Daily Cyber Headlines

Daily Cyber Headlines | TLP:WHITE | Alert ID : e6037915 | Oct 13, 2023, 06:46 AM

Today's Headlines:

Leading Story

- Ransomware Attacks Now Target Unpatched WS_FTP Servers

Data Breaches & Data Leaks

- SEC Investigating MOVEit Hack That Exposed Data of at least 64 million People

Cyber Crimes & Incidents

- USB Attacks - No One Suspected the Man in a FedEx Uniform
- ToddyCat Hackers Use Disposable Malware to Target Asian Telecoms
- DarkGate Operator Uses Skype, Teams Messages to Distribute Malware

Vulnerabilities & Exploits

- Unpatched Vulnerabilities Expose Yifan Industrial Routers to Attacks

Trends & Reports

- Nothing to Report

Privacy, Legal & Regulatory

- California Enacts Delete Act for Data Privacy

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

Ransomware Attacks Now Target Unpatched WS_FTP Servers

Summary

- Threat actors are targeting unpatched WS_FTP servers affected by CVE-2023-40044.

Analysis & Action

Sophos X-Ops incident responders reported on an observed intrusion attempting to exploit a critical vulnerability affecting Progress WS_FTP servers.

The vulnerability tracked as CVE-2023-40044 could enable unauthenticated attackers to execute commands on the underlying OS via HTTP requests remotely. The attacker attempted to escalate privileges using the open-source GodPotato tool, however, they were not successful in deploying a ransomware payload and, as a consequence, were not able to encrypt any data.

Progress Software released a patch on September 27; however, many servers remain unpatched. While the attack was unsuccessful, we advise members to immediately patch or, in case patching is not possible, disable the vulnerable WS_FTP Server Ad Hoc Transfer Module as a temporary workaround.

Health-ISAC delivered Targeted Alerts to member organizations with instances of Progress WS_FTP.

More on the vulnerability is available in Health-ISAC's vulnerability bulletin here.

Data Breaches & Data Leaks

SEC Investigating MOVEit Hack That Exposed Data of at least 64 million People

Summary

- The SEC has subpoenaed Progress Software and is presently investigating the MOVEit incident.

Analysis & Action

The U.S. Securities and Exchange Commission (SEC) has initiated an investigation into the MOVEit data breach incident from May.

According to reports, the investigation is a "fact-finding inquiry," and there is no evidence that Progress broke any laws. The incident, which was carried out by a Clop ransomware gang that exploited a zero-day vulnerability in Progress MOVEit Software, exposed around 64 million people through breaches of over 2000 enterprises around the world.

FBI (Federal Bureau of Investigation) is currently offering 10 million dollars for information that attributes the Clop's operation to a foreign government. Currently,

there are multiple class action lawsuits against Progress Software due to the incident, which may result in further financial losses for the company.

Cyber Crimes & Incidents

USB Attacks - No One Suspected the Man in a FedEx Uniform

Summary

- A man in Phoenix, Arizona, dressed as a FedEx employee, would go into offices and ask the receptionist for directions; if vacant, he would plug in a USB and download malware onto their network.

Analysis & Action

The man conducted this act numerous times in and around the Phoenix area. The malware-infected USB stick tracked the movement and communication of employees, then around twelve to 18 months later, would convince them to wire money to a bank account.

This attack is different than most, as the malware delivery system was a physical USB, rather than via an email or another online mode of phishing. The use of a USB eliminates the possibility of an employee reporting the email as spam or never opening it, as it instead goes right into the system. The malware used just rode on the back of programs of employees all throughout the office and on their IT network, rather than actively causing havoc and disruptions.

It is important that members recognize the numerous ways in which malware can be delivered onto a system. Members should also ensure their employees have their computers password protected and locked when they get up from their desks. Random/source unknown USBs should never be opened on a work machine, members are advised to disable USB ports and encourage the use of USB data blockers should incidents of unauthorized removable media use increase.

ToddyCat Hackers Use Disposable Malware to Target Asian Telecoms

Summary

- Chinese threat actors are targeting Asian government organizations and telecommunications providers.

Analysis & Action

The Chinese threat actor ToddyCat has been using spear-phishing messages to target Asian government organizations and telecommunications providers since 2021. The campaign has been dubbed Stayin' Alive. These emails contain malicious attachments that deploy malware loaders and backdoors when opened.

These attachments are malicious dynamic-link library (DLLs) that exploit a vulnerability listed as CVE-2022-23748 to sideload the backdoor, known as CurKeep, into the

compromised system. This backdoor can extract information about what software the victim is using, execute commands, send them to the C2 server, and execute other tools, such as CurLu loader, CurCore, and CurLog loader.

Since this malware is spread through spear-phishing messages through email, members are recommended to validate the source of any unexpected and/or suspicious emails to prevent the spread of the malware.

DarkGate Operator Uses Skype, Teams Messages to Distribute Malware

Summary

- DarkGate malware associated with incidents using compromised Skype and Microsoft Teams accounts.

Analysis & Action

Threat actors were observed using compromised Skype and Microsoft Teams accounts to distribute DarkGate malware associated with malicious activities like information theft, keylogging, cryptocurrency miners, and ransomware such as Black Basta.

The attackers are using various techniques to deliver the payload, such as using hijacked accounts to infiltrate message threads and send malicious PDFs to recipients, or to lure victims into the SharePoint site, to download a malicious document.

According to TrendMicro researchers, DarkGate is being sold as a malware-as-a-service, which resulted in a recent increased activity. To mitigate the risk of getting infected with the said malware, members are advised to implement strict rules on the use of messaging applications within the organization, such as blocking external domains, controlling attachments, and implementing scanning of messages where possible.

Vulnerabilities & Exploits

Unpatched Vulnerabilities Expose Yifan Industrial Routers to Attacks

Summary

- Organizations using Yifan industrial routers are at risk of cyberattacks as numerous critical vulnerabilities are found in the router's systems.

Analysis & Action

Several critical vulnerabilities found in industrial routers made by Chinese company Yifan place consumer organizations at risk of threat actors initiating cyberattacks. The device is being used for a multitude of fields, such as self-service terminals, intelligent transportation, industrial automation, smart grid, water supply, finance, and point-of-sale systems.

The vulnerabilities allow threat actors to execute an arbitrary shell on the targeted router. There, the threat actors can change the admin credentials on the device and obtain root access. These vulnerabilities, labeled CVE-2023-32632 and CVE-2023-24479, have been classified as critical.

Members who use the Yifan routers are recommended to patch their routers to the latest version to minimize risk.

Trends & Reports

- Nothing to Report

Privacy, Legal & Regulatory

California Enacts Delete Act for Data Privacy

Summary

- California signed the Delete Act into law, which equips residents with a way to delete their information from around 113 data brokers in the state.

Analysis & Action

The first bill in the United States that compels data brokers to delete all personal data of state residents upon request has been signed into law in California. SB 362, the Delete Act, provides California residents with a delete button via the California Privacy Protection Agency (CPPA), which will delete one's information from the registered data brokers in the state.

The Delete Act is a way for residents of California to protect their data from being exposed and sold off due to a data breach. Incogni's report finds there have been more than 10 data broker breaches to date that have resulted in more than 444.5 million records being exposed. This act represents a step in the right direction for protecting the personal data of citizens in the United States and around the globe.

Members in the state of California should learn about SB-362 and see if they or someone they contract with are considered data brokers in the state of California. Those affected members should be advised that non-compliant brokers will be penalized starting in 2026.

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.

Reference | References

Engadget
Infosecurity Magazine
Bleeping Computer
Bleeping Computer
IT World Canada
Security Week
Dark Reading

Tags

Yifan, ToddyCat, WS_FTP, MOVEit, USB, Progress, DarkGate

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