# DAILY CYBER HEADLINES

## Daily Cyber Headlines

TLP:GREEN

Nov 06, 2024

**Today’s Headlines:**

### Leading Story

- Warning: Hackers Could Take Over Your Email Account by Stealing Cookies, Even if You Have MFA

### Data Breaches & Data Leaks

- Nokia Starts Investigating Source Code Data Breach Claims

### Cyber Crimes & Incidents

- Exfiltration Over Telegram Bots: Skidding Infostealer Logs
- Memorial Hospital and Manor Recovering from Ransomware Attack

### Vulnerabilities & Exploits

- Google Warns of Actively Exploited CVE-2024-43093 Vulnerability in Android System

**Trends & Reports**

- Nothing to Report

**Privacy, Legal & Regulatory**

- Canadian Hacker Behind Snowflake Data Breach Arrested in High-Profile Cyber Case
- South Korea Fines Meta $15.67M for Illegally Sharing Sensitive User Data with Advertisers

**Upcoming Health-ISAC Events**

- Global Monthly Threat Brief
  - Americas – November 26, 2024, 12:00-01:00 PM ET
  - European – November 27, 2024, 03:00-04:00 PM CET
- T-SIG Webinar for SMB Members – November 14, 2024 at 11:30 AM ET
- Fall Americas Summit, Phoenix, Arizona - December 2-6, 2024

## Leading Story

Warning: Hackers Could Take Over Your Email Account by Stealing Cookies, Even if You Have MFA

### Summary

- FBI warns threat actors have managed to find a way to bypass multi-factor authentication and access accounts.

### Analysis & Action

The FBI warns that cybercriminals are stealing session cookies to access email accounts despite multi-factor authentication (MFA).

When you log in and create a session, a unique session ID is stored in a session cookie on your browser. If stolen, criminals can access your account, even with MFA. This is a significant threat to email services like Gmail and Outlook. Once in your account, hackers can gather personal info, send phishing emails, and reset passwords on other accounts. Deploying malware on a device is a common way for criminals to steal session cookies.

To protect email accounts, Health-ISAC advises using security software, keeping devices updated, reconsidering using the Remember me option, deleting cookies, visiting secure sites, and monitoring login history regularly. Be vigilant to prevent unauthorized access to your sensitive information.

## Data Breaches & Data Leaks

Nokia Starts Investigating Source Code Data Breach Claims

### Summary

- Threat actor IntelBroker's claims of a cyberattack on Nokia have sparked investigations by the company.

### Analysis & Action

In the past three days, threat actor IntelBroker has spread the idea of a committed data breach on tech company Nokia. In response, Nokia has launched a forensic investigation to track the attack and its origins.

The potential of these attacks is concerning as data stolen could contain highly sensitive data like SSH keys, source code, SMTP credentials, Bitbucket credentials, RSA keys, and webhooks. If the data is proven to have been compromised, threat actors can exploit the company's systems and intellectual properties. Currently, sources point to stolen data being sold on BreachForums, an underground site, for $20,000. The data involved is believed to be source code and access credentials, attracting threat groups to purchase for acts of espionage or further financial compensation. Fortunately, there does not seem to be an immediate risk to Nokia’s infrastructure; however, early claims state that core data infrastructure and internal systems have not been directly impacted. The company is likely to come out with a statement regarding the situation to address those concerned in the near future.

Data breaches and leaks are becoming common tactics used by threat actors to gain compensation and notoriety, making protective measures all the more important. Health-ISAC recommends its members back up and encrypt sensitive data to minimize the impacts of similar attacks.

## Cyber Crimes & Incidents

### Exfiltration Over Telegram Bots: Skidding Infostealer Logs

**Summary**

- The rising popularity of the Telegram platform allows threat actors to engage in illicit activities, including exfiltration methods for info stealer malware.

**Analysis & Action**

The Telegram platform is seeing increasing growth from threat actors, who are used for both messaging and the illicitation of activities and methods.

The service can now be used by threat actors as a server for data exfiltration. This server can be used for the well-known infostealer malware in addition to a marketplace in which stolen data from victims can be sold. Amongst the stolen data could be information such as credentials pertaining to users or employees. These credentials can be utilized further to access corporate systems and environments, creating further risks due to the collaboration. The main targets for these infostealer malware incidents are countries like the US, Russia, and Turkey, with Germany and India also seeing some incidents. Through an analysis, a total of 27 logs were parsed, each generated by infostealer families, SnakeKeylogger and AgentTesla holding the majority of those uploaded logs. A large number of these families have been discovered to be open source as well. Additionally, 28 million credentials have been extracted in relation to 5 million logs, with over 400,000 unique domains and 10,000 unique IP addresses. Credentials discovered relate mainly to Technology but span all sectors like Finance and Government.

Enhancements to security protocols and services are best to prevent processes from being exploited due to these discrepancies. Health-ISAC recommends its members block APIs that aren't utilized by your business and implement authentication and encryptions to company accounts to prevent possible incidents in the future.

Memorial Hospital and Manor Recovering from Ransomware Attack

**Summary**

- Memorial Hospital and Manor works to maintain transparency regarding the latest cyberattack.

**Analysis & Action**
Memorial Hospital and Manor in Georgia, United States, swiftly informed patients about a ransomware attack just one day after it was discovered.

The attack affected the hospital's IT systems, including its electronic medical record system, email system, and website. Despite this disruption, patient care is still being provided, albeit with potential delays due to manual record-keeping. The hospital chose to disclose the incident promptly to maintain transparency.

Memorial Hospital and Manor is currently investigating the extent of the attack and considering recovery options, with unknown impact on patient data at this time. Health-ISAC advises members to monitor their systems for suspicious activity continuously to be able to detect an intrusion as fast as possible.

## Vulnerabilities & Exploits

Google Warns of Actively Exploited CVE-2024-43093 Vulnerability in Android System

**Summary**

- The Android operating system used by Google has been impacted by a new security flaw through active exploitation.

**Analysis & Action**
A  new security flaw has been discovered, impacting the Android operating system utilized by tech giant Google. Google has since issued warnings about the flaw, which is under active exploitation.

The vulnerability has been marked as CVE-2024-43093. Details show the vulnerability to revolve around a flaw regarding the escalation of privileges in Androids Framework component. The result of this flaw can lead to unauthorized access being gained to a variety of directories and sub directories including “Android/data”, “Android/sandbox”, “and “Android/obb”. At this time, no information has been released on how these vulnerabilities are being utilized in real-world scenarios, with Google indicating the possibility of their being exploited under limited, targeted exploitation. This comes after another vulnerability was recently patched by Google, CVE-2024-43047, which was actively exploited using Qualcomm chipsets. This new vulnerability is the second within the year pertaining to Android frameworks, the other being CVE-2024-32896, which was patched back in the month of June. It is unknown at this time if any of these vulnerabilities are part of a larger chain for privilege elevations and code execution methods.

Health-ISAC recommends its members assign specific permissions to control content access, use authentication realms, and use forms of encryption to work against those trying to access differing types of directories and prevent similar incidents.

## Trends & Reports

Nothing to Report.

## Privacy, Legal & Regulatory

### Canadian Hacker Behind Snowflake Data Breach Arrested in High-Profile Cyber Case

### Summary

- Law enforcement in Canada has arrested a threat actor who committed a cyberattack on Snowflake Inc.

### Analysis & Action

An arrest has been made on a singular threat actor who committed a data breach on Snowflake Inc., a large warehousing company for cloud data with customers such as AT&T, Capital One, Adobe, and Mastercard. The man is now set to appear in court and faces the possibility of extradition.

The threat actor had executed a number of data breaches, impacting a minimum of 165 customers of services. An assessment of the actor's past actions points to his campaign beginning in the early months of the year and escalating in April. The man targeted more than 100 organizations, and his actions would cause large disruptions to their services. In Snowflake's case, the man could obtain demo accounts that lacked secure protection. Cybercriminals often use these methods to gain attention from the media and gain profits. In the attacks, malware tools such as Racoon Stealer, Lumma, MetaStealer, Vidar, Redline, and RisePro were utilized to steal users' credentials. Snowflake identified an employee account as the threat actor's entry point, and it is now bolstering its security practices despite releasing statements detailing the breach not being due to platform flaws.

Cloud-based security services continue growing in popularity, highlighting the importance of protection against critical breaches like this. Health-ISAC recommends its members issue the latest patches and limit file sharing to weaken threat actors' opportunities to administer malware to critical systems.

### South Korea Fines Meta $15.67M for Illegally Sharing Sensitive User Data with Advertisers

#### Summary

- South Korea fined Meta for gathering user information and selling it to advertisers without permission.

#### Analysis & Action

South Korea's data privacy watchdog has fined Meta 15,67 million dollars for gathering sensitive personal information from Facebook users and sharing it with advertisers without consent.

The Personal Information Protection Commission found Meta collected data on 980,000 users' religious beliefs, political views, and same-sex marriage status, and shared it with advertisers. Specific behavioral information was used to create advertising topics based on sensitive data.

Meta was accused of processing this information without a legal basis and failing to secure inactive accounts, leading to a leak of personal data from 10 users. The commission will ensure Meta complies with corrective measures to protect citizens' data.

### Health-ISAC Cyber Threat Level

On October 17, 2024, 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:

The Threat Level of Yellow (Elevated) is due to threats from elections-related smishing campaigns, DPRK remote worker activity, potential repercussions of recent activity in the Middle East, commodity malware, and a recent uptick in ransomware events.

**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)** | Malwarebytes Labs, thecyberexpress, The Hacker News, FBI, Bitsight, The Hacker News, HIPAA Journal, cybersecurity-insiders |
| **Report Source(s)** | Health-ISAC |

**Alert ID** 37780d9c

**View Alert**

Share Feedback
was this helpful?

👍 👎

**Tags** Snowflake Incident, Source Code Leak, Account Takeover, Meta, Infostealers, Android vulnerability, Nokia, Ransomware

**TLP:GREEN** TLP:GREEN Limited disclosure, recipients can ONLY share this within their TRUST community. Recipients should consider the information proprietary and may ONLY share TLP:GREEN information with peers and partner organizations within their TRUST community, SHARING IS NOT PERMITTED via social media, public websites and/or other publicly accessible channels.

**Share Threat Intel**
For guidance on sharing indicators with Health-ISAC via HTIP, please visit the Knowledge Base article "HTIP - Share Threat Intel" here.

The "Share Threat Intel" feature allows for attributed or anonymous sharing across ISACs and other cybersecurity-related entities.

**Turn off Categories**
For guidance on disabling alert categories, please visit the Knowledge Base article "HTIP Alert Categories" here.

**Access the Health-ISAC Threat 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 Health-ISAC Threat Intelligence Portal (HTIP).

**For Questions or Comments**

Please email us at toc@h-isac.org

Download Health-ISAC’s Information Sharing App.

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

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