Health-ISAC Daily Cyber Headlines

Daily Cyber Headlines **TLP:WHITE** **Alert Id: 9c0f6741** **2022-10-24 12:31:14**

Today's Headlines:

Leading Story

- US Government Warns of Daixin Team Targeting Health Organizations with Ransomware

Data Breaches & Data Leaks

- Hacktivists Steal 100,000 Emails from Iran Nuclear Agency

Cyber Crimes & Incidents

- Wholesale Giant Metro Hit by IT Outage After Cyberattack

Vulnerabilities & Exploits

- Hackers Started Exploiting Critical Text4Shell Apache Commons Text Vulnerability
- Cisco Users Informed of Vulnerabilities in Identity Services Engine

Trends & Reports

- Thousands of GitHub Repositories Deliver Fake PoC Exploits with Malware

Privacy, Legal & Regulatory

- Nothing to Report

Upcoming Health-ISAC Events

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

Leading Story

US Government Warns of Daixin Team Targeting Health Organizations with Ransomware

Summary

- Various U.S. Governmental agencies have warned that the threat actor known as Daixin Team is actively targeting healthcare organizations with ransomware attacks.

Analysis & Action

The U.S. Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigations (FBI), and the Department of Health and Human Services (HHS) have released a warning about Daixin Team, a threat actor that is actively targeting healthcare organizations with ransomware attacks.

The agencies' warning included various tactics, techniques, and procedures (TTPs) as well as indicators of compromise (IOCs) related to the malicious activities of the Daixin Team. Security researchers have observed that the threat actor has been targeting the healthcare sector since June 2022, by encrypting systems used for multiple healthcare services. It was observed that the threat actor also exfiltrates patient health information as part of its extortion techniques.

To remain protected against Daixin Tema's malicious activity it is advised to install updates for operating systems, software, and firmware as soon as they are released. Also, it is recommended to enable phishing-resistant multi-factor authentication, as well as to establish cybersecurity awareness training for employees to remain safe.

H-ISAC's Threat Bulletin regarding Daixin Team can be accessed here.

Data Breaches & Data Leaks

Hacktivists Steal 100,000 Emails from Iran Nuclear Agency

Summary

- Hacktivists have claimed that they have stolen 100,000 emails from Iran's nuclear energy agency, but Iran has rejected the threat actor's claims.

Analysis & Action

Black Reward, an Iranian hacktivist group, has claimed that it was able to access an email server run by a company related to Iran's Atomic Energy Organization.

The threat actor claimed that it was able to exfiltrate 324 inboxes comprising over 100,000 messages and a total of 50GB worth of files. According to Black Reward's post on telegram, they were able to access sensitive information such as construction plans for a nuclear power plant, as well as personally identifiable information of Iran's nuclear energy agency employees.

As a response to the threat actor's claims, the Iranian government has dismissed the data exfiltration claims and it was stated that the threat group is a front for Iran's foreign enemies.

Cyber Crimes & Incidents

Wholesale Giant Metro Hit by IT Outage After Cyberattack

Summary

- Metro is currently experiencing infrastructure outages and store payment issues as the company became the victim of a recent cyberattack.

Analysis & Action

Metro, the international wholesale giant, operates in over 30 countries and employs approximately 95,000 people worldwide. However, it was recently observed that it has experienced infrastructure outages and store payment issues due to a recent cyberattack.

It was stated by the organization that a team of security experts has been hired to help solve the issue and investigate the cause of the interruption of the services. The impact of cyberattack has affected Metro's online payment systems and has caused operational disruption as delays in orders have been experienced.

Although the company has not offered detailed information about the security incident yet, IT infrastructure outages, most of the time, are linked to ransomware attacks. As the organization is currently investigating the incident it is expected that more information will be released as findings emerge.

Vulnerabilities & Exploits

Hackers Started Exploiting Critical Text4Shell Apache Commons Text Vulnerability

Summary

- Wordfence has recently stated that exploitation attempts were detected as a new vulnerability was disclosed in Apache Commons Text.

Analysis & Action

Wordfence is WordPress's security company, which has recently stated that exploitation attempts against a flaw in Apache Commons Text were observed.

The vulnerability in Apache Commons Text is tracked as CVE-2022-42889 and is also known as Text4Shell. The vulnerability was assigned a CVSS score of 9.8 out of 10 affecting versions 1.5 through 1.9 of the libraries. According to the security researchers that identified the vulnerability, an attacker could achieve remote code execution by sending a crafted payload remotely by using a script, DNS, and URL lookups, which could open the door for follow-on attacks.

It is advised to upgrade Apache Commons Text to the fixed version to mitigate the risk associated with the exploitation of the vulnerability.

Cisco Users Informed of Vulnerabilities in Identity Services Engine

Summary

- A security researcher was able to identify two new vulnerabilities affecting Cisco's Identity Services Engine product.

Analysis & Action

According to the security researcher that identified the flaw in Cisco's Identity Services Engine product, the web-based management interface is affected by unauthorized file access.

This vulnerability is tracked as CVE-2022-20822 and it could allow a remote authenticated attacker to read and delete files on impacted devices putting at risk the confidentiality, integrity, and availability of valuable information. For the moment, no exploitation in the wild has been observed and Cisco stated that it is working on software updates to patch the vulnerability.

Once the vulnerability has been fixed Cisco would release a proof-of-concept exploit code which will only be available after software fixes are released in November 2022 and January 2023.

Trends & Reports

Thousands of GitHub Repositories Deliver Fake PoC Exploits with Malware

Summary

- Thousands of repositories on GitHub that offer fake proof of concept (PoC) exploits for various vulnerabilities have been observed to contain malware.

Analysis & Action
It was discovered by security researchers at Leiden Institute to Advanced Computer Science that thousands of repositories on GitHub that offer fake PoC for vulnerabilities include malware.

According to the research, the possibility of getting infected with malware instead of obtaining a PoC could be as high as 10.3%. To reach this conclusion the researchers analyzed 47,300 repositories advertising an exploit for a vulnerability disclosed between 2017 and 2021, and it was observed that of the 150,734 Ips extracted, 2864 matched blocklist entries, 1522 were detected as malicious by VirusTotal, and 1069 were present in the AbuseIPDB database. Therefore, in total, 4893 repositories out of the 47,300 repositories tested were malicious.

When using a repository on GitHub it is recommended to read carefully the code that will be run. If the code is too obfuscated, it is advised to use a sandbox or virtual machine to check for anomalies in network traffic.

Leiden Institute to Advanced Computer Science's full paper can be accessed here.

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-ISAC, Bleeping Computer, The Register, Bleeping Computer, The Hacker News, Security Week, Bleeping Computer, ArXiv

Tags: Text4Shell, Iran Nuclear Agency, Black Reward, Daixin, Daily Cyber Headlines, Metro, DCH, Cisco Identity Services Engine (ISE), Github, 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