Cloud Consultancy
For Digitalization & Security

CCDS CYBER SECURITY PICKS

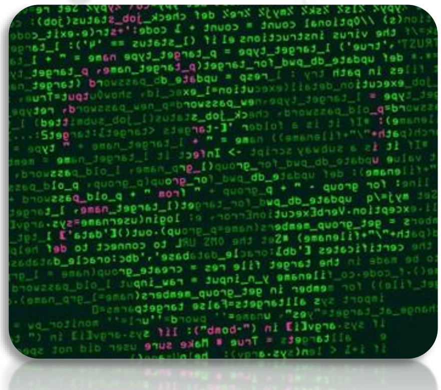
41st Release August 2022

FBI Warns Investors to Take Precautions with Decentralized Financial Platforms

The U.S. Federal Bureau of Investigation (FBI) on Monday warned of cyber criminals increasingly exploiting flaws in decentralized finance (DeFi) platforms to plunder cryptocurrency.

"The FBI has observed cyber criminals exploiting vulnerabilities in the smart contracts governing DeFi platforms to steal investors' cryptocurrency," the agency said in a notification

Source:https://thehackernews.com/2022/08/fbi-warns-investors-to-take-precautions.html



New Golang-based 'Agenda Ransomware' Can Be Customized For Each Victim

A new ransomware strain written in Golang dubbed "Agenda" has been spotted in the wild, targeting healthcare and education entities in Indonesia, Saudi Arabia, South Africa, and Thailand.

"Agenda can reboot systems in safe mode, attempts to stop many server-specific processes and services, and has multiple modes to run," Trend Micro researchers said in an analysis last week.

Source:https://thehackernews.com/2022/08/new-golang-based-agenda-ransomware-can.html

Okta Hackers Behind Twilio and Cloudflare Breach Hit Over 130 Organizations

The threat actor behind the attacks on Twilio and Cloudflare earlier this month has been linked to a broader phishing campaign aimed at 136 organizations that resulted in a cumulative compromise of 9,931 accounts.

The activity has been condemned 0ktapus by Group-IB because the initial goal of the attacks was to "obtain Okta identity credentials and two-factor authentication (2FA) codes from users of the targeted organizations."

Source:https://thehackernews.com/2022/08/okta-hackers-behind-twilio-and.html

Researchers Warn of AiTM Attack Targeting Google G-Suite Enterprise Users

The threat actors behind a large-scale adversary-in-the-middle (AiTM) phishing campaign targeting enterprise users of Microsoft email services have also set their sights on Google Workspace users."This campaign specifically targeted chief executives and other senior members of various organizations which use [Google Workspace]," Zscaler researchers Sudeep Singh and Jagadeeswar Ramanukolanu detailed in a report published this month.

Source:https://thehackernews.com/2022/08/researchers-warn-of-aitm-attack.html

CISA Warns of Active Exploitation of Palo Alto Networks' PAN-OS Vulnerability

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Monday added a security flaw impacting Palo Alto Networks PAN-OS to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation. The high-severity vulnerability, tracked as CVE-2022-0028 (CVSS score: 8.6), is a URL filtering policy misconfiguration that could allow an unauthenticated, remote attacker to carry out reflected and amplified TCP denial-of-service (DoS) attacks

Source:https://thehackernews.com/2022/08/cisa-warns-of-active-exploitation-of.html

The Rise of Data Exfiltration and Why It Is a Greater Risk Than Ransomware

Ransomware is the de facto threat organizations have faced over the past few years. Threat actors were making easy money by exploiting the high valuation of cryptocurrencies and their victims' lack of adequate preparation.

Think about bad security policies, untested backups, patch management practices not up-to-par, and so forth. It resulted in easy growth for ransomware extortion, a crime that multiple threat actors around the world perpetrate.

Something's changed, though. Crypto valuations have dropped, reducing the monetary appeal of ransomware attacks due to organizations mounting a formidable defense against ransomware.

Source: https://thehackernews.com/2022/08/the-rise-of-data-exfiltration-and-why.html

Microsoft Issues Patches for 121 Flaws, Including Zero-Day Under Active Attack

As many as 121 new security flaws were patched by Microsoft as part of its Patch Tuesday updates for the month of August, which also includes a fix for a Support Diagnostic Tool vulnerability that the company said is being actively exploited in the wild.

Of the 121 bugs, 17 are rated Critical, 102 are rated Important, one is rated Moderate, and one is rated Low in severity. Two of the issues have been listed as publicly known at the time of the release.

Topping the list of patches is CVE-2022-34713 (CVSS score: 7.8), a case of remote code execution affecting the Microsoft Windows Support Diagnostic Tool (MSDT)

Source:https://thehackernews.com/2022/08/microsoft-issues-patches-for-121-flaws.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.