WEEKLY CYBER SECURITY BRIEFING

Armoryze
Be More Secure

Protecting Europe's digital future: EU proposes $1.2 billion cybersecurity initiative

The European Commission has proposed the Cyber Solidarity Act to improve cybersecurity measures in the EU, allocating €1.1bn towards new initiatives. The act aims to create a safe digital environment for citizens, businesses, and essential services. It establishes EU capabilities to strengthen cooperation mechanisms and create a European Cyber Shield. The Shield will consist of national and cross-border entities that detect and share warnings about cyber threats, enabling authorities to respond more effectively. The act also establishes Security Operations Centres and a Cyber Emergency Mechanism to test the preparedness of critical entities.

The Cybersecurity Incident Review Mechanism will help the EU improve its resilience to cyberattacks. Approval from EU member states and the European Parliament is mandatory.

READ MORE

Cybersecurity Alert: NCR hit by ransomware attack

American software company NCR reported an issue with its Aloha restaurant point-of-sale system, which was later revealed to be a ransomware attack impacting cloud-based systems. Although the affected restaurants were still able to serve customers, certain features were not functioning properly. NCR has enlisted the assistance of third-party cybersecurity specialists and law enforcement authorities, and is working to restore services.

WEEKLY CYBER SECURITY BRIEFING

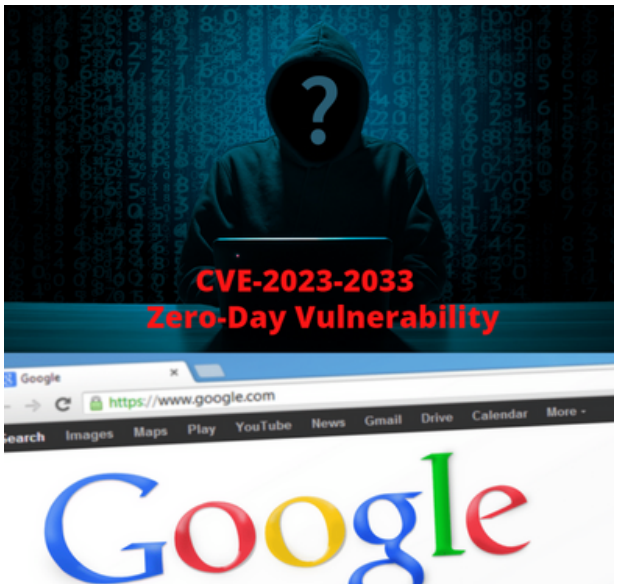
Armoryze
Be More Secure

while strengthening cybersecurity measures. The BlackCat ransomware group initially claimed responsibility for the attack, but the announcement was subsequently deleted, indicating possible negotiations for payment. To protect against ransomware attacks, it is recommended to keep software updated, use strong passwords, and enable multi-factor authentication. Armoryze offers Managed Detection and Response services to protect businesses from cyber threats.

READ MORE

Attention all google chrome users: A critical zero-day vulnerability (CVE-2023-2033) has been exploited - Take action now!

Google has released an emergency update to fix a zero-day vulnerability (CVE-2023-2033) that was actively exploited in the Chrome web browser. The vulnerability, a high-severity type confusion problem in the V8 JavaScript engine, can enable a remote attacker to carry out heap corruption through a specially crafted HTML page. A patch for this vulnerability is now available on Chrome 112.0.5615.121 for Windows, Mac, and Linux. It is recommended that all users upgrade their systems immediately to the latest version of Chrome to prevent any potential attacks.



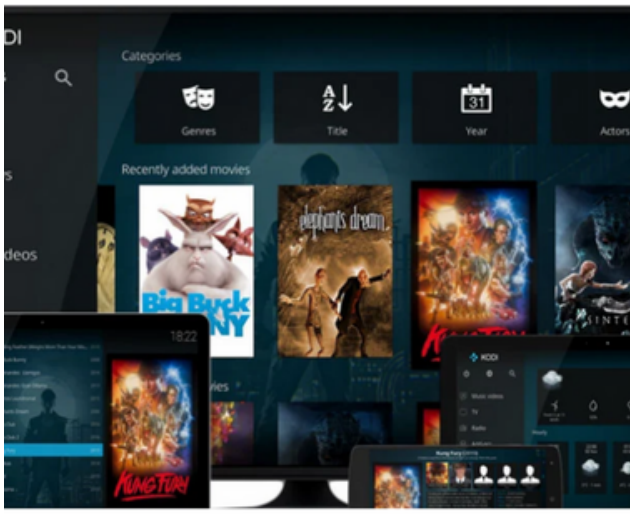
To further secure your business, implementing zero trust security solutions such as multi-factor authentication, endpoint security, and network segmentation is suggested.

READ MORE

WEEKLY CYBER SECURITY BRIEFING

Armoryze
Be More Secure

Kodi's confirm data breach: 400K users records and private messages comprised



Kodi, the open-source media player software provider, suffered a security breach resulting in the exposure of private messages and user information of 400,000 users. The attackers attempted to sell the information on a cybercrime marketplace. The breach was caused by a trusted admin team member's account being used to access the web-based MyBB admin console twice in February. Kodi is implementing additional security measures and has announced a global password reset as a precautionary measure.

Kodi users are advised to create unique and robust passwords for each account, enable two-factor authentication, and avoid suspicious emails or messages. For additional protection, consider Armoryze's managed detection and response service. Armoryze offers 24/7 threat monitoring and incident response services to detect and respond to security threats before they cause damage. Schedule a free consultation to learn more about how Armoryze can help secure your business.

READ MORE

WEEKLY CYBER SECURITY BRIEFING

Armoryze
Be More Secure

Joint Advisory Released by Security Agencies on APT28's Tactics.

A joint advisory from the National Security Agency, Cybersecurity and Infrastructure Security Agency, FBI and the U.K. National Cyber Security Centre has been released to alert organizations of the tactics used by APT28 to exploit and gain access to Cisco routers.

APT28 uses malware and exploits the vulnerability CVE-2017-6742 to perform reconnaissance of routers. The threat actor also uses default and weak Simple Network Management Protocol community strings to gain access to sensitive network data.

SNMP allows network administrators to remotely configure and track network devices, which can be exploited by threat actors. To prevent unauthorized access of routers, organizations should take mitigation measures such as patching devices, avoiding the use of SNMP, enforcing strong password policies and using logging tools to record commands executed on network devices.

The advisory also provides information on APT28, which is known as the Russian General Staff Main Intelligence Directorate (GRU) 85th Special Service Center military intelligence unit 26165, STRONTIUM, Fancy Bear, Pawn Storm, Sofacy and the Sednit Gang.

In conclusion, organizations should take these steps to protect themselves from APT28's tactics and secure their network infrastructure.

READ MORE