QUALYSEC
BEYOND CYBERSECURITY

2023

JUNE 1ST WEEK

CYBER SECURITY NEWS

CONTACT US

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

New Zero-Click iOS Malware Actively Attacks iPhone Through iMessage

Kaspersky recently reported that a number of iPhones connected to its network were compromised through an iOS vulnerability.

The attackers exploited iMessage's zero-click exploits, allowing them to install malware on the devices without any user interaction.

Through the exploitation of a vulnerability, a message is delivered in a manner that triggers code execution without the need for user involvement.

Consequently, this exploit enables the automatic download of further malicious content from the server under the attacker's control.

Following the incident, the message and its attachment are swiftly erased from the device, leaving no trace.

However, the payload itself remains, operating with elevated root privileges. Its purpose is to gather vital system and user data while simultaneously executing commands issued by the attackers.

Since 2019, Kaspersky has been tracking an ongoing campaign called "Operation Triangulation," which continues to pose threats.

While besides this, Kaspersky also encourages individuals with relevant information about the campaign to come forward and share their knowledge and findings to gather more insights.

Source : https://cybersecuritynews.com/zero-click-ios-malware/

MOVEit Transfer Critical Vulnerability Let Attackers Escalate Privileges

MOVEit Transfer software was discovered to be vulnerable to a potential privilege escalation and unauthorized access to the environment.

Users are recommended to take the actions mentioned below until a patch is released by the MOVEit team.

SQL Injection (CVE – Pending – Submitted to MITRE)

MOVEit transfer web application was vulnerable to potential SQL injection, allowing threat actors to gain unauthorized access to MOVEit's Transfer Database.

The database can be MySQL, Microsoft SQL Server, or Azure SQL, which a remote attacker can exploit by executing SQL statements for modifying or deleting database information.

Affected Versions and Patches

All of the MOVEit transfer versions are affected by this vulnerability. Patches are available for some of the affected versions.

Service account credentials for affected systems are recommended to be reset.

Progress researchers have also provided a complete step-by-step approach to remediate this vulnerability. MOVEit transfer users are requested to apply available patches for the affected versions.

A complete report has been published, including Indicators of compromise, remediation steps, and other information.

Source : https://cybersecuritynews.com/moveit-transfer-vulnerability/

‘Migraine’ Flaw Let Hackers Bypass macOS Security Integrity

A recently discovered vulnerability called “Migraine” is linked to macOS migration and poses a serious threat.

It enables attackers with **root privileges to circumvent System Integrity Protection (SIP)** on macOS, granting them unrestricted control over the compromised device.

The security flaw, named “Migraine,” was identified by security researchers at Microsoft Threat Intelligence, who promptly alerted Apple. The vulnerability has since been assigned the tracking identifier CVE-2023-32369.

Apple addressed the identified vulnerability on May 18, 2023, by incorporating a solution into the security updates Apple had already released.

So, the users can protect their systems by promptly installing these updates to mitigate potential risks.

System Integrity Protection Bypass

System Integrity Protection (SIP) serves as a vital security measure in macOS, effectively limiting the capabilities of a root user to prevent any actions that could risk the system’s overall integrity.

Source : https://cybersecuritynews.com/migraine-macos/

Ghost Sites – Hackers May Steal Corporate Data From Deactivated Salesforce Communities

Researchers at Varonis Threat Labs discovered that some Salesforce sites were improperly deactivated or unmaintained SalesforceGhost Sites.

Threat actors can exfiltrate PII and business data by simply manipulating the host headers for these websites.

Salesforce partners and customers are provided an option to create customized communities to help them collaborate.

When these communities are not needed, they are set aside instead of deactivated.

In addition to this, these kinds of community sites are not maintained, which means that they are not scanned or tested for vulnerabilities.

Admins often fail to security test these websites due to the newer guidelines for site security.

However, researchers discovered that these websites can still pull data from Salesforce sites. These sites are very within reach for threat actors and easily exploitable.

As these sites are unmonitored, threats often go undetected and are exploited by threat actors. These sites are named "Ghost Sites."

Source : https://cybersecuritynews.com/ghost-sites/

Beware of New Cryptomining Malware Delivered Using TeamViewer Accounts

In May 2023, Huntress ThreatOps Center analysts detected a cryptocurrency miner (XMRig) on an endpoint, identified the miner's associated site and wallet address by locating the config file, and validated the infection.

The analyst observed activity on numerous infected endpoints, including the one they investigated, by accessing the miner's website.

Suspicious Windows Service

The initial detection of the cryptocurrency miner occurred when a suspicious Windows service was found running on the endpoint, triggering an alert shortly after the miner was installed and the service was created to ensure its persistence.

The Huntress team examined EDR telemetry from the affected endpoint to discover abnormal activity before creating the Windows service.

They then searched through available EDR telemetry across all Huntress customers to find other affected endpoints.

The team discovered one system where similar activity was noticed, but no associated detection or alert was detected.

Source : https://cybersecuritynews.com/cryptomining-using-teamviewer-accounts/

DogeRAT Android Malware Mimic Popular Apps to Steal Sensitive Data

DogeRAT (Remote Access Trojan) is an open-source Android malware that targets a sizable customer base from various businesses, particularly banking, and entertainment.

CloudSEK's TRIAD team detected it. Although this campaign primarily targeted consumers in India, it aims to be accessible to everyone.

Specifics of the DogeRAT Android Malware

The malware is being disseminated disguised as a legitimate app through social networking and messaging apps.

The malware can take significant information from the victim's device after it has been installed, including contacts, messages, and banking credentials.

Particularly, the malware can also be used to hijack the victim's device and carry out harmful tasks like sending spam messages, making unauthorized purchases, editing files, reading call logs, and even snapping pictures with the infected device's front- and rear-facing cameras.

The impersonated apps include Opera Mini – a fast web browser, Android VulnScan, YOUTUBE PREMIUM, Netflix Premium, ChatGPT, Lite 1 [Facebook], and Instagram Pro.

It was discovered that the malware's creator had marketed DogeRAT in two Telegram channels.

Source : https://cybersecuritynews.com/android-malware-mimic-popular-apps/

Lazarus Hacking Group Attack IIS Web Servers to Install Web Shell

The AhnLab Security Emergency Response Center (ASEC) confirmed recent attacks on Windows IIS web servers by the nationally supported Lazarus group.

Typically, threat actors exploit vulnerable web server versions to install web shells or execute malicious commands during their scans.

Lazarus, a financially motivated hacking group, is believed to fund North Korea's weapons development programs while also engaging in espionage operations.

Lazarus Targets IIS Servers

Organizations, regardless of their size, employ Windows IIS web servers to host various web content, including websites, applications, and services like Outlook on the Web from Microsoft Exchange.

Since the release of Windows NT, this has been one of the most flexible solutions on the market, supporting protocols such as:-

- HTTP, HTTPS, FTP, FTPS, SMTP , NNTP

In the event of inadequate management or outdated configurations, servers have the potential to serve as vulnerable access points for hackers to infiltrate a network.

Source : https://cybersecuritynews.com/lazarus-hacking-group-attack-iis/

Over 421,000,000 Times Installed Android Apps from Google Play Contain Malware

A spyware-enabled Android app module that can gather details about files kept on devices and send them to attackers.

Additionally, clipboard contents can be replaced and uploaded to a remote server.

"This malicious SDK collects information on files stored on Android devices and can transfer them to attackers; it can also substitute and upload clipboard contents to a remote server," Dr. Web reports.

According to Dr. Web's classification, this module is known as Android[.]Spy[.]SpinOk is offered as a marketing SDK.

Developers can incorporate it into a variety of Google Play-compatible apps and games.

The SpinOk module appears to keep users interested in apps through mini-games, a system of activities, and purported awards and reward systems.Capabilities of Trojan SDK

- obtain the list of files in specified directories,
- verify the presence of a specified file or a directory on the device,
- obtain a file from the device, and
- copy or substitute the clipboard contents.

After initialization, this trojan SDK communicates to a C&C server by sending a request containing a substantial amount of technical data about the infected device.

Source : https://cybersecuritynews.com/spyware-enabled-android-app/

CYBER SECURITY NEWS

GobRAT Malware Attacking Linux Routers to Deploy Backdoor

In February 2023, JPCERT/CC confirmed malware attacks on routers in Japan, specifically targeting Linux routers with a new Golang RAT known as GobRAT.

The attacker exploits publicly accessible routers WEBUIs, leveraging potential vulnerabilities to infect them with the GobRAT ultimately.

After an internet-exposed router is compromised, a loader script is deployed to deliver GobRAT, which disguises itself as the Apache daemon process (apached) to avoid being detected.

How the Attack Chain Works

The attacker begins by targeting a publicly accessible router with an open WEBUI, exploits vulnerabilities through script execution, and ultimately spoils the GobRAT.

The Loader Script is a multifunctional loader, encompassing tasks like script generation, GobRAT downloading and containing a hard-coded SSH public key for the assumed backdoor.

Loader Script utilizes crontab to ensure the persistence of the file path for Start Script, while GobRAT lacks this capability, highlighting the functions of the Loader Script.

Source : https://cybersecuritynews.com/gobrat-malware-linux-routers/

New Wi-Fi MITM Attack That Can Evade WPA3 Security Mechanisms

The recent discovery of a critical vulnerability in the NPU chipset by Tsinghua University and George Mason University researchers allows attackers to eavesdrop on data transmitted over 89% of real-world Wi-Fi networks by exploiting it.

Hardware acceleration, such as using NPU chipsets in Wi-Fi networks, improves data transmission rate and reduces latency but also introduces security concerns due to the direct transmission of wireless frames by Access Point (AP) routers.

Wi-Fi MITM Attack Model

The recently discovered flaw in the NPU's wireless frame forwarding procedure allows attackers to launch Man-in-the-Middle (MITM) attacks on Wi-Fi networks without requiring rogue APs.

The attack, capable of bypassing link-layer security mechanisms such as WPA3 and intercepting plaintext traffic, has been detailed in a research paper accepted by the 2023 IEEE Symposium on Security and Privacy.

An attacker is connected to a Wi-Fi network at this point so that the attacker has access to the Internet in order to attack the victim

Source : https://cybersecuritynews.com/wi-fi-mitm-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

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