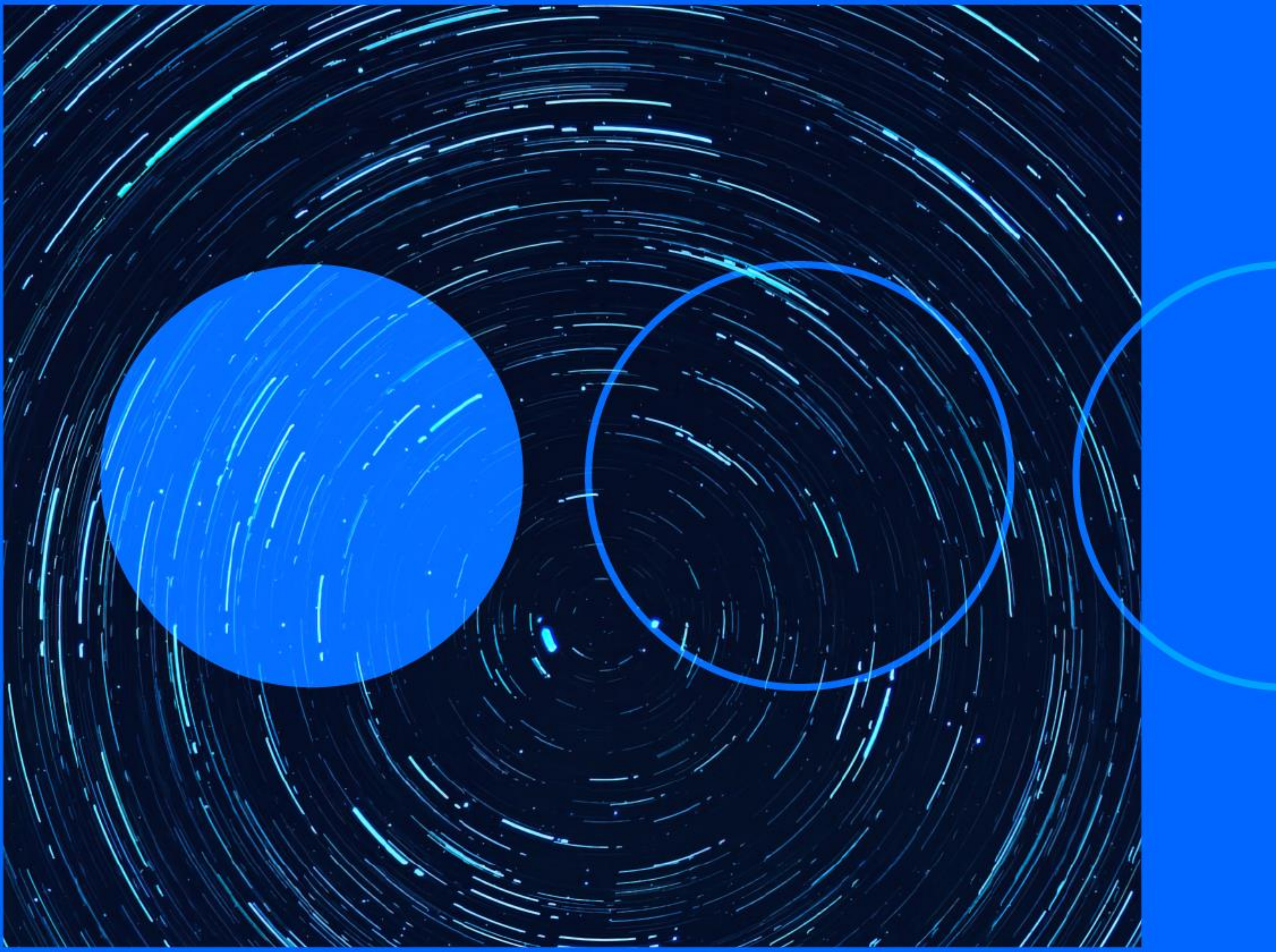
Telefónica Tech

17.03.2023

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

A new version of the Xenomorph banking trojan

INTERNATIONAL

ThreatFabric researchers have detected a new variant of the Android banking trojan Xenomorph. This malware family was first detected in February 2022 and is attributed to Hadoken Security Group. Xenomorph V3 or Xenomorph.C, which is how this new variant has been classified, is being distributed via the Zombinder platform, in the Google Play store, appearing as a supposed currency converter, which downloads an update to an application posing as Google Protect. One of the main new features of this version is the introduction of an ATS (Automated Transfer Systems) framework used to automatically extract credentials, account balance, initiate transactions, obtain MFA tokens and finalise fund transfers. It has also added Cookie stealer capabilities. Xenomorph V3 is capable of attacking more than 400 banking and financial institutions, including cryptocurrency wallets, a very significant increase in the volume of victims, as in its first version it only targeted 56 European banks. It should also be noted that Spanish banking institutions are the main targets, followed by Turkey, Poland and the United States. Researchers point out that this is one of the most advanced and dangerous trojans in circulation, and that it could become more so as it is likely to start being distributed as MaaS.

URL: https://www.threatfabric.com/blogs/xenomorph-v3-new-variant-with-ats.html

Microsoft Patch Tuesday includes two actively exploited 0-days

INTERNATIONAL

In its latest security update, Microsoft has fixed a total of 83 vulnerabilities affecting several of its products, including Microsoft Windows, Office, Exchange and Azure. Nine of these vulnerabilities are reported to have received a critical severity score, and another 69 are reported to have been rated as "important". Among them, two of these security bugs are reported to be 0-day actively exploited, CVE-2023-23397, a privilege escalation vulnerability in Outlook with a CVSSv3 score of 9.8 and CVE-2023-24880, a security feature bypass vulnerability in Windows SmartScreen with a CVSSv3 score of 5.4. In relation to vulnerability CVE-

2023-23397, Microsoft has also published a script for this vulnerability. It should be noted that according to the research, this vulnerability has been exploited as a 0-day since at least April 2022, with fifteen organisations known to have been attacked using this vulnerability. The vulnerability was discovered by the Ukrainian Computer Emergency Response Team (CERT-UA), which informed Microsoft. This vulnerability could be exploited by an attacker to send a specially crafted email against an Outlook client, which is automatically triggered when Outlook retrieves and processes it, leading to exploitation before the email is seen in the preview pane, and thus stealing NTLM credentials.

URL: https://msrc.microsoft.com/update-guide/

YoroTrooper: new threat actor focused on cyber espionage

INTERNATIONAL

Researchers at Cisco Talos have detected a new threat actor focused on executing cyberespionage campaigns. YoroTrooper, as the researchers have named it, has been active since at least June 2022, although it was not until February 2023 that it gained popularity. YoroTrooper campaigns have so far been detected targeting government and energy organisations in Commonwealth of Independent States (CIS) countries, as well as the World Intellectual Property Organisation (WIPO) and a European Union healthcare agency. The entry vector for the attacks is via phishing emails with a malicious attachment. YoroTrooper uses several remote access trojans such as AveMaria/Warzone RAT, LodaRAT and a custom Python implant. It also uses stealers such as Stink Stealer, and the Nuitka or PyInstaller frameworks. Telegram is also used as C2 for communications between the operators and the installed malware.

URL: https://blog.talosintelligence.com/yorotrooper-espionage-campaign-cis-turkey-europe/

CISA warns of 0-day exploit in Adobe and urges patch application

INTERNATIONAL

The US Cybersecurity and Infrastructure Security Agency (CISA) has warned of 0-day exploitation of vulnerability CVE-2023-26360 in Adobe ColdFusion and has given all government agencies a three-week deadline to apply the patch released Wednesday by Adobe. Although Adobe's Patch Tuesday stated that the vulnerability had been exploited in a very limited way, CISA raised the alert level by calling the need for patching urgent and mandatory, confirming the words of Charlie Arehart, who discovered the vulnerability and criticised Adobe for the lack of importance given to the vulnerability, which allows the execution of arbitrary code.

URL: https://www.cisa.gov/news-events/alerts/2023/03/15/cisa-adds-one-known-exploited-vulnerability-catalog

0-day vulnerabilities in Samsung's Exynos chipsets

INTERNATIONAL

Google's security team, Project Zero, disclosed in a publication the existence of 18 0-day vulnerabilities in Samsung's Exynos chipsets, used in mobile devices, laptops and cars. Four of these flaws are the most serious; this would be the case of the vulnerability identified as CVE-2023-24033 and three others that have not yet been assigned a CVE, whose exploitation would allow remote code execution from the Internet to the baseband and for which the attacker would not need the interaction of the victim, only their phone number. On the other hand, the rest of the vulnerabilities, some of them identified as CVE-2023-26072, CVE-2023-26073, CVE-2023-26074, CVE-2023-26075, CVE-2023-26076, have not been scored as serious as they require a malicious mobile network operator or the attacker to have local access to the device. As for the affected devices, Samsung has issued a security update indicating which devices are affected. Finally, in terms of patches, Pixel devices have received a fix for one of the vulnerabilities, while other affected users are advised to disable Wi-Fi and Voice-over-LTE calling.

URL: https://googleprojectzero.blogspot.com/2023/03/multiple-internet-to-baseband-remote-rce.html

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

The information disclosed in this document is the property of Telefónica Cybersecurity & Cloud Tech S.L.U. ("Telefónica Tech") and/or any other entity within Telefónica Group and/or its licensors. Telefónica Tech and/or any Telefonica Group entity or Telefónica Tech's licensors reserve all patent, copyright and other proprietary rights to this document, including all design, manufacturing, reproduction, use and sales rights thereto, except to the extent said rights are expressly granted to others. The information in this document is subject to change at any time, without notice.
Neither the whole nor any part of the information contained herein may be copied, distributed, adapted or reproduced in any material form except with the prior written consent of Telefónica Tech.
This document is intended only to assist the reader in the use of the product or service described in the document. In consideration of receipt of this document, the recipient agrees to use such information for its own use and not for other use.
Telefónica Tech shall not be liable for any loss or damage arising out from the use of the any information in this document or any error or omission in such information or any incorrect use of the product or service. The use of the product or service described in this document are regulated in accordance with the terms and conditions accepted by the reader.
Telefónica Tech and its trademarks (or any other trademarks owned by Telefónica Group) are registered service marks.