DAILY CYBER HEADLINES

Health-ISAC Daily Cyber Headlines

TLP:GREEN

Nov 24, 2021

Today's Headlines:

Leading Story

- Increased Risk of Cyber and Ransomware Attacks Over Thanksgiving Weekend

Data Breaches & Data Leaks

- Nothing to Report

Cyber Crimes & Incidents

- DBS Bank Offers Few Details About Hours-Long Service Disruption
- FBI Warns of Phishing Targeting High-Profile Brands' Customers
- Suspect Arrested in Ransom Your Employer Criminal Scheme

Vulnerabilities & Exploits

- Nothing to Report

Trends & Reports

- HC3 Warns Healthcare Sector about Risk of Zero-Day Attacks
- Threat Actors Find and Compromise Exposed Services in 24 Hours

Privacy, Legal & Regulatory

- Apple Sues NSO Group Over Pegasus Spyware

Upcoming Health-ISAC Events

- Health-ISAC Monthly Threat Brief – December 21, 2021, 12:00 PM Eastern

Upcoming Health-ISAC Holidays

On Thursday, November 25, 2021, and Friday, November 26, 2021, Health-ISAC will not be publishing the Daily Cyber Headlines in accordance with the United States Thanksgiving Day Holiday. Please look forward to us resuming the Daily Cyber Headlines on Monday, November 29, 2021.

Leading Story

Increased Risk of Cyber and Ransomware Attacks Over Thanksgiving Weekend

Summary

- The US Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) have warned organizations in the United States about the risk of cyberattacks over Thanksgiving weekend.

Analysis & Action

Cyber threat actors are often at their most active during holidays and weekends, as there are likely to be fewer IT and security employees available to detect attempts to breach networks. Recent attacks have demonstrated holiday weekends are prime time for cyber threat actors.

Their warning applies to all organizations and businesses, but especially critical infrastructure firms. Cyber actors around the world may choose Thanksgiving weekend to conduct attacks to disrupt critical infrastructure and conduct ransomware attacks.

CISA and the FBI are urging all entities to take steps to ensure risk is effectively mitigated ahead of the holiday weekend to help prevent them from becoming the next victim of a costly cyberattack. Multi-factor authentication should be activated on all remote and administrative accounts, default passwords should be changed, and strong passwords set on all devices, with steps taken to ensure they are not reused.

Previously issued CISA response playbooks can be found here. Health-ISAC has published an additional alert, containing additional analysis and mitigation strategies, which can be accessed here.

Data Breaches & Data Leaks

There is nothing to report.

Cyber Crimes & Incidents

DBS Bank Offers Few Details About Hours-Long Service Disruption

Summary

- Customers have not been able to log into or access a Singapore bank's online and mobile services in a service outage that remains unresolved.

Analysis & Action

Several customers of DBS Bank have not been able to access or log into the Singapore bank's online and mobile services since late November 2021. The service disruption remains unresolved, with few details from DBS about what is going on to address the issue.

Other customers report being able to access their account, but that the balance listed was inaccurate. According to the bank's website, scheduled maintenance was carried out which stated that login and digital access may be intermittently unavailable. At this time, the bank has not confirmed whether the incident is the result of maintenance or of a cyberattack.

FBI Warns of Phishing Targeting High-Profile Brands' Customers

Summary

- The US Federal Bureau of Investigation (FBI) warned of recently detected spear-phishing email campaigns targeting customers of brand-name companies in attacks known as brand phishing.

Analysis & Action

The targets are sent to phishing landing pages through various means, including emails, text messages, or web and mobile apps that may spoof the identity or the online address of a company's official site. Attackers then embed login forms or malware onto their phishing pages with the end goal of stealing their victim's personally identifiable information.

In addition to these attacks, threat actors are also likely developing tools to bait potential targets into revealing info by bypassing account protections two-factor authentication by intercepting emails, and compromising accounts.

The FBI encourages private sector partners to stay vigilant and evaluate their internal security policies and provide their consumers with information regarding account security protocols.

Their full report can be read here.

Suspect Arrested in Ransom Your Employer Criminal Scheme

Summary

- A Nigerian man has been arrested in connection to a scheme attempting to lure insiders to deploy ransomware on employer systems.

Analysis & Action

In late November 2021, security experts reported that the suspect was arrested by Nigerian authorities. The suspect is allegedly linked to a ransom your employer scheme investigated by Abnormal Security in August.

Customers of the cybersecurity firm were sent emails with the subject: Partnership Affiliate Offer, requesting that the recipient considered becoming an accomplice in a cyberattack. The emails offered a 40% cut of an anticipated $2.5 million ransomware payment

made in Bitcoin after the recipients installed the DemonWare Ransomware on their employer's systems.

Security researchers responded under the guise of a fictional person and confirmed they were sent ransomware executables hosted on two file-sharing websites. Charges are expected to be brought against the subject later in the month.

Vulnerabilities & Exploits

There is nothing to report.

Trends & Reports

HC3 Warns Healthcare Sector about Risk of Zero-Day Attacks

Summary

- The Health Sector Cybersecurity Coordination Center (HC3) has issued a threat brief warning to the healthcare and public health sector about an increase in financially motivated zero-day attacks.

Analysis & Action

The HC3 has issued a threat brief warning the healthcare and public health sector about an increase in financially motivated zero-day attacks, outlining mitigation tactics that should be adopted to reduce

risk to a low and acceptable level. The number of detected exploits for zero-day vulnerabilities has more than doubled between 2019 and 2021, where a single exploit could be worth more than $1 million.

The best defense against zero-day vulnerabilities is to patch promptly, but patching is often slow. The advice of HC3 is to patch early, patch often, patch completely. They provide up-to-date information on actively exploited zero-days and the available process to fix zero-day vulnerabilities. They also suggest implementing a web-application firewall to review incoming traffic and filter out malicious input, as this can prevent threat actors from gaining access to vulnerable systems.

The full threat brief can be located here.

Threat Actors Find and Compromised Exposed Services in 24 Hours

Summary

- Researchers have set up 320 honeypots to see how quickly threat actors would target exposed cloud services and report that 80% of them were compromised in under 24 hours.

Analysis & Action

Malicious actors are constantly scanning the internet for exposed services that could be exploited to access internal networks or perform other malicious activities. To track what software and services are targeted by threat actors, researchers create publicly accessible honeypots. Honeypots are servers configured to appear as if they are running various software as lures to monitor threat actors' tactics.

In a new study conducted by Palo Altos Networks' Unit 42, researchers set up 320 honeypots and found that 80% of honeypots were compromised within the first 24 hours. The deployed honeypots included ones with emote desktop protocol, secure shell protocol, server message block, and Postgres database services and were kept alive from July to August 2021. These honeypots were deployed worldwide, with instances in North America, Asian Pacific, and Europe.

The full report can be read here.

Privacy, Legal & Regulatory

Apple Sues NSO Group Over Pegasus Spyware

Summary

- Apple is seeking a permanent injunction that bans NSO Group from using any Apple software, services, or devices.

Analysis & Action

Apple has filed a lawsuit against mercenary spyware company NSO Group and its parent company, seeking a permanent injunction that bans NSO Group from using any Apple software, services, and devices. The complaint also provides new information on how NSO Group infected victims' Apple devices with its Pegasus Spyware.

Apple's complaint says that NSO Group delivered its FORCEDENTRY exploit to Apple devices by creating Apple IDs that sent malicious data to a victim's device. This enabled the installation of Pegasus spyware without a victim's knowledge. Researchers discovered the zero-day in September, and Apple released a security update for Mac, iPhone, iPad, and Watch users to patch the vulnerability.

Apple says that Apple servers were misused to deliver FORCEDENTRY but were not hacked or compromised. The company says it is notifying the small number of users that it discovered may have been targeted by FORCEDENTRY.

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)	HIPAA Journal, HHS.gov, IC3, Palo Alto Networks, cisa, Health-ISAC, ZDNet, HIPAA Journal, ZDNet, Bleeping Computer, ZDNet, cisa, Health-ISAC, Bleeping Computer

Alert ID 17921826

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**