CCDS CYBER SECURITY PICKS

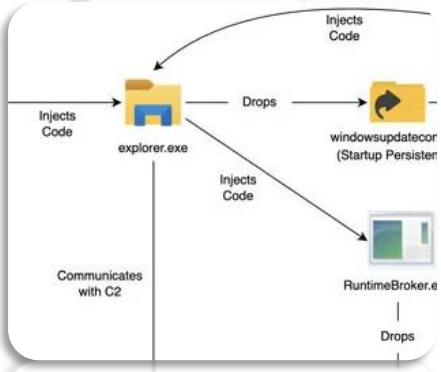
34th Release January 2022

Apple Releases iOS and macOS Updates to Patch Actively Exploited 0-Day Vulnerability

Apple on Wednesday released iOS 15.3 and macOS Monterey 12.2 with a fix for the privacy-defeating bug in Safari, as well as to contain a zero-day flaw, which it said has been exploited in the wild to break into its devices.

Tracked as CVE-2022-22587, the vulnerability relates to a memory corruption issue in the IOMobileFrameBuffer component that could be abused by a malicious application to execute arbitrary code with kernel privileges.

Source:
https://thehackernews.com/2022/01/apple-releases-ios-and-ipados-updates.html



North Korean Hackers Using Windows Update Service to Infect PCs with Malware

The notorious Lazarus Group actor has been observed mounting a new campaign that makes use of the Windows Update service to execute its malicious payload, expanding the arsenal of living-off-the-land (LotL) techniques leveraged by the APT group to further its objectives.

The Lazarus Group, also known as APT38, Hidden Cobra, Whois Hacking Team, and Zinc, is the moniker assigned to the North Korea-based nation-state hacking group that's been active since at least 2009.

Source:
https://thehackernews.com/2022/01/north-korean-hackers-using-windows.html

Google Details Two Zero-Day Bugs Reported in Zoom Clients and MMR Servers

An exploration of zero-click attack surface for the popular video conferencing solution Zoom has yielded two previously undisclosed security vulnerabilities that could have been exploited to crash the service, execute malicious code, and even leak arbitrary areas of its memory.

Natalie Silvanovich of Google Project Zero, who discovered and reported the two flaws last year, said the issues impacted both Zoom clients and Multimedia Router (MMR) servers.

Source:
https://thehackernews.com/2022/01/google-details-two-zero-day-bugs.html

Hackers Exploited MSHTML Flaw to Spy on Government and Defense Targets

Cybersecurity researchers on Tuesday took the wraps off a multi-stage espionage campaign targeting high-ranking government officials overseeing national security policy and individuals in the defense industry in Western Asia.

The attack is unique as it leverages Microsoft OneDrive as a command-and-control (C2) server and is split into as many as six stages to stay as hidden as possible

Source: https://thehackernews.com/2022/01/hackers-exploited-mshtml-flaw-to-spy-on.html

Hackers Using Device Registration Trick to Attack Enterprises with Lateral Phishing

Microsoft has disclosed details of a large-scale, multi-phase phishing campaign that uses stolen credentials to register devices on a victim's network to further propagate spam emails and widen the infection pool.

The tech giant said the attacks manifested through accounts that were not secured using multi-factor authentication (MFA)

Source: https://thehackernews.com/2022/01/hackers-using-device-registration-trick.html

Initial Access Broker Involved in Log4Shell Attacks Against VMware Horizon Servers

An initial access broker group tracked as Prophet Spider has been linked to a set of malicious activities that exploits the Log4Shell vulnerability in unpatched VMware Horizon Servers.

According to new research published by BlackBerry Research & Intelligence and Incident Response (IR) teams today, the cybercrime actor has been opportunistically weaponizing the shortcoming to download a second-stage payload onto the victimized systems.

"It's likely that we will continue to see criminal groups exploring the opportunities of the Log4Shell vulnerability, so it's an attack vector against which defenders need to exercise constant vigilance," -Tony Lee, vice president, Blackberry.

Source: https://thehackernews.com/2022/01/initial-access-broker-involved-in.html

12-Year-Old Polkit Flaw Lets Unprivileged Linux Users Gain Root Access

A 12-year-old security vulnerability has been disclosed in a system utility called Polkit that grants attackers root privileges on Linux systems, even as a proof-of-concept (PoC) exploit has emerged in the wild merely hours after technical details of the bug became public.

Dubbed "PwnKit" by cybersecurity firm Qualys, the weakness impacts a component in polkit called pkexec, a program that's installed by default on every major Linux distribution such as Ubunti, Debian, Fedora, and CentOS.

Source: https://thehackernews.com/2022/01/12-year-old-polkit-flaw-lets.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.