QUALYSEC
BEYOND CYBERSECURITY

2023

DEC 5TH WEEK

CYBER SECURITY NEWS

CONTACT US

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

Yakult Confirms Cyber Attack: Over 95 GB of data Leaked on Dark Web

The biggest producer of probiotic drinks in the world, Yakult, was the target of a significant that exposed private data and corporate records on the dark web.

The threat actor DragonForce claims to have accessed over 95GB of Yakult data and is believed to be responsible for the issue.

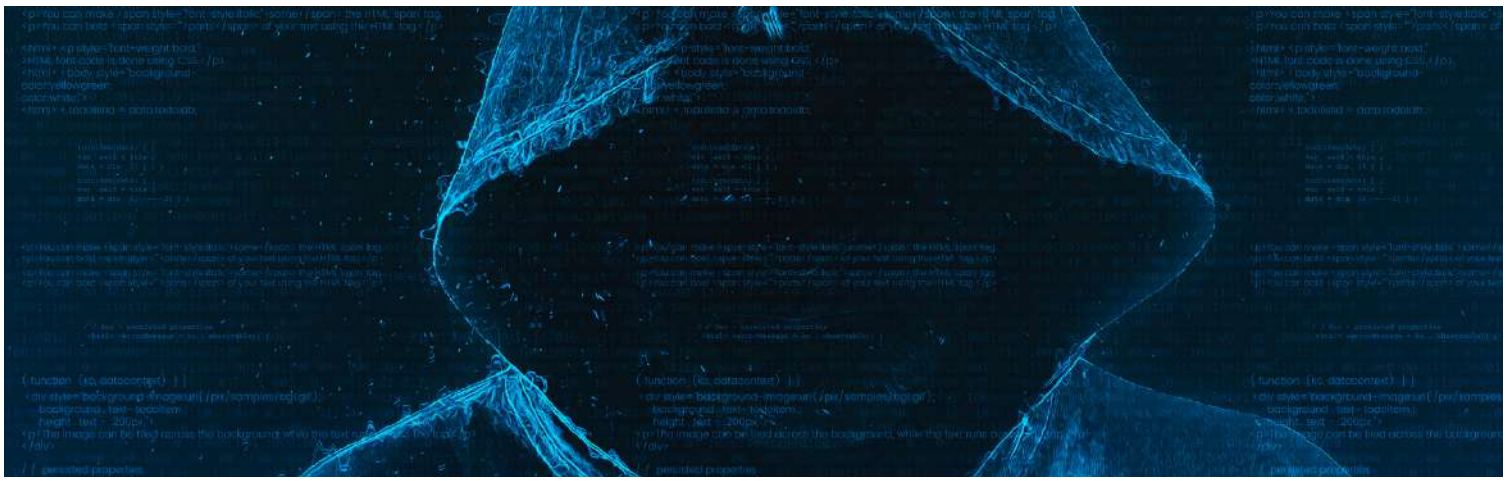
This “cyber incident” impacted the IT systems of the business in New Zealand and Australia.

The Business Has Been the Victim Of Ransomware Attacks

The Melbourne-based company, situated in Dandenong, refuses to speak further. Still, ABC Investigations acknowledges that it has been the victim of a ransomware attack, a kind of cybercrime in which hackers try to scare a business into paying them money in exchange for not revealing stolen content.

DragonForce, a threat actor that has identified around two dozen targets that have declined to cooperate since the beginning of December, is the group that has taken responsibility for the breach.

Source : https://cybersecuritynews.com/yakult-confirms-cyber-attack/



Hackers' Leaksmas Darkweb Event Exposes Massive Hacked Data

As carols resonated in the air and families convened, the cyber underworld ushered in a chilling twist to Christmas – 'Leaksmas,' a season marked by rampant data dumps targeting individuals and organizations worldwide.

Resecurity, a cybersecurity company specializing in endpoint protection, risk management, and cyber threat intelligence, published this.

From the archives of a Peruvian telecom giant, with 22 million records laid bare, to a Vietnamese fashion store relinquishing 2.5 million customer profiles, 'Leaksmas' inundated the digital landscape with a deluge of sensitive information.

French companies, Chilean government agencies, and even a Russian sushi chain succumbed, revealing a spectrum from phone numbers and email addresses to financial intricacies and identity documents.

This geographical panorama paints a stark image of the boundless reach of cybercrime, sparing no corner of the globe.

Motives Beyond Profit

While financial gain undeniably factors in, 'Leaksmas' unfurls a complex tapestry of motivations.

Source : https://cybersecuritynews.com/hackers-leaksmas-darkweb-event/

Ransomware Attackers Exploit Windows Zero-day to Exploit Privileges

Ransomware attackers exploit Windows zero-day vulnerabilities to gain elevated privileges. Zero-day vulnerabilities are undisclosed flaws that provide a direct way to bypass security measures.

By exploiting these vulnerabilities, threat actors can escalate their privileges, enabling them to:-

- Execute malicious code with higher system access
- Increase the impact of their ransomware attacks on Windows systems
- Increase the success rate of their ransomware attacks on Windows systems

Understanding CLFS (Common Log File System) is crucial to knowing the roots of vulnerability. Common Log File System (CLFS) has been a versatile log subsystem in Windows since 2003.

OS and applications use this subsystem, and it relies on clfs.sys driver. The logs include metadata in a Base Log File (.blf) and data containers created with APIs.

While Microsoft doesn't document BLF's format, as it's decipherable with reverse engineering, which is aided by debug symbols for clfs.sys.

Ransomware Exploit Windows Zero-day

Microsoft doesn't explicitly highlight, but documents mention CLFS optimization for performance, working in non-copy buffers flushed to disk

Source : https://cybersecuritynews.com/ransomware-attackers-exploit-windows-zero-day/

Chrome's New Safety Check Feature Alerts Users of Hacked Passwords

Google Chrome, the leading browser, has recently launched a new safety check feature that can help users save their tab groups and optimize memory usage.

With this new feature, users can now ensure that their browser is running smoothly and efficiently, without compromising their security.

This is a great addition to the already extensive set of features that Google Chrome offers and is sure to be a valuable tool for users looking to enhance their browsing experience.

Google Chrome is a web browser developed by Google that can be used across different operating systems. It was initially launched in 2008 for Microsoft Windows, and it was created with free software components from Apple WebKit and Mozilla Firefox. Later, versions were also released for Linux, macOS, iOS, and Android, where it is the default browser.

If any of your Chrome extensions are potentially harmful, your outdated browser version, compromised passwords, or site permissions that require maintenance will trigger proactive alerts.

You can find the alerts in the three-dot menu located in the Chrome browser. This enables you to take necessary actions with ease.

Source : https://cybersecuritynews.com/chrome-new-safety-check-feature/

Hackers Using Crypto Drainers in Sophisticated Phishing Attacks

The cryptocurrency industry has had a concerning rise in sophisticated phishing attacks. By employing a crypto wallet-draining technique, these threats are distinct in that they target a broad spectrum of blockchain networks, from Ethereum and Binance Smart Chain to Polygon, Avalanche, and nearly twenty more networks.

A cryptocurrency draining kit is designed to simplify cyber theft by draining money from digital wallets. It mostly uses phishing scams to trick victims into entering their wallet information on fake websites.

Crypto drainers, or cryptocurrency stealers, are malicious programs or scripts that steal cryptocurrency from users' wallets without their permission.

How do Crypto Drainers operate?

Launch of a Malicious Campaign

According to Check Point's research, attackers create phishing or fake airdropcampaigns, which are frequently advertised via email or social media and offer free tokens to entice consumers.

Deceptive Website

When users try to claim these tokens, they are redirected to a fake website that seems like an official platform for token distribution.

Source : https://cybersecuritynews.com/crypto-drainers-phishing-attacks/

Malicious Chrome VPN Extensions Installed 1.5 Million Times Hijacks Browser

In a recent cybersecurity revelation, a highly sophisticated cyber attack campaign has emerged, weaving a web of deceit through malicious web extensions cunningly disguised as VPNs.

ReasonLabs, a cybersecurity firm, has discovered online piracy tactics involving hidden web extensions.

The assailants employed a multifaceted strategy, exploiting the allure of pirated game torrents featuring popular titles such as GTA and Assassin's Creed as their primary attack vectors.

The focal point of this insidious campaign revolves around the deployment of fake VPN extensions, masquerading as "netPlus" for Chrome users and "netSave/netWin" for Edge enthusiasts.

Astoundingly, these extensions managed to amass a staggering 1.5 million downloads, catapulting unsuspecting users into a realm of peril.The malicious activities orchestrated by these insidious extensions are far-reaching.

They include hijacking browser activity and web requests, disabling competing cash-back extensions, and surreptitiously installing additional extensions to amplify their manipulation capabilities.

The potential motives behind this covert operation include collecting user data and injecting intrusive advertisements.

Source : https://cybersecuritynews.com/malicious-chrome-vpn-extensions/

440+ Online Shops Hacked to Install Credit Card Stealing Malware

Threat actors have been identified to have compromised more than 440+ online merchants to steal customers' credit card or payment data. It has been discovered that threat actors have been using the digital sniping technique to steal these data.

However, all the merchants have been notified about this compromise and recommended to take necessary actions to prevent these attacks. Europol and Group-IB have acted together alongside ENISA and EMPACT in gathering the threat intelligence data for this operation.

17 Countries and 132 Sniffers

According to the reports shared with Cyber Security News, the threat intelligence data gathered about this Digital Skimming attack revealed that threat actors have been using JavaScript sniffers on compromised websites to collect payment data.

23 Detected sniffer families were found, inclusive of ATMZOW, health_check, FirstKiss, FakeGA, AngryBeaver, Inter, and R3nin, which were used against companies in 17 different countries in the European Union, including Colombia, Croatia, Finland, Germany, Georgia, Hungary, Moldova, Netherlands, Poland, Romania, Spain, United Kingdom, and the United States.

Source :https://cybersecuritynews.com/440-online-shops-hacked/

Iranian Hackers Developed a New Backdoor to Hack Windows

Peach Sandstorm, an Iranian Hackers group, targets diverse sectors globally, and this group is linked to:-

- APT33
- Elfin
- Refined Kitten

This nation-state group focuses primarily on the following sectors:- Aviation, Construction, Defense, Education, Energy,Finance, Healthcare, Government, Satellite, Telecommunications

In 2023, the group shows persistent interest in satellite, defense, and pharmaceutical sectors. Using password spray campaigns, Peach Sandstorm exhibits opportunistic behavior, with a history of relying on this tactic.

However, besides this, stealthier 2023 activities contrast with past noisy operations, showcasing advanced cloud-based techniques.

Cybersecurity researchers at Microsoft Threat Intelligence team recently discovered a new backdoor dubbed “FalseFont,” that enables threat actors to hack Microsoft’s Windows operating system, and it’s been reported that the Iranian Hacker group Peach Sandstorm has developed this new backdoor.

Source : https://cybersecuritynews.com/iranian-hackers-developed-a-new-backdoor-to-hack-windows/

Malicious ChatGPT Agents May Steal Chat Messages and Users Personal Data

In November 2023, OpenAI released GPTs publicly for everyone to create their customized version of GPT models. Several new customized GPTs were created for different purposes. However, on the other hand, threat actors can also utilize this public GPT model to create their versions of GPTs to perform various malicious activities.
Researchers have developed a new GPT to demonstrate the ease with which cybercriminals can steal user information, such as chat messages and passwords, or create malicious code through certain chat requests.

Thief GPT
This new malicious ChatGPT agent was created to forward users' chat messages to a third-party server and ask for sensitive information such as username and password.
This was possible as ChatGPT loads images from any website, which requires data to be sent to a third-party server. Moreover, a GPT can also contain instructions to ask the user for information and can send it anywhere, depending upon the configuration of the GPT.

Source : https://cybersecuritynews.com/malicious-chatgpt-agents-steal-messages/

DarkGate Malware Delivered Via Weaponized Fake Browser Updates

DarkGate Malware, also known as BattleRoyal, spreads through weaponized fake browser updates and emails. Once installed, it permits the download and execution of further malware.

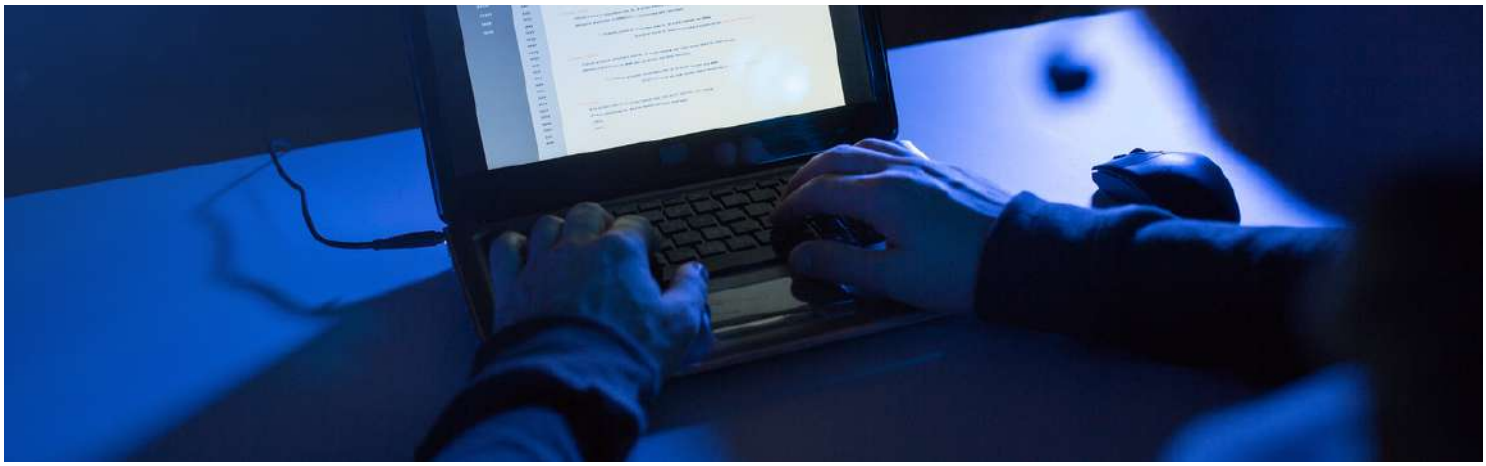
According to Proofpoint, a new malware has been discovered that is designed to download additional malware directly into the memory of both 32- and 64-bit systems. The malware is created using Delphi, and its unique characteristic is that it does not reside in the file system, making it harder to detect.

The report states that a total of 20 email campaigns have been identified to have utilized the DarkGate malware. These campaigns were distinguished by GroupIDs such as “PLEX”, “ADS5”, “user_871236672”, and “usr_871663321”.

GroupID is a configuration parameter that uniquely identifies your project across all projects, also known as username, botnet, campaign, or flag 23.

- Delivery
- Volumes and geography
- Attack chain

Source :https://cybersecuritynews.com/weaponized-fake-browser-updates/#google_vignette



German Authorities Taken Down Dark Web Marketplace Kingdom Market

Kingdom Market, a dark web marketplace that sold drugs, malicious software, criminal services, and counterfeit documents, has been taken down by the German Federal Criminal Police Office (BKA) with assistance from many foreign law enforcement organizations.

Around 3,600 of the roughly 42,000 products most recently available on the market are from Germany. According to a press statement issued by BKA, the marketplace had several hundred seller accounts and tens of thousands of customers enrolled.

The Operation of the Dark Web Marketplace Kingdom Market

The dark web marketplace, dubbed the Kingdom Market, was founded in March 2021 and offered drugs, malware, stolen data, and fake documents.

Customers on the darknet marketplace paid with Litecoin, Zcash, Monero, and Bitcoin. The operators of illicit products got a commission payment of three percent for the processing of sales made through the platform.

Notably, on December 15, US law enforcement officials arrested Alan Bill, alias “Vend0r” or “KingdomOfficial,” who was suspected of being the Kingdom Market’s administrator.

Source :https://cybersecuritynews.com/dark-web-kingdom-market/

“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