Health-ISAC Daily Cyber Headlines

Daily Cyber Headlines **TLP:WHITE** **Alert Id: 2b6f95fe** **2022-10-21 12:39:32**

Today's Headlines:

Leading Story

- Internet Connectivity Worldwide Impacted by Severed Fiber Cables in France

Data Breaches & Data Leaks

- Microsoft Confirms Data Leak but Disputes Scope

Cyber Crimes & Incidents

- Battle with Bots Prompts Mass Purge of Amazon, Apple Employee Accounts on LinkedIn
- OldGremlin Hackers Use Linux Ransomware to Attack Russian Organizations

Vulnerabilities & Exploits

- Vulnerabilities in Abode Systems Home Security Could Allow Hacker to Take Over Cameras

Trends & Reports

- Only 4% of Security and IT Leaders Believe All of Their Cloud Data is Sufficiently Secured

Privacy, Legal & Regulatory

- Nothing to Report

Upcoming Health-ISAC Events

- Health-ISAC Monthly Threat Brief – October 25, 2022, 12:00 PM Eastern

Leading Story

Internet Connectivity Worldwide Impacted by Severed Fiber Cables in France

Summary

- A major internet cable in the South of France was severed on October 20, 2022, which impacted subsea cable connectivity to multiple regions in the world.

Analysis & Action

It was reported that a major internet cable in the South of France was severed yesterday, which impacted subsea cable connectivity to Europe, Asia, and the United States.

It was assessed that due to the incident data packet losses and increased website response latency were registered. It was observed that users experienced issues when connecting to applications hosted overseas, however, routing adjustments were made to mitigate the impact. Additionally, researchers determined that the incident impacted three different links including Marseille-Lyon, Marseille-Milano, and Marseille-Barcelona.

Apart from this incident, it was also reported that a subsea cable linking the Shetland Islands to the Scottish mainland has been damaged too, leaving individuals leaving on the island without access to the internet.

Data Breaches & Data Leaks

Microsoft Confirms Data Leak but Disputes Scope

Summary

- Microsoft has recently confirmed that one of its misconfigured cloud systems led to customer information being exposed on the internet.

Analysis & Action

According to Microsoft Security Response Center (MSRC), it was reported that due to a misconfigured endpoint business transaction data related to interactions between Microsoft and its customers has been exposed.

The company that reported the incident to Microsoft was SOCRadar. It was assessed by security researchers that the information exposed included sensitive data such as proof of execution and statements of work documents, user information, product offers and orders, project details, as well as personally identifiable information.

The leak has been referred to as BlueBleed and it is estimated that Microsoft-managed public cloud storage buckets contained information on more than 150,000 companies in 123 countries and that 2.4TB containing information about emails, projects, and users were leaked. Microsoft has argued that SOCRadar has greatly exaggerated the scope of this issue, as their research shows various cases of duplicated information.

Additional information about Microsoft's data leak can be accessed here.

Cyber Crimes & Incidents

Battle with Bots Prompts Mass Purge of Amazon, Apple Employee Accounts on LinkedIn

Summary

- Security researchers have observed a massive spike in phony Apple and Amazon employee profiles on LinkedIn.

Analysis & Action

Security researchers saw a massive increase followed by a massive decrease in the Apple and Amazon employee counts on LinkedIn. It has been speculated that these accounts have been created using artificial intelligence for information-gathering purposes.

LinkedIn is an incredibly powerful source to gather information on aspiring employees. However, this same information can be used with great success to facilitate social engineering attacks.

This newest development on LinkedIn highlights the existence of LinkedIn being used for OSINT activities. As threat actors become more innovative and AI goes more mainstream, the looming threat of deepfakes grows in severity.

OldGremlin Hackers Use Linux Ransomware to Attack Russian Organizations

Summary

- Security researchers have observed that the threat actor OldGremlin has incorporated new features in its toolkit with file-encrypting malware.

Analysis & Action

It was observed by security researchers that the threat actor OldGremlin, has expanded its toolkit with file-encrypting malware for Linux machines.

OldGremlin has been assessed to be one of the few ransomware groups that attack Russian corporate networks and has targeted various industries including logistics, insurance, retail, real estate, and finance, as well as other sectors. OldGremlin was observed targeting a Linux machine with a Go variant of the TinyCrypt ransomware used to encrypt Windows machines.

The new Linux variant works in the same way as the Windows counterpart, however, this represents a clear evolution and adaptation of the threat actors' TTPs to target additional operating systems. The TinyCrypt ransomware also encrypts files with a 256-bit key. It is advised to track the threat actor's campaigns as OldGremlin is a highly skilled actor with a powerful toolkit that increases the probability of the threat actor receiving the ransom payment.

Vulnerabilities & Exploits

Vulnerabilities in Abode Systems Home Security Could Allow Hackers to Take Over Cameras

Summary

- Cisco Talos has recently disclosed multiple vulnerabilities in Abode Systems iota All-in-One Security Kit that could allow attackers to take over cameras.

Analysis & Action

The vulnerabilities disclosed by Cisco Talos include a main security camera and hub that alert users of unwanted movement in their homes; however, the vulnerabilities could lead to multiple issues.

If the vulnerabilities are exploited, attackers could be able to change users' login passwords, inject code onto the device, manipulate sensitive device configurations, and cause the system to shut down. The vulnerabilities that could lead to code execution are tracked as CVE-2022-27804, CVE-2022-2947, CVE-2022-32586, and CVE-2022-30603.

However, the most sensitive vulnerabilities with a CSSV score of 10 out of 10 are tracked as CVE-2022-33192 - CVE-2022-33195, CVE-2022-33189, CVE-2022-30541, and CVE-2022-32773, which could allow an attacker to execute arbitrary system commands with root privileges.

Trends & Reports

Only 4% of Security and IT Leaders Believe All of Their Cloud Data is Sufficiently Secured

Summary

- BigID has released a new report on cloud data security that offers valuable insights with results from over 1,500 IT and security professionals.

Analysis & Action

According to BigID's newest Cloud Data Security Research Report 2022, there are multiple characteristics regarding data on the cloud and trends that should be considered.

The report has highlighted that organizations are struggling with securing and tracking sensitive data in the cloud as only 4% of the respondents believe all their cloud data is sufficiently secured. Also, it was assessed that 82% of organizations considered capturing dark data a moderate to high priority during 2022, as 79% of organizations expressed concerns regarding the proliferation of dark data in their organization.

Additionally, it was stated that tracking data across SaaS has become a priority and that 62% of organizations report that they are likely to experience a cloud data breach in the next year.

BigID's full Cloud Data Security Research Report can be accessed here.

Privacy, Legal & Regulatory

Nothing to Report

Health-ISAC Cyber Threat Level

On September 15, 2022, 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) was chosen in response to credential thieving and social engineering attempts with CEO Impersonation, fraudulent payment processing, EU energy crisis, Russia-Ukraine ongoing conflict, railroad strike and supply chain Issues, and IcedID and Qbot reemergence.

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(s): The Register, Bleeping Computer, Ars Technica, Krebs on Security, Bleeping Computer, Cisco Talos, Dark Reading, bigid

Tags: Internet Cables, Daily Cyber Headlines, OldGremlin hacking group, DCH, Cloud Data, LinkedIn, Cisco Talos, Apple, amazon, Microsoft

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