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

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.

REDRABBIT SECURITY

Cyber Headlines

Identity Theft Alert: Massive Data Breach Hits NYC, Exposes 4 Million to Risk

New York Attorney General Letitia James has disclosed a staggering data breach at medical transcription company Perry Johnson & Associates, impacting nearly nine million patients. Approximately four million New York residents are believed to be among those affected, with major healthcare providers, Northwell Health and Crouse Health, falling victim to the breach.

The breach, discovered by Perry Johnson & Associates in May, revealed the compromise of sensitive information, including social security numbers and insurance details from medical files. Most affected individuals, predominantly in NYC and Syracuse, have been notified, and the Attorney General has urged them to remain vigilant against potential identity theft.

The Attorney General provides crucial steps for protection, highlighting the pressing need for enhanced cybersecurity measures in the healthcare sector.

Read more about the attack here:
https://www.nbcnewyork.com/news/local/at-least-4-million-new-yorkers-impacted-by-medical-companys-data-breach-what-to-know/4900676/
cont.

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.

REDRABBIT SECURITY

Cyber Headlines

Play Ransomware Strikes Again, Targeting 17 Companies Across US, UK, Netherlands, and Canada

In a chilling development, the notorious Play ransomware group has expanded its victim list, targeting 17 companies spanning the US, UK, Netherlands, and Canada. The cybercriminals, operating since 2022, have threatened data exposure if ransom demands aren't met by December 4. The victims include major entities across IT services, outsourcing, retail, real estate, shipping, engineering, consulting, and management services, amplifying the risk of identity theft for individuals associated with these companies.

As the Play ransomware group evolves its tactics, experts warn of paying ransoms, emphasizing the need for stringent preventive measures such as offline backups, network monitoring, and avoiding ransom payments to mitigate cybersecurity risks.

Security experts suspect the Play ransomware group's ties to Russia, while affected companies are advised to disconnect compromised devices, assess severity, reset passwords, and ensure secure backups for data restoration. This latest wave of attacks underscores the imperative for businesses to enhance cybersecurity measures.

https://thecyberexpress.com/play-ransomware-attack-us-uk-canada-netherland/?&web_view=true cont.

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. I

REDRABBIT SECURITY

Cyber Headlines

Major Cyber Espionage Campaign Targets NXP, Leading Semiconductor Company

A significant cyber espionage operation, attributed to the group "Chimera" with suspected ties to China, has been exposed for infiltrating NXP, a prominent Netherlands-based chipmaker. Lasting over two years from late 2017 to early 2020, the attack went unnoticed until the threat actors were discovered infiltrating a separate company network connected to compromised NXP systems. The breach, reportedly involving periodic access to employee mailboxes and network drives, raises concerns about potential compromises of chip designs and intellectual property critical to smartphones, smartcards, and electric vehicles.

Despite the severity of the intrusion, NXP refrained from alerting customers or shareholders promptly, with details only surfacing recently. The breach, revealed through a report published by security firm Fox-IT, underscores the sophistication of Chimera, utilizing cloud services for data exfiltration and demonstrating a high level of persistence. The incident prompts broader concerns about the security of supply chains, as NXP is a key supplier for a range of products, including iPhones, Apple Watches, and components for electric vehicles.
https://arstechnica.com/security/2023/11/hackers-spent-2-years-looting-secrets-of-chipmaker-nxp-before-being-detected/?&web_view=true

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. I

REDRABBIT SECURITY

Did You Know

➢ **Did you know?** Stolen credentials remain a primary access vector for cybercriminals, with 49% of breaches involving unauthorized access.

➢ **Did you know?** Identity-focused attacks on SMBs in Q3 2023 revealed notable trends, with 64% involving malicious forwarding or inbox rules, while 24% were associated with logons from unusual locations. These tactics, often part of Business Email Compromise (BEC) operations, underscore the importance of defensive visibility and the need for robust measures during the account takeover phase.

➢ **Did you know?** In the evolving landscape of cyber threats, "malware-free" attacks are on the rise, constituting 56% of incidents in Q3 2023. Cyber adversaries now favor sophisticated techniques such as multi-channel phishing campaigns, targeting mobile devices, and leveraging AI to enhance the credibility of phishing content.

➢ **Did you know?** Despite advancements in cybersecurity awareness, 17% of small and medium-sized businesses (SMBs) in the UK struggle to recognize signs of online fraud and scams, according to a quiz conducted by UK Finance.

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.

REDRABBIT SECURITY

Threat Intelligence

Critical Vulnerability Exposes Ray AI Compute Framework to Unauthorized Access

A critical vulnerability, tracked as CVE-2023-48023, poses a significant security risk for the Ray open source compute framework for AI, warns cybersecurity firm Bishop Fox. The flaw arises from Ray's failure to enforce authentication in its dashboard and client components, allowing remote attackers to submit or delete jobs without proper authentication. Exploiting this vulnerability could grant unauthorized access to all nodes in the Ray cluster, potentially compromising sensitive information and enabling the execution of arbitrary code. Bishop Fox highlights the framework's lack of authentication, leading to additional security vulnerabilities, including unauthenticated remote code execution via the job submission API and critical-severity issues such as server-side request forgery (SSRF) and insecure input validation.

Despite reporting some of these issues to Ray's maintainers, Bishop Fox notes that the vendor's stance considers unauthenticated remote code execution intentional and not a vulnerability, leaving certain security concerns unaddressed. This revelation underscores the importance of patching and securing open source AI frameworks to prevent potential unauthorized access and exploitation.

cont.

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. I

REDRABBIT SECURITY

Threat Intelligence

'BLUFFS' Exploits Fundamental Bluetooth Flaws, Posing Global Security Threat

Security researchers at Eurecom have unveiled a series of attacks named 'BLUFFS' that exploit two previously unknown flaws in the Bluetooth standard, impacting versions 4.2 through 5.4. These architectural vulnerabilities, tracked as CVE-2023-24023, compromise the forward and future secrecy of Bluetooth sessions, potentially exposing billions of devices to device impersonation and man-in-the-middle attacks. BLUFFS manipulates the session key derivation process, forcing the generation of weak and predictable keys, subsequently decrypted by attackers through brute force. The impact spans various devices, including smartphones, earphones, and laptops, urging a Bluetooth SIG-recommended implementation of security measures to mitigate the threat.

Key Recommendations and Impact:
Eurecom researchers propose backward-compatible modifications to enhance Bluetooth security, including the introduction of a new Key Derivation Function and the enforcement of Secure Connections (SC) mode. The potential impact on billions of devices underscores the urgency for industry-wide awareness and swift implementation of these security measures to protect against BLUFFS and similar emerging threats in the Bluetooth ecosystem.

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. I

REDRABBIT SECURITY

Released Patches and Updates

Google Chrome Addresses Zero-Day Exploits in Latest Security Update

In a crucial security move, Google has released updates for its Chrome browser, targeting seven vulnerabilities, with one marked as CVE-2023-6345—a high-severity zero-day flaw actively exploited in the wild. Uncovered by Benoît Sevens and Clément Lecigne of Google's Threat Analysis Group, the integer overflow bug in the Skia graphics library prompted the urgent patch release. Google revealed the existence of an exploit but refrained from sharing specifics about the ongoing attacks or the threat actors involved.

Of notable concern is the possibility that CVE-2023-6345 serves as a patch bypass for a similar zero-day (CVE-2023-2136) addressed in April 2023. This emphasizes the need for users to update to Chrome version 119.0.6045.199/.200 to fortify against potential threats. The broader context reveals Google's proactive approach, having resolved a total of six zero-days in Chrome this year, reinforcing the importance of timely browser updates for enhanced cybersecurity. Users of Chromium-based browsers are advised to stay vigilant and apply forthcoming fixes promptly.

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.

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

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. I

REDRABBIT SECURITY

Webinars, Conference, and Events

2023 CyberMaryland Conference

The CyberMaryland Conference stands as a yearly gathering orchestrated by the CyberMaryland Advisory Board in collaboration with academic institutions, government entities, and private industry organizations. Scheduled for December 6th and 7th, 2023, this two-day educational conference and trade show will take place at the College Park Marriott Hotel & Conference Center. We extend an invitation for you to participate in this distinguished event, offering unparalleled networking opportunities. The conference serves as a platform to foster information exchange, promoting continuous advancements and knowledge enrichment in cybersecurity across various levels, encompassing professionals, students, and educators alike.

Key Information

December 06, 2023
Event Duration: 2 Days
Maryland United States

More Details:
https://www.fbcconferences.com/e/cybermdconference/default.aspx

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.

REDRABBIT SECURITY

Featured Article of the Week

Henry Schein Faces Second Cyberattack by BlackCat Ransomware Gang

Fortune 500 healthcare company Henry Schein has encountered a second cyberattack within a month, orchestrated by the BlackCat/ALPHV ransomware gang. The initial breach occurred in October, prompting the company to take certain applications and its e-commerce platform offline. The threat actors, who claim responsibility for both incidents, recently added Henry Schein to their dark web leak site, asserting the theft of 35 terabytes of sensitive data. Despite ongoing negotiations between the company and the cybercriminals, the attackers re-encrypted Henry Schein's devices, resulting in the publication of internal payroll data and shareholder folders on the threat actors' collections blog. Henry Schein has now restored its U.S. e-commerce platform, with expectations that its platforms in Canada and Europe will follow suit shortly.

The repeated targeting of Henry Schein underscores the persistent and evolving threat landscape posed by ransomware adversaries. The healthcare industry's vulnerability to cyberattacks raises concerns about the security of patient data and the imperative for organizations to adopt robust cybersecurity measures.
https://www.bleepingcomputer.com/news/security/healthcare-giant-henry-schein-hit-twice-by-blackcat-ransomware/?&web_view=true

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.