DAILY CYBER HEADLINES

Health-ISAC Daily Cyber Headlines

TLP:GREEN

Nov 22, 2021

Leading Story

- North Korean APT Group Steps Up Espionage Ops in 2021

Data Breaches & Data Leaks

- Utah Medical Center Hit By Data Breach Affecting 582k Patients

Cyber Crimes & Incidents

- Hackers Targeted Thousands of Online Retailers to Steal Credit Card Details
- Microsoft Exchange Servers Hacked in Internal Reply-Chain Attacks
- US SEC Warns Investors of Ongoing Govt Impersonation Attacks

Vulnerabilities & Exploits

- Vulnerabilities Identified in Philips IntelliBridge, Patient Information Center, and Efficia Patient Monitors
- Six Million Sky Routers Exposed to Takeover Attacks for 17 Months

Trends & Reports

- Nothing to Report

Privacy, Legal & Regulatory

- Nothing to Report

Upcoming Health-ISAC Events

- Health-ISAC Monthly Threat Brief – November 23, 2021, 12:00 PM Eastern

Leading Story

North Korean APT Group Steps Up Espionage Ops in 2021

Summary

- North Korean Advanced Persistent Threat (APT) group TA406, also known as Kimsuky, is ramping up its cyberespionage operations in 2021, targeting diplomats and policy experts across Asia, the United Kingdom (UK), and the United States (US).

Analysis & Action

In early 2021, TA406 launched weekly campaigns featuring themes that included nuclear weapons safety, US President Joe Biden, and Korean foreign policy. The group attempted to collect credentials, such as Microsoft logins or corporate logins, from targeted individuals. In some cases, they used benign emails, but the messages may have been attempts by attackers to engage with victims before sending them a malicious link or attachment.

TA406 has been involved in frequent credential theft campaigns against multiple research, education, media, finance, and nonprofit organizations. The latest targets have been organizations related to cryptocurrency for financial gain. TA406 has also been known to conduct spear-phishing campaigns in 2021 to deliver credential harvesting links and malware such as Babyshark.

A full Proofpoint report on the threat group can be accessed here.

Data Breaches & Data Leaks

Utah Medical Center Hit By Data Breach Affecting 582k Patients

Summary

- Utah Imaging Associates (UIA), a radiology center, has announced a data breach affecting 582,170 people after their personal information was exposed.

Analysis & Action

The security incident was discovered in early September of 2021 and was remediated on the same day, but threat actors had access to the system for about a week beforehand and were able to access personal information concerning patients, such as names, mailing addresses, dates of birth, social security numbers, policy numbers, and medical information. UIA has received no reports of this data being leaked online.

Hackers tend to target medical centers like UIA as they handle sensitive data considered valuable in the cybercrime underground. AS healthcare visits require patients to provide a lot of personal information, the responsibility of securing their sensitive data can be difficult for healthcare providers. UIA urges patients within the past year to take advantage of offered credit monitoring services.

Cyber Crimes & Incidents

Hackers Targeted Thousands of Online Retailers to Steal Credit Card Details

Summary

- Over 4k online retailers have been warned by the NCSC that their websites have been hacked by cybercriminals trying to steal payment information and other personal information from customers.

Analysis & Action

In total, the National Cyber Security Center (NCSC) has identified a total of 4,151 retailers that have been compromised by hackers attempting to exploit vulnerabilities on checkout pages to divert payments and steal details. They alerted the retailers to the breaches over the past 18 months.

The majority of the online shops that cybercriminals exploited for payment skimming attacks were compromised by known vulnerabilities in the e-commerce platform Magento. Most of those affected and alerted to compromises and vulnerabilities are small to medium-sized businesses. The NCSC notified the businesses ahead of Black Friday and is urging all retailers to ensure that their websites are secure ahead of the busiest online shopping period of the year in order to protect their businesses, and their customers, from cybercriminals.

Microsoft Exchange Servers Hacked in Internal Reply-Chain Attacks

Summary

- Threat actors are hacking Microsoft Exchange servers using ProxyShell and ProxyLogon exploits to distribute malware and bypass detection using stolen internal reply-chain emails, according to TrendMicro researchers.

Analysis & Action

Threat actors have begun distributing malicious emails to a company's internal users using the victim's compromised Microsoft Exchange Servers. The actors behind the attack are believed to be TR, a known threat actor who distributes emails with malicious attachments that drop malware, including Qbot, Iced ID, and Cobalt Strike payloads.

They use the compromised Exchange servers to reply to the company's internal emails in reply-chain attacks containing links to malicious documents that install various malware. Microsoft has fixed the ProxyLogon vulnerabilities as of March 2021 and the ProxyShell vulnerabilities in April and May 2021, addressing them as zero-days.

The full TrendMicro report can be accessed here.

US SEC Warns Investors of Ongoing Govt Impersonation Attacks

Summary

- The United States Securities and Exchange Commission (SEC) has warned investors of scammers impersonating SEC officials in government impersonator schemes via phone calls, voicemails, emails, and letters.

Analysis & Action

The alert comes from SEC's Office of Investor Education and Advocacy, which regularly issues warnings to inform investors about the latest developments in investment frauds and scams.

The calls and messages raised purported concerns about unauthorized transactions or other suspicious activity in the recipients' checking or cryptocurrency accounts. Investors are advised not to provide personal information until they verify they're actually speaking with an SEC official since these phone calls and voicemails are in no way connected to the SEC. The SEC department clarified that it does not seek money from any person or entity as a penalty or disgorgement for alleged wrongdoing outside of its formal enforcement process.

Vulnerabilities & Exploits

Vulnerabilities Identified in Philips IntelliBridge, Patient Information Center, and Efficia Patient Monitors

Summary

- Five vulnerabilities have been identified in several patient monitors, including the Intellibridge EC 40 and EC 80 Hub, Philips Patient Information Center iX, and Efficia CM series.

Analysis & Action

Two vulnerabilities affect the EC 40 and EC 80 Hub. Successful exploitation of the vulnerabilities could allow an unauthorized individual to execute software, change system configurations, and view files that may include unidentifiable patient data. Philips has not yet issued an update the correct the vulnerabilities but expects to fix the flaws by the end of 2021.

Three vulnerabilities have also been identified that affect the Philips Patient Information Center iX and Efficia CM series patient monitors. The flaws could be exploited to gain access to patient data and to conduct a denial-of-service attack. To reduce the potential for exploitation of the vulnerabilities, the products should only be used in accordance with Philips authorized specifications, which include isolating the devices from the hospital local network.

Six Million Sky Routers Exposed to Takeover Attacks for 17 Months

Summary

- Around six million Sky Broadband customer routers in the United Kingdom were affected by a critical vulnerability that took over 17 months to roll out a fix to customers.

Analysis & Action

The vulnerability is a DNS binding flaw that threat actors could easily exploit if the user had not changed the default admin password, or a threat actor could brute-force the credentials. The result of the exploitation would be to compromise the customer’s home network, change the router’s configuration, and potentially pivot to other internal devices.

The DNS rebinding attacks are used to bypass a browser security measure called Same Origin Policy which blocks a site from sending requests to websites other than its own origin. This origin is usually the domain you visited in the browser. For the attack to work, the victim must be tricked into clicking a malicious link or website, which can be obtained through phishing. It then downloads a malicious payload on the server, which triggers DNS requests.

The vulnerability was patched 17 months after it was found.

Trends & Reports

There is nothing to report.

Privacy, Legal & Regulatory

There is nothing to report.

Health-ISAC Cyber Threat Level

On November 4, 2021, the H-ISAC Threat Intelligence Committee (TIC) evaluated the current Cyber Threat Level and collectively decided to maintain the current Cyber Threat Level at Blue (Guarded). The Threat Level is remaining Blue (Guarded) due to ongoing threats from Qakbot, Zloader, and Dridex campaign observances, observed threat actors initiating phishing email campaigns and observances of BazarLoader malware

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.

Reference(s)	Bleeping Computer, Health-ISAC, Bleeping Computer, Proofpoint, ZDNet, Gov Info Security, Health-ISAC, Bleeping Computer, Bleeping Computer, HIPAA Journal

Alert ID af8fc558

View Alert

Tags Daily Cyber Headlines, DCH

TLP:GREEN Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.

Access the Health-ISAC 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 Cyware.

For Questions or Comments Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.

For more update and alerts, visit: **https://health-isac.cyware.com**