DAILY CYBER HEADLINES

Daily Cyber Headlines

TLP:GREEN

Nov 08, 2024

Today's Headlines:

Leading Story

- CISA Alerts to Active Exploitation of Critical Palo Alto Networks Vulnerability

Data Breaches & Data Leaks

- Nothing to Report

Cyber Crimes & Incidents

- China-linked Hackers Tasked with Japanese Targets Pursue Them Through Europe
- Threat Actors Increasingly Use Winos4.0 Post-Exploitation Kit In Attacks

Vulnerabilities & Exploits

- CISA Adds Known Exploited Vulnerabilities to Catalog

Trends & Reports

- ENISA Hosts 9th eHealth Security Conference To Tackle Cybersecurity Challenges In Healthcare
- The Five Most Common Malware Techniques in 2024

Privacy, Legal & Regulatory

- Exploring DORA: How To Manage ICT Incidents and Minimize Cyber Threat Risks

Upcoming Health-ISAC Events

- Global Monthly Threat Brief
  - Americas – November 26, 2024, 12:00-01:00 PM ET
  - European – November 27, 2024, 03:00-04:00 PM CET
- T-SIG Webinar for SMB Members – November 14, 2024 at 11:30 AM ET
- Fall Americas Summit, Phoenix, Arizona - December 2-6, 2024

Leading Story

CISA Alerts to Active Exploitation of Critical Palo Alto Networks Vulnerability

Summary

- Palo Alto Networks' Expedition tool flaw CVE-2024-5910 is being exploited.

Analysis & Action

CISA has warned about actively exploiting a critical vulnerability, CVE-2024-5910, in Palo Alto Networks' Expedition tool.

CVE-2024-5910 is a missing authentication flaw that could allow threat actors with network access to control an Expedition admin account, posing significant security risks.

Health-ISAC advises immediate patching of this flaw in cases where this has not already been done, as well as continuous monitoring of systems for suspicious activity to prevent a possible intrusion.

Data Breaches & Data Leaks

- Nothing to Report.

Cyber Crimes & Incidents

China-linked Hackers Tasked with Japanese Targets Pursue Them Through Europe

Summary

- European diplomatic organization targeted for the first time by threat actors believed to be in alignment with China.

Analysis & Action
The threat actor has been identified as MirrorFace, a group believed to be aligned with China. In new reports, the group has been analyzed to target an organization within the European Union, the first time for the group.

ESET researchers detailed the analysis quarterly, showing the threat actors' steps to expand their targets. The threat actor originally targeted just entities within Japan but now seems to be expanding outwards. Lure documentation used by the threat actor still uses a Japanese theme; however, it prompts targets to download their document. The document is titled The EXPO Exhibition in Japan in 2025. These attacks are set up to gain access to organizations, such as media or politics, along with universities, institutions, and manufacturers.

Though the threat actor has expanded the number of those who it attacks, researchers still report the threat actor attacking Japanese

organizations as well, mainly political parties and institutions of research. China-linked threat actors and groups continue to expand, creating an issue for Japanese entities, and now other entities and expansion begin to take place with these groups and their targets.

Spearphishing is a common utilization used by threat actors to gain access to one's system and sensitive information. Health-ISAC recommends that its members exercise caution on email and messaging platforms and utilize trusted anti-phishing add-ons to mitigate the risks of similar incidents.

Threat Actors Increasingly Use Winos4.0 Post-Exploitation Kit In Attacks

Summary

- Windows users are being maliciously targeted with Winos4.0 framework by threat actors.

Analysis & Action

A malicious framework, Winos4.0, is distributed from what seemed to be benevolent applications related to games. A further analysis identified the framework as equivalent to post-exploitation frameworks such as Sliver and Cobalt Strike.

Threat actors named Void Arachne, also known as Silver Fox, would lure their victims in, offering software like VPNs that were modified to have malicious components. An evolution of these activities has now led to threat actors focusing on games and their files to continue their attacks, targeting Chinese users. These begin on installation; while masked as legitimate, a DLL file will execute from ad59t82g[.]com to begin a multi-step infection process. Next, a shellcode that has been injected will follow a number of steps, including the loading of APIs, retrieval of config data, and, finally, the establishment of a connection with the C2 server. The third phase of the attack will have another DLL retrieve the data from the C2 server, storing it in “HKEY_CURRENT_USER\\Console\\o”, then updating the addresses of the C2. The final stage of the attack chain will load the DLL login module, performing a number of malicious actions that can result in the exfiltration of data and the stealing of documents on one's system. Threat actors have been using the Winos4.0 framework for a number of months at this time, as new campaigns also begin to take place.

Health-ISAC recommends its members implement access controls, network monitoring, and encryption to help act against threat actors and their means for committing data exfiltration practices on systems.

Vulnerabilities & Exploits

CISA Adds Four Known Exploited Vulnerabilities to Catalog

Summary

- Based on evidence of active exploitation, CISA has added new vulnerabilities to its KEV catalog.

Analysis & Action
CISA has added new vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog. These vulnerabilities are used as attack vectors for cyber actors to administer malicious attacks to their targets, posing risks for organizations.

The identified vulnerabilities are as follows: CVE-2024-43093, CVE-2024-51567, and CVE-2019-16278. The first vulnerability, CVE-2024-43093, involved privilege escalations within Android Frameworks. CVE-2024-51567 included an incorrect default permission within CyberPanel that caused a vulnerability to be established. CVE-2019-16278 alludes to a vulnerability within Nostromo nhttpd Directory traversal. CISA has since urged organizations to mitigate their exposure to these attacks and threat actors through means of remediation and keeping awareness of constant updates within their catalog.

CISA constantly adds new vulnerabilities to its catalogs upon meeting specific criteria. Health-ISAC recommends its members stay aware of these updates and install the latest patches on their systems to mitigate the risks of falling victim to one of these cyberattacks.

Trends & Reports

ENISE Hosts 9th eHealth Security Conference To Tackle Cybersecurity Challenges In Healthcare

Summary

- ENISA hosts a security conference focused on challenges faced within eHealth cybersecurity.

Analysis & Action
Over the last couple of years, an emphasis has been placed on cybersecurity issues within healthcare organizations as it is becoming a growing concern. ENISA looks to bring more awareness to the variety of issues that threat actors have posed to organizations, fortifying security against them in the process.

The European Union Agency for Cybersecurity's (ENISA) conference highlights the growing challenges posed by threat actors of ransomware, phishing, and other cybercrime attacks. A total of 487 of the incidents reported on ENISA's landscape report came about to be related to or in reference to the health sector. Assessments show that 45% of these reported incidents were ransomware attacks, while 28% of the incidents were data breaches. ENISA reports that ransomware has been one of, if not the biggest, disruption faced in the healthcare industry. A number of high-profile incidents were under reports for the period, as emphasis is being placed on the security of patients' information going forward.

Ransomware is a common and effective strategy used by threat actors to gain access to an organization's sensitive information. Health-ISAC recommends its members be wary of emails from unknown senders avoiding attached files or links.

The Five Most Common Malware Techniques in 2024

Summary

- Here's a glimpse into some common TTPs observed in ANY.RUN's Q3 2024 Malware Trends report, along with real-world examples.

Analysis & Action
Understanding how attackers operate is crucial for building strong defenses against cyber threats. This is where Tactics, Techniques, and Procedures (TTPs) come in. Unlike indicators of compromise (IOCs) that can change quickly, TTPs represent the underlying methods attackers use.

According to ANY.RUN’s Q3 2024 report on malware trends, the most commonly used techniques include disabling Windows Event Logging, PowerShell Exploitation, Abuse of Windows Command Shell, modification of registry keys, and time-based evasion.

Health-ISAC recommends viewing the ANY.RUN's Q3 2024 report on malware trends is available here.

Privacy, Legal & Regulatory

Exploring DORA: How To Manage ICT Incidents and Minimize Cyber Threat Risks

Summary

- DORA is set to improve the cyber resilience of the entities in scope.

Analysis & Action
In 2024, the financial sector faced an average cost of $6.08 million per data breach, highlighting the importance of robust IT security regulations. One of these regulations is the European Union’s Digital Operational Resilience Act (DORA), which will require compliance by January 2025.

DORA requires financial institutions and ICT service providers who work with financial entities to strengthen their defenses against cyber threats by ensuring their systems can withstand disruptions without risking operations or data. DORA introduces a harmonized reporting system for serious ICT incidents and significant cyber threats, requiring classifications based on specific criteria and prompt reporting to the financial supervisory authority.

It is crucial to train security teams on new regulations and reporting procedures, implement processes for capturing and analyzing incidents, and establish clear communication plans to ensure compliance and avoid fines.

Health-ISAC Cyber Threat Level

On October 17, 2024, the Health-ISAC Threat Intelligence Committee (TIC) evaluated the current Cyber Threat Level and collectively decided to raise the Cyber Threat Level to **Yellow (Elevated)**. The Threat Level of Yellow (Elevated) is due to threats from:

The Threat Level of Yellow (Elevated) is due to threats from elections-related smishing campaigns, DPRK remote worker activity, potential repercussions of recent activity in the Middle East, commodity malware, and a recent uptick in ransomware events.

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.

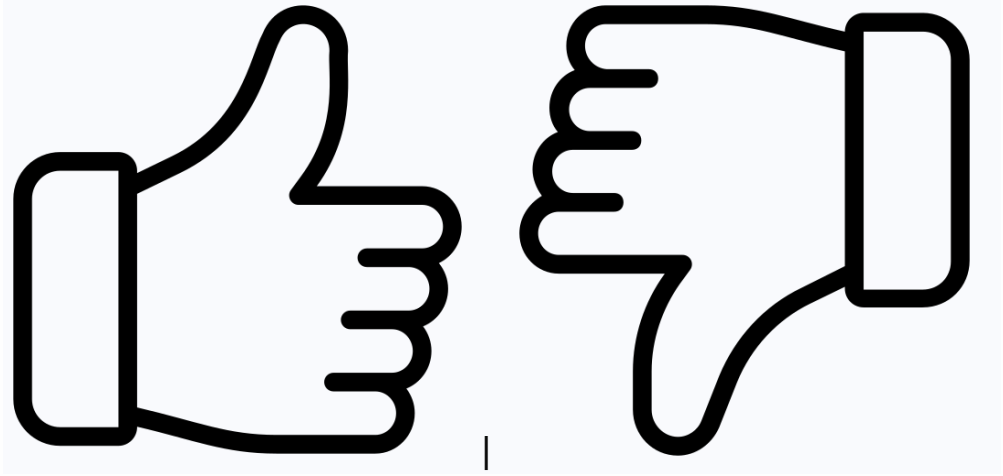
You must have Cyware Access to reach the Threat Advisory System document. Contact membership@h-isac.org for access to Cyware.

Reference(s)	The Record, The Hacker News, industrialcyber, The Hacker News, Bleeping Computer, Security Intelligence, cisa
Report Source(s)	Health-ISAC

Alert ID e4d5eeca

View Alert

Share Feedback
was this helpful?



Tags Malware Techniques, Winos4.0 Post-Exploitation Kit, Dora, ENISA, CISA, Palo Alto Networks

TLP:GREEN TLP:GREEN Limited disclosure, recipients can ONLY share this within their TRUST community. Recipients should consider the information proprietary and may ONLY share TLP:GREEN information with peers and partner organizations within their TRUST community, SHARING IS NOT PERMITTED via social media, public websites and/or other publicly accessible channels.

Share Threat Intel
For guidance on sharing indicators with Health-ISAC via HTIP, please visit the Knowledge Base article "HTIP - Share Threat Intel" here.

The "Share Threat Intel" feature allows for attributed or anonymous sharing across ISACs and other cybersecurity-related entities.

Turn off Categories
For guidance on disabling alert categories, please visit the Knowledge Base article "HTIP Alert Categories" here.

Access the Health-ISAC Threat 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 Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments

Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.  

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**