Health-ISAC Daily Cyber Headlines

Daily Cyber Headlines	○ TLP:WHITE	Alert ID : 0f2f28b2	Oct 14, 2021, 09:38 AM

Today's Headlines:

Leading Story

- EU Legislation Introduced to Ban Anonymous Domain Registration

Data Breaches & Data Leaks

- Acer Confirms Breach of After-Sales Service Systems in India

Cyber Crimes & Incidents

- Israeli Hospital Targeted by Ransomware Attack

Vulnerabilities & Exploits

- Apple Silently Fixes iOS Zero-Day, Asks Bug Reporter to Keep Quiet

Trends & Reports

- Telehealth Reimbursement Needed to Address Demand, Staffing Issues

Privacy, Legal & Regulatory

- Texas Lawmaker Eyes Telehealth Program for Rural 911 Services
- Lawmakers Ask US Congress to Create a Rural Telehealth Access Task Force

Upcoming Health-ISAC Events

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

Additional Info

Leading Story

EU Legislation Introduced to Ban Anonymous Domain Registration

Summary

- The European Union (EU) is drafting legislation that could soon end individuals registering domains anonymously on the continent.

Analysis & Action

Typically, when an Internet domain is registered, a service provider will collect information such as the purchaser's name, address, email, and phone number. However, this information is not verified to be accurate and could contain false information. The new EU directive will add new provisions regarding how domain registrars collect information from registrants and who will have access to said information.

Entities providing domain name registration services should aim to ensure the integrity and availability of such data by implementing technical and organizational measures, such as a confirmation process for registrants, according to the proposed legislation. More specifically, registrants of new domains will be required to provide a valid telephone number belonging to them, while their full name, email, and physical address will have to be verified too.

The Internet Corporation for Assigned Names and Numbers (ICANN) has taken a clear stance in favor of the new directive along with various copyright holder representatives and organizations. The proposed bill can be accessed here.

Data Breaches & Data Leaks

Brazilian E-commerce Firm Hariexpress Leaks 1.75 Billion Sensitive Files

Summary

- Around 1.75 billion sensitive files were leaked by a Brazilian e-commerce integrator that provides services to some of the country's largest online shopping websites.

Analysis & Action

According to a security researcher at Safety Detectives, who discovered the leak in July 2021, the incident is attributed to a misconfigured and unprotected ElasticSearch server. It involves more than 610GB of exposed data. The researchers noted they were unsuccessful in their attempts to resume communication with the company after initial contact.

According to the researcher, banking information relating to customers was not compromised, but the leak exposed a vast set of sensitive information, including customers' full names, email addresses, business, and residential addresses, company registration, and social security numbers.

Cyber Crimes & Incidents

Israeli Hospital Targeted by Ransomware Attack

Summary

- Hillel Yaffe Medical Center in Hadera has been targeted by a ransomware attack that affected its sensitive computer systems.

Analysis & Action

Since the attack, which occurred earlier this week, the hospital has been using alternate systems while treating patients and has been writing patients’ information down by hand. The hospital is operating as normal, except for elective, non-urgent operations. All critical equipment is working as it should, including medical equipment.

Another local hospital is prepared to accept patients who cannot be treated at Hillel Yaffe due to the cyberattack. Hillel Yaffe has asked the Israeli Health Ministry to bring patients who don't need urgent care to other hospitals. Recovery efforts remain ongoing.

Vulnerabilities & Exploits

Apple Silently Fixes iOS Zero-Day, Asks Bug Reporter to Keep Quiet

Summary

- Apple has silently fixed a zero-day vulnerability with the release of iOS 15.0.2, a security flaw that could let attackers gain access to sensitive user information.
- The company addressed the bug without crediting a software developer for the discovery even though the researcher reported the flaw seven months before iOS 15.0.2 was released.

Analysis & Action

This is not the first time the researcher was not credited. In July of 2021, Apple silently patched a zero-day flaw with the release of 14.7 without crediting the researcher, Denis Tokarev, in the security advisory, instead promising to acknowledge his report in security advisories for an upcoming update. Since then, Apple published multiple security advisories addressing iOS vulnerabilities but, each time, they failed to credit the bug report to Tokarev.

In total, Tokarev has found four iOS zero-days and reported them to Apple between March 10 and May 4, 2021. If attackers would successfully exploit the four vulnerabilities on unpatched iOS devices, they could gain access to Apple ID emails, full names, Apple ID authentication tokens, installed apps info, WiFi info, and analytics logs.

In September of 2021, Tokarev published proof-of-concept (PoC) exploit code and details on all iOS vulnerabilities after the company failed to credit him after patching the gamed zero-day in July. The full PoC code can be accessed here.

Trends & Reports

Telehealth Reimbursement Needed to Address Demand, Staffing Issues

Summary

- Telehealth reimbursement is key to continuing virtual care innovation and addressing healthcare staffing issues at primary care practices, according to a new survey from the Larry A. Green Center.

Analysis & Action

The survey found that primary care practices have come to rely on telehealth. About 40 percent of primary care clinicians surveyed as part of the ongoing survey said that at least a fifth of all office visits are done through telemedicine. Additionally, 64 percent said telehealth has been integral to maintaining access to care.

However, 41 percent of survey respondents are worried that their practice will not be able to support telehealth/telemedicine services if pre-pandemic regulations are restored. Availability of telehealth reimbursement is a major concern with the regulations, with 21 percent of clinicians saying their practice has already had to pull back on the use of telehealth since payments were reduced.

The full survey results can be accessed here.

Privacy, Legal & Regulatory

Texas Lawmaker Eyes Telehealth Program for Rural 911 Services

Summary

- A Texas lawmaker is calling for a statewide pilot project that would use telehealth to train and assist emergency responders in rural parts of the state.

Analysis & Action

Texas State Representative Drew Darby has introduced HB 76 87(3), which calls on the state to launch what he designates an next-generation telemedicine medical services and telehealth services pilot project through the Texas Tech University Health Sciences Center. The project’s goal is to give rural emergency medical service (EMS) providers a connected health resource to improve treatment and care coordination in the field.

Through the established virtual care channels, EMS providers could improve care in the field and make better decisions on whether to transport a patient to a hospital, take him or her to an alternate site of care, or help schedule an appointment with a care provider. The legislation is one of several programs proposed for telehealth services in Texas. The full bill can be accessed here.

Lawmakers Ask US Congress to Create a Rural Telehealth Access Task Force

Summary

- The Rural Telehealth Access Task Force Act, introduced by US House Representatives, would launch a federal study of how telehealth is being used, and what barriers it faces, in rural America.

Analysis & Action

US Representatives Greg Pence and Angie Craig have introduced the Rural Telehealth Access Task Force Act (HR 5506), which aims to create a federal task force to study how telehealth is used in rural parts of the country, what barriers it faces in adoption and expansion, and how federal programs to expand broadband connectivity are fostering telehealth growth.

This isn’t the first effort to develop a national rural telehealth policy. Late last year, the US Federal Communications Commission, the Department of Health and Human Services, and the Department of Agriculture signed a Memorandum of Understanding to launch an interagency Rural Telehealth Task Force to study the US Executive Order on Improving Rural and Telehealth Access.

The full bill has yet to be voted on and can be accessed here.

Reference | References

Bleeping Computer
Europa Analytics
mhealthintelligence
texas
pcpcc
Bleeping Computer
Health-ISAC
mhealthintelligence
Health-ISAC
congress
Bleeping Computer
The Jerusalem Post
ZDNet
revcycleintelligence

Tags

Daily Cyber Headlines, DCH

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