Cloud Consultancy
DIGITALIZATION & SECURITY

CCDS CYBER SECURITY PICKS

52nd Release - July 2023

Threat actors abuse Google AMP for evasive phishing attacks

Security researchers are warning of increased phishing activity that abuses Google Accelerated Mobile Pages (AMP) to bypass email security measures and get to inboxes of enterprise employees.

Google AMP is an open-source HTML framework co-developed by Google and 30 partners to make web content load faster on mobile devices.

The idea behind using Google AMP URLs embedded in phishing emails is to make sure that email protection technology does not flag messages as malicious or suspicious due to Google's good reputation.

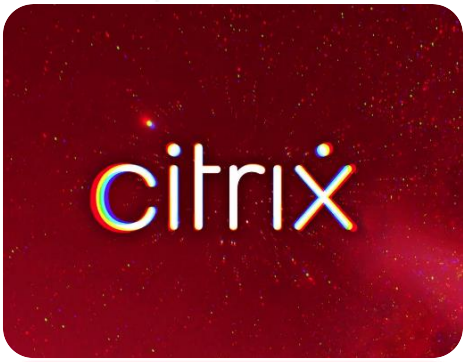
Source:https://www.bleepingcomputer.com/news/security/threat-actors-abuse-google-amp-for-evasive-phishing-attacks/

Russian hackers target govt orgs in Microsoft Teams phishing attacks

Microsoft says a hacking group tracked as APT29 and linked to Russia's Foreign Intelligence Service (SVR) targeted dozens of organizations worldwide, including government agencies, in Microsoft Teams phishing attacks.

The threat actors utilized compromised Microsoft 365 tenants to create new technical support-themed domains and send tech support lures, attempting to trick users of the targeted organizations using social engineering tactics.

Source:https://www.bleepingcomputer.com/news/security/russian-hackers-target-govt-orgs-in-microsoft-teams-phishing-attacks/



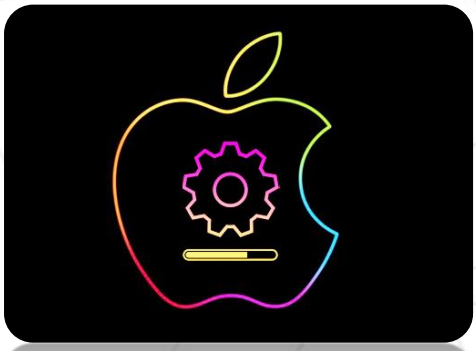
Over 640 Citrix servers backdoored with web shells in ongoing attacks

Hundreds of Citrix Netscaler ADC and Gateway servers have already been breached and backdoored in a series of attacks targeting a critical remote code execution (RCE) vulnerability tracked as CVE-2023-3519.

Security researchers from the Shadowserver Foundation, a non-profit organization dedicated to enhancing internet security, now disclosed that attackers had deployed web shells on at least 640 Citrix servers in these attacks.

Source:https://www.bleepingcomputer.com/news/security/over-640-citrix-servers-backdoored-with-web-shells-in-ongoing-attacks/

BY Muhammed Rafeek (CYBER SECURITY ANALYST – SOC TEAM)

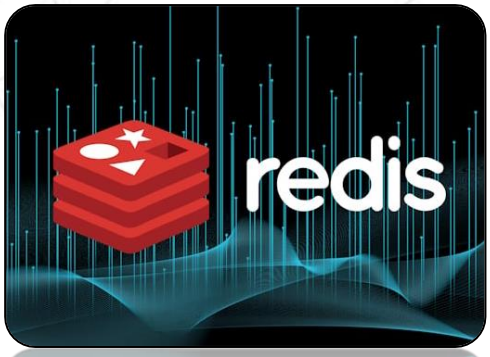


Apple Rolls Out Urgent Patches for Zero-Day Flaws Impacting iPhones, iPads and Macs

Apple has rolled out security updates to iOS, iPadOS, macOS, tvOS, watchOS, and Safari to address several security vulnerabilities, including one actively exploited zero-day bug in the wild.

Tracked as CVE-2023-38606, the shortcoming resides in the kernel and permits a malicious app to modify sensitive kernel state potentially. The company said it was addressed with improved state management.

Source:https://thehackernews.com/2023/07/apple-rolls-out-urgent-patches-for-zero.html



New P2PInfect Worm Targeting Redis Servers on Linux and Windows Systems

Cybersecurity researchers have uncovered a new cloud targeting, peer-to-peer (P2P) worm called P2PInfect that targets vulnerable Redis instances for follow-on exploitation.

"The P2PInfect worm appears to be well designed with several modern development choices," the researchers said. "The design and building of a P2P network to perform the auto-propagation of malware is not something commonly seen within the cloud targeting or cryptojacking threat landscape."

Source:https://thehackernews.com/2023/07/new-p2pinfect-worm-targeting-redis.html

Fake PoC for Linux Kernel Vulnerability on GitHub Exposes Researchers to Malware

In a sign that cybersecurity researchers continue to be under the radar of malicious actors, a proof-of-concept (PoC) has been discovered on GitHub, concealing a backdoor with a "crafty" persistence method.

The repository masquerades as a PoC for CVE-2023-35829, a recently disclosed high-severity flaw in the Linux kernel. It has since been taken down, but not before it was forked 25 times. Another PoC shared by the same account, ChriSanders22, for CVE-2023-20871, a privilege escalation bug impacting VMware Fusion, was forked twice.

The backdoor comes with a broad range of capabilities to steal sensitive data from compromised hosts as well as allow a threat actor to gain remote access by adding their SSH key to the .ssh/authorized_keys file.

Source: https://thehackernews.com/2023/07/blog-post.html

MITRE Unveils Top 25 Most Dangerous Software Weaknesses of 2023: Are You at Risk?

MITRE has released its annual list of the Top 25 "most dangerous software weaknesses" for the year 2023.

"These weaknesses lead to serious vulnerabilities in software," the U.S. Cybersecurity and Infrastructure Security Agency (CISA) said. "An attacker can often exploit these vulnerabilities to take control of an affected system, steal data, or prevent applications from working."

The development also follows new findings from Censys that nearly 250 devices running on various U.S. government networks have exposed remote management interfaces on the open web, many of which run remote protocols such as SSH and TELNET.

Source:https://thehackernews.com/2023/06/mitre-unveils-top-25-most-dangerous.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.