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

IN THIS ISSUE

REDRABBIT SECURITY

Cyber Headlines

Cyberattack on Kronos Research Results in $26 Million Cryptocurrency Theft

Cryptocurrency trading and investment firm Kronos Research reported a cyberattack that led to the unauthorized access of its application programming interface (API) keys, resulting in the theft of $26 million worth of cryptocurrency. The company promptly halted trading, launched an investigation, and assured affected parties that all losses would be internally covered, with no impact on partners.

Despite the significant financial setback, Kronos expressed gratitude for the support received from exchanges and partners. The stolen funds, identified as 12,800 ETH, were distributed to six different wallets, according to blockchain researchers. Cybersecurity experts highlighted the exploitation of API keys, emphasizing that hackers can manipulate prices and force unauthorized transactions.

CertiK cybersecurity experts pointed out that more than half of crypto theft in 2023 involved compromises of private keys. Jason Kent, a cybersecurity expert, criticized Kronos for allowing the attacker to have six accounts, describing it as a failure to defend against modern attacks. Read more here: https://therecord.media/crypto-firm-kronos-research-26-million-stolen-cyberattack?&web_view=true

cont.

IN THIS ISSUE

REDRABBIT SECURITY

Cyber Headlines

Boeing Targeted in Cyberattack; LockBit 3.0 Exploits Citrix Software Vulnerability

In a significant cybersecurity breach, Boeing faces the aftermath of a targeted attack by the LockBit 3.0 ransomware group, leveraging the Citrix Bleed vulnerability. Despite Citrix's efforts to remedy the flaw, LockBit successfully exploited it, leading to unauthorized access and data compromise. LockBit, claiming responsibility, demanded a ransom from Boeing, ultimately resulting in the release of approximately 50GB of sensitive data when negotiations broke down. Shockingly, LockBit is reported to have received a staggering $90 million in ransom payments from various U.S. organizations between 2020 and mid-2023.

Prompted by the severity of the situation, the Cybersecurity, and Infrastructure Security Agency (CISA) issued a cybersecurity advisory in collaboration with the FBI and the Australian Cyber Security Center. The advisory urges immediate patch installation for approximately 300 affected organizations to mitigate further risks associated with the Citrix vulnerability. LockBit's extensive cyber campaign extends beyond Boeing, affecting major entities such as the Industrial & Commercial Bank of China and the UK's Royal Mail, highlighting the escalating threat landscape and the need for robust cybersecurity measures industry wide.

https://www.csoonline.com/article/1249034/flaw-in-citrix-software-led-to-the-recent-cyberattack-on-boeing-report.html

IN THIS ISSUE

REDRABBIT SECURITY

Did You Know

➢ **Did you know?** Generative AI, such as WormGPT and FraudGPT, is empowering threat groups with the ability to craft sophisticated and evasive phishing emails, posing an increased risk to retailers during the busy holiday season. LockBit stands out as a prominent ransomware threat, comprising one-third of attacks targeting the retail sector, according to Trustwave.

➢ **Did you know?** With the surge in e-commerce traffic, retailers face heightened risks from cyber threats, utilizing social engineering and advanced AI. About 19% of retailers have fallen victim to cyberattacks, reflecting the growing concerns within the industry during the crucial holiday season, according to the 2023 Travelers Risk Index.

➢ **Did you know?** Despite the escalating need for robust cybersecurity measures, a mere 9% of IT budgets are allocated to security, leaving organizations vulnerable in the face of evolving threats, according to insights from Vanta.

➢ **Did you know?** As businesses grapple with limited resources and increased risk, 67% acknowledge the imperative to enhance security and compliance measures, with 24% rating their strategies as reactive. Automation and AI adoption emerge as critical strategies, with 83% planning to increase their use to streamline tasks, saving at least two hours per week.

IN THIS ISSUE

REDRABBIT SECURITY

Threat Intelligence

New MacOS Threat - ClearFake Delivers AMOS Stealer via Fake Browser Updates

A concerning development reveals that the popular MacOS stealer, Atomic Stealer (AMOS), is now being distributed to Mac users through a fake browser update chain known as 'ClearFake.' This marks a shift in social engineering campaigns, traditionally focused on Windows, now extending to MacOS. ClearFake, discovered in August, utilizes compromised websites to distribute fake browser updates and has evolved with smart contracts for a sophisticated redirect mechanism.

Security researcher Ankit Anubhav observed ClearFake targeting Mac users on November 17. The malicious payload, disguised as Safari or Chrome updates, prompts victims for administrative passwords and executes commands for password and file theft. Mac users are urged to exercise caution, and web protection tools are recommended to thwart this evolving threat landscape.

Read the detailed analysis here:
https://www.malwarebytes.com/blog/threat-intelligence/2023/11/atomic-stealer-distributed-to-mac-users-via-fake-browser-updates?&web_view=true

cont.

IN THIS ISSUE

REDRABBIT SECURITY

Threat Intelligence

New Phobos Ransomware Variant Targets VX-Underground

A new variant of the Phobos ransomware has emerged, marking an interesting turn as it attempts to frame the VX-Underground malware-sharing collective. Phobos, operational since 2018, operates as a ransomware-as-a-service, with a group of threat actors managing its development and holding the master decryption key, while other affiliates execute network breaches and device encryption. Despite not gaining notoriety for massive attacks, Phobos still represents a considerable threat, contributing to 4% of all submissions to the ID Ransomware service in 2023.

This latest Phobos variant takes an unusual approach by appending ".VXUG" to encrypted files, implicating VX-Underground in the process. The ransom note humorously pokes fun at VX, suggesting victims contact "staff@vx-underground.org" for decryption. Such tactics echo previous instances where threat actors incorporated taunts directed at security researchers within ransomware campaigns, underscoring the complex dynamics between cybercriminals and the information security community.

cont.

IN THIS ISSUE

CYBER NEWS

11/2023 Vol. III

REDRABBIT SECURITY

Threat Intelligence

Active Exploitation of Sophos Web Appliance Vulnerability (CVE-2023-1671)

CISA has identified ongoing exploitation of a critical pre-auth command injection vulnerability (CVE-2023-1671) in Sophos Web Appliance. The flaw, patched by Sophos in April 2023, allows attackers to execute arbitrary code. The web gateway appliance, functioning as a proxy and malware scanner, was flagged for reaching end of life on July 20, 2023. Despite a public PoC exploit being available since April, attackers seem to have recently capitalized on the vulnerability.

This incident underscores the persistent risk of exploitation of known vulnerabilities, especially in instances where patching practices may be inconsistent within organizations. CISA's Known Exploited Vulnerabilities catalog also added CVE-2020-2551, emphasizing the recurrent use of older vulnerabilities by threat actors.

IN THIS ISSUE

REDRABBIT SECURITY

Released Patches and Updates

Johnson Controls Addresses Critical Flaw in Industrial Refrigeration Products

Johnson Controls has issued patches for a critical vulnerability (CVE-2023-4804) discovered by an external researcher in its industrial refrigeration products, including Frick Quantum HD Unity Compressor. The flaw could permit unauthorized access to accidentally exposed debug features, potentially allowing an attacker to gain full administrative control over a Quantum HD system. Impacted products are used globally, particularly in the food and beverage industry.

Johnson Controls, acknowledging the wider impact than initially anticipated, released updates for affected control panels, scoring the vulnerability at a critical CVSS score of 10. The researcher praised Johnson Controls' responsible disclosure process but noted a six-month patch rollout delay due to the broader impact and complexity of fixing multiple platforms simultaneously. The incident highlights supply chain issues resulting from mergers and acquisitions.

Read more here: https://www.securityweek.com/johnson-controls-patches-critical-vulnerability-in-industrial-refrigeration-products/?web_view=true

IN THIS ISSUE

REDRABBIT SECURITY

Webinars, Conference, and Events

Event Spotlight: BLACK HAT EUROPE 2023

Explore the forefront of Information Security at Black Hat Europe, where leading professionals and researchers gather for a comprehensive four-day event. Delve into deeply technical hands-on Trainings for the initial two or four days, followed by the latest research insights and vulnerability disclosures in the Briefings. Join this event to stay abreast of the industry's cutting-edge developments and trends.

Key Details:

December 4, 2023
Event Duration: 4 Days
London, England
Cost: £699

More details:https://www.blackhat.com/eu-23/

cont.

IN THIS ISSUE

REDRABBIT SECURITY

Webinars, Conference, and Events

Event Spotlight: HackSydney [HCKSYD] 2023

HackSydney aspires to be the most inclusive, diverse, and educational APACJ InfoSec Conferences. HackSydney aims to be one of the most inclusive, varied, and educational infosec conferences in the area. HackSydney aims to bring together experts from all facets of the information security industry and will be held in Sydney, the largest city in Australia. The conference will cover every aspect of security, from offensive to defensive, as well as everything in between. Don't miss this opportunity to be part of a dynamic event that transcends boundaries and fosters learning.

Key Information

November 23, 2023
Event Duration: 2 Days
Sydney Australia

More details: https://www.hack.sydney/

IN THIS ISSUE

CYBER NEWS

11/2023 Vol. III

REDRABBIT SECURITY

Featured Article of the Week

Featured Article for the Week

Security Concerns Amidst Generative AI Adoption

Organizations are succumbing to the allure of generative AI (GenAI) tools like ChatGPT, with 95% already using them despite 89% recognizing the associated security risks, reveals a survey by Zscaler. Concerningly, 23% aren't monitoring usage, and 33% lack additional security measures.

While IT teams predominantly drive adoption (59%), only 5% attribute it to employee demand. Zscaler urges proactive steps, including implementing a holistic zero-trust architecture and conducting thorough security risk assessments. With 51% anticipating increased GenAI interest, organizations must swiftly bridge the gap between adoption and robust security measures.

Read more here:
https://www.helpnetsecurity.com/2023/11/20/genai-usage-pressure-security/?web_view=true

IN THIS ISSUE