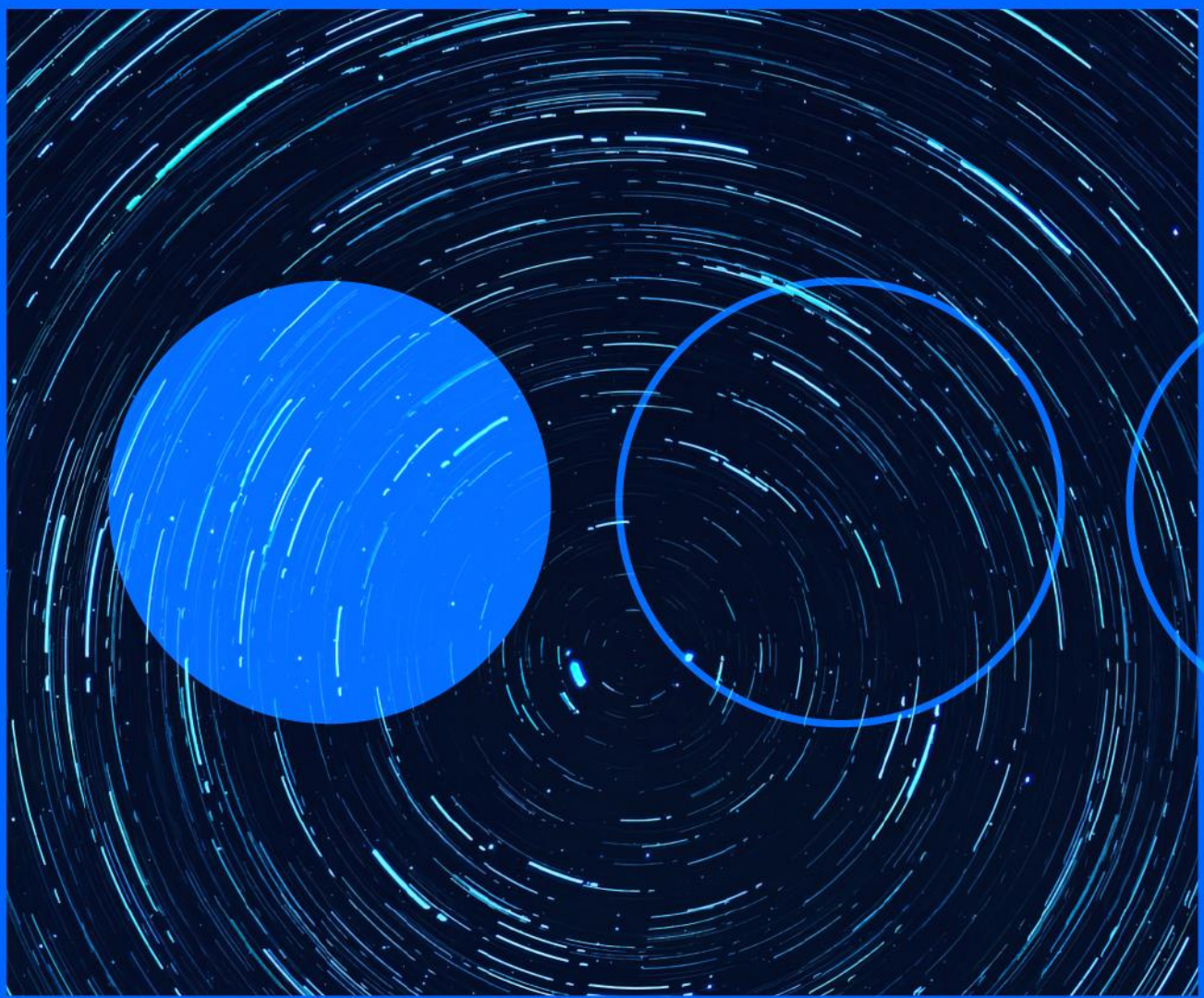
Telefónica Tech

31.03.2023

Cyber threats weekly briefing 2023



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

GitHub exposes its RSA SSH host key by mistake

INTERNATIONAL

GitHub announced last Friday that they had replaced their RSA SSH host key used to protect Git operations. According to the company, this key was accidentally exposed in a public GitHub repository last week. They acted quickly to contain the exposure and an investigation was launched to discover the cause and impact. While this key does not give access to GitHub infrastructure or user data, this action has been taken to prevent potential spoofing. Users are advised to remove the key and replace it with the new one.

URL: https://github.blog/2023-03-23-we-updated-our-rsa-ssh-host-key/

Apple fixes an actively exploited 0-day

INTERNATIONAL

Apple has released security updates fixing an actively exploited 0-day vulnerability in older iPhone, macOS and iPad devices. The flaw, identified as CVE-2023-23529, is a WebKit-type confusion bug, which has a CVSS of 8.8 and could lead to arbitrary code execution, data theft, access to Bluetooth data, etc. It should be noted that, in terms of devices, the vulnerability affects iPhone 6s, iPhone 7, iPhone SE, iPad Air 2, iPad mini and iPod touch, in addition to Safari 16.3 on macOS Big Sur and Monterey, macOs Ventura, tvOS and watchOS. The company recommends updating as soon as possible to avoid possible exploit attempts.

URL: https://www.bleepingcomputer.com/news/apple/apple-fixes-recently-disclosed-webkit-zero-day-on-older-iphones/

Malicious campaign impersonating the Spanish Government and banks

INTERNATIONAL

The Oficina de Seguridad del Internauta (OSI) has issued a security warning informing about a malicious smishing campaign impersonating government agencies and banking institutions. Malicious actors are particularly employing social engineering techniques by sending smishing campaigns in which they try to trick the victim into believing that they have a refund due to the tax campaign. If the victim accesses the malicious link, they will be redirected to a website that simulates the website of La Moncloa, where they are asked to indicate which bank they belong to. Once selected, the victim will again be redirected to a phishing campaign that impersonates the name and logo of the selected bank. The aim of the malicious actors behind this campaign is to exfiltrate the banking credentials of their victims.

URL: https://www.osi.es/es/actualidad/avisos/2023/03/campana-de-smishing-que-suplanta-la-moncloa-y-entidades-bancarias-para

Supply chain attack via 3XC video conferencing platform

INTERNATIONAL

Researchers from various security firms such as SentinelOne, Sophos y CrowdStrike have warned of a supply chain attack via the 3CX video conferencing programme. While the investigation into the attack is still ongoing, it has been confirmed to affect Windows platforms where the compromised 3CXDesktopApp application would download ICO files from GitHub, ultimately leading to the installation of a stealer malware. The first detections of the app's suspicious behaviour in security solutions were reportedly in mid-March 2023, but researchers have identified infrastructure used in the attack with registration dates in February last year. The campaign, which SentinelOne has dubbed SmoothOperator, has no clear attribution, although some researchers point to possible connections to Labyrinth Chollima, part of the North Korean Lazarus Group. 3CX has not made any statement regarding the campaign.

URL: https://www.sentinelone.com/blog/smoothoperator-ongoing-campaign-trojanizes-3cx-software-in-software-supply-chain-attack/

Analysis of campaigns exploiting 0-days on Android, iOS and Chrome

INTERNATIONAL

Google's Threat Analysis Group has published a report sharing details about two campaigns that used 0-day exploits against Android, iOS and Chrome. In the first campaign, 0-day exploit strings targeting Android and iOS were detected and distributed via shortened links sent via SMS to users located in Italy, Malaysia and Kazakhstan. The vulnerability, already fixed in 2022, which affected iOS in versions prior to 15.1, is identified as CVE-2022-42856 and CVSS 8.8, which refers to a type confusion bug in the JIT compiler that can lead to arbitrary code execution. On the other hand, the one identified as CVE-2021-30900, with CVSS 7.8, also fixed, deals with an out-of-bounds writing and privilege escalation bug. As for the Android exploit chain, these targeted users of phones with an ARM GPU running versions earlier than 106. As for the bugs, all fixed, one of them is CVE-2022-3723 (CVSS 8.8), type confusion in Chrome; CVE-2022-4135 (CVSS 9.6), buffer overflow in Chrome's GPU; and CVE-2022-38181 (CVSS 8.8), privilege escalation. It is worth noting that the latter vulnerability was found to be actively exploited. The second campaign, targeting devices in the United Arab Emirates via SMS, consists of several 0-days and n-days targeting Samsung's web browser. The link redirects users to a page developed by spyware vendor Variston and exploits vulnerabilities CVE-2022-4262, CVE-2022-3038, CVE-2022-22706 and CVE-2023-0266.

URL: https://blog.google/threat-analysis-group/spyware-vendors-use-0-days-and-n-days-against-popular-platforms/

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