CCDS CYBER SECURITY PICKS

36th Release March 2022

Google Issues Urgent Chrome Update to Patch Actively Exploited Zero-Day Vulnerability

Google on Friday shipped an out-of-band security update to address a high severity vulnerability in its Chrome browser that it said is being actively exploited in the wild.

Tracked as CVE-2022-1096, the zero-day flaw relates to a type confusion vulnerability in the V8 JavaScript engine. An anonymous researcher has been credited with reporting the bug on March 23, 2022.

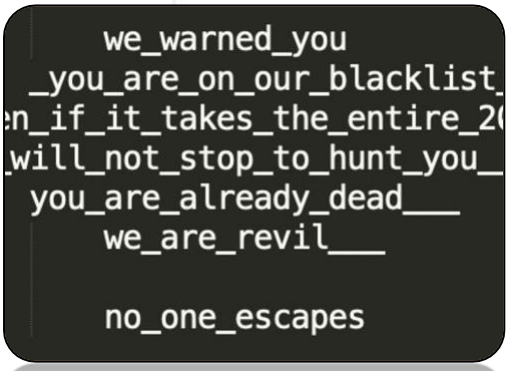
Source:
https://thehackernews.com/2022/03/google-issues-urgent-chrome-update-to.html

CISA Adds Another 95 Flaws to its Actively Exploited Vulnerabilities Catalog

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) this week added 95 more security flaws to its Known Exploited Vulnerabilities Catalog, taking the total number of actively exploited vulnerabilities to 478.

"These types of vulnerabilities are a frequent attack vector for malicious cyber actors and pose significant risk to the federal enterprise," the agency said in an advisory published on March 3, 2022

Source:
https://thehackernews.com/2022/03/cisa-adds-another-95-flaws-to-its.html

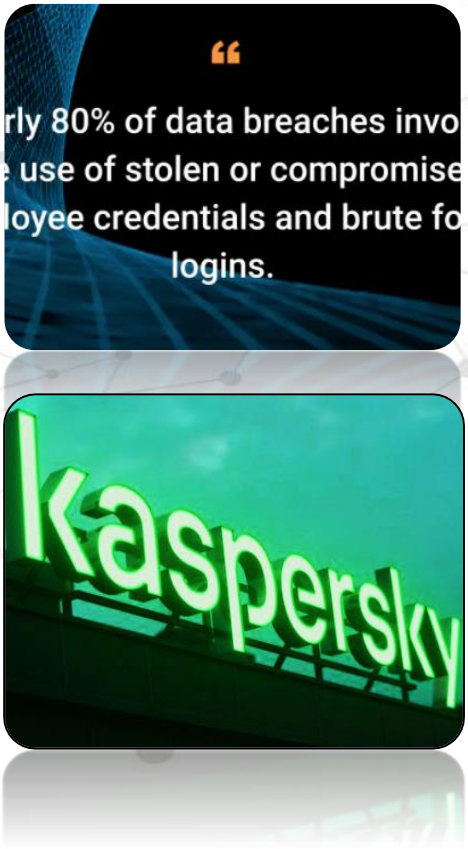


Imperva Thwarts 2.5 Million RPS Ransom DDoS Extortion Attacks

Cybersecurity company Imperva on Friday said it recently mitigated a ransom distributed denial-of-service (DDoS) attack targeting an unnamed website that peaked at 2.5 million requests per second (RPS).

"While ransom DDoS attacks are not new, they appear to be evolving and becoming more interesting with time and with each new phase," Nelli Klepfish, security analyst at Imperva, said. "For example, we've seen instances where the ransom note is included in the attack itself embedded into a URL request."

Source:
https://thehackernews.com/2022/03/imperva-thwarts-25-million-rps-ransom.html



What's Driving Multi-Factor Authentication Adoption?

It's been almost a year since Akamai launched its innovative multi-factor authentication (MFA) service: Akamai MFA. Since we introduced the service, we have talked to numerous customers about what's driving them to either deploy MFA for the first time or to enhance their existing MFA solution. Of course, the primary reason for deploying MFA is usually to improve the security of workforce logins, but it's been fascinating to find out what other factors are driving adoption beyond that.

Source: https://www.akamai.com/blog/security/mfa-adoption

FCC Adds Kaspersky and Chinese Telecom Firms to National Security Threat List

The U.S. Federal Communications Commission (FCC) on Friday moved to add Russian cybersecurity company Kaspersky Lab to the "Covered List" of companies that pose an "unacceptable risk to the national security" of the country.

The development marks the first time a Russian entity has been added to the list that's been otherwise dominated by Chinese telecommunications firms.

Source: https://thehackernews.com/2022/03/fcc-adds-kaspersky-and-chinese-telecom.html

Experts Uncover Campaign Stealing Cryptocurrency from Android and iPhone Users

Researchers have blown the lid off a sophisticated malicious scheme primarily targeting Chinese users via copycat apps on Android and iOS that mimic legitimate digital wallet services to siphon cryptocurrency funds.

"These malicious apps were able to steal victims' secret seed phrases by impersonating Coinbase, imToken, MetaMask, Trust Wallet, Bitpie, TokenPocket, or OneKey," said Lukáš Štefanko, senior malware researcher at ESET in a report shared with The Hacker News.

ESET, which has been tracking the campaign since May 2021, attributed it to the work of a single criminal group.

Source: https://thehackernews.com/2022/03/experts-uncover-campaign-stealing.html

New Variant of Chinese Gimmick Malware Targeting macOS Users

Researchers have disclosed details of a newly discovered macOS variant of a malware implant developed by a Chinese espionage threat actor known to strike attack organizations across Asia.

Attributing the attacks to a group tracked as Storm Cloud, cybersecurity firm Volexity characterized the new malware, dubbed Gimmick, as a "feature-rich, multi-platform malware family that uses public cloud hosting services (such as Google Drive) for command-and-control (C2) channels."

Source: https://thehackernews.com/2022/03/new-variant-of-chinese-gimmick-malware.html

Cloud Consultancy

Contact Us

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.