QUALYSEC
BEYOND CYBERSECURITY

2023

JULY 1ST WEEK

CYBER SECURITY NEWS

CONTACT US

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

Texas City Website Hacked – Gigabytes Of Data Stolen

The City of Fort Worth recently experienced a cyber-attack, yet after examining the leaked data, they stated that there is currently no indication that sensitive information about residents or staff is associated with this incident.

The city said that the data was not sensitive and would be made available to the public via a Public Information Request.

Specifics of the City of Forth Cyber-Attack

On June 23, the City of Fort Worth was made aware of a data breach. The Texas Department of Information Resources Computer Incident Response Team notified the City of an online posting; the posting was made public.

According to the post, someone broke into the City's website and stole data related to the City of Fort Worth. In their online release, the hackers included links to copies of the data.

The data was from a "Vueworks application" that was part of an internal information system. Vueworks streamlines work orders for the Transportation & Public Works and Property Management departments.

Source : https://cybersecuritynews.com/texas-city-website-hacked/

Phone Tracking App LetMeSpy Hacked: Attackers Stole User's Messages, Call Logs, & Locations

LetMeSpy, a phone monitoring app, was breached, resulting in unauthorized access to website users' data. Hacker has taken control of the messages, call history, and locations captured by the app.

The App is also called 'stalkerware' or 'spouseware', since these kinds of phone tracking applications are frequently set up by someone, such as partners or spouses. It is an Android-compatible mobile application.

Calls, SMS, and GPS positions of the phone on which it is installed are all tracked while continuing to be "invisible to the user."

The firm presents itself as a tool for employee or parental monitoring, but it doesn't take much imagination to see that it may also be used for abuse.

"As a result of the attack, the criminals gained access to e-mail addresses, telephone numbers, and the content of messages collected on accounts," according to a notice on the LetMeSpy login page.

Niebezpiecznik, a Polish security research blog, was the first to reveal the incident. When the spyware creator approached for comment, a hacker who claimed to have full access to the spyware company's website responded.

Source : https://cybersecuritynews.com/letmespy-hacked/

Mockingjay – A New Injection Technique to Bypass Endpoint Detection and Response (EDR)

The cybersecurity researchers at Security Joes recently discovered a new injection technique that is dubbed “Mockingjay.”

The threat actors could actively exploit this newly discovered injection technique to run and execute malicious code on compromised systems by evading the EDR (Endpoint Detection and Response) and other security solutions.

Utilizing DLLs with RWX sections, this technique easily bypasses the EDR hooks and injects code into remote operations.

By injecting code into trusted running processes, the process injection enables threat actors to execute undetected malicious code.

Attackers employ Windows APIs, system calls, process/thread creation, and process memory writing in these techniques.

Security tools can detect and intervene in suspicious incidents by monitoring specific actions mentioned above.

Commonly abused Windows API calls are not used

- Set special permissions
- Perform memory allocation
- Start a thread

Source : https://cybersecuritynews.com/mockingjay-bypass-edr/

81% of ChatGPT users are concerned about Security Risks (Survey Report)

After seven months, the temptation of ChatGPT, the game-changing chatbot, appears to be weakening. Malwarebytes' recent survey reveals serious concerns over ChatGPT, while positiveness remains alarmingly low.

The concerns outlined in the survey report depict the direction of the news surrounding ChatGPT, which has been ongoing since its debut in November 2022.

Here below, we have mentioned all the concerns that are outlined in this survey report of Malwarebytes:-

81% of users expressed worries about possible security and safety risks.

The information produced by it is not trusted by 63% of users.

51% of users want to pause their work until regulations can align.

The capabilities of ChatGPT shocked all the users with a big blow since it emerged as a versatile tool that can do several tasks like:-

- Coding
- Write essays
- Writing Songs
- Develop computer programs
- Answers to your questions

Source : https://cybersecuritynews.com/chatgpt-security-reports/

European Dismantle of EncroChat Led To 6,500 Arrests & Seizure Of $979 Million Funds

More than 6,500 people were arrested as a result of the takedown of the encrypted phone service platform Encrochat, and 900 million euros ($980 million) worth of assets were confiscated.

Following the work of a joint investigation team (JIT) formed by both nations in 2020 with assistance from Eurojust and Europol, EncroChat was successfully taken down.

Users of EncroChat phones were promised unbreakable encryption, anonymity, and no traceability via a special, hardened version of Android that operated on these devices.

In addition, the service included panic device wipes, tamper-proof booting, and a hardware cryptographic engine that was resistant to brute force attacks and FIPS 140-2 certified.

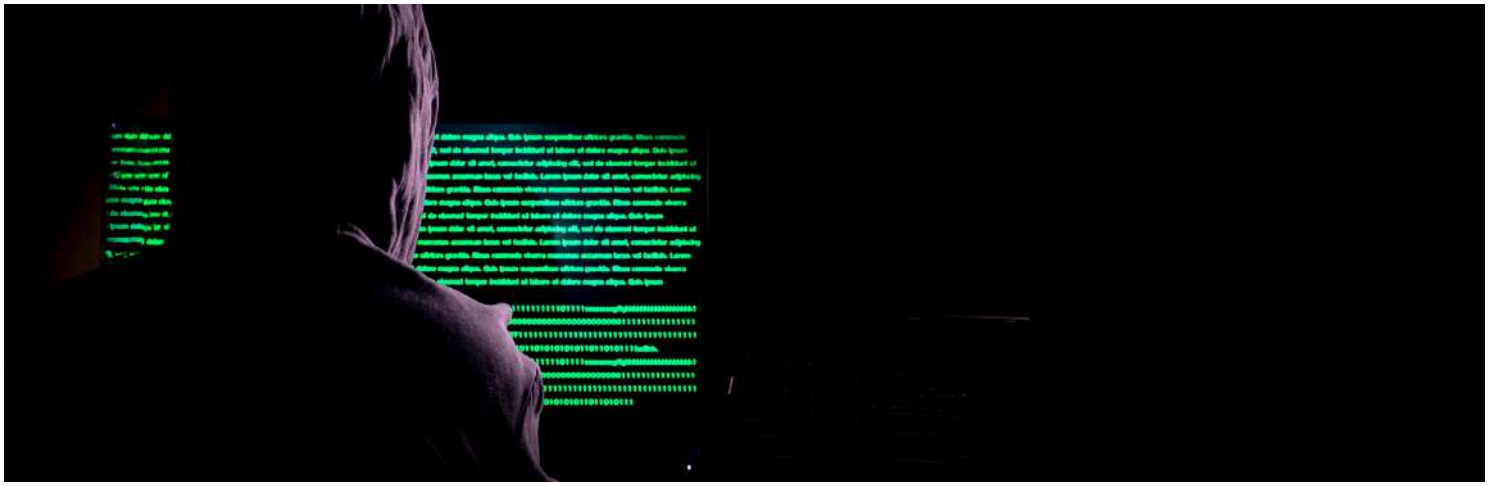
With a “panic button” function that may delete all data, EncroChat devices were well-liked by criminals.

The devices might boot into a hidden encrypted partition for safe connection through French servers.

The service was priced at €1,000 per device and €1,500 for a contract of six months.

Additionally, it had features to guarantee the automated deletion of messages and a unique PIN to erase all data stored on the device.

Source : https://cybersecuritynews.com/european-dismantle-of-encrochat/



New Ransomware Variant Recruit users for Russian Wagner Group

New Ransomware Variant Recruit users for Russian Wagner Group. Recently, the cybersecurity researchers at Cyble Research and Intelligence Labs (CRIL) identified a new ransomware which is a variant of Chaos ransomware dubbed “Wagner.”

While analyzing, security analysts discovered that the ransom note from this ransomware doesn’t ask for money but encourages users to join PMC Wagner.

The ransom note urges war on Shoigu, the notable Russian politician and military officer currently serving as Russia’s Minister of Defence since 2012.

Content of the Ransom Note

The opening sentence of the ransom note states:-

The ransom note matches WAGNER GROUP Telegram channel’s bio section details. Wagner Group, also called PMC Wagner, is a Russian paramilitary force.

A private military company consisting of mercenaries, deemed as a de facto private army associated with Yevgeny Prigozhin, a former ally of Russian President Vladimir Putin.Wagner group hasn’t officially claimed responsibility for this ransomware, leaving the culprits of this variant unidentified.

Source : https://cybersecuritynews.com/russian-wagner-group-ransomware/

University of Manchester Hack – Over One Million NHS patient data Exposed

It has come to light that the University of Manchester fell victim to a Ransomware Hack, which resulted in the breach of 1.1 million NHS patients' information from 200 hospitals.

This event has caused great concern and raised important questions about data security.

Ransomware is malicious software (malware) designed to lock devices and prevent users or organizations from accessing their computer files.

In the attack more than a million NHS (National Health Services) patients' data has been breached; the senior health chief has warned that.

The information exploited includes NHS numbers and the first three letters of patients' postcodes. Also, it includes trauma patients and people treated after terror attacks.

These pieces of information are gathered by the university for research purposes.

The universities have confirmed that backup servers were accessed, but they don't know who was responsible for the attack or how many patients were impacted by the breach. According to the investigation, they found 250 gigabytes of data had been accessed, according to The Independent report.

Source : https://cybersecuritynews.com/nhs-patient-data-exposed/

AI Tools Flaw Lead to Access Bypass & Compromise Sensitive information

AI Tools have become extremely popular in the software industry and are currently in the initial phase of adoption by other industries as well. There have been several AI-based projects that are gaining popularity day by day.

However, the security and risks of these AI and AI-based projects seem extremely concerning.

An analysis from the OSSF (Open Source Security Foundation) among 50 LLM (Large Language Models) /GPT (Generative Pre-trained Transformer) shows that the security posture of these projects is extremely low.

Mature Vs Immature Projects

While these AI-based projects are reaching users widely, attackers lay their eyes on them, making them prime target.

In addition to this, the security posture of these popular AI-based projects is extremely low, which can have a high success ratio for a data breach.

The analysis provided insight into these AIs which shows the average rating of these 50 LLM-based projects is 15000+ stars.

These projects have an average age of just 3.77 months which makes them extremely immature.

Source : https://cybersecuritynews.com/ai-tools-flaw/

NSA and CISA Shared Best Practices To Harden CI/CD Cloud Deployments

Released by the National Security Agency (NSA) and the Cybersecurity and Infrastructure Security Agency (CISA), the cybersecurity information sheet (CSI) titled “Defending Continuous Integration/Continuous Delivery (CI/CD) Environments” offers suggestions and best practices for enhancing defenses in cloud implementations of development, security, and operations (DevSecOps).

Securing a CI/CD environment critically depends on being aware of the many security threats that might impact operations and taking action to protect against each one.

The CI/CD environments and software supply chains are prime targets for cybercriminals, as shown by the rising number of intrusions over time.

CI/CD Environments – Popular Targets

The Continuous Integration/Continuous Delivery (CI/CD) development approach helps organizations maintain a consistent application code base while dynamically merging code changes. It allows for speedy construction and testing of code changes.

Source : https://cybersecuritynews.com/ci-cd-cloud-deployments/

JokerSpy – Multi-Stage macOS Malware Attacking Organisation Worldwide

MacOS is reported to be one of the most security Operating Systems. As of the beginning of 2023, there are over 100 million macOS devices worldwide. Due to its popularity, threat actors have begun to target macOS devices recently.

Based on the recent reports from SentinelOne, Bitdefender and Elastic, a new type of macOS malware is in the wild, exploiting multiple macOS devices in organisations. The number of victims of this malware is yet to be confirmed.

This malware is capable of providing an active adversary deployment, a backdoor and it is a form of open-source reconnaissance. It is a multi-platform exploitable tool and is capable of macOS exploitation.

JokerSpy – Multi-Stage macOS Malware

The Initial phase of compromise of this malware is still being investigated. As per the current reports, the initial level of compromise is discovered to be linked with a trojanized QR generator in a file QRWriter.java that hides inside an open-source QR project.

Once the host OS is detected, the malware decodes an embedded base64 blob which is written and executed inside the temporary directory. This decoded file acts as the communication to the C2 (Command and Control) server at hxxps://git-hub[.]me/view/php.

Source : https://cybersecuritynews.com/jokerspy-macos-malware/

New Research Reveals 187% Increase in Sophisticated Attacks Against Mobile Devices

The rapid growth in Mobile Devices and app usage has created an ever-growing attack surface and risks in organizations.

According to last year's report, 60% of endpoints accessing company assets were mobile devices.

Mobile-powered firms must strengthen mobile security procedures to secure employee's personal data and critical organizational information."

Improper configurations and minimal user awareness of phishing and smishing create devices prone to high-security risks.

Zimperium, a mobile security platform for mobile devices and apps, has released its highly anticipated Global Mobile Threat Report 2023.

Mobile Threat Report Key Findings:

As per the Global threat report of 2023 is that 43% of all compromised devices were fully exploited, an increase of 187% year-over-year.

Phishing attacks on mobile devices are becoming more prevalent. 80% of phishing sites are designed to run on both desktop and mobile platforms.

Meanwhile, SMS phishing or smishing attacks are six to ten times more likely to be successful than email-based attacks.

Source : https://cybersecuritynews.com/mobile-threat-report/

DNS TXT Records Can Be Used by Hackers to Execute Malware

DNS TXT record enables domain administrators to input text into DNS, initially for human-readable notes, but now it's utilized for diverse purposes like:-

- Spam prevention
- Domain ownership verification

Spam email senders disguise domains to evade detection, but servers verify emails using the DNS TXT record as a key element.

Moreover, the domain owners can verify their ownership by uploading a TXT record with specific information or modifying the existing one.

ASEC from AhnLab has confirmed the use of DNS TXT Records in malware execution, which is a rare technique that holds importance for detection and analysis purposes.

Malware Execution using DNS TXT Records

The malware uses DNS TXT records differently, closer to the original purpose of entering DNS-related info, rather than the common method mentioned earlier. A phishing email included a fake "Order Inquiry" with a PowerPoint add-in (PPAM) file. PPAM files have user-defined macros and VBA code, and executing the PowerPoint macro triggered PowerShell's nslookup management tool.

Source : https://cybersecuritynews.com/dns-txt-records-to-execute-malware/

New Proxyjacking Campaign Attack SSH Servers to Build Docker Services

It has been observed that a new Proxyjacking campaign attack SSH servers and subsequently builds Docker services that share the victim's bandwidth for money.

This is an active campaign that Akamai Security Intelligence Response Team (SIRT) has identified. Through this, the attacker uses SSH for remote access and malicious scripts that discreetly enroll target servers for peer-to-peer (P2P) proxy networks like Peer2Proxy or Honeygain.

Additionally, it enables the attacker to make money from the excess bandwidth of an unaware victim using a small fraction of the resources needed for crypto-mining and with less risk of detection.

What is Proxyjacking?

The most recent method for hackers to profit from hacked devices in both the corporate and consumer ecosystems is proxyjacking. Here, the attacker takes advantage of the victim's unused bandwidth in addition to stealing resources."The victim's system is covertly used to run various services as a P2P proxy node that the attackers have recently started to monetize through organizations such as Peer2Profit or Honeygain", researchers explain.

Source : https://cybersecuritynews.com/proxyjacking-campaign-attack-ssh-servers/

PhonyC2 – MuddyWater's New C2 (command & control) Center Uncovered

Recently, it has been found by the security analysts at Deep Instinct that MuddyWater (aka Mango Sandstorm and Mercury), an Iranian state-backed group, has been using a new command-and-control framework since 2021 that is dubbed "PhonyC2."

PhonyC2, an actively developed framework, was used in the Technion attack (Feb 2023), and the MuddyWater keeps updating the PhonyC2 and modifying the TTPs to evade detection.

Leveraging social engineering, MuddyWater breaches patched systems as its primary access point. The threat research team of Deep Instinct discovered three malicious PowerShell scripts in April 2023 within the PhonyC2_v6.zip archive.

MuddyWater's New PhonyC2

MuddyWater, a cyber espionage group linked to Iran's MOIS since 2017, and Microsoft implicated them in destructive attacks on hybrid environments and collaboration with Storm-1084 for:-

- Reconnaissance
- Persistence
- Lateral movement

Source : https://cybersecuritynews.com/phonyc2-muddywater/

“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