Health-ISAC Daily Cyber Headlines

Daily Cyber Headlines **TLP:WHITE** **Alert Id: 24e7e823** **2022-10-27 11:51:27**

Today's Headlines:

Leading Story

- Notorious BestBuy Hacker Arraigned for Running Dark Web Market

Data Breaches & Data Leaks

- Online Ticketing Company See Pwned for 2.5 years by Attackers

Cyber Crimes & Incidents

- Unknown Actors are Deploying RomCom RAT to Target Ukrainian Military
- Kimsuky Hackers Spotted Using 3 New Android Malware to Target South Koreans

Vulnerabilities & Exploits

- Microsoft Warns of Actively Exploited Vulnerabilities in Exchange Server

Trends & Reports

- Ransomware Gang Ramp Up Industrial Attacks in the U.S.

Privacy, Legal & Regulatory

- Nothing to Report

Upcoming Health-ISAC Events

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

Leading Story

Notorious BestBuy Hacker Arraigned for Running Dark Web Market

Summary

- A British hacker was arraigned by the U.S. Department of Justice due to his alleged involvement in running a dark web marketplace.

Analysis & Action

Daniel Kaye, a 34-year-old British hacker, was brought to court as he was believed to be responsible for running The Real Deal dark web marketplace.

It was assessed by the authorities that Kaye run the dark web marketplace between 2015 and 2016 before it shut down. Within The Real Deal, threat actors had the opportunity to sell stolen information from U.S. government agencies as well as other illegal assets such as weapons and drugs.

Some of the observed data offered for sale in the dark web marketplace is linked to various organizations such as NASA, the Centers for Disease Control and Prevention, and the U.S. Postal Service. Kaye is accused of attempting to sell Social Security Numbers, as well as laundering cryptocurrencies.

Data Breaches & Data Leaks

Online Ticketing Company See Pwned for 2.5 years by Attackers

Summary

- See tickets has recently disclosed that malicious actors breached its network which have compromised confidential information.

Analysis & Action

See tickets is a major global player in the online event ticketing business, however, it has recently disclosed a major data breach that has been ongoing since 2019.

According to the organization, malicious actors were able to infiltrate their systems in 2019 by implanting data stealing malware on event checkout pages. It was assessed that due to this malicious activity, the threat actors would have been able to access affected individuals' names, addresses, zip codes, payment card numbers, card expiry dates, and CVV numbers. Therefore, individuals could be exposed to financial-related cybercrime activities, as well as extortion.

In March 2021 the forensic investigation was launched, and it was not until August of the same year that the unauthorized activity was finally shut down. For instance, the breach lasted approximately two and a half years and so far, the company has not been able to assess how many customers' data has been compromised.

Cyber Crimes & Incidents

Unknown Actors are Deploying RomCom RAT to Target Ukrainian Military

Summary

- A new spear phishing campaign has been recently observed by security researchers targeting Ukrainian military institutions.

Analysis & Action

Security researchers have observed a new spear phishing campaign that leverages RomCom, a remote access trojan, and that targets Ukrainian military institutions.

The spear phishing campaign is new as it was first observed on October 21, 2022, and it was analyzed by security researchers that once the victim installs a trojanized bundle, it drops RomCom RAT into the system. Also, researchers have observed that the threat actor behind this malicious activity continues to refine and evolve its tactics, techniques, and procedures, as it has switched the use of a trojanized Advanced Ip scanner to a pdfFiller.

This highlights the interest of the threat actor to thwart detection to ensure information is being harvested and capturing screenshots that will then be exported to a remote server.

Kimsuky Hackers Spotted Using 3 New Android Malware to Target South Koreans

Summary

- The North Korean espionage-focused actor known as Kimsuky has been observed using three different Android malware strains to target users located in its southern counterpart.

Analysis & Action

Findings from South Korean cybersecurity company S2W has identified these malware families as FastFire, FastViewer, and FastSpy. The FastFire malware is disguised as a Google security plugin, and the FastViewer malware disguises itself as Hancom Office Viewer, while FastSpy is a remote access tool based on AndroSpy.

Kimsuky, also known by the names Black Banshee, Thallium, and Velvet Chollima, is believed to be tasked by the North Korean regime with a global intelligence-gathering mission, disproportionately targeting individuals and organizations in South Korea, Japan, and the U.S.

Researcher has observed Kimsuky group has continuously performed attacks to steal the target's information targeting mobile devices. In addition, various attempts are being made to bypass detection by customizing Androspy, an open-source remote access tool.

Vulnerabilities & Exploits

Microsoft Warns of Actively Exploited Vulnerabilities in Exchange Server

Summary

- Cisco Talos has released a threat advisory regarding two vulnerabilities that are under active exploitation and affect Microsoft Exchange Servers.

Analysis & Action

According to Cisco Talos’ threat advisory, two threats affecting Microsoft Exchange Servers are under active exploitation. The vulnerabilities are tracked as CVE-2022-41040 and CVE-2022-41082 and in conjunction could allow an attacker to execute remote code on the targeted server as well as enabling remote code execution when PowerShell is accessible to the attackers.

Both vulnerabilities only affect Microsoft Exchange Servers 2013, 2016, and 2019, however, no patches have been released yet by Microsoft. Cisco Talos was able to determine that webShells such as Antsword, a popular Chinese language-based open-source webshell, SharPyShell an ASP.NET-based webshell and China Chopper have been deployed on compromised systems.

Although no patches have been addressed for these two vulnerabilities Microsoft has provided mitigations until patches are released.

Microsoft’s recommended mitigations can be accessed here.

Trends & Reports

Ransomware Gang Ramp Up Industrial Attacks in the U.S.

Summary

- Dragos has released its Q3 2022 Industrial Ransomware Analysis which has provided valuable insights regarding the ransomware threat landscape, its geographical distribution, and the main sectors targeted.

Analysis & Action

According to Dragos, thirty six percent of the 128 ransomware attacks targeted industrial organizations and infrastructures in North America, for a total of 46 incidents. Also, it was observed that after North America, Europe and Asia are the most targeted regions with 33% and 22% respectively.

It was also possible to determine that ransomware targeted the manufacturing sector the most as 88 organizations experienced incidents, followed by the food and beverage industry with 12 incidents, oil and gas with eight, energy with seven, and pharmaceuticals with six registered ransomware attacks. The most active ransomware by groups observed were LockBit 3.0 with 35% of total ransomware and accounting for 45 attacks in Q3 2022, followed by BlackBasta with 11%, and Hive with 7%.

Dragos has assessed with high confidence that ransomware will continue to disrupt industrial operations and that, due to LockBit's ransomware builder leak, more ransomware groups will be formed.

Dragos' full Industrial Ransomware Analysis: Q3 2022 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): Sophos, Bleeping Computer, The Hacker News, The Hacker News, Cisco Talos, Microsoft, Dark Reading, Dragos

Tags: RomCom RAT, See ticketing, Daily Cyber Headlines, darkweb markets, Industrial, Kimsuky, Dragos, DCH, Microsoft Exchange servers, Ukraine, Ransomware

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