Daily Cyber Headlines

Daily Cyber Headlines | TLP:WHITE | Alert ID : 496d9ef6 | Oct 28, 2024, 07:49 AM

Today's Headlines:

Leading Story

- Black Basta Ransomware Poses As IT Support on Microsoft Teams to Breach Networks

Data Breaches & Data Leaks

- OnePoint Patient Care Data Breach Impacted 795,916 Individuals

Cyber Crimes & Incidents

- BRICS Summit: Russia's Foreign Ministry Attacked
- Ukraine Warns of Mass Phishing Campaign Targeting Citizens' Data

Vulnerabilities & Exploits

- Windows 11 CLFS Driver Vulnerability Allows Attackers To Escalate Privileges: PoC Exploit Released

Trends & Reports

- AWS Seizes Domains Used by Russia's APT29
- Fog Ransomware Targets SonicWall VPNs to Breach Corporate Networks

Privacy, Legal & Regulatory

- Nothing to Report

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 – November 14, 2024 at 11:30 AM ET
- Fall Americas Summit, Phoenix, Arizona - December 2-6, 2024

Additional Information

Leading Story

Black Basta Ransomware Poses As IT Support on Microsoft Teams to Breach Networks

Summary

- BlackBasta ransomware was observed disguising itself as IT support to gain initial network access.

Analysis & Action

The BlackBasta ransomware group has changed its tactics to target victims through Microsoft Teams by impersonating corporate help desk personnel.

The operation includes contacting employees and posing as help desk personnel to resolve spam attacks after the threat actors initially bombarded the potential victims with unsolicited communications. During the vishing attack, the threat actors trick their targets into installing AnyDesk or providing them with remote access to their Windows devices through Windows Quick Assist.

Once the threat actors are granted access, malicious scripts to install payloads, including ScreenConnect, NetSupport Manager, and Cobalt Strike, are executed as persistence mechanisms to maintain remote access to the user's corporate device. After the threat actors gain access, they move throughout the network laterally, steal data, and eventually deploy the ransomware encryption tool.

Health-ISAC recommends that organizations implement comprehensive security awareness training, strong password policies, multi-factor authentication, and vigilant monitoring of network activity to defend against social engineering attacks that can lead to threat actors gaining initial access.

Data Breaches & Data Leaks

OnePoint Patient Care Data Breach Impacted 795,916 Individuals

Summary

- OnePoint Patient Care, a US hospice pharmacy's recent data breach, has impacted nearly 800,000 individuals.

Analysis & Action

The pharmacy is known for its specialization in palliative and hospice care services for those with advanced illnesses. It works with other healthcare providers to provide patients with complex medication regimens in their homes.

The recent data breach exposed approximately 795,916 people, reported by the US Department of Health and Human Services. This came after suspicious activity was noticed on the organization's network back on August 8, 2024, which generated an internal investigation. Upon investigation, a data breach was discovered to have occurred between August 6 and 8 of the year. The data from the breach included resident information, names, diagnoses, medical records, social security numbers, and prescription details. As a result of the data breach, it has been recommended that affected personnel monitor their credit reports and statements to report fraudulent activity to law enforcement. The organization was recently added to threat actor Inc Ransom's list of victims on its leak site, making them the likely assailant of the attacks. The company has not paid ransom.

Threat actors' tactics of ransomware attacks remain common among their strategies, highlighting the importance of protecting network security and its data. Health-ISAC recommends issuing the latest patches to all devices and conducting regular vulnerability scans to mitigate the risks of experiencing a data breach and leak.

Cyber Crimes & Incidents

BRICS Summit: Russia's Foreign Ministry Attacked

Summary

- A major attack transpires during the major Russian BRICS Summit.

Analysis & Action

The attack was identified to be a Distributed Denial-of-Service Incident (DDoS) attack, causing a major outage. The attack occurred at the same time as the major Brazil, Russia, India, China, and South Africa (BRICS) Summit.

Attacks of this vein are typically nothing new for their website, but the implications faced in this instance were described to reach a rather large scale. The DDoS attack caused a delay in a briefing that had been planned prior; the delay spanned four hours total due to the technical issues caused by the attack. During the delay, problems within the website were worked on while attempting to restore the Ministry's Internet functionality and resources. The intentions of the Summit were to express the international prestige that Russia holds while creating harmony within the relationships of China and India. This attack highlights the imposed threat of international threat actors and their actions going forward.

DDoS attacks are a common strategy used by threat actors to slow or shut down one's systems temporarily. Health-ISAC recommends utilizing rate-limiting processes on networks, applications, and DNS levels to limit traffic throughout servers and networks to mitigate potential future DDoS attacks via threat actors.

Ukraine Warns of Mass Phishing Campaign Targeting Citizens' Data

Summary

- Warnings of a mass phishing campaign detail threat actors stealing citizens' personal data.

Analysis & Action

The threat actors are being addressed at this time as UAC-0218. They send links disguised as billing or payment details while actually downloading malware-containing data. The script is capable of searching victim devices in differing formats to send to the threat actor's server, allowing them to steal personal or financial data.

In a data exfiltration operation, phishing emails will contain account details emails with a link, downloading RAR archives using the same name. Within the archives are two decoy documents protected by passwords. These documents are named Договір20102024.doc and Рахунок20102024.xlsx along with a VBS script Password.vbe. The VBS script will run code to do a recursive search for file types across various directories from the users folder once clicked. All files

under 10MB are then exfiltrated to the server of the threat actor. Additionally, CERT-UA analysts found a one-line Powershell command executable file on systems of victims as well that uses a similar function. In August of this year, over 100 computers owned by the Ukrainian government have been compromised due to the phishing campaign in which targets were lured to click a malicious link containing ANONVNC malware which would then download to the device.

Health-ISAC recommends its members exercise caution when clicking links or opening emails. Additionally, blocking phishing emails on email clients or using automated services can help prevent similar phishing campaigns.

Vulnerabilities & Exploits

Windows 11 CLFS Driver Vulnerability Allows Attackers To Escalate Privileges: PoC Exploit Released

Summary

- A critical flaw discovered allows users to exploit system functions using elevated privileges.

Analysis & Action

The vulnerability involves Windows 11's Common Log File System (CLFS) driver. The flaw allows users to gain higher privileges and exploit the functions within the system.

The vulnerability lies within the CClfsBaseFilePersisted::WriteMetadataBlock function. Issues arise due to the return value of ClfsDecodeBlock not being checked properly, allowing threat actors to corrupt the system structures and elevate their privileges. The vulnerability also poses the potential to leak kernel pool addresses through the process of bypassing Windows 11 24H2 mitigations; this PoC, however, does not use the method. The steps involved in this particular exploit start with creating a log file and then adding containers.

Afterward, the threat actor will manipulate the file's structure to control sector tags. Then, the threat actor will create a fake structured CClfsContainer in user space, allowing them to leak information regarding the system, like process thread and kernel addresses. Finally, the threat actor can bypass security checks by changing system settings and escalating their privileges. Though Microsoft has claimed the vulnerability has been addressed previously, reports show the exploit is still functional on Windows 11's latest version. No CVE has been provided at this time.

Health-ISAC recommends that its members utilize prevention tools for data loss security and encryption methods to assess and mitigate possible attacks from threat actors.

Trends & Reports

AWS Seizes Domains Used by Russia's APT29

Summary

- Amazon Web Services identified and seized infrastructure used by APT29 to execute phishing attacks.

Analysis & Action

Amazon Web Services recently identified malicious domains used by Russian threat actor APT29 for phishing. The infrastructure was aimed at collecting Windows credentials via Microsoft Remote Desktop. The targets included government agencies, enterprises, and military organizations.

According to Amazon, the malicious domains used by APT29 were made to impersonate AWS domains. During their phishing campaign, the threat actors were observed sending emails with lures referencing integration with Amazon and Microsoft services and implementing a zero-trust architecture. Through the phishing emails, RDP configuration files were delivered that would grant a threat actor remote access to compromise the device when executed.

Successfully executed attacks provided threat actors access to the local disk, printers, network resources, and the clipboard. Additionally, threat actors could run malicious applications and scripts on the compromised system. Health-ISAC recommends that organizations implement email security controls and employee training to bolster their defenses against phishing attacks.

Fog Ransomware Targets SonicWall VPNs to Breach Corporate Networks

Summary

- Ransomware operators have been observed exploiting SonicWall VPN vulnerabilities to compromise enterprise networks.

Analysis & Action

The Fog and Akira ransomware groups have been actively exploiting a critical vulnerability tracked as CVE-2024-40766, which affects SonicWall VPNs, to gain unauthorized access to enterprise networks. Despite SonicWall having fixed the vulnerability in late August, the security flaw was actively exploited roughly a week later.

According to security researchers, there has been an upward trend in ransomware attacks targeting SonicWall VPNs. Both Akira and Fog ransomware have been responsible for at least 30 intrusions initiated by gaining remote access through vulnerable accounts. Of these cases, Akira accounts for 75% of these attacks and Fog ransomware takes up the remainder.

In most cases, the ransomware attacks were swift, as data encryption occurred within a short timeframe. The time from intrusion was small, often less than ten hours, and sometimes as little as 1.5-2 hours. To conceal their tracks, the threat actors leverage VPN or VPS services to mask their IP addresses. Organizations should implement layered security controls, including strong endpoint security, regularly updating software, backup and recovery plans, and employee security awareness training to mitigate risks associated with ransomware attacks.

Privacy, Legal & Regulatory

- Nothing to Report.

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

Bleeping Computer
Security Week
cybersecurityintelligence
Bleeping Computer
Infosecurity Magazine
Security Affairs
cybersecuritynews

Tags

Windows 11 CLFS Driver Vulnerability, BRICS, Fog Ransomware, BlackBasta, APT29, Data Breaches, Phishing, Ukraine

---

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