Cloud Consultancy
DIGITALIZATION & SECURITY

CCDS CYBER SECURITY PICKS

42nd Release September 2022

Cyber Attacks Against Middle East Governments Hide Malware in Windows logo

An espionage-focused threat actor has been observed using a steganographic trick to conceal a previously undocumented backdoor in a Windows logo in its attacks against Middle Eastern governments.

Broadcom's Symantec Threat Hunter Team attributed the updated tooling to a hacking group it tracks under the name Witchetty, which is also known as LookingFrog, a subgroup operating under the TA410 umbrella.

Source:https://thehackernews.com/2022/09/cyber-attacks-against-middle-east.html

New Malware Families Found Targeting VMware ESXi Hypervisors

Threat actors have been found deploying never-before-seen post-compromise implants in VMware's virtualization software to seize control of infected systems and evade detection.

Google's Mandiant threat intelligence division referred to it as a "novel malware ecosystem" that impacts VMware ESXi, Linux vCenter servers, and Windows virtual machines, allowing attackers to maintain persistent access to the hypervisor as well as execute arbitrary commands.

Source:https://thehackernews.com/2022/09/new-malware-families-found-targeting.html

Zoom Users Beware: New Malware Spreading Disguised as Legitimate Zoom Application

When Cyble Research and Intelligence Labs (CRIL) was carrying out routine threat hunting exercises, it came across a tweet that mentioned numerous fake Zoom sites being created, which caught the attention of the researchers.

There is a lot of similarity in the user interfaces of these sites. The purpose of these sites is to infect people with malware disguised as Zoom's legitimate application, using this site as a vehicle for spreading malware.

Source:https://cybersecuritynews-com.cdn.ampproject.org/c/s/cybersecuritynews.com/zoom-users-beware/?amp

Microsoft Confirms 2 New Exchange Zero-Day Flaws Being Used in the Wild

Microsoft officially disclosed it investigating two zero-day security vulnerabilities impacting Exchange Server 2013, 2016, and 2019 following reports of in-the-wild exploitation.

"The first vulnerability, identified as CVE-2022-41040, is a Server-Side Request Forgery (SSRF) vulnerability, while the second, identified as CVE-2022-41082, allows remote code execution (RCE) when PowerShell is accessible to the attacker," the tech giant said.

Source:https://thehackernews.com/2022/09/microsoft-confirms-2-new-exchange-zero.html

Hackers Using PowerPoint Mouseover Trick to Infect System with Malware

The Russian state-sponsored threat actor known as APT28 has been found leveraging a new code execution method that makes use of mouse movement in decoy Microsoft PowerPoint documents to deploy malware.
The technique "is designed to be triggered when the user starts the presentation mode and moves the mouse," cybersecurity firm Cluster25 said in a technical report. "The code execution runs a PowerShell script that downloads and executes a dropper from OneDrive."
Source:https://thehackernews.com/2022/09/hackers-using-powerpoint-mouseover.html

Why Organisations Need Both EDR and NDR for Complete Network Protection

As organizations become increasingly complex and add more end-user devices to their networks, they require a reliable monitoring solution to protect their endpoints from potential threats. However, Endpoint Detection and Response (EDR) provides such endpoint protection only to a certain extent.

There are numerous drawbacks of EDR that allow sophisticated cybercriminals to surpass their security perimeter and exploit network vulnerabilities.

To fill the security gaps left by EDR solutions, organisations must reinforce their security defences. Network Detection and Response (NDR) solutions like ExeonTrace are a reliable and proven way to monitor network traffic and thus complete enterprise cybersecurity stacks. As EDR and NDR solutions are complementary, their combined detection capabilities can effectively protect organisations from sophisticated cyberattacks.

Source: https://thehackernews.com/2022/09/why-organisations-need-both-edr-and-ndr.html

5 Network Security Threats And How To Protect Yourself

Traditionally, endpoints would all live on one "corporate network," - networks today are often just made up of the devices themselves, and how they're connected: across the internet, sometimes via VPNs, to the homes and cafes people work from, to the cloud and data centres where services live. So what threats does this modern network face?

#1 Misconfiguration

#2 Outdated software

#3 DoS attack

#4 Application bugs

#5 Attack surface management

Source:https://thehackernews.com/2022/09/5-network-security-threats-and-how-to.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