CCDS CYBER SECURITY PICKS

40th Release July 2022

Over a Dozen Android Apps on Google Play Store Caught Dropping Banking Malware

A malicious campaign leveraged seemingly innocuous Android dropper apps on the Google Play Store to compromise users' devices with banking malware.
These 17 dropper apps, collectively dubbed DawDropper by Trend Micro, masqueraded as productivity and utility apps such as document scanners, QR code readers, VPN services, and call recorders, among others.
Attack chains involved the DawDropper malware establishing connections with a Firebase Realtime Database to receive the GitHub URL necessary to download the malicious APK file.

Source:https://thehackernews.com/2022/07/over-dozen-android-apps-on-google-play.html

Microsoft Details App Sandbox Escape Bug Impacting Apple iOS, iPad OS, macOS Devices

Microsoft on Wednesday shed light on a now patched security vulnerability affecting Apple's operating systems that, if successfully exploited, could allow attackers to escalate device privileges and deploy malware.

“An attacker could take advantage of this sandbox escape vulnerability to gain elevated privileges on the affected device or execute malicious commands like installing additional payloads," Jonathan Bar Or of the Microsoft 365 Defender Research Team said in a write up.

Source:https://thehackernews.com/2022/07/microsoft-details-app-sandbox-escape.html

North Korean Hackers Using Malicious Browser Extension to Spy on Email Accounts

A threat actor operating with interests aligned with North Korea has been deploying a malicious extension on Chromium-based web browsers that's capable of stealing email content from Gmail and AOL.
Cybersecurity firm Volexity attributed the malware to an activity cluster it calls SharpTongue, which is said to share overlaps with an adversarial collective publicly referred to under the name Kimsuky.SharpTongue has a history of singling out individuals working for organizations in the U.S., Europe, and South Korea.

Source:https://thehackernews.com/2022/07/north-korean-hackers-using-malicious.html

Spanish Police Arrest 2 Nuclear Power Workers for Cyberattacking the Radiation Alert System

Spanish law enforcement officials have announced the arrest of two individuals in connection with a cyberattack on the country's radioactivity alert network (RAR), which took place between March and June 2021..The act of sabotage is said to have disabled more than one-third of the sensors that are maintained by the Directorate-General for Civil Protection and Emergencies (DGPCE) and used to monitor excessive radiation levels across the country.

Source:https://thehackernews.com/2022/07/spanish-police-arrest-2-nuclear-power.html

Microsoft Resumes Blocking Office VBA Macros by Default After 'Temporary Pause'

Microsoft has officially resumed blocking Visual Basic for Applications (VBA) macros by default across Office apps, weeks after temporarily announcing plans to roll back the change.

Earlier this February, Microsoft publicized its plans to disable macros by default in Office applications such as Access, Excel, PowerPoint, Visio, and Word as a way to prevent threat actors from abusing the feature to deliver malware.

Source:https://thehackernews.com/2022/07/microsoft-resumes-blocking-office-vba.html

Update Google Chrome Browser to Patch New Zero-Day Exploit Detected in the Wild

Google on Monday shipped security updates to address a high-severity zero-day vulnerability in its Chrome web browser that it said is being exploited in the wild.

The shortcoming, tracked as CVE-2022-2294, relates to a heap overflow flaw in the WebRTC component that provides real-time audio and video communication capabilities in browsers without the need to install plugins or download native apps.

Heap buffer overflows, also referred to as heap overrun or heap smashing, occur when data is overwritten in the heap area of the memory, leading to arbitrary code execution or a denial-of-service (DoS) condition.

Users are recommended to update to version 103.0.5060.114 for Windows, macOS, and Linux and 103.0.5060.71 for Android to mitigate potential threats. Users of Chromium-based browsers such as Microsoft Edge, Brave, Opera, and Vivaldi are also advised to apply the fixes as and when they become available.

Source: https://thehackernews.com/2022/07/update-google-chrome-browser-to-patch.html

Microsoft Uncovers Austrian Company Exploiting Windows and Adobe Zero-Day Exploits

The company, which Microsoft describes as a private-sector offensive actor (PSOA), is an Austria-based outfit called DSIRF that's linked to the development and attempted sale of a piece of cyberweapon referred to as Subzero, which can be used to hack targets' phones, computers, and internet-connected devices.Microsoft is tracking the actor under the moniker KNOTWEED, continuing its trend of terming PSOAs using names given to trees and shrubs. The company previously designated the name SOURGUM to Israeli spyware vendor Candiru. KNOTWEED is known to dabble in both access-as-a-service and hack-for-hire operations, offering its toolset to third parties as well as directly associating itself in certain attacks.

Source:https://thehackernews.com/2022/07/microsoft-uncover-austrian-company.html

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.

Contact Us