QUALYSEC
BEYOND CYBERSECURITY

2023
JANUARY 3RD WEEK

CYBER SECURITY NEWS

CONTACT US

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

WhatsApp Fined €5.5 Million for Breaching Privacy Laws

Reports mention that users were not given a clear explanation of the legal basis WhatsApp Ireland was using, in violation of its transparency obligations.

As a result, users were not adequately informed about the processing operations being carried out on their personal data, and the purposes for which they were being used.

“Imposed a very substantial fine of €225 million on WhatsApp Ireland for breaches of this and other transparency obligations over the same period of time”, reports DPC.

“In terms of sanctions, and in light of this additional infringement of the GDPR, the DPC has imposed an administrative fine of €5.5 million on WhatsApp Ireland and ordered that WhatsApp Ireland must bring its processing operations into compliance with the GDPR within a period of 6 months”, according to DPC.

Notably, earlier this month, the DPC fined Meta a combined €390 million ($414 million) sum for GDPR violations and directed the social media group to “bring its data processing operations into compliance within a period of 3 months.”

Source : https://cybersecuritynews.com/whatsapp-fined/

Data Breach – Thousands of Users Accounts Compromised

The unauthorized parties used login credentials to access PayPal user accounts, according to a PayPal notification of a security incident.

Between December 6 and December 8, 2022, hackers gained unauthorized access to the accounts of thousands of individuals. A total of 34,942 accounts were reportedly accessed by threat actors employing a 'credential stuffing attack'.

Attacks called "credential stuffing" include trying different username and password combinations obtained from data leaks on numerous websites in an effort to get access to an account.

"The unauthorized third parties were able to view, and potentially acquire, some personal information for certain PayPal users", reads the PayPal notice of security incident.

According to PayPal, the personal information that was leaked may have included name, address, Social Security number, individual tax identification number, and/or date of birth.

On December 20, 2022, PayPal confirms that a third party used the login information to access the PayPal customer account.

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

Mailchimp Hacked – Attackers Accessed Internal Customer Support and Admin Tool

Another breach has occurred at MailChimp, which allowed threat actors to access 133 customers' data after hackers gained access to its account admin tool and internal customer support system.

It has been determined that further steps are being taken to further protect the platform as part of the company's investigation into the matter. However, the actions that are being taken by the company are not being publicly discussed for operational security reasons.

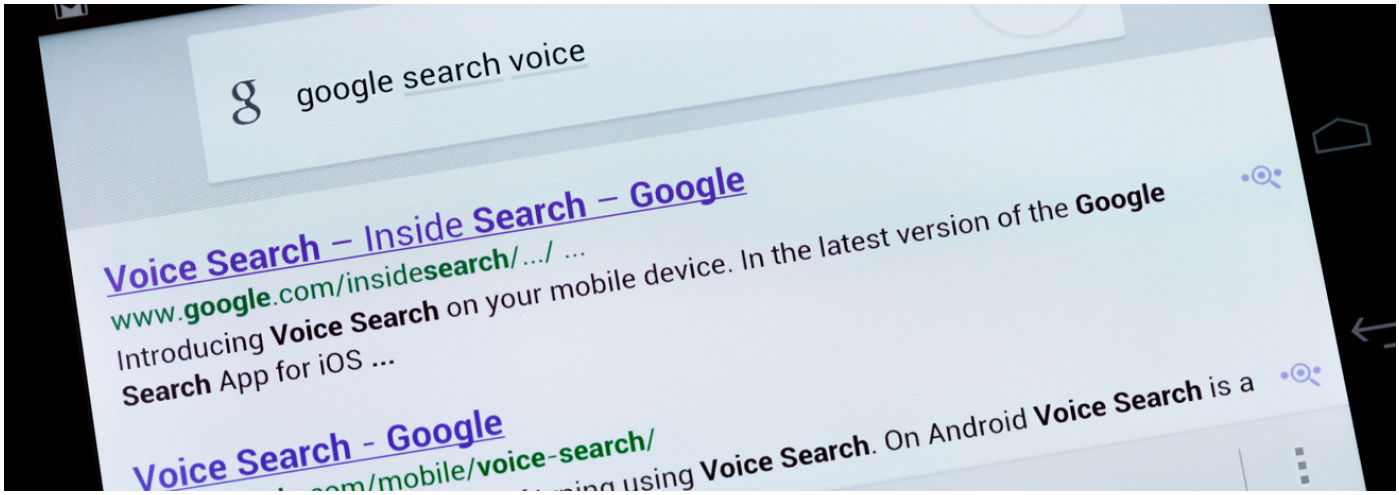
You may contact the company through the following official email if you have questions regarding the incident or the notice you received:-

- ciso[@]mailchimp.com

For such an uncertain situation, the company also apologized:-
"We know that incidents like this can cause uncertainty, and we're deeply sorry for any frustration."

Moreover, the company affirmed that throughout the investigation, they will continue to provide timely and accurate information to all affected account holders and will monitor the situation closely.

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



Beware! New Infostealer Malware Spreading Through Google Ads

Cyble Research & Intelligence Labs (CRIL) discovered a brand-new malware variant called “Rhadamanthys Stealer.” This malware stealer variation is now in use and the threat actors who created it are offering it for sale via the Malware as a Service (MaaS) business model.

The Rhadamanthys stealer spreads by tricking users into visiting phishing websites that look like popular programmes like Zoom, AnyDesk, Notepad++, Bluestacks, etc. It can propagate through spam emails that include an attachment that contains the harmful payload.

Further, fake Google Ads are used in this campaign that aimed at consumers trying to download popular software.

“It targets different browsers such as Brave, Edge, Chrome, Firefox, Opera Software, Sleipnir5, Pale Moon, CocCoc, etc”, CRIL Researchers say the stealer malware is also made to target different crypto wallets and gather data from them.

Source : https://cybersecuritynews.com/rhadamanthys-stealer-delivered-google-ads/

“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

+91 865 866 3664 www.qualysec.com contact@qualysec.com