QUALYSEC

BEYOND CYBERSECURITY

2023

JUNE 2ND WEEK

CYBER SECURITY NEWS

CONTACT US

🌐 www.qualysec.com

☎ 865 866 3664

✉ contact@qualysec.com

Half&Half – Intel Processor’s Hidden Security Feature Stop Attack Against Spectre Like Vulnerabilities

Computer scientists uncover a previously unknown security feature in Intel processors that provides robust protection against attacks, including the notorious Spectre vulnerability, Cyber Security News learned from researchers at UC San Diego and Purdue University.

In a groundbreaking study titled “Half&Half: Demystifying Intel’s Directional Branch Predictors for Fast, Secure Partitioned Execution,” researchers from UC San Diego and Purdue University have successfully reverse-engineered Intel’s flagship processors, unraveling their conditional branch predictors spanning over a decade.

Conditional branch instructions play a crucial role in modern software, influencing the execution of instructions based on data values—approximately 10 to 20 percent of all instructions executed fall under this category.

Intel’s Branch Predictor

To optimize processing speed, modern processors employ branch predictors that anticipate the outcome of conditional branches, enabling uninterrupted execution until the branch’s result becomes known much later in the pipeline.

Source : https://cybersecuritynews.com/halfhalf/

New Horabot Malware Steals Banking and Outlook Credentials

Since November 2020, a covert campaign utilizing the 'Horabot' botnet malware has specifically targeted Spanish-speaking users across Latin America, infecting them with a banking trojan and spam tool, all while operating undetected.

Threat actors take control of the victim's email accounts (Gmail, Outlook, Hotmail, or Yahoo) by exploiting the malware to steal all the essential and confidential email data.

Not only that, even threat actors also use those compromised email accounts to send phishing emails to other victims.

Cybersecurity researchers at Cisco Talos recently uncovered this new Horabot operation, revealing that the threat actor responsible for it is believed to have roots in Brazil.

However, most of the infections are located in the following countries:-

- Mexico
- Uruguay
- Brazil
- Venezuela
- Argentina
- Guatemala
- Panama

Source : https://cybersecuritynews.com/horabot-malware/

Lessons From The 1,802 Data Breaches Of 2022: A Deeper Dive Into Internet Safety

The year 2022 has been a wake-up call for the digital world. A staggering 1,802 data compromises were reported globally, affecting 422 million individuals, emphasizing the urgent need to ramp up online security measures. These breaches served as a harsh reminder that no entity is immune to cyber threats and underscored the importance of reevaluating our approach to internet safety. Here’s what we’ve learned.

Cybersecurity Is Not A Choice, But A Necessity

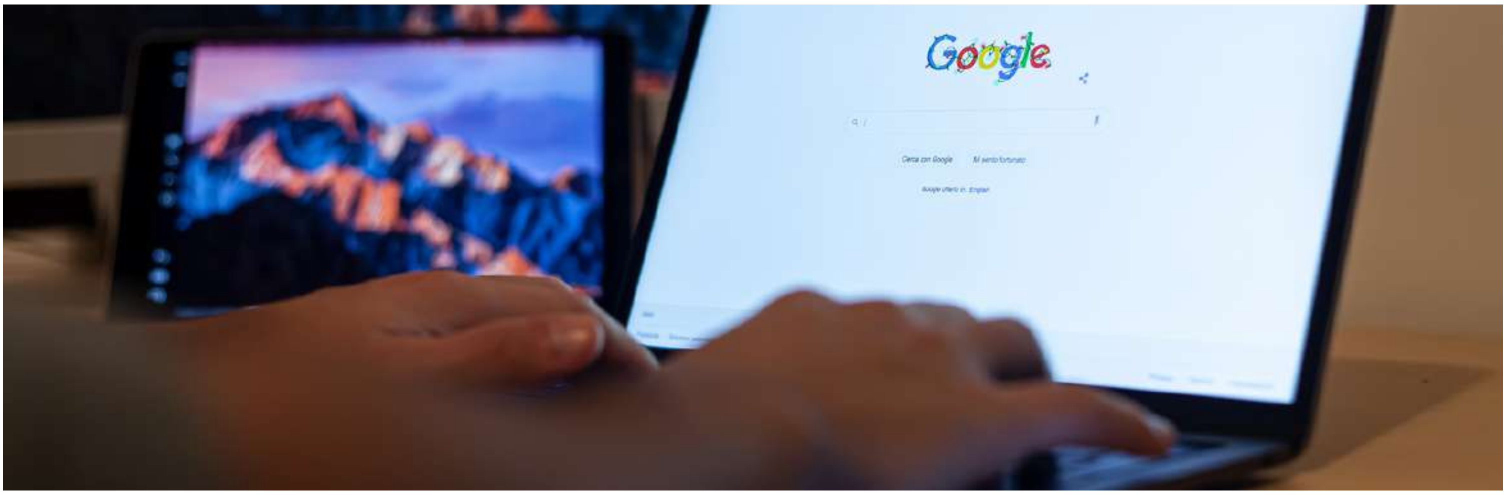
2022 was a stark demonstration that cybersecurity is no longer optional. From small businesses to multinational corporations, public sectors to private individuals, data breaches spared none. We must incorporate robust cybersecurity strategies at every level to navigate this digital age safely.

The Human Factor Remains The Weakest Link

Despite technological advancements, human error continues to be a significant factor in cybersecurity breaches. Be it falling for phishing scams, using weak passwords, or not updating software regularly, people often inadvertently create openings for cybercriminals.

Source : https://cybersecuritynews.com/lessons-from-the-1802-data-breaches-of-2022/

CYBER SECURITY NEWS



New Google Chrome Zero-Day Bug Actively Exploited in Wild– Emergency Update!

Google released new security updates for actively exploited Chrome zero-day vulnerability exploit in the Wild, which allows attackers to execute an arbitrary code to take complete control of the system remotely.

Google released Chrome 114.0.5735.106 for Mac and Linux and 114.0.5735.110 for Windows, a new update that fixes its first actively exploited the zero-day vulnerability of the year. Chrome is available for Windows, Mac, and Linux.

CVE-2023-3079, a high-severity zero-day vulnerability, was found and reported by Clément Lecigne of Google's Threat Analysis Group.

"Google is aware that an exploit for CVE-2023-3079 exists in the wild," This update includes 2 security fixes, Google says.

Chrome Zero-day Bug Details – CVE-2023-3079

All Chrome versions are vulnerable to the high-severity type Confusion vulnerability in the V8 Javascript engine, which lets attackers remotely exploit the flaw by running arbitrary code.

By reading or writing outside the buffer's limits, this zero-day flaw causes browser crashes when it is successfully exploited.

Source : https://cybersecuritynews.com/new-google-chrome-zero-day-bug-actively-exploited/

ChatGPT May Create Deadly Polymorphic Malware That Evades EDR

From handling simple inquiries to instantly generating written works and even developing original software programs, including malware, ChatGPT proves to be an all-encompassing solution.

However, this advancement also introduces the potential for a dangerous new cyber threat.

Traditional security solutions such as EDRs harness multi-layered data intelligence systems to combat the highly sophisticated threats prevalent in recent times.

Despite the claims made by most automated controls to detect and prevent irregular or novel behavior patterns, the actual implementation rarely aligns with these claims.

While apart from this, the availability of AI-generated, polymorphic malware in the hands of malicious threat actors will worsen the situation.

Creation of BlackMamba

The cybersecurity analysts at Hyas have created a simple proof of concept (PoC) to demonstrate the potential capabilities of AI-based malware.

Source : https://cybersecuritynews.com/chatgt-may-create-deadly-polymorphic-malware-that-evades-edr/

CYBER SECURITY NEWS

‘Triangulation’ Malware- New Tool to Find iPhones & iOS Devices Infection

Kaspersky reported earlier this month that they have discovered a new Zero-click iOS exploit currently being exploited by threat actors.

The exploitation involves using iMessage as the delivery channel to gain root privileges.

Threat actors were using Command and Control (C2) servers to manage and control the compromised iOS devices.

Recent reports suggest that a new tool named “triangle-check” was released, which could scan iTunes backups for traces of IoCs (Indicators of Compromises).

This was released as a pypi project, “**triangle-check 1.1**”.

Triangle Check

This project is released as a Python script that can scan iTunes backups of iPhones and check for any traces of compromise.

The script has two Python dependencies, **colorama,** which is used for pretty printing, and **pycryptodome**.

For using this package, the exact location of the iTunes backup directory is required, which includes many sub-directories and files like “Manifest.db” and “Manifest.plist”. For decryption, the password used for encryption is required (If the backup is set up in iTunes). For advanced back creation, the idevicebackup2 tool can be used, which is dependent on the open-source package named “libimobiledevice”

Source : https://cybersecuritynews.com/triangle-check/

Hackers Inject Shell Scripts into eCommerce Sites to Steal Credit Card Data

A recently discovered credit card theft operation, Magecart, has adopted an innovative approach by utilizing authentic websites as makeshift C2 servers.

This strategy enables them to illicitly implant and conceal skimming malware within specific eCommerce websites.

During the checkout process, hackers execute a Magecart attack by breaching online stores and implanting malicious scripts designed to stealthily harvest the customers' credit card details and personal information.

Large-scale & Long-term Attack

As per the diligent monitoring conducted by Akamai's researchers on this particular campaign, numerous organizations in the subsequent countries have fallen victim to compromise:-

- The United States
- The United Kingdom
- Australia
- Brazil
- Peru
- Estonia

Source :https://cybersecuritynews.com/shell-scripts-ecommerce-sites/

Malicious Chrome Extension With Over 75 Million Downloads Install Malware

Google has removed 32 malicious extensions from the Chrome Web Store that could have changed search results and pushed spam or unwanted adverts. They have received 75 million downloads altogether.

The PDF Toolbox extension, which has had 2 million downloads from the Chrome Web Store, was examined by cybersecurity expert Wladimir Palant, who discovered that it contained code disguised as an extension API wrapper.

Reports say to protect users from the harmful behavior that was concealed in obfuscated code to deliver the payloads, the extensions included legal functionality.

Malicious Extensions In Chrome Web Store

The researcher describes how the code allowed the “serasearchtop[.]com” domain to insert arbitrary JavaScript code into any page the user visited in a report published earlier.

The possibility of abuse includes everything from stealing sensitive information to adding advertisements to web pages.

Additionally, the code was designed to activate 24 hours after the extension was installed, which is a behavior that is frequently indicative of malicious intent, as the researcher discovered.

Source : https://cybersecuritynews.com/chrome-extension-75-million-downloads/

Google Drive Security Flaw Let Hackers Exfiltrate Data Without Any Trace

Google Drive is one of the most used cloud-based storage platforms, and due to its immense popularity and capabilities, it's actively targeted by threat actors.

Data theft is a prevalent method employed by malicious actors once they have obtained entry into a platform. It serves as a common attack vector for stealing information.

Mitiga's research team has recently conducted a comprehensive investigation into data exfiltration techniques within Google Workspace, highlighting the significance of this attack method and platform.

This research aligns with their ongoing efforts to explore and understand cloud and Software as a Service (SaaS) attacks and forensic practices.

Attack on Google Drive

Malicious actors frequently aim to **exploit vulnerabilities within Google Drive** to gain unauthorized access to sensitive files and user data.

Experts conducting an in-depth analysis uncovered a critical security flaw within Google Workspace, revealing a troubling deficiency in its forensic measures.

Source : https://cybersecuritynews.com/google-drive-security-flaw/

“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