Cloud Consultancy
DIGITALIZATION & SECURITY

CCDS CYBER SECURITY PICKS

49th Release April 2023

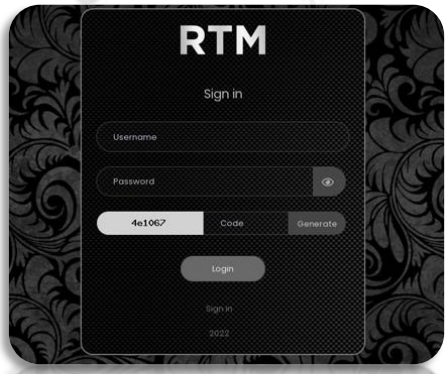
U.S. and U.K. Warn of Russian Hackers Exploiting Cisco Router Flaws for Espionage

U.K. and U.S. cybersecurity and intelligence agencies have warned of Russian nation-state actors exploiting now-patched flaws in networking equipment from Cisco to conduct reconnaissance and deploy malware against select targets.

The intrusions, per the authorities, took place in 2021 and targeted a small number of entities in Europe, U.S. government institutions, and about 250 Ukrainian victims.

The activity has been attributed to a threat actor tracked as APT28, which is also known as Fancy Bear.

Source:https://thehackernews.com/2023/04/us-and-uk-warn-of-russian-hackers.html



RTM Locker: Emerging Cybercrime Group Targeting Businesses with Ransomware

Cybersecurity researchers have detailed the tactics of a "rising" cybercriminal gang called "Read The Manual" (RTM) Locker that functions as a private ransomware-as-a-service (RaaS) provider and carries out opportunistic attacks to generate illicit profit.

"The 'Read The Manual' Locker gang uses affiliates to ransom victims, all of whom are forced to abide by the gang's strict rules," cybersecurity firm Trellix said in a report shared with The Hacker News.

Source:https://thehackernews.com/2023/04/rtm-locker-emerging-cybercrime-group.html

Microsoft Issues Patches for 97 Flaws, Including Active Ransomware Exploit

Microsoft has released another set of security updates to fix a total of 97 flaws impacting its software, one of which has been actively exploited in ransomware attacks in the wild.

The security flaw that's come under active exploitation is CVE-2023-28252 (CVSS score: 7.8), a privilege escalation bug in the Windows Common Log File System (CLFS) Driver."An attacker who successfully exploited this vulnerability could gain SYSTEM privileges," Microsoft said in an advisory, crediting researchers Boris Larin, Genwei Jiang, and Quan Jin for reporting the issue.

Source:https://thehackernews.com/2023/04/urgent-microsoft-issues-patches-for-97.html

Taiwanese PC Company MSI Falls Victim to Ransomware Attack

Taiwanese PC company MSI (short for Micro-Star International) officially confirmed it was the victim of a cyber attack on its systems.

The company said it "promptly" initiated incident response and recovery measures after detecting "network anomalies." It also said it alerted law enforcement agencies of the matter.That said, MSI did not disclose any specifics about when the attack took place and if it entailed the exfiltration of any proprietary information, including source code.

Source:https://thehackernews.com/2023/04/taiwanese-pc-company-msi-falls-victim.html

Google Gets Court Order to Take Down CryptBot That Infected Over 670,000 Computers

Google said it obtained a temporary court order in the U.S. to disrupt the distribution of a Windows-based information-stealing malware called CryptBot and "decelerate" its growth.

CryptBot is estimated to have infected over 670,000 computers in 2022 with the goal of stealing sensitive data such as authentication credentials, social media account logins, and cryptocurrency wallets from users of Google Chrome..

Source:https://thehackernews.com/2023/04/google-gets-court-order-to-take-down.html

Google Chrome Hit by Second Zero-Day Attack - Urgent Patch Update Released

Google rolled out emergency fixes to address another actively exploited high-severity zero-day flaw in its Chrome web browser.

The flaw, tracked as CVE-2023-2136, is described as a case of integer overflow in Skia, an open source 2D graphics library. Clément Lecigne of Google's Threat Analysis Group (TAG) has been credited with discovering and reporting the flaw on April 12, 2023.

"Integer overflow in Skia in Google Chrome prior to 112.0.5615.137 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page," according to the NIST's National Vulnerability Database (NVD).

Users are recommended to upgrade to version 112.0.5615.137/138 for Windows, 112.0.5615.137 for macOS, and 112.0.5615.165 for Linux to mitigate potential threats.

Source: https://thehackernews.com/2023/04/google-chrome-hit-by-second-zero-day.html

Google Launches New Cybersecurity Initiatives to Strengthen Vulnerability Management

Google outlined a set of initiatives aimed at improving the vulnerability management ecosystem and establishing greater transparency measures around exploitation.

"While the notoriety of zero-day vulnerabilities typically makes headlines, risks remain even after they're known and fixed, which is the real story," the company said in an announcement. "Those risks span everything from lag time in OEM adoption, patch testing pain points, end user update issues and more."

Security threats also stem from incomplete patches applied by vendors, with a chunk of the zero-days exploited in the wild turning out to be variants of previously patched vulnerabilities.
Source:https://thehackernews.com/2023/04/google-launches-new-cybersecurity.html

Contact Us

Cloud Consultancy

Cloud Consultancy for Digitalization & Security – CCDS's is a Specialized Company in IT and Information Security Services, which has its international headquarters in the UAE. It also has branch offices throughout the MENA Region with its premier office in Saudi Arabia. Innovative and professional in its approach, it always partners with best-in-class products and services, to identify and solve security threats and issues for its clients.