Health-ISAC Daily Cyber Headlines

Daily Cyber Headlines **TLP:WHITE** **Alert Id: ca125818** **2022-10-03 12:42:25**

Today's Headlines:

Leading Story

- BlackCat Malware Lashes Out at US Defense IT Contractor

Data Breaches & Data Leaks

- Ransomware Gangs Leaks Data Stolen from LAUSD School System

Cyber Crimes & Incidents

- Lazarus Hackers Abuse Dell Driver Bug Using New FudModule Rootkit

Vulnerabilities & Exploits

- Hackers Exploit Critical Bitbucket Server Flaw in Attacks
- Canon Medical Product Vulnerabilities Expose Patient Information

Trends & Reports

- Nothing to Report

Privacy, Legal & Regulatory

- CISA Issues Guidance on Transitioning to TLP 2.0

Upcoming Health-ISAC Events

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

Leading Story

BlackCat Malware Lashes Out at US Defense IT Contractor

Summary

- The BlackCat ransomware group has allegedly compromised NJVC, an IT firm that provides services to multiple U.S. governmental agencies.

Analysis & Action

It was observed by security researchers that the BlackCat ransomware group added to its data leak site, information that belongs to NJVC.

NJVC is an IT firm that provides services to civilian U.S. government agencies and the Department of Defense, however, after the threat actor threatened to leak the compromised data, its website went offline shortly after providing proof of the security breach. Although the website was offline for some time the ransomware group came back online and the post regarding NJVC was deleted.

BlackCat is one of the most active ransomware groups and since its emergence in 2021 more than 60 organizations have been attacked, therefore, security researchers have hypothesized that leaking data from the U.S. Department of Defense was not the best move for its long-term strategy, or the claims regarding NJVC's incident were false.

Data Breaches & Data Leaks

Ransomware Gangs Leaks Data Stolen from LAUSD School System

Summary

- The Vice Society Ransomware gang has recently published data that belongs to Los Angeles Unified School District.

Analysis & Action

Los Angeles Unified School District was recently targeted by a ransomware attack that compromised confidential information.

Although the threat actor was pressing its victim to pay its ransom demands, the LAUSD decided not to pay the ransom. Therefore, as a consequence of LAUSD's decision, the ransomware group decided to leak the compromised information. LAUSD has stated that it is closely working with law enforcement agencies to assess the nature of the leaked data and determine what type of compensatory measures could be offered to affected individuals in case that personally identifiable information was leaked.

LAUSD previously notified the school community and its partners that it will offer free credit monitoring services to prevent cybercriminal activity against the affected individuals.

Cyber Crimes & Incidents

Lazarus Hackers Abuse Dell Driver Bug Using New FudModule Rootkit

Summary

- The notorious North Korean hacking group known as Lazarus was observed installing a Windows rootkit that has the capability of abusing Dell hardware.

Analysis & Action

Security researchers identified a new spear phishing campaign conducted by Lazarus, which its main goal was cyberespionage and data theft.

According to the research, it was possible to determine that the malicious campaign unfolded in the autumn of 2021 and was observed to abuse the Dell hardware driver in a Bring Your Own Vulnerable Driver attack. Additional tools that were deployed present in the campaign were the previously described FudModule Rootkit, an HTTPS uploader used for securing data exfiltration, and multiple trojanized open-source applications such as wolfSSL and Finger Text.

By using these tools, the threat actor also disabled mechanisms in the Windows operating system offers to monitor its actions, such as registry, file system, process creation, and event tracing.

Vulnerabilities & Exploits

Hackers Exploit Critical Bitbucket Server Flaw in Attacks

Summary

- The U.S. Cybersecurity and Infrastructure Agency (CISA) added three new vulnerabilities to its catalog of Known Exploited Vulnerabilities including flaws in Bitbucket Server RCE and Microsoft Exchange zero-days.

Analysis & Action

CISA has included the vulnerabilities affecting Bitbucket Server RCE and Microsoft Exchange zero-days to its catalog of Known Exploited Vulnerabilities.

The vulnerabilities affecting Microsoft Exchange servers are tracked as CVE-2022-41040 and CVE-2022-41082 which can only be exploited in limited and targeted attacks. On the other hand, the vulnerability affecting Bitbucket Server is a remote code execution vulnerability that is tracked as CVE-2022-36804 which could allow threat actors to inject commands as there is available proof of concept exploit code.

CISA has ordered all Federal Civilian Executive Branch Agencies to apply the appropriate patches by October 21st. It is recommended to ensure that these vulnerabilities are prioritized for patching to avoid becoming a victim of cybercrime.

Canon Medical Product Vulnerabilities Expose Patient Information

Summary

- Two vulnerabilities affecting Canon Medical imaging sharing tool Vitrea View were found which could expose patient information.

Analysis & Action

Two new cross-site scripting (XSS) vulnerabilities were identified affecting Canon Medical imaging sharing tool Vitrea View.

Vitrea View is widely used by healthcare providers, physicians, and radiologists as it allows healthcare professionals to share medical images to be viewed on desktop as well as mobile devices. However, new vulnerabilities affect this product which are tracked collectively as CVE-2022-37461 and could allow a threat actor to retrieve patient information and modify the information, affecting in this way the confidentiality and integrity of patient data.

The cybersecurity firm that identified the flaws has published a proof of concept on targeting the vulnerability, however, Cannon issued a patch with the release of Vitrea View version 7.7.6.

Trends & Reports

Nothing to Report

Privacy, Legal & Regulatory

CISA Issues Guidance on Transitioning to TLP 2.0

Summary

- CISA has released guidance for private and public organizations to facilitate the transition to the Traffic Light Protocol (TLP) 2.0.

Analysis & Action

TLP is an effective method to inform recipients of sensitive information on the extent to which they can share the provided data.

The TLP 1.0 version employs four labels namely TLP:RED, TLP:AMBER, TLP:GREEN, and TLP:WHITE. However, the TLP 2.0 version is replacing TLP:WHITE for TLP:CLEAR and includes a new label TLP:AMBER+STRICT to supplement TLP:AMBER. CISA is urging private and public organizations to ensure that the transition to TLP 2.0 version is implemented effectively.

Additionally, it was stated that the new version of TLP will facilitate greater information sharing and collaboration between organizations which will contribute to the strengthening of cybersecurity and cyber resilience.

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 Register, Bleeping Computer, Bleeping Computer, Bleeping Computer, Security Week, Security Week

Tags: LAUSD, BlackCat, Daily Cyber Headlines, Bitbucket, DCH, Lazarus, Canon, data breaches, Microsoft Exchange, 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