Cloud Consultancy
DIGITALIZATION & SECURITY

CCDS CYBER SECURITY PICKS

54th Release - September 2023

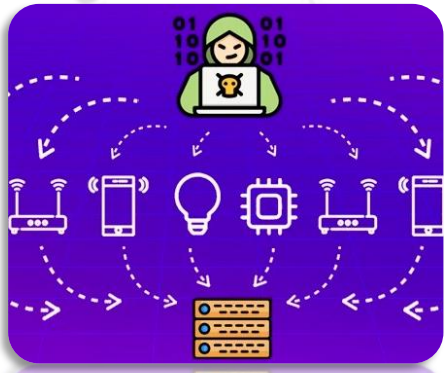
Mysterious 'Sandman' Threat Actor Targets Telecom Providers Across Three Continents

A previously undocumented threat actor dubbed Sandman has been attributed to a set of cyber attacks targeting telecommunic koation providers in the Middle East, Western Europe, and the South Asian subcontinent.

Notably, the intrusions leverage a just-in-time (JIT) compiler for the Lua programming language known as LuaJIT as a vehicle to deploy a novel implant called LuaDream.

String artifacts contained within the implant's source code reference June 3, 2022, indicating that the preparatory work has been underway for more than a year.

Source:https://thehackernews.com/2023/09/mysterious-sandman-threat-actor-targets.html



DDoS 2.0: IoT Sparks New DDoS Alert

The Internet of Things (IoT) is transforming efficiency in various sectors like healthcare and logistics but has also introduced new security risks, particularly IoT-driven DDoS attacks.

Botnets are nothing new, but IoT botnets pose a specific threat. The number of IoT devices reached 16 billion in 2022 and is expected to exceed 30 billion by 2025. These devices often suffer from infrequent updates or insecure default settings, or are simply left unattended, making them less secure than traditional computers and are at risk of being hijacked with relative ease to form potent botnets.

Source:https://thehackernews.com/2023/09/ddos-20-iot-sparks-new-ddos-alert.html

Cybercriminals Combine Phishing and EV Certificates to Deliver Ransomware Payloads

The threat actors behind RedLine and Vidar information stealers have been observed pivoting to ransomware through phishing campaigns that spread initial payloads signed with Extended Validation (EV) code signing certificates.

"This suggests that the threat actors are streamlining operations by making their techniques multipurpose," Trend Micro researchers said in a new analysis published this week.

Source:https://thehackernews.com/2023/09/cybercriminals-combine-phishing-and-ev.html

Update Chrome Now: Google Releases Patch for Actively Exploited Zero-Day Vulnerability

Google rolled out fixes to address a new actively exploited zero-day in the Chrome browser.

Tracked as CVE-2023-5217, the high-severity vulnerability has been described as a heap-based buffer overflow in the VP8 compression format in libvpx, a free software video codec library from Google and the Alliance for Open Media (AOMedia).

Source:https://thehackernews.com/2023/09/update-chrome-now-google-releases-patch.html

Apple Rushes to Patch 3 New Zero-Day Flaws: iOS, macOS, Safari, and More Vulnerable

Apple has released yet another round of security patches to address three actively exploited zero-day flaws impacting iOS, iPadOS, macOS, watchOS, and Safari, taking the total tally of zero-day bugs discovered in its software this year to 16.

Apple did not provide additional specifics barring an acknowledgement that the "issue may have been actively exploited against versions of iOS before iOS 16.7."

Source:https://thehackernews.com/2023/09/apple-rushes-to-patch-3-new-zero-day.html

Beware: Fake Exploit for WinRAR Vulnerability on GitHub Infects Users with Venom RAT

A malicious actor released a fake proof-of-concept (PoC) exploit for a recently disclosed WinRAR vulnerability on GitHub with an aim to infect users who downloaded the code with Venom RAT malware.

"The fake PoC meant to exploit this WinRAR vulnerability was based on a publicly available PoC script that exploited a SQL injection vulnerability in an application called GeoServer, which is tracked as CVE-2023-25157," Palo Alto Networks Unit 42 researcher Robert Falcone said.

whalersplonk, the GitHub account that hosted the repository, is no longer accessible. The PoC is said to have been committed on August 21, 2023, four days after the vulnerability was publicly announced.

Source: https://thehackernews.com/2023/09/beware-fake-exploit-for-winrar.html

Trend Micro Releases Urgent Fix for Actively Exploited Critical Security Vulnerability

Cybersecurity company Trend Micro has released patches and hotfixes to address a critical security flaw in Apex One and Worry-Free Business Security solutions for Windows that has been actively exploited in real-world attacks.

Tracked as CVE-2023-41179 (CVSS score: 9.1), it relates to a third-party antivirus uninstaller module that's bundled along with the software.

As a workaround, it's recommending that customers limit access to the product's administration console to trusted networks.

Source:https://thehackernews.com/2023/09/trend-micro-releases-urgent-fix-for.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.