Cloud Consultancy
DIGITALIZATION & SECURITY

JUNE 2022

39TH RELEASE

+966112388882 (24/7 Operation Support Center) info@ccds.ws www.ccds.ws

Cloud Consultancy
For Digitalization & Security

CCDS CYBER SECURITY PICKS

39th Release June 2022

Google warns of 'hermit spyware' infecting Android and iOS devices

Google’s Threat Analysis Group (TAG) released a report on spyware campaigns targeting Android and iOS users.

Google TAG researchers Benoit Sevens and Clement Lecigne go into detail about the use of entrepreneurial grade spyware dubbed "Hermit." This sophisticated spyware tool allows attackers to steal data, private messages and make phone calls.

Source: https://www.msn.com/en-us/money/other/google-warns-of-hermit-spyware-infecting-android-and-ios-devices/ar-AAYRV3I?ocid=msedgntp&cvid=2f7ff15e71434407bf27441bbd3170df

Log4Shell Still Being Exploited to Hack VMWare Servers to Exfiltrate Sensitive Data

The U.S. Cybersecurity and Infrastructure Security Agency (CISA), along with the Coast Guard Cyber Command (CGCYBER), on Thursday released a joint advisory warning of continued attempts on the part of threat actors to exploit the Log4Shell flaw in VMware Horizon servers to breach target networks

In one instance, the adversary is said to have been able to move laterally inside the victim network, obtain access to a disaster recovery network, and collect and exfiltrate sensitive law enforcement data.

Source:
https://thehackernews.com/2022/06/log4shell-still-being-exploited-to-hack.html

New NTLM Relay Attack Lets Attackers Take Control Over Windows Domain

A new kind of Windows NTLM relay attack dubbed DFSCoerce has been uncovered that leverages the Distributed File System (DFS) Namespace Management Protocol (MS-DFSNM) to seize control of a domain.

The NTLM relay attack allows malicious parties to sit between clients and servers and intercept and relay validated authentication requests in order to gain unauthorized access to network resources, effectively gaining an initial foothold in Active Directory environments.
Source:
https://thehackernews.com/2022/06/new-ntlm-relay-attack-lets-attackers.htmlss

BY TOUSEEF UR REHMAN (CYBER SECURITY ANALYST – SOC TEAM)

HelloXD Ransomware Installing Backdoor on Targeted Windows and Linux Systems

Windows and Linux systems are being targeted by a ransomware variant called HelloXD.

Unlike other ransomware groups, this ransomware family doesn't have an active leak site instead it prefers to direct the impacted victim to negotiations through Tox chat and onion-based messenger instances.

Source: https://thehackernews.com/2022/06/hello-xd-ransomware-installing-backdoor.html

A New Golang-based Peer-To-Peer Botnet Targeting Linux Servers

A new Golang-based peer-to-peer (P2P) botnet has been spotted actively targeting Linux servers in the education sector.

Dubbed Panchan by Akamai Security Research, the malware "utilizes its built-in concurrency features to maximize spread ssability and execute malware modules" and "harvests SSH keys to perform lateral movement."

Source: https://thehackernews.com/2022/06/panchan-new-golang-based-peer-to-peer.html

Avoiding Social Engineering Attacks

In a social engineering attack, an attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems.
An attacker may seem unassuming and respectable, possibly claiming to be a new employee, repair person, or researcher and even offering credentials to support that identity. However, by asking questions, he or she may be able to piece together enough information to infiltrate an organization's network.

How to protect against Social Engineering Attacks

1-Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.
2- Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.

Source: https://www.cisa.gov/uscert/ncas/tips/ST04-014

Avoiding Phishing Attacks

Phishing is a form of social engineering. Phishing attacks use email or malicious websites to solicit personal information by posing as a trustworthy organization. Phishing attacks may appear to come from different types of organizations, such as charities. Attackers often take advantage of current events and certain times of the year.

How to protect against Phishing Attacks
1-Do not reveal personal or financial information in email, and do not respond to email solicitations for this information.
2-Don't send sensitive information over the internet before checking a website's security.
3-Install and maintain anti-virus software, firewalls, and email filters to reduce some of this traffic.

Source: https://www.cisa.gov/uscert/ncas/tips/ST04-014

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