Daily Cyber Headlines

Daily Cyber Headlines | TLP:WHITE | Alert ID : 087baa3c | Oct 16, 2023, 06:56 AM

Today's Headlines:

Leading Story

- The ALPHV Ransomware Gang Stole 5TB of Data from the Morrison Community Hospital

Data Breaches & Data Leaks

- Regulators, Insurers, and Customers All Coming for Progress After MOVEit Breach

Cyber Crimes & Incidents

- FBI, CISA Warn of Rising AvosLocker Ransomware Attacks Against Critical Infrastructure

Vulnerabilities & Exploits

- Dozens of Squid Proxy Vulnerabilities Remain Unpatched 2 Years After Disclosure

Trends & Reports

- Ransomware Attacks Doubled Year by Year. Are Organizations Equipped to Handle the Evolution of Ransomware in 2023?

Privacy, Legal & Regulatory

- CISA Plans to Share More Information on Ransomware Actors in Its Exploited Vulnerability Alerts

Cybersecurity Awareness Month

- The Daily Cyber Headlines are being shared during the month of October at **TLP:WHITE** for Cybersecurity Awareness Month.

Upcoming Health-ISAC Events

- Americas Hobby Exercise - October 25, 2023. Registration is available here.
- Health-ISAC Monthly Threat Brief – October 31, 2023, 12:00 PM Eastern

Additional Information

Leading Story

[The ALPHV Ransomware Gang Stole 5TB of Data from the Morrison Community Hospital]

Summary

- The ALPHV/BlackCat ransomware group claims to have stolen 5TB of data containing personally identifiable information (PII) from the Morrison Community Hospital.

Analysis & Action

The ALPHV ransomware gang has contacted journalists and threatened to call patients using information stolen in the breach if the hospital does not pay the ransom.

This is the latest healthcare data breach in a series of ransomware attacks against hospitals and healthcare organizations. The attacks often impact patient care and raise questions about the security of sensitive medical data, including personal health information (PHI).

The increasing ransomware attacks against hospitals are a serious concern. Hospitals hold a lot of sensitive data about their patients, and a breach could have serious consequences for patient care. It is important for hospitals to take steps to improve their cybersecurity and develop contingency plans in case of a breach.

Data Breaches & Data Leaks

[Regulators, Insurers, and Customers, All Coming for Progress After MOVEit Breach]

Summary

- The exploitation of a critical vulnerability in Progress Software's MOVEit file transfer software has the US Securities and Exchange Commission (SEC) now investigating and many affected parties seeking compensation.

Analysis & Action

Progress Software has admitted to receiving a subpoena from the SEC in which the Commission asked for various documents and information relating to the MOVEit Vulnerability. The company has also admitted to facing other litigation over the breach, including 58 class action lawsuits filed by individuals who claim to have been impacted by the exfiltration of data.

Progress has also been cooperating with several inquiries from domestic and foreign data privacy regulators, inquiries from several state attorneys general, and an unnamed federal law enforcement agency.

The ongoing fallout from the MOVEit data breach is a stark reminder of the importance of cybersecurity and the risks associated with using software that is not properly patched and maintained.

Cyber Crimes & Incidents

FBI, CISA Warn of Rising AvosLocker Ransomware Attacks Against Critical Infrastructure

Summary

- Critical infrastructure sectors are at risk of ransomware attacks targeting Windows, Linux, and VMware ESXi servers.

Analysis & Action

According to the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI), the AvosLocker ransomware gang has been responsible for numerous ransomware attacks against critical infrastructure sectors.

The ransomware group uses several tactics, techniques, and procedures (TTPs) to exfiltrate private data, such as using legitimate software, open-source remote system administration tools, and custom web shells. The ransomware group targets Windows and VMware ESXi servers through vulnerabilities found.

Members are encouraged to continuously update their software, employ multi-factor authentication, and maintain offline backups to decrease the chances of data exfiltration and ransomware attacks.

Vulnerabilities & Exploits

Dozens of Squid Proxy Vulnerabilities Remain Unpatched 2 Years After Disclosure

Summary

- Vulnerabilities have been detected in Squid Proxy, putting users at greater risk of exploitation.

Analysis & Action

55 vulnerabilities affecting the Squid caching and forwarding web proxy were disclosed this week. A few handfuls of the flaws were assigned Common Vulnerabilities and Exposures (CVE) identifiers, while 35 of the flaws remain unpatched.

Squid is mainly used in content delivery architectures, as well as speeding up broadband and dial-up internet access. These vulnerabilities put consumers at risk of causing a crash in their systems and being victims of exploitation by arbitrary code execution from threat actors. There are currently more than 2.5 million Squid instances exposed on the open internet.

The Squid Team is reportedly understaffed and does not have the resources to patch all the vulnerabilities. Members who use Squid are recommended to update their Squid

systems to the most current version to patch the already fixed vulnerabilities.

Trends & Reports

Ransomware Attacks Doubled Year by Year. Are Organizations Equipped to Handle the Evolution of Ransomware in 2023?

Summary

- A sharp increase in ransomware and malware attacks this year has drawn immense concern for data security.

Analysis & Action

Ransomware and malware attacks have doubled this year and continue to become more complex and capable of bypassing security systems. The manufacturing and healthcare sectors have been the prime targets this year, with healthcare companies becoming the most victimized of ransomware attacks.

Trends report that threat actors will continue to exploit vulnerabilities and develop zero-days for private information and credentials. LockBit's attacks were slightly lower than the previous quarter, but the threat actor group still holds the highest number of victims in Q3-2023. Newer threat actor groups, such as Cactus, INC Random, MedusaLocker, and Cyclop Group, remain potent threats.

This uptick in ransomware attacks against the healthcare sector concerns data privacy and patient care. Members are encouraged to refresh employee training on cyber-awareness and cybersecurity, back up any sensitive data, and implement multi-factor authentication (MFA) to decrease the chances of a ransomware attack.

Privacy, Legal & Regulatory

CISA Plans to Share More Information on Ransomware Actors in Its Exploited Vulnerability Alerts

Summary

- The Cybersecurity and Infrastructure Security Agency (CISA) is giving all organizations access to its known exploited vulnerabilities (KEV) catalog.

Analysis & Action

The announcement by CISA officials gives all organizations access to CISA's KEV, which lists vulnerabilities that are commonly associated with ransomware attacks. Previously, CISA offered the Ransomware Vulnerability Warning Pilot Program (RVWP), which includes private warnings about vulnerabilities associated with known ransomware exploitation.

The KEV will also now include a known-to-be-used-in-ransomware-campaigns column as a central place to find misconfigurations and weaknesses used in ransomware campaigns. CISA plans on continuously updating the KEV list as new and advanced ransomware continues to make its way to the surface.

Members should continuously check the new KEV list to understand trends of ransomware campaigns and protect themselves against any new developments that occur. Members should also continue to look at the RVWP to receive CISA's private warnings about vulnerabilities associated with ransomware exploitation.

Health-ISAC Cyber Threat Level

On September 20, 2023, 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) is due to threats from concerns regarding malvertising, rogue USB drives, Async RAT, MFA Bypass, and persistent credential stuffing/spraying.

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 Register
The Hacker News
Security Affairs
Security Week
The Hacker News
The Record

Tags

MOVEit, ALPHV, AvosLocker

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