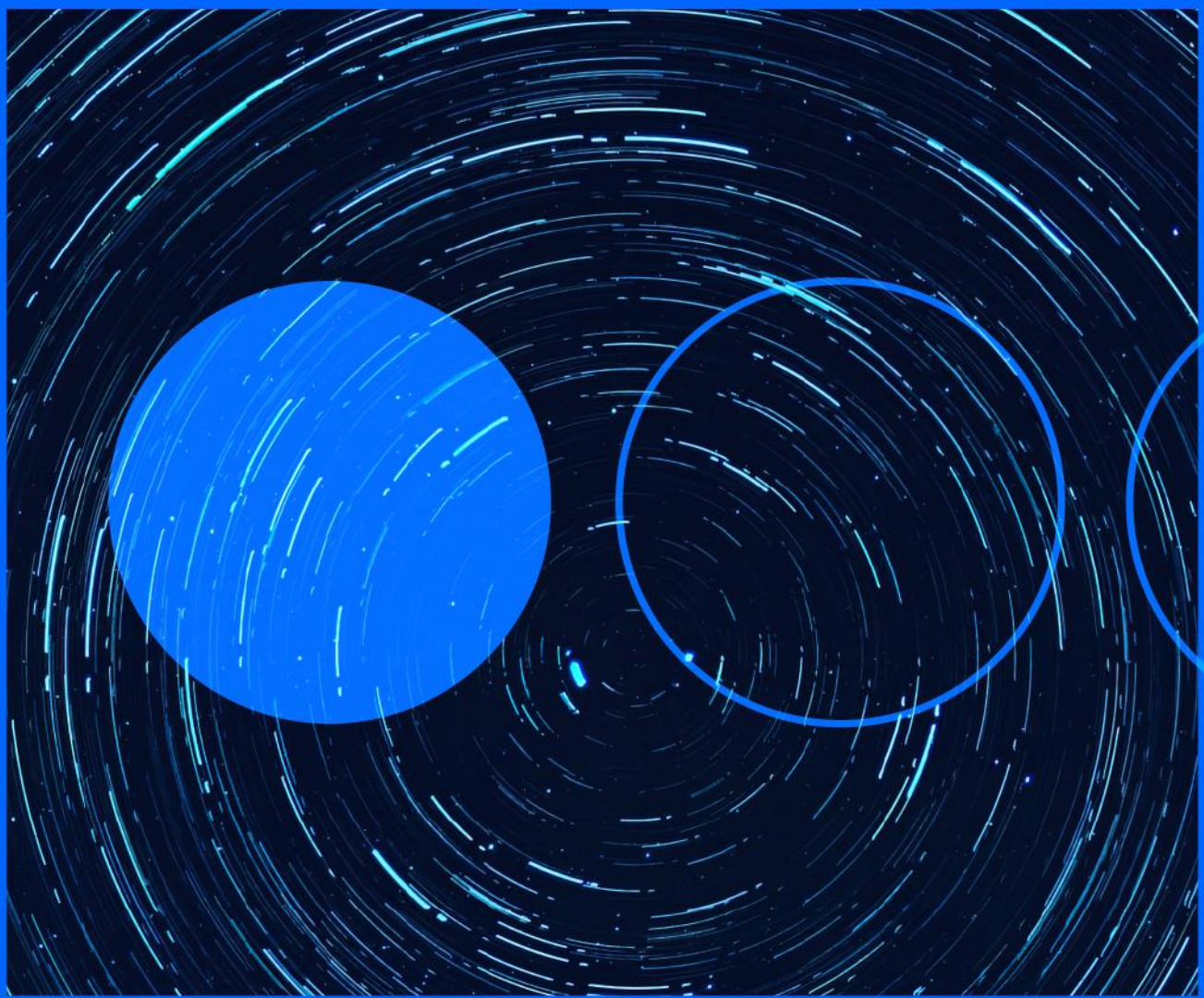
Telefónica Tech

16.12.2022

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

Microsoft fixes in its December Patch Tuesday two 0-day vulnerabilities and 49 other bugs

INTERNATIONAL

Among the fixed vulnerabilities, two of them are 0-day, one of them actively exploited and identified as CVE-2022-44698 and CVSS 5.4, which refers to a bypass vulnerability in the Windows SmartScreen security feature. An attacker could exploit this vulnerability by creating a malicious file that bypasses Mark Of The Web (MOTW) security, resulting in the loss of security features such as protected view in Microsoft Office. Threat actors exploited this vulnerability through malicious JavaScript files in numerous malware distribution campaigns. The other 0-day, identified as CVE-2022-44710 and CVSS 7.8, would allow privilege escalation of the DirectX graphics kernel. The rest of the fixed bugs would allow information disclosure, denial of service and impersonation. Finally, Microsoft has included in its update, 29 improvements and fixes among which fix problems in Task Manager, Microsoft OneDrive or Windows Spotlight.

URL: https://www.bleepingcomputer.com/news/microsoft/microsoft-december-2022-patch-tuesday-fixes-2-zero-days-49-flaws/

Citrix fixes actively exploited 0-day vulnerability

INTERNATIONAL

Citrix has issued a security alert warning administrators of a critical, actively exploited, 0-day vulnerability affecting Citrix ADC and Gateway. This flaw, tracked as CVE-2022-27518 and still awaiting CVSS score, would allow an attacker to remotely execute code without authentication. Affected Citrix ADC and Citrix Gateway versions would be those prior to 13.0-58.32 and would be corrected by updating to current 13.0-88.16 or 13.1 versions. Although the company has not yet offered any further details, the security note mentions a small number of targeted attacks taking advantage of this vulnerability. The National Security Agency has issued an advisory stating that the attacks would be attributed to the group known as APT5, UNC2630 or MANGANESE and includes detection and mitigation steps.

URL: https://www.citrix.com/blogs/2022/12/13/critical-security-update-now-available-for-citrix-adc-citrix-gateway/

New Apple 0-day vulnerability exploited

INTERNATIONAL

Apple has released the monthly security bulletin fixing vulnerabilities affecting iOS/iPadOS 15.7.2, Safari 16.2, tvOS 16.2 and macOS Ventura 13.1, including the tenth 0-day of the year affecting iPhone devices, which could be actively exploited. Specifically, this security flaw identified as CVE-2022-42856 is a problem in Apple's Webkit browser engine, which could allow threat actors to create a malicious website specially designed to use code execution on a vulnerable device. This vulnerability was discovered by security researcher Clément Lecigne, a member of Google's threat analysis team, and although no further details on this issue are available at the moment, it is expected that more information on this vulnerability will be published some time after the patches are released once users update their devices.

URL: https://www.cybereason.com/blog/royal-ransomware-analysis

Royal ransomware becomes a potential threat

INTERNATIONAL

Researchers from Cybereason Global SOC and Cybereason Security Research Teams have published an analysis of the Royal ransomware group, describing its tactics, techniques and procedures (TTP). The ransomware was detected earlier this year, but it was not until September that it began using its own ransomware, making it the most active ransomware at the moment, surpassing Lockbit. Royal's entry vectors are diverse, one of them being through phishing campaigns, also using loaders such as Qbot or BATLOADER, which subsequently implement a Cobalt Strike payload in order to continue the infection operation. The ransomware is also known to employ multiple threads to speed up encryption, and to use partial encryption, making detection more difficult. Researchers estimate that Royal is made up of former members of other ransomware groups, specifically pointing to Conti. Cybereason also points out that Royal ransomware is a high-potential threat, because its victims are not sector-specific and are spread across the globe

URL: https://www.cybereason.com/blog/royal-ransomware-analysis

Atlassian cookies allow unauthorized access even with two-factor login enabled

INTERNATIONAL

Recently, security company CloudSek was the victim of a cyberattack and its internal investigation has uncovered a vulnerability in Atlassian products. CloudSek identified that the threat actor gained access to an

employee's Jira account by using a session cookie stolen with a stealer and sold on the darkweb, which led the investigation to reveal that cookies in Atlassian products (Jira, Confluence, Trello and BitBicket) remain valid for 30 days even if the user's password has been changed or two-factor authentication is enabled.Atlassian has not yet patched the vulnerability, so Cloudsek warns of the wide-ranging impact it could have given that it affects more than 10 million users of the 180,000 companies that have signed up for Atlassian products.

URL: https://cloudsek.com/security-flaw-in-atlassian-products-jira-confluencetrello-bitbucket-affecting-multiple-companies

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