Health-ISAC™

Collaborating for Resilience in Healthcare

Daily Cyber Headlines

Daily Cyber Headlines ○ TLP:WHITE Alert ID : 1068b954 Oct 25, 2023, 08:14 AM

Today's Headlines:

Leading Story

- Cyberattack on Health Services Provider Impacts 5 Canadian Hospitals

Data Breaches & Data Leaks

- Cyber-Attack Shuts Down South Florida Imaging Clinic

Cyber Crimes & Incidents

- 34 Cybercriminals Arrested in Spain for Multi-Million Dollar Online Scams
- Ukraine Cyber Officials Warn of a Surge in Smokeloader Attacks

Vulnerabilities & Exploits

- VMware Warns Admins of Public Exploit for vRealize RCE Flaw

Trends & Reports

- Cyberattacks on Kenya Drop in Third Quarter
- September Was a Record Month for Ransomware Attacks in 2023

Privacy, Legal & Regulatory

- Nothing to Report

Cybersecurity Awareness Month

- The Daily Cyber Headlines are being shared during the month of October at **TLP:WHITE** for Cybersecurity Awareness Month.

Upcoming Health-ISAC Events

- Health-ISAC Monthly Threat Brief – October 31, 2023, 12:00 PM Eastern

Additional Information

Leading Story

Cyberattack on Health Services Provider Impacts 5 Canadian Hospitals

Summary

- Shared service provider, TransForm, was impacted by a cyber-attack and the consequences have impacted five Canadian hospitals.

Analysis & Action

A cyberattack on TransForm, a shared service provider used by hospitals in Canada resulted in a negative impact on patient care, resulting in the mandatory rescheduling of appointments. TransForm is a shared service provider founded by five Canadian hospitals to manage multiple facets of IT infrastructure.

This service monitored IT infrastructure, supply chain, and accounts payable, making it an attractive target to threat actors. The five hospitals that founded TransForm, and were affected when it was attacked are as follows: Windsor Regional Hospital; Hotel Dieu Grace; Erie Shores Healthcare; Hospice of Windsor-Essex; Chatham-Kent Health Alliance.

There has been very limited correspondence from TransForm regarding the nature of the cyber-attack, but members are advised to be wary of a potential uptick in suspicious communications citing this incident.

Data Breaches & Data Leaks

Cyber-Attack Shuts Down South Florida Imaging Clinic

Summary

- Radiology and oncology healthcare provider from Florida facing severe operational disruptions due to a ransomware attack.

Analysis & Action

Akumin, an outpatient radiology and oncology healthcare provider from Florida, was impacted by a cyber-attack this month.

The attack was allegedly discovered on October 11, when the company detected suspicious activity on their network. The discovery was followed by a shutdown of IT systems. 50 Akumin centers and offices faced operational disruptions which are still ongoing. Akumin stated they are currently unable to see patients at these locations and that most of the clinical and diagnostic operations are postponed for the moment.

The incident was reportedly a ransomware attack. It is currently unclear which, if any, files, and patient data were breached in the attack. We advise members to continuously monitor their systems for suspicious activity to prevent substantial breaches.

Health-ISAC created a Slack channel with additional details on the incident available to members here.

Cyber Crimes & Incidents

34 Cybercriminals Arrested in Spain for Multi-Million Dollar Online Scams

Summary

- Spanish Law Enforcement officials arrested 34 members of a criminal group responsible for online scams.

Analysis & Action

The unnamed threat actors had 34 members arrested and 16 different locations searched. While the Spanish Law Enforcement uncovered items like swords, cash, and cars, they also found a database with the information of more than four million people after they infiltrated the databases of financial and credit institutions.

After gaining access to these databases, the threat actors added funds to customer accounts and asked that they pay it back by clicking on a link that captured the user credentials. The threat actors were believed to have used both false documentation and spoofing techniques to hide their identity and directly invest their profits in cryptocurrencies.

Members are advised to train their employees and inform patients to report any potential scams to them to get them resolved. Employees should confirm that any emails or texts they receive are legitimate, and not click on any links in these messages until they have made sure of such.

Ukraine Cyber Officials Warn of a Surge in Smokeloader Attacks

Summary

- Russian hacking groups have increased activity targeting Ukrainian financial and government organizations.

Analysis & Action
Russian hacking groups have increased activity targeting Ukrainian financial and government organizations with Smokeloader malware.

Threat actors are targeting these organizations with phishing attacks trying to gain initial access to their systems and ultimately steal sensitive information. Smokeloader can install malicious software on infiltrated computers and perform a variety of functions such as data and credential theft, denial-of-service (DDoS) attacks, and keyboard interception. In the latest campaign on Ukrainian organizations, attackers used financial themed phishing emails to get victims to download malicious attachment, and ultimately gain access to the system.

According to the Ukraine's National Cyber Security Coordination Center (NCSCC) researchers, Ukrainian organizations have been frequently targeted by both financially and state-sponsored actors, indicating that the threat landscape has evolved into a multifaceted arena.

Vulnerabilities & Exploits

VMware Warns Admins of Public Exploit for vRealize RCE Flaw

Summary

- VMware warns of PoC exploit code being available for CVE-2023-34051.

Analysis & Action
VMware warned its customers about proof-of-concept (PoC) exploit code made publicly available for the authentication bypass vulnerability affecting vRealize Log Insight, also known as VMware Aria Operations for Logs.

The vulnerability, tracked as CVE-2023-34051 allows, under certain conditions, unauthenticated users with root privileges to execute code remotely. Publicly available POC exploit code might trigger an increase in activity of threat actors attempting to exploit the vulnerability on unpatched devices.

Members who use VMware devices are advised to immediately apply the latest patches to mitigate the risk of a successful attack. More information can be accessed in VMware’s advisory here.

Trends & Reports

Cyberattacks on Kenya Drop in Third Quarter

Summary

- Kenya has noticed an 11.36% decrease in cyber threats due to increased training of their cybersecurity personnel and increased cybersecurity awareness.

Analysis & Action
A report from the Kenya Computer Incident Response Team Coordination Centre (KE-CIRT/CC) found a sharp decline in the number of cyber threat events. From July to September of this year (2023), the KE-CIRT/CC detected around 124 million cyber threat events, which is around 11.36% less than the 139.7 million threat events detected in the previous quarter.

Kenya has been a hotspot for cyber-attacks, being the third most targeted country in Africa behind South Africa and Nigeria. From July 2022 up until June 2023, Kenya was victim to more than 855 million attacks.

Members should ensure not only their cybersecurity teams, but all their other employees receive proper cybersecurity awareness education and training for what to do in the event of an attack.

September Was a Record Month for Ransomware Attacks in 2023

Summary

- The National Cybersecurity Center (NCC) reports on the concerning number of ransomware cyberattacks that occurred in September 2023.

Analysis & Action
The number of ransomware cyberattacks in September 2023 has surpassed the number of ransomware cyberattacks that occurred in March 2023 with 55 more attacks than the latter. The most targeted sectors in September were the industrial (Engineering, construction, and commercial services) sector, consumer cyclicals (Retail, media, hotels) sector, technology sector, and healthcare sector.

Threat groups, such as LockBit 3.0, LostTrust, and BlackCat have aided in setting these records, with LostTrust being a new threat actor group. The NCC's findings show that roughly one out of five attacks that occurred in September came from a new ransomware group, highlighting emerging threat groups in their ability to advance and adapt.

The increasing number of ransomware attacks will continue to grow if mitigations are not considered. Members are encouraged to refresh staff memory on identifying suspicious content within unprompted emails and downloads. The ability to swiftly identify threat actors from legitimate email sources will help decrease the number of ransomware attacks.

Privacy, Legal & Regulatory

- Nothing to Report.

Health-ISAC Cyber Threat Level

On October 19, 2023, the Health-ISAC Threat Intelligence Committee (TIC) evaluated the current Cyber Threat Level and collectively decided to raise the Cyber Threat Level to Yellow (Elevated). The Threat Level of Yellow (Elevated) is due to threats from concerns regarding hacktivist activity related to the conflict in the Middle East, an uptick in LinkedIn profile impersonations, MFA Bypass, QR code phishing, and the actively exploited Cisco IOS XE bug.

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

Dark Reading
Bleeping Computer
VMware
The Record
Bleeping Computer
islandernews
The Hacker News
Bleeping Computer

Tags

Ukraine Targeting, VMware, Ransomware

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