Daily Cyber Headlines

Daily Cyber Headlines | TLP:WHITE | Alert ID : 3399455d | Oct 18, 2023, 07:08 AM

Today's Headlines:

Leading Story

- TetrisPhantom: Cyber Espionage via Secure USBs Targets APAC Governments

Data Breaches & Data Leaks

- D-Link Confirms Data Breach: Employee Falls Victim to Phishing Attack

Cyber Crimes & Incidents

- Russia's Sandworm Hacking Unit Targets Ukrainian Telecom Providers
- Watch Out: Attackers Are Hiding Malware in Browser Updates

Vulnerabilities & Exploits

- Over 40,000 Admin Portal Accounts Use Admin as a Password

Trends & Reports

- Chinese Government Limits What Biometrics and Data Can Be Used to Train Generative AI

Privacy, Legal & Regulatory

- Nothing to Report

Cybersecurity Awareness Month

- The Daily Cyber Headlines are being shared during the month of October at **TLP:WHITE** for Cybersecurity Awareness Month.

Upcoming Health-ISAC Events

- Americas Hobby Exercise - October 25, 2023. Registration is available here.
- Health-ISAC Monthly Threat Brief – October 31, 2023, 12:00 PM Eastern

Additional Information

Leading Story

TetrisPhantom: Cyber Espionage via Secure USBs Targets APAC Governments

Summary

- A new cyber espionage campaign dubbed TetrisPhantom is targeting government entities in the Asia-Pacific (APAC) region.

Analysis & Action

The attackers are exploiting a particular type of secure USB drive to covertly spy on and harvest sensitive data.

The USB drives offer hardware encryption and are employed by government organizations worldwide to securely store and transfer data, raising the possibility that the attacks could expand in the future to have a global footprint.

The malware components are capable of self-replicating through connected secure USB drives to breach air-gapped networks and executing other malicious files on the infected systems.

The full blog post from Kaspersky is available for your review here.

Data Breaches & Data Leaks

D-Link Confirms Data Breach: Employee Falls Victim to Phishing Attack

Summary

- D-Link has confirmed a data breach that led to the exposure of low-sensitivity and semi-public information.

Analysis & Action

D-Link has confirmed a data breach likely originating from an old D-View 6 system that reached its end of life in 2015. The data was used for registration purposes back then and did not contain any user IDs or financial information.

The breach was caused by an employee falling victim to a phishing attack. D-Link is working with cybersecurity firm Trend Micro to investigate the incident and is taking steps to enhance the security of its operations.

Current active customers are unlikely to be impacted by this incident.

D-Link has provided an announcement including details about the information disclosure incident available here.

Cyber Crimes & Incidents

Russia's Sandworm Hacking Unit Targets Ukrainian Telecom Providers

Summary

- Sandworm, a Russian state hacking group, has targeted at least 11 internet and telecom providers in Ukraine since May.

Analysis & Action

Sandworm's attack on Ukrainian internet and telecom providers has sparked numerous disruptions and potential data breaches. Ukraine's Computer Emergency Response Team (CERT-UA) was the first to respond and report these attacks.

Sandworm has used different malware, like Poemgate and Poseidon, in their recent attacks to steal credentials and control infected devices. They have also been using Whitecat to erase forensic evidence that leads back to them. Sandworm was believed to have stolen documents, schemes, contracts, and passwords using official social media accounts belonging to the targets. CERT-UA stated that Sandworm would disable active network and server equipment, including data storage systems, as a final phase of their attack.

It is recommended that members ensure they have enabled multi-factor authentication (MFA) as a second layer of protection if passwords get stolen. Members in and around

Ukraine should continue to prepare for cyberattacks against these internet and telecom providers, which have the potential to cause cascading impacts.

Watch Out: Attackers Are Hiding Malware in Browser Updates

Summary

- Fake browser updates deployed by threat actors target unsuspecting users with malware.

Analysis & Action

The trend of threat actors deploying malware through fake browser updates has been increasing in recent years and has not shown signs of stopping. Multiple industries have been affected by these attacks, such as the media and local sports associations.

Legitimate websites that have vulnerabilities in their software have been the prime targets of threat actors injecting their own malicious JavaScript code into the systems. When a victim clicks to update their browser, the code is injected into the victim's systems and proceeds to extract information about the victim's system to determine malware eligibility. If a system is determined to meet the criteria, they are referred to a fake update page which delivers malware to the victim.

Members are encouraged to take precautions with browser updates by observing the language used and behaviors exhibited by these sites and avoiding downloading anything from unverified sites. Members are also encouraged to avoid links and attachments from unrecognized sources.

Vulnerabilities & Exploits

Over 40,000 Admin Portal Accounts Use Admin as a Password

Summary

- According to security researchers, over 40,000 privileged enterprise portal accounts are using weak passwords.

Analysis & Action

Allegedly, over 40,000 administrator accounts in enterprise network portals are still using admin as their password. The large-scale use of this password was discovered in a study on over 1.8 million administrator credentials stolen by information-stealing malware.

Cybersecurity firm, Outpost24, conducted a study on credentials stolen using info-stealer malware logs from 2023. From this, the company was able to identify 20 commonly used weak passwords for privileged accounts, highlighting the need for greater password complexity at the administrator level.

Guessable passwords, such as admin, can lead to unauthorized network access and possible ransomware deployment. Members are advised to consistently change passwords and require some level of password complexity to avoid predictable password use. To view the top 20 weak passwords observed by Outpost24 in their info-stealer study, click here.

Trends & Reports

Chinese Government Limits What Biometrics and Data Can Be Used to Train Generative AI

Summary

- Chinese Communist Party (CCP) agencies have stated that the training data used to train Chinese generative AI models are compliant with information blocklists.

Analysis & Action

Two agencies within the CCP have released guidelines for auditing training data used in artificial intelligence models. Additionally, all biometric data being used should be used with consent from consumers.

The CCP AI oversight committee, the Cyberspace Administration, released a statement that no less than 5% of illegal and harmful information is allowed in the training data.

The body is also cracking down on the commercial use of AI-enabled facial recognition software, stating that users must consent to its use in commercial applications. This is a stark contrast to the government-sponsored automatic facial recognition cameras used for public safety in China.

As artificial intelligence technology from China spreads around the world, training data auditing that ensures proper storage of biometric data is necessary to avoid unwanted customer data breaches.

Privacy, Legal & Regulatory

- Nothing to Report

Health-ISAC Cyber Threat Level

On September 20, 2023, 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 concerns regarding malvertising, rogue USB drives, Async RAT, MFA Bypass, and persistent credential stuffing/spraying.

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 | References

D-Link
Bleeping Computer
The Record
biometricupdate
Dark Reading
The Hacker News
Kaspersky Lab
The Hacker News

Tags

TetrisPhantom, Sandworm, D-Link

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