QUALYSEC
BEYOND CYBERSECURITY

2023
MARCH 3RD WEEK

CYBER SECURITY NEWS

CONTACT US

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

Google Uncovers 18 Zero-Day Vulnerabilities in Samsung's Exynos Chipsets

The Project Zero team at Google has recently found and reported 18 zero-day vulnerabilities in Samsung's Exynos chipsets, which are mainly used in:-

1. Mobile devices 2. Wearables 3. Automobiles

Among the 18 zero-day vulnerabilities, four vulnerabilities were classified as the most serious, as they enabled remote code execution (RCE) over the internet to the baseband.

In order to pull off the attack, all that is necessary is the victim's phone number in order to get the job done. Moreover, it's also possible for experienced attackers to effortlessly create exploits to remotely breach vulnerable devices without alerting the targets.

As a precaution, users with affected devices are advised to disable WiFi calling as well as Voice-over-LTE (VoLTE) in their device settings for now, so they will not be exposed to the baseband remote code execution vulnerabilities.

The end users are advised to update their devices in a timely manner to ensure that their devices are running the latest builds that are capable of addressing the disclosed security vulnerabilities and those that are yet to be disclosed.

Source : https://cybersecuritynews.com/vulnerabilities-exynos-chipsets/

Weaponized Telegram and WhatsApp Apps Attack Android & Windows Users

Cybersecurity analysts at ESET recently identified several fraudulent websites mimicking the popular messaging apps, Telegram and WhatsApp.

While these fake websites are primarily targeted at the users of the following platforms to attack them with tampered versions of Telegram and WhatsApp apps:-

- Android
- Windows

Apart from this, the security researchers found that a significant number of the apps they examined are classified as “clippers”. So, these are types of malware that have the capability to steal or modify clipboard data.

Most of them mainly target the users’ cryptocurrency wallets, and not only that, but even some of them also target the victims’ cryptocurrency funds. The Android clippers specifically targeting instant messaging were seen for the first time.

From the affected devices, these apps also seek the saved screenshots, from which they identify the texts with the help of OCR, and for Android malware, this event is also observed for the first time.

Source : https://cybersecuritynews.com/weaponized-telegram-and-whatsapp-apps-2/

U.S Federal Agency Hacked – Attackers Exploited Telerik Vulnerability in IIS Server

Multiple hackers group initiated this attack, including APT actors. The successful exploitation of the vulnerability lets attackers execute an arbitrary code remotely on the federal civilian executive branch (FCEB) agency network where the vulnerable Telerik user interface (UI) is presented in the IIS webserver.

The IOC identified by the federal agencies belongs to the exploit that triggers the Telerik UI for ASP.NET AJAX builds before R1 2020 (2020.1.114).

How Does the Vulnerability Was Exploited

The attack was conducted from November 2022 through early January 2023, targeting the .NET deserialization vulnerability (CVE-2019-18935) in the RadAsyncUpload function, leading attackers to exploit the exposure when the encryption keys are known due to the presence of CVE-2017-11317.

FCEB agency's Microsoft IIS server is configured with Telerik UI for ASP.NET AJAX Q2 2013 SP1 (version 2013.2.717), and the vulnerability, upon the successful remote code execution, lets attackers gain interactive access to the web server.

FCEB agency has an appropriate plug-in to detect this vulnerability CVE-2019-18935. However, the detection failed due to the Telerik UI software being installed in a file path that doesn't have access to scan and find the vulnerability.

Source :https://cybersecuritynews.com/u-s-federal-us-federal-agency-hacked/

Hackers Exploiting Microsoft Outlook Privilege Escalation Flaw in The Wild

In response to the discovery of a critical vulnerability in Microsoft Outlook, CVE-2023-23397, actively exploited in the wild by the threat actors, Cisco Talos urges all Outlook users to update their email clients as soon as possible after the vulnerability has been discovered.

While Microsoft later determined that the activities resulted from Russian-based actors, and they were being used in targeted attacks against a limited number of organizations.

As a result of the exploitation of this security vulnerability, the attacks were conducted between mid-April and December 2022. During this time, threat actors targeted and breached the networks of about 15 critical organizations related to:-

- Government
- Military
- Energy
- Transportation

To steal NTLM hashes, the hackers sent malicious Outlook notes and tasks to the targeted devices to force them to authenticate to the attacker-controlled SMB that shares the hashes.

Source : https://cybersecuritynews.com/outlook-privilege-escalation-flaw/

Hackers Exploiting Silicon Valley Bank (SVB) Collapse to Launch Cyber-Attacks

The failure of Silicon Valley Bank (SVB) on March 10, 2023, as a result of a bank run on its deposits, is expected to have a significant impact on this society because SVB had previously been the preferred banking partner for many businesses globally.

This failure was the second-biggest in American history and the greatest bank failure since the financial crisis of 2007–2008.

“The collapse of SVB has been severe, with many startups now facing financial instability and even potential layoffs”, reports Cyble Research & Intelligence Labs (CRIL).

These impacted businesses, therefore, look for alternate finance sources to maintain their functioning. They have become a top target for Threat Actors (TAs), who are exploiting the current circumstance by carrying out different malicious acts, due to their need for financial stability.

Several companies and individuals who used SVB’s services have been impacted by this incident, including those in the technology, life science, healthcare, private equity, venture capital, and premium wine sectors.

In order to protect their sensitive data from potential cyber threats, affected enterprises must be vigilant and take immediate action.

Source : https://cybersecuritynews.com/hackers-exploiting-svb-collapse/

Attackers Offering Fake Malware Analysis Job Offers Targeting Security Researchers

Mandiant security researchers have recently identified a group of hackers which is believed to be from North Korea is actively seeking security researchers and media outlets with fake job proposals in the following regions:-

- The U.S.
- Europe

As a result, three different families of malware are deployed into the target's environment. Using social engineering techniques, the threat actors persuade their targets to engage in a WhatsApp conversation with them.

In order to establish a foothold within the target's corporate environment, a C++ malware payload called "PlankWalk" is dropped through this channel.

Campaign and Operators

Mandiant has been tracking the particular campaign since June 2022, the observed activity overlaps with "Operation Dream Job," attributed to the North Korean cluster known as the "Lazarus group."

Source :https://cybersecuritynews.com/attackers-offering-fake-job-offers/

Hackers Abuse Google Search Ads to Deliver Vidar and Ursnif Malware

Recently, the cybersecurity researchers at eSentire have identified a shady piece of malware downloader, BatLoader, that has been engaged in a wicked campaign of exploiting Google Ads to distribute malicious secondary payloads such as:-

- Vidar Stealer
- Ursnif

In this ongoing operation, there is a large variety of legitimate apps and newly registered websites that have been spoofed by malicious ads.

As part of its designated tasks as a loader, BatLoader distributes malware such as the following we have mentioned below:-

- Information stealers
- Banking malware
- Cobalt Strike
- Ransomware

From the beginning of its existence in 2022, BatLoader has seen constant changes and improvement. While for malware delivery, BatLoader practices software impersonation tactics, and it’s one of its key characteristics.

Source : https://cybersecuritynews.com/google-ads-malware/

ChatGPT Powered Polymorphic Malware Bypasses Endpoint Detection Filters

The number of monthly users of ChatGPT exceeded 100 million at the end of January, which sets a new record for the fastest-growing app since it was launched at the end of 2022.

OpenAI's ChatGPT is a natural language processing tool that uses AI to process text and is developed by OpenAI. However, recent research revealed that ChatGPT could build code that can be used maliciously.

Jeff Sims, who works at the HYAS Institute, has created a polymorphic keylogger using artificial intelligence called "Blackmamba," which uses Python to tweak its program randomly based entirely on the input that has been taken from the user.

As a result of Jeff's malicious prompt, text-davinci-003 created a keylogger in Python 3. To accomplish this, Jeff had to use the python exec() function to "dynamically execute Python code at runtime."

Due to technological advancements like this, cyberattacks are likely to be launched by less skilled threat actors.

That's why organizations must review their cybersecurity strategy and ensure third-generation defenses are in place to take on these cyberattacks to stay ahead of cybercriminals.

Source : https://cybersecuritynews.com/chatgpt-powered-polymorphic-malware/

“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