CYBER NEWS

11/2023 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

IN THIS ISSUE

CYBER NEWS

11/2023 Vol. II

REDRABBIT SECURITY

Cyber Headlines

Truepill Data Breach Exposes 2.36 Million Patients: Virtual Pharmacy Faces Class Action Lawsuits

Hayward-based Truepill, a virtual pharmacy, discloses a cyberattack compromising patient data, prompting six federal class action lawsuits. Intruders accessed pharmacy management files, exposing patient names, medications, and more. Truepill, operating as Postmeds, took swift action, but the breach occurred over three days in August. No Social Security numbers were compromised. Lawsuits allege negligence and HIPAA violations, seeking damages and enhanced data security.

This incident underscores the intensifying threat landscape for online pharmacies, emphasizing the critical need for robust cybersecurity protocols in the healthcare sector. The lawsuits collectively shine a spotlight on the industry-wide vulnerability, compelling healthcare entities to fortify defenses against evolving cyber threats, safeguard patient data, and ensure the resilience of digital healthcare ecosystems.

For further details and in-depth information on these events, you can find the article in https://www.bankinfosecurity.com/truepill-mail-order-pharmacy-hack-affects-nearly-24-million-a-23590?&web_view=true

cont.

IN THIS ISSUE

CYBER NEWS

11/2023 Vol. II

REDRABBIT SECURITY

Cyber Headlines

Hackers Drain Over $100 Million from Poloniex Crypto Exchange

On Friday, cryptocurrency trading platform Poloniex fell victim to a massive heist, with hackers making off with over $100 million in Bitcoin and Ethereum. Poloniex confirmed the breach on social media, assuring an ongoing investigation and a commitment to fully reimburse affected users. In a controversial move, the platform proposed offering a 5% bounty to the hacker for the safe return of the funds, urging a response within seven days before involving law enforcement.

Poloniex, known for its lax customer controls, was founded in 2014, acquired by Circle in 2018, and later sold to crypto entrepreneur Justin Sun in 2020. Sun asserted that the losses were manageable, with frozen assets covering part of the breach. Security firms estimated varying amounts stolen, ranging from $114 million to $130 million. The incident follows a period of relative calm in crypto platform attacks, with previous notable breaches affecting Exactly Protocol, Harbor Protocol, and a $61 million heist exploiting Vyper, a popular Web3 programming language.

For further details and in-depth information on these events, you can find the article in https://therecord.media/poloniex-cryptocurrency-platform-millions-stolen?&web_view=true

IN THIS ISSUE

CYBER NEWS

11/2023 Vol. II

REDRABBIT SECURITY

Did You Know

➢ **Did you know?** The success of a cybersecurity strategy is closely tied to staff size and compensation. According to a survey by IANS and Artico, retaining top cybersecurity talent requires keeping compensation at the high end, with the top 25% of earners perceived as top performers in their roles and averaging around $523,000 per year in cash compensation.

➢ **Did you know?** Redline Stealer is the preferred choice among cybercriminals for information-stealing malware, targeting valuable data such as cryptocurrency wallets and remote access credentials.

➢ **Did you know?** Browser data, including credentials for popular websites like Google, Live.com, Facebook, and others, remains a lucrative target for cybercriminals deploying info-stealing malware, underscoring the ongoing threat to online users' sensitive information.

➢ **Did you know?** The UK's National Cyber Security Centre (NCSC) warns of an escalating threat to critical infrastructure from emboldened state-backed actors, pointing fingers at Russia for potential destructive attacks and highlighting ransomware groups sheltered by the Kremlin responsible for high-profile cyber-attacks against the UK.

IN THIS ISSUE

REDRABBIT SECURITY

Threat Intelligence

Critical Unpatched Vulnerability Exposes VMware Cloud Director to Authentication Bypass

VMware has revealed a critical authentication bypass vulnerability affecting Cloud Director appliance deployments, particularly those upgraded from older releases to VCD Appliance 10.5. The flaw enables unauthenticated attackers to exploit the bug remotely on ports 22 and 5480 without user interaction. Notably, this doesn't impact fresh installs or other appliances.

While VMware lacks a patch, it offers a workaround involving a custom script to mitigate the issue without service disruptions. The absence of a fix heightens the urgency for admins to implement the provided workaround. This revelation underscores the persistent threat landscape, necessitating vigilance and rapid response in the face of emerging vulnerabilities, especially in widely-used virtualization solutions like VMware

Read the comprehensive analysis here: https://www.bleepingcomputer.com/news/security/vmware-discloses-critical-vcd-appliance-auth-bypass-with-no-patch/?&web_view=true

cont.

IN THIS ISSUE

CYBER NEWS

11/2023 Vol. II

REDRABBIT SECURITY

Threat Intelligence

Cryptocurrency Wallets at Risk: Millions Affected by Critical Open Source Vulnerability

New research from Unciphered reveals a critical open source software vulnerability impacting millions of cryptocurrency wallets created between 2011 and 2015. The vulnerability, named 'Randstorm,' stems from programming mistakes in the BitcoinJS library and affects the random numbers generated to secure wallets.

Unciphered, which spent 22 months investigating and coordinating disclosure, warns that attackers could exploit the flaw to gain access to wallet keys. The company notified various cryptocurrency wallet developers active between 2011 and 2015 and provided a workaround for affected versions. While no CVE exists for the flaw, it underscores broader concerns about open source software security and the potential risk to billions of dollars in cryptocurrency assets.

Delve into the details here:
https://www.techtarget.com/searchsecurity/news/366559456/Cryptocurrency-wallets-might-be-vulnerable-to-Randstorm-flaw?&web_view=true

IN THIS ISSUE

REDRABBIT SECURITY

Released Patches and Updates

Microsoft Addresses 63 Vulnerabilities in November Patch Release and Urges Immediate Action

Microsoft has released a comprehensive set of fixes in its November 2023 patch update, targeting 63 security vulnerabilities. Among them, three are actively exploited in the wild. The breakdown includes three critical, 56 important, and four moderate flaws, with two already publicly known.

Notably, Microsoft highlights five zero-days, including CVE-2023-36025, allowing the bypass of Windows SmartScreen security checks, and CVE-2023-36033/CVE-2023-36036, both elevating privileges to SYSTEM level. Users are cautioned against clicking on crafted internet shortcuts, a potential vector for compromise.

Urgency is underscored by the U.S. Cybersecurity and Infrastructure Security Agency (CISA) adding these issues to its Known Exploited Vulnerabilities catalog and urging federal agencies to apply fixes by December 5, 2023. This emphasizes the critical need for immediate action to secure systems against potential exploitation.

For more information, check out the Microsoft release notes here: https://msrc.microsoft.com/update-guide/releaseNote/2023-Nov

IN THIS ISSUE

REDRABBIT SECURITY

Webinars, Conference, and Events

Event Spotlight: HackFest Summit 2023

Immerse yourself in the captivating world of cybersecurity at this year's HackFest Hollywood Summit. Join global security practitioners in Tinseltown for two days filled with enlightening keynote presentations, interactive workshops, thrilling CTF competitions, and Hollywood-themed festivities.

Key Details:

November 16, 2023
Event Duration: 2 Days
California, United States
Cost: $425

More details: https://www.sans.org/cyber-security-training-events/hackfest-summit-2023/

cont.

IN THIS ISSUE

CYBER NEWS

11/2023 Vol. II

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. II

REDRABBIT SECURITY

Featured Article of the Week

Featured Article for the Week

New York Governor Proposes Stricter Cybersecurity Measures for Hospitals

New York Governor Kathy Hochul aims to bolster cybersecurity in the healthcare sector following recent cyberattacks. The proposed rules mandate hospitals to establish cybersecurity programs, appoint chief information security officers, and conduct regular tests for patient care continuity during system restoration.

With a $500 million budget for technology upgrades, the regulations also address secure software practices, multifactor authentication, and other cybersecurity measures. The move underscores Hochul's commitment to fortifying the state's healthcare infrastructure against evolving cyber threats.

Check out the details here: https://therecord.media/new-york-state-hospital-cybersecurity-regulations-proposed?&web_view=true

IN THIS ISSUE