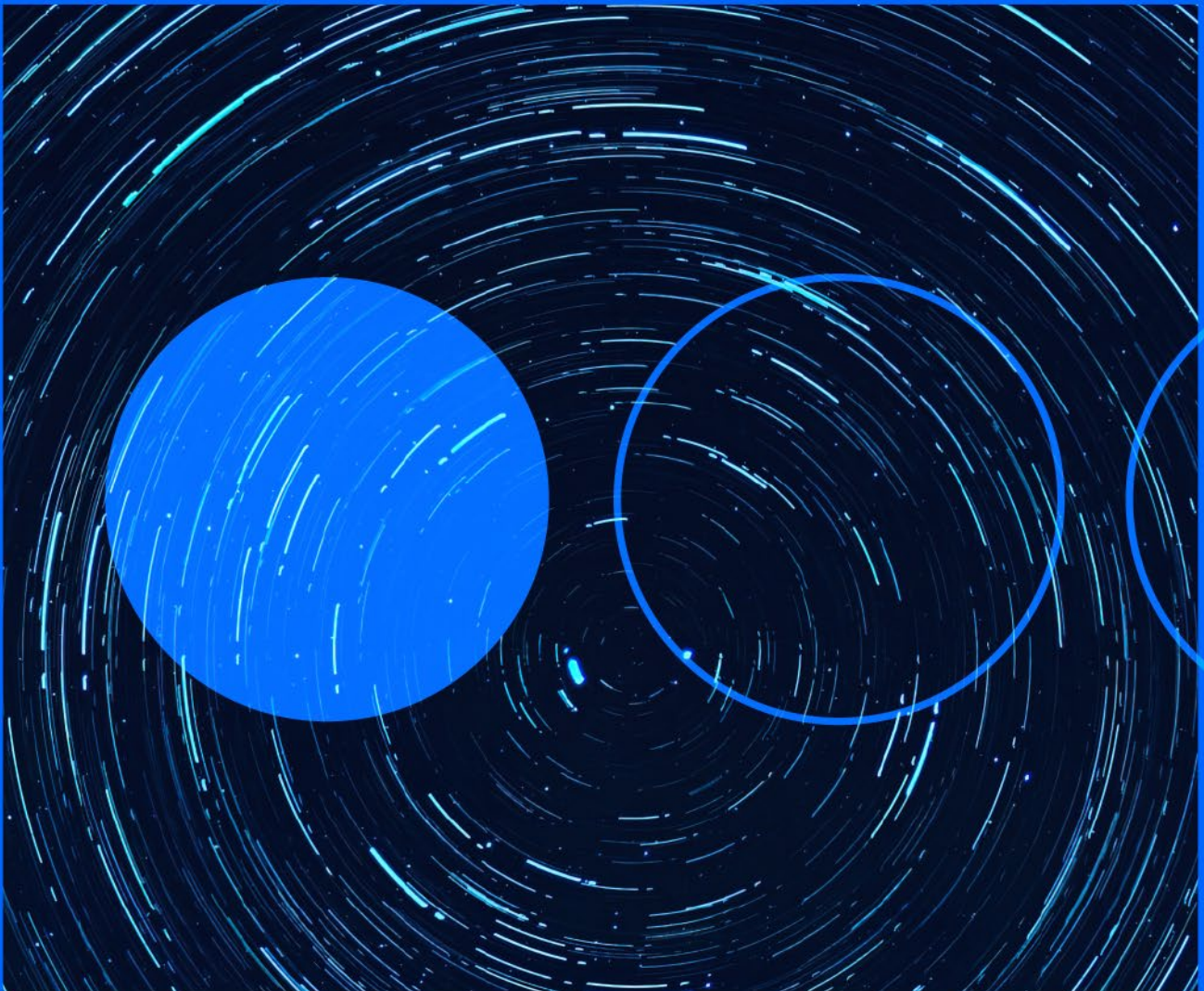







25.11.2022

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



Exploit for ProxyNotShell vulnerabilities published

INTERNATIONAL

The first publications about new critical vulnerabilities in Microsoft Exchange Server, CVE-2022-41040 and CVE-2022-41082, which were named ProxyNotShell, were published at the end of September. However, it was not until this November's Patch Tuesday that Microsoft released patches for these security flaws, even though the company had confirmed that it was aware that malicious actors had actively exploited these vulnerabilities on 30 September through limited targeted attacks. Security researcher Janggggg published an exploit for these vulnerabilities last week, which would be functional in Exchange Server versions 2016 and 2019, and even against 2013 with some modifications, according to confirmations made by security researcher Will Dormann. Microsoft recommends its users to apply the patches as soon as possible to prevent possible future attacks against these vulnerabilities.

URL: <https://twitter.com/wdormann/status/1593311129874403335>



Atlassian fixes vulnerabilities in Crowd and Bitbucket

INTERNATIONAL

The Atlassian team has released a new update in its Crowd Server and Data Center identity management platforms, as well as in Bitbucket Server and Data Center. This update is meant to fix two vulnerabilities considered serious by the company itself and which affected several versions of the aforementioned software. These vulnerabilities are CVE-2022-43781 and CVE-2022-43782. In the first case, it is a command injection vulnerability in Bitbucket that allows the attacker to control the session in order to execute code under certain conditions and permissions. In the case of Crowd, the flaw allows an attacker to bypass password checking during Crowd's authentication process and gain privileges to make API calls to endpoints. Regarding Bitbucket, all versions from 7.0 to 7.21 are affected, as well as versions 8.0 to 8.4, unless they are

instances running PostgreSQL or hosted on Bitbucket's domain. In the case of Crowd, affected versions range from 3.0.0 to 3.7.2 (which will not be fixed) and 5.0.0 to 5.0.2.

URL: <https://confluence.atlassian.com/crowd/crowd-security-advisory-november-2022-1168866129.html>



Cisco Secure Email Gateway Anti-Malware Protection Failure

INTERNATIONAL

The Cisco team confirmed today the existence of a filtering flaw in its Secure Email Gateway and IronPort Email Security Appliance Software versions 14.2.0, as reported by an anonymous researcher earlier last week after allegedly receiving no response from the company. The researcher's discovery consisted of several attack methods that can be used to bypass certain filters within Secure Email Gateway to send malware via specially crafted emails. This would be done via three different attack vectors that exploit a bug in the identification of emails and attachments, if they include malicious MIME Content-Type headers. The attack would be relatively easy to carry out and, according to the anonymous researcher, exploits exploiting the flaw have already been observed. However, the company has denied that this is a vulnerability in its products and blames the flaw on a problem in the anti-malware scanning engines of Sophos and McAfee.

URL: <https://seclists.org/fulldisclosure/2022/Nov/2>



Activity analysis of the Quantum Locker group

INTERNATIONAL

The Belgian company Computerland has shared information on the Tactics, Techniques and Procedures of the malicious actor Quantum Locker. The data comes as a result of the analysis conducted by the organisation during the latest attacks perpetrated by Quantum Locker against geolocated companies in Central Europe. The researchers note that the actor's targets include the complete takeover of Azure cloud services through root account compromise (T1531). In addition, the actor also focuses on locating and deleting all of the victim's Azure blob storage in order to delete backups (T1485). Computerland also warns that the main targets of its attacks are IT administrators and network personnel, so that it can gain access to their resources to collect credentials from the victim's network and extend its attack (T1530). Finally, it is worth noting that Quantum combines new and old techniques to distribute ransomware, such as modifying domain group policies (T1484.001) and exploiting the Any Desk tool as a remote access tool (T1219).

URL: <https://securityaffairs.co/wordpress/138873/cyber-crime/quantum-locker-lands-in-the-cloud.html>



Malicious phishing campaign uses Google Translate to hide malicious links

INTERNATIONAL

Kaspersky researchers have identified a phishing campaign that uses Google Translate links to spread phishing pages. The links are sent by email under various pretexts and end up leading to the attacker's pages, but these are served via Google's translation services which allow full web pages to be translated by entering the URL address. The recipient will see a link to an apparently legitimate Google service (the translate.google domain) that translates the website on the fly and serves the content, in this case malicious content, through an apparently innocuous connection, but which could have the same unwanted effects as a conventional phishing scam.

URL: <https://www.kaspersky.com/blog/google-translate-scheme/46377>

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.