QUALYSEC
BEYOND CYBERSECURITY

2024

MAR 3RD WEEK

CYBER SECURITY NEWS

CONTACT US

🌐 www.qualysec.com

☎ 865 866 3664

✉ contact@qualysec.com

Chinese Attackers Hack American Businesses Digital Locks To Steal Sensitive Data

United States Senator Ron Wyden warned and notified the Director of the National Counterintelligence and Security Center (NCSC), Michael C. Casey, that Chinese hackers are actively backdooring digital locks to steal sensitive data.

As a result, Hackers target and backdoor the digital locks to gain unauthorized access to sensitive information and resources.

Backdooring allows hackers to maintain access even after the initial breach, facilitating the threat actors' ability to keep ongoing unauthorized activities active.

Technical AnalysisRyden urges NCSC to warn businesses about substandard commercial safe lock risks. Many have undisclosed manufacturer backdoor reset codes that are known only to makers.

According to the report, Lock companies receive demands from agencies for these codes granting safe access. Foreign threat actors could exploit the backdoors to steal trade secrets and IP stored in business safes.

The Department of Defense (DoD) emailed on November 8, 2023, that manufacturer reset codes are prohibited in approved government locks due to a threat.

Source : https://cybersecuritynews.com/chinese-hackers-digital-locks-data-theft/

Google Chrome To Roll Out Real-Time URL Protection For Malware & Phishing Attack

Google Chrome has been protecting users from malicious websites and files with Safe Browsing, which maintains a locally-stored list updated every 30-60 minutes.

It is becoming insufficient as unsafe sites can emerge and disappear within 10 minutes. To address it, Chrome is introducing a new version of Safe Browsing that provides real-time URL protection without compromising user privacy.

This is achievable through a new API that checks URLs against a real-time list without revealing the actual URLs to Google, improves protection against short-lived threats, and scales better to the growing number of malicious sites.

Real-Time And Privacy-Preserving Safe Browsing

Chrome utilizes real-time Safe Browsing to identify unsafe websites. Upon visiting a URL, it first checks its local cache for known safe addresses; if not found, the URL undergoes a real-time check.

To protect user privacy, it muddies the URL through hashing and encryption before sending it to the Safe Browsing server. The server decrypts, compares the hash with its database of unsafe URLs, and returns matching full hashes.

Source : https://cybersecuritynews.com/google-chrome-real-time-phishing-protection/

CYBER SECURITY NEWS

How to Set Up a Network Research Laboratory for Malware Analysis (SOC & DFIR Teams)

To analyze a security vulnerability (CVE-2024-21413) in Outlook, a controlled environment can be set up using a virtual machine (ANY.RUN) within a local virtual private network (VPN).

Researchers can learn more about the exploit by making a proof-of-concept (PoC) and testing its functionality in a separate environment.

During the PoC execution, tools like Impacket can be used within the VPN to record network traffic, which could reveal private data like NTLM hashes.

Analyzing this data can identify indicators of compromise (IoCs) unique to the exploit and use them to draft detection rules capable of recognizing future attacks.

Let's talk about how to set up a working environment to gather IOCs and write detection rules, using CVE-2024-21413 as an example.

Analyzing CVE-2024-21413: PoC Creation and ANY.RUN Integration in a Local VPN

Clicking a malicious link in an email exploits a vulnerability (CVE-2024-2143) in Outlook, enabling attackers to silently download and execute a file without user awareness.

It leaks the victim's NTLM hash during attempted SMB authentication, potentially granting attackers unauthorized code execution capabilities on the compromised machine.

Source : https://cybersecuritynews.com/how-to-set-up-a-network-research-laboratory/

CYBER SECURITY NEWS

Hackers Deliver FakeBat Malware via MSIX Installer Files

Cybercriminals have been distributing a new strain of malware, dubbed FakeBat, by exploiting the trust in MSIX installer files.
This alarming trend has raised concerns as it involves masquerading as legitimate software applications, including popular productivity tools like Notion, Trello, Braavos, and OneNote.
The Lure of Legitimacy
The attackers have cleverly designed their campaign to impersonate well-known software brands, thereby increasing the likelihood of users downloading and executing the malicious installers.
By leveraging the reputation of these trusted names, the cybercriminals aim to bypass the natural skepticism that users might have towards unknown sources.Camouflaged Links and Obfuscated Scripts
To further evade detection, the malvertisements have utilized URL shorteners, a common tactic for hiding the true destination of the links and making them appear less suspicious to potential victims.
Once clicked, these links lead to downloading MSIX files containing obfuscated PowerShell scripts.

Source : hhttps://cybersecuritynews.com/hackers-deliver-fakebat/

Hackers Unveiled Notorious Android Brata RAT Tool Features

A threat actor recently shared details about the Brata RAT (Remote Administration Tool) Program online.

This advanced Android remote management software raises alarms due to its extensive capabilities, which could be exploited for malicious purposes.

Advanced Evasion Techniques

The Brata RAT Program boasts various features designed to evade detection and maintain persistence on infected devices.

Notably, it includes anti-kill and anti-delete functions, making it difficult for users to remove the software once it has infiltrated their device.

One of the Brata RAT's most invasive features is its real-time monitoring capability. This allows threat actors to track the activities of a compromised device as they occur, potentially capturing sensitive personal and financial information.

Banking Security Bypass

Alarmingly, the Brata RAT can reportedly bypass the application screens of banking apps. This suggests that the tool could circumvent security measures by financial institutions, leading to unauthorized access to users' banking details.

Source : https://cybersecuritynews.com/android-brata-rat-tool-features/

CYBER SECURITY NEWS

Hackers Abuse Venmo Payment Service to Steal Login Details

Venmo, a mobile payment service owned by PayPal, has become a household name in the United States. It facilitates a convenient way for friends to exchange money and for businesses to transact with customers.

With significant year-over-year growth, Venmo reported a total payment value of $68 billion in Q3 of 2023, according to Statista, ranking it among the top three payment brands in the U.S. However, with over 62.8 million active users, the platform has inevitably attracted the attention of cybercriminals.

Phishing Scams: A Persistent Threat

Historically, PayPal has been a target for phishing scams, and now its subsidiary, Venmo, is facing similar threats.

Hackers have been crafting deceptive emails that mimic official Venmo communication, tricking users into calling fraudulent phone numbers to rectify false charges.

Harmony Email researchers have identified this new wave of attacks and alerted Venmo on February 13th.

One such email informs the recipient of a $99.99 payment to Coinbase via Venmo, which the user knows to be incorrect.

Source :https://cybersecuritynews.com/hackers-abuse-venmo-payment/

CYBER SECURITY NEWS

Gitgub Campaign Attacking GitHub Users To Steal Login Credentials

Threat actors often target GitHub users due to the plenty of valuable code repositories and sensitive information stored on the platform.

However, the collaborative nature of GitHub makes it an exceptional target for surveillance by threat actors seeking to gather intelligence on organizations and their development practices.

Cybersecurity analysts at G Data Defense recently discovered that threat actors are actively attacking GitHub users to steal login credentials via the Gitgub campaign.

Gitgub Campaign Attacking GitHub Users

RisePro employs encrypted strings and bloated installers crashing reverse-engineering tools. “Gitgub” exfiltrated over 700 data archives to Telegram. 13 repos from this RisePro stealer campaign featured the README lures. While the fake green Unicode circles mimicked build statuses for recency illusion. Red and green circles usually indicate real build outcomes on GitHub.The following download link remains the same across repos:- hxxps://site/INSTALLER%20PASSWORD.rar The user unpacks nested archives with “GIT1HUB1FREE” password. While the Installer_Mega_v0.7.4t.msi is the first executable.

Orca shows it unpacks the next stage using the “LBjWCsXKUz1Gwhg” password, and the final payload is “Installer-Ultimate_v4.3e.9b.exe.

Source : https://cybersecuritynews.com/gitgub-campaign-steals-github-credentials/

CYBER SECURITY NEWS

DarkGPT – AI OSINT Tool to Detect Leaked Databases

AI (Artificial Intelligence) systems can process large amounts of data and uncover threats that human beings might overlook.

This makes quick action possible, as AI can monitor network traffic, user activities, and system logs and identify abnormal actions, intrusions, and cyberattacks.

As many cybersecurity tasks could be automated. Not only this even, it also improves efficiency, and due to this, there is less probability of human mistakes.

A Spanish pentester with a “luijait” alias on Github recently unveiled an AI OSINT tool dubbed “DarkGPT” that helps detect leaked databases.

DarkGPT – AI OSINT Tool

Based on GPT-4-200K, DarkGPT is an AI (Artificial Intelligence) assistant that can run queries on databases that have been compromised.

Its ability to learn and adapt is another important advantage of AI in cybersecurity.

On the other hand, as new threats come up, AI systems may be trained to identify and respond to these threats.

Source : https://cybersecuritynews.com/darkgpt-ai-osint-tool/

CYBER SECURITY NEWS

Emerging Threat: Rabbit Hole Ransomware Group Unveiled

Cybersecurity experts have raised the alarm over a newly identified ransomware group, “Rabbit Hole,” which has been making headlines for its sophisticated attacks and elusive tactics.

DarkWebInformer, a reliable source for dark web and cybercrime news, first reported the group’s activities.

Origins and Discovery

The Rabbit Hole ransomware group was discovered after coordinated attacks on various high-profile targets

Initial analysis suggests that the group has been active for several months. Still, it has only recently come to the attention of cybersecurity firms due to the unique signature of its ransomware strain Rabbit Hole’s approach involves a multi-layered attack strategy, including phishing campaigns, software vulnerability exploitation, and advanced encryption to lock victims’ data.

Unlike other ransomware groups, Rabbit Hole is known for its selective targeting and customized ransom demands based on the victim’s financial capacity and the perceived value of the encrypted data. According to a recent tweet by Dark Web Informer, a new ransomware group called Rabbit Hole has been identified. Fortunately, no victims have been reported yet.

Source :https://cybersecuritynews.com/rabbit-hole-ransomware/

GhostRace Attack: Major CPU and Software Giants Flaw Let Attackers Steal Passwords

Race conditions arise when there is no insufficient synchronization with a shared resource allowing multiple threads to access it simultaneously.

The use of synchronization primitives such as mutexes, spinlock, etc. prevents these race conditions,

However, researchers have discovered a new race condition called “GhostRace ” which bypasses these synchronization primitives on speculatively executed code paths and performs a race condition on critical regions.

Additionally, these race conditions focussed on Speculative Concurrent Use-After-Free (SCUAF) conditions alongside 1283 potentially exploitable vulnerabilities present in the Linux Kernel.

GhostRace Attack

According to the reports shared with Cyber Security News, GhostRace is the first systematic analysis of Speculative Race Conditions (SRCs), a new class of speculative execution vulnerabilities that affect all common synchronization primitives.

Source : https://cybersecuritynews.com/ghostrace-attack/

CYBER SECURITY NEWS

Hackers using Weaponized PDF Files to Deliver Remcos RAT

Cybercriminals have launched a sophisticated campaign targeting individuals and organizations across Latin America, utilizing weaponized PDF files to deploy dangerous Remote Access Trojans (RATs) such as Remcos.

This alarming development has raised concerns about cybersecurity preparedness in the region.

Attack Method

According to ANY.RUN analysis attackers initiate the infection by impersonating Colombian government agencies and sending out PDF documents that falsely accuse recipients of traffic violations or other legal issues.

These documents contain links that, when clicked, prompt the download of a ZIP file.

This file includes a Visual Basic Script (VBS) obfuscated with dead code to evade detection.

The campaign cleverly masquerades as official communication from entities like the COLOMBIANA DE MUNICIPIOS, leveraging the trust in government institutions to deceive victims.

Source : https://cybersecuritynews.com/hackers-using-weaponized/

Researchers Uncover SnakeKeylogger Attacks, Techniques & Tactics

Threat actors use keyloggers to capture sensitive information by recording keystrokes on infected devices, as covert techniques and tactics allow them to steal valuable information without the victim's knowledge.

Governments or threat actors can deploy Keyloggers as espionage tools to gather intelligence or monitor their targets.

Recently, the cybersecurity researchers at Splunk Threat Research Team unveiled SnakeKeylogger attacks, techniques, and tactics.

SnakeKeylogger Attack Techniques

Snake Keylogger steals credentials and logs keystrokes. It was developed in .NET and captures screenshots, clipboard data, browser credentials, and system information.

It uses FTP, email, and Telegram for data exfiltration. Diverse C2 infrastructure enhances the operational effectiveness against traditional defenses.

Snake Keylogger spreads through phishing and obfuscates code with cryptors/loaders to evade sandboxes. This loader parses .RSRC entry name computes the SHA256 hash of the key string for AES-ECB decryption of encrypted .RSRC payload.

Source : https://cybersecuritynews.com/researchers-uncover-snakekeylogger/

Hackers Use TMChecker Remote Access Tool to Attack Popular VPN & Mail Servers

A new tool has surfaced on the Dark Web, signaling a shift in cybercriminals' methods for gaining unauthorized remote access to corporate networks.

TMChecker, a tool recently identified by ReSecurity, is designed to attack remote-access services and popular e-commerce applications.

It combines corporate access login checking capabilities with a brute-force attack kit.

Developed by a threat actor known as "M762" on the XSS cybercrime forum, TMChecker is available on a monthly subscription basis for $200.

This tool is a step ahead of its counterparts like "ParanoidChecker," targeting corporate remote access gateways, often the primary intrusion vectors for ransomware infections and other high-level attacks.

According to a report by ReSecurity, TMChecker supports 17 different services, including various VPN solutions, enterprise mail servers, database management tools, and e-commerce platforms.

Source :https://cybersecuritynews.com/arubaos-remote-code-execution-flaw/

Beware of Malicious Notepad++ Websites that Attack Developers

Threat actors target Notepad++ as it is a widely used text editor among developers and users, offering a large potential victim pool.

Exploiting vulnerabilities in Notepad++ can provide access to sensitive data or even systems as well.

Besides this targeting popular software increases the likelihood of successful attacks and intensifies the impact.

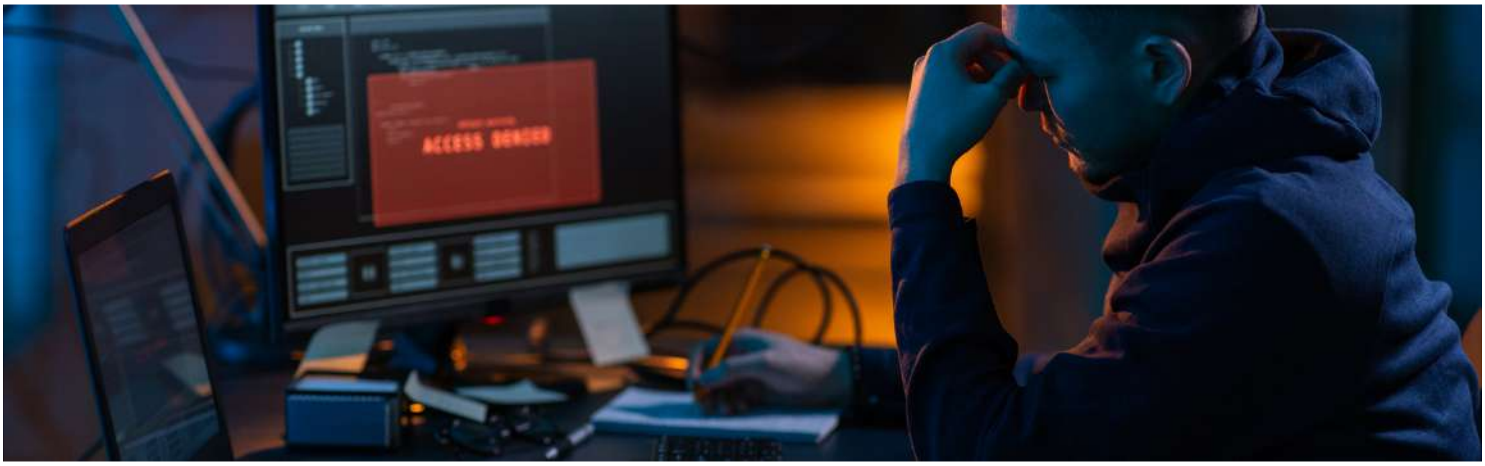
Cybersecurity researchers at Kaspersky Lab recently discovered that threat actors are actively targeting and attacking developers via malicious Notepad++ websites.

Technical analysis

Malvertising lures victims via malicious ads atop search results, as the top results seem trustworthy.

Last year, RedLine stealer spread via Google Ads malvertising campaign using typosquatting. A similar threat now affects major Chinese search engines. Threat actors are distributing modified versions of text editors, one via ad section, another atop results. The malicious Notepad++ site uses an ad block.The site has amusing inconsistencies – the URL mentions “vnote”, the title offers “Notepad–” (Notepad++ analog), and the image shows Notepad++.

Source :https://cybersecuritynews.com/beware-of-malicious-notepad/



Nissan Hack: 10K+ Users Data Stolen by Hackers

Nissan Motor Corporation and its financial services in Australia and New Zealand, collectively known as Nissan Oceania, have been the victims of a malicious cyberattack, compromising the personal information of over 10,000 individuals.

This incident, which came to light on December 5, 2023, has raised serious concerns about data security and the protection of personal information.

Nissan Oceania disclosed that an unauthorized third party accessed its local IT servers, prompting an immediate response to contain the breach.

Since then, the company has been working closely with government authorities, including the Australian and New Zealand national cyber security centers and privacy regulators, to assess the damage and implement measures to mitigate the impact on affected individuals.

The compromised data includes a wide range of personal information, affecting Nissan customers and its associated brands, dealers, and even some current and former employees.

The breach has potentially exposed sensitive information, including government identification numbers, Medicare cards, driver's licenses, passports, and tax file numbers.

Source : https://cybersecuritynews.com/nissan-hack-10k-users-data-stolen-by-hackers/

OpenCTI With ANY.RUN: OSINT Platform to SOC & MDR Teams for Malware Analysis

ANY.RUN integrates with OpenCTI to streamline threat analysis, which allows enriching OpenCTI observations with data directly from ANY.RUN analysis.

OpenCTI is a central hub that collects threat data from various sources, like ANY.RUN, through connectors, stores this data as "observations," including indicators like file hashes and IP addresses.

ANY.RUN is a cloud-based malware analysis sandbox that assists security teams in investigating suspicious files that utilizes YARA and Suricata rules for initial detection within 40 seconds and offers real-time interaction with the virtual environment.

It allows analysts to bypass automated malware techniques and delve deeper into analyzing sophisticated threats and its cloud-based nature also eliminates setup and maintenance burdens for security teams.

"ANY.RUN released connectors for MITRE ATT&CK techniques and tactics, an ANY.RUN TI Feeds connector that imports data into OpenCTI once every 24 hours, and an ANY.RUN sandbox connector that you can use to enrich observations with data from sandbox analysis tasks, like malware family labels and maliciousness scores."

Source : https://cybersecuritynews.com/opencti/

CYBER SECURITY NEWS

Google’s Gemini AI Vulnerability let Hackers Gain Control Over Users’ Queries

Researchers discovered multiple vulnerabilities in Google’s Gemini Large Language Model (LLM) family, including Gemini Pro and Ultra, that allow attackers to manipulate the model’s response through prompt injection. This could potentially lead to the generation of misleading information, unauthorized access to confidential data, and the execution of malicious code.

The attack involved feeding the LLM a specially crafted prompt that included a secret passphrase and instructed the model to act as a helpful assistant.

Researchers could trick the LLM into revealing the secret passphrase, leaking internal system prompts, and injecting a delayed malicious payload via Google Drive by manipulating the prompt and other settings.

According to HiddenLayer, these findings highlight the importance of securing LLMs against prompt injection attacks. These attacks can potentially compromise the model’s integrity and lead to the spread of misinformation, data breaches, and other harmful consequences.

Source : https://cybersecuritynews.com/googles-gemini-ai-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

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