Health-ISAC Daily Cyber Headlines

Daily Cyber Headlines **TLP:WHITE** **Alert Id: dce7b55a** **2022-10-04 12:14:52**

Today's Headlines:

Leading Story

- White House Highlights Cybersecurity Awareness Month

Data Breaches & Data Leaks

- Russian Retail Chain DNS Confirms Hack After Data Leaked Online

Cyber Crimes & Incidents

- Comm100 Chat Provider Hijacked to Spread Malware in Supply Chain Attack
- Researchers Link Cheerscrypt Linux-Based Ransomware to Chinese Hackers

Vulnerabilities & Exploits

- Microsoft Exchange Server Zero-Day Mitigation Can Be Bypassed

Trends & Reports

- Bumblebee Malware Loader's Payload Significantly Vary by Victim System

Privacy, Legal & Regulatory

- Nothing to Report

Upcoming Health-ISAC Events

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

Leading Story

White House Highlights Cybersecurity Awareness Month

Summary

- Joe Biden has designated October as Cybersecurity Awareness Month as a way to encourage public and private organizations to take immediate action to protect against cyber threats.

Analysis & Action

Cybersecurity has been considered as a wicked problem due to the different academic domains and sectors it encompasses, and it has been demonstrated that cooperation is essential for ensuring cybersecurity.

Cybersecurity awareness can be used and leveraged by public and private organizations to improve or enhance their current cybersecurity and cyber resilience. For instance, the U.S. President has stated that the government cannot meet cyber resilience goals alone, as private and public sector collaboration is essential to protect critical infrastructure and prevent threat actors from destroying, corrupting, or stealing information.

Cybersecurity Awareness Month's objectives are also to encourage citizens to increase their cybersecurity at home by enabling multifactor authentication, setting strong and unique passwords, as well as fostering cybercrime reporting.

Data Breaches & Data Leaks

Russian Retail Chain DNS Confirms Hack After Data Leaked Online

Summary

- The Russian retail chain Digital Network System (DNS) was the victim of a cyberattack that caused the leak of confidential data.

Analysis & Action

The Russian retail chain, DNS, has recently disclosed that due to a security incident it has suffered a data breach that compromised and exposed the confidential information of its customers and employees.

According to the company, the cyberattack was perpetrated by a threat actor outside of Russia and was observed to be leveraging DNS' security gaps to perform the attack. DNS did not provide any major details on what type of data was compromised, however, it mentioned that financial information was compromised.

According to the information posted on a hacking forum, the data breach included names, usernames, email addresses, and phone numbers of approximately 16 million individuals. The leaked information could expose individuals to cybercrime-related activities such as phishing, extortion, and identity theft.

Cyber Crimes & Incidents

Comm100 Chat Provider Hijacked to Spread Malware in Supply Chain Attack

Summary

- Threat actors attributed to a new supply chain attack that involves the use of a trojanized installer for the COmm100 Live Chat application to distribute a JavaScript backdoor.

Analysis & Action

The scale of the attack is currently unknown, but the trojanized file is said to have been identified at organizations in the industrial, healthcare, technology, manufacturing, insurance, and telecom sectors in North America and Europe. Comm100 is a Canadian provider of live audio/video chat services with more than 15,000 customers in 51 countries. Researchers have concluded the threat actor is most likely in association with China.

Embedded within the weaponized executable is a JavaScript-based implant that executes a second-stage JavaScript code hosted on a remote server, which is designed to provide the actor with

surreptitious remote shell functionality.

Supply chain compromises, like that of SolarWinds and Kaseya, are becoming an increasingly lucrative strategy for threat actors to target popular software providers to gain a foothold in victim's networks.

Researchers Link Cheerscrypt Linux-Based Ransomware to Chinese Hackers

Summary

- Security researchers have linked the newly discovered ransomware strain known as Cheerscrypt to a Chinese cyber espionage group.

Analysis & Action

Security researchers at the security firm Sygnia have linked the new ransomware strain Cheerscrypt to the Chinese cyberespionage group Emperor Dragonfly, also known as Bronze Starlight.

According to the research, it was possible to determine that the open-source tools leveraged by Emperor Dragonfly are written in Chinese, which reinforces the claim that the attacker operates from China. Emperor Dragonfly could be understood as a dynamic threat actor as it has employed multiple ransomware families in its arsenal including LockFile, Night Sky, Pandora, LockBit 2.0, and now it is employing Cheerscrypt.

The Cheerscrypt ransomware has the capacity to target VMware ESXi servers and threat actors leveraging this ransomware family commonly employ double extortion techniques.

Vulnerabilities & Exploits

Microsoft Exchange Server Zero-Day Mitigation Can Be Bypassed

Summary

- Microsoft released mitigations for two Microsoft Exchange zero-day vulnerabilities, however, researchers argue that the mitigations can be bypassed.

Analysis & Action

Two zero-day vulnerabilities were recently disclosed affecting Microsoft Exchange, the vulnerabilities are tracked as CVE-2022-41040 and CVE-2022-41082.

After the disclosure of these vulnerabilities, Microsoft released mitigation recommendations for organizations to remain secure until patches are released. However, security researchers have published their findings demonstrating that the mitigations are not efficient and could be bypassed with little effort.

Although in the advisory released by Microsoft it was established that the mitigations apply for on-premise Exchange Server and that Exchange Online clients did not need to take action, many organizations have a hybrid setup combining on-prem with cloud deployment making hybrid setups also vulnerable. At the moment of writing no patches have been released for the vulnerabilities.

Trends & Reports

Bumblebee Malware Loader's Payload Significantly Vary by Victim System

Summary

- The Bumblebee malware has been observed developing and employing new characteristics that make this malware an evolving threat.

Analysis & Action

The Bumblebee malware is evolving as security researchers observed that its payload for systems that are part of an enterprise network is different from its payload for standalone systems.

Also, the malware behaves differently after infecting machines and different threat groups have been registered leveraging the malware. Also, Bumblebee has attracted attention due to its sophistication levels as it has the capacity to ensure anti-virtualization and anti-sandbox checks and is able to check for running processes for signs of malware activity.

The malware has been constantly evolving over 2022 as it was observed switching from using ISO files to VHD format files by applying a PowerShell script before switching back to ISO. It is recommended for organizations to use Bumblebee indicators of compromise to apply detection and prevention measures within their environment.

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): Health IT Security, Bleeping Computer, The Hacker News, The Hacker News, Bleeping Computer, Dark Reading

Tags: Cybersecurity Awareness Month, Comm100 Live Chat, BumbleBee Loader, Daily Cyber Headlines, DCH, data breaches, Microsoft Exchange, DNS

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