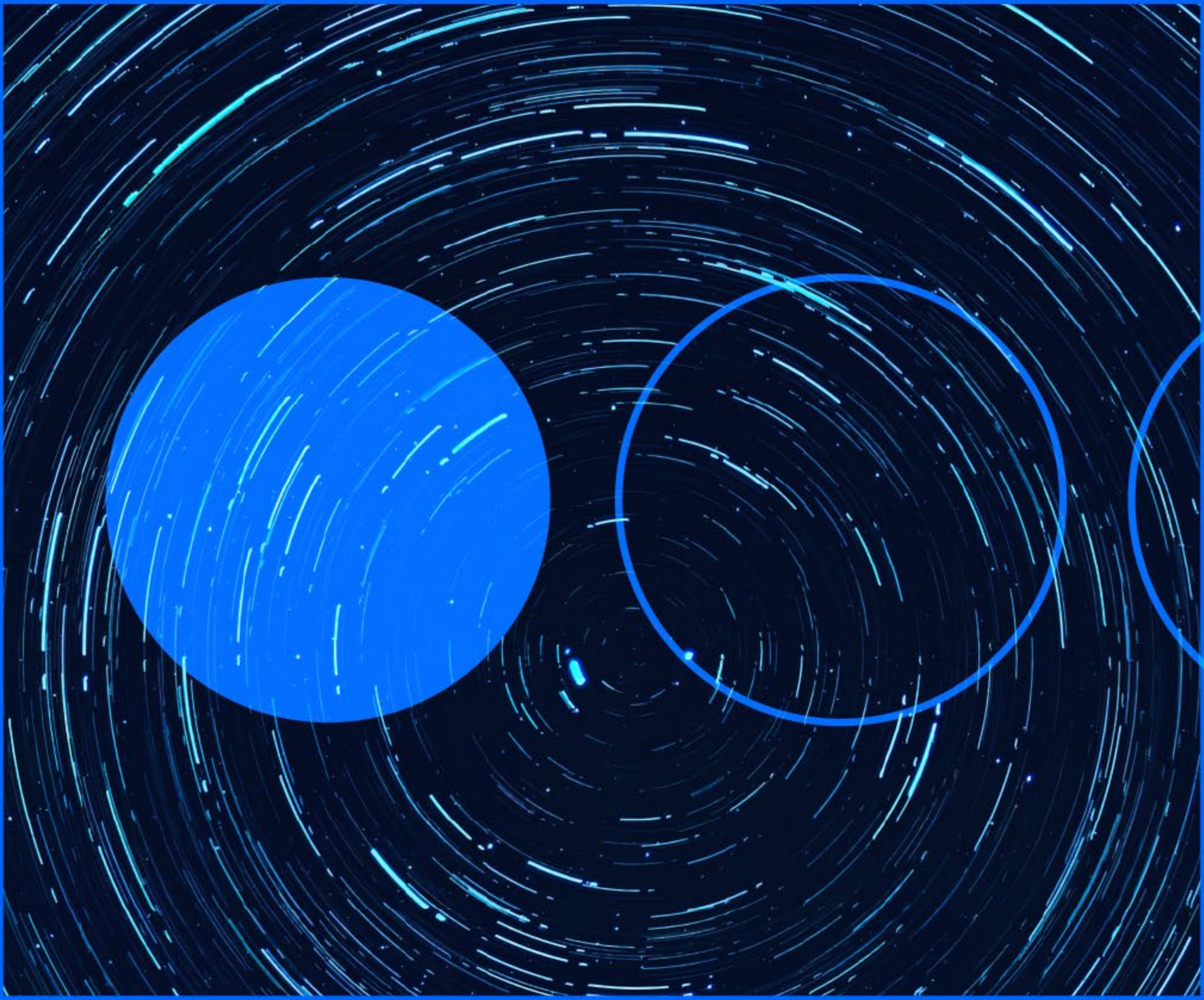
Telefónica
Tech

16.09.2022

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

Microsoft fixes two 0-day and 63 other vulnerabilities in Patch Tuesday

INTERNATIONAL

Microsoft has fixed 63 vulnerabilities in its September Patch Tuesday, including two 0-days, one of them actively exploited, and another five critical flaws that would allow remote code execution. The actively exploited 0-day, identified as CVE-2022-37969 and CVSS 7.8, was discovered by researchers from DBAPPSecurity, Mandiant, CrowdStrike and Zscaler and affects the Common Log File System (CLFS), allowing an attacker to gain system privileges. On the other hand, the second 0-day that has not been exploited is listed as CVE-2022-23960 and with CVSS 5.6, and it refers to a cache speculation restriction vulnerability. Microsoft Dynamics CRM (CVE-2022-35805 and CVE-2022-34700), 2 others in IKE (CVE-2022-34722 and CVE-2022-34721) and, finally, a flaw in Windows TCP/IP (CVE-2022-34718), all of which would allow remote code execution.

URL: https://msrc.microsoft.com/update-guide/releaseNote/2022-Sep

Analysis of the OriginLogger keylogger

INTERNATIONAL

Researcher Jeff White from Unit 42 in Palo Alto has published the results of his recent analysis on the OriginLogger keylogger, which is considered to be the heir to Agent Tesla. It is used to steal credentials, screenshots and all kinds of device information and is for sale on sites that specialise in spreading malware. Its infection chain is initiated through different types of droppers, but usually a Microsoft Office document with malicious macros, which redirect to a page from which a file with an obfuscated script is downloaded, used at the same time for downloading a payload that will be used to create persistence and schedule different tasks. The payload will also contain PowerShell code and two encrypted binaries, one of which is a loader and the other the actual OriginLogger payload. Another feature that makes OriginLogger a separate version of Agent Tesla is the variety of data exfiltration methods, using SMTP and FTP protocols and servers, web pages with their own panels or Telegram channels and bots.

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

Lampion malware distributed in new phishing campaign

INTERNATIONAL

Cofense researchers have analysed a phishing campaign distributed by email, in which the attachment contains a script that downloads and executes the Lampion malware. This malware, discovered in 2019, corresponds to a banking trojan that seeks to steal information from the infected device. It connects to its command-and-control (C2) server and is able to superimpose a page on top of banking login forms to get the user's information. As for the campaign, it is distributed by sending via stolen corporate accounts various fraudulent emails, which attach malicious payment proofs hosted on WeTransfer and urge them to be downloaded. Once the recipient of the fraudulent email downloads the malicious document and opens it, several VBS scripts are executed and the attack chain begins. It is worth noting that Lampion focuses mainly on Spanish-speaking targets, abusing cloud services to host the malware, including Google Drive and pCloud.

URL: https://cofense.com/blog/lampion-trojan-utilizes-new-delivery-through-cloud-based-sharing

SAP Security Bulletins

INTERNATIONAL

SAP has issued 16 security advisories on its September Security Patch Day, fixing 55 Chromium and other high-priority vulnerabilities. First, SAP is issuing security updates for the Google Chromium browser that affect several versions of SAP Business Client. On the other hand, among the high priority vulnerabilities fixed is an XSS vulnerability affecting SAP Knowledge Warehouse, identified as CVE-2021-42063 and with CVSS 8.8. Also among the most critical is CVE-2022-35292, with CVSS of 7.8, which affects the service path in SAP Business One and would allow privilege escalation to SYSTEM. The second priority note corresponds to the SAP BusinessObjects service, affected with two vulnerabilities, one of them, with CVE-2022-39014 and CVSS 7.7, would make it possible for an attacker to gain access to unencrypted confidential information; while the other vulnerability, designated with CVE-2022-28214 and CVSS 7.8, corrects for the possibility of information disclosure in the service. A related vulnerability update, CVE-2022-35291 and CVSS 8.1, affecting SuccessFactors is published, which resumes the functionality of file attachments.

URL: https://dam.sap.com/mac/app/e/pdf/preview/embed/ucQrx6G?ltr=a&rc=10

Webworm activity analysis

INTERNATIONAL

Symantec's threat research team published a post yesterday detailing the activities of a group called Webworm, which reportedly has the same TTPs and devices in use as the threat actor known as Space Pirates, leading researchers to believe they could be the same group. According to the investigation, the group has been active since 2017 and has been engaged in attacks and espionage campaigns against government agencies and companies in the IT, aerospace and energy sectors, especially in Asian countries. Among its usual resources are modified versions of the Trochilus, Gh0st RAT and 9002 RAT remote access trojans, used as a backdoor and spread via loaders hidden in fake documents. It is worth noting that the RATs used by Webworm remain difficult to detect by security tools, as their evasion, obfuscation and anti-analysis tricks are still remarkable.

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

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.