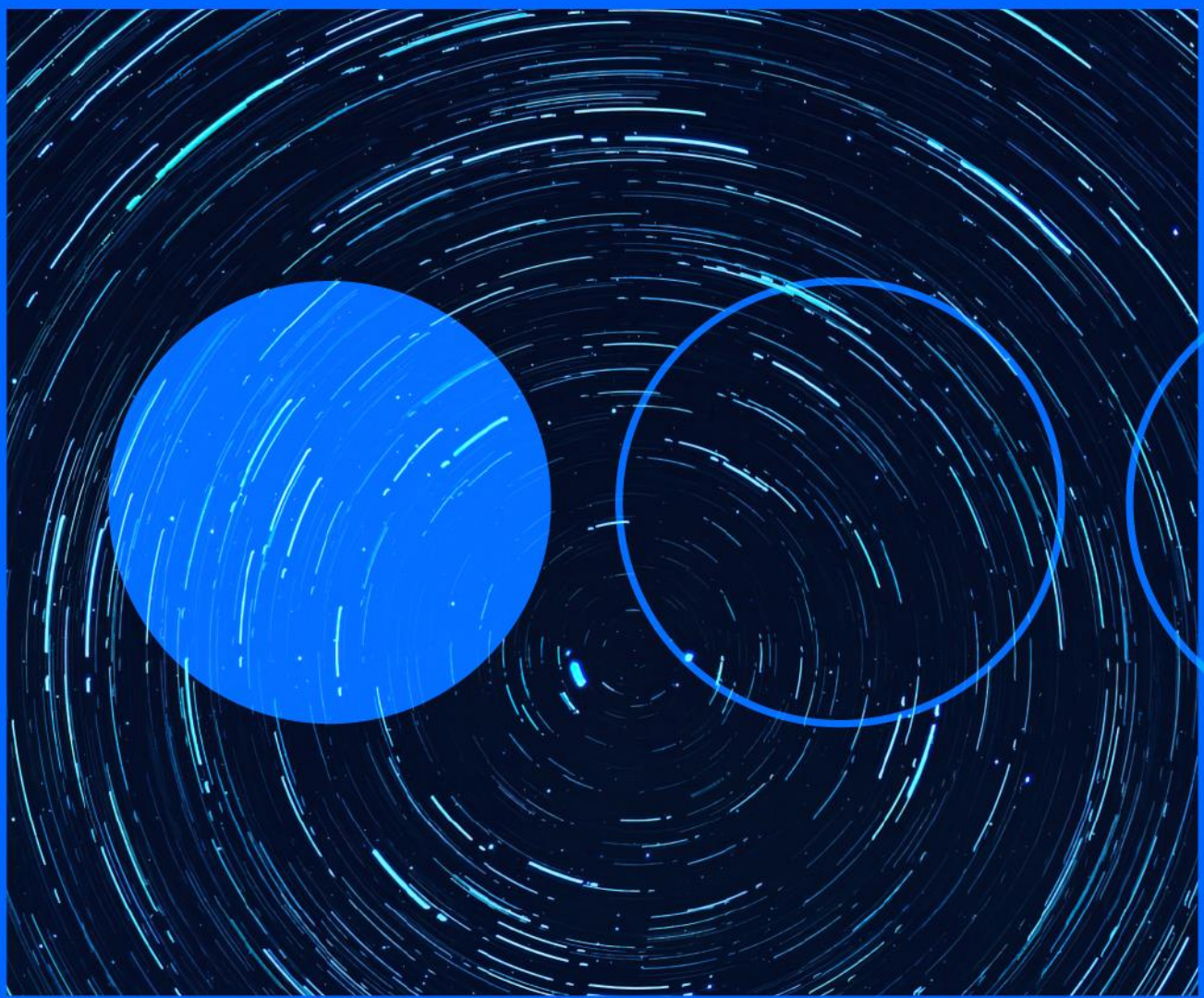
Telefónica Tech

02.12.2022

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

Urgent update to Chrome to prevent the eighth 0-day of 2022

INTERNATIONAL

Google has released an urgent security update for Chrome to prevent exploitation of the eighth 2022 0-day in the browser. The release patches vulnerability CVE-2022-4135, a stack overflow issue. This type of vulnerability allowed an attacker to execute arbitrary code. Google became aware that the vulnerability was being actively exploited by malicious actors, so it released the patch just days after its Threat Analysis Group team discovered the vulnerability. The company has declined to provide details of the problem until users have had time to apply the patch to prevent its exploitation from spreading. Chrome users are advised to update to version 107.0.5304.121/122 for Windows and 107.0.5304.122 for Mac and Linux, which fixes CVE-2022-4135.

Data of 5.4 million Twitter users exposed

INTERNATIONAL

Security researcher Chad Loder posted on Twitter that a database containing 5.4 million entries was currently being shared for free on a forum on the dark web, and that it collected both public (usernames, IDs, followers, location, biography, etc.) and confidential (phone numbers and email addresses) information on users of the social network itself. After the publication, Twitter suspended Loder's account, so he shared the information through Mastodon. According to Loder, this database is the same one that was offered for sale in July and was obtained by exploiting a (now patched) vulnerability in Twitter's API that allowed an attacker to learn the account associated with phone numbers or email addresses. When the sale of the database came to light, Twitter acknowledged the authenticity of the database.

- https://kolektiva.social/@chadloder/109406380942373215

Phishing ring that defrauded 12 million euros broken up in Spain

INTERNATIONAL

The Spanish National Police has issued a statement reporting the success of an operation that has led to the dismantling of a criminal group that had defrauded a total of almost 300 victims of more than 12 million euros by phishing. The six people arrested in Madrid and Barcelona have been charged with alleged membership of a criminal organisation, fraud, money laundering and usurpation of civil status. According to the police statement, the investigation began with the complaint of a Spanish bank for a case of phishing in which it was being impersonated by criminals, who offered through these fake websites financial operations of equities, cryptocurrencies and contracting of financial products to French customers. The police have not made public the malicious URLs used by the criminal organisation.

Three vulnerabilities in industrial products from Festo and Codesys

INTERNATIONAL

Forescout researchers have discovered three vulnerabilities in industrial automation products from the companies Festo and Codesys. The most critical of the three is vulnerability CVE-2022-3270 which, pending publication at NIST, Forescout has preemptively given a CVSS score of CVSS 9.8. The flaw lies in Festo PLCs and would allow an unauthenticated attacker to take control of the device or achieve a denial of service (DoS). Vulnerability CVE-2022-4048, which Forescout has scored with a CVSS 7.7, affects Codesys V3 products and is a weak coding issue that would allow an attacker to logically manipulate the product. Finally, vulnerability CVE-2022-3079, with a CVSS 7.5, allows an unauthenticated attacker to remotely access critical functions of the product website and could allow a denial of service. At this time, no patches have been released for these vulnerabilities.

Google's research on the Heliconia framework

INTERNATIONAL

Google's Threat Analysis Group (TAG) has published the results of an investigation into an exploitation framework targeting already patched vulnerabilities in Chrome, Firefox and Microsoft Defender that could deploy a payload in affected devices, in particular spyware. Google researchers became aware of this framework through an anonymous submission to its Chrome bug-reporting program. It contained three bugs, with instructions and a source code file. Firstly, "Heliconia Noise" allows deploying an exploit for a Chrome renderer bug followed by a sandbox escape. Secondly, "Heliconia Soft" deploys a PDF containing a Windows Defender exploit. Thirdly, "Heliconia Files" contains a set of Firefox exploits for Windows and Linux. According to Google, although no active exploitation has been detected, the vulnerabilities were most likely exploited as 0-days before remediation in 2021 and early 2022. It should also be noted that Google has been able to trace the origin of this exploitation framework Heliconia thanks to the analysis of the source code, being able to link its development to the Barcelona-based company Variston IT, a provider of security solutions, according to the information on its website.

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