QUALYSEC
BEYOND CYBERSECURITY

2024

FEB 4TH WEEK

CYBER SECURITY NEWS

CONTACT US

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

Hijacked PyPI Package Installs NovaSentinel Stealer on Windows

Researchers identified a sophisticated cyberattack through a dormant Python Package Index (PyPI) package named Django-log-tracker, which was unexpectedly updated to deploy the NovaSentinel stealer malware.

This discovery highlights a significant threat to the software supply chain, emphasizing the need for heightened security measures among developers and organizations.

The django-log-tracker package, initially published in April 2022, remained inactive until a suspicious update on February 21, 2024, caught Phylum's attention. The update's divergence from the package's GitHub repository activity suggested a potential compromise of the developer's PyPI account. This incident marks a concerning trend of attackers targeting dormant packages to execute supply chain attacks.The malicious update stripped the package to its bare essentials, leaving only an __init__.py and example.py file, both containing identical, malicious code. Four sites on VirusTotal marked the exe as dangerous. We can easily get the binary's data out because it turns out to be an NSIS launcher when we look at it in more detail. It has an Electron app inside.

Source : https://cybersecuritynews.com/hijacked-pypi-package-installs-novasentinel-stealer-on-windows/

Windows Malware Dropped From Fake Software Developers Job Offers Scheme

February 24, 2024 – Phylum, a leader in cybersecurity research, has unveiled a sophisticated malware campaign aimed at software developers seeking employment.

This alarming scheme, identified in collaboration with Palo Alto Network's Unit 42, involves fake developer job offers that serve as a conduit for delivering malware onto unsuspecting victims' Windows systems.

You can analyze such malware files, networks, modules, and registry activity with the ANY.RUN malware sandbox, and the Threat Intelligence Lookup which will let you interact with the OS directly from the browser. The campaign, linked to North Korean actors, leverages obfuscated JavaScript and has been tied to the notorious BeaverTail malware. This revelation is part of Phylum's ongoing efforts to safeguard the open-source ecosystem from malicious actors.

The company's latest findings spotlight an npm package, masquerading as a code profiler that installs malicious scripts designed to steal cryptocurrency and credentials.

According to the Phylum report shared with Cyber Security News, The attackers ingeniously hid their malware within a test file, exploiting the common oversight of developers to scrutinize such code for threats. This tactic, however, contained critical flaws that enabled Phylum's

Source: https://cybersecuritynews.com/malware-from-fake-software-developers-job-offers-scheme/

New Wi-Fi Authentication Bypass Flaw Puts Enterprise and Home Networks at Risk

Security researchers Mathy Vanhoef and Héloïse Gollier, have recently uncovered several critical vulnerabilities in the Wi-Fi authentication protocols used in modern WPA2/3 networks collaborating with VPN testing company Top10VPN.

The identified flaws pose a significant security risk as they could potentially enable unauthorized access to sensitive data transmitted over wireless networks and compromise the security of all connected devices.

The vulnerabilities are present in two commonly used open-source Wi-Fi implementations – wpa_supplicant and Intel's iNet Wireless Daemon (IWD).

Wpa_supplicant is a widely used software that offers robust support for WPA, WPA2, and WPA3 security protocols. It is an integral part of the Android operating system and is also present in most Linux-based devices, including the ChromeOS used in Chromebooks.

iNet wireless daemon (IWD) is a wireless daemon designed by Intel for Linux-based devices. It offers a complete and robust Wi-Fi connectivity solution, providing advanced features such as advanced roaming, WPA/WPA2 support, and power management. It is a highly reliable and efficient solution for wireless connectivity on Linux devices .Two Security Flaws. As researchers were examining the system for logical implementation flaws, they came across two distinct vulnerabilities that require immediate attention. They published a research article outlining the technical weaknesses.

Source : https://cybersecuritynews.com/new-wi-fi-authentication-bypass-flaw/

Huge Surge In Attacks Exploiting User Credentials To Hack Enterprises

There are currently billions of compromised credentials available on the Dark Web, making it the easiest route for criminals to exploit legitimate accounts.

Info-stealing malware, which is meant to obtain personally identifiable information such as email addresses, passwords for social networking and messaging apps, bank account information, cryptocurrency wallet data, and more, is expected to increase 266% in 2023.

This indicates that attackers were investing greater resources in identity theft.

Major attacks triggered by attackers using legitimate accounts required approximately 200% more sophisticated response procedures from security teams than the average incident, with defenders having to discern between legitimate and malicious user behavior on the network.

This extensive monitoring of users' online behavior was made clear when the FBI and European law enforcement took down a global criminal forum in April 2023, gathering the login credentials of over 80 million accounts.

Source : https://cybersecuritynews.com/user-credentials-hack-enterprises/

Researchers Unveild Apple's Shortcuts Vulnerability

Researchers uncovered the vulnerability in Apple's Shortcuts application, which could leave users' privacy at risk. This vulnerability highlights the importance of maintaining constant and rigorous security measures to protect sensitive data.

The vulnerability, CVE-2024-23204, has raised concerns due to the widespread use of Shortcuts for automating tasks across macOS and iOS devices.

The Nature of CVE-2024-23204

Shortcuts, a powerful automation tool by Apple, allows users to create personalized workflows to streamline tasks and enhance productivity.

These shortcuts can be distributed through various channels, including Apple's gallery, where users can discover and share automation workflows.

However, CVE-2024-23204 exposes a critical flaw in this sharing mechanism, potentially allowing malicious shortcuts to exploit user data without their knowledge.

The vulnerability has a CVSS score 7.5, indicating a high severity level. It primarily concerns how Shortcuts handles permissions, allowing a shortcut to use sensitive data with specific actions without prompting the user.

Source : https://cybersecuritynews.com/apples-shortcuts-vulnerability/

LockBit Gang Money Flow Uncovered : New Strain Under Development

Over the past few years, LockBit, a ransomware-as-a-service (RaaS) operation, has been linked to multiple security incidents affecting organizations worldwide.

Yet, they appear to have experienced a lot of logistical, technological, and reputational issues recently. Due to this, LockBit had to decide to act and begin developing a much-needed version of their malware.

The new version of the ransomware that is still under development and is identified as LockBit-NG-Dev (NG for Next Generation) might ultimately be considered a true 4.0 version by the group.

Particularly, the NCA and FBI declared on Tuesday that the law enforcement operation, known as Operation Cronos, had taken over LockBit's administration system and infrastructure, took its dark-web leak site, accessed its source code, seized approximately 11,000 domains and servers, and gathered member information.

The New LockBit-NG-Dev VersionResearchers at TrendMicro have obtained a sample that they believe to be the latest version of LockBit. This malware variant is distinct from other iterations and is still in development.Since the sample appends a "locked_for_LockBit" suffix to encrypted files, it is believed that this is a forthcoming, undeployed version from the group because it is still subject to change as part of the configuration.

Source : https://cybersecuritynews.com/lockbit-gang-new-ransomware-version/

ScreenConnect Security Flaw Exploited In The Wild By Attackers

The ScreenConnect software is a popular choice for remote access among organizations worldwide. However, recent vulnerabilities have raised concerns about potential exploitation by attackers.

Specifically, these vulnerabilities could allow attackers to access vulnerable instances and distribute ransomware or other malicious payloads to downstream clients.

ConnectWise has issued an urgent notification to users of its ScreenConnect remote access software, urging them to apply the latest patch immediately.

This follows the discovery of two highly critical vulnerabilities affecting versions 23.9.7 and earlier.

The two vulnerabilities, namely CVE-2024-1709 and CVE-2024-1708, can lead to authentication bypass and path traversal, thereby posing a grave threat to the security and integrity of the impacted systems.

The first one, CVE-2024-1709, is critical and could enable attackers to bypass authentication mechanisms using an alternate path or channel.

This flaw could allow unauthorized access to the system, leading to further exploitation.

The second vulnerability, CVE-2024-1708, has a base score of 8.4 and involves an issue with restricting a pathname to a specified directory.

Source : https://cybersecuritynews.com/screenconnect-vulnerability-exploitation/

New SSH-Snake Malware Abuses SSH Credentials To Spread Itself In The Network

Threat actors abuse SSH credentials to gain unauthorized access to systems and networks. By exploiting weak or compromised credentials, they can execute malicious activities.

SSH credential abuse provides a stealthy entry point for threat actors to compromise and control the targeted systems.

On January 4th, 2024, the Sysdig Threat Research Team (TRT) discovered a network mapping tool dubbed SSH-Snake that was being used as a self-propagating worm.

The tool was found to be exploiting SSH credentials in its attempt to spread and infect other systems. As a result, it poses a significant threat to network security and should be handled with caution.

It hunts for credentials and shell history for its next targets, and currently, threat actors are actively using SSH-Snake malware.

SSH-Snake Malware Abuses SSH Credentials

After gaining system access, attackers often use lateral movement to find and reach other targets. Previous research uncovered a worm seeking SSH credentials to connect and repeat the process.

Source : https://cybersecuritynews.com/snake-malware-abuses-ssh/

Russian Government Software Hijacked to Install Konni RAT

A critical cybersecurity incident recently occurred where the Konni Remote Access Trojan (RAT), a highly covert and sophisticated malware that specializes in data exfiltration, infiltrated the software systems of the Russian Government.

This incident, uncovered by the German cybersecurity firm DCSO, highlights the ongoing cyber espionage activities targeting Russian entities, including the Ministry of Foreign Affairs (MID), and underscores the complex cyber threat landscape nations worldwide face.

The Konni RAT Malware

Konni RAT is a sophisticated malware tool cyber threat actors use to gain unauthorized access to systems, execute commands remotely, and exfiltrate sensitive data.

First observed in 2014, Konni RAT has been linked to several campaigns attributed to North Korea, showcasing its use in geopolitical cyber espionage efforts23.

The malware can capture keystrokes, take screenshots, and steal data, posing a significant threat to the integrity and security of compromised systems.

Source : https://cybersecuritynews.com/konni-rat-russia/

Apple Adds PQ3 post-quantum Encryption for iMessage

Apple has released its new PQ3 (post-quantum) cryptographic protocol, claimed to be the first-ever messaging protocol to reach Level 3 security.

Apple announced its cryptographic protocol change in 2019 when it shifted from RSA to Elliptic Curve Cryptography (ECC), and several upgrades were made.

“PQ3 introduces a new post-quantum encryption key in the set of public keys each device generates locally and transmits to Apple servers as part of iMessage registration,” reads the whitepaper by Apple.

However, Apple announced that PQ3 support would start to roll out in the public releases of iOS 17.4, iPadOS 17.4, macOS 14.4, and watchOS 10.4.

This new protocol has been discovered to mitigate the risk of threat actors using quantum computers for attacking purposes. The retaining of this data now and decrypting it later is an attack scenario named “Harvest Now, Decrypt Later“.

Source : https://cybersecuritynews.com/apple-pq3-post-quantum-imessage/

Hackers launched 250,000+ Attacks to Exploit Ivanti VPN 0-Day

Ivanti Connect Secure vulnerabilities were disclosed in January 2024 as a potential gateway for threat actors to penetrate corporate networks.The two vulnerabilities, CVE-2023-46805 and CVE-2024-21887 were associated with authentication bypass and arbitrary command execution. Combining these two could result in an unauthenticated remote command execution on affected systems.

However, Ivanti addressed these vulnerabilities in its security advisory. Ever since threat actors have found several attempts of exploitation in the wild.

In addition to the disclosure, a proof of concept for these vulnerabilities was also released by Volexity researchers, providing additional information for threat actors and security researchers to find them more easily.Exploitation Observed

According to the reports shared by Akami, roughly 250,000 exploitation attempts have been observed daily against Ivanti Connect Secure devices.

This narrows down to 1000+ customers and 10,000+ domains with more than 3,300+ unique IPs involved in this exploitation. These attacks originate from 18 different countries.

Source : https://cybersecuritynews.com/hackers-launched-250000-attacks/

Hackers Heavily Abusing Google Cloud Run to Deliver Banking Malware

Large-scale malware distribution campaigns are abusing Google Cloud Run to transmit banking trojans, including Astaroth (also known as Guildma), Mekotio, and Ousaban, to European and Latin American targets.

With Cloud Run, you can promptly execute your code on top of Google's scalable infrastructure due to a fully managed platform. It enables the operation of front-end and back-end services, batch processing, website and application deployment, and task queuing without requiring infrastructure management.

In particular, after September 2023, the amount of emails related to these efforts has expanded dramatically, and experts are still routinely seeing new email distribution campaigns.

Emails Leveraging Google Cloud Run

With the vast majority of emails being sent in Spanish, the language distribution of the emails seen in these campaigns also shows a strong concentration on LATAM. It also looks like victims who speak Italian are the target of lower-volume activities.

Source : https://cybersecuritynews.com/hackers-heavily-abusing-google-cloud/

VoltSchemer – Wireless Charger Attack Boils Phone and Injects Voice Commands

Threat actors target wireless chargers for multiple malicious activities, such as implanting malware or conducting power-related attacks.

The rising popularity of wireless charging brings convenience. Still, recent research by Zihao Zhan, Yirui Yang, Haoqi Shan, Hanqiu Wang, Yier Jin, and Shuo Wang from the University of Florida and CertiK uncovered vulnerabilities.

They discovered that electromagnetic interference can manipulate the chargers, which poses security risks.

Researchers discovered VoltSchemer, which enables the execution of innovative attacks on wireless chargers by tweaking power supply voltage without any modification.

Threats include voice assistant manipulation, device damage, and Qi-standard bypass. VoltSchemer Wireless Charger Attack

VoltSchemer attacks exploit newly found wireless charger vulnerabilities that allow complete control via intentional electromagnetic interference (IEMI).

By manipulating the magnetic fields, the threat actors gain control of voice assistants and initiate harmful power transfers.

Source : https://cybersecuritynews.com/voltschemer-wireless-charger-attack/

Wyze webcam Flaw let strangers see into some users' homes

Threat actors target wireless chargers for multiple malicious activities, such as implanting malware or conducting power-related attacks.

The rising popularity of wireless charging brings convenience. Still, recent research by Zihao Zhan, Yirui Yang, Haoqi Shan, Hanqiu Wang, Yier Jin, and Shuo Wang from the University of Florida and CertiK uncovered vulnerabilities.

They discovered that electromagnetic interference can manipulate the chargers, which poses security risks.

Researchers discovered VoltSchemer, which enables the execution of innovative attacks on wireless chargers by tweaking power supply voltage without any modification.

Threats include voice assistant manipulation, device damage, and Qi-standard bypass. VoltSchemer Wireless Charger Attack

VoltSchemer attacks exploit newly found wireless charger vulnerabilities that allow complete control via intentional electromagnetic interference (IEMI).

By manipulating the magnetic fields, the threat actors gain control of voice assistants and initiate harmful power transfers.

Source : https://cybersecuritynews.com/voltschemer-wireless-charger-attack/

“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