QUALYSEC
BEYOND CYBERSECURITY

2024

JAN 1ST WEEK

CYBER SECURITY NEWS

CONTACT US

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

How Smart Car is Probably Tracking You? Automative Data Security Risks

If you drive a smart car, its high-tech, internet-connected systems are likely monitoring your every move. Vehicles with these features typically have telematics systems that track information like location, speed, and driving patterns, as well as GPS systems for navigation.

Improving the vehicle's performance, maintenance, and safety features are all possible with this information. There are privacy issues, too, because the data may end up in the hands of other parties like insurance firms, advertising companies, or even the police. Managing the privacy settings in your smart car is essential for controlling the information that is tracked and shared.

According to ExpressVPN, there's a concerning number of car manufacturers that collect data on their drivers, and an impressive 84% of them then share or sell this data.

The Mechanics of Tracking in smart cars

1. GPS Tracking: One of the simplest ways that smart cars work is by using GPS technology to determine where the vehicle is at all times. Not only can this be used for navigation, but it can also be stored and used to study habits routes and even find a stolen vehicle.

Source : https://cybersecuritynews.com/how-smart-car-is-probably-tracking-you/

Hackers Employ New Evasion Mechanisms to Bypass Security Solutions

The digital landscape, once a serene meadow, has morphed into a battleground where attackers and security vendors engage in a perpetual arms race.

As defenses become more sophisticated, attackers adapt, devising ingenious evasion techniques to bypass security products and inflict harm.

One such tactic, recently uncovered by Trellix Email Security, leverages the foundation of security – caching – to weave a web of deceit and compromise unsuspecting users.

Diverse tools in an attacker's arsenal:

- Geofencing: Malicious content masquerades as benign in specific regions, evading detection elsewhere.
- Captcha Bypass: Automated mechanisms circumvent captchas, hindering URL payload analysis.
- IP Evasion: Blacklisted IPs shield attackers from scrutiny, ensuring their payloads remain hidden.
- QR Code Phishing: QR code obscurity bypasses traditional email security filters, paving the way for phishing attacks.

Source https://cybersecuritynews.com/hackers-evasion-mechanisms/

Hackers Flood Dark Web Markets With Hijacked X (Twitter) Gold account

In the age of social media, verification badges hold significant power.

On Twitter, the coveted blue tick (now replaced with “Gold”) signifies legitimacy and influence, commanding increased trust and engagement from followers.

However, with the platform’s recent monetization of verification, a disturbing trend has emerged: CloudSEK unmasks a nefarious scheme: Compromised Twitter Gold accounts for sale on the dark web

The Rise of Twitter Gold on the Dark Web:

Since December 2022, Twitter has offered paid verification through its “Twitter Gold” subscription.

This move opened a loophole for cybercriminals, who exploit various methods to acquire and sell verified accounts on the dark web.

These accounts, advertised on forums and Telegram channels, typically fall into three categories:

Fresh accounts with bought verification: These accounts are newly created and quickly verified through paid subscriptions. They often lack followers and activity, making them ideal for impersonation scams.

Brute-forced existing accounts: Hackers use automated tools to crack passwords and gain access to dormant accounts. Once hijacked,

Source :https://cybersecuritynews.com/hijacked-x-gold-accounts/

Attackers Can Bypass Windows Security Using New DLL Hijacking Technique

Threat actors using the DLL Hijacking technique for persistence have been the order of the day and have been utilized in several attacks.

This attack method allows bypassing the privilege requirement for executing certain malicious codes on the affected system.

However, a new DLL Hijacking method has been discovered to be used by the threat actors, which uses the trusted WinSxS folder and exploits it by the use of the traditional DLL Search Order Hijacking technique.

This new method has been compatible with both Windows 10 and 11.

Windows Security Using DLL

According to Security Joe's report, this approach allows for improvement and simplification of the DLL Search Order Hijacking method.

The behavior was possible due to the native behavior of Windows and the functionalities it offers for developers and end-users.

This new DLL hijacking method has a low probability of detection since the malicious code operates within the memory space of a trusted binary located in the Windows folder WinSxS.

Threat actors using the DLL Hijacking technique for persistence have been the order of the day and have been utilized in several attacks.

Source : https://cybersecuritynews.com/dll-hijacking-technique/

Mandiant’s X Account Hacked to Push Crypto Scams

The exploitation of crypto scams by hackers can be attributed to the inherent characteristics of cryptocurrencies that provide two critical environments that enable the concealment of illicit activities.

Cryptocurrencies’ decentralized nature and the anonymity they afford create a challenging landscape for authorities to track and identify cyber criminals.

As a result, hackers leverage these characteristics to execute scams that are difficult to trace, thereby covering their tracks and evading legal consequences.

The potential for quick financial gains and the lack of regulatory oversight make the crypto space a lucrative target for fraudulent schemes, attracting threat actors.

An American cybersecurity firm, which is a subsidiary of Google, Mandiant’s X (formerly known as Twitter) account was recently hacked to push crypto scams.

Mendiant’s X Account Hacked

Mandiant was acquired by Google in 2022 for $5.4 billion, which specializes in unveiling the tactics of nation-state-backed threat actors that give a sharp boost to cybersecurity.

Source : https://cybersecuritynews.com/mandiants-x-account-hacked/

SonicWall Acquires Banyan Security for Security Service Edge (SSE) Solutions

SonicWall has made a strategic move in the evolving cybersecurity landscape, acquiring Banyan Security, a leading provider of identity-centric Secure Service Edge (SSE) solutions.

This acquisition promises to significantly enhance SonicWall's platform, enabling seamless security coverage across traditional networks, cloud environments, and remote workforces.

Traditional network perimeters are fading as employees, empowered by flexible work models, access resources from diverse locations and devices.

This shift to cloud-based applications and SaaS platforms further complicates security, introducing vulnerabilities and demanding new approaches.

Legacy infrastructure built for centralized networks struggles to adapt to this decentralized reality.

Zero Trust and the Rise of SSE:

Enter Zero Trust Network Access (ZTNA) and Security Service Edge (SSE). These concepts address the evolving threat landscape by granting access based on identity and context, not network location.

Source :https://cybersecuritynews.com/sonicwall-acquires-banyan-security/

Hackers Modifying Registry Keys to Establish Persistence via Scheduled Tasks

Persistence is one of the key things for threat actors to maintain their access to compromised systems and establish connections whenever they require. One of the key methods used to maintain persistence is the use of scheduled tasks.

A threat actor who is identified as "HAFNIUM" has been discovered to be using an unconventional method to tamper with scheduled tasks for establishing persistent connections by modifying the registry keys in their Tarrask malware. This enables the threat actor to create stealthy scheduled tasks

Hackers Modifying Registry Keys

According to the reports shared by the Purple team, a proof of concept called GhostTask has been published, which exploits the scheduled tasks via a beacon object file that can enable red teamers and threat actors to use it within a C2 framework.

The scheduled task tampering technique is re-created by creating the associated registry keys that prevalently required elevated privileges. GhostTask requires a scheduled task that already exists in the target system.

Once the registry keys are modified, the system requires a restart for changes to take effect. Still alternatively, the schtasks utility can be used to initiate the task and establish persistence.

Source : https://cybersecuritynews.com/hackers-modifying-registry-keys/

Over 11M SSH Servers are Vulnerable to new Terrapin Attacks

Previously, in December 2023, it was reported that SSH servers were vulnerable to the new Terrapin Attack in which threat actors can downgrade an SSH protocol version, making it vulnerable to exploitation. In addition, this attack can also be used to redirect victims into an attacker-controlled shell.

The root causes of this attack were an authentication flaw in the SSH handshake and the non-resetting of sequence numbers. This contributes to several attacks over SSH servers, such as Prefix Truncation, sequence number manipulation, and extension negotiation downgrade attacks.

11 Million Vulnerable Servers

According to the reports shared with Cyber Security News, nearly 11 million SSH servers worldwide were discovered to be vulnerable to this terrapin attack, according to Shadowserver. Though there are no confirmed reports of exploitation, every country has many servers that could be exploited.This report was based upon the search conducted with Shadowserver with search queries containing “ssh,” “ssh6,” and “CVE-2023-48795” with current dates. Additionally, these servers include IPv4 and IPv6 SSH servers. The CVE has been given a severity rating of 5.9 (Medium).

Source : https://cybersecuritynews.com/11m-ssh-servers-terrapin-attack/

Xerox’s US subsidiary Hit by Cyber Attack: Personal Information Exposed

Recently, Xerox’s US subsidiary, Xerox Business Solutions (XBS), experienced a cyber incident, prompting immediate action from Xerox’s cybersecurity personnel.

While the specifics of the intrusion remain under investigation, initial reports indicate containment within XBS US, mitigating further escalation.

Active Investigation and Third-Party Collaboration:

Xerox recognizes the gravity of the situation and is actively collaborating with third-party cybersecurity experts to conduct a comprehensive investigation.

This rigorous approach aims to determine the exact nature and extent of the incident, identify any vulnerabilities exploited, and formulate robust measures to enhance XBS’s IT security posture.

Thankfully, Xerox highlights that the incident did not impact its corporate systems, operations, or data.

Additionally, XBS operations appear unaffected, suggesting a targeted intrusion within the subsidiary’s specific IT environment.

However, Xerox’s preliminary investigation does raise concerns about the potential compromise of limited personal information within XBS.

Source : https://cybersecuritynews.com/xeroxs-us-subsidiary-hit-by-cyber-attack-personal-information-exposed/

Researchers Hunted Malicious Stockpiled Domains Analyzing DNS Records

SSH protocol is one of the most used protocols across several organizations to establish a remote terminal login and file transfer. SSH consists of an authenticated key exchange for establishing the secure channel connection to ensure integrity and confidentiality.

However, a new technique named “Terrapin attack” has been discovered, which will allow threat actors to downgrade the SSH protocol version, thus allowing the exploitation of vulnerable servers. Additionally, the threat actor can redirect the victim’s login into a shell under the attacker’s control.

Terrapin Attacking SSH Protocol

Terrapin attack is a kind of prefix truncation attack in which the initial encrypted packets sent through the secure SSH channel can be deleted without the server or client noticing it.

There are two root causes for this flaw; one of them is the optional messages that are allowed in the SSH handshake, which do not require authentication. Second, the SSH handshake does not reset message sequence numbers when encryption is enabled.

Source : https://cybersecuritynews.com/malicious-stockpiled-domains/

KernelGPT: Automated Analysis of Kernel Components to Detect Vulnerabilities

Kernel vulnerabilities are prevalent in operating systems and can affect billions of devices. One of the most widely used tools for kernel fuzzing is the "Syzkaller," which generates syscall sequences based on predefined specifications written in zlang.

There is existing research in automating Syzkaller specifications generation, which is still being done manually. However, a new research paper has been proposed that integrates LLMs (Large Language Models) and Syskaller specifications that can provide enhanced fuzzing. This has been named as "KernelGPT".

KernelGPT Auto-Detect Vulnerabilities

LLMs have been into several use cases in pre-training and have seen many kernel codes during their development, which can be leveraged to make valid syscalls. Additionally, KernelGPT uses an iterative approach to include all specification components automatically.

The initial level of research demonstrated that KernelGPT enhanced Syzkaller to achieve higher coverage and find multiple previously unknown bugs. This is the first automated approach to using LLMs for kernel fuzzing.

Source : https://cybersecuritynews.com/kernelgpt/

CYBER SECURITY NEWS

Google Pays $5 Billion to End ‘private mode’ Tracking Lawsuit

A landmark settlement has been reached in a class-action lawsuit against Google, accusing the tech giant of breaching user privacy by tracking activity in “private mode” browsing modes.

This decision, announced on Thursday, marks a significant victory for consumers and underscores the intensifying scrutiny directed toward Big Tech’s data collection practices, reads BBC report.

Unmasking the Unaccountable Trove

The lawsuit, filed in 2020, alleged that Google surreptitiously tracked user activity even when browsing in “Incognito” mode on Chrome and similar “private” modes on other browsers. According to the plaintiffs, this covert data gathering transformed Google into an “unaccountable trove of information” on user preferences and potentially sensitive online behavior. The lawsuit further argued that Google’s practices constituted an egregious violation of user privacy, demanding immediate cessation. In its defense, Google maintained that it had been transparent about the data it collected during private browsing, even if many users held different expectations. The company argued that collecting search history, even in private mode, enabled website owners to “better evaluate the performance of their content, products, marketing and more.”

Source : https://cybersecuritynews.com/google-pays-5-billion/

“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