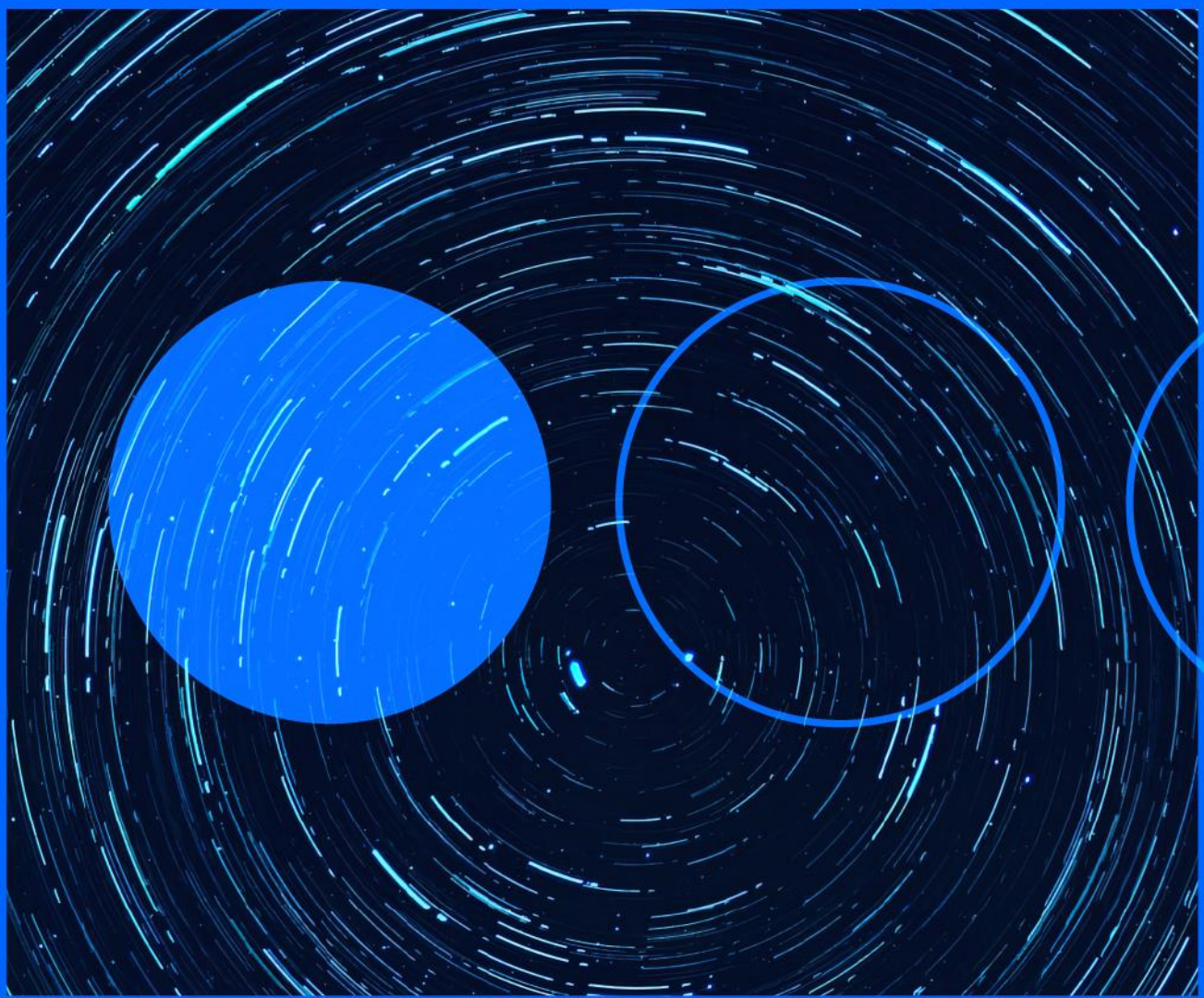
Telefónica Tech

15.07.2022

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

Rozena: backdoor distributed by exploiting Follina vulnerability

INTERNATIONAL

Fortinet researchers have published an analysis of a malicious campaign in which they have detected the distribution of a new backdoor exploiting the well-known Follina vulnerability (CVE-2022-30190)[1]. This new malware has been named Rozena and its main function is to inject a reverse shell into the attacker's host, allowing malicious actors to take control of the victim's system, as well as to enable monitoring and information capture, and/or to maintain a backdoor to the compromised system. Regarding the methodology used to carry out the infection, it consists of distributing malicious office documents, which when executed, connect to a Discord URL that retrieves an HTML file that, in turn, invokes the vulnerable Microsoft Windows Support Diagnostic Tool (MSDT), resulting in the download of the payload, in which Rozena is included.

[1] https://nvd.nist.gov/vuln/detail/CVE-2022-30190

URL: https://www.fortinet.com/blog/threat-research/follina-rozena-leveraging-discord-to-distribute-a-backdoor

Microsoft fixes an actively exploited 0-day

INTERNATIONAL

Microsoft has published its security bulletin for the month of July in which it fixes a total of 84 vulnerabilities, including one actively exploited 0-day. Out of the total number of detected flaws, 5 correspond to denial of service vulnerabilities, 11 to information disclosure, 4 to omission of security functions, 52 to elevation of privileges, and 12 to remote code execution. Within this last type are the four vulnerabilities classified as critical (CVE-2022-30221 [1], CVE-2022-22029 [2], CVE-2022-22039 [3], CVE-2022-22038 [4]), with the rest of the vulnerabilities being of high severity. It is worth noting the 0-day, catalogued as CVE-2022-22047 with a CVSSv3 7.8 [5], discovered by Microsoft Threat Intelligence Center (MSTIC) and Microsoft Security Response Center (MSRC), involves a Windows CSRSS elevation of privilege vulnerability, which could allow

an attacker to gain SYSTEM privileges. According to Microsoft, active exploitation of this flaw has been detected [6], although no further details have been provided so far, and it is recommended that patches be applied as soon as possible. Also, CISA [7] has added this vulnerability to its catalogue [8] of actively exploited vulnerabilities.

[1] https://nvd.nist.gov/vuln/detail/CVE-2022-30221

[2] https://nvd.nist.gov/vuln/detail/CVE-2022-22029

[3] https://nvd.nist.gov/vuln/detail/CVE-2022-22039

[4] https://nvd.nist.gov/vuln/detail/CVE-2022-22038

[5] https://nvd.nist.gov/vuln/detail/CVE-2022-22047

[6] https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-22047

[7] https://www.cisa.gov/uscert/ncas/current-activity/2022/07/12/microsoft-releases-july-2022-security-updates

[8] https://www.cisa.gov/uscert/ncas/current-activity/2022/07/12/cisa-adds-one-known-exploited-vulnerability-catalog

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

Vulnerability in the authentication of an AWS Kubernetes component

INTERNATIONAL

Security researcher Gafnit Amiga has discovered several security flaws in the authentication process of AWS IAM Authenticator, a component for Kubernetes used by Amazon Elastic Kubernetes Service (EKS). The flaw lies in incorrect validation of query parameters within the authenticator plugin when configuring the use of the template's "AccessKeyID" parameter within query strings. Exploiting it could allow an attacker to bypass existing protection against replay attacks or obtain the highest permissions in the cluster by impersonating other identities, i.e., escalate privileges within the Kubernetes cluster. According to the researcher, two of the identified flaws have existed since the first release in 2017, while the third, which is the one that allows impersonation, has been exploitable since September 2020. The flaws as a whole have been identified as CVE-2022-2385 [1] and have been given a high criticality. AWS has confirmed [2] that since 28 June all EKS clusters have been updated with a new version of IAM Authenticator that fixes the issue. Customers who manage their own clusters and use the "AccessKeyID" parameter of the authenticator plugin should upgrade to AWS IAM Authenticator for Kubernetes version 0.5.0.

[1] https://github.com/kubernetes-sigs/aws-iam-authenticator/issues/472

[2] https://aws.amazon.com/es/security/security-bulletins/AWS-2022-007/

URL: https://blog.lightspin.io/exploiting-eks-authentication-vulnerability-in-aws-iam-authenticator

VMware fixes vCenter Server vulnerability

INTERNATIONAL

VMware has recently published a new version of vCenter Server 7.0 3f in which it corrects, eight months later, a vulnerability in the integrated authentication mechanism with Windows discovered by Crowdstrike and with CVE-2021-22048. This flaw can only be exploited from the same physical or logical network as the affected server, and although it is a complex attack, it requires few privileges and no user interaction. However, NIST suggests that it could be exploited remotely. The versions of vCenter Server affected by the vulnerability are 6.5, 6.7 and 7.0. The company has provided mitigation measures for those who are unable to upgrade to the latest patched version by switching to an Active Directory over LDAP authentication model [1]. CVE-2021-22048 also affects WMware Cloud Foundation versions 3 and 4 but has not yet been fixed.

[1] https://kb.vmware.com/s/article/86292

URL: https://www.vmware.com/security/advisories/VMSA-2021-0025.html#:~:text=2022%2D07%2D12%20VMSA%2D2021%2D0025.2

Phishing campaign via Anubis Network

INTERNATIONAL

Portuguese media outlet Segurança Informatica has published details of a new wave of the persistent phishing campaign, which uses the Anubis Network portal to set up its attacks and has been active since March 2022. Affected users, mainly in Portugal and Brazil, receive smishing or phishing messages from financial services where users are forced to enter their phone number and PIN number, only to be redirected to banking pages where they are asked for their login credentials. According to the researchers, the Command & Control server, hosted by Anubis Network, is controlled by around 80 operators. The analysis also shows how Anubis provides facilities for tracking user data, fake domains created to impersonate banks and temporary email addresses that operators can set up for each case.

URL: https://seguranca-informatica.pt/anubis-networks-is-back-with-new-c2-server/#.Ys0fxnZBw2y

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