Daily Cyber Headlines

Daily Cyber Headlines | TLP:WHITE | Alert ID : 3735a444 | Oct 18, 2024, 07:48 AM

Today's Headlines:

Leading Story

- Organization Extorted Following Hiring of North Korean Remote IT Worker

Data Breaches & Data Leaks

- Nothing to Report

Cyber Crimes & Incidents

- Members of Threat Actor Group Charged In Ransomware Attacks On Hospitals And DDoS
- DDoS Attacks Against Japan

Vulnerabilities & Exploits

- F5 BIG-IP Updates Patch High-Severity Elevation of Privilege Vulnerability
- Fake Google Meet Pages Deliver Infostealers

Trends & Reports

- Google: 70% of Exploited Flaws Disclosed In 2023 were Zero-Days

Privacy, Legal & Regulatory

- Brazilian Police Arrest Notorious Threat Actor USDoD

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

Organization Extorted Following Hiring of North Korean Remote IT Worker

Summary

- An unidentified firm has fallen victim to a cyberattack after unknowingly hiring a cybercriminal from North Korea

Analysis & Action

Organizations face a growing threat posed by North Korean operatives. A new case has exemplified an unknown insider threat in a recent cyberattack. The firm that faced the attack has yet to be identified but is known to be based in either Australia, the US, or the UK.

The cybercriminal was hired by the firm as a remote IT worker after submitting a false history of his employment and personal details. After being hired as a contractor, he received access to the company's network remotely. Using his remote access, he then downloaded critical information and data, demanding to be paid a sum of six figures in cryptocurrency for the information to not be sold or published.

This incident highlights a larger issue: fraudulent North Korean IT workers continue to disguise themselves as experienced IT workers. A number of companies have unknowingly hired North Koreans who misrepresent their work experience and identities, following the same process of using fake profiles.

North Korean threat actors continue to exploit the convenience of remote work opportunities, highlighting the need for vigilance regarding the hiring of new staff members. To prevent similar incidents, Health-ISAC recommends conducting thorough background checks and verifying personnel's identities before allowing them to begin the onboarding process.

Data Breaches & Data Leaks

- Nothing to Report

Cyber Crimes & Incidents

Members of Threat Actor Group Charged In Ransomware Attacks On Hospitals And DDoS

Summary

- Two brothers, both members of Anonymous Sudan, have been charged due to their hospital cyberattacks.

Analysis & Action

The threat actor, Anonymous Sudan is notorious for its cyberattacks, distributing over 35,000 DDoS attacks on a number of organizations. These organizations include hospitals, mainly in the United States, India, Denmark, and Sweden. Investigations discovered that attacks were using Skynet botnet network along with Godzilla botnet.

The brothers' past of committing cyber attacks is also a part of the case, having disabled rocket attacks back in October of last year. The brothers also committed attacks on Los Angeles based health systems, intentionally targeting hospitals to cause harm to its patients. In response to their attacks, hospitals were forced to move their patients to different facilities. The DDoS attack by threat actor Anonymous Sudan led to a medical center shutting down temporarily as they dealt with the issues posed by the attacks for a total of 8 hours. In all, Anonymous Sudan has cost over $10 million to victims. The brothers are now in custody at this time as they are to face some of the harshest charges to be brought against individuals that have committed DDoS attacks in the past.

DDoS attacks are a common strategy used by threat actors to disrupt systems within facilities, highlighting the protective measures needed to prevent similar attacks. Health-ISAC recommends its members issue flood guards to protect against DDoS attacks, blocking malicious traffic whenever detected.

DDoS Attacks Against Japan

Summary

- Threat actor tandem, NoName057 and Russian Cyber Army team issued a DDoS attack targeting Japanese organizations in response to Japan's call for more engagement in alliances led by the US military.

Analysis & Action

The targeted attacks by threat actors NoName057 and Russian Cyber Army Team took place on October 14, putting its focus towards manufacturing, logistics, governmental, and political organizations. These attacks are believed to be sparked from an October 11 interview publishing regarding Japan and their increase in militarization.

Three days later, the threat actors used several direct path DDoS attack vectors that were not under any spoofing. The origin of these attack vectors were mainly from often used nuisance networks, VPN networks, and cloud providers. As far as the distribution of the attacks goes, half of attacks were aimed at the Manufacturing & Logistics sector, this was intentionally done to affect both harbors and the building of ships. The second most substantial of the attacks were aimed at the government, in which social and political organizations were targeted, including Japan's prime minister.

At this time, 40 Japanese domains have been identified to be targeted in these attacks with over 30 different configurations being administered by the threat actors to present the harshest impacts possible. As of now, the campaign for these attacks is ongoing with the threat actors pushing any new targets they mark to their botnet named DDoSia.

Health-ISAC recommends utilizing defense tools that can serve as reverse proxies, shielding internet services and applications from malicious traffic attempts and mitigating chances of any similar attacks taking place.

Vulnerabilities & Exploits

F5 BIG-IP Updates Patch High-Severity Elevation of Privilege Vulnerability

Summary

- F5 released updates for two vulnerabilities affecting its BIG-IP and BIG-IQ enterprise products.

Analysis & Action

The first vulnerability, tracked as CVE-2024-45844, is a high-severity security flaw that affects the BIG-IP appliance's monitor functionality. The vulnerability could allow authenticated threat actors to elevate their privileges and make configuration changes. Security fixes for the vulnerability are available in BIG-IP versions 17.1.1.4, 16.1.5, and 15.1.10.5.

The second vulnerability, tracked as CVE-2024-47139, affects the BIG-IQ and is considered to be a stored cross-site scripting (XSS) security flaw in an undisclosed page of the appliance's user interface. Successful exploitation of the flaw allows a threat actor who has gained administrator privileges to run JavaScript as the currently logged-in user. F5 released BIG-IQ centralized management versions 8.2.0.1 and 8.3.0 to address the defect.

Health-ISAC recommends that organizations update their vulnerable F5 BIG-IP or BIG-IQ instances to prevent targeted exploitation attacks from threat actors attempting to compromise those products.

Fake Google Meet Pages Deliver Infostealers

Summary

- Threat actors have been observed using the ClickFix tactic to infect Google Meet users with infostealer malware.

Analysis & Action

The tactic is innately deceptive and is used to get potential victims to download and execute malware on their devices without using a web browser or requiring them to manually run malicious files. This ultimately provides the opportunity for threat actors to bypass browser security features and avoid appearing suspicious.

Successful usage of this tactic largely relies on unsuspecting users landing on compromised websites following links from phishing emails or from search engines. The compromised sites often contain fake browser alerts. These alerts warn users that the webpage or document cannot be

viewed unless they click a button and follow instructions that lead to them executing malware on their system unknowingly.

According to cybersecurity researchers, fake alerts customized to target Google Meet and other services users are being placed on compromised sites as lures to infect systems with malware.

Health-ISAC recommends that organizations implement appropriate endpoint management security controls to monitor and combat suspicious or malicious activity identified on enterprise assets.

Trends & Reports

Google: 70% of Exploited Flaws Disclosed In 2023 Were Zero-Days

Summary

- A new trend regarding threat actors' capabilities to find and exploit zero-days is leading to cautionary concerns for Google's security analysts.

Analysis & Action

Threat actors' continued improvement in taking advantage of zero-day vulnerabilities in software has raised alarms, as an analysis of the previous year shows.

A total of 138 vulnerabilities were counted to have been disclosed within the year of 2023, of those 138 vulnerabilities, 97 or 70% of those vulnerabilities were zero-days. In years past, ratios between fixed flaws or n-days and zero-days have been fairly even at 4:6, but within the last year the ratio has changed, now sitting at 3:7. In an explanation by Google, they state that this is due to the increase in exploitation done to zero-day vulnerabilities rather than a drop in n-days being exploited. The alarm is raised even more so when accounting for the increased number of vendors that were impacted by the exploited flaws, reaching 56 within 2023, a record number. Additionally, research has shown that TTE or time taken to exploit has shrunken as well, with 2018-2019 taking 63 days and TTE now falling to just 5 days.

The increasing nature of threat actors and their capabilities shines a light on the importance of prompt patch protection against all vulnerabilities. Health-ISAC recommends performing rigorous patch management to mitigate risks and protect against possible zero-day vulnerabilities.

Privacy, Legal & Regulatory

Brazilian Police Arrest Notorious Threat Actor USDoD

Summary

- Brazil's Federal Police recently arrested a cybercriminal known for targeting major organizations and leaking stolen information.

Analysis & Action

The cybercriminal USDoD, otherwise known as EquationCorp, was recently arrested by Brazil's Federal Police. USDoD is a notorious cybercriminal who previously targeted major organizations, including the FBI, Airbus, TransUnion, National Public Data (NPD), and CrowdStrike.

The true identity of the cybercriminal was revealed as Luan BG, a native to the Brazilian state of Minas Gerais, to which the threat actor confirmed to be accurate.

The arrest was part of a search and seizure warrant served for incidents that took place in 2020 and 2022.

Health-ISAC Cyber Threat Level

On September 19, 2024, the Health-ISAC Threat Intelligence Committee (TIC) evaluated the current Cyber Threat Level and collectively decided to maintain the Cyber Threat Level at Blue (Guarded). The Threat Level of Blue (Guarded) is due to threats from:

The Threat Level of Blue (Guarded) is due to threats from DPRK IT fraud, elections-induced cyber activity, potential repercussions of recent activity in the Middle East, potential Ivanti Endpoint Manager exploitation, and ongoing observances of infostealer's logs being posted on Telegram.

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

Incident Date

Oct 18, 2024, 11:59 PM

Reference | References

NetScout
cybershafarat
Security Week
Security Week
GB Hackers
Bleeping Computer
Help Net Security

Tags

USDoD, Remote Fraud, F5 BIG-IP

TLP:WHITE: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

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