CYBER NEWS

1/2024 Vol. I

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

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

1/2024 Vol. I

REDRABBIT SECURITY

Cyber Headlines

New NoaBot Threat: Linux Servers at Risk from Evolving SSH Brute-Force Attack

A new botnet named NoaBot has emerged, targeting vulnerable Linux servers through SSH brute-force attacks. Utilizing a modified Mirai worm, the botnet evolved to employ P2PInfect, exploiting Redis vulnerabilities. NoaBot's unique SSH scanner uses a distinctive "hi" message, making it detectable. The cryptomining component deploys XMRig with encrypted configurations, possibly running a private mining pool. Authors also utilize a custom P2PInfect variant, showcasing tech-savviness. Security measures, such as restricting SSH access and adopting key-based authentication, are crucial for defense. Akamai researchers provide indicators of compromise for identification. Stay vigilant and secure your servers against this evolving threat.

Read more about the threat here: https://www.csoonline.com/article/1289758/mirai-based-noabot-botnet-spreads-via-ssh-and-deploys-cryptominer.html

IN THIS ISSUE

CYBER NEWS

1/2024 Vol. I

Cyber Headlines

IntelBroker Claims Responsibility for Major U.S. Department of Transportation Data Breach

A threat actor known as IntelBroker has taken credit for a significant data breach targeting the U.S. Department of Transportation (DOT). The breach, allegedly involving the exfiltration of 5.8 million flight logs from 2015, raises concerns about national security and air travel safety. Despite the claim, the DOT's official website remains fully functional, prompting skepticism about the breach's authenticity. The incident adds to a series of cyberattacks on U.S. government entities, emphasizing the need for heightened cybersecurity measures across departments and affiliated organizations.

The recurring nature of these attacks points to a concerted effort by threat actors to exploit vulnerabilities within governmental institutions. As the investigation unfolds, the cybersecurity community awaits official statements from the DOT and related authorities to ascertain the full extent of the breach and the measures being taken to mitigate its consequences.

Read more about the breach here:
https://thecyberexpress.com/united-states-department-of-transportation/?&web_view=true

IN THIS ISSUE

CYBER NEWS

1/2024 Vol. I

Cyber Headlines

Massive Data Breach Exposes Private Information of Millions of Brazilians

Private data belonging to hundreds of millions of Brazilians was recently discovered in a publicly accessible Elasticsearch instance, as reported by Cybernews. The exposed information, including full names, dates of birth, gender, and Cadastro de Pessoas Físicas (CPF) numbers—an 11-digit tax identification unique to Brazil—was found on a cloud server with no specific attribution to any company or organization. The leak, totaling over 223 million records, potentially impacts the entire Brazilian population. Although the data is no longer public, the breach poses serious risks, leaving individuals vulnerable to identity theft, fraud, and targeted cybercrimes, underlining the urgent need for enhanced data security measures.

The incident underscores a concerning trend of massive data leaks affecting various countries, heightening the risks of unauthorized access and financial losses for individuals. Cybernews previously reported similar incidents involving governmental entities' data being sold online, emphasizing the critical importance of robust cybersecurity practices to safeguard sensitive personal information.

https://cybernews.com/security/brazil-data-leak-cpf-card/

IN THIS ISSUE

CYBER NEWS

1/2024 Vol. I

RED RABBIT SECURITY

Did You Know

➢ **Did you know?** In 2023, Cloudflare observed a record-breaking surge in Distributed Denial of Service (DDoS) attacks, more than doubling year over year in the fourth quarter. The mass exploitation of the HTTP/2 Rapid Reset zero-day vulnerability during the third quarter contributed significantly to the unprecedented rise in these cyber threats.

➢ **Did you know?** The landscape of DDoS attacks is evolving, with attackers now requiring significantly fewer resources to launch massive assaults. In 2024, it takes only 5,000 to 20,000 virtual machines to execute attacks exceeding 100 million requests per second, a stark contrast to 2019 when launching a similar attack would have necessitated at least a million IoT bots.

➢ **Did you know?** In the first half of 2023, out of 45 billion analyzed emails, a staggering 36.4% were categorized as unwanted, with over 585 million identified as malicious. This highlights the pervasive nature of email-based threats, underlining the critical need for robust email security measures.

➢ **Did you know?** Bots and human fraud farms accounted for a remarkable 73% of all website and app traffic measured in the first half of 2023, demonstrating that nearly three-quarters of digital property traffic is malicious. This rise in automated attacks poses a significant challenge for organizations seeking to secure their online presence.

IN THIS ISSUE

CYBER NEWS

1/2024 Vol. I

REDRABBIT
SECURITY

Threat Intelligence

CISA Alerts on Active Exploitation: 6 Critical Vulnerabilities Impacting Apple, Apache, Adobe, D-Link, and Joomla

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) issues a warning on six actively exploited vulnerabilities affecting major platforms. Among these, CVE-2023-27524 in Apache Superset poses a high-severity threat, enabling remote code execution with potential data compromise. Additionally, Apple's CVE-2023-41990, exploited in real-world Operation Triangulation spyware attacks, emphasizes the urgency for iOS users to patch vulnerabilities promptly. Adobe ColdFusion faces two high-severity deserialization flaws, while D-Link and Joomla! also grapple with critical vulnerabilities.

CISA urges Federal Civilian Executive Branch agencies to implement fixes by January 29, 2024, stressing the need for swift action to secure networks against evolving cyber threats.

Read more about it here:
https://thehackernews.com/2024/01/cisa-flags-6-vulnerabilities-apple.html?&web_view=true

IN THIS ISSUE

CYBER NEWS

1/2024 Vol. I

REDRABBIT
SECURITY

Threat Intelligence

Urgent: Critical Flaw in WordPress AI Engine Plugin Threatens Security

The widely-used free version of the AI Engine plugin for WordPress, boasting over 50,000 active installations, is facing a critical security vulnerability as revealed by Patchstack. This flaw, residing in the plugin's rest_upload function, exposes a risk of remote code execution for any unauthenticated user. The absence of proper validation for file types and extensions enables the upload of potentially malicious PHP files. To counter this, the plugin's developers have swiftly released a patch in version 1.9.99, introducing permission checks and file type validation. Users are strongly advised to promptly update to at least version 1.9.99 to fortify their systems against potential exploitation, with CVE-2023-51409 designated to monitor the issue

Patchstack emphasizes vigilant scrutiny of processes involving $_FILES parameters, robust checks on filenames and extensions, and heightened attention to permission checks on custom REST API endpoints.

To know more about this critical flaws, read the original post here: https://www.infosecurity-magazine.com/news/flaw-ai-plugin-exposes-50000-wp/?&web_view=true_

IN THIS ISSUE

CYBER NEWS

1/2024 Vol. I

REDRABBIT SECURITY

Released Patches and Updates

Microsoft's January 2024 Patch Tuesday: Critical Fixes for Remote Code Execution Vulnerabilities and Intriguing Flaws Addressed

Microsoft's January 2024 Patch Tuesday addresses a total of 49 vulnerabilities, with 12 categorized as remote code execution (RCE) flaws. Among the critical issues is a Windows Kerberos Security Feature Bypass and a Hyper-V RCE vulnerability. Notably, a fascinating flaw patched this month involves an Office Remote Code Execution Vulnerability (CVE-2024-20677), allowing threat actors to execute code through maliciously crafted Office documents with embedded FBX 3D model files.

Microsoft responded by disabling the ability to insert FBX files in Word, Excel, PowerPoint, and Outlook for Windows and Mac. Additionally, a critical Windows Kerberos bug (CVE-2024-20674) was fixed, addressing a vulnerability that could enable attackers to bypass authentication through a machine-in-the-middle (MITM) attack or local network spoofing techniques.

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

1/2024 Vol. I

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

1/2024 Vol. I

REDRABBIT SECURITY

Webinars, Conference, and Events

SANS Classic 2024

Experience one of our frequently updated and proven courses that stand as the building blocks of the entire SANS curriculum. “After my second time through FOR508, there is still such a vast amount of knowledge and learning to be had. SANS does an awesome job of keeping the information current and relevant to today, and the labs and exercises are comprehensive and extremely helpful for practicing and reinforcing course concepts.” – Andrew C., US Military SANS Classic 2024 – Live Online Features Practical cyber security training taught by real-world practitioner’s Real-time support from GIAC-certified teacher assistants Dedicated chat channels for networking Hands-on labs in a virtual environment Courseware in electronic and printed books Most courses align with GIAC certifications Earn CPE credits towards a certification renewal

Key Details:

January 15, 2024
Event Duration: 6 Days
In Person
Cost: Depending on Training Taken

https://www.sans.org/cyber-security-training-events/classic-2024-live-online/

IN THIS ISSUE

CYBER NEWS

1/2024 Vol. I

REDRABBIT SECURITY

Featured Article of the Week

NoaBot Emerges: A Closer Look at the Advanced Mirai-Based Botnet Fueling Cryptocurrency Mining

A new Mirai-based botnet dubbed NoaBot has emerged, employed by threat actors in a crypto mining campaign since early 2023. NoaBot, with roots in the Mirai worm's source code, showcases advanced modifications, using an SSH scanner for dictionary attacks on servers. Its unique features include a self-spreader and an SSH key backdoor, enabling additional binary downloads and spreading to new victims. Despite Mirai's common detection, NoaBot's use of uClibc in compilation alters antivirus signatures, making it challenging to detect. The botnet's evasion tactics extend to crypto mining, employing a custom mining pool to conceal the wallet address, adding a layer of sophistication to its illicit activities.

Akamai's research identified 849 victim IP addresses globally, with a significant concentration in China, constituting almost 10% of all attacks on their honeypots in 2023. Notably, NoaBot's lateral movement relies on SSH credentials dictionary attacks, emphasizing the importance of securing SSH access by restricting it to trusted IPs and using strong, non-default passwords. As the botnet landscape evolves, organizations are urged to enhance their cybersecurity measures, recognizing the adaptability and persistence of threat actors behind campaigns like NoaBot. https://thehackernews.com/2024/01/noabot-latest-mirai-based-botnet.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.