# DAILY CYBER HEADLINES

## Health-ISAC Daily Cyber Headlines

 TLP:GREEN

Aug 17, 2023

**Today's Headlines:**

**Leading Story**

- Incident Response Lessons Learned from the Russian Attack on Viasat

**Data Breaches & Data Leaks**

- 1.5 million Impacted by Ransomware Attack at Canadian Dental Service

**Cyber Crimes & Incidents**

- Mirai Common Attack Methods Remain Consistent, Effective

**Vulnerabilities & Exploits**

- Critical Security Flaws Affect Ivanti Avalanche, Threatening 30,000 Organizations

**Trends & Reports**

- Google Introduces First Quantum Resilient FIDO2 Security Key

**Privacy, Legal & Regulatory**

- Meta Expected to Face Health Privacy Lawsuit

**Upcoming Health-ISAC Events**

- Health-ISAC Monthly Threat Brief – August 29, 2023, 12:00 PM Eastern

## Leading Story

Incident Response Lessons Learned from the Russian Attack on Viasat

**Summary**

- The National Security Agency (NSA) and Ukrainian Viasat discussed the details of a significant cyber-attack against satellite infrastructure.

**Analysis & Action**

At two major cybersecurity conferences taking place in the United States, representatives from Viasat and the NSA gave detailed accounts of the cyber-attack which shut down tens of thousands of modems in early 2022.

The modems in question were used by commercial elements in Ukraine and by the government of Ukraine. Therefore, the outage was labeled the first significant cyber-attack of the Russia/Ukraine conflict.

The attack was originally categorized as a wiper attack, but the effects were much farther reaching in actuality. To read the comprehensive overview of the incident, click here.

## Data Breaches & Data Leaks

1.5 million Impacted by Ransomware Attack at Canadian Dental Service

**Summary**

- Canadian dental benefits administrator Alberta Dental Service Corporation (ADSC) has started informing roughly 1.47 million individuals that their personal information was compromised in a ransomware attack last month.

**Analysis & Action**

ADSC was able to recover the affected systems and data with minimal impact to its operations.

Potentially compromised information varies depending on the benefits plan but may include names, addresses, birth dates, government-issued identification numbers, details of dental benefits claims, personal bank account numbers, corporate emails, and corporate bank accounts.

While ADSC did not share specific details on the ransomware gang, IT World Canada reported a ransom payment was made to 8Base for proof of deletion.

The attack appears to have been the result of a phishing email being opened.

## Cyber Crimes & Incidents

### Mirai Common Attack Methods Remain Consistent, Effective

**Summary**

- The Internet of Things botnet, Mirai, has been observed to have consistent attack patterns.

**Analysis & Action**

According to security researchers, the IoT botnet Mirai has kept its attack methodology relatively consistent. However, this does not mean that the botnet is ineffective.

Mirai is responsible for some of the largest attacks by volume ever seen. It has also been observed to be using actively updated modules to continue to exploit vulnerabilities in IoT devices to amass a large attack platform.

Health-ISAC recommends implementing mitigation strategies listed in the Health-ISAC DDoS Mitigation White Paper to minimize organizational exposure.

## Vulnerabilities & Exploits

### Critical Security Flaws Affect Ivanti Avalanche, Threatening 30,000 Organizations

**Summary**

- Critical security flaws in Ivanti Avalanche enterprise mobile device management were discovered that could allow an attacker to execute code.

**Analysis & Action**

The vulnerabilities include stack-based buffer overflows in v6.4.0.0 of Avalanche Server as well as a directory traversal bug.

The issues were discovered by researchers at Tenable. Additional details from the Tenable team are available for review here.

Ivanti has released v6.4.1 to remediate all seven of the vulnerabilities.

## Trends & Reports

Google Introduces First Quantum Resilient FIDO2 Security Key

**Summary**

- Google announced the first quantum resilient security key implementation as part of its OpenSK security keys initiative.

**Analysis & Action**

Google's first quantum resilient FIDO2 key uses a novel ECC/Dilithium hybrid signature schema. The key benefits from the security of the ECC against standard attacks and Dilithium's resilience against quantum attacks. OpenSK is an open-source implementation for security keys written in Rust that supports both FIDO U2F and FIDO2 standards.

Google plans to add support for quantum-resistant encryption algorithms in Chrome 116 to set up symmetric keys in TLS connections. Google's proposed FIDO2 security key implementation is a mix of Elliptic and Curve Digital Signature Algorithm (ECDSA) and the quantum resistant signature algorithm Dilithium. The hybrid signature schema is ideal to run on security keys' constrained hardware as it only requires 20 KB of memory.

Google said it is hoping that the implementation or a variant of it being standardized as part of the FIDO2 key specification and supported by major web browsers so that users' credentials can be protected against quantum attacks.

**Privacy, Legal & Regulatory**

Meta Expected to Face Health Privacy Lawsuit

**Summary**

- Facebook users allege Meta Platforms tracks online visits to hospital websites and monetizes the data collected from those sites.

**Analysis & Action**

In May of 2022, several patients alleged in a class-action complaint that Meta tracks their visits to hospital websites via the Meta Pixel.

The complaint included claims that Meta violated wiretap and privacy laws, and that the company misrepresented its policies by claiming that publishers only send data to Meta if they have the legal right to do so.

Meta stated outside developers configure their websites and decide what information to transmit and added that web developers are instructed not to send health information.

**Health-ISAC Cyber Threat Level**

On July 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 Citrix NetScaler exploitation, MOVEit transfer MFT active exploitation, an observed spike in phishing attacks leveraging QR codes, and increased domain squatting.

**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(s)** | CSO Online, Security Week, IT World Canada, Dark Reading, The Hacker News |

**Alert ID** af7851c4

## View Alert

**Tags** FIDO2, Viasat, Ivanti, Mirai

**TLP:GREEN** Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.

### 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

Download Health-ISAC’s Information Sharing App.

For more update and alerts, visit: **https://health-isac.cyware.com**

If you are not supposed to receive this email,
please contact us at **toc@h-isac.org**.