QUALYSEC
BEYOND CYBERSECURITY

2023
APRIL 1ST WEEK

CYBER SECURITY NEWS

CONTACT US

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

Apple Zero-Days Exploited to Hack iPhones and MacOS

Recently, two new zero-day vulnerabilities were identified and exploited in the wild to compromise Apple devices. These vulnerabilities have been addressed by emergency security updates released recently by Apple.

Here below, we have mentioned the Apple devices that were targeted and could be compromised:-

- iPhones
- Macs
- iPads

Apart from this, the most shocking thing is that Apple might have already been aware of the active exploitation of these vulnerabilities in the wild. As usual with Apple, few details about the zero-day attacks were revealed.

Zero-day Vulnerabilities

The zero-day flaws are tracked as:-

CVE-2023-28206

CVE-2023-28205

Source : https://cybersecuritynews.com/apple-zero-days/

Adobe Reset User Password in Awake of Data Breach Risks

An email has been dispatched by Adobe, a renowned software firm recognized for its widely-used creative tools, requesting its users to modify their passwords.

The sent password reset emails inform users to change the password for their Adobe ID since they might have been compromised in recent data breaches from other vendors.

Many Users on Twitter stated that they received hundreds of password reset emails.

A few users stated that they cannot complete the password reset process.

Adobe states that the next time users log in to Adobe ID, they will be prompted with a password reset notification

According to the email, Adobe has reset the password for the Adobe ID-linked account of its users, citing potential compromise due to data breaches from various other online services.

After Adobe detected several events relating to information leakage, they took a countermeasure to protect their user information to eliminate the risk.

Adobe stated that this is a preventive step to secure user accounts from unauthorized access.

They have also requested their users change their password on other websites where they have used the same password as that of Adobe.

Source : https://cybersecuritynews.com/adobe-reset-user-password/

New Money Message Ransomware Attacks Both Windows & Linux Users

Cyble Research and Intelligence Labs (CRIL) discovered a new ransomware group called Money Message. Both Windows and Linux operating systems are targeted by this ransomware, which can encrypt network shares. Experts believe that threat actors may use stealer logs in their operations.

More than five victims publicly identified as having been impacted by Money Message, the majority of whom are Americans, have already been reported since it was first noticed in March 2023.

Industries represented by the victims include BFSI, transportation and logistics, and professional services.

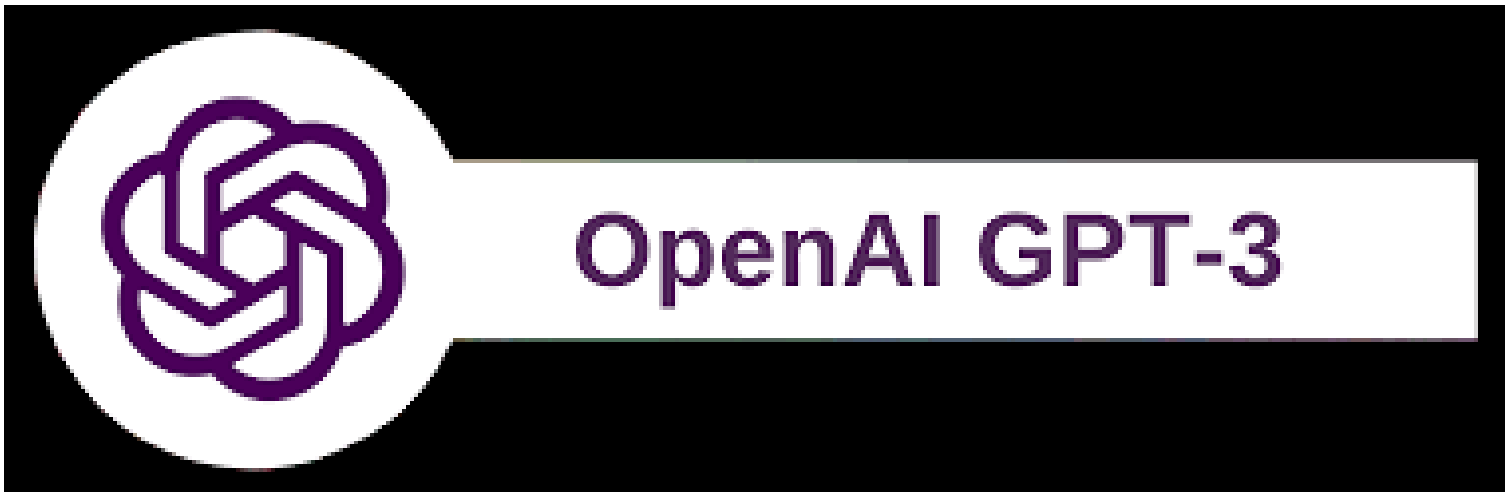
Specifics of the New Money Message Ransomware Attacks

The gang targets its victims using a double extortion method that entails exfiltrating the victim's data before encrypting it. The group posts the data on their leaked website if the ransom is unpaid.

The Elliptic Curve Diffie-Hellman (ECDH) key exchange and ChaCha stream cipher algorithm are used by the Money message ransomware to encrypt data on a victim's Computer and demand a ransom for its release.

Researchers stated that, like other ransomware groups, this ransomware does not rename the file after encryption.

Source :https://cybersecuritynews.com/money-message-ransomware/



ChatGPT Leaks Samsung Data After Permitting ChatGPT at Semiconductor Plants

With 20 days of ChatGBT implementation at the Samsung semiconductor plant, ChatGPT leaked Samsung corporate data accidentally.

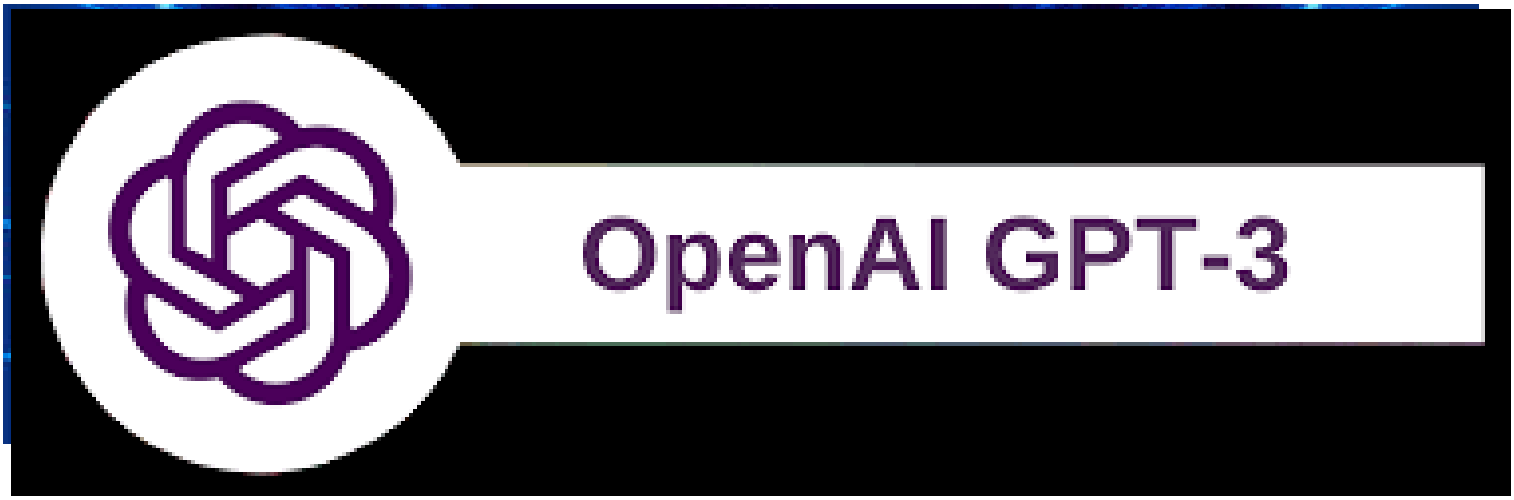
The leaked content related to semiconductors is ‘facility measurement’ and ‘yield/defect, and the report states that if corporate secrets are entered in the question, the contents can be leaked to an unspecified number of people.

There were 3 incidents of accidentally entering Samsung Electronics’ corporate information into ChatGPT. Meanwhile, ChatGPT specifies, “Do not enter sensitive information through the ChatGPT usage guide in the 8th point.

As a result, Samsung Electronics has been blocking the use of ChatGPT within its workplaces out of concern about leaks of internal confidential information.

“However, from the 11th, the DS division permitted ChatGPT. The device experience sector (DX, mobile, and home appliances) still prohibits ChatGPT”. South Korean Economist report says.

Source : https://cybersecuritynews.com/chatgpt-leaks-samsung-data/



Italy Blocks ChatGPT Temporarily Over Privacy Concerns

According to the government's privacy regulatory body, Italian authorities have recently placed a temporary hold on the ChatGPT due to concerns regarding data privacy.

With the recent emergence of artificial intelligence chatbots, the Italian government is the first country from the Western region to take action against one of these bots, ChatGPT.

As a result of the restriction, the web version of ChatGPT, one of the most popular writing assistants, cannot be used.

Italy Temporarily Blocks ChatGPT

On March 20th, 2023, ChatGPT experienced a data loss that resulted in a data breach of user conversations and payment information of paying customers.While this data breach raised privacy concerns, and as a result, the Italian government decided to block ChatGPT over this issue.

The Privacy Guarantor has pointed out that OpenAI fails to inform users and parties whose data is collected. In short, in their provision, OpenAI lacks a legal justification for mass collecting and storing personal user information and uses it to train the platform's algorithms.

Source : https://cybersecuritynews.com/italy-blocks-chatgpt/

Microsoft & Fortra to Take Down Malicious Cobalt Strike Servers

A recent collaboration between Microsoft's Digital Crimes Unit (DCU), Fortra, and the Health-ISAC has resulted in a significant legal crackdown targeting servers hosting cracked and illicit versions of Cobalt Strike.

Since threat actors actively use this tool, Cobalt Strike is one of their most essential tools for hacking.

As a company dedicated to protecting the legitimate use of its security tools, Fortra has undertaken this vital action to protect such use.

Additionally, Microsoft takes a similar approach to ensuring that its services and products are used legitimately.

The most imperative thing to be followed is to remain persistent in removing the cracked copies of Cobalt Strike currently being hosted worldwide.

Disruption Plan

In an attempt to allow Microsoft, Fortra, and Health-ISAC to destroy and seize the complete malicious infrastructure of the threat actors, a court order has been issued by the U.S. District Court for the Eastern District of New York on March 31, 2023.

Source : https://cybersecuritynews.com/malicious-cobalt-strike-servers/

Google VS North Korean APT – How Google Fight With Gov-Backed NK APT Hackers

Google's TAG (Threat Analysis Group) released defensive measures that followed to protect users from the infamous North Korean government-backed APT group attacks.

After Mendiant's recent analysis of APT43, Google's TAG has been sharing how they effectively protect the users, and the APT43 activities have been tacking underneath the name of the ARCHIPELAGO operation since 2012.

APT 43 targets the Google and non-Google users' accounts belonging to government and military officials, policymakers, and researchers in U.S. and outside of the US.

To keep the users safe and secure their accounts, Google keeps adding malicious websites, domains, and IOCs to its Safe Browsing
and sending alerts to the targeted users' emails about the APT 43 activities to ensure the user's security from further attacks and exploitation.ARCHIPELAGO Activities

Google found that the Threat actors often send sophisticated phishing emails that mimic a media outlet to prompt receipt to check the interview questions or request information.

Source : https://cybersecuritynews.com/google-vs-north-korean-apt/

STYX – A New Dark Web Marketplace Selling DDOS Tools & Banking Malware

Researchers from Rsecurity discovered a recently opened marketplace named STYX; it was found to be opened around January 19, 2023.

Cybercriminals operating this marketplace primarily focus on financial fraud, money laundering, and identity theft.

The portal was found to be designed using the escrow module, which enables threat actors to brokerage between the buyers and sellers.

Tools and Compromised Payment Data

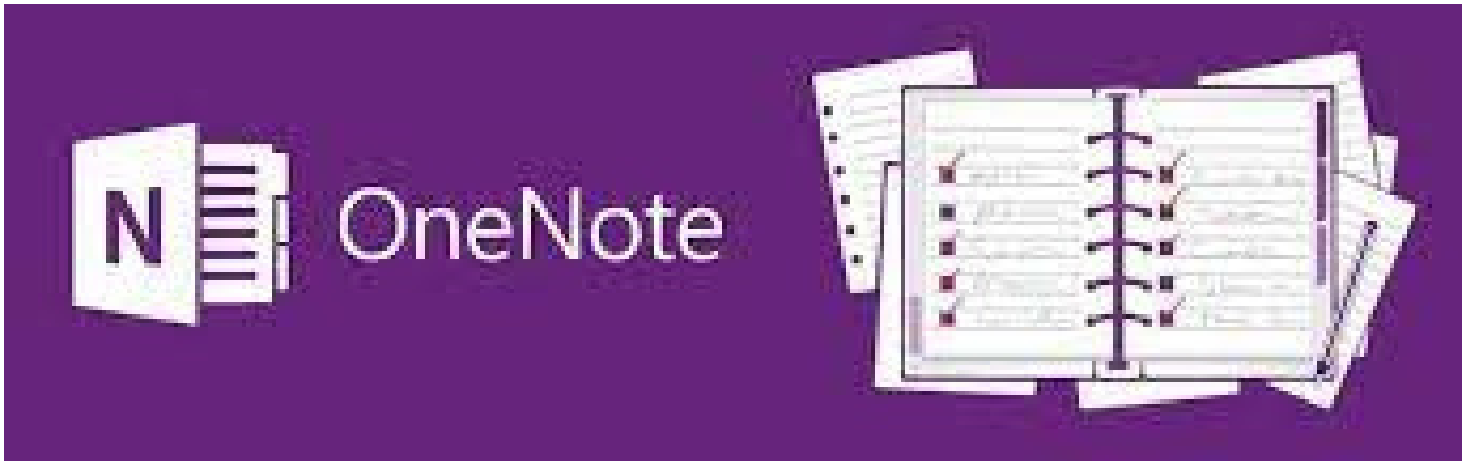
To access any services, users are required to register with the portal. Once registered, they can browse a wide range of services.

“STYX also offers a Trusted Sellers section, presumably where the admins of STYX have vetted reliable vendors, before whitelisting them.” reads the Rsecurity blog post.

Users are linked to Telegram groups that grant access to tools for online banking theft and fraud, such as anti-detects, device fingerprint emulators, and spoofers.

The portal also got listed in the “Enclave Service,” which is known to be a reputable service on the dark web.

Source : https://cybersecuritynews.com/web-marketplace/



Microsoft OneNote Security Blocks 120 File Extensions to Tighten Security

To better protect users, Microsoft has published detailed information on the dangerous embedded files that OneNote will soon block.

“To help protect you and your recipients against computer viruses, Outlook blocks the sending and receiving of certain types of files (such as .exe and certain database files) as attachments,” Microsoft.

Threat actors embed dangerous files and scripts in malicious Microsoft OneNote documents, covering them with design elements.

Following recent and ongoing phishing attacks propagating malware, Microsoft initially disclosed that OneNote will have improved security in a Microsoft 365 roadmap article released recently last month.

As Microsoft patched a MoTW, bypassed zero-day exploit to spread malware via ISO and ZIP files, and finally disabled Word and Excel macros by default, threat actors began employing OneNote documents in spear phishing campaigns around the middle of December 2022.

Blocked File Types in Outlook

According to Microsoft, the files considered dangerous and blocked in OneNote will be aligned with those blocked in Outlook, Word, Excel, and PowerPoint.

Source : https://cybersecuritynews.com/microsoft-onenote-security/

HP LaserJet Printers Flaw Let Attacker Gain Unauthorized Access

According to a security advisory from HP, some HP Enterprise LaserJet and HP LaserJet Managed printers may be susceptible to information exposure when IPsec is enabled with FutureSmart version 5.6.

All HP Enterprise devices run HP FutureSmart firmware, making it simple to administer and maintain various features across your fleet, from the user experience to app security support.

Users can operate and set up printers using a control panel located at the printer or a web browser for remote access.

The IP network security protocol suite, IPsec (Internet Protocol Security), is used in business networks to secure internal and external communications and stop unwanted access to resources, such as printers .A critical rating and a CVSS v3.1 score of 9.1 have been given to the issue, tracked as CVE-2023-1707.

Indeed, HP has not yet released a fix for the concerned firmware. According to HP, a new firmware version that rectifies the problem should be available in 90 days.

Notably, the information disclosure flaw in this condition could give an attacker access to sensitive information sent between the affected HP printers and other networked devices.

Source : https://cybersecuritynews.com/hp-laserjet-printers-flaw/

Western Digital Hacked – Hackers Breached The Network & Accessed The Data

Well-known Scandisk drive manufacturer Western Digital (WD) disclosed a data breach on its network in which attackers accessed multiple systems' unauthorized data.

WD is an American computer drive manufacturer and data storage company that produce and sell data storage devices, data center systems, and cloud storage services.

Since it's an ongoing incident, the company immediately deployed the Incident responders and investigated the attack with the help of Digital forensic experts.

"Western Digital identified a network security incident involving Western Digital's systems. In connection with the ongoing incident, an unauthorized third party gained access to a number of the Company's systems." WD said in a Press release.

The company also said that there are working to restore the affected systems and believes that the unauthorized party obtained specific data from its systems and is working to understand the nature and scope of that data.

"The Company is implementing proactive measures to secure its business operations, including taking systems and services offline, and will continue taking additional steps as appropriate."

Source : https://cybersecuritynews.com/western-digital-hacked/

“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