Health-ISAC Daily Cyber Headlines

Daily Cyber Headlines | TLP:WHITE | Alert ID : 32c1d9e0 | Oct 07, 2022, 08:41 AM

Today's Headlines:

Leading Story

- Lloyd's of London Investigating Cybersecurity Incident

Data Breaches & Data Leaks

- Nothing to Report

Cyber Crimes & Incidents

- Eternity Group Hackers Offering New LilithBot Malware as a Service to Cybercriminals.
- FBI Warns of Disinformation Threats Before 2022 Midterm Elections

Vulnerabilities & Exploits

- Top CVEs Actively Exploited by People's Republic of China State-Sponsored Cyber Actors
- Cisco Patches High-Severity Vulnerabilities in Communications and Networking Products

Trends & Reports

- Research Reveals Microsoft Teams Security and Backup Flaws

Privacy, Legal & Regulatory

- Nothing to Report

Upcoming Health-ISAC Events

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

In observance of the federal holiday, the daily cyber headlines will not be distributed on Monday, October 10th.

Additional Info

Leading Story

Lloyd's of London Investigating Cybersecurity Incident

Summary

- Lloyd's of London is currently investigating a cybersecurity incident that has forced the insurance company to disconnect some of its systems.

Analysis & Action

Lloyd's of London, one of the largest insurance companies in the world, has recently announced that due to a security incident it had to reset its network and system as a precaution after an unusual activity was registered.

Although no major details have been disclosed regarding the type of incident as well as the potential impact it could have on Lloyd's information, it was stated that the best options for reconnecting the systems are being evaluated. As the company has communicated to the public, all the necessary security measures have been implemented in response to the incident.

Lloyd's of London would not be the first insurance company targeted during 2022, and the incident occurs weeks after the insurance company decide to include exclusion clauses for state-backed cyberattacks in future insurance policies.

Data Breaches & Data Leaks

Nothing to Report

Cyber Crimes & Incidents

Eternity Group Hackers Offering New LilithBot Malware as a Service to Cybercriminals

Summary

- The threat actor behind the malware-as-a-service (MaaS) called Eternity has been linked to new piece of malware called LilithBot.

Analysis & Action

LilithBot is an advanced piece of malware that is capable of being used as a, miner stealer, and a clipper along with its persistence mechanisms. Eternity runs

a MaaS toolkit called Eternity Project. Other threat actors are able to subscribe to the Eternity project at little to no cost.

The group markets its product in both English and Russian and appears to have links to the Russian Jester Group, which has been active since July 2021.

The development is a sign that the Eternity Project is actively expanding its malware arsenal and adopting sophisticated techniques to bypass detections.

FBI Warns of Disinformation Threats Before 2022 Midterm Elections

Summary

- The U.S. Federal Bureau of Investigations (FBI) has warned the public about foreign disinformation campaigns that may attempt to affect the U.S. incoming midterm elections.

Analysis & Action

The FBI has recently released a warning as it has assessed with confidence that foreign actors have the intent to affect the elections' results by developing disinformation campaigns.

The federal law agency has established that it is likely that the disinformation campaigns will try to impact public opinion, discredit the electoral process, and encourage a lack of trust sentiments against democratic institutions. It was also assessed that threat actors may leverage various tools and platforms to spread disinformation such as spoofed websites, fake social media personas, as well as the dark web, and publicly available media channels.

It is recommended to carefully evaluate the sources of information before and after the 2022 midterm elections to avoid becoming a victim of disinformation campaigns.

Vulnerabilities & Exploits

Top CVEs Actively Exploited by People's Republic of China State-Sponsored Cyber Actors

Summary

- CISA has recently shared a new alert regarding the top vulnerabilities that have been exploited by Chinese-sponsored threat actors.

Analysis & Action

CISA has published an alert that highlights the vulnerabilities that the People's Republic of China state-sponsored threat actors have exploited the most.

The alert has been jointly developed by CISA, the National Security Agency (NSA), and the FBI. The alert contains 20 vulnerabilities that have been exploited since 2019

and includes vulnerabilities such as the Apache Log4j tracked as CVE-2021-4428, Atlassian vulnerability tracked as CVE-2022-26134, F5 Big-IP vulnerability tracked as CVE-2020-5902, and Microsoft Exchange vulnerability tracked as CVE-2021-26855, among others.

The vulnerability types are mainly remote code execution, arbitrary file read, command line execution, command injection, and path traversal. CISA has also provided mitigation recommendations that are encouraged to be applied to remain safe and avoid becoming a victim of cybercrime.

Additional information on China's Cyber Threat Overview and Advisories can be accessed here.

Cisco Patches High-Severity Vulnerabilities in Communications and Networking Products

Summary

- Cisco announced that it has patched two vulnerabilities that affect some of its networking and communication products.

Analysis & Action

Cisco released the patches for two vulnerabilities that were discovered affecting networking and communication products such as Enterprise NFV, Expressway, and TelePresence.

The two vulnerabilities are tracked as CVE-2022-20814 and CVE-2022-20853, which in conjunction could allow an attacker to access sensitive data through man-in-the-middle attacks and allow cross-site request forgery attacks. The attacker could also deploy Distributed Denial of Service (DDoS) attacks as well as intercept and alter network traffic.

No active exploitation of the vulnerabilities has been observed in the wild, however, it is recommended to ensure that the affected products have been properly updated.

Additional security advisories addressing other medium severity vulnerabilities have been released which can be accessed here.

Trends & Reports

Research Reveals Microsoft Teams Security and Backup Flaws

Summary

- New research has demonstrated that a greater backup for Microsoft teams is necessary as a considerable percentage of information is not being properly secured.

Analysis & Action

It was assessed on the research developed by Hornet security that nearly 45% of Microsoft Teams users are sending confidential and critical information via the platform, which demonstrates the necessity for stricter security and recurrent backups.

The survey has evaluated that Teams user chat or direct messaging is the preferred form of communication where 51% of users have admitted to sending restricted and confidential data over the platform. Also, the survey shows that 48% of users have sent messages via Teams that they should not.

The research has highlighted the fact that, beyond cybersecurity vulnerabilities, Teams does not offer the appropriate protection of data, as well as safe options for backed-up information in a secure and responsible way.

Hornet security's full survey 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 | References

The Hacker News
Security Week
Bleeping Computer

CISA
CISA
Security Week
Dark Reading
hornetsecurity

Tags

LilithBot, Lloyds of London, Daily Cyber Headlines, CISA Alert, DCH, Microsoft Teams, Disinformation Campaigns, cisco

---

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