Health-ISAC Daily Cyber Headlines

Daily Cyber Headlines	○ TLP:WHITE	Alert ID : d4e80790	Oct 20, 2021, 10:23 AM

Today's Headlines:

Leading Story

- Blackbyte Ransomware Decryptor Released to Recover Files for Free

Data Breaches & Data Leaks

- VPN Provider's Misconfiguration Exposes One Million Users

Cyber Crimes & Incidents

- Man Gets 7 Years In Prison for Hacking 65K Health Care Employees
- Customer Services Firm Atento Hit by Cyberattack

Vulnerabilities & Exploits

- Nothing to Report

Trends & Reports

- Analysis: Top Ransomware Gangs Targeting Healthcare Sector
- Report: 83% of Ransomware Victims Pay the Demand

Privacy, Legal & Regulatory

- Black Market Traders Cash in on Fake COVID-19 Vaccination Records
- FCC Mulls Over New Rules Demanding Carriers Block Spam Robot Texts at Network Level

Upcoming Health-ISAC Events

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

Additional Info

Leading Story

Blackbyte Ransomware Decryptor Released to Recover Files for Free

Summary

- A free decryptor for the BlackByte ransomware has been released, allowing past victims to recover their files for free.

Analysis & Action
In a report released by Trustwave, BlackByte uses AES symmetrical encryption while deploying, meaning the same key is used for both the encryption and decryption of files. While BlackByte also encrypts this downloaded AES encryption key and appends it to the ransom note, Trustwave discovered that the ransomware gang was reusing a duplicate file for multiple victims. As the same encryption key was being reused, Trustwave could use that key to build a decryptor that recovers a victim's files for free.

However, there are always drawbacks when releasing free decryptors like this as it alerts the ransomware gangs of the bugs in their programs and quickly fixed. Trustwave's report and decryptor did not go unnoticed by the ransomware gang, who warned that they have used more than one key and that utilizing the decryptor with the wrong key would corrupt a victim's files.

Due to this, it is strongly advised that victims backup files before attempting to decrypt them. The source code of the decryptor can be accessed here.

Data Breaches & Data Leaks

VPN Provider's Misconfiguration Exposes One Million Users

Summary
- At least one million users of a Chinese-run VPN service have had their personally identifiable information (PII) exposed due to a misconfigured Elasticsearch server.

Analysis & Action
The server belongs to Quickfox, a VPN used mainly by Chinese citizens to visit sites otherwise inaccessible from outside mainland China. The 100GB dataset found by the researchers contained 500 million records, including personally identifiable information (PII) on one million users and system data on 300,000 customers. The exposed PII included customers’ emails, IP addresses, phone numbers, details to identify device type, and MD5 hashed passwords.

By unmasking the MD5 hashed passwords and using credential stuffing techniques, cyber-criminals could also try to hijack other accounts across the web, which users might protect with the same credential.

The server has yet to be secured.

Cyber Crimes & Incidents

Man Gets 7 Years In Prison For Hacking 65K Health Care Employees

Summary
- Threat actor sentenced to seven years in prison for a 2014 hack of a health care provider and insurer, stealing more the information of over 65,000 employees and selling it on the dark web.

Analysis & Action

Justin Sean Johnson, formerly referred to as TheDearthStar and Dearthy Star, was sentenced to seven years in prison for the 2014 hack of the University of Pittsburgh Medical Center (UPMC). Johnson breached UPMC’s human resources databases after hacking the Oracle PeopleSoft management system, then stole the Personally Identifiable Information (PII) and W-2 information of over 65,000 employees and sold it on the dark web.

Johnson was charged in a forty-three-count indictment of conspiracy, wire fraud, and aggravated identity theft, and pleaded guilty. The stolen information was used by fraudsters to file hundreds of false 1040 tax returns and claim approximately $1.7 million in false tax refunds, that were converted into gift cards.

In addition to the thousands of UPMC sets of PII data, Johnson stole almost 90,000 additional non-UPMC sets of data to clients on the dark web.

Customer Services Firm Atento Hit by Cyberattack

Summary

- Business process outsourcing (BPO) and customer relationship management multinational firm Atento has been hit by a cyberattack.

Analysis & Action

The firm informed its customers earlier this week about the attack against its systems in Brazil, which caused an interruption of service as the company sought to contain and evaluate the extent of the threat, according to local news website. Atento's note to customers added that its security team was working towards containing it and ensuring the security of the affected environments before bringing them back online as soon as possible.

The firm is the latest of a string of companies operating in Brazil that have suffered cyber-attacks recently. Last week, one of Brazil's largest insurance groups, Porto Seguro, suffered a cyberattack that resulted in downtime to its service channels and some of its internal systems.

Vulnerabilities & Exploits

Nothing to Report.

Trends & Reports

Analysis: Top Ransomware Gangs Targeting Healthcare Sector

Summary

- The Department of Health and Human Services’ Health Sector Cybersecurity Coordination Center (HC3) has identified 10 major ransomware groups affecting organizations.

Analysis & Action

After analyzing the ransomware activity in the U.S. and global healthcare sector during the third quarter, HC3 has identified 10 major ransomware groups affecting organizations across the U.S. and globally, with the most active group being Conti.

The top countries impacted by ransomware incidents in the health sector outside the U.S. include France, Brazil, Thailand, Australia, and Italy. The U.S states experiencing the most incidents involving healthcare include California, Florida, Illinois, Michigan, Texas, Arizona, Indiana, Maryland, New York, and Georgia. The most affected groups continue to be health and medical clinics, then healthcare industry service firms and hospitals.

Conti, Avaddon, and REvil/Sodinokibi were the top three ransomware groups targeting the global health sector during the third quarter of 2021. 50% of all cyberattacks against healthcare begin with phishing attacks, and experts warn the surge in ransomware attacks will continue.

The full report can be accessed here.

83% of Ransomware Victims Pay the Demand

Summary

- 83% of ransomware victims in the last 12 months felt they had no option but to pay the extortion demand to restore their data, according to a new report by ThycoticCentrify.

Analysis & Action

The study, which was based on a survey of 300 US IT business decision-makers, also found that 64% of companies were victims of ransomware attacks in the last 12 months.

The research further highlighted the substantial damage caused to organizations by ransomware attacks. 50% of respondents said their company had experienced a loss of revenue and reputational damage from an attack, and 42% admitted they lost customers due to an attack. Additionally, around one-third attributed the ransomware attack as the cause for employee layoffs.

Encouragingly, there appears to be growing recognition of the need to improve cyber defenses amid surging ransomware incidents. Nearly three-quarters of respondents have seen their cybersecurity budgets increase due to ransomware threats, while 93% of businesses are allocating a special budget to fight ransomware threats. The full ThycoticCentrify report can be accessed here.

Privacy, Legal & Regulatory

Black Market Traders Cash in on Fake COVID-19 Vaccination Records

Summary

- Researchers have uncovered a lively trade online in the sale of fake vaccination records and passports.

Analysis & Action

According to research conducted by Intel 471, numerous cybercriminals are now offering fake COVID-19 vaccine certifications focused on US and EU entry requirements. The US Centers for Disease Control and Prevention (CDC) vaccination cards are issued by vaccine providers in a paper format. The EU also offers a vaccine passport, the EU Digital COVID Certificate, which is issued to European residents in a paper and digital form.

Underground forum posts advertise their fake certificate wares together with coronavirus claims and misinformation.

On one forum, a trader is offering counterfeit CDC cards, whereas, on another, EU and specifically French documents containing QR codes are being displayed. The QR codes on legitimate vaccine passports are designed to pull vaccination records from healthcare providers. However, these codes may go to fraudulent websites containing fake records.

FCC Mulls Over New Rules Demanding Carriers Block Spam Robot Texts at Network Level

Summary

- The US Federal Communications Commission (FCC) is due to consider a new proposal to suppress robot texts.

Analysis & Action

On October 18, 2021, FCC Acting Chairwoman Jessica Rosenworcel unveiled a new set of proposed rules that would force wireless carriers to block illegal robot texts, potentially at the network level.

According to the chairwoman, the US regulator received roughly 14,000 complaints from consumers concerning unwanted, robot texts in 2020. So far, the commission has received over 9,800 complaints, which suggests that this is a rising trend that needs to be tackled alongside robot calls

Rosenworcel said that if the proposal is accepted, mobile carriers in the United States would be required to protect customers from illegal text messages, and this could include initiatives such as blocking texts at the network level or applying caller authentication standards to text messaging.

The full set of proposed FCC rules can be accessed here.

Reference | References

ZDNet
ZDNet
ZDNet
Info Security Magazine
Info Security Magazine
Bleeping Computer
fcc
Bleeping Computer
Health-ISAC
HHS.gov
Healthcareinfosecurity
GitHub
thycotic
Health-ISAC

Tags

Daily Cyber Headlines, DCH