QUALYSEC
BEYOND CYBERSECURITY

2023

DEC 4TH WEEK

CYBER SECURITY NEWS

CONTACT US

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

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/apache-struts-2-vulnerability/

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/

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/

Hackers Using Malicious JavaScript Samples to Steal Sensitive Data

Is your online data safe? A recent study by Unit 42 researchers reveals a disturbing trend: JavaScript malware is evolving, employing sophisticated techniques to steal sensitive information like passwords and credit card numbers. Unit 42 researchers are the elite cyber sleuths of Palo Alto Networks, a leading cybersecurity company.

Evading the Watchful Eye:

Traditional static and dynamic analysis methods used by security tools often struggle against these new threats.

Obfuscation, unusual DOM interactions, and selective payload detonation are just a few tricks these malicious scripts employ to fly under the radar.

Where the Data Goes:The research identified several exfiltration methods used by the malware:

- Phishing Pages: These deceptively legitimate-looking websites trick users into surrendering their information.
- Skimming Sites: Attackers inject malicious scripts into compromised websites, capturing data as users interact with them.
- Chat and Survey APIs: Abusing legitimate APIs designed for communication and data collection provides a seemingly innocuous channel for stolen information to flow.

Source : https://cybersecuritynews.com/hackers-using-malicious-javascript/

New Instagram Phishing Attack Steals 2FA Backup Codes

A new phishing campaign targeting Instagram users has been discovered, which uses several different techniques to lure victims into phishing websites and steal Instagram's two-factor backup codes. The threat actors use the "Copyright Infringement" template along with some context, creating a sense of urgency for the users to take prompt actions.

Instagram backup codes are five eight-digit codes used when users want to log in to an unrecognized device when two-factor authentication has been enabled. This list of backup codes can be regenerated when the users log into their Instagram accounts.

Instagram Phishing Attack Steals 2FA Backup Codes

According to a report by TrustWave, during the initial phase of the attack, the attackers impersonated Meta, which is the parent company of Instagram, and sent emails to multiple victims.

The email states that an Instagram account infringed copyrights and an "appeal form" must be filled in 12 hours. Failing to do so, the Instagram account will be permanently deleted according to the threat actors' email.

Source : https://cybersecuritynews.com/new-instagram-phishing-attack/

Google Chrome Zero-day Exploited in the Wild: Patch Now!

Google has released urgent upgrades to fix the Chrome zero-day high-severity vulnerability that has been widely exploited, which could lead to software crashes or arbitrary code execution.

To address the actively exploited zero-day vulnerability, the stable channel will be updated to 120.0.6099.129 for Mac and Linux and 120.0.6099.129/130 for Windows. Over the coming days and weeks, the update will be implemented.

Chrome Zero-day Bug Details- CVE-2023-7024

The CVE-2023-7024 vulnerability has been defined as a heap-based buffer overflow flaw in the WebRTC framework that might be exploited to cause software crashes or arbitrary code execution.

“Google is aware that an exploit for CVE-2023-7024 exists in the wild”, Google said.

The issue was found and reported by Clément Lecigne and Vlad Stolyarov from Google’s Threat Analysis Group (TAG).

Google withheld information regarding the attacks that took use of the vulnerability in the wild.e wild.

“Access to bug details and links may be kept restricted until a majority of users are updated with a fix. We will also retain restrictions if the bug exists in a third party library that other projects similarly depend on, but haven’t yet fixed”, Google reports.

Source : https://cybersecuritynews.com/chrome-zero-day-exploited/

Iranian Hackers Attack Telecom Companies Using Custom Tools and Living-Off-The-Land Techniques

The telecommunications companies in Egypt, Sudan, and Tanzania have been the target of the Iranian espionage group Seedworm, which is known as Muddywater.

The attack took place in November 2023, and the attackers used a range of tools, including the recently found and published MuddyC2Go infrastructure by Deep Instinct. Along with other publicly accessible and living-off-the-land tools, the attackers also use a custom keylogging tool, the SimpleHelp remote access tool, and Venom Proxy, which have been linked to Seedworm activities in the past.

MuddyC2Go Framework and Custom Keylogger Used

The attacks in this campaign, which targeted one specific telecom company, took place in November 2023. The initial indications of malicious behavior were certain PowerShell executions connected to the MuddyC2Go backdoor. According to Symantec's Threat Hunter Team, to establish a connection with its command-and-control (C&C) server, the MuddyC2Go launcher executed the following PowerShell code:The variables at the initial stage of the code seem to be there merely to try and evade detection by security software because they are irrelevant and unutilized.

Source : https://cybersecuritynews.com/iranian-hackers-attack-telecom-companies-using-custom-tools-and-living-off-the-land-techniques/

New Hacker Group Uses SQL Injection to Hack Companies in APAC Region

A new threat actor has been discovered to be using SQL injection attacks to gain unauthorized access to organizations in the APAC region.

This threat actor has been named “GambleForce” and is using publicly available open-source instruments that are generally used by penetration testers.

The threat actor has targeted more than 20 websites, including government, gambling, retail, and travel sites in Australia, China, Indonesia, the Philippines, India, South Korea, Thailand, and Brazil. Among the 20, the threat actor successfully infiltrated six organizations with the legacy SQL injection attack.

Hacker Group Uses SQL Injection

In the case of the tool configurations, no unique modifications were found as the threat actors were using almost all the default settings of all the tools they used. Some of the tools used by the threat actor include dirsearch, sqlmap, tinyproxy, redis-rogue-getshell, and Cobalt strike. As an interesting factor, the threat actor used language-based “export” commands in 95 out of 750 commands they executed on each server.

Source : https://cybersecuritynews.com/hacker-group-uses-sql-injection/

New Terrapin Attack Downgrades SSH Protocol Connection Security

SSH protocol is one of the most used protocols across several organizations to establish a remote terminal login and file transfer. SSH consists of an authenticated key exchange for establishing the secure channel connection to ensure integrity and confidentiality.

However, a new technique named “Terrapin attack” has been discovered, which will allow threat actors to downgrade the SSH protocol version, thus allowing the exploitation of vulnerable servers. Additionally, the threat actor can redirect the victim’s login into a shell under the attacker’s control.

Terrapin Attacking SSH Protocol

Terrapin attack is a kind of prefix truncation attack in which the initial encrypted packets sent through the secure SSH channel can be deleted without the server or client noticing it.

There are two root causes for this flaw; one of them is the optional messages that are allowed in the SSH handshake, which do not require authentication. Second, the SSH handshake does not reset message sequence numbers when encryption is enabled.

Source :https://cybersecuritynews.com/new-terrapin-attacking-ssh-protocol/

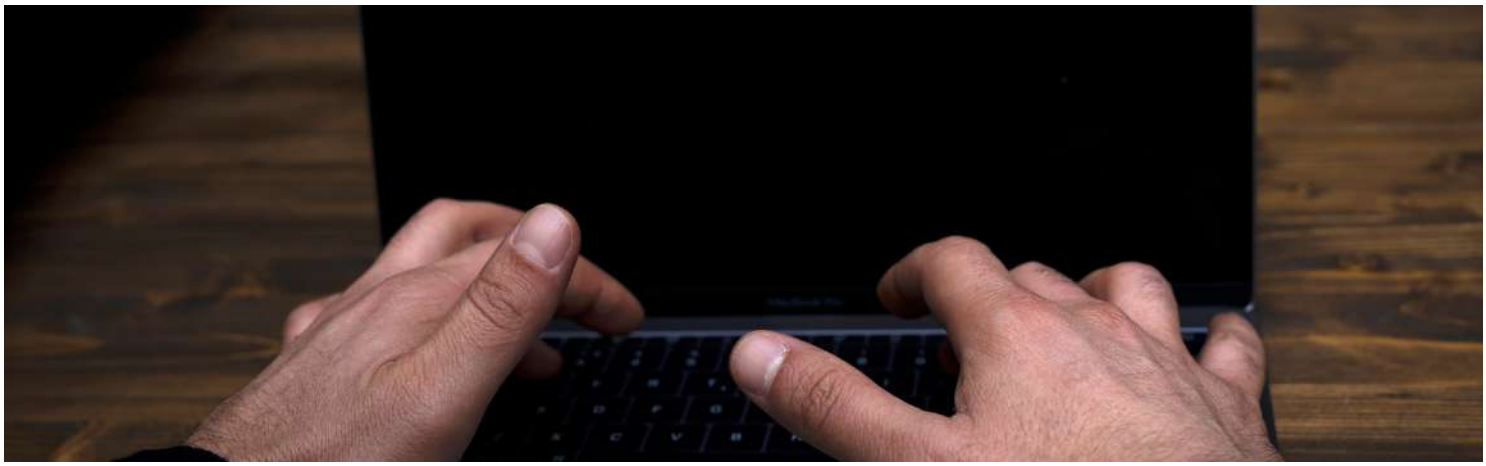
Zoom Launches Open-source Vulnerability Impact Scoring System

Zoom, the popular video conferencing platform, has recently announced the launch of its Open-Source Vulnerability Impact Scoring System.

This system is designed to provide a standardized method for evaluating the impact of vulnerabilities discovered in open-source software.

The system's version 1.0 specification has been made available to the public, which will help software developers and security researchers to better identify and prioritize vulnerabilities and take appropriate actions to mitigate them. Zoom Video Communications, Inc. is a communications technology company headquartered in San Jose, California. The company offers a cloud-based, peer-to-peer software platform that allows users to make phone calls, video conferences, send messages, host virtual events, and operate contact centers. The platform provides video telephony and online chat services. The Vulnerability Impact Scoring System (VISS) has been specifically developed to address the primary effects of software, hardware, and firmware vulnerabilities that are relevant to the connected infrastructure, technology stack, and security of customer information.

Source : https://cybersecuritynews.com/zoom-launches-open-source-vulnerability/



Hackers Actively Exploiting QNAP VioStor NVR Vulnerability to Deploy Mirai Malware

Hackers exploit QNAP devices because they often have known vulnerabilities or misconfigurations that can be exploited for unauthorized access.

Besides this, QNAP devices store valuable data, which makes them lucrative targets for threat actors seeking to:-

- Compromise sensitive information
- Deploy ransomware
- Deploy malware

Recently, cybersecurity researchers at Akamai during InfectedSlurs research identified that hackers are actively exploiting the QNAP VioStor NVR (network video recorder) vulnerability to deploy “Mirai” malware.

QNAP VioStor NVR Vulnerability

The vulnerability has been tracked as CVE-2023-47565 and marked as a “High” severity flaw with a CVSS v3 score of 8.0.

NVR is a high-performance network surveillance solution for IP cameras and this high severity vulnerability poses risks to:-

- Video recording
- Playback
- Remote data access

Source : https://cybersecuritynews.com/hackers-actively-exploiting-qnap-viostor/

Hackers are Actively Exploiting Apache Struts 2 Vulnerability

Hackers are taking advantage of a Critical Apache Struts Bug's initial activity with limited IP addresses engaged in exploitation attempts.

Apache is an open-source framework for creating Java EE web applications called Apache Struts. It is used by numerous Fortune 100 businesses and international governments.

On December 7, the Apache Foundation, which manages the Struts library, asked developers to implement a patch to address a vulnerability that allowed a path traversal attack.

This means that an attacker could gain access to directories on a web server that they shouldn't have, and in certain situations, they could upload a malicious file for remote code execution.

The vulnerability, CVE-2023-50164, has a 9.8 out of 10 CVSS score.

The Australian Cyber Security Center and CERT-FR have recently detected a wave of exploitation attacks happening across the globe.

These attacks target vulnerable systems and exploit security loopholes to gain access to sensitive data and cause potential harm.

Apache Struts 2 Vulnerability

In some cases, this can result in uploading a malicious file that can be used to carry out Remote Code Execution. An attacker can change file upload parameters to enable pathway traversal.

Source : https://cybersecuritynews.com/apache-struts-2-vulnerability/

“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