QUALYSEC
BEYOND CYBERSECURITY

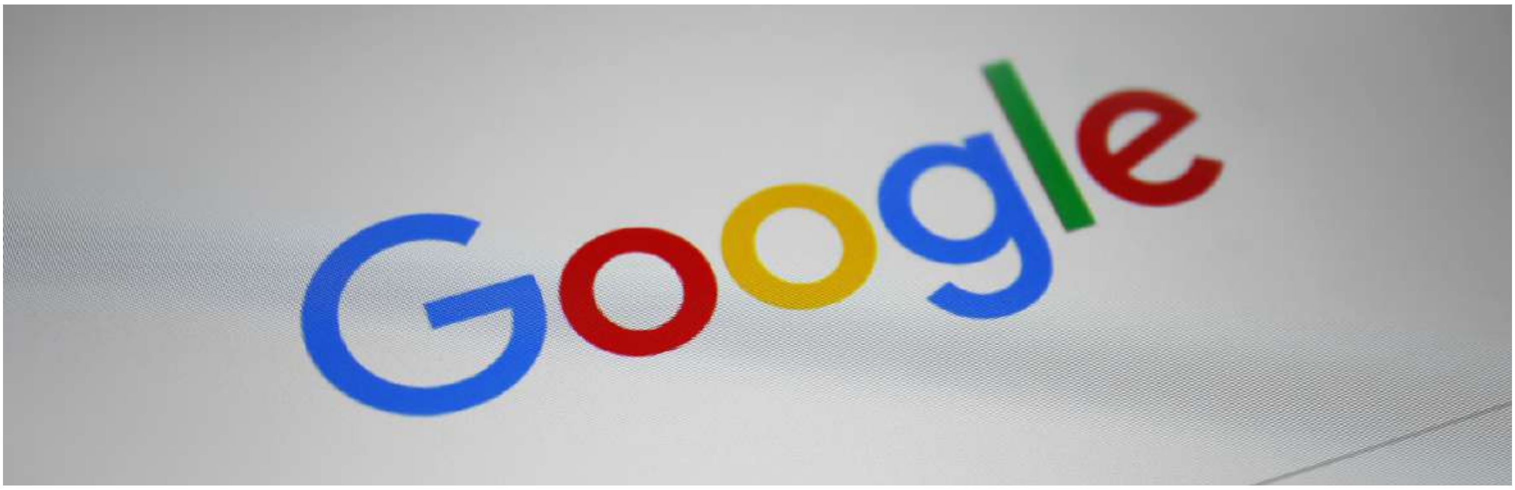
2024

April 3rd week

CYBER SECURITY NEWS

CONTACT US

🌐 www.qualysec.com
☎ +91 865 866 3664
✉ contact@qualysec.com



Poisoned Google Ads Targeting Infra Teams with Weaponized IP Scanners

Security researchers uncovered a sophisticated malvertising campaign targeting IT professionals, particularly those in security and network administration roles.

The threat actor behind this attack has been leveraging Google Ads to distribute trojanized versions of popular IP scanning and IT management software.

Attack Chain

The attack begins with the threat actor registering multiple look-alike domains that spoof well-known network scanning tools, such as Advanced IP Scanner, Angry IP Scanner, and PRTG IP Scanner.

They then run Google Ads campaigns to push these malicious domains to the top of search results for relevant keywords.

When unsuspecting users click on the malicious ads, they are redirected to the spoofed websites, which have been carefully crafted to mimic legitimate software.

The websites contain modified JavaScript code that redirects users to download a malicious ZIP archive file.

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

MITRE Hacked – Attackers Compromised R&D Networks Using Ivanti Zero-days

The MITRE Corporation, a non-profit organization that runs federally funded research and development centers, has disclosed that a sophisticated cyber attack recently compromised one of its internal research and development networks.

- MITRE detected the attack on one of its internal R&D networks and took immediate action to contain the incident.
- The attack was believed to have been initiated by the UNC5221 group from China.
- The attack had no impact on the organization's business and public-facing networks.
- MITRE collaborates with its federal sponsors and law enforcement agencies to investigate the attack and identify the perpetrators.
- The organization has not disclosed any further details about the attack, citing the ongoing nature of the investigation.

MITRE's cybersecurity team detected a sophisticated cyber attack targeting one of the organization's internal research and development networks. Upon discovery, MITRE promptly implemented its incident response protocols to contain the attack and minimize its impact.

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

PoC Exploit Released for Cisco IMC Flaw – Urgent Update Advised

Proof of Concept (PoC) exploit has been released for a critical vulnerability in Cisco's Integrated Management Controller (IMC).

This flaw, identified as CVE-2024-20356, allows for command injection and could enable attackers to gain root access to affected systems.

Overview of the Vulnerability

The vulnerability resides in the web-based management interface of the Cisco Integrated Management Controller (IMC), a crucial component used for remotely managing Cisco hardware.

According to Cisco's official security advisory, the flaw is due to insufficient user input validation in the IMC interface. This oversight allows an authenticated, remote attacker with administrative privileges to inject malicious commands.

The affected products include a range of Cisco servers and computing systems, notably:

- 5000 Series Enterprise Network Compute Systems (ENCS)
- Catalyst 8300 Series Edge uCPE
- UCS C-Series M5, M6, and M7 Rack Servers in standalone mode
- UCS E-Series Servers
- UCS S-Series Storage Servers

Source : https://cybersecuritynews.com/poc-exploit-cisco-imc/

CYBER SECURITY NEWS

Hackers Posing as LastPass Employee to Steal Master Password & Hijack Accounts

In a sophisticated cyber attack, hackers have been discovered impersonating LastPass employees in an elaborate phishing campaign designed to steal users' master passwords and hijack their accounts.

This alarming development was recently highlighted by LastPass on their official blog, shedding light on the dangers posed by the CryptoChameleon phishing kit.

The campaign, initially identified by cybersecurity firm Lookout, utilizes the CryptoChameleon phishing kit—a notorious tool linked to previous crypto thefts.

.This software allows cybercriminals to create counterfeit websites that look like legitimate services, complete with authentic graphics and logos.

The primary aim is to deceive users into entering their login credentials, which can then be used or sold by the attackers.

Modus Operandi of the Hackers

The attack unfolds in stages, beginning with the victim receiving a phone call from a number that appears to be associated with LastPass. The caller, who speaks with an American accent, claims to be a LastPass employee.

During the conversation, the supposed employee informs the victim of a security issue affecting their account and offers to send an email to help reset their access.

Source : https://cybersecuritynews.com/hackers-posing-lastpass-employee/

New Redline Stealer Variant Leverages Lua Bytecode For Stealthiness

Redline Stealer is a powerful information-stealing malware, and hackers often exploit this stealthy stealer to gain unauthorized access to a victim's sensitive data.

Threat actors can steal many sensitive and valuable data by exploiting the Redline Stealer.

Threat actors can use The stolen data later for financial gain or other malicious purposes.

Cybersecurity researchers at McAfee recently discovered a new variant of Redline stealer that leverages the Lua Bytecode for stealthiness.

Redline Stealer Variant

Telemetry data from McAfee demonstrates that this malware is quite widespread on different continents like North and South America, Europe, Asia, and Australia.

The McAfee Web Advisor has blocked the malware file called "Cheat.Lab.2.7.2.zip" that is hosted in the vcpkg repository of Microsoft's official GitHub.The zip file has an MSI installer with modified Lua binaries and a purported text file for compilation and execution.

Source : https://cybersecuritynews.com/new-redline-stealer-lua-bytecode/

Cerber Linux Ransomware Exploits Atlassian Servers To Take Full Control

Hackers often use Linux ransomware due to its prevalence in server environments. This type of ransomware offers higher potential payouts from organizations with critical data.

Cybersecurity analysts at Cado Security Labs recently analyzed the Linux variant of the Cerber ransomware, which is being deployed on Confluence servers via CVE-2023-22518, after receiving recent reports.

Unlike the well-covered Windows version, little is known about the Linux variant.

It consists of three highly obfuscated, 64-bit UPX-packed C++ ELF payloads, an older approach as threat actors now favor languages like Rust or Go.

Technical Analysis

The aging C++ payloads, almost 8 years old and receiving updates, suggest the original language and tooling choices persist despite Cerber's decreasing activity since its 2016 peak.

While infrequent nowadays, the campaign leverages the popular Confluence vulnerability for distribution.

Following an attacker's use of CVE-2023-22518, researchers tracked Cerber ransomware cases on compromised Confluence. Through an unsecured configuration restore endpoint that facilitates code execution and ransomware, this new flaw enables a threat actor to generate a new administrator account.

Source : https://cybersecuritynews.com/cerber-linux-atlassian-exploit/

Cybercrime Index” Ranks: Russia, Ukraine, and China at the Top

A new “Cybercrime Index” has been introduced, ranking countries based on the threat level posed by cybercriminals.

The Index reveals that many countries, led by Russia, Ukraine, and China, are the primary hubs for cybercriminal activities globally.

Key Findings from the Study

The World Cybercrime Index, developed through a partnership between the University of Oxford, and UNSW, and funded by the European Union-supported CRIMGOV project, provides a detailed ranking of countries based on their cybercrime capabilities and activities.

The top ten nations identified as the most threats are Russia, Ukraine, China, the USA, Nigeria, Romania, North Korea, the UK, Brazil, and India.

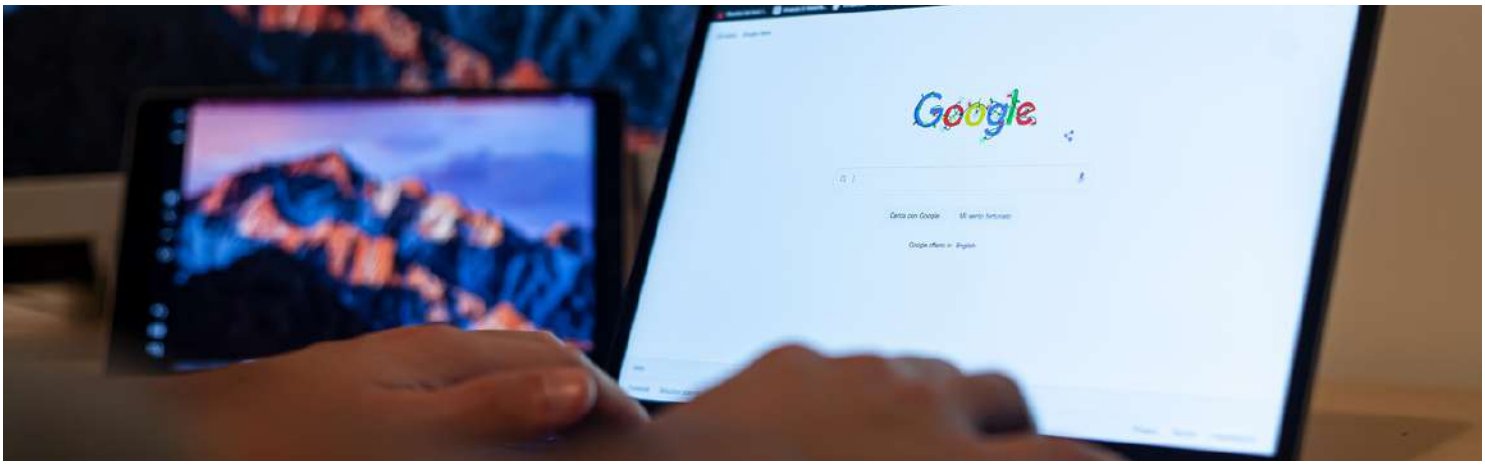
This comprehensive index is based on surveys from 92 leading global experts in cybercrime intelligence and investigations.

The “World Cybercrime Index” ranks countries based on the impact, professionalism, and technical skill of their cybercriminals across five major categories of cybercrime:

1. Technical products/services
2. Attacks and extortion
3. Data/identity theft
4. Scams
5. Cashing out/money laundering

Source : https://cybersecuritynews.com/cybercrime-index-ranks/

CYBER SECURITY NEWS



Chrome Security Update: 23 Vulnerabilities Fixed in Latest Release

Google has announced a comprehensive update to the Chrome and Extended Stable channels.

The latest release, version 124.0.6367.60/.61 for Windows and Mac and version 124.0.6367.60 for Linux, addresses 23 security vulnerabilities.

This update underscores Google's ongoing commitment to safeguarding users against the evolving landscape of cyber threats.

Version and Platform Details

The update has been rolled out for Chrome and Extended Stable channels.

The new version is 124.0.6367.60/.61 for Windows and Mac users, while Linux users will receive version 124.0.6367.60.

Google has indicated that the update will be deployed over the coming days and weeks, ensuring a broad and systematic reach to its global user base.

Highlighted Security Fixes and Rewards

Google's latest security update includes fixes for various high to low-severity vulnerabilities. Notably, the company has awarded a total of $38,000 in rewards to researchers who reported some of these vulnerabilities, highlighting the value of collaborative security research.

Source : https://cybersecuritynews.com/chrome-security-update-23-vulnerabilities/

R00TK1T Claims that They have Acquired Confidential Data from Nestle

The hacker group known as R00TK1T has announced that it has successfully entered the systems of Nestle, the world's largest food and beverage company, and acquired confidential data.

The claim was made through a social media post, which has since caught the attention of cybersecurity experts and corporate watchdogs.

R00TK1T took to social media to declare their latest cyber conquest.

In a ThreatMon tweet that has since circulated among cybersecurity forums, the group boasted about breaching Nestle's defenses and obtaining sensitive data.

The data's specifics and the breach's extent remain unclear, as the group has not released further details.

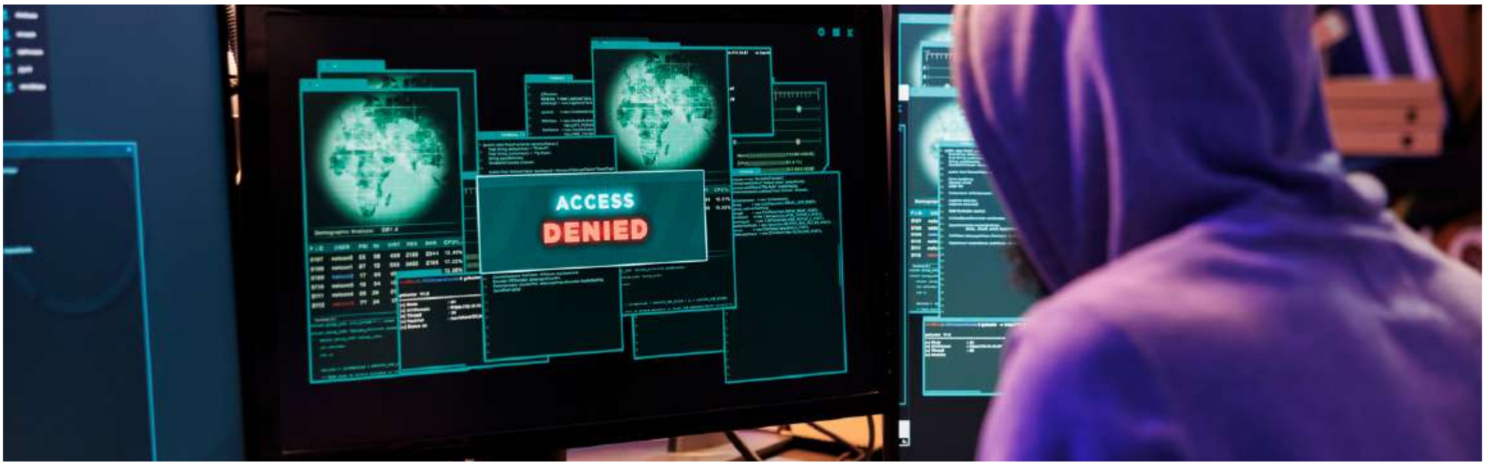
Nestle's Response

Nestle has yet to issue a formal statement regarding the alleged breach.

However, sources within the company have indicated that an internal investigation is underway.

Nestle's spokesperson has assured customers and stakeholders that protecting their data is the utmost priority and that they are taking all necessary steps to assess and address the situation.

Source :https://cybersecuritynews.com/r00tk1t-claims/



Kubernetes Clusters Under Attack: Critical Open Metadata Vulnerabilities Exploited

Microsoft Security recently revealed a sophisticated cyber-attack campaign that targets Kubernetes clusters by exploiting newly discovered vulnerabilities in the OpenMetadata platform.

The attackers have set their sights on Kubernetes workloads, leveraging critical vulnerabilities in the OpenMetadata platform to infiltrate and exploit these systems for cryptomining activities.

OpenMetadata, an open-source platform designed for comprehensive metadata management across various data sources, has become the latest target due to its widespread use and central role in data governance and discovery.

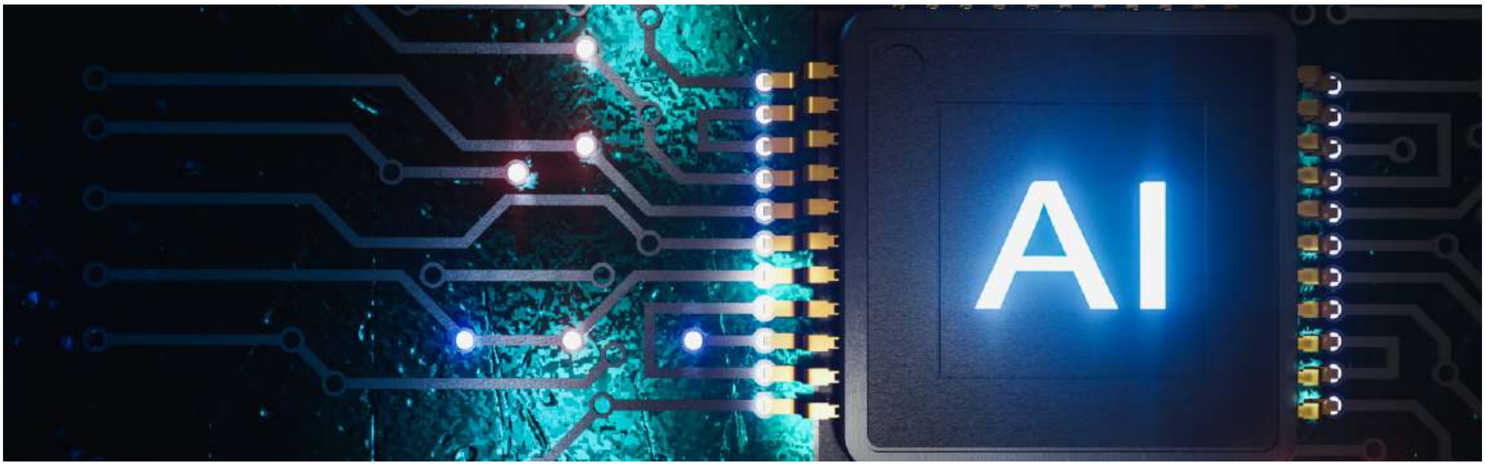
On March 15, 2024, a series of vulnerabilities within the OpenMetadata platform were disclosed, affecting versions prior to 1.3.1.

These vulnerabilities, identified as CVE-2024-28255, CVE-2024-28847, CVE-2024-28253, CVE-2024-28848, and CVE-2024-28254, pose a significant risk as they allow attackers to bypass authentication mechanisms, enabling unauthorized code execution on containers running the vulnerable OpenMetadata versions.

Initial Access and Exploitation

Microsoft said the attack begins by identifying Kubernetes workloads running OpenMetadata that are exposed to the Internet.

Source :https://cybersecuritynews.com/kubernetes-openmetadata-flaws/



Cisco Unveils Hypershield: AI-Powered Automated Vulnerability Shield

Cisco introduced its latest innovation, Cisco Hypershield, marking a significant milestone in the evolution of cybersecurity.

Described as the most consequential security product in the company’s history, Hypershield is a cloud-native, AI-powered solution designed to enhance the security of AI-scale data centers.

This new technology is integrated directly into the network’s fabric, offering a revolutionary approach to protecting digital infrastructures.

Revolutionizing Data Center Security

Cisco Hypershield represents a paradigm shift in network security, turning traditional models on their heads by leveraging the scalability and robustness of hyperscaler security frameworks.

This shift is crucial in an era where digital capacities are expanding exponentially, driven by the widespread adoption of AI technologies across various sectors.

As AI continues to facilitate a new age of digital abundance, the demand for data centers—both public and private—has surged.

Cisco is at the forefront of reimagining how these data centers are connected and secured, ensuring they can handle the increased load without compromising on safety.

Source : https://cybersecuritynews.com/cisco-unveils-hypershield/

“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