Health-ISAC™
Collaborating for Resilience in Healthcare

Daily Cyber Headlines

Daily Cyber Headlines ○ TLP:WHITE Alert ID : 1e823f37 Oct 12, 2023, 08:00 AM

Today's Headlines:

Leading Story

- LinkedIn Smart Links Attacks Return to Target Microsoft Accounts

Data Breaches & Data Leaks

- Nothing to Report

Cyber Crimes & Incidents

- Simpson Manufacturing Shuts Down IT Systems After Cyberattack
- Data Thieves Test-Drive Unique Certificate Abuse Tactic

Vulnerabilities & Exploits

- CISA Warns of Attacks Exploiting Adobe Acrobat Vulnerability
- Microsoft October 2023 Patch Tuesday Fixes 3 Zero-Days, 104 Flaws

Trends & Reports

- Survey Sees Cyberattacks Impacting Primary Health Care Services

Privacy, Legal & Regulatory

- Progress Software's Financial Hit from MOVEit Cuts Deeper

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

LinkedIn Smart Links Attacks Return to Target Microsoft Accounts

Summary

- Threat actors are targeting Microsoft accounts by abusing LinkedIn Smart Links.

Analysis & Action

Microsoft account credentials are at risk of being stolen by threat actors utilizing LinkedIn Smart Links. Over 800 emails were linked to the LinkedIn Smart Link abuse and targeted numerous sectors, the most targeted being finance, manufacturing, energy, construction, and healthcare.

Smart Links are being used in phishing scams to appear trustworthy and authentic to lure victims into giving up private information. These scam links also replicate Microsoft's login page for victims to fill in their email and password.

Members are encouraged to validate the source of any emails that are deemed suspicious and utilize multiple security tools to ensure the protection of private data and information.

Data Breaches & Data Leaks

- Nothing to Report

Cyber Crimes & Incidents

Simpson Manufacturing Shuts Down IT Systems After Cyberattack

Summary

- Simpson Manufacturing detected IT problems and outages in applications, concluding the cause of these issues was from a cyberattack.

Analysis & Action

Before moving their impacted systems offline, Simpson Manufacturing was the victim of a cyberattack. Simpson faced disruptions in their IT infrastructure and local applications. Simpson has not yet identified either the specific type of attack or the group responsible for the attack.

After the SEC 8-K filing from Simpson, its affected systems were immediately taken offline. Due to the proprietary information that Simpson Manufacturing holds, there will be a lengthy remediation process that will continue to hinder parts of day-to-day operations.

Members who contract with Simpson Manufacturing for ongoing projects should expect large delays and extensions to projected end dates. While we do not know the exact method of attack, members should still ensure all PHI is encrypted and inaccessible in the event of an attack.

Data Thieves Test-Drive Unique Certificate Abuse Tactic

Summary

- Attackers are using search engine optimization (SEO) poisoning to deliver results promoting illegal software downloads to spread information-stealing malware.

Analysis & Action

As attackers continue to find new ways to collect credentials and protected health information (PHI), new info-stealing malware is becoming more prominent. The newest development is using SEO poisoning to deliver specific search results that include malicious pages. When the user clicks on these pages, a remote access Trojan (RAT) is delivered. South Korean lab AhnLab revealed that attackers are using LummaC2 and RecordBreaker (Racoon Stealer).

The most recent sample of RecordBreaker includes a string of URL-encoded script to download and execute PowerShell commands but was unsuccessful in both the download and execution. While the sample has failed and will likely fail any verification, they have the potential to confuse and slip past defenses.

Members are encouraged to be careful of any software being downloaded from unverified online sources. It is also important to continue to stay up to date on new developments from LummaC2 and Racoon Stealer.

Vulnerabilities & Exploits

CISA Warns of Attacks Exploiting Adobe Acrobat Vulnerability

Summary

- The Cybersecurity Infrastructure & Security Agency (CISA) warns users of Adobe Acrobat and Reader actively exploited vulnerabilities.

Analysis & Action
CISA has reported in its Known Exploited Vulnerabilities (KEV) catalog that users of Adobe Acrobat and Reader are at risk of malware being deployed into their systems through a use-after-free vulnerability issued as CVE-2023-21608.

The flaw allows threat actors to deploy malware into the victim's compromised systems and access the victim's system privileges when the victim opens a malicious PDF file.

Members who use Adobe Acrobat and Reader are recommended to update their software to the most recent version to decrease the chanced of an exploit by threat actors and to look over the CISA's KEV catalog to identify other vulnerabilities that need to be patched.

Microsoft October 2023 Patch Tuesday Fixes 3 Zero-Days, 104 Flaws

Summary

- Microsoft patched 104 vulnerabilities, three of which were zero-day flaws.

Analysis & Action
As a part of the October Patch Tuesday, Microsoft has fixed three zero-day vulnerabilities in its latest security update, which are being actively exploited in the wild.

The update covered a total of 104 vulnerabilities, with 12 of them being labeled as critical. The bugs are all remote code execution (RCE) bugs. The first vulnerability, CVE-2023-41763, allows an attacker to send a specially crafted network call to a target Skype for Business server, potentially revealing IP addresses or port numbers. The second vulnerability, CVE-2023-36563, allows disclosure of NTLM hashes in WordPad. The final zero-day vulnerability, CVE-2023-44487, has been exploited in the wild to launch some of the biggest DDoS attacks.

Members are advised to patch their Microsoft products immediately to mitigate the risk of successful exploitation by threat actors.

Trends & Reports

Survey Sees Cyberattacks Impacting Primary Health Care Services

Summary

- A new report highlights the risk that cyberattacks on healthcare organizations threaten patient lives.

Analysis & Action
Proofpoint, a cybersecurity and compliance firm, and Ponemon Institute, an IT security research group, released a survey on cyberattacks in the healthcare business.

According to a survey of 653 healthcare security professionals, 88% of firms suffered an average of 40 intrusions in the previous 12 months. A cyberattack on a health care company costs an average of $4.99 million. 66% reported operational and patient care disruption, including poor patient outcomes (57%), increased medical procedure problems (50%), and increased patient fatality rates (23%). This data highlights the dangers of cyberattacks on healthcare institutions, which pose a direct threat to patient treatment and, as a result, human lives.

Cloud compromise, ransomware, supply chain, and business email compromise (BEC) were the most common forms of cyberattacks seen by healthcare providers. Ransomware assaults were the most alarming, with 54% of respondents reporting a ransomware attack on their firm in 2022.

Privacy, Legal & Regulatory

Progress Software's Financial Hit from MOVEit Cuts Deeper

Summary

- Progress Software's costs associated with the MOVEit disaster could grow as class-action lawsuits continue to pile up.

Analysis & Action

Progress Software, the company behind the MOVEit file-transfer service, has disclosed a $2.9 million loss due to continuing cyberattacks on its MOVEit environments.

The insurance covered the majority of the costs. The Securities and Exchange Commission (SEC) is formally investigating the situation since October 2 when it issued a subpoena to Progress. Progress insists that the probe does not imply that it or anybody in the company violated federal securities laws. The company is cooperating with the SEC's inquiry and will continue to interact with the cybersecurity community and its customers.

Currently there it at least 58 class-action lawsuits filed by individuals who want compensation for the impact of the MOVEit attack, therefore it is expected that a growing number of class-action lawsuits and claims filed by customers will lead to further costs for the company.

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

Security Week
Bleeping Computer
Cybersecurity Dive
Security Boulevard
Bleeping Computer
Bleeping Computer
Dark Reading

Tags

LinkedIn, Progress

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