QUALYSEC
BEYOND CYBERSECURITY

2023

MAY 4TH WEEK

CYBER SECURITY NEWS

CONTACT US

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

Tesla Data Leak Exposes Thousands Of Safety Complaints

According to a report in the German newspaper Handelsblatt, Tesla Inc consumers made over 2,400 complaints about self-acceleration issues and 1,500 complaints about brake problems between 2015 and March 2022.

Reports stated that a massive data dump based on a whistleblower's breach of internal Tesla documents reveals that issues with Tesla's automated driving system may be much more prevalent than regulators and the media have indicated.

Based on stolen information from Tesla's IT system, complaints regarding these Full Self Driving (FSD) features came from all around the world, including the United States, Europe, and Asia.

Tesla's Autopilot Issues And Inadequate Data Privacy Policies

Particularly, in an article headed "My autopilot almost killed me," Handelsblatt reported receiving 100 gigabytes of data and 23,000 files, including 3,000 entries concerning customers' safety concerns and accounts of more than 1,000 collisions.

The publication added saying that the data contained customer phone numbers.

Source : https://cybersecuritynews.com/tesla-data-leak-safety/

CYBER SECURITY NEWS

Windows XP Activation Algorithm Cracked – Works With Linux

Getting around Windows XP’s activation scheme has never been an impossible challenge for individuals with adequate time, a sense of urgency, or moral flexibility.

Newly activated Windows XP installations can now be safely and securely accomplished offline with the help of crack, granting the persisting Microsoft operating system a renewed lease of life over 21 years later.

Cracking Windows XP Activation Algorithm

Recently, Tinyapps revealed that Linux could successfully defeat Microsoft’s algorithm and methods for validating Windows XP product keys.

Valid activation codes for Windows XP can be generated without an internet connection, which is useful, as the offline OS cannot communicate with Microsoft’s servers for activation.

MSKey Readme has been celebrated for nearly two decades for its ability to crack the encryption algorithm of Windows XP’s product activation rather than simply bypassing it.

Microsoft’s GitHub platform witnessed the launch of WindowsXPKg four years

Source : https://cybersecuritynews.com/windows-xp-activation-algorithm/

Chinese Hackers Attack US Critical Infrastructure Using Network Administration Tools

The US and global cybersecurity agencies have issued a joint advisory to bring attention to the activities of “Volt Typhoon,” a state-sponsored cyber actor from China.

The impact of this activity on networks across critical infrastructure sectors in the United States has been acknowledged by private-sector collaborators.

However, it’s believed that to target both of these sectors and others on a global scale, similar methodologies could be used by the threat actors.

Security Agencies Involved

Here below we have mentioned all the cybersecurity agencies that are involved in this joint advisory:-

- The United States National Security Agency (NSA)
- The U.S. Cybersecurity and Infrastructure Security Agency (CISA)
- The U.S. Federal Bureau of Investigation (FBI)
- The Australian Signals Directorate’s Australian Cyber Security Centre (ACSC)
- The Communications Security Establishment’s Canadian Centre for Cyber Security (CCCS)

Source : **https://cybersecuritynews.com/chinese-hackers-attack-us-critical-infrastructure/**

ABB Hack – Attackers Dropped Ransomware on IT Systems

As per reports, ABB (ASEA Brown Boveri), the technological giant in electrification and automation, has been impacted by an IT security incident. ABB is investigating this incident with law enforcement and data protection authorities.

ABB has an employee base of over 105,000 and a net worth of $69.02 billion as of 2023. Earlier this month, ABB faced an attack from the Black Basta ransomware group that works as Ransomware-as-a-Service (RaaS).

Press Release from ABB

According to a recent report, An unauthorized third party has gained access to ABB systems and deployed ransomware to extract specific data. The company has been analyzing and identifying the nature and scope of the impacted data.

The company has also taken necessary steps to communicate with all the affected customers, suppliers, and individuals whose information was affected.

ABB stated that they are in the early stages of the investigation, and the extent of the impact caused is yet to be confirmed.

ABB's press release states, "ABB remains focused on working diligently with law enforcement, its customers, suppliers, partners, and advisors to resolve this situation and minimize its impact."

Source : https://cybersecuritynews.com/abb-hack/

IT Security Analyst Pleaded Guilty for Attacking his Own Company

The insider threat has been a significant concern for organizations in terms of security. Though they do not happen very often, it is still a major threat to the business.

Ashley Liles, a 28-year-old IT Security Analyst working at Oxford BioMedica, was tasked with investigating a cybersecurity incident involving unauthorized access to a portion of the company's systems.
The intruder had already notified the company's senior staff members about the infiltration and demanded a ransom payment. Ashley Liles and his colleagues were working towards mitigating this issue.
Liles Became An Insider Threat

At one point, Liles decided to change the circumstances of this incident for his benefit. He devised a plan and exchanged the Bitcoin payment address of the attacker with his own. Furthermore, he also set up an email address that was similar to the attacker's.
From that point, he acted as the attacker and forced the company to pay the ransom. Unfortunately, Oxford BioMedica didn't pay a single dollar for ransom. In addition to this, his unauthorized access to private emails was revealed during the investigation, which was traced back to his home.

Source : https://cybersecuritynews.com/it-security-analyst-pleaded-guilty/

How the Forensic Tools Can Retrieve Deleted WhatsApp Messages

Law enforcement agencies can potentially retrieve deleted data, including from encrypted chat apps like WhatsApp if they acquire and search your iPhone.

Following the disclosure of recent case details published in Forbes, law enforcement officials in Eastern California impounded the mobile device belonging to a suspect involved in an ongoing investigation related to drug trafficking.

The phone's data was instrumental in monitoring the transportation of methamphetamine and fentanyl shipments from Mexico to the state.

Outlined in a search warrant, an FBI agent from Sacramento provided a comprehensive account of the suspect's WhatsApp conversations with an alleged accomplice, highlighting the presence of encryption, rendering some of the messages incomprehensible.

The investigator explained that the messages retrieved by the extraction software appeared disordered or "scrambled" due to the encryption functionalities employed by WhatsApp, thus attributing this phenomenon as the cause.

Recent evidence suggests that the technology still operates similarly, as a Discord user claiming to be a Cellebrite employee in March 2023 referred to a 2021 post when questioned about deleted WhatsApp messages.

Source : https://cybersecuritynews.com/retrieve-deleted-whatsapp-messages/

CYBER SECURITY NEWS

Hackers Using New ‘URL Obfuscation’ Technique to Deliver Malware Silently

Mandiant researchers recently identified “URL Schema Obfuscation” as an adversary technique that conceals the final URL destination by manipulating the URL schema during the distribution of various malware families.

The method has the potential to enhance the chances of a phishing attack being successful, as well as introduce errors in domain extraction within logging or security tools.

The reliance on server identification by network defense tools may lead to bypassing and gaps in visibility, impacting threat detection and understanding of malicious campaigns and infrastructure.

New URL Obfuscation Technique

An investigation by Mandiant revealed that SMOKELOADER employs various obfuscation techniques to obscure URL destinations, leading to the distribution of numerous malware variants, as highlighted in a tweet by @ankit_anubhav.

This tweet exemplifies the use of two simultaneous obfuscation techniques, demonstrated by the URL “hxxp://google.com@1157586937,” which leads to the unexpected outcome of a Rick Roll video.

Source : https://cybersecuritynews.com/hackers-use-url-obfuscation/

Apple Blocks Employees Use of ChatGPT, Fearing Data Leak

Apple has been very concerned when it comes to the exposure of its confidential data, which resulted in several actions taken by the company, including the one against the FBI.

ChatGPT has become extremely popular among employees at various organizations as it can be used for everything from writing a simple email to developing sophisticated software.

Recent reports suggest that Apple has restricted some of its employees from using ChatGPT or any other external Artificial Intelligent tools. It was stated that Apple was concerned about the leakage of its confidential data to the developers of the Artificial Intelligence Bot.

In addition to this, Apple has also ordered its employees not to use Microsoft-owned GitHub's Copilot, which can be used for writing codes for software.

Apple's own Artificial Intelligence bot

Apple has been working on a large language model and developing its own Artificial Intelligence bot, which will be able to answer questions and perform tasks like a human.

They have already acquired several artificial intelligence-based startups since John Giannandrea (Former Google employee) became Apple's Senior Vice President.

Source : https://cybersecuritynews.com/apple-blocks-chatgpt/

Exclusive! Scientists Developed an AI Model that Automatically Links Vulnerabilities With Cyber Attacks

Scientists developed a new AI model that automatically maps vulnerabilities to attack patterns using Large Language Models and identifies all relevant attack techniques—scientists from the Pacific Northwest National Laboratory report to Cyber Security News.

Imagine you're the new manager of a large apartment building, and someone has stolen one of your keys—but you're not sure which one. Was it to a first-floor apartment? The mail room? Maybe it's a master key to all the units.

As you know, all locks are vulnerable, and you'll need to change every lock to be completely secure.

But if you knew exactly which key went missing, you could target your efforts, changing just the relevant lock and eliminating the threat posthaste.

Multiply that problem thousands of times, and you'll understand what cyber defenders grapple with.

There are more than 213,800 known "keys"—unofficial entry points into computer systems, better known as vulnerabilities or bugs—and they're already in the hands of criminals.

Source : https://cybersecuritynews.com/ai-model-automatically-links-vulnerabilities-with-cyber-attacks/

DarkBERT: A New AI Trained Exclusively on the Dark Web

South Korean researchers (Youngjin Jin, Eugene Jang, Jian Cui, Jin-Woo Chung, Yongjae Lee, Seungwon Shin) at KAIST (Korea Advanced Institute of Science & Technology) developed DarkBERT.

This AI model ventured into the depths of the dark web, an anonymous and concealed part of the internet, to index and gathered information from its shadiest domains.

The "Dark Web" is an inaccessible and concealed segment of the internet, known for its anonymous websites and illicit marketplaces that facilitate activities like illegal trade, data breaches, and cybercrime.

DarkBERT on Dark Web

The 'Dark Web' relies on sophisticated methods to hide user identities, making it challenging to track their online activities. Tor is the favored software for accessing this section, used by millions daily.

DarkBERT, built on the RoBERTa architecture, has experienced a resurgence as researchers found untapped performance potential due to its initial undertraining, leading to enhanced efficiency beyond its 2019 capabilities.

Source : https://cybersecuritynews.com/darkbert-ai/

CYBER SECURITY NEWS

18-Year-Old Charged for Hacking Into 60,000 Users' Accounts

An 18-year-old Wisconsin teenager has been accused by federal authorities of a cyberattack that compromised 60,000 user accounts at the sports betting website DraftKings last year.

A "credential stuffing attack" was allegedly planned by Joseph Garrison to steal money from DraftKings user accounts.

U.S. Attorney Damian Williams said: "As alleged, Garrison used a credential stuffing attack to hack into the accounts of tens of thousands of victims and steal hundreds of thousands of dollars. Today, thanks to the work of my Office and the FBI, Garrison learned that you shouldn't bet on getting away with fraud."

During a credential stuffing attack, a cyber threat actor gathers stolen credentials, or username and password pairs, obtained from other significant data breaches of other firms, which are available for purchase on the dark web.

"The threat actor then systematically attempts to use those stolen credentials to obtain unauthorized access to accounts held by the same user with other companies and providers to compromise accounts where the user has maintained the same password.", DOJ reported.

Source : https://cybersecuritynews.com/teenager-hacked-60000-users-account/

“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