QUALYSEC
BEYOND CYBERSECURITY

2023
FEBRUARY 4TH WEEK

CYBER SECURITY NEWS

CONTACT US

www.qualysec.com
865 866 3664
contact@qualysec.com

Beware! Fake ChatGPT Windows & Android Apps Deliver Dangerous Malware

Fake ChatGPT Apps for Windows & Android

The fraudulent website displays a deceptive “DOWNLOAD FOR WINDOWS” button, which upon clicking, triggers the download of malicious files that can put users’ devices at risk.

Upon clicking the deceptive “DOWNLOAD FOR WINDOWS” button, from the below-mentioned URL users are directed to an automatic download of a compressed file called “ChatGPT-OpenAI-Pro-Full-134676745403.gz”:-

- hxxps://rebrand.ly/qaltfnuOpenAI

The compressed file in question contains a hazardous program referred to as “ChatGPT-OpenAI-Pro-Full-134676745403.exe”. This program is categorized as a “stealer malware” due to its ability to covertly gather sensitive data from a system.

After conducting an extensive investigation, CRIL has uncovered more than 50 counterfeit and malevolent applications that exploit the ChatGPT logo to execute malicious activities. These apps have been designed to deceive users into thinking they are legitimate, but they are, in fact, harmful to your device.

At present, ChatGPT is a web-based platform that is solely accessible via the official website. As of now, there are no ChatGPT mobile or desktop applications available for any operating systems.

Source : https://cybersecuritynews.com/fake-chatgpt/

Google Paid Over $12 Million As Bug Bounty Rewards In 2022

In 2022, Google distributed $12 million as a reward through its bug bounty program. This includes a payout of $605,000, the most ever given by the firm.

“We have been able to identify and fix over 2,900 security issues and continue to make our products more secure for our users around the world”, Google.

“In 2022 we awarded over $12 million in bounty rewards – with researchers donating over $230,000 to a charity of their choice”.

For Android:

Google released Vulnerability Reward Program (VRP) statistics in 2022, providing an overview of how the security research community contributed to making the company’s products more secure.

“The Android VRP had an incredible record-breaking year in 2022 with $4.8 million in rewards and the highest paid report in Google VRP history of $605,000!”, Google

For Chrome Browser: More than 100 flaw hunters received more than $110,000 due to Google’s reward scheme for open-source products, which was introduced in August 2022.

“Chrome VRP had another unparalleled year, receiving 470 valid and unique security bug reports, resulting in a total of $4 million of VRP rewards”, Google

Source : https://cybersecuritynews.com/google-bug-bounty/

Russian National Charged for Smuggling Devices Used in Counterintelligence Operations

According to the allegations, Ilya Balakaev, a 47-year-old individual, has violated the United States sanctions imposed against North Korea and the Russian Federal Security Service (FSB) by furnishing them with U.S. equipment.

The said act of Balakaev is considered a serious breach of law that undermines the U.S. government's efforts to maintain international peace and stability.

Balakaev is a criminal at the moment as reported by the Department of Justice, and he was indicted by a federal grand jury on Friday in New York and the charges have been unsealed.

Upon capture and conviction, he will face a sentence of up to 75 years in prison. Balakaev was affiliated with the Military Unit 43753 of FSB Center 8, a branch of the Russian intelligence agency that specializes in communication security and cryptology.

The enterprise of Balakaev, Radiotester, was involved in repairing specialized equipment, including those that were designed to detect covert surveillance devices or transmit classified messages.

The defendant, in pursuit of his alleged plan, engaged in approximately 10 contractual agreements with FSB Military Unit 43753.

Source : https://cybersecuritynews.com/russian-national-charged/

Researchers Warn of Cyber Attacks Targeting Data Center Providers Globally

Recently, there has been a surge in cyber-attacks against cloud service providers (CSPs) and managed services providers (MSPs).

All these attacks were orchestrated by the threat actors who attempted to exploit vulnerabilities in the cybersecurity supply chain, with the ultimate aim of gaining unauthorized access to sensitive information belonging to targeted government organizations and businesses.

The cybersecurity analysts at Resecurity unveiled that a number of large data center customers have been affected by this breach, including the following:-

- Alibaba Group Holding
- Amazon
- Goldman Sachs Group
- Walmart

Recently, it has come to light that the login credentials for certain data center organizations have been posted on an underground forum called “Breached[.]to.”

The importance of having transparent communication with suppliers is also vital if a cyber-attack occurs that may compromise the private data of clients and their accounts.

Source : https://cybersecuritynews.com/data-center-providers/

Hackers Using Pirated macOS Apps to Deploy Evasive Malware

Jamf Threat Labs identified a specific threat targeting macOS and conducted an investigation that traced its origin to torrents containing malicious files shared on The Pirate Bay. The individual who shared these files used the username [wtfisthat34698409672].

While digging deeper into their online activities, it was revealed that they had been regularly uploading macOS apps since 2019, including popular ones like:-

- Adobe Photoshop
- Logic Pro X

Upon delving deeper into their investigation, the researchers made a fascinating discovery. The malware had gone through not one, not two, but three major developmental phases. With each new iteration, the malicious program had become more sophisticated and equipped with complex evasion techniques.

The first generation of this sneaky malware had already set the tone for its insidious nature. To ensure that its communication with its C2 went undetected, it employed an i2p network layer.

For a brief period between April and October of 2021, the second iteration of the malware made its presence known. In this gen, the malware had undergone significant changes to its codebase.

Source : https://cybersecuritynews.com/pirated-macos-apps/

Fortinet Critical RCE Flaws Lets Attackers Execute Arbitrary Code

FortiNAC is affected by the first vulnerability that has been identified as CVE-2022-39952 and marked as “Critical” with a CVSS score of 9.8.

The FortiNAC solution is designed to help organizations gain more control over network access by offering:-

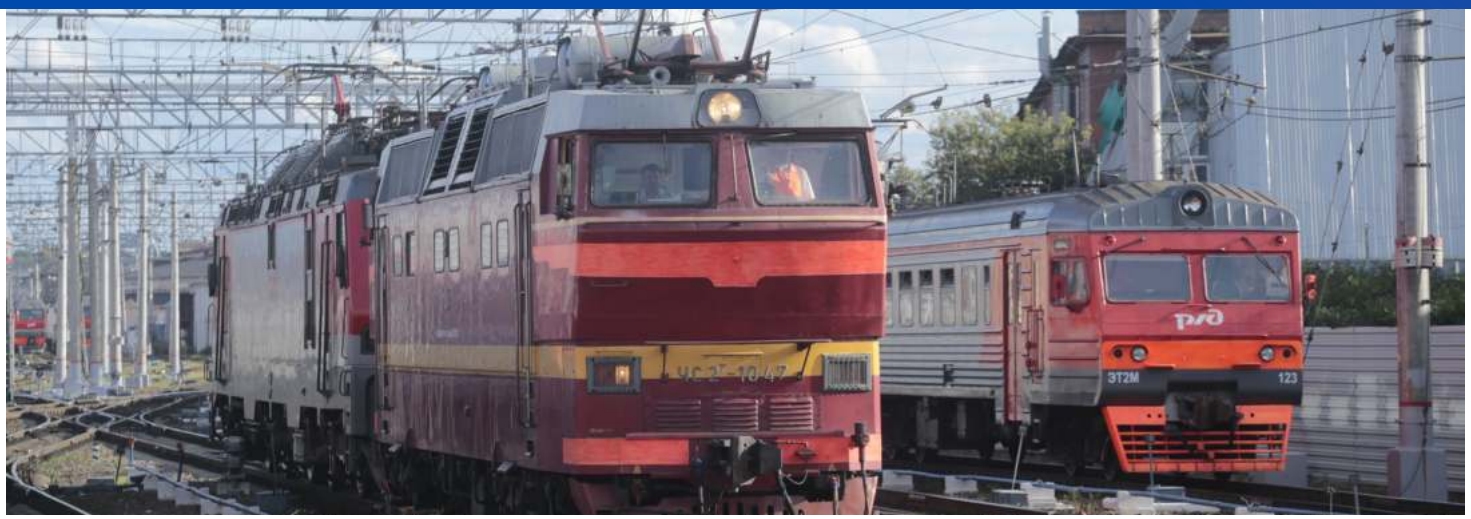
- Real-time network visibility
- Enforce security policies
- Detect and mitigate threats

FortiWeb is vulnerable to the second vulnerability that has been tracked as CVE-2021-42756 and has been marked as “Critical” with a CVSS score of 9.3. The FortiWeb web application firewall (WAF) is a web application security solution that’s designed to protect the:-

- Web apps
- API from cross-site scripting (XSS)
- SQL injection
- Bot attacks
- DDoS

FortiWeb’s proxy daemon has been discovered to contain several stack-based buffer overflow vulnerabilities, identified as CWE-121.

Source : https://cybersecuritynews.com/fortinet-critical-rce-flaws/



RailYatri Data breach – Over 31 Million Users Data Exposed

India's government-approved online travel agency, RailYatri suffered a massive data breach, exposing the personal information of over 31 million people. The database of private information has been released online, and the breach is suspected to have happened in late December 2022.

The Indian Railway Catering and Tourism Corporation (IRCTC) bus and train tickets are available for purchase on RailYatri's website. Users may also check live train timings, trip status, offline timetables, seat availability, and offline GPS train status.

The RailYatri data breach is not a common instance of hackers taking advantage of flaws, collecting data, and releasing it.

Actually, reports say it all started in 2020 when cybersecurity expert Anurag Sen discovered a misconfigured Elasticsearch server that was accessible to everyone online without a security password or any authentication.It was found that the partial credit and debit card payment logs including the name on the card, the first and last four digits of the card number, the card-issuing bank, and card expiry information possibly the most damaging aspect of the data breach.

Source : https://cybersecuritynews.com/railyatri-data-breach/

“It is crucial for users to exercise caution when receiving spam emails or to visit phishing websites and to verify the source before downloading any applications”, concludes the researchers.

It's a fact that cybercrime is on the rise and it's more important than ever to protect your business from cyber threats.

But the good news is that you don't have to navigate the complex world of cybersecurity alone. Our team of experts is here to help you cyber security testing services need to protect your application or business.

Don't wait for a cyber attack to happen. Contact us now to learn more about how we can help secure your business and give you peace of mind.

Contact now and protect your business with our expert cyber security services.

CONTACT US AT