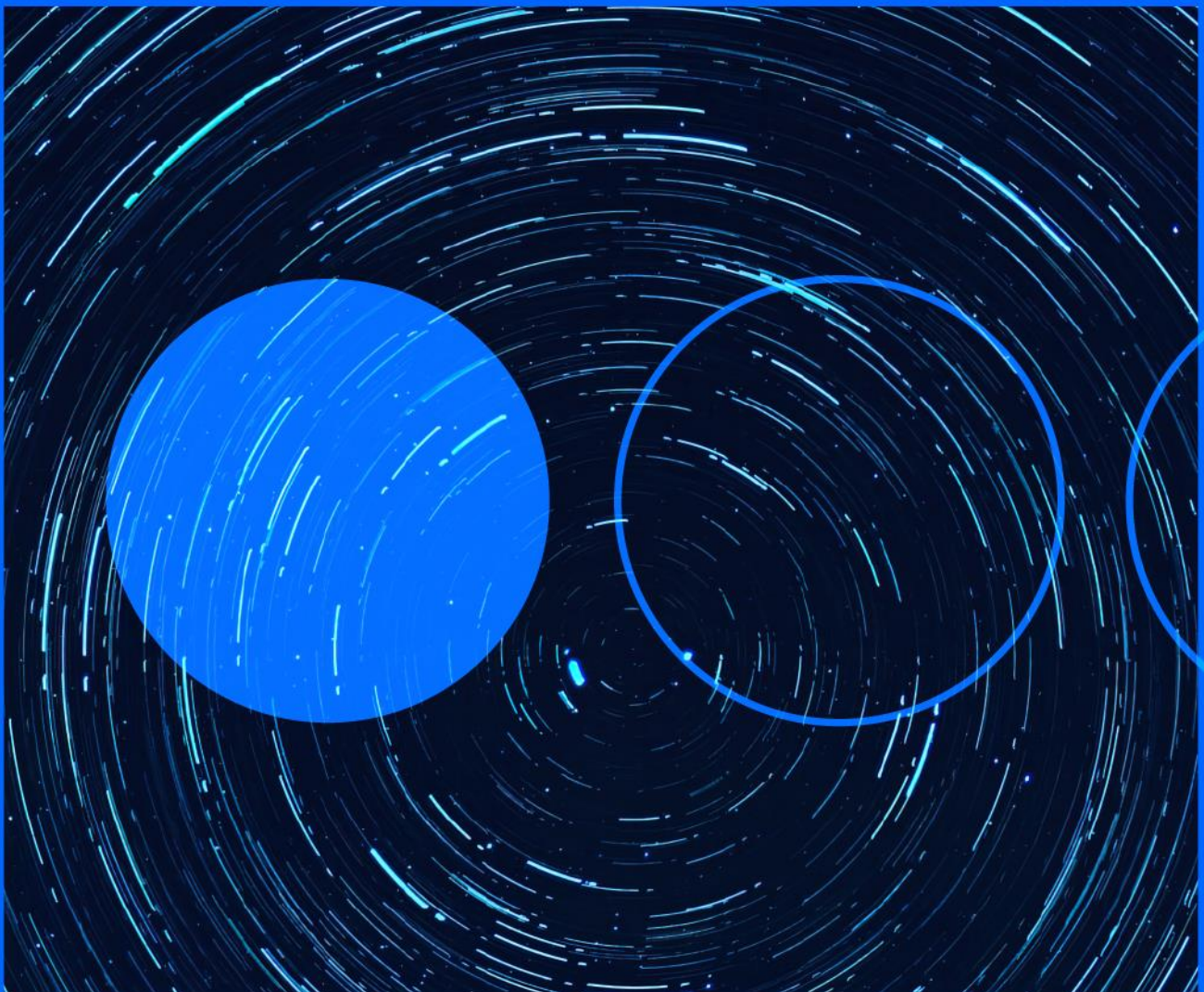







24.02.2023

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



Fortinet fixes critical vulnerabilities in FortiNAC and FortiWeb

INTERNATIONAL

Fortinet has issued a security advisory fixing two critical vulnerabilities affecting its FortiNAC and FortiWeb products. The security flaws have been registered as [CVE-2022-39952](https://www.fortiguard.com/psirt/FG-IR-22-300), with a CVSSv3 of 9.8, which affects FortiNAC and could allow an unauthenticated attacker to execute unauthorised code or commands via a specially crafted HTTP request. The other vulnerability, identified as [CVE-2021-42756](https://www.fortiguard.com/psirt/FG-IR-22-300), has a CVSSv3 of 9.3, affects FortiWeb and its exploitation could allow an unauthenticated remote attacker to perform arbitrary code execution via specially crafted HTTP requests. Fortinet recommends that affected users upgrade FortiNAC to versions 9.4.1, 9.2.6, 9.1.8, and 7.2.0 on the one hand, and upgrade FortiWeb to 7.0.0, 6.3.17, 6.2.7, 6.1.3, and 6.0.8 or later on the other hand.

URL: <https://www.fortiguard.com/psirt/FG-IR-22-300>



Access credentials of two major data centre operators exposed

INTERNATIONAL

The Resecurity team has published an investigation into the sale of login credentials of two data centre operators in Asia, namely GDS Holdings Ltd. (China) and ST Telemedia Global Data Centres (Singapore). The security incidents, which have yet to be clarified, took place in 2021, but only became public knowledge on 20 February, when the stolen data was published on an underground forum. Among the exfiltrated data are credentials, emails, phone numbers or ID card references, with an estimated compromise of more than 3,000 records in total. Indirectly, large global corporations that used these data centres have also been compromised, with logins of [companies](#) such as Apple, BMW, Amazon, Walmart, Alibaba, Microsoft and Ford Motor, among others, being exposed. It should be noted that both data centres forced their customers to change their passwords last January, although Resecurity has confirmed several attempts to access different

customer portals. Finally, it should be noted that researchers have also been unable to attribute these attacks to any particular group.

URL: <https://www.resecurity.com/blog/article/cyber-attacks-on-data-center-organizations>



Fake ChatGPT applications used to distribute malware

INTERNATIONAL

Kaspersky researchers are warning of a fake Windows desktop version of ChatGPT being used to distribute malware. The authors of this campaign, taking advantage of the growing popularity of the OpenAI chatbot, are reportedly using social media accounts to advertise the platform and include a link to the supposed download site. Some of the profiles identified by Kaspersky also offered trial accounts to increase the interest of potential victims. Once the download is complete, an error message is displayed warning of a problem with the installation, while in reality a Trojan with infostealer capabilities has been downloaded and named "Fobo". Cyble's intelligence team [has also investigated](#) the same campaign distributing other malware families such as the Lumma and Aurora stealers. Security researcher Dominic Alvieri [has also published](#) about other cases of campaigns distributing the RedLine stealer.

URL: <https://www.kaspersky.com/blog/chatgpt-stealer-win-client/47274/>



Vulnerabilities in VMware products

INTERNATIONAL

VMware has issued two security advisories warning of two critical vulnerabilities affecting several of the company's products. The most critical security flaw has been reported as [CVE-2023-20858](#), with a CVSSv3 of 9.1 according to the vendor, which affects Carbon Black App Control. Exploiting this vulnerability could allow a malicious actor to use a specially crafted entry in the App Control management console to gain access to the server's operating system. Meanwhile, another vulnerability [has been published](#) as [CVE-2023-20855](#), with a CVSSv3 of 8.8 according to the vendor, which impacts vRealize Orchestrator, vRealize Automation and Cloud Foundation products. In this case, a malicious actor could use specially crafted entries to bypass XML parsing restrictions that terminate access to sensitive information or allow privilege escalation on affected systems.

URL: <https://www.vmware.com/security/advisories/VMSA-2023-0005.html>



Phishing campaign via PayPal

INTERNATIONAL

Avanan researchers have reported a new phishing campaign sent from the PayPal platform. The malicious actors are taking advantage of the ease of creating free PayPal accounts, which offer the ability to create and send invoices to multiple recipients at once. In this way, the messages received by the victims come directly from the PayPal domain, circumventing possible security detections. In the detected campaign, several messages have been observed in which victims are told that their account has been debited, and that in case it has not been authorised, they should call a telephone number. This phone number is not associated with PayPal, and by calling it the attackers get the victims' phone number and other personal details, which can be used in future attacks. Due to the difficulty of implementing security measures to block these emails, researchers recommend searching for the phone number on the Internet in order to see whether or not it is related to PayPal.

URL: <https://www.avanan.com/blog/phishpal-how-paypal-became-a-hackers-haven>

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.