Daily Cyber Headlines

Daily Cyber Headlines	TLP:WHITE	Alert Id: 16ddcc97	2024-10-25 11:12:59

Today's Headlines:

Leading Story

- Cisco Patches Vulnerability Exploited in Large-Scale Brute-Force Campaign

Data Breaches & Data Leaks

- Insurance Admin Landmark Says Data Breach Impacts 800,000 People

Cyber Crimes & Incidents

- Cerberus Malware: Understanding the Evolving Android Banking Trojan and the ErrorFather Campaign
- Iranian Hackers Target U.S. Election Systems Ahead of 2024 Presidential Race

Vulnerabilities & Exploits

- Nothing to Report

Trends & Reports

- Why Phishing-Resistant MFA Is No Longer Optional: The Hidden Risks of Legacy MFA

Privacy, Legal & Regulatory

- Irish Watchdog Imposes Record €310 Million Fine on LinkedIn for GDPR Violations
- UK Government Introduces New Data Governance Legislation

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

Leading Story

Cisco Patches Vulnerability Exploited in Large-Scale Brute-Force Campaign

Summary

- Cisco issues security updates to address multiple vulnerabilities in its ASA, FMC, and FTD products.

Analysis & Action
Cisco released updates for multiple vulnerabilities in its ASA, FMC, and FTD products. One of the vulnerabilities, tracked as CVE-2024-20481, has already been exploited by threat actors. This vulnerability impacts the remote access VPN (RAVPN) service of ASA and FTD, which could allow unauthenticated threat actors to execute a denial of service (DoS) condition.

Additionally, other vulnerabilities, including a critical flaw in ASA, could allow a threat actor to launch malicious commands with root privileges and several high-severity flaws in FTD that can be exploited to cause denial of service attacks. Cisco has also provided updates for a handful of medium-severity vulnerabilities in these products.

Health-ISAC recommends that organizations apply the updates to mitigate the risks of targeted exploitation attacks executed by threat actors. For more information, organizations may reference Cisco's security advisories here.

Data Breaches & Data Leaks

Insurance Admin Landmark Says Data Breach Impacts 800,000 People

Summary

- Over 800,000 people were impacted by a data breach that occurred in May at insurance firm Landmark Admin.

Analysis & Action
The insurance administrative services company disclosed a data breach that may have impacted the personal information of over 800,000 individuals. On May 13, 2024, the insurance firm shut down its IT systems after identifying suspicious activity to prevent the attack's spread.

A third-party cybersecurity firm was engaged to help investigate the incident and determine the extent of the data theft. During the investigation, the company confirmed that some files containing the personal information of 806,519 people were accessed during the breach.

Impacted individuals are advised to monitor their credit reports and bank accounts for signs of fraudulent behavior. At this time, no threat actor has been attributed to the data breach. Organizations should implement appropriate security measures, including vulnerability assessments, strong access controls, and employee training, to minimize the likelihood of data breaches.

Cyber Crimes & Incidents

Cerberus Malware: Understanding the Evolving Android Banking Trojan and the ErrorFather Campaign

Summary

- Cerberus banking Trojan has resurged, targeting healthcare, digital wallets, and government entities.

Analysis & Action
The malware first appeared in 2019. Since then, it has evolved substantially, now targeting applications within the government, healthcare, and digital wallets. This comes in the midst of a dramatic rise in financially motivated attacks by threat actors, with Android devices constantly targeted.

Within the year, there has been a 29% growth in malware pertaining to banking, while spyware has seen a 111% growth throughout the year. The difficulty in detecting Cerberus malware, being part of the movement, enhanced its capabilities with modifications like the dynamic switching of command and control servers to evade being detected. Cerberus Android Banking Trojan boasts several capabilities, the first being the use of multi-staged droppers to mitigate manual and automated analysis of threats for both detection and removal. Additionally, the malware holds various malicious functions like keylogging, remote access controls provided by overlay attacks, and Virtual Network Computing. The malware also utilizes a Domain Generation Algorithm (DGA) to prevent its malware from being blocked. The malware is now known to only target Android devices, slightly shrinking its base for attacks but highlighting the importance of avoiding the trojan.

To keep devices safe, avoid downloading unnecessary applications from the Google Play Store and use a trusted security application on your device. Additionally, avoid providing applications with sensitive information and enable MFA at all possible entry points for threat actors. Finally, maintain caution for SMS, email, and chat links to mitigate all risks of similar attacks.

Iranian Hackers Target U.S. Election Systems Ahead of 2024 Presidential Race

Summary

- United States websites and media targeted by Iranian hacking groups as the US presidential election approaches.

Analysis & Action
In light of a recent report by Microsoft, a threat actor named Cotton Sandstorm has targeted election-based websites and media as the US election approaches. The group has since been discovered to be part of Iran's Islamic Revolutionary Guard Corps (IRGC).

The threat actor has been identified for its reconnaissance and probing of critical election systems within various states. This activity has raised concerns regarding possible interference by foreign entities in the election. However, this isn't Cotton Sandstorm's first time partaking in such activities, as they followed through with a cyber-influence operation in the 2020 presidential election to create chaos, spreading false information. This included sending emails with threats to voters, while the aftermath of the election saw the threat actor encourage violent acts against government officials. More recently, research from Microsoft found the threat actor to have ramped up its activities again with beliefs that the actions were part of a broader campaign. The threat actor will probably use similar methods to spread misinformation to voters as the election approaches. Microsoft's MTAC report surrounds the general importance of detecting these campaigns through fact-checking and public awareness.

As foreign actors continue to spread divisive narratives to various regions and countries, it is important to remain vigilant and fact-check all incoming and outgoing information. A peak in the level of misinformation is expected within the 48-hour window before and after election day.

Vulnerabilities & Exploits

Nothing to Report.

Trends & Reports

Why Phishing-Resistant MFA Is No Longer Optional: The Hidden Risks of Legacy MFA

Summary

- A collaboration advisory from CISA and the FBI issued warnings regarding SMS-based OTP MFA.

Analysis & Action
Ransomware has grown significantly throughout the year, with payment averages increasing by 500%. These statistics' alarming implications create an urgency to stop data breaches and ransomware attacks.

Sophistication by threat actors is ever-growing; the continuing rise in incidents highlights this, along with the weakness of outdated security practices. A leading cause of this issue is the use of legacy MFA, which has since been rendered ineffective against more recent threat actors. Reports from CISA state that 90% of ransomware attacks that were successful started with phishing. A call is being made for individuals to move to phishing-resistant MFA instead. Additionally, part of cybercriminals' phishing strategies now includes generative AI that has been implemented to create more convincing emails, personalizing to specific targets. As cyberattacks and their technologies continue to expand, so should users' protective strategies against them. With next-generation phishing-resistant MFA solutions, organizations can be safeguarded from the devastation of data breaches and ransomware attacks.

Health-ISAC recommends considering swift action to transition away from legacy multifactor authentication and move to phishing-resistant tools to mitigate risks of future cyber attacks from threat actors.

Privacy, Legal & Regulatory

Irish Watchdog Imposes Record €310 Million Fine on LinkedIn for GDPR Violations

Summary

- LinkedIn was fined €310 Million for breaching user privacy by using personal data for behavioral targeting.

Analysis & Action
LinkedIn was penalized under the General Data Protection Regulation (GDPR), which establishes a framework for the collection, processing, storage, and transfer of personal data within the EU and the European Economic Area (EEA).

Due to a complaint filed to the French Data Protection Authority in 2018, it was discovered that LinkedIn violated three different GDPR principles regarding transparency and fairness, including Article 6 GDPR and Article 5(1)(a), Articles 13(1)(c) and 14(1)(c), and Article 5(1)(a).

LinkedIn failed to obtain explicit consent or provide adequate notice to users before processing third-party data and incorrectly leveraged legitimate interests as a legal basis for processing first-party data for targeted advertising. Health-ISAC recommends that organizations strictly follow regulatory guidelines to avoid facing financial penalties imposed for violating compliance standards.

UK Government Introduces New Data Governance Legislation

Summary

- The UK government has enacted new legislation to control how personal data is used and shared online.

Analysis & Action
The new legislation establishes a system for certifying digital verification services. As a result, companies offering these services can obtain a government-approved trust mark from the newly formed Office for Digital Identities and Attributes (OfDIA) within the Department of Science Innovation and Technology (DSIT).

The purpose of the trust mark is to increase public confidence in the security and privacy of digital verification services. This could help facilitate more efficient processes in areas such as parcel collection, opening bank accounts, and relocation.

Ultimately, the bill's implementation is deemed to enhance data privacy, reduce fraud, and facilitate secure access to services for individuals and businesses.

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.
Reference(s): feedly, Bleeping Computer, The Hacker News, thecyberexpress, mallocprivacy, Infosecurity Magazine, Security Week, Cisco
Report Source(s): Health-ISAC

Tags: Phishing-Resistant MFA, GDPR, US Elections, UK government, Iranian Hackers, Data Breaches, Cisco
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