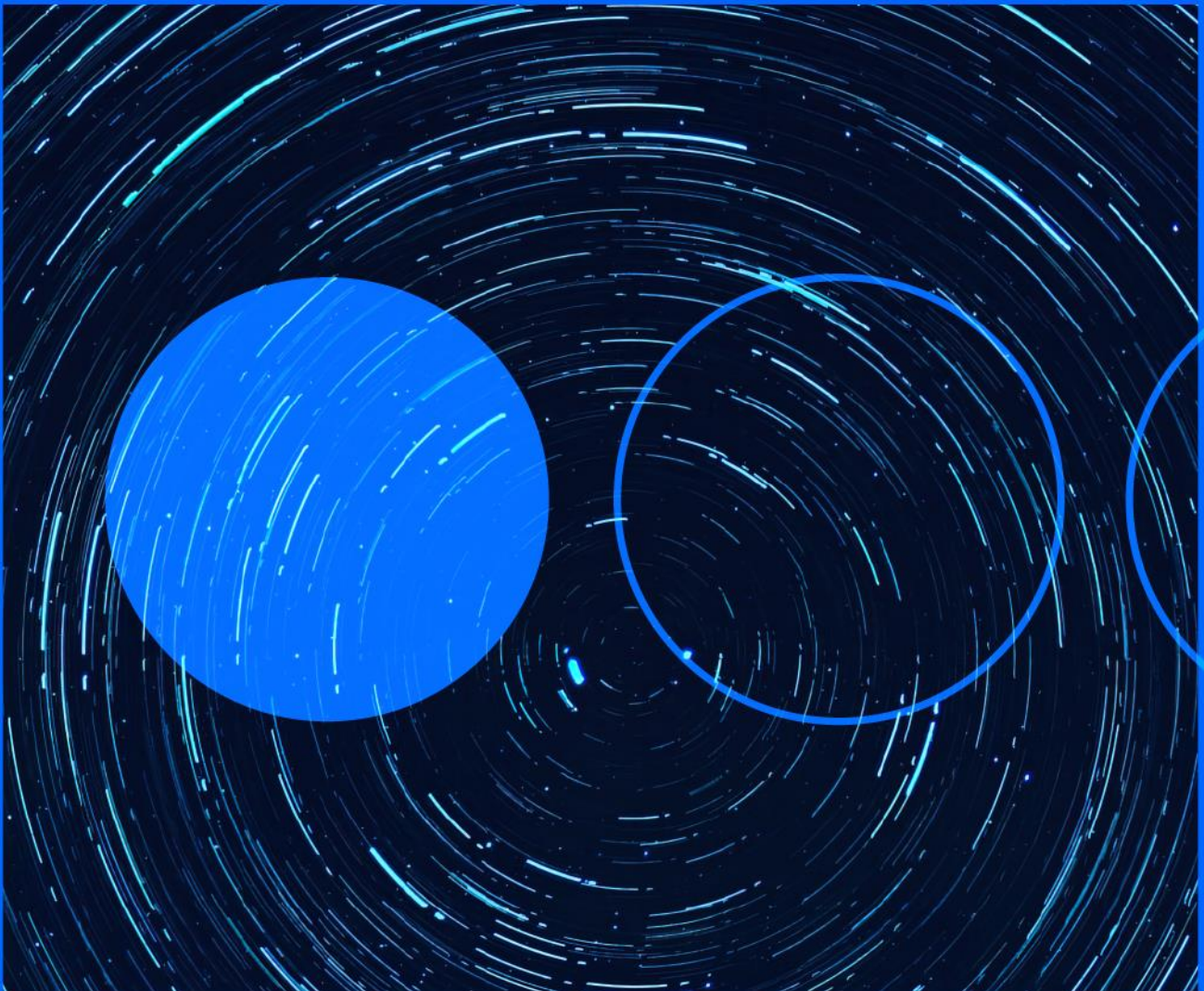







10.02.2023

Cyber threats weekly briefing 2023



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



Campaign against VMware servers to distribute ransomware ESXiArgs

INTERNATIONAL

On Friday 3 February, the French CERT (CERT-FR) published an alert reporting an attack campaign against VMware ESXi servers. The attacks were exploiting the known vulnerability patched in 2021, CVE-2021-21974. After exploitation, the servers were infected by a new ransomware, called ESXiArgs. Over the course of the week, new details of the campaign have been released, with the most affected country being France, followed by the United States and Germany. It is also estimated that more than 2,800 servers have been infected, based on the bitcoin addresses collected, which were published in the ransom notes left by the ransomware. In addition, CISA published a script to recover files encrypted by the ransomware. It should be noted, however, that on Wednesday 8, a new ransomware variant was detected in a new wave of attacks, where the encryption routine was improved, invalidating the CISA script and thus increasing the effectiveness of encryption on infected devices, as well as removing the bitcoin address for payment from the ransom note. In other matters, it should be noted that the incident suffered last Sunday by the Italian telecommunications company Gruppo TIM (Telecom Italia), which left its users without services, had nothing to do with this attack campaign, as it was an international interconnection problem.

URL: <https://www.cert.ssi.gouv.fr/alerte/CERTFR-2023-ALE-015/>



Critical vulnerability in Atlassian Jira

INTERNATIONAL

Atlassian has issued a security advisory in which it releases fixes to resolve a critical vulnerability in Jira Service Management Server and Data Center. According to the vendor, this security flaw has been registered as [CVE-2023-22501](#), CVSSv3 of 9.4, and has been classified as a low attack complexity because a malicious actor could gain access to registration tokens sent to users with accounts that have never been logged in. This could lead to a user impersonation that would allow unauthorised access to critical instances of Jira Service Management. Atlassian says the security issue affects versions 5.3.0 to 5.5.0, and advises upgrading to versions 5.3.3, 5.4.2, 5.5.1 and 5.6.0 or later. In case the patches cannot be applied as soon as possible, the manufacturer has provided a workaround to manually update the asset.

URL: <https://confluence.atlassian.com/jira/jira-service-management-server-and-data-center-advisory-cve-2023-22501-1188786458.html>



Mustang Panda campaign to distribute PlugX

INTERNATIONAL

Researchers at EclecticiQ have detected the existence of a PlugX malware distribution campaign and attribute it to the APT Mustang Panda. According to the published information, Mustang Panda sent out EU-themed emails containing a supposed Word file that was in fact an LNK-like executable that downloads PlugX onto the victim's system. EclecticiQ claims that the target of the campaign is European governmental institutions and recalls that a similar campaign was attributed to the same actor last October, although in the recently detected campaign Mustang Panda has implemented more evasion techniques to avoid detection.

URL: <https://blog.eclecticiq.com/mustang-panda-apt-group-uses-european-commission-themed-lure-to-deliver-plugx-malware>



Tor and I2P networks hit by DDoS attacks

INTERNATIONAL

Tor and peer-to-peer (I2P) networks have recently been hit by distributed denial-of-service (DDoS) attacks that have caused connectivity and performance problems. On the one hand, Isabela Dias Fernandes, executive director of the Tor Project, issued a statement saying that the network had been under DDoS attacks since July. The target of these ongoing attacks or the identity of the threat actor behind these events has not been detailed. The company has stated that it is continuing to work to improve its defences so that users are not affected. The I2P network has also been the victim of an attack of this type over the last three days, causing performance and connectivity problems. According to the project administrator's statements, as in the case of Tor, the threat actors behind these attacks are using a variety of tactics to perpetrate these DDoS attacks.

URL: <https://blog.torproject.org/tor-network-ddos-attack/>



New Google Chrome update

INTERNATIONAL

Google has released a new version of Chrome 110 which fixes a total of 15 vulnerabilities, 10 of which have been identified by security researchers outside the company. The breakdown of these vulnerabilities according to their criticality is as follows: 3 with high criticality, 5 medium and 2 low. Among these, the three with the highest severity are those identified as: firstly CVE-2023-0696, which could allow a remote attacker

to exploit it through a specially crafted HTML page. In second place, CVE-2023-0697 affecting Chrome for Android, which could allow a remote attacker to use a manipulated HTML page to spoof the content of the security user interface. Lastly, CVE-2023-0698 which would allow a remote attacker to perform an out-of-bounds memory read via a malicious HTML page. It is recommended to update to Chrome versions 110.0.5481.77/.78 for Windows and 110.0.5481.77 for Mac and Linux to fix these vulnerabilities.

URL: <https://chromereleases.googleblog.com/2023/02/stable-channel-update-for-desktop.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



2022 © Telefónica Cybersecurity & Cloud Tech S.L.U. All rights reserved.

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.