScaler ADC and NetScaler Gateway Code Injection

CVE-2023-35082: Ivanti Endpoint Manager Mobile (EPMM) & MobileIron Core Auth Bypass

CVE-2023-34048: VMware vCenter Server Out-of-Bounds Write

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