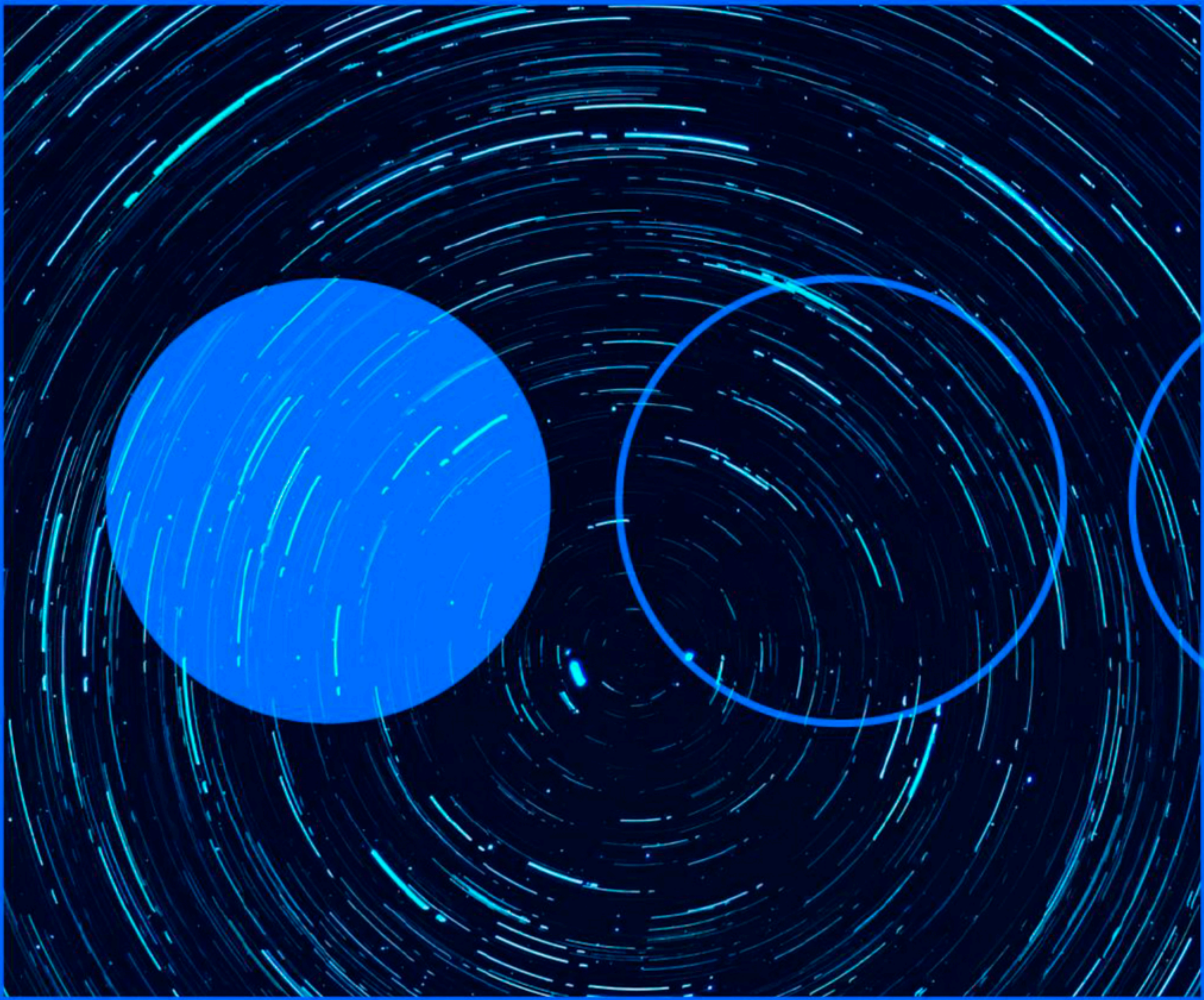
19.08.2022

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

Google reports largest DDoS attack in history

INTERNATIONAL

Google researchers have reported the largest DDoS attack ever recorded. Last 1 June, a Google Cloud Armor client received a series of HTTP DDoS attacks, which reached 46 million requests per second (RPS). This layer 7 DDoS attack has become the largest attack of its kind, being 76% larger than the largest known attack to date [1]. According to the researchers, the attack was executed from 5,256 IP addresses spread across 132 countries, taking advantage of encrypted (HTTPS) requests. Furthermore, 3 per cent of the requests were executed from Tor exit nodes. Researchers have determined that the geographical distribution and the types of unsecured services leveraged to generate the attack match the Mēris botnet attack family. The attack lasted approximately 69 minutes and was stopped when, the researchers believe, the actor realised that the attack was not having the expected impact given the resources employed. Cloud Armor was able to block the attack and the victim was able to keep the services online.

[1] https://blog.cloudflare.com/26m-rps-ddos/

URL: https://cloud.google.com/blog/products/identity-security/how-google-cloud-blocked-largest-layer-7-ddos-attack-at-46-million-rps

Cisco suffers cybersecurity incident

INTERNATIONAL

Cisco has issued a statement confirming that it was the victim of a data compromise at the end of May, on the 24th. According to the company, the entry vector was the theft of an employee's Google credentials stored in the browser. They used social engineering and phishing attacks to get the employee to accept malicious multi-factor notifications, thus gaining access to the corporate VPN and escalating privileges from it. The Yanluowang ransomware group [1] has also claimed responsibility, confirming that the data breach involved 2.75GB of information in 3,100 files in an email sent to Bleeping Computer[2], claiming responsibility and providing evidence. On the other hand, Cisco says that the attackers were only able to steal non-sensitive data from a folder linked to the compromised employee's account, adding that they found no evidence that they managed to access critical internal documentation such as that related to product development, sensitive customer or employee data, and claims that the ransomware would not have been deployed as they have not suffered encryption of any of their data.

[1] https://twitter.com/Cyberknow20/status/1557419082210676736

[2] https://www.bleepingcomputer.com/news/security/cisco-hacked-by-yanluowang-ransomware-gang-28gb-allegedly-stolen/

URL: https://blog.talosintelligence.com/2022/08/recent-cyber-attack.html

11 vulnerabilities in Chrome fixed

INTERNATIONAL

Google has released Stable Channel version 104.0.5112.101 for Mac and Linux, and version 104.0.5112.102/101 for Windows, which fixes a total of 11 vulnerabilities. Among these vulnerabilities, the one catalogued as CVE-2022-2856 stands out, due to the fact that its active exploitation has been detected. This vulnerability was discovered by Google Threat Analysis Group researchers Ashley Shen and Christian Resell, and involves poor validation of untrusted inputs in Intents. On the other hand, vulnerability CVE-2022-2852 is also worth mentioning, as it has been classified as critical. This vulnerability was discovered by Sergei Glazunov of Google Project Zero, being a use after free flaw in FedCM. Google has not provided further details of the vulnerabilities so far in order to allow the majority of users to upgrade.

URL: https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_16.html

Microsoft warns of ongoing phishing campaigns by SEABORGIUM actor

INTERNATIONAL

Researchers at the Microsoft Threat Intelligence Center (MSTIC) have issued an advisory warning of new phishing campaigns by the threat actor SEABORGIUM, also known as ColdRiver or TA446. These campaigns are reportedly mainly targeting NATO organisations and NATO members to obtain sensitive information, although Microsoft has detected attacks against countries in the Baltics, Nordic and Eastern Europe. SEABORGIUM mainly targets defence and intelligence companies, non-governmental organisations (NGOs) and intergovernmental organisations (IGOs), think tanks and higher education. SEABORGIUM operators use social engineering to trick their victims with fraudulent social media profiles to carry out credential theft, which ultimately ends with the sending of phishing emails with malicious URLs or attachments where the victim enters their credentials.

URL: https://www.microsoft.com/security/blog/2022/08/15/disrupting-seaborgiums-ongoing-phishing-operations/

New ransomware GwisinLocker

INTERNATIONAL

Security researchers have tracked down a new ransomware family, called GwisinLocker, targeting South Korean healthcare, industrial and pharmaceutical companies. It has the ability to encrypt Windows and Linux servers, including ESXi servers and virtual machines. Operated by the threat actor Gwisin, which means "ghost" or "spirit" in Korean, it is believed, based on ransom note data, to be in the hands of an advanced persistent threat (APT) group linked to North Korea. On Windows devices [1], the infection is initiated by the execution of an MSI installer that requires special parameters in the command console to execute the DLL file included in the MSI itself. This DLL will perform encryption actions by injecting itself into a Windows system process, thus evading detection by antivirus systems. It also supports a function to encrypt files in safe mode. Regarding the Linux version [2], the analysed sample suggests that it is a sophisticated malware with features particularly designed to manage Linux servers, targeting VMware ESXi virtual machines. Notably, GwisinLocker combines AES symmetric key encryption with SHA256 hashing, generating a unique key for each file.

URL: https://www.bleepingcomputer.com/news/security/new-gwisinlocker-ransomware-encrypts-windows-and-linux-esxi-servers/

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.