Health-ISAC Daily Cyber Headlines

Daily Cyber Headlines | TLP:WHITE | Alert ID : 3b192201 | Oct 06, 2022, 08:11 AM

Today's Headlines:

Leading Story

- Former Uber CSO Convicted for Concealing 2016 Data Theft

Data Breaches & Data Leaks

- Telstra Telecom Suffers Data Breach Potentially Exposing Employee Information
- The city of Tucson Discloses Data Breach Affecting Over 125,00 People

Cyber Crimes & Incidents

- Iranian Hackers Target Enterprise Android Users with New RatMilad Spyware
- Hundreds of Microsoft SQL Servers Backdoored with New Malware

Vulnerabilities & Exploits

- Nothing to Report

Trends & Reports

- SCADA Systems Involved in Many Breaches Suffered by US Ports

Privacy, Legal & Regulatory

- Nothing to Report

Upcoming Health-ISAC Events

- Health-ISAC Monthly Threat Brief – October 25, 2022, 12:00 PM Eastern

Additional Info

Leading Story

Former Uber CSO Convicted for Concealing 2016 Data Theft

Summary

- Uber's former Chief Security Officer has been found guilty of illegally covering up the theft of Uber drivers and customers' personal information.

Analysis & Action

Joe Sullivan was Uber's Chief Security Officer when in November 2016 Uber became the victim of a large data breach as the data of 57 million customers and driver records were compromised.

It was assessed by U.S. law enforcement institutions that Sullivan tried to pay the threat actors to recover the data pretending to pay for a bug bounty reward to cover the intention of paying for the ransom. However, as it is stipulated in California's law, any data breach should be disclosed to the authorities, therefore, Sullivan has been charged under federal statutes.

Although Sullivan's strategy on how to deal with the data breach was known by Travis Kalanick, Uber's CEO at the time, Kalanick has not been charged yet for his involvement in this case.

Data Breaches & Data Leaks

Telstra Telecom Suffers Data Breach Potentially Exposing Employee Information

Summary

- Australia's largest telecommunications company Telstra has reported that it was a victim of a data breach.

Analysis & Action

Researchers have observed the breach targeted a third-party platform called Work Life NAB that's no longer actively used by the company, and that the leaked data posted on the internet concerned a now-obsolete Telstra employee rewards program.

Telstra also noted it became aware of the breach last week, adding the information included first and last names and the email addresses used to sign up for the program. It further clarified that the data posted was from 2017. It is estimated that around 30,000 employees were affected.

The revelation comes a day after its rival Optus confirmed that nearly 2.1 million of its current and former customers suffered a leak of their personal information in the aftermath of a massive hack.

[The city of Tucson Discloses Data Breach Affecting Over 125,00 People]

Summary

- The City of Tucson has recently disclosed a data breach that has compromised the confidential information of approximately 125,000 individuals.

Analysis & Action

The City of Tucson discovered suspicious activity on its network on May 2022, and it was in September of the same year that the data breach was disclosed.

According to the City, threat actors were able to access their network between May 17 and May 31, 2022, where the personal information of 123,513 individuals was compromised. Based on the City's investigation and findings it was determined that threat actors could have potentially accessed personally identifiable information such as names, Social Security numbers, driver's licenses, and passport numbers.

The leaked information could expose the affected individuals to cybercrime-related activity such as phishing, extortion, and identity theft. The City has recommended to the notified individuals to monitor their credit reports and has offered 12 months of free access to Experian credit monitoring and identity protection services.

Cyber Crimes & Incidents

[Iranian Hackers Target Enterprise Android Users with New RatMilad Spyware]

Summary

- Security researchers have identified new Android spyware used by Iranian threat actors against enterprise users.

Analysis & Action

According to security researchers from the company Zimperium, a new Android Spyware dubbed RatMilad has been leveraged by Iranian threat actors to spy on enterprise users.

The newly discovered spyware has the capability of manipulating files, recording audio, and modifying application permissions. It was assessed that the threat actor behind this malicious campaign is known as AppMilad which distributes the spyware app through links on social media and messaging services. The threat actor also employs phishing tactics to lure the victims into sideloading the spyware into their devices.

It was also observed that the spyware can access the MAC address and user's precise location, as well as access to contacts, phone calls, SMS messages, media files, and the device's camera and microphone.

[Hundreds of Microsoft SQL Servers Backdoored with New Malware]

Summary

- A new piece of malware targeting Microsoft SQL servers has been observed by security researchers which have already infected hundreds of machines worldwide.

Analysis & Action

Security researchers were able to identify a new piece of malware dubbed Maggie, which is currently targeting Microsoft SQL servers and was observed to have infected hundreds of machines around the world.

Maggie is able to run commands and interact with files as well as extending brute-forcing administrator logins to other Microsoft SQL servers. The malware was recently discovered by a German researcher who observed that the malware has been mainly spread in India, Thailand, and China, as well as in Russia, and various European and American countries with lower intensity.

The malware also enables backdoor access to the attacker, and it offers a simple TCP redirection functionality that allows threat actors to connect to any IP address the infected MS-SQL server can reach.

Vulnerabilities & Exploits

Nothing to Report

Trends & Reports

SCADA Systems Involved in Many Breaches Suffered by US Ports

Summary

- According to the research developed by Jones Walker, there is a significant increase in cyberattacks targeting the ports and terminals industry.

Analysis & Action

The survey developed by Jones Walker has provided valuable insights that highlight how SCADA systems are involved in many of the cyberattacks that have taken place against the ports and terminals industry.

The survey included the response of 125 c-suite executives, directors, and security professionals, which demonstrated that 55% detected an attempt to breach their environment and 45% admitted having suffered a breach within the last year.

However, it was estimated that of all the data breaches, 36% involved SCADA systems. Also, it was observed that SCADA systems have been named the top cybersecurity vulnerability of U.S. ports and terminals.

The full Jones Walker survey can be accessed here.

Privacy, Legal & Regulatory

Nothing to Report

Health-ISAC Cyber Threat Level

On September 15, 2022, the Health-ISAC Threat Intelligence Committee (TIC) evaluated the current Cyber Threat Level and collectively decided to maintain the Cyber Threat Level at Blue (Guarded). The Threat Level of Blue (Guarded) was chosen in response to credential thieving and social engineering attempts with CEO Impersonation, fraudulent payment processing, EU energy crisis, Russia-Ukraine ongoing conflict, railroad strike and supply chain Issues, and IcedID and Qbot reemergence.

For more information about the Health-ISAC Cyber Threat Level, including definitions and response guidelines for each of the alert levels, please review the Threat Advisory System.

You must have Cyware Access to reach the Threat Advisory System document. Contact membership@h-isac.org for access to Cyware.

Reference | References

The Register
The Hacker News
Bleeping Computer
Security Week
Bleeping Computer
Security Week
joneswalker

Tags

RatMilad, City of Tucson, Tesltra Telecom, Daily Cyber Headlines, Uber, SCADA, DCH, Microsoft SQL Server, data breaches

Share Threat Intel: For guidance on sharing indicators with Health-ISAC via CSAP, please visit the Knowledge Base article CSAP “Share Threat Intel” Documentation at the link address provided here:

https://health-isac.cyware.com/webapp/user/knowledge-base Additionally, this collaborative medium provides opportunities for attributed or anonymous sharing across ISACs and other cybersecurity related entities.

Turn off Categories: For guidance on disabling this alert category, please visit the Knowledge Base article CSAP "Alert Categories" Toggle Documentation at the link address provided here: https://health-isac.cyware.com/webapp/user/knowledge-base

Access the Health-ISAC Intelligence Portal: Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Cyware.

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