Health-ISAC Daily Cyber Headlines

Daily Cyber Headlines | TLP:WHITE | Alert ID : 1013d5ae | Oct 20, 2021, 03:43 PM

Today's Headlines:

Leading Story

- US Authorities Issue BlackMatter Ransomware Alert

Data Breaches & Data Leaks

- Accenture Confirms Data Stolen in Ransomware Attack
- University Hospital Newark Notifies 9,000 Individuals About Historic Insider Data Breach

Cyber Crimes & Incidents

- Suspected Chinese Hackers Behind Attacks on Ten Israeli Hospitals

Vulnerabilities & Exploits

- Microsoft Fixes Windows 10 Auth Issue Impacting Remote Desktop

Trends & Reports

- US Treasury Tracks $5.2bn of Ransomware Transactions in Six Months

Privacy, Legal & Regulatory

- Missouri Refers Coordinated Bug Disclosure to Prosecutors

Upcoming Health-ISAC Events

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

Additional Info

Leading Story

US Authorities Issue BlackMatter Ransomware Alert

Summary

- US authorities have released details on emerging ransomware group BlackMatter, which the agencies claim that the group has already targeted multiple critical infrastructure providers in the country.

Analysis & Action

The alert, published earlier this week, comes from the US Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the National Security Agency (NSA).

Demanding payments of up to $15m from its victims, BlackMatter has been observed using remote monitoring and desktop software to achieve persistence when targeting various entities. BlackMatter is said to target healthcare, non-government organizations, government, oil and gas, and other critical infrastructure sectors.

The US agencies recommended in the report that organizations limit access to network resources, enforce the principle of least privilege in identity and access management, and enforce best practice backup and restoration policies.

Health-ISAC will be releasing an accompanying threat bulletin containing additional details, analysis, and mitigation strategies.

Data Breaches & Data Leaks

Accenture Confirms Data Stolen in Ransomware Attack

Summary

- Accenture has confirmed an August 2021 data breach that compromised sensitive data.
- There was no impact on Accenture or client systems, although Lockbit 2.0 claimed credit for the ransomware attack and dumped the stolen data after Accenture failed to pay the ransom.

Analysis & Action

Accenture confirmed a data breach occurring in early August 2021, stating that there was no impact on Accenture's operations or on client systems. The attacker, now known as Lockbit 2.0, exfiltrated data and demanded ransom payment so it would not leak the stolen data. As attackers often lie about owning stolen or sensitive data, Accenture declined to pay, and Lockbit 2.0 responded by dumping the stolen data across its leak site.

The data consisted of PowerPoints, quotes, case studies, and similar files, but Accenture did not issue a statement addressing employee, client, or business partner personal information.

University Hospital Newark Notifies 9,000 Individuals About Historic Insider Data Breach

Summary

- University Hospital Newark discovered the protected health information of thousands of patients has been accessed by a former employee without authorization over the course of a year and subsequently disclosed that information to other unqualified individuals.
- The access occurred between January 2016 and December 2017, and impacted individuals have been notified.

Analysis & Action

The former employee had been provided with access to patient data to complete work duties but had exceeded the authorized use of access and had viewed patient data not

pertinent to job functions. The information obtained by the individual included names, addresses, dates of birth, Social Security numbers, health insurance information, medical record numbers, and clinical information related to care patients received at the hospital.

University Hospital reported the case to law enforcement and there is an ongoing investigation. In addition, the hospital also began mailing notification letters to affected individuals in October 2021 and says they have taken steps to reduce the risk of further similar data breaches.

University Hospital did not disclose the reason for the access or how the breach was discovered, but that the former employee accessed the Protected Health Information of patients who visited the emergency department and received treatment for injuries from motor vehicle accidents between 2016 and 2017.

Cyber Crimes & Incidents

Suspected Chinese Hackers Behind Attacks on Ten Israeli Hospitals

Summary

- A group of Chinese threat actors utilizing the DeepBlueMagic ransomware strain attacked the systems of nine health institutes in Israel in mid-October 2021.
- The attacks resulted in no damage to the hospitals and medical organizations, although Hillel Yaffe Medical Center is still using pen and paper to admit patients for the sixth day since the initial attack.

Analysis & Action

The Ministry of Health and the National Cyber Directorate in Israel announced a spike in ransomware attacks during mid-October 2021, that targeted nine health institutions around the country. Thanks to national-level cooperation and the quick response to the local IT teams, no lasting damage to the hospitals and medical organizations occurred. The authorities had previously carried out numerous defense activities to identify open vulnerabilities and secure them before the weekend came in response to a Wednesday attack on Hillel Yaffe Medical Center.

The attack was carried out by Chinese threat actors who used the DeepBlueMagic ransomware strain, which disables security solutions that usually detect and block file encryption attempts. They also used the BestCrypt hard drive encryption tool to encrypt devices. The ransomware actors accessed the backup system and wiped all copies of medical records stored there. The attacker's motives were purely financial; however, the Hillel Yaffa center is a government-owned hospital, and as such, will not negotiate with hackers.

A full report on the Hillel Yaffe Medical Center attack can be accessed here.

Vulnerabilities & Exploits

Microsoft Fixes Windows 10 Auth Issue Impacting Remote Desktop

Summary

- Microsoft has fixed a known Windows 10 issue causing smartcard authentication to fail when trying to connect using the Remote Desktop Protocol (RDP) after

installing the cumulative updates released during September Patch Tuesday.

Analysis & Action

After installing KB5005611 or later updates, when connecting to devices in an untrusted domain using Remote Desktop, connections might fail to authenticate when using smart card authentication, Microsoft explained. Windows platforms affected by this issue include both client and server versions.

Microsoft has already rolled out a fix to address this issue via the Known Issue Rollback (KIR) feature to affected Windows 10 devices. For enterprise-managed devices, customers can also install and configure group policies to resolve the issue.

Trends & Reports

US Treasury Tracks $5.2bn of Ransomware Transactions in Six Months

Summary

- The US Treasury has tracked $5.2bn worth of Bitcoin transactions reportedly to have been ransomware payments in the first half of 2021.

Analysis & Action

The Treasury's Financial Crimes Enforcement Network (FinCEN) bureau suggested in a new report that this initial figure might only be a small portion of overall payments. The $5.2bn figure is associated with 177 wallet addresses mentioned in the suspicious activity reports (SARs) sent by banks to the authorities to combat financial crime and money laundering.

FinCEN said it identified 68 ransomware families in total for all sent payments. The most frequently reported variants were REvil/Sodinokibi, Conti, DarkSide, Avaddon, and Phobos.

Although FinCEN couldn't say with complete certainty that all of the $5bn transactions it identified through blockchain analysis were ransomware related, the figures certainly re-emphasize the huge financial impact of ransomware. The full FinCEN report can be accessed here.

Privacy, Legal & Regulatory

Missouri Refers Coordinated Bug Disclosure to Prosecutors

Summary

- A newspaper reporter in Missouri who reported the exposure of Social Security numbers on a state government website has been accused of malicious hacking by the state's governor.

Analysis & Action

Missouri Governor Michael L. Parson tweeted that the person, who works for the St. Louis Post-Dispatch, gained access to the data by decoding the HTML source code through a web browser. Parson says the reporter viewed the Social Security numbers of three employees for the state's Department of Elementary and Secondary Education, known as DESE.

This individual did not have permission to do what they did, they had no authorization to convert or decode, so this was clearly a hack, the Governor said in a press conference. However, the paper says that it discovered a vulnerability in a web application on DESE's website and that the sensitive data was in plain view. The paper is rejecting accusations that its employee violated the law.

In another press conference, the governor claimed the incident could cost Missouri taxpayers as much as $50 million and divert resources from other state agencies. Parson says his office has contacted the Cole County prosecutor as well as the Missouri State Highway Patrol's digital forensics unit. Parson also alleged that the newspaper's reporting of the incident was intended to embarrass the state and is part of a political vendetta. The investigation remains ongoing.

Reference | References

Bleeping Computer
HIPAA Journal
Bleeping Computer
Healthcareinfosecurity
Gov Info Security
Health-ISAC
Gov Info Security
cisa
Info Security Magazine
Health-ISAC
Info Security Magazine
FinCEN

Tags

Daily Cyber Headlines, DCH