SHARING SINCE 2010 Health-ISAC™
Collaborating for Resilience in Healthcare

Daily Cyber Headlines

Daily Cyber Headlines ○ TLP:WHITE Alert ID : 57296aa1 Oct 06, 2023, 07:33 AM

Today's Headlines:

Leading Story

- Red Cross Releases Ethical Guidelines for Hacktivists in War

Data Breaches & Data Leaks

- Lyca Mobile Investigates Customer Data Leak After Cyberattack

Cyber Crimes & Incidents

- Cyberattacks in Arizona, Missouri Limit Access to Community Services

Vulnerabilities & Exploits

- Nothing to Report

Trends & Reports

- Amazon to Make MFA Mandatory for 'Root' AWS Accounts by Mid-2024
- Cybercrime Gangs Now Deploying Ransomware Within 24 Hours of Hacking Victims

Privacy, Legal & Regulatory

- New Cybersecurity FAR Rules Poised to Have a Major Impact on Contractors

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

- Americas Hobby Exercise - October 25, 2023. Registration is available here.
- Health-ISAC Monthly Threat Brief – October 31, 2023, 12:00 PM Eastern

Additional Information

Leading Story

Red Cross Releases Ethical Guidelines for Hacktivists in War

Summary

- The International Committee of the Red Cross (ICRC) has released the first ethical guidelines for hacktivists during armed conflicts.

Analysis & Action

The ICRC has asked hacktivists to comply with 8 humanitarian law-based rules to protect themselves and avoid harming others. The rules do not prohibit hacking military targets during armed conflicts, but they should refrain from targeting civilian objects or deploying malware that impacts both military and civilian targets.

Additionally, the ICRC urges attackers not to target medical and humanitarian facilities, drinking water systems, and hazardous plants and that they should not threaten civilians or attempt to enlist other hackers in their cause. The ICRC guidelines also say that governments should not promote or accept civilian hackers engaging in cyber operations and should create laws and regulations governing civilian hacking.

This is the first attempt by an organization at regulating hacktivist activities. It is unclear whether more international bodies or any governments will attempt to implement any regulations regarding hacktivist groups. Members should monitor any future hacktivist regulations that emerge.

Data Breaches & Data Leaks

Lyca Mobile Investigates Customer Data Leak After Cyberattack

Summary

- Lyca Mobile experienced unexpected disruptions due to a cyberattack that potentially compromised consumer data.

Analysis & Action

Lyca Mobile, a mobile telecommunication and Voice Over Internet Protocol (VoIP) company headquartered in the United Kingdom, was a victim of a cyberattack over the weekend. The attack resulted in interruptions in 56 out of the 60 countries that Lyca Mobile provides services to.

While Lyca believes that all records are fully encrypted, a statement released about encrypted customer data indicates that they suspect there was some unauthorized access to its databases. The statement does not, however, specify or clarify the type of encryption they use to protect customer data. Most of Lyca Mobile's services are available, but there are certain operational services that are unavailable in some affected countries.

It is recommended that members who use Lyca Mobile as their telecommunications provider stay alert for any further updates and statements from the company regarding their services and potential data breach impacts.

Cyber Crimes & Incidents

Cyberattacks in Arizona, Missouri Limit Access to Community Services

Summary

- Incidents of cyberattacks affecting hospitals in both Arizona and Missouri have prevented patients from accessing critical services.

Analysis & Action

According to The Record, cyberattacks have affected the systems of Mt. Graham Regional Medical Center (MGRMC) in Arizona and the St. Louis Metro Call-A-Ride service for people with disabilities in Missouri.

Both entities are currently investigating the source of the cyberattacks. MGRMC is currently determining the status of patient data and information while IT officials are working on bringing back phone and computer lines to those who utilize the St. Louis Metro Call-A-Ride service.

Cyberattacks against hospitals and key health transportation services can lead to immense impacts on critical systems and patients. Members are encouraged to update their security systems regularly to prevent attacks against hospital systems and auxiliary services.

Vulnerabilities & Exploits

- Nothing to Report

Trends & Reports

Amazon to Make MFA Mandatory for 'Root' AWS Accounts by Mid-2024

Summary

- Starting in mid-2024, Amazon will require privileged Amazon Web Services (AWS) accounts to use Multi-Factor Authentication (MFA).

Analysis & Action

Amazon AWS is a very popular cloud service provider used by many companies. To keep customer data safe, Amazon is going to begin to require all privileged account users to enable MFA in 2024.

At the time of writing, enabling MFA on AWS accounts is an optional security measure that customers can choose to enable. The MFA mechanism used in AWS supports third-party authenticator apps. Authenticator apps that meet the Fast Identity Online 2 (FIDO2) standards may exhibit enhanced reverse proxy man-in-the-middle attack resistance. This kind of attack has been becoming increasingly popular in 2023 and is typically conducted in phishing attacks.

Members are advised to encourage employees to enable MFA on all accounts so threat actors must bypass an additional layer of security after obtaining a username and password, minimizing the risk of data loss.

Cybercrime Gangs Now Deploying Ransomware Within 24 Hours of Hacking Victims

Summary

- Recent trends are showing an uptick in quicker deployments of ransomware.

Analysis & Action

Cybercriminals have been adapting to intensifying sanctions and crackdowns against cybercriminal activity. These threat actors are implementing simpler and quicker operations against targeted systems rather than complex enterprise-wide attacks to save time.

The simplification of threat actor operations proves to be just as dangerous, as threat actors have been able to lower their dwelling time of 4.5 days to just 24 hours for implementing malware and ransomware. The sudden decrease in dwell time is due to the cybercriminals' desire for a lower chance of detection from their victim's updated security.

Members are recommended to verify sources of downloads and/or emails that are deemed suspicious and update their security systems as soon as possible to patch up any vulnerabilities.

Privacy, Legal & Regulatory

New Cybersecurity FAR Rules Poised to Have a Major Impact on Contractors

Summary

- The Federal Acquisition Regulatory (FAR) Council issued two new rules. The first rule imposes incident reporting and the second standardizes requirements for unclassified federal information systems.

Analysis & Action

The Federal Acquisition Regulatory (FAR) Council has proposed two new rules to implement specific parts of US President, Joe Biden's Executive Order that aims to improve the nation's cybersecurity. The two rules will change compliance and reporting for government contractors in all industries.

The first, FAR Case 2021-017, proposes a new clause to FAR 52.239-ZZ and FAR 52.239-AA that, if passed, would create new incident reporting and all information to be submitted to the Cybersecurity & Infrastructure Security Agency (CISA) within eight hours of discovering the initial incident. The second, FAR Case 2021-019, creates a minimum set of standards and requirements for all Federal Information Systems (FIS). The new clauses to FAR 52.239 YY and 52.239 XX would direct agencies to use Federal Information Processing Standards (FIPS) Publication 199 as a means of assessment for all FIS.

Any members who are either currently government contractors or plan to be should read FAR Cases 2021-017 and 2021-019 with great scrutiny and prepare to comply with these new rules if passed. Members who are currently a part of the government or under a government contract have until December 4 to comment on these new proposed rules.

Health-ISAC Cyber Threat Level

On September 20, 2023, 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) is due to threats from concerns regarding malvertising, rogue USB drives, Async RAT, MFA Bypass, and persistent credential stuffing/spraying.

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 Record
Bleeping Computer
The Record
Bleeping Computer
The Record
hklaw

Tags

Deployment Times, FAR Council, Mandatory MFA, Ethical Guidelines, Telecommunication Company, cyber attacks

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