QUALYSEC
BEYOND CYBERSECURITY

2023

SEP 4TH WEEK

CYBER SECURITY NEWS

CONTACT US

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

BlackTech APT Hackers Attacking Network Routers to Breach Corporate Networks

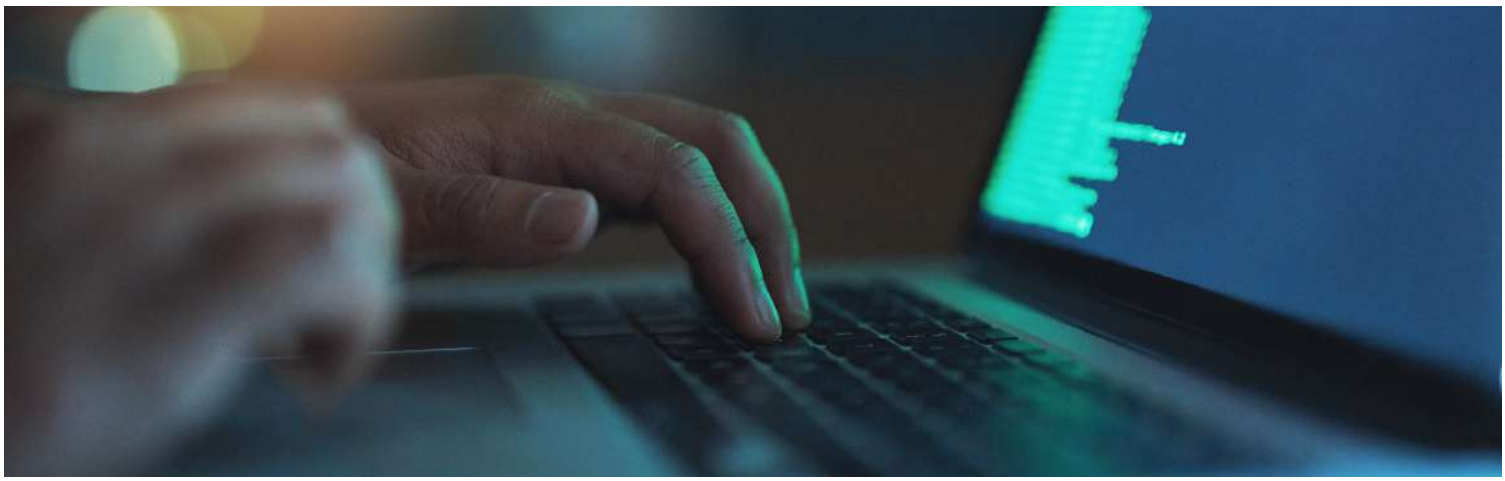
Hackers called BlackTech APT have been doing bad things since 2010. They attack places like the government, factories, technology, media, electronics, phones, and the military.

The group behind the attack employs custom-made malicious software, tools that can be used for both good and bad purposes, and cunning techniques that involve leveraging the resources that already exist within a system, like turning off data recording capabilities on routers, all in an effort to mask their activities.

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) and the Japan National Police Agency (NPA) demonstrated the capabilities of BlackTech in modifying router firmware without detection and exploiting routers' domain-trust relationships for pivoting from international subsidiaries to headquarters in Japan and the U.S.

BlackTech actors continue to update their tools to evade detection, and they also steal code-signing certificates to make their malware appear legitimate.

Source : https://cybersecuritynews.com/blacktech-apt-hackers-routers/



ZenRAT Malware Delivered Through Fake Bitwarden Installation Packages

According to the recent findings by Proofpoint, a new malware called ZenRAT has been discovered. This malware is being spread via fraudulent download packages disguised as Bitwarden installations.

This malware primarily targets Windows users and redirects non-Windows users to benign web pages.

The method of distribution remains unknown, but historical precedents include SEO Poisoning, adware bundles, and email.

ZenRAT is a modular Remote Access Trojan (RAT) with information-stealing capabilities.

The threat landscape in the digital realm is ever-evolving, with malicious actors constantly devising new tactics to exploit unsuspecting victims.

On August 10, 2023, Jérôme Segura, Senior Director of Threat Intelligence at Malwarebytes, brought to light a concerning discovery – a malware sample concealed within a Windows software installation package.

This sample was initially found on a website posing as Bitwarden, bitwariden[.]com, an eerily convincing replica of the legitimate Bitwarden website, reads the report.

Source : https://cybersecuritynews.com/zenrat-malware-bitwarden/

HiddenGh0st Malware Attacking MS-SQL & MySQL Servers

A remote control malware called Gh0st RAT, which is popular with Chinese threat actors and has publicly available source code was created by China's C. Rufus Security Team.

ASEC (AhnLab Security Emergency Response Center) finds the Gh0st RAT variant using a Hidden rootkit to target MS-SQL servers, hiding malware presence and preventing its removal.

The HiddenGh0st is a Gh0st RAT variant with QQ Messenger data theft capabilities that have persisted since 2022 and are likely to target Chinese users. Cybersecurity researchers at ASEC recently reported that HiddenGh0st malware actively targets and attacks poorly managed MS-SQL and MySQL servers.

Hackers Attacking MS-SQL & MySQL Servers

HiddenGh0st evades detection by packing, decrypting, and executing its PE file in memory while transmitting 0x848-sized configuration data.

Besides this, it covers the following things:-

- C&C URL
- Installation method
- Path
- File name
- Rootkit activation

Source :https://cybersecuritynews.com/hiddengh0st-malware/

OPNsense Firewall Flaws Let Attackers Employ XSS to Escalate Privileges

OPNsense is a firewall and routing platform that is based on FreeBSD. It is open-source, making it freely available for use.

Additionally, OPNsense is designed to be user-friendly, with a straightforward interface and simple installation process. Furthermore, it offers the flexibility to customize and tailor to specific needs.

As of its debut in January 2015, it is a fork of pfSense. In addition to its firewall functionality, OPNsense also offers traffic shaping, load balancing, and VPN services, with even more features available via plugins.

Multiple OPNsense Firewall Flaws

The identified vulnerability is located within the OPNsense dashboard, which serves as a graphical user interface presenting various widgets. These widgets provide users with real-time information regarding the system, including running services, gateways, and other relevant data.

The server stores and retrieves the order of the widgets for users, ensuring that it remains unmodified during each visit.

The potential for abuse arises when a user with limited privileges exploits this vulnerability to inject unauthorized content, thereby initiating a cross-site scripting (XSS) attack that can escalate privileges.

Source : https://cybersecuritynews.com/opnsense-firewall-flaws/

‘Ransomed.Vc’ Group Attacking Japanese Giants in New Operations

In the ever-evolving cyber threat landscape, Ransomed.vc, a ransomware syndicate with a rapidly growing reputation on the Dark Web, has once again made headlines. This time, their target is Japan’s telecommunications giant, NTT Docomo.

This development comes hot on the heels of the recent data breach at Sony, which appears to be connected to the activities of Ransomed.vc.

The group is demanding a hefty ransom of $1,015,000 from NTT Docomo after Sony refused to meet their demands, leading to the public release of stolen data, reads Resecurity report.

The big question now is whether this signals the beginning of a new wave of cyberattacks targeting Japan.

Ransomed.vc, which started as an underground forum in August 2023, has rapidly transformed into a formidable ransomware syndicate.

Initially focusing on data leaks, access brokerage, vulnerabilities, exploits, and other cybercriminal tradecrafts, the forum aimed to build a thriving community of like-minded individuals.

Their credit system, rewarding members based on their activity, incentivized the sharing of valuable, previously undisclosed information.

Source : https://cybersecuritynews.com/ransomed-vc-japanese-giants/

Threat Actors Use Abnormal Certificates to Deliver Info-stealing Malware

Malicious certificates can be highly dangerous as they can be used to deceive users into trusting malicious websites or software.

This can lead to various security threats, including:-

- Data breaches
- Malware infections
- Phishing attacks
- Compromise user privacy
- Compromise system integrity

Cybersecurity researchers at ASEC (AhnLab Security Emergency Response Center) recently identified that threat actors are exploiting abnormal certificates to deliver info-stealing malware.

Technical Analysis

Malicious code mimics certificates with randomly entered info, causing unusually long Subject and Issuer Names.

Certificate info remains hidden in Windows, which is only detectable with specific tools. So, the incorrect certificate and its information are useless for signature verification.

The signature uses non-English languages and special characters and shows little variation for over two months, suggesting a specific intention.

Source : https://cybersecuritynews.com/threat-actors-abnormal-certificates/

Cisco DNA Center Vulnerability Let Attacker Modify Internal Data

An attacker can exploit the vulnerability in question by using a carefully crafted API request directed toward a device that is susceptible to the vulnerability.

The potential for a successful exploit exists, which would grant the attacker unauthorized access to read and manipulate data that is managed by an internal service on the device that has been impacted.

Workarounds & Updates

Cisco has recently made available free software updates that effectively mitigate the vulnerability as described. Customers who are unable to upgrade to a fixed release have the option to implement a workaround to address this vulnerability.

Cisco recommends contacting their Cisco Technical Assistance Center (TAC) for guidance and support during implementation.

According to the Cisco Product Security Incident Response Team (PSIRT), there are no public announcements or instances of malicious exploitation about the vulnerability outlined in this advisory.

Source : https://cybersecuritynews.com/cisco-dna-center-vulnerability/

Firefox 118 Released With the Fix for 6 High-Severity Vulnerabilities

Mozilla has recently launched Firefox 118, which addresses a total of nine security vulnerabilities. Notably, this release effectively resolves six high-severity vulnerabilities that were previously identified.

The majority of vulnerabilities identified are associated with memory-related concerns, which have the potential to result in exploitable crashes.

The vulnerabilities identified as CVE-2023-5168 and CVE-2023-5169 pertain to high-severity instances of Out-of-bounds writing in the PathOps and FilterNodeD2D1 components.

It can be leveraged through the provision of compromised content, resulting in a potentially exploitable crash.

The vulnerability identified as CVE-2023-5170 pertains to a memory leak concern that has the potential to facilitate the creation of a sandbox escape, provided that the specific data required for leakage is obtained.

Another vulnerability with the identifier CVE-2023-5171 occurs during the garbage collection process and leads to a use-after-free condition.

Source : https://cybersecuritynews.com/firefox-118-released/

New GPU Side Channel Vulnerability Impacts GPUs from Intel, AMD, Apple & Nvidia

A new research paper has been published that mentions a side-channel attack that threat actors can exploit to leak sensitive visual data from modern GPU cards when visiting a malicious website.

This method was published under the name “GPU.zip” by four American universities: the University of Texas at Austin, Carnegie Mellon University, the University of Washington, and the University of Illinois. The attack simulation was based on a cross-origin SVG filter pixel-stealing attack via Chrome browser for research purposes.

GPU Side-Channel Vulnerability

The lead author Yingchen Wang mentions in his research paper that this attack was due to the undocumented ways of compression used by vendors like Intel and AMD. These vendor-specific compressions took place even when the software program did not specifically request compression.

“Compression induces data-dependent DRAM traffic and cache utilization, which can be measured through side-channel analysis. Unfortunately, besides its well-recognized performance benefits, compression is also a known source of side-channel data leakages. ” reads the research paper.

Source :https://cybersecuritynews.com/gpu-side-channel-vulnerability/

Google Fixes Actively Exploited Zero-day Vulnerability : Patch Now!

Google Chrome version 117.0.5938.132 for Windows, Mac, and Linux has been set to release with multiple bug fixes and features. As per Google, this new version will be rolled out in a few weeks or days.

Previously, Google has fixed multiple vulnerabilities in Chrome version 117.0.5938.62, which were associated with Insufficient policy enforcement, Inappropriate Implementation of Prompts, Inputs, Intents, and much more.Google Chrome Zero-day

As per the release from Google Chrome, 10 security fixes were issued along with three high-severity vulnerabilities as part of this release. The vulnerabilities were CVE-2023-5217, CVE-2023-5186, and CVE-2023-5187. The severity of these vulnerabilities is being analyzed for categorization by the National Vulnerability Database (NVD).

However, CVE-2023-5217 is known to have been exploited in the wild. This was a Heap buffer overflow vulnerability that existed in the vp8 encoding in libvpx. Google provided no further information about this vulnerability.

CVE-2023-5186 was a Use-after-free condition in the Passwords, and CVE-2023-5187 was another Use-after-free condition in Extensions of Google Chrome.

Source : https://cybersecuritynews.com/google-chrome-zero-day-flaw/

Chinese Hackers Breached Microsoft's Email Platform to Steal 60,000+ US Govt Emails

In a significant cybersecurity breach, Chinese hackers successfully infiltrated Microsoft's email platform earlier this year, leading to the theft of tens of thousands of emails from the U.S. State Department accounts, according to information shared by a Senate staffer who attended a briefing by State Department IT officials.

The breach came to light as State Department IT officials revealed that approximately 60,000 emails were stolen from ten State Department accounts during the attack.

Notably, nine of the affected accounts were linked to individuals working on matters concerning East Asia and the Pacific, while one account was focused on European affairs.

This revelation is part of an ongoing investigation into a series of cyberattacks that have rocked various U.S. organizations.

Sophisticated Infiltration:

In July, both U.S. officials and Microsoft disclosed that state-linked Chinese hackers had gained unauthorized access to email accounts in approximately 25 different organizations, including the U.S. Commerce and State Departments.

Source :https://cybersecuritynews.com/chinese-hackers-microsofts-email-platform/

“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