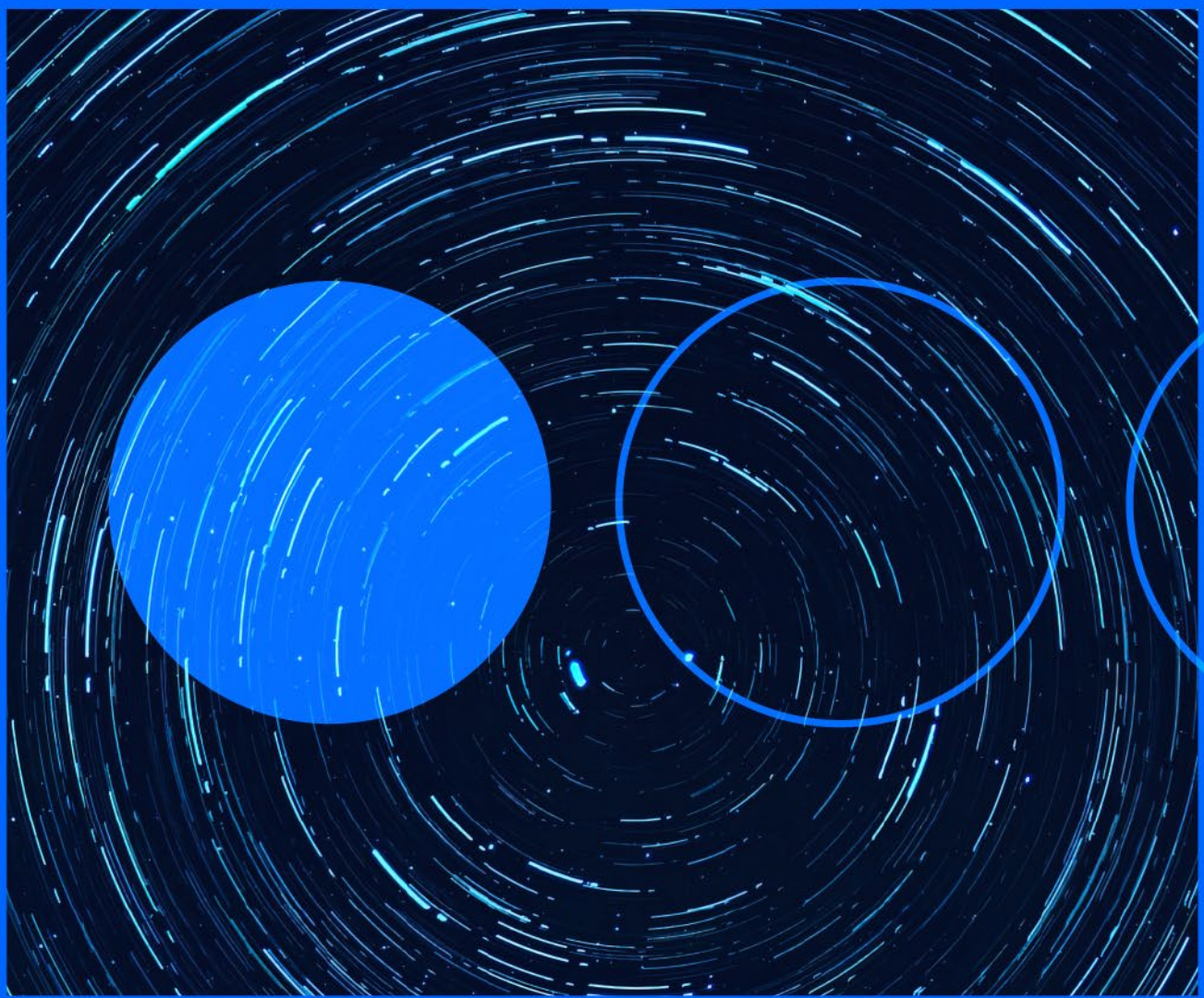
Telefónica Tech

30.09.2022

# Cyber threats weekly briefing 2022



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 |

## Two 0-day vulnerabilities exploited in Microsoft Exchange

### INTERNATIONAL

The Vietnamese cybersecurity team GTSC reported two 0-day vulnerabilities in Microsoft Exchange three weeks ago through the Zero Day Initiative (ZDI) that are reportedly being actively exploited by threat actors. Chaining both security flaws together would allow an attacker to remotely execute code (RCE) on compromised systems. Registered as CVE-2022-41040 and CVE-2022-41082, the first vulnerability consists of a server-side request forgery (SSRF) allowing an authenticated attacker to remotely trigger and exploit the second vulnerability. According to the researchers, active campaigns have been detected making use of the 0-days pair for the implementation of the popular web shell, China Chopper, on vulnerable servers. Once the system is compromised and persistence is achieved, the malicious script will collect information and move laterally to other systems in its victims' networks. Microsoft currently recommends considering implementing a temporary mitigation that would block attack attempts by adding a new rule in IIS via the URL Rewrite Rule module.

URL: https://gteltsc.vn/blog/warning-new-attack-campaign-utilized-a-new-0day-rce-vulnerability-on-microsoft-exchange-server-12715.html

## Critical vulnerability in Sophos Firewall actively exploited

### INTERNATIONAL

Sophos has reported the discovery of a critical vulnerability affecting the Sophos Firewall User Portal and Webadmin which would allow an attacker to perform remote code execution (RCE). The security flaw, listed as CVE-2022-3236 with a CVSS of 9.8, is reportedly being used in campaigns primarily affecting organisations in the South Asia region, which have already been reported, the company said. Sophos has released fixes to address the vulnerability, which affects Sophos Firewall v19.0 MR1 (19.0.1) and earlier. Sophos Firewall applies the new versions by default without any action required from customers, users without this default setting enabled will need to manually upgrade to the new version. If this is not possible, the company advises disabling WAN access to the User Portal and Webadmin.

2022 © Telefónica Cybersecurity & Cloud Tech S.L.U. Todos los derechos reservados.

URL: https://unit42.paloaltonetworks.com/originlogger/

## Chaos: Versatile GO-based malware

### INTERNATIONAL

Researchers at Black Lotus Labs have released a statement with information about the Chaos malware, a new multi-functional GO-based botnet that is experiencing rapid expansion in recent months. First detected in April, Chaos is developed for Windows and Linux devices, with the ability to infect various types of architectures, has capabilities to perform DDoS attacks, cryptomining, establish persistence and propagate automatically, either by brute-force on private SSH keys or using stolen SSH keys. The malware has been associated with a Chinese threat actor, given the language in which it is written and the use of a Chinese-based command-and-control (C2) infrastructure. Although the victims of its attacks tend to be European, the bots are also being distributed across devices in the Americas and Asia, targeting a wide range of industries, as well as devices and systems not so closely linked to a business environment, such as SOHO routers, or the FreeBSD operating system.

URL: https://blog.lumen.com/chaos-is-a-go-based-swiss-army-knife-of-malware/

## New malware on VMware ESXi with backdoor capabilities

### INTERNATIONAL

The Mandiant research team has discovered a new malware family targeting VMware systems and aimed at installing multiple persistent backdoors on ESXi hypervisors. Mandiant links its discovery to the threat actor tracked as UNC3886, which appears to have focused on developing and deploying malware on systems that do not normally support EDR. The detected malware currently targets VMware ESXi, Linux vCenter servers and Windows virtual machines, and would allow transferring files between hypervisors and guest machines, modifying registries and executing arbitrary commands between virtual machines. It would also allow persistence as an administrator on infected systems by installing backdoors, named by researchers as VirtualPita and VirtualPie, via malicious vSphere installation packages ("VIBs").

URL: https://www.mandiant.com/resources/blog/esxi-hypervisors-malware-persistence

2022 © Telefónica Cybersecurity & Cloud Tech S.L.U. Todos los derechos reservados.

## WhatsApp fixes critical 0-day vulnerabilities

**INTERNATIONAL**

Over the last few days, it has come to light that WhatsApp has fixed two 0-day vulnerabilities affecting Android and iOS versions that have received a CVSS rating of up to 9.8, making them critical. Both flaws, CVE-2022-36934 and CVE-2022-27492, would allow attackers to execute arbitrary code remotely. The first one is an Integer overflow vulnerability that allows code execution via a video call without the need for user interaction, by exploiting bugs in the Video Call Handler component code and is present in WhatsApp versions prior to v2.22.16.12. The second one is an Integer underflow flaw that, on the contrary, does require user interaction. The attacker will send a manipulated video file via WhatsApp that will allow the manipulation of Video Call Handler components and will cause additional memory corruption bugs. The versions affected by this vulnerability are versions prior to v2.22.16.2 on Android and v2.22.15.9 on iOS. There are currently no known active attempts to exploit both flaws..

URL: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/webworm-espionage-rats

## 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.