STORM WATCH

CYBERSECURITY NEWS

Dateline: 2024-02-20

LIKE

SUBSCRIBE

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

HIGH FIVE

THE SITE IS NOW UNDER CONTROL OF LAW ENFORCEMENT

This site is now under the control of The National Crime Agency of the UK, working in close cooperation with the FBI and the international law enforcement task force, 'Operation Cronos'.

We can confirm that Lockbit's services have been disrupted as a result of International Law Enforcement action – this is an ongoing and developing operation.

Return here for more information at:

11:30 GMT on Tuesday 20th Feb.

https://www.reuters.com/technology/cybersecurity/lockbit-cybercrime-gang-disrupted-by-international-police-operation-2024-02-19/

NCA National Crime Agency · ROCU · Metropolitan Police · EUROPOL · Politie · Kanton Zürich · Gendarmerie · SH Schleswig-Holstein · POLIISI

- 2,300 attacks since it emerged in late 2019
- Attempted to extort $70 million from Taiwanese chipmaker TSMC
- Made $91 million in 2022
- 21 percent of all known ransomware attacks from January 2023 to December 2023

- Attack on the United Kingdom’s Royal Mail
- Canadian Children’s Hospital
- Capital Health
- Industrial and Commercial Bank of China
- Fulton County, Georgia
- Alleged Extortion of TSMC

https://www.justice.gov/opa/pr/justice-department-conducts-court-authorized-disruption-botnet-controlled-russian

News

All News

Blogs

Photo Galleries

Podcasts

Press Releases

Speeches

Videos

PRESS RELEASE

Justice Department Conducts Court-Authorized Disruption of Botnet Controlled by the Russian Federation's Main Intelligence Directorate of the General Staff (GRU)

Thursday, February 15, 2024

Share >

For Immediate Release

Office of Public Affairs

A January 2024 court-authorized operation has neutralized a network of hundreds of small office/home office (SOHO) routers that GRU Military Unit 26165, also known as APT 28, Sofacy Group, Forest Blizzard, Pawn Storm, Fancy Bear, and Sednit, used to conceal and otherwise enable a variety of crimes. These crimes included vast spearphishing and similar credential

- A network of hundreds of small office/home office (SOHO) routers was neutralized in a court-authorized operation in January 2024

- The network was controlled by GRU Military Unit 26165, known by various names including APT 28 and Fancy Bear

- The operation targeted routers infected with "Moobot" malware, used by the GRU for cyber espionage

- It marks the third time since Russia's invasion of Ukraine that the U.S. has stripped Russian intelligence services of a key cyber tool

- The GRU did not create the botnet from scratch but repurposed it using Moobot malware, initially installed by non-GRU cybercriminals on Ubiquiti Edge OS routers with default passwords

- The operation involved copying and deleting stolen and malicious data from compromised routers

- It also modified routers' firewall rules to block remote management access, temporarily disrupting GRU's access

- Temporary collection of non-content routing information was enabled to expose GRU attempts to thwart the operation

STORM WATCH

CYBERSECURITY NEWS

HEADS UP

Search ARM Documentation

ARM 2023.2.3 Release Notes
ARM 2023.2.2 Release Notes
ARM 2023.2.1 Release Notes
ARM 2023.2 Release Notes
ARM 2022.4 Release Notes
ARM 2022.2 Release Notes
ARM 2021.4 Release Notes
ARM 2020.2 Release Notes
ARM 2019.4 Release Notes
ARM 9.2 Release Notes
ARM 9.1 Release Notes
ARM release history

ARM 2023.2.3 Release Notes

Release date: February 15, 2024

Access Rights Manager 2023.2.3 is a service release providing bug and security fixes for release 2023.2. For information about the 2023.2 release, including EOL notices and upgrade information, see Access Rights Manager 2023.2 Release Notes.

CVEs

SolarWinds would like to thank our Security Researchers below for reporting on the issue in a responsible manner and working with our security, product, and engineering teams to fix the vulnerability.

CVE-ID	Vulnerability Title	Description	Severity	Credit
CVE-2023-40057	SolarWinds ARM Deserialization of Untrusted Data Remote Code Execution	The SolarWinds Access Rights Manager was found to be susceptible to a Remote Code Execution Vulnerability. If exploited, this vulnerability allows an authenticated user to abuse a SolarWinds service resulting in remote code execution. We thank Trend Micro Zero Day Initiative (ZDI) for its ongoing partnership in coordinating with SolarWinds on responsible disclosure of this and other potential vulnerabilities.	9.0 Critical	Anonymous working with Trend Micro Zero Day Initiative
CVE-2024-23476	SolarWinds Access Rights Manager Directory Traversal Remote Code Execution Vulnerability	The SolarWinds Access Rights Manager (ARM) was found to be susceptible to a Directory Traversal Remote Code Execution Vulnerability. If exploited, this vulnerability allows an unauthenticated user to achieve the Remote Code Execution. We thank Trend Micro Zero Day Initiative (ZDI) for its ongoing partnership in coordinating with SolarWinds on	9.6 Critical	Anonymous working with Trend Micro Zero Day Initiative

https://documentation.solarwinds.com/en/success_center/arm/content/release_notes/arm_2023-2-3_release_notes.htm

a Remote Code Execution.

We thank Trend Micro Zero Day Initiative (ZDI) for its

Day Initiative

- CVE-2023-40057: Successful exploitation of the input validation vulnerability may allow an authenticated attacker to abuse a SolarWinds service to perform remote code execution

- CVE-2024-23476: Successful exploitation of the directory traversal vulnerability may allow an unauthenticated attacker to perform remote code execution

- CVE-2024-23479: Successful exploitation of the directory traversal vulnerability may allow an unauthenticated attacker to perform remote code execution

I-S00N/I-S00N

https://github.com/I-S00N/I-S00N/

1 Contributor

18 Issues

2k Stars

924 Forks

mttaggart/I-S00N

Anxun Shanghai (I-SOON) Data Dump Translations (PII Redacted)

https://github.com/mttaggart/I-S00N/blob/main/README-en.md

1 Contributor

0 Issues

3 Stars

2 Forks

安坂星海 Azaka 🐼 VTuber
@AzakaSekai_

Feb 18 • 47 tweets • 17 min read • Read on X

#threatintel
someone just leaked a bunch of internal Chinese government documents on GitHub

https://threadreaderapp.com/thread/1759326049262019025.html

From the looks of it, it looks like a bunch of spyware developed by the company 安洵信息

Some of these software features includes obtaining the user's Twitter email and phone number, realtime monitoring, publishing tweets on their behalf, reading DMs.

1.2.2 产品功能

- **Twitter 注册信息查询：** 平台支持根据 Twitter 账号查询注册时使用的手机号码和邮箱。
- **Twitter 账号反制：** 平台可根据用户指定链接（真实存在或是自定义链接）生成取证链接，发送给目标并诱导其点击并进行相关操作，即可实

- Shanghai Anxun is a Chinese government spyware vendor.
- Custom Remote Access Trojans (RATs) for all major operating systems, which allow remote control over infected devices.
- Tools designed to unmask social media users, likely for surveillance or intelligence-gathering purposes.
- Distributed Denial of Service (DDoS) systems, which can overwhelm targeted servers with traffic, rendering them inaccessible.
- A Tor-like device for agents working overseas, providing a secure and anonymous communication channel.
- Dedicated hardware disguised as everyday objects like power strips or external batteries, capable of compromising Wi-Fi networks.

https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-046a

CYBERSECURITY ADVISORY

Threat Actor Leverages Compromised Account of Former Employee to Access State Government Organization

Release Date: February 15, 2024

Alert Code: AA24-046A

RELATED TOPICS: CYBER THREATS AND ADVISORIES, INCIDENT DETECTION, RESPONSE, AND PREVENTION, MALWARE, PHISHING, AND RANSOMWARE

ACTIONS TO TAKE TODAY TO MITIGATE MALICIOUS CYBER ACTIVITY:

1. Continuously remove and disable accounts and groups from the enterprise that are no longer needed, especially privileged accounts.
2. Enable and enforce multifactor authentication with strong passwords.
3. Store credentials in a secure manner, such as with a credential manager, vault, or other privilege account

A state government organization was notified that documents containing host and user information, including metadata, were posted on a dark web brokerage site.

Compromised account used to access a state government organization.

The incident involved the compromise through network administrator credentials of a former employee, which allowed the threat actor to successfully authenticate to an internal virtual private network (VPN) access point.

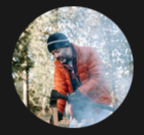
The advisory provides network defenders with the tactics, techniques, and procedures (TTPs) utilized by a threat actor and methods to protect against similar exploitation.

STORM WATCH

CYBERSECURITY NEWS

CYBER SPOTLIGHT

Detail



Tyson, Chicken Rancher 🐓
@tsupasat@infosec.ex...

Soooo ... that integrity checker tool that Ivanti wants customers to use to detect compromise? It doesn't scan more than a dozen directories including /data, /etc, /tmp, and /var. As a test of what was possible, @n0x08 installed the Sliver C2 tool in /data and ran the integrity checker tool and it passed. Patched Ivanti VPNs could very well still be compromised even if the integrity checker tool gave them an all-clear.

We also found numerous extremely old software packages, including a Linux kernel that was EOL in 2020 (CentOS 6.4). Yikes!

eclypsium.com/blog/flatlined-a...

#ivanti #connectsecure #connectaround

2 19

Feb 15, 2024 at 12:27

https://infosec.exchange/@tsupasat/111936670855414515

https://eclypsium.com/blog/flatlined-analyzing-pulse-secure-firmware-and-bypassing-integrity-checking/

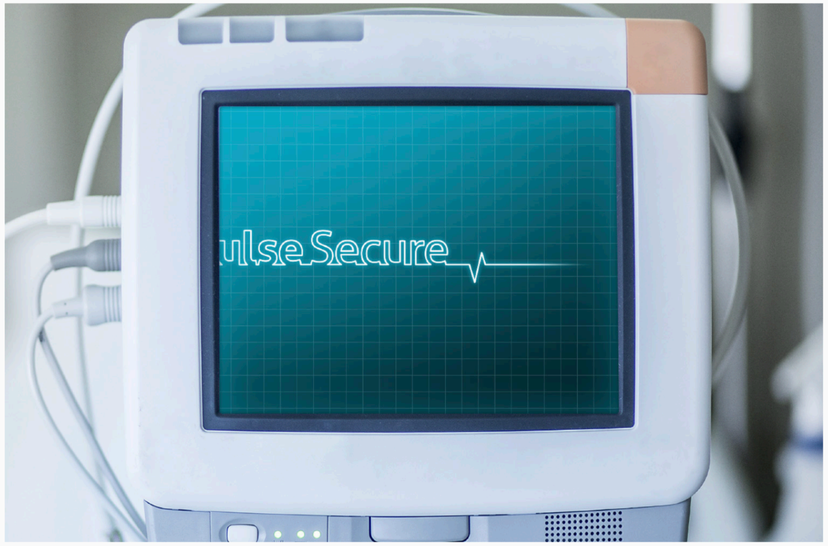
eclypsium

PLATFORM SOLUTIONS RESOURCES RESEARCH COMPANY GET A DEMO TAKE A TOUR

BLOG

FLATLINED: ANALYZING PULSE SECURE FIRMWARE AND BYPASSING INTEGRITY CHECKING

By: Eclypsium | February 15, 2024



Pulse Secure runs an 11-year-old version of Linux which hasn't been supported since November 2020

- Linux kernel 2.6.32 (end of life in February 2016)
- OpenSSL 1.0.2n (December 2017)
- Python 2.6.6 (August 2010)
- Perl v5.6.1 built for i386-linux (not x64, April 2001)
- Bash 4.1.2 which, surprisingly, has been patched for Shellshock
- A number of outdated libraries with known CVEs and exploits as seen below

“There’s also a huge security hole in the logic of their script: it excludes over a dozen directories from being scanned, meaning an attacker could theoretically leave their persistent C2 implants in one of these paths and the device will still pass the integrity check! There is a persistent storage partition mounted as /data on the device and this entire partition is excluded as are /etc, /tmp, /var and others. Ivanti uses the /home partition to store all their product specific daemons and configuration files and this is scanned by their tool, in theory, this might detect attackers modifying system files but it does leave a large post-exploitation persistence surface for attackers.”

The vast majority of the Pulse Secure GUI is written in Perl

O_o

https://www.ntia.gov/page/software-bill-materials

SOFTWARE BILL OF MATERIALS

A "Software Bill of Materials" (SBOM) is a nested inventory for software, a list of ingredients that make up software components. The following documents were drafted by stakeholders in an open and transparent process to address transparency around software components, and were approved by a consensus of participating stakeholders. More information about the NTIA multistakeholder process on software component transparency is available here.

Introduction to SBOM

SBOM at a Glance (2021)
This resource provides an introduction to the practice of SBOM, supporting literature, and the pivotal role SBOMs play in providing much-needed transparency for the software supply chain. (Japanese translation)

SBOM FAQ (2021)
This document outlines detailed information, benefits, and commonly asked questions.

SBOM Myths vs. Facts (2021)
This document is intended to help the reader to understand and dispel common, often sincere myths and misconceptions about SBOM.

SBOM Explainer Videos on YouTube (2020-2021)
This collection of videos provides a wide range of information about SBOM including introductory concepts, technical

STORM WATCH

CYBERSECURITY NEWS

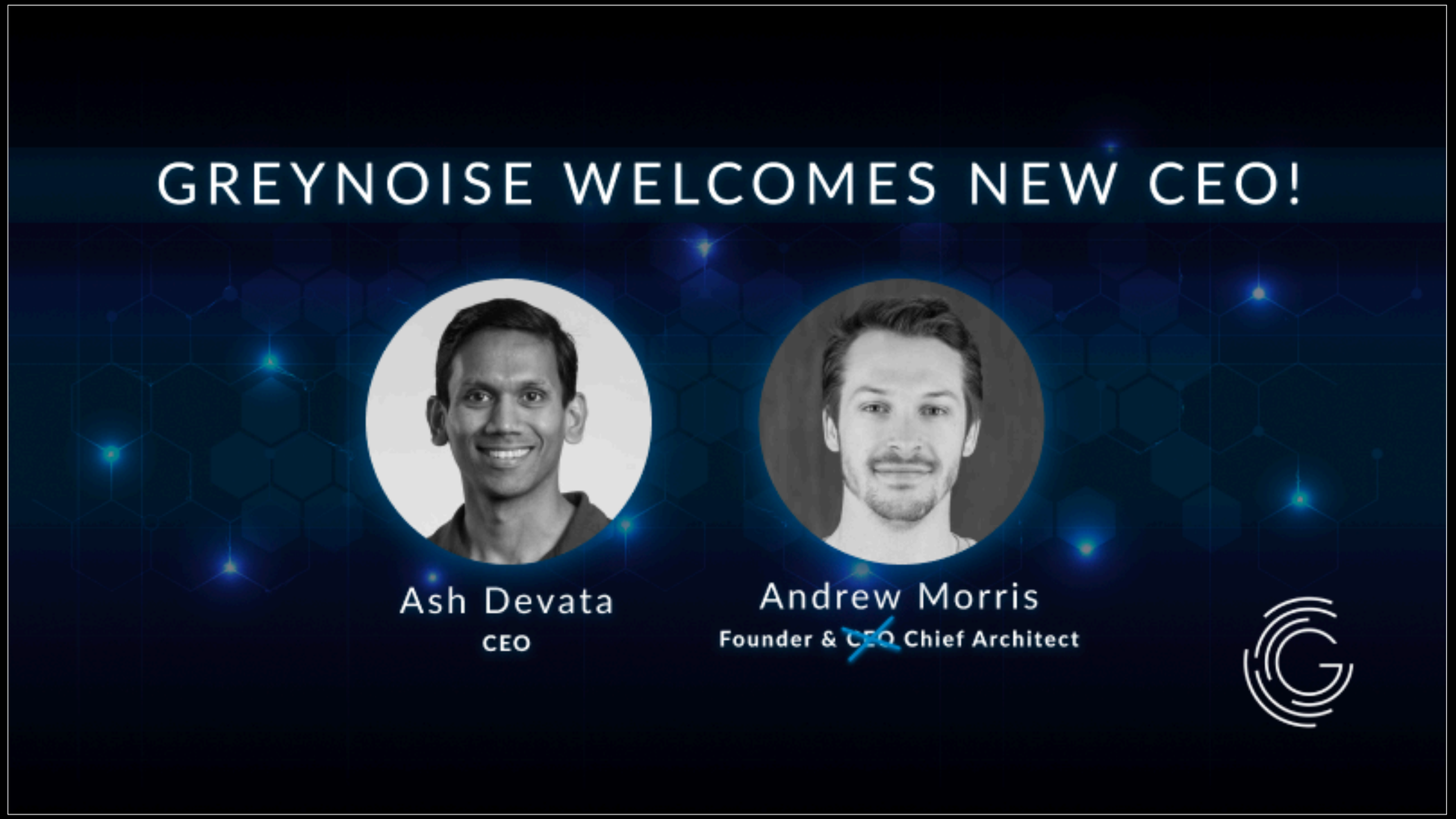
REZONATE

https://www.rezonate.io/blog/top-10-features-to-enhance-your-okta-security-posture/

STORM WATCH

CYBERSECURITY NEWS

SHAMELESS SELF-PROMOTION



https://www.greynoise.io/blog/weve-hired-ash-devata-as-ceo-at-greynoise-and-i-get-my-dream-job

https://www.labs.greynoise.io//grimoire/2024-02-what-is-this-old-ivanti-exploit/

Code injection or backdoor: A new look at Ivanti's CVE-2021-44529

In 2021, Ivanti patched a vulnerability that they called "code injection". Rumors say it was a backdoor in an open source project. Let's find out what actually happened!

IVANTI BACKDOOR PHP CVE-2021-44529 CSRF-MAGIC

AUTHOR
Ron Bowes

PUBLISHED
February 15, 2024

This is yet another, "Ron got nerdsniped by a thing and wasted enough time that he needs something to show for it" blog. Which, come to think of it, are pretty much all my blogs. :)

Recently, a tweet from Steven Seeley (Mr_Me) caught my eye - an exploit for an issue mentioned in a tweet from nearly two years ago. The tweets link to an Ivanti Endpoint Manager advisory from 2021 and an exploit from 2022. The vulnerability is identified as CVE-2021-44529. I wasn't aware of any of this, but I immediately got curious!

While finalizing this blog, I found this AttackerKB post from h00die-gr3y that covers the exact same material in roughly the same way. So if you don't like my writing, go read that one :)

The software

In the thread, Tuan Anh Nguyen (@haxor31337) mentioned it's a backdoor in csrf-magic. I googled `csrf-magic backdoor`, but found nothing except for that tweet. The tweet links to the project, but the project is dead and gone.

Every once in awhile, I remember that the Way Back Machine exists and is an invaluable

STORM WATCH

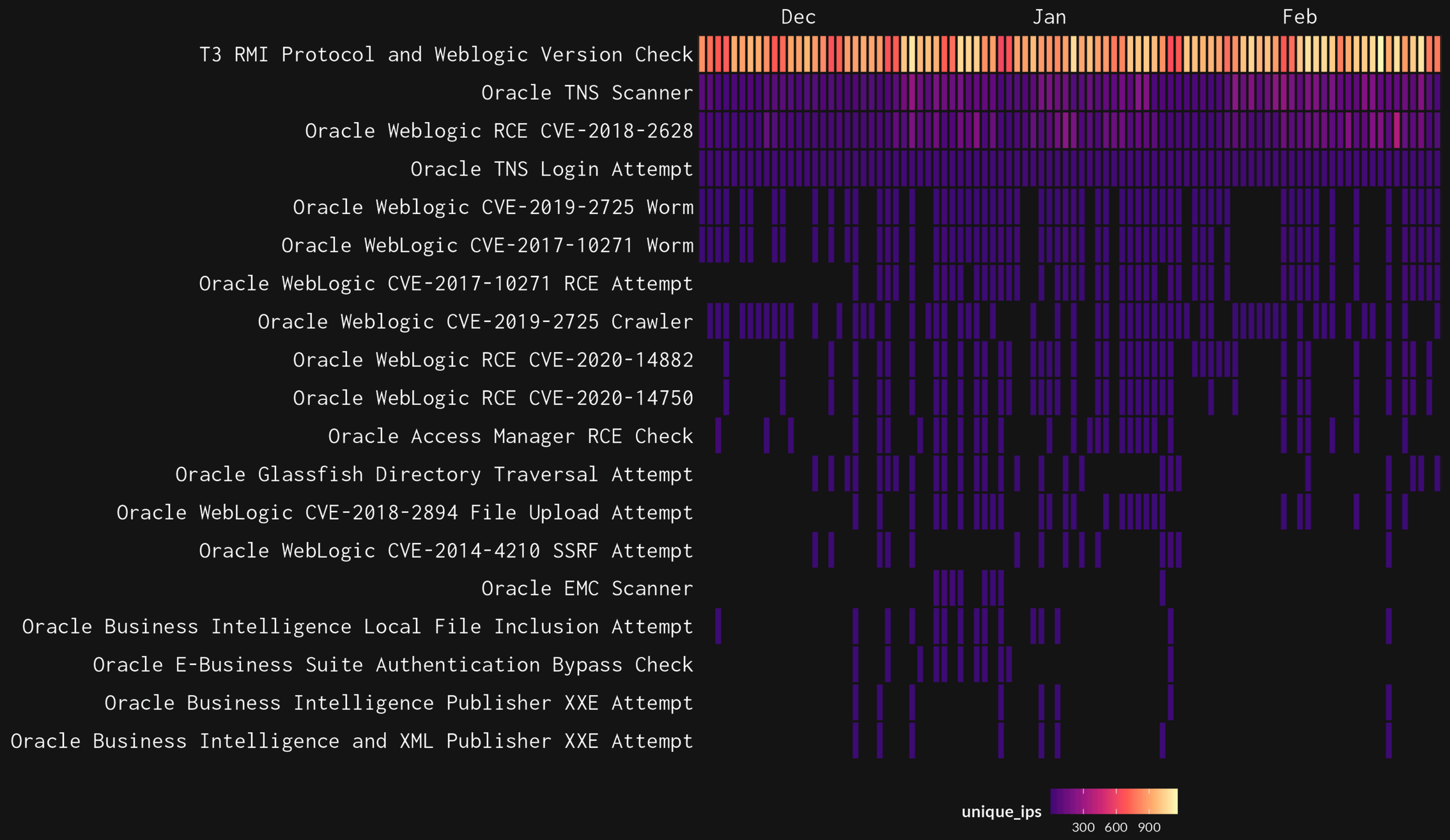
CYBERSECURITY NEWS

TAG ROUND-UP

- Yunabao Cloud Box FastJson RCE Attempt
- QNAP QTS Command Injection CVE-2023-47218 Attempt (CVE-2023-33617)
- Ivanti Connect Secure XXE CVE-2024-22024 Attempt (CVE-2024-22024)
- IBM Maximo Asset Management Information Disclosure Attempt (CVE-2020-4463)
- Hadoop Scanner
- HP SiteScope issueSiebelCmd RCE Attempt (CVE-2013-4835)
- Wordpress SupportCandy SQLi Attempt

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


Jan 22
Jan 29
Feb 05
Feb 12
Feb 19
Hadoop Scanner
Ivanti Connect Secure XXE CVE-2024-22024
active_ips
50
100
150


Dec
Jan
Feb
T3 RMI Protocol and Weblogic Version Check
Oracle TNS Scanner
Oracle Weblogic RCE CVE-2018-2628
Oracle TNS Login Attempt
Oracle Weblogic CVE-2019-2725 Worm
Oracle WebLogic CVE-2017-10271 Worm
Oracle WebLogic CVE-2017-10271 RCE Attempt
Oracle Weblogic CVE-2019-2725 Crawler
Oracle WebLogic RCE CVE-2020-14882
Oracle WebLogic RCE CVE-2020-14750
Oracle Access Manager RCE Check
Oracle Glassfish Directory Traversal Attempt
Oracle WebLogic CVE-2018-2894 File Upload Attempt
Oracle WebLogic CVE-2014-4210 SSRF Attempt
Oracle EMC Scanner
Oracle Business Intelligence Local File Inclusion Attempt
Oracle E-Business Suite Authentication Bypass Check
Oracle Business Intelligence Publisher XXE Attempt
Oracle Business Intelligence and XML Publisher XXE Attempt
unique_ips
300 600 900

WE NEED

TO TALK

ABOUT

KEV

It Has Been

5

Days Since The
Last KEV Release

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

CVE-2024-21412: Microsoft Windows Internet Shortcut Files Security Feature Bypass

CVE-2024-21351: Microsoft Windows SmartScreen Security Feature Bypass

CVE-2020-3259: Cisco ASA and FTD Information Disclosure

CVE-2024-21410: Microsoft Exchange Server Privilege Escalation

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