Health-ISAC Daily Cyber Headlines

Daily Cyber Headlines | TLP:WHITE | Alert ID : 34cc9fd6 | Oct 08, 2021, 09:32 AM

Today's Headlines:

Leading Story

- Foreign Hacking Group Targets Hospitals, Clinics with Ransomware Attacks, Says New Report

Data Breaches & Data Leaks

- Almost 54,000 Patients Affected by OSF HealthCare Ransomware Attack

Cyber Crimes & Incidents

- Microsoft: Russia Dominates State-Sponsored Attacks

Vulnerabilities & Exploits

- Twitch Attributes Breach to Server Configuration Error, Resets All Stream Keys

Trends & Reports

- 73% of Ransomware Detections in Q2 2021 Credited to REvil/Sodinokibi
- Patching Too Tortuous for IT Pros, Says New Report

Privacy, Legal & Regulatory

- US Creates National Cryptocurrency Enforcement Team

Upcoming Health-ISAC Events

- Health-ISAC Monthly Threat Brief – October 26, 2021, 12:00 PM Eastern

Additional Info

Leading Story

Foreign Hacking Group Targets Hospitals, Clinics with Ransomware Attacks, Says New Report

Summary

- Threat group FIN12 is expanding its hacking operations and repeatedly targeting the health care industry with more ransomware attacks, according to a new report by cybersecurity firm Mandiant.

Analysis & Action

The group is shutting down systems, hampering access to patient records, and other malicious functions that heighten the risk to patients until a ransom is paid. The group checks financial statements before picking their victims, demanding ransoms in the millions of dollars in exchange for protected health information.

Nearly 20% of the group's overall victims are part of the healthcare industry, according to the Mandiant report, and over 70% of targets are based in the United States. But FIN12's attacks outside of North America doubled in the first half of 2021, surpassing 2019 and 2020 collectively.

We do not believe that others refusing to target healthcare has a direct correlation to FIN12's willingness to target this industry, commented a researcher at Mandiant, FIN12 may perceive that there is a higher willingness for hospitals to quickly pay ransoms to recover critical systems rather than spend weeks negotiating with actors or remediating the issue.

The full Mandiant report can be accessed here.

Data Breaches & Data Leaks

Almost 54,000 Patients Affected by OSF HealthCare Ransomware Attack

Summary

- OSF HealthCare has started notifying 53,907 patients about a cyberattack that was discovered on April 23, 2021.

Analysis & Action

OSF HealthCare said upon discovery of the breach, steps were taken to prevent further unauthorized access and a third-party forensic investigator was engaged to conduct an investigation into the attack to determine the extent of the breach. The investigator confirmed the attackers first accessed its systems with sensitive, protected health information on March 7, 2021, and access remained possible until April 23, 2021.

Individuals whose Social Security number or driver's license number was compromised in the attack have been offered complimentary credit monitoring and identity protection services through Experian. OSF HealthCare says it has implemented additional safeguards and technical security measures to prevent further attacks.

Cyber Crimes & Incidents

Microsoft: Russia Dominates State-Sponsored Attacks

Summary

- Russia accounted for the majority of state-sponsored attacks over the past year, with the SolarWinds attackers dominating threat activity, according to new data from Microsoft.

Analysis & Action

The firm's Digital Defense Report 2021 covers the period from July 2020 to June 2021 and examines cybercrime activity. Kremlin-backed raids accounted for 58% of all nation-state

attacks during the period, with Nobelium, also known as APT29, Cozy Bear, generating 92% of notifications Microsoft made to customers about attacks. Microsoft claimed that Russian state-backed attacks are increasingly successful: compromise rates jumped from 21% to 31% year on year.

After Russia, the largest volume of attacks came from North Korea, with 23%, Iran, with 11%, and China, with 8%. The full Microsoft report can be accessed here.

Vulnerabilities & Exploits

Twitch Attributes Breach to Server Configuration Error, Resets All Stream Keys

Summary

- Twitch has announced that it reset all stream keys as it seeks to address the massive data breach that was revealed earlier this week.

Analysis & Action

A hacker leaked the entirety of Twitch's source code alongside a 128GB trove of data that included creator payouts going back to 2019, proprietary development kits, and internal Amazon Web Services (AWS) used by Twitch, as well as all of the company's internal cybersecurity red teaming tools. Security experts warned that all Twitch streamers needed to take immediate actions to protect their bank accounts and themselves from a potential wave of attacks by opportunistic cybercriminals.

As a result of the breach, Twitch announced that it was resetting all stream keys, directing streamers to this website for new stream keys. In an earlier statement, the company said it learned that the breach originated from a Twitch server configuration change error that left data exposed to the internet.

Twitch added that it was still trying to understand the scope of the breach as it continues to investigate the incident.

Trends & Reports

73% of Ransomware Detections in Q2 2021 Credited to REvil/Sodinokibi

Summary

- McAfee's quarterly cyber threat report revealed statistics about the current state of ransomware, showing that 73% of ransomware detections in Q2 2021 were credited to the notorious hacking group REvil.

Analysis & Action

Behind the financial services sector, healthcare was the most targeted industry for cloud security incidents in Q2. Public sector security incidents increased by 64% in Q2. Malware attacks were the most used attack technique in Q2, while spam showed the highest increase in reported incidents, at 250%. Spearphishing and Windows command shell techniques also gained popularity in Q2 of this year.

McAfee observed that two of the most influential underground forums for cybercriminals announced a ban on ransomware advertisements last quarter. Despite this action,

researchers found that threat actors are still very active on these forums under different personas.

The full McAfee report can be accessed here.

Patching Too Tortuous for IT Pros, Says New Report

Summary

- Patching vulnerabilities is too labor-intensive and convoluted a process for most IT security professionals, according to new research by Ivanti.

Analysis & Action

The software company surveyed over 500 enterprise IT and security professionals across North America, Europe, the Middle East, and Africa about their patch management challenges.

71% of respondents found patching to be overly complex, cumbersome, and time-consuming, with 54% saying that remote work has increased the intricacy and scale of patch management. Patching was reported to have an impact upon productivity, with 60% of respondents saying that the process disrupts the workflow of users.

These results come at a time when IT and security teams are dealing with the challenges of the everywhere workplace, in which workforces are more distributed than ever before, and ransomware attacks are intensifying and impacting economies and governments, said a representative from Ivanti. The full Ivanti report can be accessed here.

Privacy, Legal & Regulatory

US Creates National Cryptocurrency Enforcement Team

Summary

- The United States Department of Justice (DoJ) has formed a new task force to oversee complex investigations and prosecutions of criminal misuses of cryptocurrency.

Analysis & Action

The DoJ's Office of Public Affairs said that the National Cryptocurrency Enforcement Team's (NCET) focus would be on criminal acts committed by virtual currency exchanges, money laundering infrastructure actors, and mixing and tumbling services. NCET will assist in tracing and recovering assets lost to fraud and extortion, including crypto-currency payments to ransomware gangs.

NCET will also train and advise federal prosecutors and law enforcement agencies in developing investigative and prosecutorial strategies and provide guidance on matters including search and seizure warrants, restraining orders, criminal and civil forfeiture allegations, and indictment.

A full statement from the DoJ can be accessed here.

Reference | References

ivanti
US Department of Justice
Info Security Magazine
HIPAA Journal
ZDNet
Health-ISAC
Info Security Magazine
Business Wire
Health IT Security
CBS News
Health-ISAC
mandiant
Info Security Magazine

Tags

Daily Cyber Headlines, DCH
