QUALYSEC
BEYOND CYBERSECURITY

2023

MAY 2ND WEEK

CYBER SECURITY NEWS

CONTACT US

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

Hackers Aggressively Exploiting WordPress Plugin XSS Flaw – 2 Million Sites Affected

The cybersecurity researchers at Akamai recently affirmed as web applications and third-party tools become more prevalent, the risk of cyber-attacks increases due to a larger attack surface and low entry barriers for attackers. Shortly after the announcement of a critical vulnerability in a WordPress custom field plug-in and the release of a patch, a notable increase in XSS activity was observed, with one specific proof-of-concept query being particularly significant.

Attackers are exploiting known vulnerabilities more extensively, and it's important to analyze the vulnerability, actor, and traffic to understand the attack.

Initial Flaw Leads to XSS

CVE-2023-30777, a vulnerability detected in February with a CVSS base score of 7.1, enables a threat actor to execute a reflected XSS attack by injecting harmful scripts, redirects, ads, and URL manipulations into a targeted website.

The vulnerability's widespread impact, affecting over 2 million active plug-in users, garnered significant attention upon releasing the exploit PoC, patch, and a comprehensive write-up featuring example payloads.

Source :https://cybersecuritynews.com/wordpress-plugin-xss-flaw/

BurpGPT – ChatGPT Powered Automated Vulnerability Detection Tool

Cyber Security News came across a new ChatGPT-powered Vulnerability detection Tool called “BurpGPT,” which helps security researchers to detect the vulnerabilities that traditional scanners might miss.

Like PentestGPT, a ChatGPT Powered Automated Penetration Testing Tool, BurpGPT was developed with deep vulnerability scanning features.

BurpGPT combines Burp Suite with OpenAI’s GPT to perform a passive scan to detect vulnerabilities and traffic-based analysis.

To detect the vulnerabilities in web applications, BurpGPT sends web traffic to an OpenAI model Specified by the user, enabling sophisticated analysis within the passive scanner.

Alexandre Teyar, a security researcher from the UK, developed BurpGPT. The plugin provides customizable prompts allowing customized web traffic analysis that adapts to each user’s demands.

“The extension generates an automated security report that summarises potential security issues based on the user’s prompt and real-time data from Burp-issued requests.”Alexandre said.

The add-on accelerates vulnerability assessment and gives security experts a higher-level overview of the scanned application or endpoint by utilizing AI and natural language processing.

Source : https://cybersecuritynews.com/burpgpt/

Dragos Cyber Attack – Hackers Contacted Firm CEO's Son, Wife in Extortion Attempt

A cybercriminal group obtained contracts from cybersecurity firm Dragos Inc. as part of an extortion attempt that involved contacting the chief executive officer's wife and 5-year-old kid.

For industrial control systems, including power grids, water treatment facilities, and pipelines, Dragos excels in offering cybersecurity services.

According to the reports, a newly hired Dragos salesperson's email account was compromised, giving hackers access to internal documents. The company didn't compensate the hackers, CEO Robert M. Lee.No Dragos systems were compromised, including those connected to the Dragos Platform.

Cybercriminal Group Attempted And Failed At An Extortion Scheme

On May 8, a "known criminal group attempted and failed at an extortion scheme against Dragos," according to the blog. Dragos didn't mention who the hackers were.

According to Lee, the hackers called Lee's kid using a phone he used to call his grandma as part of the extortion effort. The boy handed his mother the phone, who then hung up. According to him, the hackers called Lee's wife separately.

Source : https://cybersecuritynews.com/dragos-cyberattack/

Researchers Uncovered C2 Infrastructure Used by Baking Malware Ursnif

Bridewell's Cyber Threat Intelligence (CTI) team has discovered previously undetected Ursnif infrastructure used in 2023 campaigns, suggesting that the malware operators have not yet utilized this highly elusive infrastructure.

Ursnif Banking Malware

Ursnif, originally a banking trojan also known as Gozi, has evolved into a ransomware and data exfiltration facilitator, with its latest variant, LDR4, being identified by Mandiant in June 2022, joining the ranks of malware like:- Emotet ,Trickbot

In January 2023, a DFIR report highlighted a campaign involving the Urnsnif backdoor, followed by Cobalt Strike deployment and subsequent data exfiltration, with the added use of legitimate RMM tools Atera and Splashtop by the threat actor.

A phishing email was delivered to the Ursnif backdoor via a malicious ISO file. In March 2023, eSentire documented a Google Ads campaign using BatLoader to drop various second-stage payloads like Redline and Ursnif disguised as legitimate tools, followed by Cobalt Strike deployment for further intrusion activity in enterprise environments.

Source : https://cybersecuritynews.com/c2-infrastructure-ursnif/

New Phishing-as-a-Service Tool Used in the Wild to Target Organizations

The cybersecurity researchers at Cisco Talos recently affirmed that threat actors are targeting the widely-used Microsoft 365 cloud-based productivity platform through the Greatness phishing platform, and not only that, even they also noticed an uncertain surge between December 2022 and March 2023.

Experiencing a notable surge in operations, the 'Greatness' Phishing-as-a-Service (PhaaS) platform has set its sights on organizations utilizing Microsoft 365 in the countries like:-

- The United States
- Canada
- The U.K.
- Australia
- South Africa
-

Here below, we have mentioned the sectors and industries from where the victims are mainly targeted, and the majority of them are located in the United States:-

Manufacturing, Healthcare, Technology, Education, Real estate
Construction, Finance, Business services

Source : https://cybersecuritynews.com/phishing-as-a-service-tool//

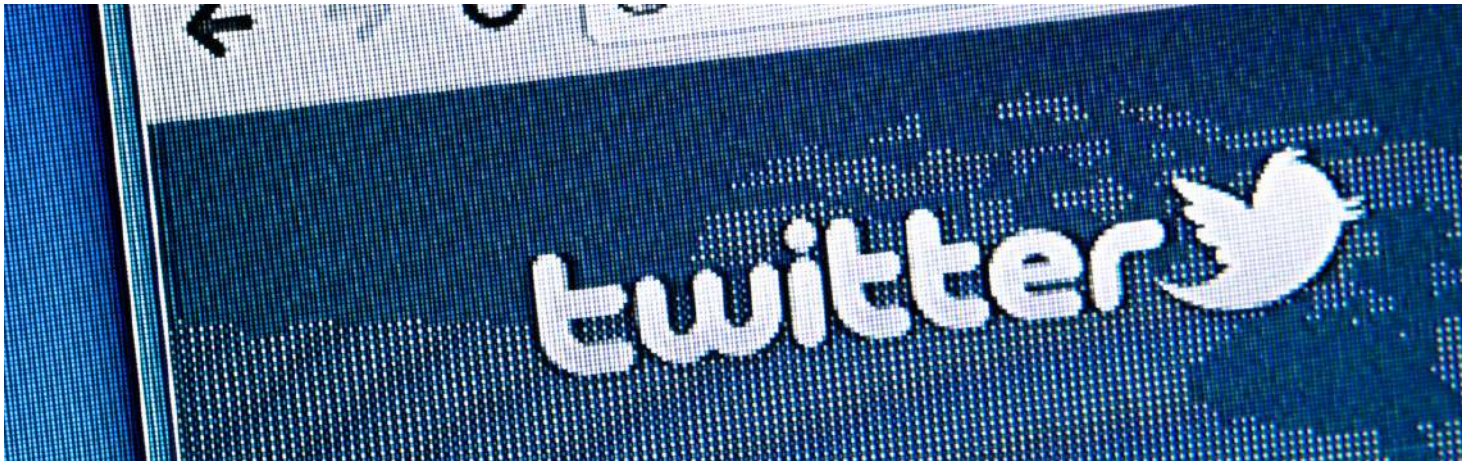
Apple co-founder Warns that AI Could Make Cyber Attacks More Sophisticated

The Artificial Intelligence race has started since the release of ChatGPT in November 2022. There have been several Artificial Intelligence bots developed by organizations all over the world.

In this rising occasion, there has been a halt in developing AI systems into more powerful ones. An open letter was signed at the end of March warning about the potential risks of having the AI systems if they are out of control.
Apple, Twitter, and Deepmind joined hands to sign this letter and agreed to train AIs for at least six months before developing them further.
In a recent interview with BBC, Steve Wozniak, Co-founder of Apple, stated that threat actors can use this technology to conduct a much more sophisticated attack on organizations.

“AI is so intelligent it’s open to the bad players, the ones that want to trick you about who they are.” said Steve to BBC.
He said he was not concerned about AI replacing people due to a lack of emotions. Instead, threat actors can conduct attacks with more convincing, strategic, and intelligent text using AI systems like ChatGPT.

Source : https://cybersecuritynews.com/apple-co-founder-warns/



Twitter Launches Encrypted Direct Messages for Verified Users

A new form of communication on Twitter called the Encrypted Direct Message has been made available by Twitter. It will appear in your inbox and regular Direct Messages as distinct conversations.

It's important to remember that the feature is now only accessible to verified Twitter users, which includes Twitter Blue subscribers and anyone who is part of a "Verified Organization."
"We employ a combination of strong cryptographic schemes to encrypt every single message, link, and reaction that are part of an encrypted conversation before they leave the sender's device, and remain encrypted while stored on Twitter's infrastructure", Twitter.
User Requirements To Send And Receive Encrypted Messages:

- Both sender and recipient are on the latest Twitter apps (iOS, Android, Web);
- Both sender and recipient are verified users or affiliates of a verified organization; and
- The recipient follows the sender or has sent a message to the sender previously, or has accepted a Direct Message request from the sender before.

Source : https://cybersecuritynews.com/twitter-encrypted-direct-messages/

Global Food Chain Company Hacked – Attackers Stole Sensitive Details

As per reports from Sysco, a leading food distribution company, had a data breach by threat actors. Sysco believes this breach started on January 14, 2023, when a threat actor gained access to their systems and claimed to have sensitive data.

Sysco sent an internal memo to all its employees on May 2nd, 2023, stating that threat actors have stolen information relating to business operations, employees, customers, and personal data (Social security numbers, account numbers, and payroll details).

“This data extraction has not impacted Sysco’s operational systems and related business functions,” Sysco stated.

The company also mentioned in the memo that they have been working with Cybersecurity and forensics professionals on investigating this event.

“Sysco initiated an forensic investigation, with the assistance of cybersecurity and forensics professionals.” Sysco’s memo reads.

The company also contacted customers who have been affected by this data breach. Over 2 months, threat actors have extracted data from their databases.

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

Beware of New Whatsapp Scam Tricking Jobs Seakers to Steal Money

WhatsApp has become one of the most widely used platforms for communication among all age groups. With the growing use of this communication platform, cybercriminals have barged in and started a new type of scamming activity.

Scamming has been very popular among threat actors to loot money from victims by cheating them. Recent reports show that threat actors have been using a new sophisticated method to scam people on a large scale.

Cyber Security consultant (Smit Kotadiya) posted and reported the scamming activity he recently identified to Cyber Security News.

This new scamming activity involves approaching the victims in the name of part-time jobs where the tasks are to like and subscribe to some youtube channels and videos.

In return, they pay you some extra money. But this is just the circumference of the larger circle.

If the victims are interested, they are given some tasks and asked to provide a screenshot after completion. Once the tasks are completed, they are redirected to a Telegram channel.

Source : https://cybersecuritynews.com/whatsapp-scam-tricking-jobs-seakers/

MSI CyberAttack – Intel Boot Guard Private Keys Leaked on the Dark Web

The private code signing keys for the multinational Taiwanese technology business Micro-Star International (MSI) Co., Ltd. have been made public on a dark website by the threat actors that launched the ransomware attack against it last month.

“Confirmed, Intel OEM private key leaked, causing an impact on the entire ecosystem,” Firmware security company Binarly’s founder and CEO, Alex Matrosov, stated in a tweet.

“It appears that Intel Boot Guard may not be effective on certain devices based on the 11th Tiger Lake, 12th Adler Lake, and 13th Raptor Lake.”

Intel BootGuard Private Keys Leaked

Reports say private signing keys for Intel Boot Guard used on 116 MSI devices and firmware image signing keys connected to 57 PCs are also included in the stolen data.

A hardware-based security mechanism, Intel Boot Guard, prevents computers from running tampered UEFI firmware.

Source : https://cybersecuritynews.com/intel-boot-guard-private-keys/

Russian Hackers Deploy Sophisticated Snake Loader Malware Worldwide

The Five Eyes member nations' cybersecurity and intelligence agencies collaborated to dismantle the infrastructure of the Snake cyber-espionage malware, originally developed by Russia's FSB, which had its roots in the Uroburos project dating back to 2003, and was deployed in attacks soon after its completion in 2004.

Operation MEDUSA, a coordinated effort by cybersecurity agencies, successfully disrupted the Snake malware associated with the Russian Turla hacking group within Center 16 of the FSB, revealing compromised devices from NATO member governments within the Snake's peer-to-peer botnet.

The Justice Department and international partners have dismantled a global network of malware-infected computers used by the Russian government for cyber espionage against NATO allies for almost 20 years.

Snake, known as the FSB's advanced long-term cyberespionage malware.

Source : https://cybersecuritynews.com/snake-loader-malware/

“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