Health-ISAC™

*Collaborating for Resilience in Healthcare*

# Daily Cyber Headlines

Daily Cyber Headlines ○ TLP:WHITE Alert ID : 862e41a6 Oct 20, 2023, 08:42 AM

**Today's Headlines:**

### Leading Story

- Ragnar Locker Ransomware's Dark Web Extortion Sites Seized by Police

### Data Breaches & Data Leaks

- Casio Discloses Data Breach Impacting Customers in 149 Countries

### Cyber Crimes & Incidents

- North Korean Hackers Exploit Critical TeamCity Flaw to Breach Networks
- Iranian Hackers Lurked in Middle Eastern Govt Network for 8 Months

### Vulnerabilities & Exploits

- Patch Now: APTs Continue to Pummel WinRAR Bug

### Trends & Reports

- Use of QR Codes in Phishing Campaigns Is on the Rise

### Privacy, Legal & Regulatory

- Nothing to Report

### Privacy, Legal & Regulatory

- Five-Year-Old Privacy Goals Still Unmet by Many Federal Agencies

### 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**

Ragnar Locker Ransomware's Dark Web Extortion Sites Seized by Police

**Summary**

- The data leak and negotiations site used by the Ragnar Locker ransomware group has been seized because of an international law enforcement operation.

**Analysis & Action**

On the morning of October 19, the data leak and negotiation sites associated with Ragnar Locker displayed a banner explaining that the infrastructure had been seized as part of an international law enforcement operation.

Ragnar Locker is a prolific ransomware group that is responsible for high-profile ransomware attacks in Europe, including the ransomware attack on the city of Antwerp, Belgium. While infrastructure has been seized, a new ransomware group, DarkAngels, has been seen using a modified version of Ragnar Locker's VMWare ESXi encryptor.

This month has resulted in numerous ransomware takedowns. Most recently, the hacktivist outfit Ukrainian Cyber Alliance (UCA) took down Trigona ransomware and exfiltrated their data which they plan to share with law enforcement. Members are advised to stay current with cybercriminal takedowns to glean an accurate view of the cyber threat landscape

**Data Breaches & Data Leaks**

Casio Discloses Data Breach Impacting Customers in 149 Countries

**Summary**

- Casio announced that they were the victim of a data breach of their ClassPad education platform.

**Analysis & Action**

Casio, the Japanese electronics manufacturer, disclosed that threat actors gained access to their ClassPad servers. The ClassPad database within the company's development environment included information such as customer names, emails, service usage details, purchase information, and more.

As of Wednesday, 91,921 pieces of information were accessed from Japanese customers, and more than 35,049 from the rest of the world. ClassPad does remain operational, as threat actors only compromised the database within the environment, not the systems themselves. Casio is working with both external cybersecurity and forensics experts to find the causes of these attacks.

Members who use Casio services or have any of their information stored in their ClassPad servers should find out what, and if any, specific information of theirs got leaked. Members should ensure their systems have sufficient operational management, in order to prevent any potential operational errors of the systems each security and development department is responsible for securing.

## Cyber Crimes & Incidents

### North Korean Hackers Exploit Critical TeamCity Flaw to Breach Networks

**Summary**

- Microsoft confirmed Lazarus and Andariel breached their TeamCity servers.

**Analysis & Action**

Microsoft announced that North Korean threat actors Lazarus and Andariel exploited the CVE-2023-42793 vulnerability to deploy backdoor malware into TeamCity servers. The vulnerability being exploited gives threat actors the unauthenticated ability to remotely execute code. CVE 2023-42793 was patched in September 2023, but many unpatched instances remain.

Microsoft believes that these attacks could be part of a larger mission to conduct supply chain attacks. Once threat actors have gained access to TeamCity servers through CVE-2023-42793, they deploy Remote Access Trojans (RATs) to maintain access into compromised networks, followed by credential harvesting to move laterally.

Members should continue to patch all known vulnerabilities to prevent access to their networks. Members should also be aware of any new admin accounts being created without authorization.

### Iranian Hackers Lurked in Middle Eastern Govt Network for 8 Months

**Summary**

- The Iranian hacking group tracked as MuddyWater breached at least 12 computers belonging to a Middle Eastern government network and maintained access for eight months.

**Analysis & Action**

Symantec observed that the attacks were used to steal passwords and data and install a PowerShell backdoor dubbed PowerExchange.

The attacks first began on February 1, 2023, and utilized a wide assortment of malware, tools, and malicious activity until September 2023. The threat actors conducted reconnaissance activities, lateral movement, and data exfiltration/harvesting, highlighting the groups' broad-spectrum capabilities. Along with their proficiency in multiple tools.

It is unclear what the group MuddyWater was looking for directly, but the threat actors remain active despite their toolset being leaked back in 2019. Members are advised to consume cyber threat intelligence to ensure their cybersecurity measures to ensure that they will hold up against the latest techniques used by threat actors.

## Vulnerabilities & Exploits

### Patch Now: APTs Continue to Pummel WinRAR Bug

**Summary**

- Advanced Persistent Threats (APTs) sponsored by Russia and China continue to target vulnerabilities in WinRAR systems with malware.

**Analysis & Action**

Organizations that use WinRAR, particularly in Ukraine and Papua New Guinea, are at risk of the vulnerability labeled as CVE-2023-38831 being exploited by state-sponsored threat actors. Ukrainian energy infrastructure has been targeted before by Russian threat actors, while Chinese threat actors
have been observed launching infostealing campaigns against users in Papua New Guinea.

Threat actors will be able to deliver backdoor malware, steal private information, and execute arbitrary code as long as these systems remain vulnerable. The combination of temporary file expansion and a Windows ShellExecute quirk while attempting to open a file tends to lead to the potential exploitation of CVE-2023-38831.

Members who use WinRAR are recommended to update their systems as soon as possible, especially members located in Ukraine and in Papua New Guinea. Keeping a consistent schedule of updating systems will decrease the chances of cyberattacks by threat actors.

## Trends & Reports

### Use of QR Codes in Phishing Campaigns Is on the Rise

**Summary**

- Phishing campaigns using QR codes are becoming increasingly popular among threat actors.

**Analysis & Action**

Threat actors are leaning more into using QR codes to launch phishing attacks. Cybersecurity firm, Hoxhunt, found that more than 22% of phishing campaigns in October used QR codes. As QR codes continue to rise in popularity, so does the effectiveness of QR-code-based attacks.

What makes these attacks so dangerous is their scope. A threat actor can place a sticker of a new QR code over the sticker on a table at a restaurant that has a phishing link from within where their information can be stolen, or malware is downloaded onto a device.  Threat actors can also engage in QRLJacking, which lures a user to scan or click on a malicious QR code sent directly to their mobile devices.

Members should inform their employees not to scan or click on QR codes coming from malicious sources. They should also be warned to look for irregularities in QR codes in public, like a peeling sticker.

## Privacy, Legal & Regulatory

- Nothing to Report

## 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

**Bleeping Computer**
**Bleeping Computer**
**Security Week**
**txone**
**SC Magazine**
**Bleeping Computer**
**IC3**

### Tags

Casio, RagnarLocker, Ragnar Locker, WinRaR

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

### 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