DAILY CYBER HEADLINES

Health-ISAC Daily Cyber Headlines

TLP:WHITE

Oct 26, 2022

Today's Headlines:

Leading Story

- Ukrainian Charged for Operating Raccoon Stealer Malware Service

Data Breaches & Data Leaks

- Dutch Police Arrest Hacker Who Breached Healthcare Software Vendor

Cyber Crimes & Incidents

- Vice Society Targets Schools with Multiple Ransomware Families

Vulnerabilities & Exploits

- CISA Warns of Attacks Exploiting Cisco, Gigabyte Vulnerabilities
- VMware Fixes Critical Cloud Foundation Remote Code Execution Bug
- 22-Year-Old Vulnerability Reported in Widely Used SQLite Database Library

Trends & Reports

- Incident Response Trends in Q3 2022

Privacy, Legal & Regulatory

- Nothing to Report

Upcoming Health-ISAC Events

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

Leading Story

Ukrainian Charged for Operating Raccoon Stealer Malware Service

Summary

- A Ukrainian national has been charged due to his involvement in the Racoon Stealer malware as a service cybercrime operation.

Analysis & Action

Mark Sokolovsky, 26 years old, has been recently charged for his involvement in the malicious cybercrime operation Raccoon Stealer malware.

Racoon Stealer is a malware-as-a-service cybercrime operation that offers malware for rent to various threat actors. Attackers can rent the service for $75 per week or $200 per month. This type of malware is very attractive for cybercriminals as it allows them to harvest various types of valuable data such as browser credentials, credit card information, cryptocurrency wallets, and other sensitive related data.

The FBI has assessed that Raccoon Stealer malware has been able to steal more than 50 million unique credentials and forms of identification and in cooperation with the Dutch authorities it was possible to arrest Sokolovsky, who is expected to be extradited to the United States.

Data Breaches & Data Leaks

Dutch Police Arrest Hacker Who Breached Healthcare Software Vendor

Summary

- Dutch authorities have arrested an individual due to his suspected involvement in breaching the systems of a healthcare software vendor.

Analysis & Action

A 19-year-old man has been arrested in the Netherlands by the Dutch police due to his involvement in a data breach affecting a healthcare software vendor in the country.

The Dutch police was able to assess that the systems' breach included various types of valuable data such as personal and medical data of patients of the health providers that use the company systems. The compromise data could expose affected individuals to cybercrime-related activity such as phishing, extortion, and identity theft.

Although the authorities have not disclosed the name of the breached company, security researchers observed that Nedap, a Dutch technology company disclosed a security incident in its Carenzorgt.nl medical portal, which is used by approximately 9,000 healthcare providers. At the moment of writing, no evidence of stolen documents has been observed on the dark web, however, investigations are still ongoing.

Cyber Crimes & Incidents

Vice Society Targets Schools with Multiple Ransomware Families

Summary

- According to Microsoft, the threat actor Vice Society has been using different payloads in its ransomware attacks against the education sector.

Analysis & Action

Vice Society has been observed targeting the education sector multiple times across this year, especially focusing its malicious targeting in the U.S., however, the threat actor is now switching payloads when performing ransomware attacks.

Researchers at Microsoft were able to determine that Vice Society is switching between BlackCat, QuantumLocker, Zeppelin, and a Vice society branded variant dubbed Zeppelin ransomware, as well as modifying the payloads of RedAlert. Apart from switching payloads, the threat actor has also employed HelloKity/Five Hands ransomware.

Some of Vice Society's latest victims include Los Angeles Unified (LAUSD), and the Austrian Medical University of Innsbruck.

Additional information on CISA and FBI's advisory regarding Vice Society can be accessed here.

Vulnerabilities & Exploits

CISA Warns of Attacks Exploiting Cisco, Gigabyte Vulnerabilities

Summary

- CISA has released a new warning and added Cisco product vulnerabilities to its Known Exploited Vulnerabilities catalog.

Analysis & Action

CISA has added two vulnerabilities affecting a Cisco product and four affecting a Gigabyte product to its Known Exploited Vulnerabilities catalog, as one of the vulnerabilities was exploited in previous attacks.

The two Cisco vulnerabilities affecting the AnyConnect Secure Mobility Client for Windows are tracked as CVE-2022-3433 and CVE-2020-3153 and could allow an attacker to execute arbitrary code and achieve elevated privileges. It was stated by Cisco that no exploitation has been registered regarding these vulnerabilities.

Additionally, four vulnerabilities affecting a Gigabyte product were added to CISA's catalog. The vulnerabilities are tracked as CVE-2018-19323, CVE-2018-19322, CVE-2018-19321 and CVE-2018-19320, and they affect GPCIDrv and GDrv low-level drivers in the Gigabyte App Center, the Aorus graphics engine, the Xtreme gaming engine, and the OC Guru utility. It was assessed that the vulnerabilities, in conjunction, could allow a local attacker to escalate privileges and take complete control of the system. From all these vulnerabilities, only CVE-2018-19320 has been observed under active exploitation by the Robinhood ransomware.

VMware Fixes Critical Cloud Foundation Remote Code Execution Bug

Summary

- A critical vulnerability affecting VMware Cloud Foundation has been fixed on a security update recently released by VMware.

Analysis & Action

The vulnerability affects VMware Cloud Foundation, and it could allow threat actors to exploit the vulnerability without authentication that does not require user interaction.

The vulnerability is tracked as CVE-2021-39144 and was assigned as CVSS score of 9.9 out of 10. The security update released by VMware explains that due to an unauthenticated endpoint that leverages XStream for input serialization in VMware Cloud Foundation NSX-V, a malicious actor can get remote code execution in the context of root on the appliance.

VMware has decided to update XStream to version 1.4.19 in order to block exploitation. If patches for this vulnerability cannot be addressed immediately it is recommended to establish a workaround that is also available in the VMware security advisory.

Additional information on workarounds regarding CVE-2021-39144 can be accessed here.

22-Year-Old Vulnerability Reported in Widely Used SQLite Database Library

Summary

- A high-severity vulnerability has been disclosed in the SQLite database library, which was introduced as part of a code change dating all the way back to October 2000 and could enable attackers to crash or control programs.

Analysis & Action

Tracked as CVE-2022-35737, the 22-year-old issue affects SQLite versions 1.0.12 through 3.39.1, and has been addressed in version 3.39.2 released on July 21, 2022.

Researchers have observed arbitrary code execution is confirmed when the library is compiled without stack canaries, but unconfirmed when stack canaries are present, and denial-of-service is confirmed in all cases.

Programmed in C, SQLite is the most widely used database engine, included by default in Android, iOS, Windows, and macOS, as well as popular web browsers such as Google Chrome, Mozilla Firefox, and Apple Safari.

Trends & Reports

Incident Response Trends in Q3 2022

Summary

- Cisco Talos Incident Response Team has released a threat summary for Q3 2022, including valuable insights regarding the ransomware threat landscape.

Analysis & Action

According to Cisco Talos Incident Response Team, there are multiple top threats that should be taken into consideration for companies to remain safe.

Some of the main threats observed by Cisco Talos is ransomware, as an equal number of ransomware and pre-ransomware engagements, approximately 40%, close out this quarter. Pre-ransomware engagements made up 185 of engagements this quarter, up significantly from less than 5% last quarter.

Also, the Incident response team was able to observe threat groups appearing in various engagements, namely Hive, Vice Society, and Black Basta. Although the main threats were related to ransomware, it was also possible to determine that commodity malware such as Qakbot banking trojan and info stealers like Redline have gained notoriety during attacks.

Cisco Talos' Q3 2022 full executive summary can be accessed here.

Privacy, Legal & Regulatory

Nothing to Report

Health-ISAC Cyber Threat Level

On October 20, 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 ongoing Qbot activity, fraudulent Help Desk activity, ongoing ransomware attacks, observed credential phishing, and foreign policy quandaries amid midterm elections.

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)	Bleeping Computer, Bleeping Computer, Bleeping Computer, CISA, Security Week, Bleeping Computer, VMware, The Hacker News, Cisco Talos

Alert ID 879bfe55

View Alert

Tags Carengzorgt, Daily Cyber Headlines, Vice Society, DCH, Raccoon Stealer, Gigabyte, VMWare, Ransomware, cisco

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

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**.