CYBER NEWS

12/2023 Vol. II

REDRABBIT SECURITY

About us

The internet is a dangerous place, and it's only becoming more dangerous. Red Rabbit Security provides managed security services to protect your data and your business from cyber threats. Whether you're looking for web security, email security, or network security, we have you covered.

Red Rabbit Security has one of the most experienced teams in the industry, with experts who are constantly staying up-to-date with the latest trends and techniques in cyber security. Our team is dedicated to proactively identifying and mitigating potential threats, ensuring that your business remains secure in an ever-evolving digital landscape. Trust Red Rabbit Security to safeguard your valuable assets and provide you with peace of mind.

Get a Free Cyber Security Assessment

www.redrabbitsec.com

IN THIS ISSUE

CYBER NEWS

12/2023 Vol. II

REDRABBIT
SECURITY

Cyber Headlines

Security Breach Warning - Threat Actors Exploit Amazon Web Services Security Token Service (AWS STS)

In a recent analysis, cybersecurity researchers Thomas Gardner and Cody Betsworth at Red Canary have uncovered a disturbing vulnerability within Amazon Web Services Security Token Service (AWS STS), revealing a potential avenue for threat actors to infiltrate cloud accounts and orchestrate subsequent attacks. AWS STS, designed to provide temporary, limited-privilege credentials for accessing AWS resources without the need for a dedicated AWS identity, is being exploited by threat actors who can impersonate user identities and roles in cloud environments. The attackers can pilfer long-term IAM tokens through various means, including malware infections, exposed credentials, and phishing emails. Once in possession of these tokens, threat actors can ascertain roles and associated privileges, creating a pathway for extensive compromise. By leveraging MFA-authenticated STS tokens, threat actors can generate multiple short-term tokens and execute post-exploitation actions such as data exfiltration, posing a severe risk to cloud security.

To safeguard against this alarming AWS token abuse, Red Canary recommends proactive logging of CloudTrail event data, vigilant detection of role-chaining events and MFA abuse, and the regular rotation of long-term IAM user access keys.
https://redcanary.com/blog/aws-sts/

IN THIS ISSUE

CYBER NEWS

12/2023 Vol. II

REDRABBIT SECURITY

Cyber Headlines

North Korean Andariel Hacks South Korean Defense, Laundering $356,000

Seoul police have uncovered a severe cybersecurity breach orchestrated by North Korean hacker group Andariel, implicating them in the theft of 1.2 terabytes of sensitive defense data, including details on advanced anti-aircraft weaponry, from South Korean defense companies. Operating through domestic servers, Andariel also managed to launder $356,000 in bitcoin ransom proceeds back to North Korea, posing a dual threat of espionage and financial crime. The group, believed to be a subset of the infamous Lazarus Group, is known for its global cyber-espionage activities, utilizing custom-built malware tools to target businesses and government entities.

This revelation underscores the pressing need for international collaboration in addressing the growing menace of cyber threats originating from nation-state actors. The global community must unite to counter the increasingly sophisticated tactics employed by groups like Andariel, emphasizing the importance of proactive cybersecurity measures to safeguard critical infrastructure and sensitive information from malicious exploitation. Stay vigilant, implement robust security protocols, and collaborate to ensure a collective defense against evolving cyber threats.

https://cybernews.com/news/andariel-north-korean-hackers-steal-laser-weapon-tech/

IN THIS ISSUE

1. Cyber Headlines - Latest cyber news from around the globe.

2. Did You Know - Short and informative cyber security facts and stats.

3. Threat Intelligence - Latest in cyber threat intelligence from across all industries.

4. Newly Released Patches and Updates - Vendor agnostic patches and updates information.

5. Upcoming Webinars, Conferences, and Events - The latest information from around the globe for learning and networking opportunities.

6. Featured Article of the Week - Articles from around the world related to cyber security.

CYBER NEWS

12/2023 Vol. II

REDRABBIT SECURITY

Cyber Headlines

Hershey Company Succumbs to Phishing Attack

In a concerning disclosure, The Hershey Company acknowledges a cyber incident resulting from a phishing campaign, compromising the financial information of 2,214 individuals. Initiated through phishing emails in early September, unauthorized access exposed a plethora of sensitive data, including names, health details, insurance information, digital signatures, dates of birth, addresses, driver's license numbers, and credit card information. While Hershey claims no evidence of data misuse, affected individuals are offered a mitigating measure with two years of Experian IdentityWorks.

The confectionery giant has taken swift action, fortifying its security measures and collaborating with third-party entities for comprehensive remediation. This incident aligns with a disturbing trend of high-profile cyber intrusions during the same period, illustrating the persistent and escalating threat landscape as the year concludes. Organizations are urged to remain vigilant against evolving cyber threats and fortify defenses to mitigate the risk of falling victim to similar phishing attacks.

Read more about the news here :

https://www.theregister.com/2023/12/04/hershey_phishes_data_breach/?&web_view=true

IN THIS ISSUE

CYBER NEWS

12/2023 Vol. II

REDRABBIT SECURITY

Did You Know

- **Did you know?** Over 30% of internet traffic is attributed to bad bots, posing a significant threat to online businesses with potential for fraud and cyberattacks, according to research by online fraud protection company DataDome?

- **Did you know?**DataDome's report reveals that 68% of US websites lack sufficient protection against simple bot attacks, emphasizing the vulnerability of US businesses, particularly e-commerce and classified ad sites, with 72.3% and 65.2% respectively failing bot tests ahead of the holiday shopping season.

- **Did you know?** That a new post-exploitation tampering technique can deceive iPhone users by creating a fake Lockdown Mode, making them believe their device is secure when it's compromised, allowing malware to operate undetected in the background?

- **Did you know?** That some states, including Florida and North Carolina, have enacted laws prohibiting entities receiving public funds from negotiating with and paying ransom to threat actors, potentially impacting public entities and private companies alike?

IN THIS ISSUE

www.redrabbitsec.com

CYBER NEWS

12/2023 Vol. II

REDRABBIT
SECURITY

Threat Intelligence

Rising Menace of Malicious Browser Extensions Unveiled

A recent report by LayerX has illuminated the escalating threat landscape posed by malicious browser extensions, shedding light on the three main categories of these threats. The report identifies initially malicious extensions purposefully crafted for harm, compromised extensions originating from legitimate ones, and risky extensions with excessive permissions. Through various installation methods such as admin, normal, developer, and sideload installations, these extensions infiltrate users' browsers, exposing critical security considerations. Of particular concern is the widespread adoption of extensions downloaded from official browser stores, accounting for 81% of installations, raising questions about the security implications of users' choices. The report emphasizes indicators of potentially malicious extensions, including missing developer contact information, outdated versions, absence of privacy policies, and unusual installation methods.

Pay attention to key factors such as user ratings, the presence of a support site, official websites, and uncommon installation types. With the focus on user-centric security practices, the report provides actionable insights to identify and mitigate the risks associated with browser extensions._
https://go.layerxsecurity.com/report-unveiling-the-threat-of-malicious-browser-extensions/?utm_source=thn_

IN THIS ISSUE

CYBER NEWS

12/2023 Vol. II

REDRABBIT SECURITY

Threat Intelligence

Critical Vulnerabilities Unveiled in Sierra Wireless AirLink Routers

A critical security concern has emerged as Forescout Vedere Labs reports the discovery of 21 security flaws, collectively known as Sierra:21, in Sierra Wireless AirLink cellular routers and associated open-source components like TinyXML and OpenNDS. These vulnerabilities expose over 86,000 devices across sectors crucial to national infrastructure, including energy, healthcare, retail, and emergency services. With one critical, nine high-severity, and 11 medium-severity vulnerabilities, attackers could exploit these flaws for remote code execution, credential theft, and unauthorized access, posing a substantial threat to critical networks.

The industrial cybersecurity company urges immediate action, emphasizing the potential for network disruption, espionage, and malware deployment by threat actors leveraging these vulnerabilities. Fixes are available, but timely implementation is crucial to safeguard against potential cyber threats exploiting these vulnerabilities across vital sectors.

https://www.securityweek.com/21-vulnerabilities-in-sierra-wireless-routers-could-expose-critical-infrastructure-to-attacks/

IN THIS ISSUE

1. Cyber Headlines - Latest cyber news from around the globe.

2. Did You Know - Short and informative cyber security facts and stats.

3. Threat Intelligence - Latest in cyber threat intelligence from across all industries.

4. Newly Released Patches and Updates - Vendor agnostic patches and updates information.

5. Upcoming Webinars, Conferences, and Events - The latest information from around the globe for learning and networking opportunities.

6. Featured Article of the Week - Articles from around the world related to cyber security.

CYBER NEWS

12/2023 Vol. II

REDRABBIT SECURITY

Released Patches and Updates

Atlassian Addresses Critical Flaws in Multiple Products

Atlassian has swiftly released software fixes to address four critical vulnerabilities in its products, posing potential risks of remote code execution if exploited. These flaws include a deserialization vulnerability in the SnakeYAML library (CVE-2022-1471), a template injection flaw in Confluence (CVE-2023-22522), a remote code execution vulnerability in Assets Discovery for Jira Service Management (CVE-2023-22523), and a similar flaw in the Atlassian Companion app for macOS (CVE-2023-22524).

Atlassian emphasizes the urgency of updating affected installations promptly, following a recent revelation of an actively exploited critical security flaw in Apache ActiveMQ affecting its Bamboo Data Center and Server products. Users are strongly advised to apply the available patches to mitigate potential cyber threats exploiting these vulnerabilities in Atlassian's widely-used software suite.

IN THIS ISSUE

CYBER NEWS

12/2023 Vol. II

REDRABBIT SECURITY

Released Patches and Updates

Kali Linux 2023.4 Released: New Tools and GNOME 45 Desktop

Kali Linux, the go-to Linux distribution for ethical hackers and cybersecurity professionals, has launched its final version for 2023, featuring fifteen new tools and the GNOME 45 desktop environment. While core operating system additions are limited, the update includes critical tools such as cabby, Havoc, and Portspoof. Kali Linux 2023.4 also introduces GNOME 45, offering enhanced features like full-height sidebars, improved search speed in the Nautilus file manager, and updated themes.

The Kali Team emphasizes the importance of prompt updates for users, presenting various deployment options, including Amazon AWS, Microsoft Azure, Hyper-V, and Raspberry Pi 5. Existing users can easily upgrade using simple commands provided by Kali Linux.

IN THIS ISSUE

CYBER NEWS

12/2023 Vol. II

REDRABBIT SECURITY

Webinars, Conference, and Events

FutureCon Houston Cybersecurity Conference

FutureCon Events brings high-level Cyber Security Training discovering cutting-edge security approaches, managing risk in the ever-changing threat of the cybersecurity workforce. Educating C-suite executives and CISOs (chief information security officers) on the global cybercrime epidemic, and how to build Cyber Resilient organizations. “Cybersecurity is no longer just an IT problem” Gain the latest knowledge you need to enable applications while keeping your computing environment secure from advanced Cyber Threats. Demo the newest technology, and interact with the world’s security leaders and gain other pressing topics of interest to the information security community. The FutureCon community will keep you updated on the future of the Cyberworld and allow you to interact with your peers and the world’s security leaders.

Key Details:

December 13, 2023
Event Duration: 1 Day
Houston, Texas
Cost: $200

https://futureconevents.com/events/houston-tx-2023/

IN THIS ISSUE

1. Cyber Headlines - Latest cyber news from around the globe.

2. Did You Know - Short and informative cyber security facts and stats.

3. Threat Intelligence - Latest in cyber threat intelligence from across all industries.

4. Newly Released Patches and Updates - Vendor agnostic patches and updates information.

5. Upcoming Webinars, Conferences, and Events - The latest information from around the globe for learning and networking opportunities.

6. Featured Article of the Week - Articles from around the world related to cyber security.

CYBER NEWS

12/2023 Vol. II

REDRABBIT
SECURITY

Featured Article of the Week

Microsoft Warns of CACTUS Ransomware Attacks Using DanaBot as Initial Access Vector

Microsoft has issued a warning about a fresh wave of CACTUS ransomware attacks utilizing malvertising schemes to deploy DanaBot as an initial access vector. The DanaBot infections facilitated "hands-on-keyboard activity by ransomware operator Storm-0216 (Twisted Spider, UNC2198)," ultimately leading to the deployment of the CACTUS ransomware.

DanaBot is a versatile tool, akin to Emotet and TrickBot, functioning as both a stealer and an entry point for subsequent payloads. UNC2198, known for infecting endpoints with IcedID, has previously deployed ransomware families like Maze and Egregor. This campaign, observed in November, suggests a shift to DanaBot following the coordinated takedown of QakBot's infrastructure in August 2023.

Read more about the attack here: https://thehackernews.com/2023/12/microsoft-warns-of-malvertising-scheme.html

IN THIS ISSUE

1. Cyber Headlines - Latest cyber news from around the globe.

2. Did You Know - Short and informative cyber security facts and stats.

3. Threat Intelligence - Latest in cyber threat intelligence from across all industries.

4. Newly Released Patches and Updates - Vendor agnostic patches and updates information.

5. Upcoming Webinars, Conferences, and Events - The latest information from around the globe for learning and networking opportunities.

6. Featured Article of the Week - Articles from around the world related to cyber security.