Health-ISAC Daily Cyber Headlines

Daily Cyber Headlines **TLP:WHITE** **Alert Id: 7e810b44** **2022-10-05 12:35:24**

Today's Headlines:

Leading Story

- Hackers Stole Data from US Defense Organization Using New Malware

Data Breaches & Data Leaks

- Hackers Strike Again in Midland Health Services

Cyber Crimes & Incidents

- YouTube Channel Caught Distributing Malicious Tor Browser Installer
- Netwalker Ransomware Affiliate Sentenced to 20 Years in Prison

Vulnerabilities & Exploits

- Microsoft Updates Mitigation for Exchange Server Zero Days

Trends & Reports

- Nothing to Report

Privacy, Legal & Regulatory

- CISA Orders Federal Agencies to Regularly Track Network Assets and Vulnerabilities

Upcoming Health-ISAC Events

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

Leading Story

Hackers Stole Data from US Defense Organization Using New Malware

Summary

- An alert has been released by the U.S. government regarding state-sponsored threat actors that have the intent of stealing data from a U.S. organization in the Defense Industrial Base sector.

Analysis & Action

According to the U.S. government, the threat actor compromised an organization in the Defense Industrial Base sector, with the intention of stealing sensitive data by employing custom CovalentStealer malware and the Impacket Framework.

The targeted organization is involved in the research, design, development, production, delivery, and maintenance of military weapons systems, and the forensic investigation determined that the compromise lasted approximately 10 months.

It was assessed that the compromise was possible as the threat actor leveraged the Microsoft Exchange Server to compromise the organization, however, the initial access vector remains unknown. A report was developed which highlights the YARA rules that were created to detect the activity of the observed threat actor.

CISA's full report on impacket and exfiltration tool used to steal sensitive information from defense industrial base organization can be accessed here.

Data Breaches & Data Leaks

Hackers Strike Again in Midland Health Services

Summary

- Malicious actors were observed to target the Pinnacle Midlands Health Network which has the potential of resulting in a data leak.

Analysis & Action

It was reported by the Pinnacle Midlands Health Network that due to a cyberattack some of its IT systems were impacted which affected the services provided in various regional offices.

According to the healthcare organization, after the incident was discovered, it was immediately contained, and remediation measures have been established. The attackers were observed to have compromised servers that may have sensitive information about commercial as well as personal details.

It was stated that it is too early to fully determine the impact of the incident and to assess the number of individuals that could have been affected by the breach. The affected practices remain operational; however, the organization has informed the public that delays when contacting some practices can be experienced.

Cyber Crimes & Incidents

YouTube Channel Caught Distributing Malicious Tor Browser Installer

Summary

- A popular Chinese-language YouTube channel has emerged as a means to distribute a trojanized version of a Windows installer for the Tor Browser.

Analysis & Action

The malicious version of the Tor Browser installer is being distributed via a link present in the description of a video that was uploaded to YouTube on January 9, 2022. It has been viewed over 64,500 times to date. The channel has a significant amount of subscribers and claims to be based in Hong Kong.

The attack banks on the fact that the actual Tor Browser website is blocked in China, thus tricking unsuspecting users searching for the Tor Browser on YouTube into potentially downloading the rogue variant. Clicking on the link redirects the user to a 74MB executable that, once installed, is

designed to store users' browsing history and data entered into website forms.

Netwalker Ransomware Affiliate Sentenced to 20 Years in Prison

Summary

- An affiliate of the Netwalker ransomware group has been sentenced to 20 years in prison due to its involvement in malicious cyber activity.

Analysis & Action

Sebastien Vachon-Desjardins was sentenced to 20 years of prison and demanded to forfeit $21.5 million for his involvement in malicious cyber activity against a Tampa company as well as other entities.

The member of the Netwalker ransomware group has also been required to serve three years of supervised release after going out of prison. It was assessed by the U.S. authorities that Sebastien Vachon-Desjardins conducted cyberattacks against various companies worldwide, including U.S. companies and 17 Canadian entities.

The main objective of the malicious activity was to steal corporate data and encrypt devices to then extort his victims. The individual was previously arrested in Quebec in January 2021; however, he was extradited to the U.S. in March 2022.

Vulnerabilities & Exploits

Microsoft Updates Mitigation for Exchange Server Zero Days

Summary

- Microsoft has released an update to the mitigation recommendations regarding the two zero-day vulnerabilities found on Microsoft Exchange Server.

Analysis & Action

During this week a security researcher was able to demonstrate that Microsoft’s mitigation recommendations to deal with the two zero-day vulnerabilities found in Microsoft Exchange Server could have been bypassed easily.

Microsoft has released an update to the mitigations previously recommended to deal with the zero-day vulnerabilities tracked as CVE-2022-41040 and CVE-2022-41082. According to Microsoft the blocking rule has been updated and enabled automatically for organizations that have enabled Microsoft’s Exchange Emergency Mitigation Service, and the script to enable the URL Rewrite mitigation measure has been updated.

It is recommended to ensure that the latest mitigation recommendations from Microsoft are applied to avoid becoming a victim of cybercrime.

Microsoft’s update on the Microsoft Exchange Server zero-day vulnerabilities can be accessed here.

Trends & Reports

Nothing to Report

Privacy, Legal & Regulatory

CISA Orders Federal Agencies to Regularly Track Network Assets and Vulnerabilities

Summary

- CISA has issued a new Binding Operational Directive that orders federal agencies to keep track of network assets and vulnerabilities on their networks.

Analysis & Action

CISA has released the new Binding Operational Directive that mandates federal agencies to keep track, for six months, of the network assets and vulnerabilities found on their network.

The main objective of the directive is to enhance asset discovery and vulnerability enumeration as that will allow security teams to have greater visibility of the risks that federal civilian networks face. This will allow agencies to have an up-to-date inventory of the network assets and vulnerabilities which will enhance the proper tracking of these to be shared with CISA periodically.

The directive has been established as a response to the continued threat of malicious actors that have the intent to target the U.S. critical infrastructure and has also encouraged private organizations to implement rigorous asset and vulnerability management programs.

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): CISA, Bleeping Computer, Healthcare IT News, The Hacker News, Bleeping Computer, Dark Reading, Microsoft, The Hacker News

Tags: Midland Health Services, CovalentStealer, Impacket, Daily Cyber Headlines, Microsoft Exchange Server, Netwalker, DCH, data breaches, YouTube, Microsoft Exchange

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