Health-ISAC Daily Cyber Headlines

Daily Cyber Headlines **TLP:WHITE** **Alert Id: cc9fb574** **2022-10-19 13:38:13**

Health-ISAC Daily Cyber Headlines

Today's Headlines:

Leading Story

- Researchers Keep a Wary Eye on Critical New Vulnerability in Apache Commons Text

Data Breaches & Data Leaks

- Hackers Target Asian Casinos in Lengthy Cyberespionage Campaign

Cyber Crimes & Incidents

- Law Enforcement Arrested 31 Suspects for Stealing Cars by Hacking Key Fobs

Vulnerabilities & Exploits

- Pro-Russia Hackers DDoS Bulgarian Government

Trends & Reports

- New Threat Perspective Outlines Risks to Australian Electric Organisations

Privacy, Legal & Regulatory

- NCSC Issues Fresh Guidance Following Recent Rise in Supply Chain Cyber Attacks

Upcoming Health-ISAC Events

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

Leading Story

Researchers Keep a Wary Eye on Critical New Vulnerability in Apache Commons Text

Summary

- Security researchers are monitoring interest in a remote code execution (RCE) vulnerability in Apache Commons Text.

Analysis & Action

Security researchers are watching with great anticipation as the proof-of-concept code in a critical RCE vulnerability in Apache Commons Text goes public. The vulnerability has a common vulnerability scoring system (CVSS) score of 9.8/10 and is being tracked as CVE-2022-42889.

This vulnerability was discovered by a benign GitHub penetration tester. However, the proof-of-concept (PoC) code is publicly available.

Apache has released a patch for this in their Apache Commons Text 1.10.0 software update. Health-ISAC recommends updating Apache Commons Text to the latest version as soon as possible.

Data Breaches & Data Leaks

Hackers Target Asian Casinos in Lengthy Cyberespionage Campaign

Summary

- A novel threat actor dubbed DiceyF has been observed utilizing sophisticated malware frameworks against casinos in the southeast Asia region.

Analysis & Action

This threat actor has been deemed an advanced persistent threat (APT) and has been observed utilizing its malware suite to commit intellectual property theft. This group does not appear to be interested in financially motivated cyber activity.

This campaign has a very heavy emphasis on Southeast Asian countries. At the time of writing, they have only been observed targeting online casinos.

According to Kaspersky, their cyber activity is aligned with the Chinese cyber campaign Operation Earth Berberoka, leading to a tentative Chinese attribution. In conclusion, Chinese cyber threat actors are still engaged in intellectual property theft.

Cyber Crimes & Incidents

Law Enforcement Arrested 31 Suspects for Stealing Cars by Hacking Key Fobs

Summary

- An international law enforcement operation led by French and Europol authorities have led to the arrest of 31 suspects in an alleged automotive wireless key fob hacking ring.

Analysis & Action

A joint endeavor by the French, Spanish, and Latvian cybersecurity authorities supported by Europol and Eurojust have led to the arrest of 31 suspects allegedly involved in the hacking of wireless car key fobs to facilitate car theft.

The criminals were arrested from three different nations and consisted of software developers, resellers, and car thieves.

This is a testament to the evolving cyber threat landscape. Not very long ago, a feat such as this would have been only possible in the world of science fiction. It also stresses the importance of cybersecurity in all aspects of technology.

Vulnerabilities & Exploits

Pro-Russia Hackers DDoS Bulgarian Government

Summary

- Russia is the likely perpetrator of a wave of distributed denial of service (DDoS) targeting the Bulgarian National Revenue Agency and other government websites.

Analysis & Action

The Bulgarian government has been the victim of a spree of DDoS attacks targeting their National Revenue Agency, the website of the president, and ministries of defense.

Russian-sympathetic hacktivist group Killnet has claimed responsibility for the attacks. This is likely due to Bulgaria's status as a NATO and EU nation that is actively providing technical aid to the Ukrainian military.

As the military campaign in Ukraine draws on longer and longer, Russian cyber-attacks are maintaining their ferocity. Should Russian cyber activity deviate from solely attacking supporters of the Ukrainian military and target the West as a whole, members may be drawn into the crosshairs. Health-ISAC recommends utilizing DDoS protection on member websites.

Trends & Reports

New Threat Perspective Outlines Risks to Australian Electric Organisations

Summary

- Dragos has observed an increase in the targeting of Australian electrical industries.

Analysis & Action

According to Dragos, Australia has seen a disproportionate amount of industrial control systems (ICS) attacks relative to its geopolitical standing. The majority of these attacks seem to be targeting the Australian energy sector.

This has led to mass scanning and assessing of Australian industrial cybersecurity capabilities by largely cybercriminal groups. With all the chatter surrounding the Australian ICS systems, nation state actors seeking to conduct their own ICS attacks have easy access to a repertoire of information.

In the current threat landscape, there is no attack surface too obscure to exploit. With the increased interest in ICS/SCADA systems, IoMT device intrusion vectors may become more popular in the future.

Privacy, Legal & Regulatory

NCSC Issues Fresh Guidance Following Recent Rise in Supply Chain Cyber Attacks

Summary

- The United Kingdom National Cyber Security Centre (NCSC) has released guidelines to mitigate supply chain risk in cybersecurity.

Analysis & Action

At the time of writing, there has been a significant in supply chain cyber-attacks in recent years, leading to renewed interest in mitigation by cybersecurity authorities.

The new guidelines are made for medium to large sized organizations according to the NCSC. The NCSC released these in the form of five new guidelines. They are as follows.

Understand why your organization should invest in the supply chain, develop a cybersecurity approach that prioritizes your organization's assets, apply the approach to new suppliers, integrate the approach into the existing supplier relationships, and then attempt to evolve the framework respectively. To see the full guidelines, click here.

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): Dark Reading, Bleeping Computer, Security Affairs, Infosecurity Magazine, Dragos, NCSC

Tags: ICS/SCADA, Apache Commons Text, Daily Cyber Headlines, Dragos, DCH, Supply Chain Attack

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