TLP:WHITE - Health-ISAC Daily Cyber Headlines

Daily Cyber Headlines | TLP:WHITE | Alert ID : 0f8a39db | Oct 04, 2021, 09:41 AM

Today's Headlines:

Leading Story

- White House to Host Transnational Ransomware Meeting

Data Breaches & Data Leaks

- Indian Creek Foundation Breach Affects 2,405 Patients
- Mankato Clinic Privacy Breach Affects 535 Patients

Cyber Crimes & Incidents

- Ex-Army Technician Gets 12 Years for Role in Fraud Scheme

Vulnerabilities & Exploits

- Nothing to Report

Trends & Reports

- Infant Fatality Could Be First Recorded Ransomware Death
- Business Leaders Admit Willingness to Pay Five-Figure Ransoms

Privacy, Legal & Regulatory

- FCC Announces Latest Awards From COVID-19 Telehealth Program

Upcoming Health-ISAC Events

- Health-ISAC Monthly Threat Brief – October 28, 2021, 12:00 PM Eastern

Additional Info

Leading Story

White House to Host Transnational Ransomware Meeting

Summary

- US President Joe Biden has announced plans to hold a meeting with representatives of 30 different countries later this month to discuss ransomware and other cybersecurity issues.

Analysis & Action

In a statement, President Biden said that the chief purpose of the confab would be to address the impact of cyber-threats on economic and national security. The session will take place virtually and be hosted online by the White House National Security Council.

This month, the United States will bring together 30 countries to accelerate our cooperation in combating cybercrime, improving law enforcement collaboration, stemming the illicit use of crypto-currency, and engaging on these issues diplomatically, reported the statement.

The full statement can be accessed here.

Data Breaches & Data Leaks

Indian Creek Foundation Breach Affects 2,405 Patients

Summary

- Indian Creek Foundation has notified 2,405 patients about a ransomware attack that occurred on February 6, 2021.

Analysis & Action

Steps were immediately taken to contain the attack and third-party computer forensics specialists were engaged to investigate the security breach, but it was later confirmed that actors had access to sensitive user data.

The data potentially viewed or exfiltrated by the attackers included names, Social Security number, driver's license number, health insurance information, medical treatment/diagnosis information, and financial account information.

Complimentary access to credit monitoring and identity restoration services have been offered to those individuals.

Mankato Clinic Privacy Breach Affects 535 Patients

Summary

- Mankato Clinic has discovered a breach of the protected health information (PHI) of 535 patients.

Analysis & Action

On August 3, 2021, a spreadsheet containing patient data was emailed to an external email account in error by an employee. The error was detected within a few minutes and the recipient was contacted and told to delete the email and spreadsheet.

The recipient confirmed that the email had been deleted and the spreadsheet had not been opened; however, the email was not encrypted so there is a small probability that it could have been intercepted in transit.

All employees have been provided with supplemental HIPAA training.

Cyber Crimes & Incidents

Ex-Army Technician Gets 12 Years for Role in Fraud Scheme

Summary

- A former US army contractor has been sentenced to more than 12 years in prison after pleading guilty to helping defraud thousands of military service members, veterans, and their families.

Analysis & Action

Fredrick Brown was sentenced to one count of conspiracy to commit wire fraud and one count of conspiracy to commit money laundering, following a guilty plea nearly two years ago.

As a civilian medical records technician and administrator at the US army's 65th Medical Brigade, Brown admitted to stealing the personal information of military staff, including by taking screenshots of his computer while logged into medical databases.

These details, which included names, social security numbers, military ID numbers, dates of birth, and contact information, were then sent to a Philippines-based co-conspirator. Brown is accused of using this info to access military benefits sites to steal millions of dollars.

Brown has also been ordered to pay over $2.3m in restitution and will be placed on supervised release for three years after completing his prison term.

Vulnerabilities & Exploits

Nothing to Report.

Trends & Reports

Infant Fatality Could Be First Recorded Ransomware Death

Summary

- A case making its way through US courts could prove to be the first recorded death due to ransomware.

Analysis & Action

According to papers filed in June 2020, Teiranni Kidd is accusing Springhill Memorial Hospital and its owners of failing to mitigate a crippling cyber-attack and then conspiring to hide its impact on patient care.

Kidd's daughter Nicko was born with her umbilical cord wrapped around her neck, a problem that has purportedly led to brain damage and the infant's death several months later. Fetal heart rate monitors would have usually picked up the issue. Yet medical staff could not access these from the usual location as a display had been locked by threat actors seeking a ransom payment.

If Kidd had known the extent of the technology outage at the hospital, she would have chosen to have her baby elsewhere, the suit contends.

The hospital denies any wrongdoing, and the case remains ongoing.

Business Leaders Admit Willingness to Pay Five-Figure Ransoms

Summary

- 40% of business executives would be willing to pay at least a five-figure ransom to restore operations following an attack, against the advice of governments and law enforcement, according to a new report.

Analysis & Action

Arctic Wolf polled 500 executives from UK firms with over 1000 employees to better understand their security challenges in the new hybrid workplace. Arctic Wolf also found that a fifth of UK execs have previously concealed a cyber-attack to preserve their reputation. Doing so not only impacts intelligence sharing and industry-wide threat prevention but could also land the organization in trouble with regulators.

Interestingly, despite 67% of respondents believing their company is more vulnerable to attacks if staff work remotely or in a hybrid environment, 62% are unsure whether IT teams can identify and detect some threats accurately.

The full Arctic Wolf report can be accessed here.

Privacy, Legal & Regulatory

FCC Announces Latest Awards From COVID-19 Telehealth Program

Summary

- More than 70 healthcare organizations will receive federal funds for new connected health projects through the US Federal Communications Commission's COVID-19 Telehealth Program.

Analysis & Action

The FCC has now approved a total of over $83 million in funding applications for Round 2 of its COVID-19 Telehealth Program, Acting FCC Chairwoman Jessica Rosenworcel said in a press release. The money is designated for telecommunications services, information services and connected devices necessary to enable telehealth services during the COVID-19 pandemic.

From community health clinics in urban city centers to hospitals serving rural communities across the country, these funds will support efforts to help our neighbors remain in the care of their doctors, nurses, physician assistants, and trusted health care providers during this pandemic, said the press release, which can be accessed here.

Reference | References

Info Security Magazine
Info Security Magazine
whitehouse
HIPAA Journal
Info Security Magazine
arcticwolf
Info Security Magazine

fcc
Health-ISAC
mhealthintelligence
Health-ISAC

Tags

Daily Cyber Headlines, DCH

TLP:WHITE: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

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