QUALYSEC
BEYOND CYBERSECURITY

2023
FEBRUARY 2ND WEEK

CYBER SECURITY NEWS

CONTACT US

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

Hackers Targeting Telecommunications Industry – Over 74 Million Clients' Data Leaked

CGM LLC, a U.S.-based SaaS provider, was targeted by the notorious ransomware group CLOP on January 5, 2023. As a specialist in Affordable Connectivity, CGM LLC assists telecommunications providers with their participation.

IntelBroker claimed to have discovered 37 million AT&T client records on the unsecured cloud storage of a third-party vendor on January 6, 2023.

This action not only confirmed the validity of their discovery but also added to the severity of the situation. To make matters worse, IntelBroker received assistance in attributing the leak to other threat actors on a public forum.

As a result of this breach, the bad actor was able to steal personal and sensitive information, including 37 million customers' personally identifiable information (PII).

Affected clients have been notified by T-Mobile which also stated that police are assisting them in the investigation. During this attack, Google Fi, which uses T-Mobile as its primary provider for Internet access and mobile phone service, was targeted for targeted SIM swapping attacks.

On February 1, 2023, IntelBroker made another shocking announcement to the public. The threat actor shared a database that contained sensitive information belonging to 144,000 clients of U.S. Cellular, one of the largest telecommunications companies in the United States.

Source : https://cybersecuritynews.com/hackers-telecommunications-industry/

GoDaddy Hacked – Attackers Breached Cpanel and Stolen Source Code

According to the company, the recent security breach that occurred over a span of several years is connected to previous breaches that were disclosed in November 2021 and March 2020.

As a result, they gained access to the following information:-

- Email addresses
- WordPress Admin passwords
- sFTP
- Database credentials
- SSL private keys of a subset of active clients

As part of an ongoing investigation into the cause of the breach, GoDaddy has enlisted the help of external cybersecurity forensics experts and law enforcement agencies around the globe.

A sophisticated and organized group, whose focus is on hosting services, including GoDaddy, was responsible for the incident, as confirmed by both GoDaddy and law enforcement.

Here's what GoDaddy stated:-

"As we continue to monitor their behavior and block attempts from this criminal organization, we are actively collecting evidence and information regarding their tactics and techniques to help law enforcement."

Source : https://cybersecuritynews.com/godaddy-hacked/

Hackers Abuse IIS Feature to Deploy New Frebniis Malware

Frebniis' method injects harmful code into the memory of iisfreb.dll, a DLL file associated with an IIS feature utilized for examining unsuccessful web page requests.

With the help of this, all HTTP requests are stealthily tracked by the malware and detect specific formats of requests from the attacker, leading to the possibility of executing remote code.

By exploiting the FREB component, the attacker can avoid detection by security measures, which is its significant benefit. This exceptional HTTP backdoor does not produce suspicious system processes, files, or traces.

While the exact route of the initial compromise is uncertain, but, it's strictly advisable to update your software on an immediate basis to mitigate the risk of threat actors exploiting vulnerabilities that are already known.

In this case, monitoring the network traffic of a company's network with the help of sophisticated network traffic surveillance tools can also assist in detecting unusual activities on the network that may be caused by Frebniis or any other malware.

Source : https://cybersecuritynews.com/frebniis-abuse-iis-feature/

RedEyes Hacking Group Uses Steganography Technique to Deploy Malware on PC & Mobile Phones

This group is now using a sophisticated malware called “M2RAT,” which is specifically designed to evade detection by security software.

In addition to using M2RAT, APT37 is also utilizing steganography, a technique that hides information within seemingly innocuous files or images, to further conceal their activities.

The APT37 hacking group is thought to be supported by North Korea, and it operates in cyberespionage. While APT37 is also known by other names like:-

- RedEyes
- ScarCruft

Initiates with Phishing

During the year 2022, this notorious hacking group was observed taking advantage of zero-day vulnerabilities in the popular web browser, Internet Explorer.

This group utilized these exploits as part of their efforts to distribute various types of malware to their targeted entities and individuals.

When a user opens the malicious attachment that was distributed in the recent series of cyber-attacks, it triggers the exploitation of an old EPS vulnerability, which is identified as CVE-2017-8291.

Source : https://cybersecuritynews.com/redeyes-hacking-group/

Pepsi Bottling Ventures Hacked – Personal Information Exposed

On January 10, 2023, the company learned that attackers gained access to their Internal IT systems.

The company said, “they took prompt action to contain the incident and to secure the systems.”

While we continue to monitor our systems for unauthorized activity, the last known date of unauthorized IT system access was January 19, 2023, reads the notification letter.

According to Pepsi’s internal investigation so far, the following are the data exposed;

- Full name
- Home address
- Financial account information (including passwords, PINs, and access numbers)
- State and Federal government-issued ID numbers and driver’s license numbers
- ID cards
- Social Security Numbers (SSNs)
- Passport information
- Digital signatures
- Information related to benefits and employment(Medical Insurance)

Source : https://cybersecuritynews.com/pepsi-bottling-ventures-hacked/

Microsoft Security Updates – 9 Critical Flaws Fixed Along With 3 Zero-Days

As part of their second Patch Tuesday for the year, Microsoft recently released patches for 78 vulnerabilities along with the three actively exploited zero-day vulnerabilities overnight, 66 of which were marked important by the company.

Moreover, there are nine vulnerabilities that allow Remote Code Execution (RCE) on vulnerable devices, so, they have been classified as 'Critical'.

Following is a list of how many bugs are found in each of the vulnerability categories:-

- Remote Code Execution Vulnerabilities: 38
- Elevation of Privilege Vulnerabilities: 12
- Denial of Service Vulnerabilities: 10
- Information Disclosure Vulnerabilities: 8
- Spoofing Vulnerabilities: 8
- Security Feature Bypass Vulnerabilities: 2

Three vulnerabilities were fixed earlier this month in Microsoft Edge, which is not included in this count.

State-sponsored threat actors in the following countries have found these flaws to be valuable assets in their arsenal of attacks:- Iran , Russia ,China

Source : https://cybersecuritynews.com/microsoft-security-updates-feb/

“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