Health-ISAC Daily Cyber Headlines

Daily Cyber Headlines | TLP:WHITE | Alert ID : c8937599 | Oct 20, 2021, 03:20 PM

Today's Headlines:

Leading Story

- Over 30 Countries Pledge to Fight Ransomware Attacks

Data Breaches & Data Leaks

- Verizon-Owned Visible Acknowledges Hack and Confirms Account Manipulations

Cyber Crimes & Incidents

- Sinclair TV Network Crippled by Potential Ransomware Attack
- Phishing Attack on Business Associate affects Tens of Thousands of Professional Dental Alliance Patients

Vulnerabilities & Exploits

- Fake Android Apps Steal Credentials from Japanese Telecom Users

Trends & Reports

- REvil Ransomware Shuts Down Again After Tor Sites were Hijacked

Privacy, Legal & Regulatory

- Australia Plans Ransomware Attack Reporting Requirement

Upcoming Health-ISAC Events

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

Additional Info

Leading Story

Over 30 Countries Pledge to Fight Ransomware Attacks

Summary

30 countries pledged to mitigate risks associated with ransomware.

Analysis & Action

Representatives from 30 countries assembled to define and discuss ransomware as an escalating global security threat with serious economic and security consequences.

Notably absent from the list of countries in the list were China and Russia.

The recent focus on ransomware has generated invaluable discussion on the value of information sharing. Organizations sharing and receiving indicators in an automated manner can better protect their infrastructure from threat actors.

The pledge promotes incident sharing between ransomware victims, law enforcement, and cyber emergency response teams (CERTs).

Additional details are available in the October 2021 Joint Statement of the Ministers and Representatives from the Counter Ransomware Initiative Meeting.

Data Breaches & Data Leaks

Verizon-Owned Visible Acknowledges Hack and Confirms Account Manipulations

Summary

Visible confirmed account manipulations and a hack on October 14, 2021, after users complained of hacked accounts and fraudulent charges A spokesperson for the company initially denied the compromise.

Analysis & Action

Visible, an all-digital wireless carrier owned by Verizon, addressed issues its users were having with their accounts over a Twitter thread after initially denying any compromises. Multiple customers complained of being locked out of accounts, changed addresses, and fraudulent charges. Customers have been urged to review account information and change password and security questions to their accounts, as well as reviewing any other accounts that share the same email, login, or password credentials.

Visible has issued a review of the issues and deployed mitigation tools as well as enabled additional controls to protect members. Threat actors were able to access login information from outside sources and exploit that information to access Visible accounts.

Cyber Crimes & Incidents

Sinclair TV Network Crippled by Potential Ransomware Attack

Summary

TV stations owned by the Sinclair Broadcast Group went down with the likely cause being a ransomware attack

Sinclair Broadcast Group is a prominent media company and a leading sports and news provider owning multiple national networks

Analysis & Action

Recently, a perceived ransomware attack involving the Sinclair Broadcast Group caused significant technical issues. Analysis of the incident revealed that the threat actors were able to impact several TV stations using Sinclair's corporate Active Directory domain as the attack vector.

The threat actors were able to shut down Active Directory services for the domain which led to wide disruption for the entire organization and affiliates by blocking access to domain resources across the network.

Several corporate assets were taken down in the incident, including the email servers, broadcasting, and newsroom systems, forcing TV stations to create Gmail accounts to receive news tips from viewers and use PowerPoint for newscasts graphics.

[Phishing Attack on Business Associate Affects Tens of Thousands of Professional Dental Alliance Patients]

Summary

Professional Dental Alliance has notified tens of thousands of patients that some of their protected health information was stored in email accounts that were accessed by an unauthorized individual between March 31 and April 1, 2021.

The breach occurred at a vendor and steps were immediately taken to secure affected accounts, with no evidence of attempted or actual misuse of patient data found.

Analysis & Action

Professional Dental Alliance's vendor, North American Dental Management, suffered a breach in protected health information (PHI) after patient data was stored in email accounts that were accessed by an unauthorized individual between March 31 and April 1, 2021. The breach occurred after employees responded to phishing emails, and investigators concluded that the breach was likely limited to credential harvesting.

The affected email accounts contained names, addresses, email addresses, phone numbers, insurance information, Social Security numbers, dental information, and financial information; however, the electronic dental records and dental images were not accessed. Affected individuals have been recommended exercising caution and monitoring their data for signs of misuse.

Vulnerabilities & Exploits

Fake Android Apps Steal Credentials from Japanese Telecom Users

Summary

The malware-lace fraudulent app steal credentials and session cookies
The app will prompt the user to grant certain permissions, thus enabling the attacker to obtain network connections on devices

Analysis & Action

Upon execution of the malicious app, the user is prompted to connect to cellular networks and disable Wi-Fi. The fraudulent app pivots to the telecommunications official webpage that accommodates payment. The log-in then requires a network PIN number that is given to the customer when the subscription is confirmed. The app will then display the official payments URL in WebView to lure the victims and continues to hide malicious strings to block reverse engineering and detection. The information is then sent to an attacker's email using Simple Mail Transfer Protocol (SMTP).

Phishing via imitating an official app of any popular software is a common yet effective tactic. Moreover, the attackers behind the malicious Android apps are using multiple techniques to stay hidden from security solutions. It is recommended that users refrain from downloading apps from unknown third-party stores and use the official app store only.

Trends & Reports

REvil Ransomware Shuts Down Again After Tor Sites were Hijacked

Summary

The REvil ransomware operation has likely shut down once again after an unknown person hijacked their Tor payment portal and data leak blog

Analysis & Action

Recently, an affiliate threat actor of the REvil ransomware operation, advised that the Tor sites used for victim payment and data
leaking were hijacked. The message was posted to the XSS hacking forum, revealing that the unknown hijacker used the same private keys as REvil's Tor sites and likely has backups of the domains.

Initially there were no signs of compromise to the ransomware gang's servers, however, the incident was grounds to shutting down the operation. As a contingency, the threat actor told affiliates to contact them for campaign

decryptions keys via the chat service Tox. This is likely so affiliates can continue extorting their victims and provide a decryptor if a ransom is paid.

The affiliate later discovered that the servers were indeed compromised and that the party responsible was targeting them. After law enforcement and other like-minded operations gained access to, and released, the master REvil decryption key some threat actors believe those entities have had access to the servers since they relaunched. It is also possible that the original REvil representative, Unknown, is trying to regain control over the operation.

Privacy, Legal & Regulatory

Australia Plans Ransomware Attack Reporting Requirement

Summary

Australia will require larger businesses to report ransomware attacks to the government as part of a comprehensive strategy that also includes criminal penalties and assistance for victims.

Analysis & Action

A multi-agency task force called Operation Orca will be created and run by the Australian Federal Police.

Another part of the action plan is helping organizations better defend themselves against ransomware. Increased preparedness will help protect organizations and reduce the incentive to pay ransoms.

The Australian Cyber Security Center (ACSC) produced the Ransomware Attacks – Prevention and Protection Guide as well as Emergency Response Guide to aid organizations.

Reference | References

The Hacker News
whitehouse
ZDNet
Bleeping Computer
HIPAA Journal
Cyble
Bleeping Computer
Healthcareinfosecurity
Australian Government

Tags

Daily Cyber Headlines, DCH