QUALYSEC
BEYOND CYBERSECURITY

2024

JAN 2ND WEEK

CYBER SECURITY NEWS

CONTACT US

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

Babuk Ransomware Decryptor Updated to Recover Files Infected by Latest Variant

Hackers use ransomware to encrypt victims' files and render them inaccessible until a ransom is paid. This forces the victims to pay a ransom to regain access to compromised systems and data.

This tactic leads to financial gains for the threat actors. While ransomware attacks can be conducted at scale and threat actors can target individuals, businesses, and organizations.

The Babuk ransomware decryptor has recently received an update from Avast cybersecurity researchers, Cisco Talos, and the Dutch Police to allow for the recovery of files infected with the most recent ransomware variant.

Technical Analysis

Babuk ransomware initially emerged in early 2021, and it is known for the following key things:-

- Targeting Windows systems
- Encrypting files
- Demanding ransom payments in exchange for decryption keys

Besides this, Babuk ransomware has gained immense attention for its Evolving tactics and the sophistication of its attacks.

Source : https://cybersecuritynews.com/babuk-ransomware-decryptor-updated/

22-yr Old Hacker from ShinyHunters Group Arrested for Hacking 60+ Organizations

A 22-year-old French citizen, Sebastian Raoult, has been sentenced to three years in prison and ordered to pay over $5 million in restitution for his role in a sprawling cybercrime ring that hacked and exploited the data of millions across the globe.

Raoult, also known online as “Sezyo Kaizen,” was apprehended in Morocco in 2022 and extradited to the United States to face justice for his multi-layered scheme.

U.S. Attorney Sarah Vogel emphasized the gravity of Raoult’s actions, stating that he “robbed people of millions of dollars.”

This wasn’t just a technical exploit but a calculated act of financial plunder.

Beyond Stolen Data, Stolen Lives:

Vogel further highlighted the broader impact, noting the “unmeasurable additional losses to hundreds of millions of individuals whose data was sold to other criminals.”

Raoult’s actions put countless people at risk of identity theft, financial fraud, and other forms of harm.

Raoult and his co-conspirators targeted businesses worldwide, including companies in Washington State.

Source https://cybersecuritynews.com/hacker-from-shinyhunters-group/

Hackers Impersonating as Security Researcher to Aid Ransomware Victims

Hackers impersonate security researchers to exploit trust and credibility. By posing as legitimate figures in the cybersecurity community, they:

- Gain access to sensitive information
- Manipulate victims into compromising actions
- Enhance the success of their malicious activities while evading suspicion

Cybersecurity researchers at Arctic Wolf Labs recently discovered that hackers are actively impersonating security researchers to aid ransomware victims.

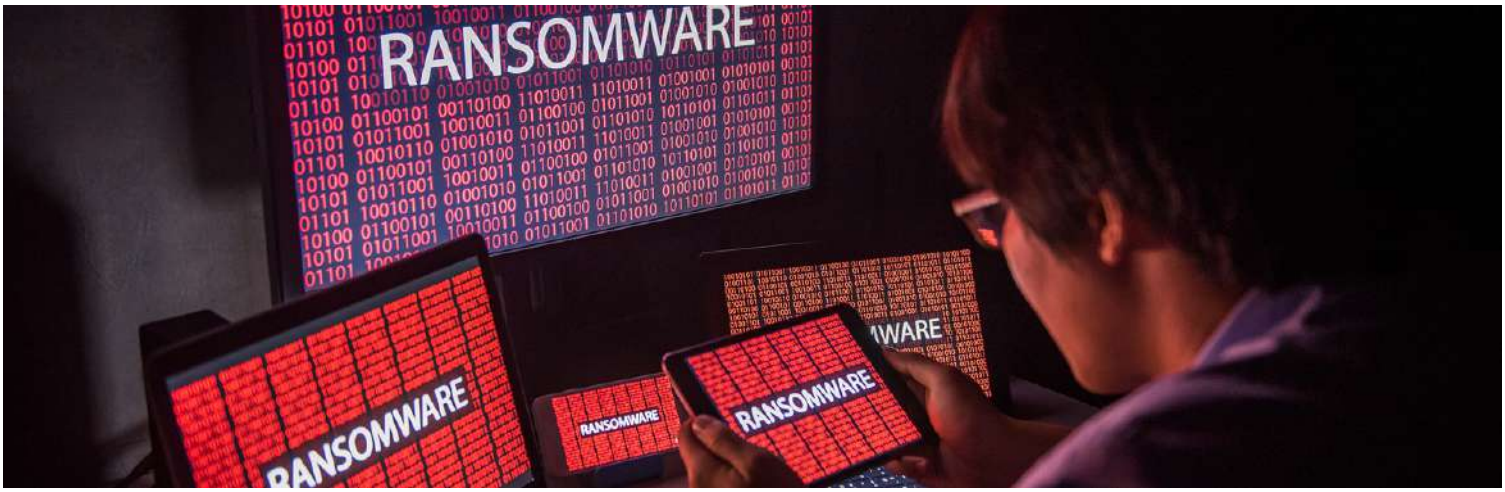
Technical Analysis

Arctic Wolf Labs researchers found ransomware victims getting extorted again, with fake 'helpers' promising to delete stolen data.

They posed as security researchers in two cases, offering to hack the original ransomware group's servers. This is the first known case of a threat actor pretending to be a legitimate researcher and offering to delete hacked data from another ransomware group.

Despite different personalities, the security analysts believe it's likely the same actor behind both extortion attempts. Despite appearing distinct, both cases share key elements. Analyzing their communication styles revealed clear similarities.

Source :https://cybersecuritynews.com/hackers-impersonating-as-security-researcher/



Microsoft Patch Tuesday 2024 Released with Fixes for 49 vulnerabilities – Update Now!

Microsoft released its first patch on Tuesday, 2024, in which nearly 49 vulnerabilities have been fixed in Microsoft products and 5 vulnerabilities in non-Microsoft products. Among these 49 vulnerabilities, there were 12 remote code execution vulnerabilities.
However, only two vulnerabilities were categorized as critical by Microsoft, which were CVE-2024-20674 and CVE-2024-20700. These two vulnerabilities were found to be related to the security feature bypass.

Vulnerability Analysis

According to the reports shared with Cyber Security News, several vulnerabilities existed in different Microsoft products,, including Microsoft Server, .NET framework, Azure Storage Movement, Visual Studio, Identity Model, Microsoft Office, and many others.
The vulnerabilities were categorized as the following:
Elevation of Privilege (10), Security Feature Bypass (7), Denial of Service (6), Remote Code Execution (12), Spoofing (3) and , Information Disclosure (11)

Source :https://cybersecuritynews.com/microsoft-patch-2024-addresses-49-vulnerabilities/

Critical Cisco Unity Connection Flaw Let Attackers Run Command as Root User

A critical vulnerability of severe severity has been found in Cisco Unity Connection's web-based management interface.

This flaw might allow a remote, unauthenticated attacker to upload arbitrary files to a compromised system and run commands on the underlying operating system.

With its various message access choices, Cisco Unity Connection is a powerful unified messaging and voicemail solution that helps you collaborate more quickly.

Cisco has published software upgrades to address this critical vulnerability. There are no workarounds for this vulnerability.

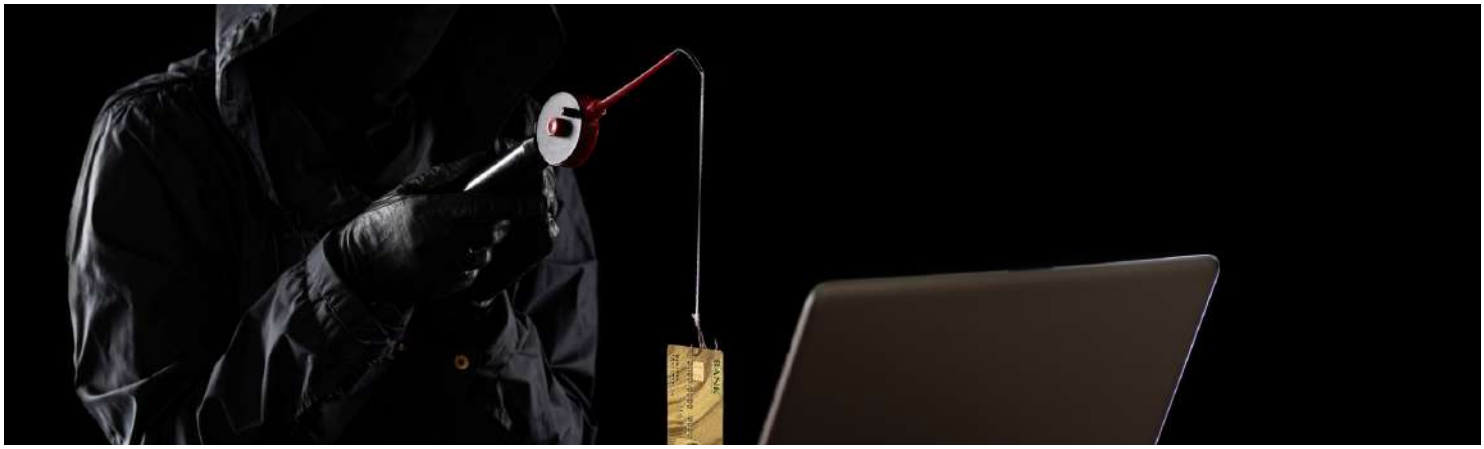
unauthenticated Arbitrary File Upload Vulnerability

With a CVSS score of 7.3, the Cisco unity connection unauthenticated arbitrary file upload vulnerability is tracked as CVE-2024-20272.

"A vulnerability in the web-based management interface of Cisco Unity Connection could allow an unauthenticated, remote attacker to upload arbitrary files to an affected system and execute commands on the underlying operating system," Cisco said.

"This vulnerability is due to a lack of authentication in a specific API and improper validation of user-supplied data."

Source : https://cybersecuritynews.com/critical-cisco-unity-connection-flaw/



SAP Security Patch Addresses Privilege Escalation Flaw

SAP is a leading enterprise software suite that integrates various business functions like:-

- Finance
- Human resources
- Supply chain management

This renowned enterprise software suite helps organizations to:-

- Streamline processes
- Enhance efficiency
- Make data-driven decisions

Recently, on a security note, the German multinational software company SAP released a security patch for vulnerabilities like privilege escalation flaws discovered in SAP products.

SAP Security Patch

To protect the SAP landscape, SAP urged customers to visit the SAP Support Portal immediately and apply the newly released security patches.

Ensure SAP software security through regular SAP Security Patch Days every second Tuesday synchronized with major vendors.

Source :https://cybersecuritynews.com/sap-security-patch-2024/

HPE Announces Acquisition of Juniper Networks for $14 Billion

The union of Juniper Networks and HPE marks a bold leap forward in the age of AI-powered networking.

Their combined focus transcends mere products, aiming to deliver complete, synergistic solutions that empower businesses across diverse sectors.

Juniper recognizes AI as the most transformative force since the internet's dawn, impacting every facet of life and revolutionizing the technology landscape.

Seven years ago, they embraced this opportunity, pioneering AIOps to streamline network operations, boost deployments, and crush tedious troubleshooting.

This proactive stance has yielded impressive results, with AI-powered product revenue experiencing a near 100% year-over-year growth for the past two quarters.

Their investments in AI-enabled data centers are also showing early promise, positioning them for potential dominance in this emerging field.

All In on AI: The HPE Merger Catalyst:

Juniper's "AI" stands for "All In," and their commitment to harnessing this transformative power manifests in their definitive agreement to be acquired by HPE.

Source :https://cybersecuritynews.com/hewlett-packard-enterprise-acquisition-of-juniper-networks/

SEC X Account Hacked to Publish Bitcoin ETFs Approval Message

In a scene ripped from a digital thriller, the U.S. The Securities and Exchange Commission (SEC) saw its Twitter account hijacked by an unknown entity, plunging the crypto world into a roller coaster ride of frenzied excitement and crushing disappointment.

The perpetrator unleashed a fabricated announcement claiming approval of Bitcoin Exchange Traded Funds (ETFs), a long-awaited development that ignites fervent anticipation within the cryptocurrency space.

The fraudulent tweet, crafted to resemble an official SEC pronouncement, spread like wildfire through social media, fueled by its tantalizing message.

This ambitious move aims to supercharge their offerings in AI-native networking, accelerating innovation across all layers: compute, storage, hardware, software, and network infrastructure.

Further investigation by X revealed the attacker's modus operandi: they gained control of a phone number associated with the SEC's account through a third-party service.

Source : https://cybersecuritynews.com/sec-x-account-hacked-to-publish-bitcoin/

Hackers Exploiting Poorly Unsecured MS SQL Servers Across the Globe

An ongoing threat campaign dubbed RE#TURGENCE has been observed, which involves targeting MS SQL servers in an attempt to deliver a MIMIC ransomware payload.

Turkish threat actors with financial motivations seem to be aiming after the US, EU, and LATAM nations.

“The analyzed threat campaign appears to end in one of two ways, either the selling of “access” to the compromised host or the ultimate delivery of ransomware payloads” ” the Securonix Threat Research team shared with Cyber Security News.

Specifics of Turkish Hackers Targeting MSSQL Servers

Researchers used the xp_cmdshell procedure to brute force access to the victim server and execute commands on the host.

This procedure should not be enabled; it is usually disabled by default (particularly on publicly exposed servers).

The campaign’s initial access phase is comparable to that of DB#JAMMER, which similarly used brute forcing administrative credentials to gain direct MSSQL access. Following their successful execution of code via the xp_cmdshell method, the attackers ran the command from the sqlservr.exe process on the server. This command helps to execute a PowerShell-encoded command, which is then decoded.

Source : https://cybersecuritynews.com/hackers-ms-sql-servers/

Sea Turtle APT Group Exploiting Known Vulnerabilities to Attack IT-service Providers

To obtain access to a variety of clients' systems and data in a single attack, hackers frequently target IT service providers.

Their strategy lets them maximize the effect of their efforts by allowing them to compromise several organizations from a single point of entry.

Cybersecurity security researchers at Hunt & Hackett recently discovered that the Turkish espionage APT group Sea Turtle has been actively exploiting the known vulnerabilities to attack IT service providers.

Sea Turtle APT Group

Sea Turtle APT group has been active since 2017 and is known for DNS hijacking; it adapts to evade detection.

Evading detection, Microsoft exposed SILICON in Oct 2021, aligning with Turkish interests. Not only that, even in 2022, the Greek National CERT shared the IOCs.

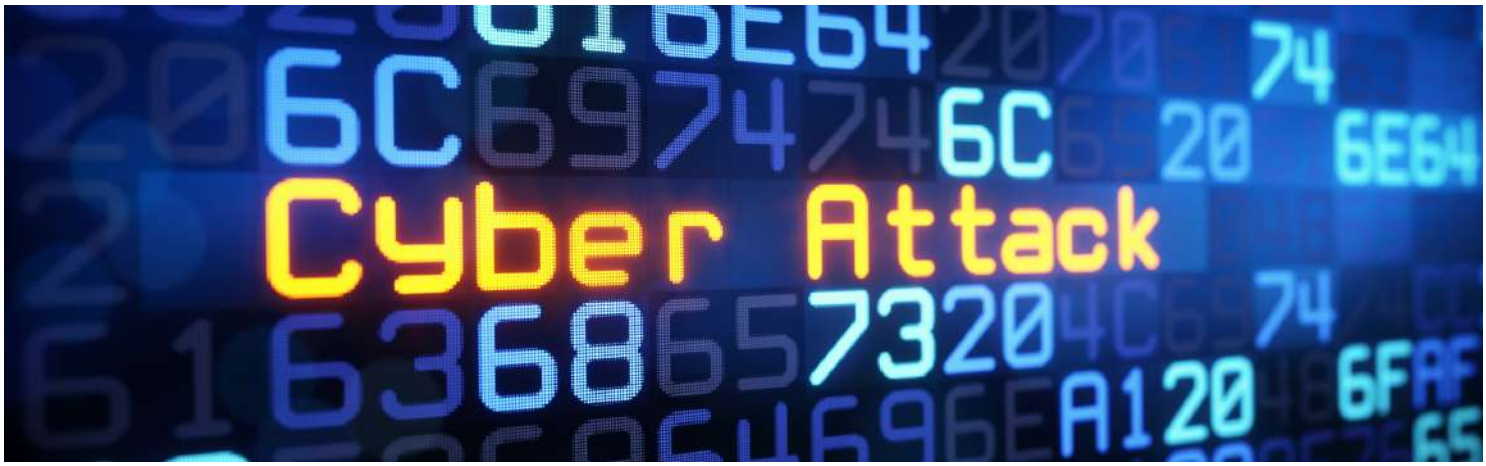
For sensitive data, Sea Turtle targets the following areas:-

Europe, Middle East, North Africa

Here below, we have mentioned all the sectors and entities targeted:-

- Gov't bodies, Kurdish groups, NGOs, Telecom, ISPs, IT, Media

Source : https://cybersecuritynews.com/sea-turtle-apt-group/



Critical Apache OFBiz Zero-day Flaw Exploited in the Wild

Researchers uncovered a critical authentication bypass zero-day flaw tracked as CVE-2023-51467, with a CVSS score of 9.8 affecting Apache OFBiz's open-source enterprise resource planning (ERP) system.

The vulnerability allows attackers to bypass simple Server-Side Request Forgery (SSRF) authentication.

The pre-authenticated RCE vulnerability tracked as CVE-2023-49070 leads to the zero-day SSRF vulnerability CVE-2023-51467 in Apache OFBiz due to an incomplete patch.

"The security measures taken to patch CVE-2023-49070 left the root issue intact, and therefore, the authentication bypass was still present", the SonicWall threat research team shared with Cyber Security News.

The vulnerability CVE-2023-49070 stems from an outdated, no-longer-maintained XML-RPC component within Apache OFBiz.

Source : https://cybersecuritynews.com/critical-apache-ofbiz-zero-day-flaw/

Silver RAT Evades Anti-viruses to Hack Windows Machines

Hackers use Remote Access Trojans (RATs) to gain unauthorized access and control over a victim's computer remotely.

These malicious tools allow hackers to perform various malicious activities like the following without the user's knowledge:-

- Execute commands
- Steal sensitive information
- Unauthorized access
- Unauthorized manipulation

Recently, cybersecurity researchers at Cyfirma discovered Silver RAT, which evades anti-virus software to hack Windows machines.

Silver RAT, which is written in C sharp, has the following capabilities:-

- Bypass anti-viruses
- Covertly launch hidden applications
- Covertly launch browsers
- Covertly launch keyloggers

Silver RAT Evades Anti-viruses

Developers active on hacker forums and social media, especially on Telegram, to offer services like:-

- Cracked RATs, Leaked databases, Carding, Social media bot sales

Silver RAT v1.0 was initially seen in November 2023

Source : https://cybersecuritynews.com/silver-rat-evades-anti-viruses/

“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