Daily Cyber Headlines

Daily Cyber Headlines | TLP:WHITE | Alert ID : 785a5125 | Oct 03, 2024, 06:52 AM

Today's Headlines:

Leading Story

- Critical Ivanti RCE Flaw with Public Exploit Now Used in Attacks

Data Breaches & Data Leaks

- Nothing to Report

Cyber Crimes & Incidents

- ESET Research Discovers New Government-Attacking APT Group
- Pisces Introduces Innovative Tools KLogEXE and FPSpy

Vulnerabilities & Exploits

- DrayTek Fixed Critical Flaws in Over 700,000 Exposed Routers
- CISA: Network Switch RCE Flaw Impacts Critical Infrastructure

Trends & Reports

- Fake Job Applications Deliver Dangerous More_eggs Malware to HR Professionals

Privacy, Legal & Regulatory

- Telegram Revealed It Shared U.S. User Data With Law Enforcement

Upcoming Health-ISAC Events

- Global Monthly Threat Brief
  - Americas – October 29, 2024, 12:00-01:00 PM ET

    - European – October 30, 2024, 03:00-04:00 PM CET
- T-SIG Webinar for SMB Members – October 10, 2024 at 11:30 AM ET
- European Summit, Athens, Greece - October 15-17, 2024
- Fall Americas Summit, Phoenix, Arizona - December 2-6, 2024

Additional Information

Leading Story

Critical Ivanti RCE Flaw with Public Exploit Now Used in Attacks

Summary

- Threat actors are actively exploiting a flaw in Ivanti Endpoint Manager (EPM).

Analysis & Action

Tracked as CVE-2024-29824, this SQL Injection vulnerability in Ivanti EPM's Core server can allow unauthenticated attackers within the same network to exploit and execute arbitrary code on unpatched systems.

Security researchers recently published details about the flaw and even created a tool (proof-of-concept exploit) that could potentially be used to exploit vulnerable EPM systems. They also suggested checking your Microsoft SQL server logs for a specific command (xp_cmdshell) as a sign of potential compromise.

Health-ISAC recommends updating your Ivanti EPM to the latest version (2022 SU5 or later) as soon as possible and reviewing your Microsoft SQL logs for the xp_cmdshell command, which might indicate unauthorized access. Health-ISAC distributed a threat bulletin on this vulnerability, which can be accessed here.

Data Breaches & Data Leaks

Nothing to Report.

Cyber Crimes & Incidents

ESET Research Discovers New Government-Attacking APT Group

Summary

- Multiple targeted campaigns discovered large amounts of data exfiltration against government institutions by the new APT group CerenaKeeper.

Analysis & Action

Cybersecurity firm ESET has recently uncovered information on a new APT group by the name of CerenaKeeper. The APT group has been identified to be behind attacks against the Thai government, with substantial amounts of data exfiltration and continued updates to backdoors to avoid detection.

The APT groups' campaigns utilize file-sharing services including GitHub, OneDrive, Dropbox, and PixelDrain in which they will then implement extraction tools and custom backdoors for their attacks. The threat actor's attacks have come at a rather rapid rate, with recurring writes and rewrites of their tools to continue avoiding detection. The threat actors Thai attacks have used versions of attacks previously leveraged by APT MustangPanda as it is believed that the two groups could be sharing tools and information with one another. Signs also point to the use of TONESHELL backdoors where the actor will dump credentials and disable machines' security products. ESET researchers are tracking the threat actor as it continues targeting Thailand's infrastructure.

Health-ISAC encourages members to prioritize patches to any systems that could be vulnerable. Additionally, strong password protection practices and multi-factor authentication can help to mitigate risks of data exfiltration.

Pisces Introduces Innovative Tools KLogEXE and FPSpy

Summary

- New research uncovers two malware samples used by threat actor Sparkling Pisces (aka Kimsuky).

Analysis & Action

Unit 42 recently discovered samples pertaining to threat actor Sparkling Pisces, also known as Kimsuky. These additions to the threat actor's already vast arsenal advance its capabilities even further.

The tools that the threat actor is using are KLogEXE and FPSpy. KLogEXE allows the threat actor to use C++ for a keylogger. This keylogger acts to record input on the keyboard along with any mouse clicks, encrypting the data into a log file in the process. Once the log file reaches its limit, it will be renamed to the current date with the extension .ini, and sent using HTTP command and control servers. FPSpy holds many similarities to the group's previous KGHSpy backdoor, as it is an early version of the tool. Additionally, a customized loader tandems with FPSpy to drop and run sys.dll, where commands can be executed, data can be collected, and encrypted modules can be downloaded.

Analysis of the campaign reveals ties between the two new malware variants and Powershell-based malware, bringing attention to the importance of strategies to avoid these campaigns. Health-ISAC suggests using non-administrative accounts when possible, limiting file sharing, and maintaining recent patches for all software.

Vulnerabilities & Exploits

DrayTek Fixed Critical Flaws in Over 700,000 Exposed Routers

Summary

- Security updates have been released for multiple router models to address various vulnerabilities.

Analysis & Action

Researchers at Forescout Vedere Labs discovered 14 vulnerabilities affecting multiple router models that are both actively supported and beyond end-of-life. The majority of the discovered vulnerabilities are medium-severity security flaws that stem from buffer overflow and cross-site scripting issues.

Conversely, of the accumulated security vulnerabilities, five require immediate action as they carry significant risks. These vulnerabilities impact 24 router models, of which 11 have reached the end of life.

According to Shodan scans on the vulnerable devices, 704,500 devices were discovered with the user interface exposed to the internet. Health-ISAC recommends that users apply the latest firmware updates to affected devices to mitigate risks of exploitation activity.

CISA: Network Switch RCE Flaw Impacts Critical Infrastructure

Summary

- The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has issued an urgent warning about two severe security vulnerabilities.

Action & Analysis

The vulnerabilities affect the Optigo Networks ONS-S8 Aggregation Switch products, commonly in critical infrastructure. These flaws could allow attackers to gain unauthorized access, execute malicious code, and potentially disrupt operations.

The first vulnerability, CVE-2024-41925, is a remote file inclusion (RFI) issue that could enable attackers to execute arbitrary code on the device. The second, CVE-2024-45367, is a weak authentication flaw that could allow attackers to bypass password protections and gain unauthorized access.

Health-ISAC recommends taking defensive measures to minimize the risk of exploitation of these vulnerabilities and to view additional mitigations here.

Trends & Reports

Fake Job Applications Deliver Dangerous More_eggs Malware to HR Professionals

Summary

- Threat actors use resumes as a lure to trick recruiters into downloading malicious files and triggering infection with More_eggs malware.

Analysis & Action

A spear-phishing email campaign targeted recruiters with a JavaScript backdoor called More_eggs, which is sold as malware-as-a-service (MaaS), posing as fake job applications.

This malware can steal information from bank accounts, emails, and IT administrator accounts. Various cybercrime groups such as FIN6, Cobalt, and Evilnum have already incorporated this malware into their toolset. The attackers utilize LinkedIn to distribute fake resumes that trigger infections upon opening. The attackers target recruitment leads seeking engineering talent. The attack deployed obfuscated commands to drop the More_eggs backdoor, communicating with a control server to receive further malware. The use of PowerShell and VBS components was also observed.

Health-ISAC recommends sharing information on this operation with HR or the internal talent acquisition team to minimize the risk of a similar cyberattack within your organization. It is also recommended to always scan documents sent from external sources in a controlled environment like VirusTotal before opening them on the device.

Privacy, Legal & Regulatory

Telegram Revealed It Shared U.S. User Data With Law Enforcement

Summary

- Telegram has started cooperating with law enforcement and will share user data if they are presented with valid legal requests.

Analysis & Action

In 2024, Telegram started cooperating with law enforcement and has fulfilled requests that allegedly required them to share IP addresses or phone numbers of 100+ users. The platform has already responded to some legal requests in Brazil, India, Europe, and the United States.

This reveal signifies a paradigm shift in how Telegram functions. Due to its anonymity and refusal to cooperate with law enforcement, this platform was previously considered a safe hub for criminal activity. CEO Pavel Durov announced this change, stating that if users violate Telegram's rules, their information may be disclosed to authorities. A policy update now allows the sharing of users' data in response to valid legal requests. The company's transparency report revealed 14 requests

fulfilled for U.S. data. A team using AI has been working to remove problematic content, and data shared with authorities will be disclosed in quarterly reports.

It is unlikely that this new policy will severely disrupt criminal networks or force criminal groups to turn to other communication channels, as most threat actors already use VPNs and other encrypted tunnels in an attempt to conceal their activity.

Health-ISAC Cyber Threat Level

On September 19, 2024, 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:

The Threat Level of Blue (Guarded) is due to threats from DPRK IT fraud, elections-induced cyber activity, potential repercussions of recent activity in the Middle East, potential Ivanti Endpoint Manager exploitation, and ongoing observances of infostealer's logs being posted on Telegram.

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.

Report Source(s)

Health-ISAC

Incident Date

Oct 03, 2024, 11:59 PM

Reference | References

The Hacker News
Bleeping Computer
ESET
Health-ISAC Threat Advisory System
CISA

CySecurity
Security Affairs
Bleeping Computer
Bleeping Computer

Tags

Switch RCE Flaw, Tools KLogEXE and FPSpy, More_eggs Malware, Chinese APT, Ivanti, Telegram

---

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 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