QUALYSEC
BEYOND CYBERSECURITY

2023
MARCH 1ST WEEK

CYBER SECURITY NEWS

CONTACT US

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

ChatGPT Down Worldwide For Millions of Users

Millions of users worldwide had issues with the OpenAI chatbot ChatGPT in the early hours of February 28. Users reported that the ChatGPT services were unavailable for more than three hours.

According to DownDetector, the outage monitoring website, In the United States, Europe, India, Japan, Australia, and other regions of the world, ChatGPT is now unavailable.

Social media users shared screenshots confirming that while attempting to use ChatGPT, users encounter the error message. Eventually, OpenAI also acknowledged that ChatGPT is having issues for a lot of users.

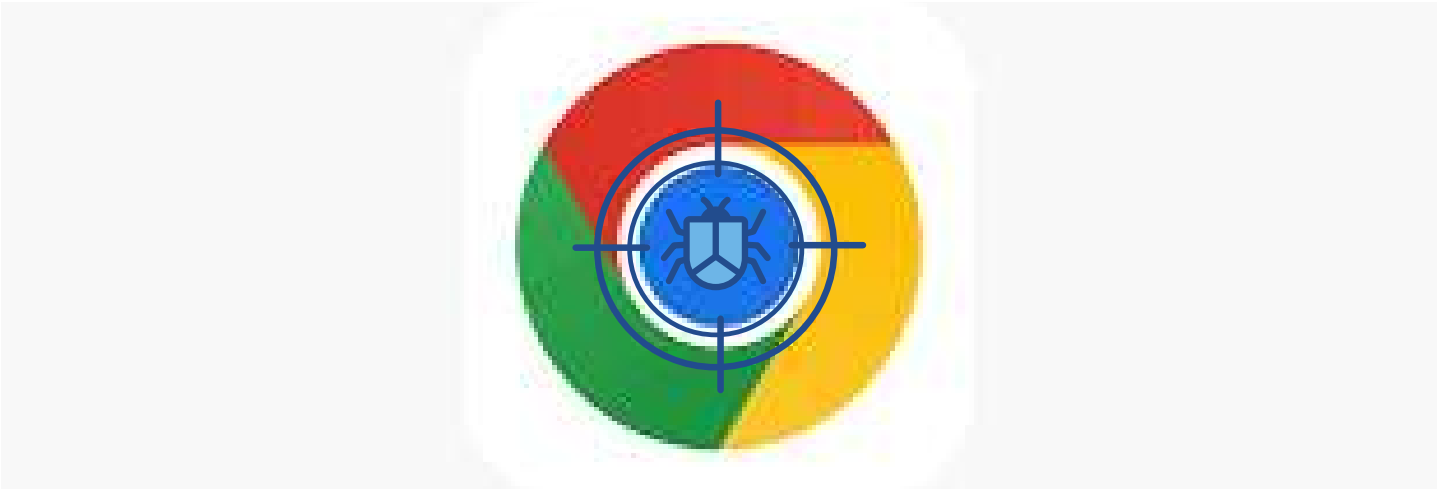
In response, OpenAI stated that “Traffic for ChatGPT is beginning to improve after initial fixes have been implemented.”

On February 28, there was a 3-hour global ChatGPT outage, which was followed by the restoration of the chatbot’s services.

When discussing how the chatbot services are down for many, Twitter users started an amusing memefest. “ChatGPT is down. I feel paralysed,” wrote a Twitter user. “Can’t believe I’m saying this, but can’t code without it now,” tweeted another user. “ChatGPT is down, 10 million people restarting their brains in the hopes it still works,” a tweet read.

OpenAI declared that problems have been resolved.

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



ChromeLoader Malware Attacking Gamers as Hacks for Nintendo and Steam Games

At the Security Emergency Response Center (ASEC) of AhnLab Security, a team of cybersecurity experts has recently uncovered a fresh wave of ChromeLoader malware that cybercriminals are employing to circumvent antivirus software and other cybersecurity defenses.

Since the attackers have used a unique type of file in this campaign to avoid detection, so, this campaign has been dubbed as an uncommon campaign.

A deviation from the typical ISO optical disc image format has been observed in the distribution of the ChromeLoader malware campaign, with cybercriminals now using virtual hard disk (VHD) files.

The use of these deceptive file names is intended to lure unsuspecting users into downloading and running the malware, allowing attackers to gain access to sensitive information or take control of their systems.malicious software has undergone significant evolution, transforming into a more sophisticated and versatile threat that is capable of carrying out a range of malicious activities like:-

Stealing sensitive data,Deploying ransomware,Dropping decompression bombs

Source : https://cybersecuritynews.com/chromeloader-malware-attacking-gamers/

WhiteSnake Stealer

Beware! New WhiteSnake Malware Attack Windows & Linux Users

The cybercriminals have recently shared an advertisement screenshot, revealing the availability of WhiteSnake Stealer for Linux OS. Interestingly, the Linux variant offers the same range of features and capabilities as its Windows counterpart.

The binary for the Linux stealer is relatively small, with a file size of just 5KB, and it can be compiled utilizing extensions like:-

- .py
- .sh

At the beginning of the infectious rampage, a sneaky spam email, cunningly disguised as a harmless PDF document, delivers the nefarious payload in the form of an executable file.

With help of the “Bat2Exe” converter, a BAT is transformed into an executable file format. In the %temp% folder a BAT file is dropped (“tmp46D2.tmp.bat”) by the executable file when it is run by the user.

Upon execution of the BAT file, a PowerShell script is initiated, which subsequently downloads a secondary BAT file named “build.bat” from a designated URL on the Discord platform.The WhiteSnake Stealer exhibits a range of sophisticated functionalities, including the ability to gain unauthorized access to cryptocurrency wallets via designated directories, as well as the capacity to extract sensitive information from browser extensions associated with such wallets.

Source :https://cybersecuritynews.com/new-whitesnake-malware/

LastPass – Hackers Breached DevOps Engineer Laptop in the Second Attack

Using information from the first incident, information from a third-party data breach and a flaw in a third-party media software package, the threat actor targeted LastPass to carry out a second “coordinated attack.”In a coordinated attack, this campaign attacked the LastPass employee, its resources, and its infrastructure.

“Our investigation has revealed that the threat actor pivoted from the first incident, which ended on August 12, 2022, but was actively engaged in a new series of reconnaissance, enumeration, and exfiltration activities aligned to the cloud storage environment spanning from August 12, 2022, to October 26, 2022”, LastPass reports.

The company assisted the DevOps Engineer with hardening the security of their home network and personal resources. Also, LastPass’ AWS S3 cloud-based storage resources were examined, and further S3 hardening measures were implemented.

Since then, according to the company, they have changed their overall security by revoking certificates, rotating sensitive credentials and authentication keys/tokens, adding more logging and alerting, and implementing tougher security standards.

Source : https://cybersecuritynews.com/hackers-breached-devops-engineer/

Dish Network Hacked – Ransomware Attack Causes Multi-Day Outage

DISH Network Corporation learned on February 27, 2023, that the recent incident involved the extraction of certain data from the Corporation's IT systems. The inquiry potentially shows that the data that's been extracted contains personal information.

"It is possible the investigation will reveal that the extracted data includes personal information", In the SEC filing, Dish Network stated.

Dish Network has now acknowledged that a multi-day network and service disruption that began on Friday was caused by a ransomware attack.

On February 23, 2023, DISH Network disclosed that there had been a network outage that had impacted internal servers and IT telephony.

After reports of a potential hack began to spread, shares of Dish Networks have been declining. Dish Network did not identify the ransomware gang responsible for the assault; however, insiders have told BleepingComputer that the attack was carried out by the Black Basta ransomware operation, which first compromised Boost Mobile and subsequently the Dish corporate networks.

Also, the Company's Windows domain controllers were compromised during the early-morning attack on February 23, and after that, VMware ESXi servers and backups were encrypted.

Source : https://cybersecuritynews.com/dish-network-hacked/

Cybercriminals Use Fake Blue Screen of Death (BSOD) Message to Trick Victims

Cyble Research and Intelligence Labs recently uncovered a fraudulent adult website that is designed to trick unsuspecting users into visiting it. Once a user visits this adult site, a harmful executable file is automatically downloaded onto their device, putting their privacy and security at risk.

The malicious executable file in question has been cleverly disguised to look like a harmless video file. This was done by using the icon of the popular VLC media player, which is a widely recognized and trusted program for playing multimedia content.Firstly, the cursor will disappear, making it difficult for the user to navigate and interact with their device. Additionally, a fake pop-up window will appear, designed to look like a legitimate notification from the system.

The pop-up will blend in with the background, making it hard to detect, and will likely contain false information or instructions.

The deceptive pop-up window that appears on the victim's device has been designed to imitate a common error screen that many Windows users are familiar with:-

- Blue Screen of Death (BSOD)

Source : https://cybersecuritynews.com/fake-blue-screen-of-death/

Beware! Insecure Redis Deployments Under Attack Using transfer.sh

The security experts at Cado Labs have recently uncovered a new crypto jacking operation that specifically targets vulnerable Redis deployments. The key element of this campaign is the utilization of a command-line file transfer service called transfer[.]sh, which is both open source and freely available.

Although the service has been operational for several years now, with the first commits made to the GitHub repository as early as 2014, instances of its employment for malware dissemination are infrequent.

As per the telemetry data collected by Cado Labs, there appears to be a shift in the trend, with an increase in the frequency of service utilization noticed since the start of the year 2023.

The reasons behind the inclination towards transfer.sh are ambiguous at the moment. However, there's a possibility that this move is a strategy to dodge detection techniques that rely on identifying typical code hosting domains, including pastebin.com.

It has been observed that in many of these malware campaigns, attackers tend to utilize popular data transfer utilities on Linux to retrieve payloads. In light of this, Transfer[.]sh could potentially replace platforms like Pastebin in the long run as a feasible alternative.

Source : https://cybersecuritynews.com/insecure-redis-deployments-under-attack/

“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