Health-ISAC Daily Cyber Headlines

Daily Cyber Headlines **TLP:WHITE** **Alert Id: cad76f69** **2022-10-20 12:37:16**

Today's Headlines:

Leading Story

- New Ursnif Variant Likely Shifting Focus to Ransomware and Data Theft

Data Breaches & Data Leaks

- Microsoft Data Breach Exposes Customers' Contact Info, Emails

Cyber Crimes & Incidents

- The Missed Link Between Ransom Cartel and REvil Ransomware Gangs
- Brazilian Police Arrest Suspected Member of Lapsus$ Hacking Group

Vulnerabilities & Exploits

- Hackers Using New Version of FurBall Android Malware to Spy on Iranian Citizens

Trends & Reports

- CISA Warns of Critical Flaws Affecting Industrial Appliances from Advantech and Hitachi

Privacy, Legal & Regulatory

- Nothing to Report

Upcoming Health-ISAC Events

- Health-ISAC Monthly Threat Brief – October 25, 2022, 12:00 PM Eastern

Leading Story

New Ursnif Variant Likely Shifting Focus to Ransomware and Data Theft

Summary

- Ursnif malware has become the latest malware to shed its roots as a banking trojan to revamp itself into a generic backdoor capable of delivering next-stage payloads.

Analysis & Action

Ursnif, also called Gozi or ISFB, is one of the oldest banker malware families, with the earliest documented attacks going as far back as 2007.

The refreshed and refactored variant is seen as an attempt to lay the groundwork for potential ransomware and data theft extortion operations.

The latest attack chain demonstrates the use of recruitment and invoice-related email lures as an initial intrusion vector to download a Microsoft Excel document, which then fetches and launches the refactored Ursnif malware.

Data Breaches & Data Leaks

Microsoft Data Breach Exposes Customers' Contact Info, Emails

Summary

- Microsoft account data on approximately 65,000 people were leaked via a faulty cloud storage configuration.

Analysis & Action

According to the analyst at SOCRadar, Microsoft misconfigured Azure Blob Storage which ultimately led to the leak. No data has been compromised at thew time of writing.

As cloud technology begins to become wildly adopted, cloud cybersecurity will become critical to business resiliency. This amount of damage caused by a faulty configuration file shows merely the tip of the iceberg when it comes to potential cloud data breaches.

In the near future, it is likely that companies will begin storing all their sensitive information with cloud service providers; emphasizing further the importance of cybersecurity.

Cyber Crimes & Incidents

The Missed Link Between Ransom Cartel and REvil Ransomware Gangs

Summary

- Security researchers at Palo Alto Networks discovered the linkage between threat actors Ransom Cartel and REvil.

Analysis & Action

In 2021, the ransomware group REvil was wreaking havoc on the cyber threat landscape. They were found to be behind the infamous Kaseya hack.

However, the group went dark in October 2021 due to pressure from law enforcement entities. About two months later, The Ransom Cartel began its operations.

Malware Analysts at Palo Alto Networks discovered that the ransomware note used by The Ransom Cartel and REvil are similar, the encryptors are similar, and they both have the same intrusion vector.

Brazilian Police Arrest Suspected Member of Lapsus$ Hacking Group

Summary

- Brazilian authorities arrested an alleged member of the Lapsus$ cybercriminal group.

Analysis & Action

This arrest was the end result of the Brazilian federal law enforcement investigation known as Operation Dark Cloud.

Operation Dark Cloud was started after a series of Brazilian national health service websites suffered data breaches due to malicious cyber activity from the Lapsus$ gang.

Lapsus$ is an international cybercrime ring with members being arrested in several countries including Israel and the United Kingdom. The successful arrests of its members show that law enforcement takes cybercrime seriously and does its best to hold people accountable for cybercrimes.

Vulnerabilities & Exploits

Hackers Using New Version of FurBall Android Malware to Spy on Iranian Citizens

Summary

- The Iranian threat actor known as Domestic Kitten has been attributed to a new mobile campaign that masquerades as a translation app to distribute an updated variant of an Android malware known as FurBall.

Analysis & Action

Furball malware, in its present form, can retrieve commands from a remote server that allows it to gather contacts, files from external storage, a list of installed apps, basic system metadata, and synced user accounts.

While the core spyware functions are retained in the latest version, the artifact requests only one permission to access contacts, limiting it from accessing SMS messages, device location, call logs, and clipboard data.

Campaigns undertaken by the group have traditionally relied on luring potential victims into installing a rogue application via different attack vectors, including Iranian blog sites, Telegram channels, and SMS messages.

Trends & Reports

CISA Warns of Critical Flaws Affecting Industrial Appliances from Advantech and Hitachi

Summary

- The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Tuesday released two Industrial Control Systems (ICS) advisories pertaining to severe flaws in Advantech R-SeeNet and Hitachi Energy APM Edge appliance.

Analysis & Action

The advisories consist of three weaknesses in the R-SeeNet monitoring solution, successful exploitation of which could result in an unauthorized attacker remotely deleting files on the system or allowing remote code execution.

The list of issues entails CVE-2022-3385, CVE-2022-3386, and CVE-2022-3387.

Also published by CISA is an update to a December 2021 advisory about multiple flaws in Hitachi Energy Transformer Asset Performance Management (APM) Edge products that could render them inaccessible.

Privacy, Legal & Regulatory

Nothing to Report

Health-ISAC Cyber Threat Level

On September 15, 2022, 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) was chosen in response to credential thieving and social engineering attempts with CEO Impersonation, fraudulent payment processing, EU energy crisis, Russia-Ukraine ongoing conflict, railroad strike and supply chain Issues, and IcedID and Qbot reemergence.

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): The Hacker News, Bleeping Computer, Security Affairs, The Hacker News, The Hacker News, The Hacker News

Tags: Lapsus$ Group, Daily Cyber Headlines, CISA Advisory, DCH, REvil, Ursnif, Microsoft

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