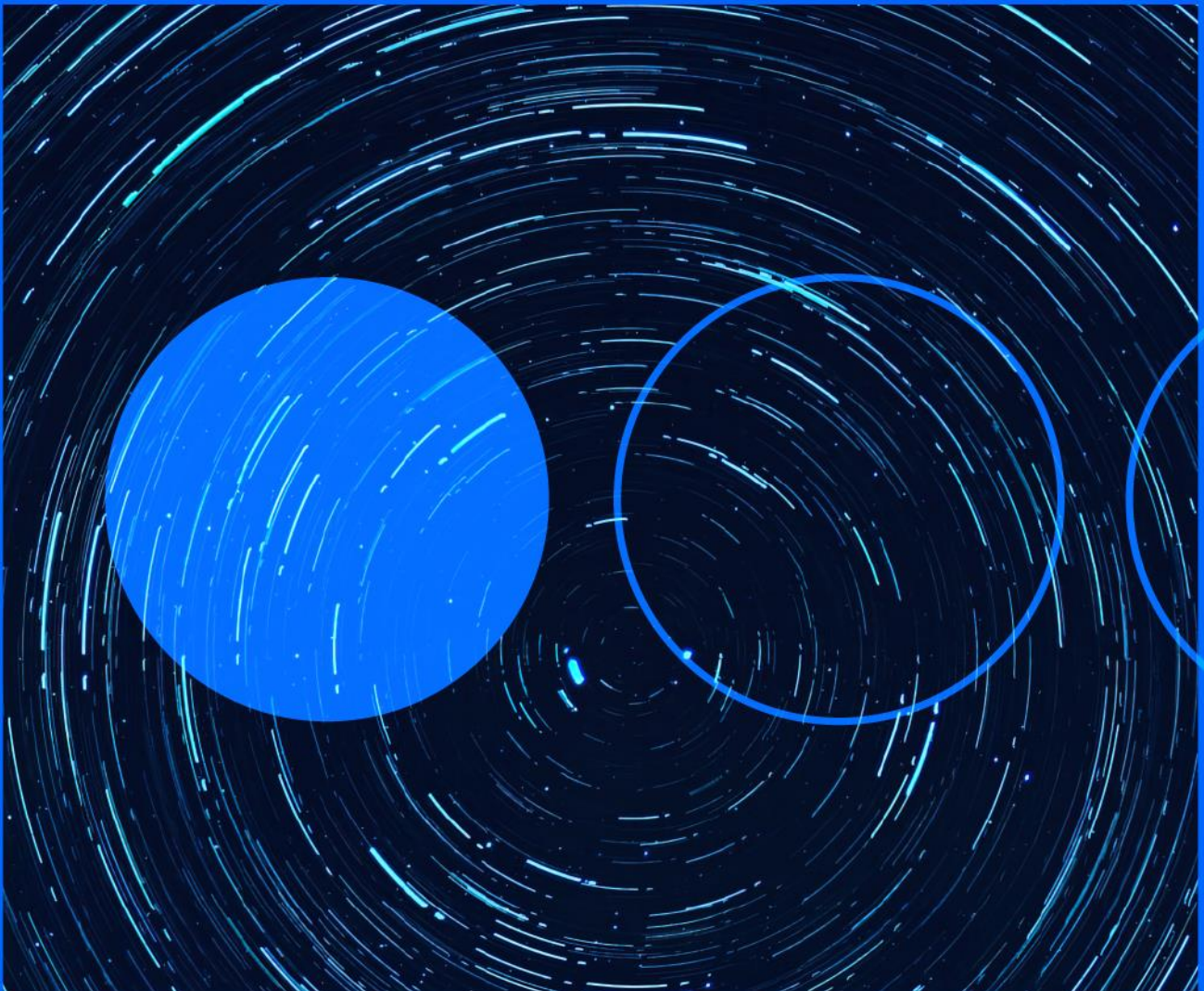







14.11.2022

Cyber threats weekly briefing 2022



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



1. Robin Banks Phishing Platform Reactivated

Researchers at IronNet have published the second part of their investigation into the Robin Banks phishing-as-a-service platform. The platform was [discovered](#) in June this year following the detection of a massive phishing campaign against US financial institutions, after which it was blocked by Cloudflare and its operations were halted.

The platform is now reportedly back in business through Russian ISP DDoS-Guard, incorporating new features such as multi-factor authentication and Adspect redirectors, which would help avoid detection by redirecting suspicious traffic to legitimate-looking websites.

In addition, Robin Banks also makes use of Evilginx2, a proxy that captures victims' session cookies and helps attackers evade protection measures such as two-factor authentication.

More Info: <https://www.ironnet.com/blog/robin-banks-still-might-be-robbing-your-bank-part-2>



2. Cybersecurity incident at an Orange provider

Orange has revealed that one of its suppliers had suffered a cybersecurity incident that resulted in the compromise of personal information of the telecommunications company's customers.

According to the company's statement, the incident at the provider occurred several days ago and involved unauthorized access to systems. As a result, the data of a limited number of customers, who have already been notified by Orange via SMS or email, have been compromised.

Some of the exposed data would be the name, postal address, email address, telephone number, ID number, date of birth, or bank IBAN code of the customers, although not all of this data would have been exposed in the affected cases. It should be noted that no passwords or credit card details were compromised.

The company proceeded to cut off access to the systems when they became aware of the attack, in addition to notifying the Spanish Data Protection Agency and the Central Technological Investigation Brigade (BCIT) of the National Police.



3. Microsoft fixes 68 vulnerabilities including six 0-day vulnerabilities

In its latest security update, Microsoft has fixed a total of 68 vulnerabilities, six of them included actively exploited 0-day flaws:

- [CVE-2022-41128](#), a remote code execution vulnerability with a CVSS score of 8.8.
- [CVE-2022-41091](#), which would allow an attacker to evade Mark-of-the-Web (MOTW) security defenses with a CVSS score of 5.4.
- [CVE-2022-41073](#) and [CVE-2022-41125](#), which would allow a malicious actor to gain system privileges and have a CVSS score of 7.8.
- [CVE-2022-41040](#) and [CVE-2022-41082](#), privilege escalation and remote code execution vulnerabilities in Microsoft Exchange with a CVSS score of 8.8.

These last two would be the vulnerabilities identified last September as ProxyNotShell. Other vulnerabilities categorized by Microsoft as critical and fixed in this latest update are [CVE-2022-37966](#) and [CVE-2022-37967](#) in Windows Kerberos, [CVE-2022-41080](#) in Microsoft Exchange Server and [CVE-2022-38015](#) in Windows Hyper-V.

More info: <https://www.bleepingcomputer.com/news/microsoft/microsoft-november-2022-patch-tuesday-fixes-6-exploited-zero-days-68-flaws/>



4. Critical vulnerabilities in Citrix Gateway and Citrix ADC

As part of its security bulletin released on Tuesday, Citrix has announced three vulnerabilities that users urgently need to patch affecting its Citrix Gateway and Citrix ADC software.

Of these vulnerabilities, [CVE-2022-27510](#) (CVSS 9.8) stands out as a critical flaw that allows bypassing the authentication process by using alternative channels or routes when the application is configured as a VPN. The other two vulnerabilities are also considered critical by NIST, although Citrix has downgraded their criticality to high and medium respectively. These are:

- [CVE-2022-27513](#) (CVSS 9.6 according to NIST, 8.3 according to manufacturer), which allows attackers to take control of the remote desktop via phishing by not correctly verifying the authenticity of the data when the RDP proxy is configured in VPN mode; and
- [CVE-2022-27516](#) (CVSS 9.8 according to NIST, 5.6 according to manufacturer), a vulnerability that allows circumvention of the protection mechanism against brute-force login attempts. This last vulnerability can be exploited in VPN mode or if configured as an AAA virtual server with a maximum number of login attempts.

The company has already patched these flaws for customers of its cloud services, but users who directly manage this software will have to patch individually.

More info: <https://support.citrix.com/article/CTX463706/citrix-gateway-and-citrix-adc-security-bulletin-for-cve202227510-cve202227513-and-cve202227516>



5. StrelaStealer: new malware to steal email credentials

Researchers at DCSO CyTec have identified a new malware, named StrelaStealer, that steals email credentials from Outlook and Thunderbird.

The malware is distributed via ISO files attached to emails with different content. In one of the variants observed, this attachment was a polyglot file, which can be interpreted as different formats depending on the application with which it is opened.

In the case analyzed, this file could either act by downloading StrelaStealer, or display a decoy document in the default browser. The campaign was reportedly first observed in November 2022 targeting Spanish-speaking users.

More info: https://medium.com/@DCSO_CyTec/shortandmalicious-strelastealer-aims-for-mail-credentials-a4c3e78c8abc

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

<https://us.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.