Daily Cyber Headlines

Daily Cyber Headlines | TLP:WHITE | Alert ID : cb6d71b5 | Oct 30, 2024, 06:45 AM

Today's Headlines:

Leading Story

- Long Island Plastic Surgical Group Confirms 161K-Record Data Breach

Data Breaches & Data Leaks

- Massive Hack-For-Hire Scandal Rocks Italian Political Elites

Cyber Crimes & Incidents

- BPFDoor Linux Malware Detected by AhnLab EDR
- Massive PSAUX Ransomware Attack Targets 22,000 CyberPanel Instances

Vulnerabilities & Exploits

- New Research Reveals Spectre Vulnerability Persists In Latest AMD and Intel Processors

Trends & Reports

- How Healthcare Organizations Can Minimize the Impact of Ransomware in the Cloud

Privacy, Legal & Regulatory

- Dutch Police Disrupt Major Info Stealers RedLine and MetaStealer in Operation Magnus

Upcoming Health-ISAC Events

- Global Monthly Threat Brief
  - European – October 30, 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

Additional Information

Leading Story

Long Island Plastic Surgical Group Confirms 161K-Record Data Breach

Summary

- A network of 13 plastic surgery practices in New York confirmed several individuals' protected health information (PHI) was compromised.

Analysis & Action

The Long Island Plastic Surgical Group recently disclosed to HHS' Office for Civil Rights (OCR) that 161,707 individuals' protected health information was compromised in a cyber incident earlier this year.

According to an investigation into the matter, a network intrusion occurred between January 4 and January 8, which led to the exfiltration of a limited amount of patient data. The information stolen during the incident were full names in combination with some or all of the following: date of birth, Social Security number, driver's license number/state identification number, passport number, financial account information, medical information, biometric information, health insurance policy information, and clinical photographs.

Despite the Radar threat group claiming responsibility in conjunction with ALPHV, the medical services firm has not confirmed if the incident was part of a ransomware attack. It is assessed that ALPHV performed the initial access aspect of the incident while Radar contributed by exfiltrating the data. Health-ISAC recommends that organizations implement comprehensive security measures and incident response plans to help with risks associated with incidents stemming from threat actor operations.

Data Breaches & Data Leaks

Massive Hack-For-Hire Scandal Rocks Italian Political Elites

Summary

- In recent events, threat actors have worked to steal confidential data from powerful politicians in various countries.

Analysis & Action

A recent 518-page document detailed a 44-year-old man's multi-year database breach of national security systems. This highlights the effects of threat actors and their impacts on governmental and political entities.

The man has committed several other high-level breaches, including penetration of the Pentagon with a threat group. The group took advantage of slow traffic on servers to initiate their attacks, downloading private data belonging to Italy's President and former Prime Minister. A computer virus allowed the threat actors to access the database, allowing remote control of servers.

The threat actors claimed to have breached the information of around 800,000 individuals. The security breach has alarmed many, now being marked as a national scandal and calling for the government to rework its security practices. 60 Individuals are under investigation at this time, while 4 have been arrested, including the male at the helm. Various investigations are underway regarding the long-term breach, with a task force being launched to perform a detailed analysis of national security and its databases.

Data breaches and leaks are a common strategy threat actors use to gain leverage on their victims, highlighting the importance of protective strategies to mitigate risks. Health-ISAC recommends issuing the latest patches to all systems along with anti-virus and anti-malware software to avoid similar computer viruses.

Cyber Crimes & Incidents

BPFDoor Linux Malware Detected by AhnLab EDR

Summary

- Threat actor Red Menshen uses BPFDoor, a backdoor, to target Asian and Middle Eastern regions.

Analysis & Action

The backdoor uses Berkeley Packet Filter, in which the threat actor takes advantage of services that are already running. These are often SSH services or web servers that do not need to connect to a C&C server like a typical backdoor, permitting it to avoid detection on the system that it infects.

The technology grants the ability for user programs to attach to network filters, choosing whether or not to deny or permit data coming through sockets. Once the backdoor is initially executed, it utilizes a series of commands that will copy itself to /dev/shm using the name kdmtmpflush, deleting itself afterward. A BPF filter is then registered and waits for a threat actor to send its commands containing a magic packet. Once that command is received, the malware then branches. From there, the threat actor has several options: connecting to IP/ports, opening new ports, or determining the infection status. Through the blindshell process, a new port is opened by the malware, setting up a firewall that redirects packets from the IP of the threat actor to a new port. Afterwards, the added firewall is removed.

Threat actors use sophisticated backdoor strategies to gain access to targeted systems. Health-ISAC recommends that its members implement network monitoring processes and antivirus solutions to help prevent backdoor attacks.

Massive PSAUX Ransomware Attack Targets 22,000 CyberPanel Instances

Summary

- Over 22,000 CyberPanel instances were exposed online, leading to mass targeting in a PSAUX ransomware attack.

Analysis & Action

According to security researcher DreyAnd, CyberPanel version 2.3.6 suffered from three separate security flaws that could be exploited by a threat actor, allowing them to gain remote root access without authentication. The three issues stem from defective authentication, input validation, and security filter bypass flaws.

On October 23, 2024, the security researcher disclosed the vulnerability to the CyberPanel developers, who shortly after released a fix for the authentication issue on GitHub. Despite these recent details, the developers have not released an updated version of CyberPanel nor issued a CVE identifier.

According to the threat intelligence search engine LeakIX, 21,761 vulnerable CyberPanel instances were exposed and subsequently dropped to approximately 400 instances. The instances were later confirmed to be mass-exploited by threat actors who installed PSAUX ransomware on them. The PSAUX ransomware operation has been around since June 2024 and targets exposed web servers through vulnerabilities and misconfigurations. It is recommended that users upgrade to the latest version available on GitHub to avoid targeted exploitation activity.

Vulnerabilities & Exploits

New Research Reveals Spectre Vulnerability Persists In Latest AMD and Intel Processors

Summary

- New findings detail recent AMD and Intel processors' susceptibility to execution attacks from aged Spectre security flaws.

Analysis & Action

An over-six-year-old security flaw involving Spectre has been revealed again after recent AMD and Intel processors were identified as susceptible to execution attacks. The attack's intention was to undercut x86 chips' Indirect Branch Predictor Barrier (IBPB).

The barrier is used to counter Branch Target Injection (BTI) practices and CVE-2017-5715, which is an execution attack across domains. The execution will allow a disclosure gadget to gain access and exfiltrate over a secret channel. Recent findings, using end-to-end cross-process descriptions, detail a bug within Intel’s Golden Cove and Raptor Cove microarchitectures. AMD’s version of IBPB also holds similar strategies to be bypassed, allowing adversaries to leak memory. Intel made patches to the microcode in 2023 and 2022, addressing CVE-2023-38575 and CVE-2022-23824, asking its users to ensure their intel microcode is part of the latest version; the lengths these patches protect are unclear. With several new disclosures regarding dated practices, these findings highlight the importance of using recent and up-to-date software.

Health-ISAC recommends its members use validation and sanitation methods for all users implemented into networks to mitigate risks of similar execution attacks across domains.

Trends & Reports

How Healthcare Organizations can Minimize the Impact of Ransomware in the Cloud

Summary

- As the trend of ransomware attacks on healthcare continues to improve, preventative strategies are being explored.

Analysis & Action

Healthcare organizations are experiencing the detrimental impacts of ransomware attacks via threat actors, seeing a 95% increase year-over-year. With improvements to these attack processes on the horizon for threat actors, a means of prevention is necessary for healthcare organizations to protect their networks.

At this point, many healthcare organizations will likely have or will experience a ransomware attack. Various private information, such as patient data, can be used for ransom payments, highlighting a need for protocols and tools to secure data and protect patient bases. One of these tools is the automation of security and its solutions, allowing for automated detection of threat actors and capabilities to recover from ransomware attacks. Additionally, providing awareness training to employees doubles down on this practice, as human error remains a large factor regarding cybersecurity incidents as well. Methods such as testing protocols, backups, and data encryption can bolster healthcare organizations' security. An action to prioritize network security with these solutions can help aid against threat actors and their malicious attacks.

It is recommended that organizations implement these security solutions and fundamentals to minimize the impacts of ransomware attacks by threat actors. Additionally, ensuring all staff is aware of potential threats pertaining to ransomware mitigates the risks of an internal error leading to a leak of sensitive data and information.

Privacy, Legal & Regulatory

Dutch Police Disrupt Major Info Stealers RedLine and MetaStealer in Operation Magnus

Summary

- Dutch police, in collaboration with international partners, disrupt infrastructure associated with infostealers.

Analysis & Action

In coordination with international partners, the Dutch National Police disrupted the infrastructure behind two information stealers, identified as RedLine and MetaStealer. On October 28, 2024, Operation Magnus was launched as part of an international law enforcement task force that included authorities from the United States, the United Kingdom, Belgium, Portugal, and Australia.

Operation Magnus shut down three servers in the Netherlands and seized two domains. Additionally, one administrator has been charged by United States authorities, and two people have been arrested by Belgian police.

Before Operation Magnus, a years-long investigation into the technical infrastructure of the information stealers began due to a tip from ESET that the servers were located in the Netherlands. An account of the data seized from the servers includes usernames, passwords, IP addresses, timestamps, and more. It is important that organizations regularly update software, use strong antivirus solutions, and educate users about the importance of cyber hygiene to defend against information stealer malware.

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.

Report Source(s)

Health-ISAC

Reference | References

HIPAA Journal
GitHub
Politico
The Hacker News
ahnlab
healthcareittoday
Bleeping Computer
The Hacker News

Tags

Ransomware in Healthcare, Operation Magnus, PSAUX Ransomware, BPFDoor Linux Malware, Hack-for-Hire, Spectre Vulnerability, Data Breaches

---

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