QUALYSEC
BEYOND CYBERSECURITY

2024

FEB 1ST WEEK

CYBER SECURITY NEWS

CONTACT US

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

URGENT: AnyDesk Servers Hacked, Customers Urged to Reset Passwords

It has been confirmed that AnyDesk, a renowned remote access software company headquartered in Germany, which boasts a staggering 170,000 customers worldwide, including big names such as Comcast and Thales, has fallen prey to a security breach that has compromised its production systems.

“We have revoked all security-related certificates, and systems have been remediated or replaced where company’s,” the company said.

According to recent media reports, AnyDesk has been targeted by attackers who are believed to have stolen source code and code signing certificates.

However, AnyDesk has not yet officially confirmed these reports. Nonetheless, the company has confirmed that the incident was not a ransomware attack, which is reassuring for its customers and users.

According to AnyDesk, their investigation has revealed that there is no evidence to suggest that the cyberattack led to the theft of any private keys, tokens, or passwords that could be used to gain access to end-user devices. Moreover, the company has confirmed that, at present, there are no indications that the breach has had any impact on any end-user devices.

Source : https://cybersecuritynews.com/anydesk-servers-hacked/

US Disrupts Chinese Botnet that Hijacks SOHO Routers

In a decisive action, the U.S. The Department of Justice (DOJ) has disrupted a cyber operation by Chinese state-sponsored hackers.

This operation, codenamed Volt Typhoon, targeted American critical infrastructure using a vast network of compromised routers.

Hundreds of small office/home office (SOHO) routers, primarily Cisco and NetGear models past their "end-of-life" status, were infected with the "KV Botnet" malware. This malware served as a hidden gateway, allowing the attackers to conceal their activities and target critical infrastructure across the nation.

Taking Back Control: A Court-Authorized Cleanup: Through a landmark court order, the DOJ conducted a meticulous operation to dismantle this cyber threat. The compromised routers were remotely accessed and cleansed of the malicious software.

Additionally, measures were taken to sever their connection to the botnet, effectively neutralizing them as tools for further attacks.

A Multi-Pronged Defense: This operation went beyond mere malware removal. The DOJ and its partners, including the FBI, CISA, and private sector entities, are proactively safeguarding critical infrastructure and educating the public.

Source :https://cybersecuritynews.com/us-disrupts-chinese-botnet/

Cloudflare's Server Hacked Using Leaked Access Token in Okta Breach

Cloudflare discovered a threat actor on the self-hosted Atlassian server on November 23, 2023. The attack was launched with the use of one stolen access token and three compromised service account credentials that were neglected to change following the October 2023 Okta compromise.

To analyze the incident, the security team engaged the help of CrowdStrike's Forensic team. On November 24, all connections and access for threat actors were cut off.

"We want to emphasize to our customers that no Cloudflare customer data or systems were impacted by this event," according to Cloudflare's blog.

"We took this incident very seriously because a threat actor had used stolen credentials to get access to our Atlassian server and accessed some documentation and a limited amount of source code."

Overview of the Incident

Threat actors conducted a survey from November 14 to November 17, after which they gained access to their internal wiki (powered by Atlassian Confluence) and bug database (powered by Atlassian Jira).

On November 20 and 21, they detected further access indicating they may have returned back to test access to ensure they had connectivity.

On November 22, they made a return visit and used ScriptRunner for Jira to gain persistent access to the Atlassian server.

Source : https://cybersecuritynews.com/cloudflare-server-hacked/

USB Malware Chained with Text Strings on Legitimate Websites Attacks Users

Despite the evolution of several tools and tactics, threat actors still go with the traditional approach to attack victims for malicious purposes. One such threat actor is UNC4990, which uses USB devices to exploit victims. UNC4990 is a financially motivated threat actor and has been conducting campaigns since 2020.

There has been a continuous evolution of this threat actor's activities. With that being said, the recent tactics involved the use of popular and legitimate websites such as GitHub, GitLab, Ars Technica and Vimeo.

In addition, the threat actor has been using EMPTYSPACE downloader and QUIETBOARD backdoor. EMPTYSPACE is capable of executing any payload served from the command and control servers, and QUIETBOARD is also delivered using EMPTYSPACE.

USB Malware Chained with Text Strings

Initial Vector

According to the reports shared with Cyber Security News, the threat actor begins the infection chain by delivering the USB drives to the victims by any means of social engineering. Once the victim connects the USB to their device, the USB removable device is shown with a shortcut (.LNK extension) under the vendor name.

Source : https://cybersecuritynews.com/usb-malware-with-text-strings/

VileRAT Attacking Windows Machines via Malicious Software

A new variant of VileRAT is being distributed through fake software pirate websites to infect Windows systems on a large scale.

This Python-based VileRAT malware family is believed to be specific to the Evilnum threat group, DeathStalker, which has been active since August 2023.

It is frequently observed being spread by the VileLoader loader, which is designed to run VileRAT in-memory and limit on-disk artifacts.

It functions similarly to conventional remote access tools, allowing attackers to record keystrokes, run commands, and obtain information remotely. Because VileRAT is extensible and modular, actors can use the framework to implement new features.

According to public reports, Evilnum is a hacker-for-hire service with a history of attacking governments, legal offices, financial institutions, and cryptocurrency-related organizations in the Middle East, the UK, the EU, and the Americas.

New Variants of VileRAT- Researchers at Stairwell have seen new activity and VileRAT variants spread through modified, legitimate installers that also carry VileLoader.Kaspersky reported that in the past, the infection was distributed via malicious documents and LNK files, as well as utilizing companies' public chatbots.

Source : https://cybersecuritynews.com/vilerat-attacking-windows-machines/

Russian APTs Employ HTTP-Shell to Attack Government Entities

Recently, Cluster25, a threat intelligence firm, uncovered a spear-phishing campaign dubbed “The Bear and the Shell,” specifically targeting entities critical of the Russian government and aligned with dissident movements.

The campaign leverages social engineering tactics, employing seemingly legitimate lures to deceive victims.

One example involves a NASA-themed email containing a ZIP file disguised as a job offer. Upon opening, the file unleashes a multiplatform reverse shell named HTTP-Shell, granting attackers remote access to the victim’s system. This shell, while open-source, can be manipulated for malicious purposes, enabling file transfers, directory navigation, and establishing connections to a command and control (C&C) server. In this case, the C&C server masqueraded as a PDF editing site to further evade detection.

Beyond NASA: A Broader Web of Deception

The investigation revealed more than just a single attack. Cluster 25 discovered additional campaigns with striking similarities.

They all utilized the same kill chain, employed identical shortcut icons, and shared some lure themes. This evidence suggests a coordinated effort targeting various individuals and organizations.

Source : https://cybersecuritynews.com/russian-apt-shell-attack/

Hackers Use Compromised Routers to Attack Government Organizations

Attackers continue to use compromised routers as malicious infrastructure to target government organizations in Europe and the Caucasus region.

APT28 threat actors (also known as Sofacy, Fancy Bear, etc.) were behind this malicious espionage effort, according to the Ukrainian government's computer emergency and incident response team (CERT-UA).

By tricking users into visiting a remote HTML page and opening a Windows shortcut, the malicious campaign used spear-phishing to distribute credential stealer (STEELHOOK), remote execution tools (MASEPIE, OCEANMAP), and a publicly accessible reconnaissance and credentials harvesting tool (Impacket).

"We believe with high confidence that the malicious infrastructure leveraged in this campaign is notably (and likely mainly) built from legitimate compromised Ubiquiti network devices," HarfangLab shared with Cyber Security News.

How is the Attack Executed?

The threat actor delivered phishing emails to the designated individuals using previously hacked email accounts. The links in the phishing emails led to malicious webpages that tricked the targets into clicking a button to display a document by showing them a blurry preview.

Source :https://cybersecuritynews.com/hackers-compromised-routers/

Hackers Exploit Trusted Platform Redirect Flaws For Phishing Attacks

Attackers abuse trustworthy platforms for redirection, which involves the use of legitimate websites to redirect users to harmful URL destinations.

In this ever-evolving world of cyber threats, phishing attempts are getting more frequent, with email being one of the primary targets. Experts have noted a notable increase in phishing attempts that take advantage of open redirect vulnerabilities.

The major purpose is to avoid detection mechanisms and exploit user confidence by leveraging the trusted platform's reputation and employing anti-phishing analytical techniques such as intricate redirection chains.

What is Open URL Redirection Vulnerability?

A web application receives user-controlled input that provides a link to an external site, which is then used in a redirect. This makes phishing attempts easier.

According to the SpiderLabs team at Trustwave, this kind of web application vulnerability arises when users can be directed to untrusted websites by using input that hasn't been verified, which could take them to websites run by attackers, including phishing sites.

Source : https://cybersecuritynews.com/open-redirect-flaws-phishing-attacks/

WhatsApp Privacy Flaw Devices Information to Any Other User

Hackers seek to exploit WhatsApp flaws to gain unauthorized access to user data, messages, and sensitive information.

Exploiting these flaws allows threat actors to compromise user privacy, conduct espionage, and engage in malicious activities.

Recently, a cybersecurity analyst, Tal Be'ery, discovered a WhatsApp privacy flaw that devices information on any other user.

WhatsApp Privacy Flaw

For message confidentiality, WhatsApp, with over 5 billion downloads and 2.4 billion active users, relies on the End-to-End Encryption (E2EE) protocol.

WhatsApp introduced E2EE in 2016, where each app generates a unique crypto key for secure messaging. This key is tied to the device that changes during reinstallation to notify other users that a device switch has occurred.

WhatsApp prevents information leaks during app reinstallation by maintaining the same key if restored from backup. In 2021, with multi-device architecture, companion devices generate their keys known as 'Identity keys,' valid until the app is uninstalled.

The sender creates session keys for each device based on its Identity Key when sending a message to a multi-device recipient.

Source : https://cybersecuritynews.com/whatsapp-privacy-flaw/

Hackers Exchanging Hundreds Of Network Operators' Credentials on Dark Web

A recent cyberattack on Orange España highlights the vulnerability of telecom network personnel and the critical need for improved digital hygiene.

Hackers are actively targeting network engineers and IT infrastructure managers, seeking access to the organization's sensitive data and infrastructure. This alarming report by Resecurity reveals a disturbing trend: hundreds of network engineers' credentials for organizations worldwide are being sold on the dark web. These compromised credentials grant attackers access to sensitive systems and data, potentially leading to devastating cyberattacks.

In January 2024, attackers hijacked an Orange España employee's computer, stealing credentials for their RIPE NCC account.

The Dark Web: A Hunting Ground for Credentials

Resecurity's investigation uncovered over 1,500 compromised credentials for regional internet registries, including RIPE, APNIC, AFRINIC, and LACNIC.

These credentials were likely stolen by info stealers, malware designed to silently collect sensitive information.

Worryingly, some credentials were offered for as little as $10, making them readily accessible to cybercriminals.

Source : https://cybersecuritynews.com/credentials-dark-web/

“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