WEEKLY CYBER SECURITY BRIEFING

Armoryze
Be More Secure

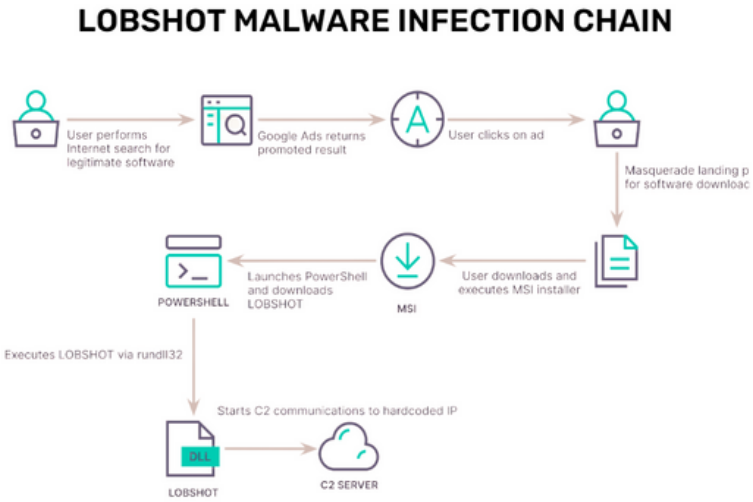
FRR - Popular routing protocol found to have new security flaws

Forescout Vedere Labs, a cybersecurity research team, has discovered three new security vulnerabilities in FRRouting version 8.4, an open-source implementation of BGP internet routing protocol suite used for Linux and Unix platforms. These vulnerabilities could lead to a denial-of-service (DoS) attack on vulnerable BGP peers, potentially rendering them unresponsive. The vulnerabilities include CVE-2022-40302, CVE-2022-40318, and CVE-2022-43681, and can be exploited by attackers to drop all BGP sessions and routing tables.

FRRouting is used by various vendors such as NVIDIA Cumulus, DENT, and SONiC, posing a supply chain risk.Forescout Vedere Labs has also created a Python-based open-source BGP Fuzzer tool to test the security of BGP suites used internally. For expert help identifying, prioritizing, and remediating vulnerabilities in your network, consider **Armoryze's risk-based vulnerability management services.**

READ MORE

LOBSHOT: The financial trojan hiding in google ads that can empty your bank accounts



Cybercriminals are distributing the LOBSHOT financial trojan via malvertising on legitimate websites using Google Ads. LOBSHOT evades detection using dynamic import resolution and performs an anti-emulation check. The malware targets 50 Chrome, Edge, and Firefox extensions related to cryptocurrency wallets and steals information using the hVNC module.

WEEKLY CYBER SECURITY BRIEFING

Armoryze
Be More Secure

The financially motivated threat actor, TA505, has been using LOBSHOT in attacks since at least 2022, with over 500 unique malware samples observed. Businesses should implement multi-factor authentication and network segmentation to reduce the risk of such attacks.

Armoryze offers managed detection and response services to help protect organizations from cyberattacks.

READ MORE

CISA issues security advisory on critical vulnerability affecting MR RTU remote terminal units

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has issued an advisory regarding a critical flaw affecting ME RTU remote terminal units, which has received the highest severity rating of 10.0 on the CVSS scoring system due to its low attack complexity. The vulnerability (CVE-2023-2131) allows for remote code execution and affects versions of INEA ME RTU firmware prior to version 3.36. CISA has also issued an alert regarding multiple security holes in Intel processors impacting Factory Automation products from Mitsubishi Electric, which could result in privilege escalation and denial-of-service conditions.

To mitigate these threats, critical infrastructure organizations are recommended to review the FCC's Covered List of communications equipment and adopt NIST's guidance to identify, assess, and mitigate supply chain risks. CISA's free Vulnerability Scanning service can also help pinpoint vulnerable and high-risk devices. To ensure comprehensive security measures,

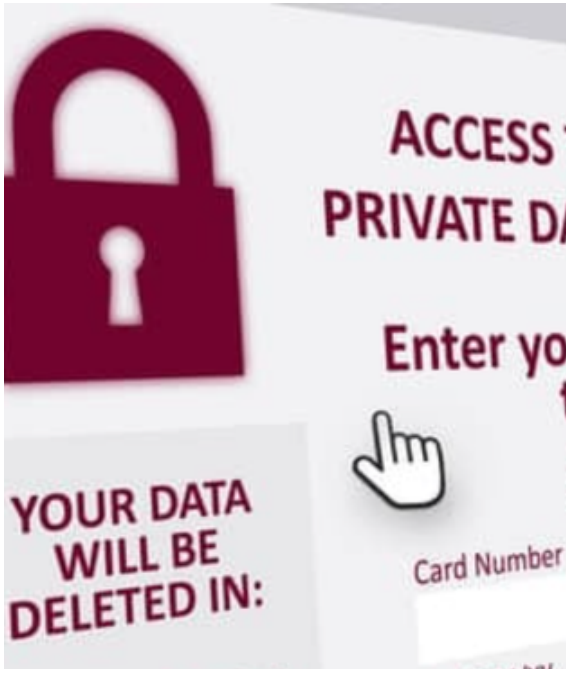
Armoryze's risk-based vulnerability management service can help identify and prioritize vulnerabilities based on their risk level, safeguarding your organization's valuable assets and reputation.

READ MORE

WEEKLY CYBER SECURITY BRIEFING

Armoryze
Be More Secure

Protecting Education: The importance of cybersecurity measures fro schools



In recent news, a ransomware attack on Hardenhuish School in Chippenham, Wiltshire, highlighted the vulnerability of the education sector to cyber threats. Due to limited IT resources, schools are often seen as soft targets for cybercriminals. Ransomware attacks can lead to school closures and business disruptions, ultimately affecting the education of children.

To combat these threats, schools must prioritize cybersecurity measures and invest in the necessary resources to reduce the risk of falling victim to a cyber-attack and ensure a safe and secure learning environment for their students.

Armoryze recommends implementing advanced security controls such as zero trust security and network segmentation to detect and resolve security issues quickly. It's important to refrain from giving in to ransom demands since paying the ransom does not guarantee the return of stolen data and only funds future attacks.

The recent audit by the National Cyber Security Centre (NCSC) found that 78% of UK schools had experienced at least one type of cyber-incident.

Armoryze offers comprehensive cybersecurity solutions tailored to the needs of educational institutions to help them assess their current security posture, identify vulnerabilities, and implement advanced security controls to keep their systems safe and secure.

READ MORE

WEEKLY CYBER SECURITY BRIEFING

Armoryze
Be More Secure

US Government takes down Try2Check, a major dark web credit card verification platform

In a significant win against cybercrime, US government partners with Austrian and German law enforcement to take down Try2Check, a platform used by cybercriminals to verify stolen credit card numbers. The platform processed $10 of millions of stolen credit card numbers annually, enabling the trade in stolen credit card information.

The operator, Denis Gennadievich Kulkov, has been indicted on multiple charges, demonstrating a commitment to disrupting cybercrime operations.

Kulkov created Try2Check in 2005, which became a primary tool for cybercriminals engaged in the illicit credit card trade. The platform enabled criminals to determine the percentage of stolen credit card numbers that remained active and victimized credit card issuers, holders, and a major US-based payment processing company. Kulkov made $18 million in bitcoin through the illegal operation of his websites, using the profits to buy luxury items such as a Ferrari. Businesses handling sensitive data must take measures to protect against cybercrime, including implementing security protocols, providing regular cybersecurity awareness training to employees, and performing security audits. Compliance with PCI DSS is essential to prevent cybercriminals from exploiting payment processing system vulnerabilities.

Armoryze offers **free consultations with their PCI experts** to assist businesses in achieving and maintaining full compliance, protecting customers' data from cyber threats.

+44-0208 427 1131

info@armoryze.co.uk