Daily Cyber Headlines

Daily Cyber Headlines | TLP:WHITE | Alert ID : 94a6222e | Oct 29, 2024, 07:40 AM

Today's Headlines:

Leading Story

- US Says Chinese Hackers Breached Multiple Telecom Providers

Data Breaches & Data Leaks

- [HANDALA] - Ransomware Victim: AGAS
- Free, France's Second Largest ISP, Confirms Data Breach After Leak

Cyber Crimes & Incidents

- HC3 Warns of Scattered Spider Hackers Leveraging AI, Social Engineering to Infiltrate Healthcare, Other Sectors

Vulnerabilities & Exploits

- Grafana Vulnerability CVE-2024-9264: PoC Exploit Released for 9.9-Rated Critical Flaw

Trends & Reports

- BeaverTail Malware Resurfaces in Malicious Npm Packages Targeting Developers

Privacy, Legal & Regulatory

- Four REvil Ransomware Group Members Sentenced To Prison In Russia

Upcoming Health-ISAC Events

- Global Monthly Threat Brief
  - Americas – October 29, 2024, 12:00-01:00 PM ET
  - European – October 30, 2024, 03:00-04:00 PM CET

- T-SIG Webinar for SMB Members – November 14, 2024 at 11:30 AM ET
- Fall Americas Summit, Phoenix, Arizona - December 2-6, 2024

Additional Information

Leading Story

U.S. Says Chinese Hackers Breached Multiple Telecom Providers

Summary

- FBI and CISA disclose that Chinese threat actors compromised enterprise telecommunication service providers in the United States.

Analysis & Action

Recently, the FBI and CISA distributed a joint statement regarding Chinese threat actors breaching U.S. telecommunications service providers.

The People's Republic of China was cited as the source of the activity. Investigations were launched regarding the unauthorized access, other potential targets were proactively alerted, and the breached entities were informed.

In early October, Chinese threat actors tracked as Salt Typhoon were identified in an activity where multiple U.S. broadband providers, including Verizon, AT&T, and Lumen Technologies, were breached. The threat actors' objectives were to gather information and gain access to a communications interception system used for maintaining lawful crime investigation requests by authorities. It is important that organizations remain vigilant to attacks in other sectors as potential fallout may have security implications with a nexus to healthcare.

Data Breaches & Data Leaks

[HANDALA] - Ransomware Victim: AGAS

Summary

- A large security breach of AGAS, a cloud service and cybersecurity sector provider, was detailed in a recent ransomware leak page.

Analysis & Action

The leak page details information on the attack process and the access gained during the attacks, identifying the threat actor who penetrated AGAS systems as the Handala Hack Team.

A detailed analysis showed once the team was able to penetrate AGAS systems, they gained access to primary storage and an additional 74 servers. This breach led to 18 terabytes of customer data affiliated with over 500 organizations, including those with government relations. The page boasts a warning regarding a data leak that is impending at this time, noting the payments made by individuals for the security services, only to face a data breach as a result. Additionally, images related to the breach are posted on the page. As of now, no links for downloads are available on the page, but the impending risk that the leak holds for organizations is considered to be significant.

Health-ISAC recommends that its members update their software regularly to protect their systems against recent threats. Additionally, encrypting data can help prevent leaks, and data loss prevention tools can be used to identify policy violations.

Free, France's Second Largest ISP, Confirms Data Breach After Leak

Summary

- Threat actors breached the internet service provider (ISP) Free over the weekend, compromising customers' personal information.

Analysis & Action

Over the weekend, threat actors breached France's second-largest internet service provider, Free, stealing customers' personal information. According to the internet service provider, no operational impact was observed; however, the threat actor targeted a management tool exposing subscribers' data. The threat actors did not access customer passwords, bank card information, or communications content.

The stolen data, however, is now being auctioned on the dark web site BreachForums. The post claims the data breach impacted 19.2 million customers and contained over 5.11 million IBAN numbers. The threat actor has also included several pieces of evidence to prove the legitimacy of the data breach, including a sample of the stolen data, screenshots, and database headers.

The internet service provider intends to notify those impacted by the data breach via email and states they have taken all necessary steps to remediate the attack as well as bolster their information systems. Health-ISAC recommends that organizations ensure that appropriate security measures are being used to protect sensitive data and that monitoring tools are in place to quickly identify suspicious activity.

Cyber Crimes & Incidents

HC3 Warns of Scattered Spider Hackers Leveraging AI, Social Engineering to Infiltrate Healthcare, Other Sectors

Summary

- A threat actor profile has been released on Scattered Spider, identifying its financial motives stemming from 2022.

Analysis & Action

The threat actor, the Scattered Spider, goes by many names, including Octo Tempest, Roasted 0ktapus, Scatter Swine, and Muddled Libra. The group mainly involves data extortion and other activities. Members are believed to be between the ages of 19 and 22.

The threat group targets several industries, including healthcare. In their attacks, they leverage tools that are publicly available and legitimate along with malware to intrude on services; there have been a number of identified ransomware variants as well. Additionally, the threat actor has used voice phishing, using AI to spoof the voices of victims to gain access to organizations. In Q2 2024, the threat actor added RansomHub and Qilin, as they are now considered to be experts in social engineering along with BlackCat/ALPHV ransomware. The group has followed through with successful high-profile breaches due to this, evolving TTPs, and evading detection strategies.

Since an analysis of the threat actor, a number of mitigation strategies have been brought to the industry's attention to combat the social engineering group. Amongst these are the implementation of WebAuth authentication or the use of Public Key Infrastructure-based Multifactor Authentication. Additionally, it is recommended that strict limits be placed on Remote Desktop Protocol and other similar services.

Vulnerabilities & Exploits

Grafana Vulnerability CVE-2024-9264: PoC Exploit Released for 9.9-Rated Critical Flaw

Summary

- Technical details and proof-of-concept release for exploit CVE-202409264, a critical vulnerability affecting multiple versions.

Analysis & Action

The vulnerability marked CVE-2024-9264 lies within Grafana, an open-source multi-platform analytics and visualization tool. The tool is often used to monitor a system's health and analyze system trends via data trends.

The vulnerability has since been detected to affect version 11.0.x, 11.1.x, and 11.2.x exploiting the systems, commanding local file inclusion and injection risks. The vulnerability has been attributed a critical CVSS score of 9.9, allowing threat actors with permission as viewers to utilize SQL expression features maliciously. The source of the vulnerability was identified to be within SQL expressions to give users new capabilities. The risks of the feature, however, allowed attacks to give SQL commands that would execute and target data that was formatted within DataFrames.

Threat actors could expose sensitive files or execute remote code against their intended targets with these methods. At this time, the vulnerability is dependent on a few factors. However, viewer access must be gained, DuckDB must be installed and configured, and SQL expressions must be introduced to actively take advantage of the flaw. The proof of concept mainly shows how threat actors can use read_csv_auto() to access critical systems. Recent releases by Grafana have addressed the vulnerability, urging users to update it immediately.

Health-ISAC recommends that its members update their systems with the latest patches to prevent similar vulnerabilities from being exploited. Additionally, securing and monitoring your network can help prevent unauthorized system access.

Trends & Reports

BeaverTail Malware Resurfaces in Malicious npm Packages Targeting Developers

Summary

- BeaverTail malware has returned and has been observed targeting developers with malicious npm packages.

Analysis & Action

A trio of malicious npm packages containing BeaverTail malware were published to the npm registry in September 2024. The npm packages were discovered to contain the malware, which is a JavaScript downloader and information stealer linked to an ongoing North Korean campaign, which was identified as Contagious Interview.

The malicious packages, identified as passports-js, bcrypts-js, and blockscan-api have since been removed for download from the npm registry. Of the three packages, blockscan-api accounted for the most downloads, with passports-js as a close second, and bcrypts-js with the least amount. The packages used were a part of a yearlong-campaign initiated by the Democratic People's Republic of Korea (DPRK) whose objectives include tricking developers into downloading malicious pages or nefarious video conferencing applications under the guise of a coding test.

The malicious campaign has been active since November 2023 and highlights threat actors' resilience and sophistication behind operations levied to compromise targets. Health-ISAC recommends that organizations remain vigilant to malicious activity observed across the threat landscape to ensure accurate prioritization of continuous intelligence monitoring and adaptation. This involves actively tracking emerging threats, analyzing threat actors' TTPs, and updating security measures accordingly.

Privacy, Legal & Regulatory

Four REvil Ransomware Group Members Sentenced To Prison In Russia

Summary

- Russia has looked to crack down on threat actors REvil and Sodinokibi, sentencing four members to prison after 2022 arrests.

Analysis & Action

Two years ago, in January 2022, Russia stated its intent to crack down on threat actors REvil and Sodinokibi. This came after the United States' operation to disrupt the threat actor after several high-profile attacks.

After Russia's announcement of the crackdown, eight individuals were detained and faced charges in court. However, we are now seeing the results of those detainments, with the court deciding to prosecute the threat actors separately, sentencing four last week. However, the threat actors have not been prosecuted for their crimes in the US. Instead, they have been charged for malware distribution and illegal use of payment cards. The threat actors were known for this; however, they stole information about victims' payment cards, though the victims chose not to press charges. In light of these sentences, however, questions loom on why the Russian government chose not to utilize the threat actors' skills for their own benefit, making them a part of Russian cyber operations against Ukraine.

As malware and phishing attacks become increasingly common for threat actors and their attack patterns, protective strategies remain crucial. Health-ISAC recommends that its members issue the most up-to-date patches and utilize trusted security software.

Health-ISAC Cyber Threat Level

On October 17, 2024, the Health-ISAC Threat Intelligence Committee (TIC) evaluated the current Cyber Threat Level and collectively decided to raise the Cyber Threat Level to **Yellow (Elevated)**. The Threat Level of Yellow (Elevated) is due to threats from:

The Threat Level of Yellow (Elevated) is due to threats from elections-related smishing campaigns, DPRK remote worker activity, potential repercussions of recent activity in the Middle East, commodity malware, and a recent uptick in ransomware events.

For more information about the Health-ISAC Cyber Threat Level, including definitions and response guidelines for each of the alert levels, please review the Threat Advisory System.

You must have Cyware Access to reach the Threat Advisory System document. Contact membership@h-isac.org for access to Cyware.

Report Source(s)

Health-ISAC

Reference | References

Bleeping Computer
Bleeping Computer
industrialcyber
The Hacker News
Security Online
Security Week
Red Packet Security

Tags

BeaverTail Malware, Grafana Vulnerability, Handala Ransomware, Scattered Spider, Chinese Hackers, REvil ransomware, Data Breaches

Share Threat Intel:

For guidance on sharing indicators with Health-ISAC via HTIP, please visit the Knowledge Base article "HTIP - Share Threat Intel" here.

The "Share Threat Intel" feature allows for attributed or anonymous sharing across ISACs and other cybersecurity-related entities.

Turn off Categories:

For guidance on disabling alert categories, please visit the Knowledge Base article "HTIP Alert Categories" here.

Access the Health-ISAC Threat Intelligence Portal:

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments:

Please email us at toc@h-isac.org