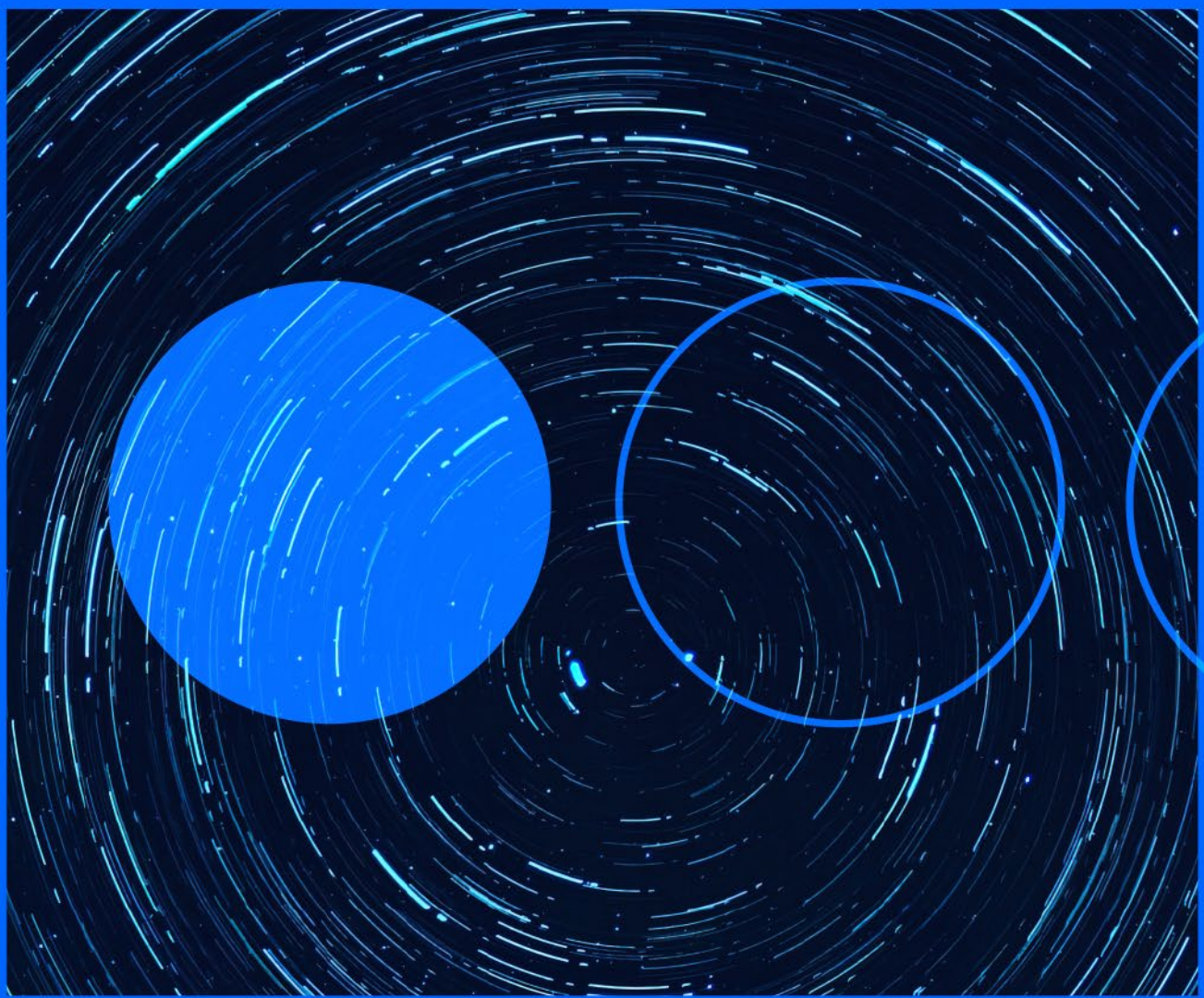
Telefónica Tech

28.10.2022

Cyber threats weekly briefing 2022



telefonicatech.com

Summary of the main attacks and vulnerabilities found by our experts in the last 7 days.

The icons stand for the following concepts.

				
Cyberoperations	Incidents	Malware	Information Leaks	Vulnerabilities

Campaigns spreading ERMAC malware

INTERNATIONAL

A team of Cyble researchers recently discovered a mass phishing campaign aimed at spreading the ERMAC banking trojan. The infection method is based on downloading fake apps that impersonate Google Wallet, PayPal, Snapchat and others. These fake apps are downloaded from fake domains with websites that impersonate some of the most popular Android markets. These impersonations also include fake domains based on the companies allegedly distributing the apps. Once these fake apps are executed, the ERMAC malware proceeds to steal data such as contact and SMS information, as well as a list of apps in use by the device. Phishing pages are displayed on the victim's screen via that latter function, which in turn sends the collected data to the malware's Command & Control via POST requests.

URL: https://blog.cyble.com/2022/10/18/ermac-android-malware-increasingly-active/

Apple fixes 0-day vulnerability for iOS and iPadOS in latest patch

INTERNATIONAL

The latest update released by Apple fixes, among others, a 0-day vulnerability that could have been actively exploited against iPhone and iPad devices. This vulnerability, identified as CVE-2022-42827 and still pending CVSS qualification by Apple, would allow an attacker to execute arbitrary code in the Kernel with the highest privileges. This could lead to data corruption, performance disruption or unauthorised code execution on the device. The update that fixes this vulnerability would be available for iPhone8 models onwards, all iPadPro models, iPad Air third generation and above, and iPad and iPad Mini fifth generation and above URL: https://research.checkpoint.com/2022/bumblebee-increasing-its-capacity-and-evolving-its-ttps/

VMware fixes critical vulnerability in Cloud Foundation

INTERNATIONAL

VMware has issued an advisory on two vulnerabilities affecting its Cloud Foundation hybrid platform, including a critical one. The first, identified as CVE-2021-39144 with a CVSS score of 8.5 (9.8 according to VMware), is a remote code execution vulnerability through the Xstream library. The second, identified as CVE-2022-31678 with a CVSS score of 5.3 assigned by VMware, could allow an attacker to cause a denial of service or expose information. Both vulnerabilities would affect VMware Cloud Foundation (NSX-V) version 3.11 and would be fixed with the latest update.

URL: https://www.vmware.com/security/advisories/VMSA-2022-0027.html

Critical vulnerability in OpenSSL announced

INTERNATIONAL

The OpenSSL Project team has announced that it will release a new version of OpenSSL, version 3.0.7 on November 1st, which will include a security patch that has been classified as critical. While no details have been released of the serious vulnerability that will be fixed in this release beyond the fact that it does not affect versions prior to 3.0, its mere existence has caused concern as it is the first critical vulnerability to be announced by OpenSSL since 2016. Although the developers have announced the deployment of the new version and the bug in advance so that users have time to take inventories and prepare their systems, OpenSSL does not believe that this will be enough for attackers to discover the vulnerability, as Mark J. Cox, a member of the team, has stated.

URL: https://mta.openssl.org/pipermail/openssl-announce/2022-October/000238.html

Zoom vulnerability could expose users to phishing attacks

INTERNATIONAL

Zoom has issued a security bulletin fixing a vulnerability susceptible to URL scanning. Listed as CVE-2022-28763 with a CVSS of 8.8, the flaw could be exploited by a malicious actor using a specially crafted Zoom meeting URL to redirect a user to an arbitrary network address, enabling additional types of attacks, including taking control of the active session. The products affected by this vulnerability include Zoom Client for Meetings (for Android, iOS, Linux, macOS, and Windows), Zoom VDI Windows Meeting Clients, and Zoom Rooms for Conference Room (for Android, iOS, Linux, macOS, and Windows), all in versions prior to version 5.12.2. Zoom recommends updating or downloading the latest software.

URL: https://explore.zoom.us/en/trust/security/security-bulletin/

Drinik: Android banking trojan re-emerges with advanced capabilities

INTERNATIONAL

Analysts at Cyble have detected a new version of the Drinik banking malware, targeting Android systems, and currently targeting 18 banking institutions in India. According to Cyble's report, the trojan poses as the country's official tax administration app (iAssist) to steal victims' personal information and banking credentials. Once installed on the victim's device, the application requests permissions to write to external storage, receive, read and send SMS, and read the call log. It will also request permission to make use of Android's accessibility service, which will disable Google Play Protect and enable the malware to perform navigation gestures, record the screen and capture keystrokes and user credentials, displaying the legitimate Indian income tax site in the app. As an end goal, Drinik redirects victims to an Income Tax Department phishing website where, under the guise of a refund in their favour, it will ask the user for their financial information, including account number, credit card number, CVV and PIN. Drinik has been known since 2016 and has been evolving continuously improving its capabilities and targeting mass audiences, such as Indian taxpayers and bank customers in this case.

URL: https://blog.cyble.com/2022/10/27/drinik-malware-returns-with-advanced-capabilities-targeting-indian-taxpayers/

About Telefónica Tech

Telefónica Tech is the leading company in digital transformation. The company has a wide range of services and integrated technological solutions for Cybersecurity, Cloud, IoT, Big Data, or Blockchain.

More information

telefonicatech.com