Health-ISAC Daily Cyber Headlines

Daily Cyber Headlines

○ TLP:WHITE

Alert ID : 405b66e7

Oct 15, 2021, 10:44 AM

Today's Headlines:

Leading Story

- US Government Warns of Insider and Ransomware Threat to Water Plants

Data Breaches & Data Leaks

- Osteopathic Professional Group Reports Year-Old Breach

Cyber Crimes & Incidents

- Crypto Romance Scam Drains $1.4M
- University of Sunderland Announced Outage Following Cyberattack

Vulnerabilities & Exploits

- Nothing to Report

Trends & Reports

- Google Sent 50,000 Warnings of State-Sponsored Attacks in 2021

Privacy, Legal & Regulatory

- New Jersey Infertility Clinic Settles Data Breach Investigation with State and Pays $495,000 Penalty

Upcoming Health-ISAC Events

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

Additional Info

Leading Story

US Government Warns of Insider and Ransomware Threat to Water Plants

Summary

- The United States (US) authorities issued an alert warning of malicious cyber-activity targeting the country’s water and wastewater systems (WWS) sector.
- The alert refers to multiple attacks over the past two years which include spear phishing, exploitation of insecure Remote Desktop Protocol (RDP), targeting of unsupported operating systems and software, and exploitation of control system devices that contain vulnerable firmware.

Analysis & Action

The alert, issued by the Cybersecurity and Infrastructure Security Agency (CISA), the Environmental Protection Agency (EPA), and the National Security Agency (NSA), highlighted multiple tactics, techniques, and procedures (TTPs) being used by a variety of actors in an attempt to compromise IT and OT systems.

It referred to multiple ransomware attacks, including a September 2020 attack on a New Jersey WWS facility, a March 2021 compromise at a Nevada plant, and an August 2021 attack at a California WWS site. In 2019, a former employee at a Kansas plant accessed and shut down key processes used to disinfect water with the intention of causing harm, and in 2021 an actor gained unauthorized access to the IT network of a WWS facility in Florida, trying to change the chemical balance of the water supply.

The agencies issuing the alert warn plant owners in the WWS sector to remain knowledgeable and aware of ongoing cyber risk to their operations, as the activity threatens the ability of WWS facilities to provide clean, potable water to, and effectively manage the wastewater of, their communities.

The full report, issued October 14, 2021, can be accessed here.

Data Breaches & Data Leaks

Osteopathic Professional Group Reports Year-Old Breach

Summary

- The American Osteopathic Association (AOA) has begun notifying nearly 28,000 individuals about a June 2020 data exfiltration incident involving their personal information.
- The medical professional organization says workforce challenges during the pandemic led to the delayed identification of people affected by the data breach.

Analysis & Action

In a breach report submitted earlier this week to the state of Maine's attorney general office, AOA says the incident affected about 27,500 individuals, including 209 Maine residents. AOA, in a sample breach notification letter provided to Maine's attorney general's office, says that on June 25, 2020, AOA became aware of suspicious activity relating to certain systems. AOA worked with third party forensic investigators to examine the nature and scope of the activity, and the AOA systems of interest, the letter notes.

AOA determined that certain information within its systems was exfiltrated by an unauthorized malicious actor. In response, AOA conducted a deliberate and thorough assessment of the information affected and to whom that information pertained, the organization says.

AOA says it is unaware of any actual or attempted malicious use of the affected information as a result of the incident but is offering affected individuals one year of complimentary credit and identity monitoring.

Cyber Crimes & Incidents

Crypto Romance Scam Drains $1.4M

Summary

- Researchers at Sophos Labs have discovered a fraudulent scam that exploits iPhone users looking for love via dating apps.

Analysis & Action

Under the CryptoRom scam, victims are contacted through their dating app account. The scammer gains the victim’s trust by exchanging direct messages with them. Once the victim becomes familiar, they ask them to install fake trading applications with legitimate-looking domains and customer support, the report stated.

Victims are then instructed to buy various financial products or invest in special “profitable” trading events. When the victim wants their money back or gets suspicious, they get locked out of the account, the report stated.

The Sophos team found that most of the scam’s victims are iPhone users based in the United States or Europe. The full Sophos report can be accessed here.

University of Sunderland Announced Outage Following Cyberattack

Summary

- A UK-based university suffered a suspected cyber-attack revealing that the public research institution suffered extensive IT issues.

Analysis & Action

Signs of an impending disruption, which occurred earlier this week, led to most of the university’s IT systems being taken down and proved to be widely impactful. According to reports, the attack affected all telephone lines, the official website, the main email servers, library WiFi, on-premise PC/laptop access, printing, and all online portals that students use for accessing eBooks, journals, and other services.

At the time of reporting, the status of the attack appeared to be in the containment phase for which no estimation was provided for when the systems would be recovered. Students with non-urgent queries were advised to follow the university's social media channels for updates in addition to referencing an alternate domain stood up by the institution.

Vulnerabilities & Exploits

- Nothing to Report.

Trends & Reports

Google Sent 50,000 Warnings of State-Sponsored Attacks in 2021

Summary

- Google has sent nearly 50,000 alerts of state-sponsored phishing or hacking attempts to customers during 2021, a considerable increase compared to the previous year.

Analysis & Action

Google sends government-backed attack alerts when detecting phishing attempts, brute-force attacks, malware delivery attempts launched from infrastructure linked to known government-sponsored threat groups. So far in 2021, we've sent over 50,000 warnings, a nearly 33% increase from this time in 2020, said a Google security engineer working with the company's Threat Analysis Group (TAG).

On any given day, TAG is tracking more than 270 targeted or government-backed attacker groups from more than 50 countries. his year, the most notable campaigns targeting Google users were coordinated by the Russian-backed APT28 hacking group linked to the GRU Russian military intelligence agency and APT35, an Iranian threat actor active since at least 2014.

Privacy, Legal & Regulatory

New Jersey Infertility Clinic Settles Data Breach Investigation with State and Pays $495,000 Penalty

Summary

- A New Jersey infertility clinic accused of violating HIPAA and New Jersey laws by failing to implement appropriate cybersecurity measures has settled the investigation with the state and will pay a $495,000 penalty.

Analysis & Action

Between August 2016 and January 2017, at least one unauthorized individual accessed Diamond Institute for Infertility and Menopause's network which contained the PHI of 14,663 patients, 11,071 of which were New Jersey residents. As a HIPAA-covered entity, Diamond is required to implement technical, physical, and administrative safeguards to ensure the confidentiality, integrity, and availability of PHI. The State of New Jersey Department of Law and Public Safety Division of Consumer Affairs investigated Diamond over the data breach to determine compliance with federal and state laws.

An investigation into the breach revealed an intruder accessed Diamond's third-party server which housed its electronic medical records within a password-protected SQL server using two compromised Diamond user accounts that had weak passwords. The investigation revealed weak security settings were in place for failed login attempts and password expiration. In addition to the financial penalty, Diamond is required to implement additional measures to improve data security, including the use of encryption to prevent unauthorized access to ePHI, and implementing a comprehensive information security program.

Reference | References

Bleeping Computer
Sophos
Info Security Magazine
Health-ISAC
Health-ISAC
Info Security Magazine
HIPAA Journal
Health-ISAC
Bleeping Computer
Healthcareinfosecurity

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