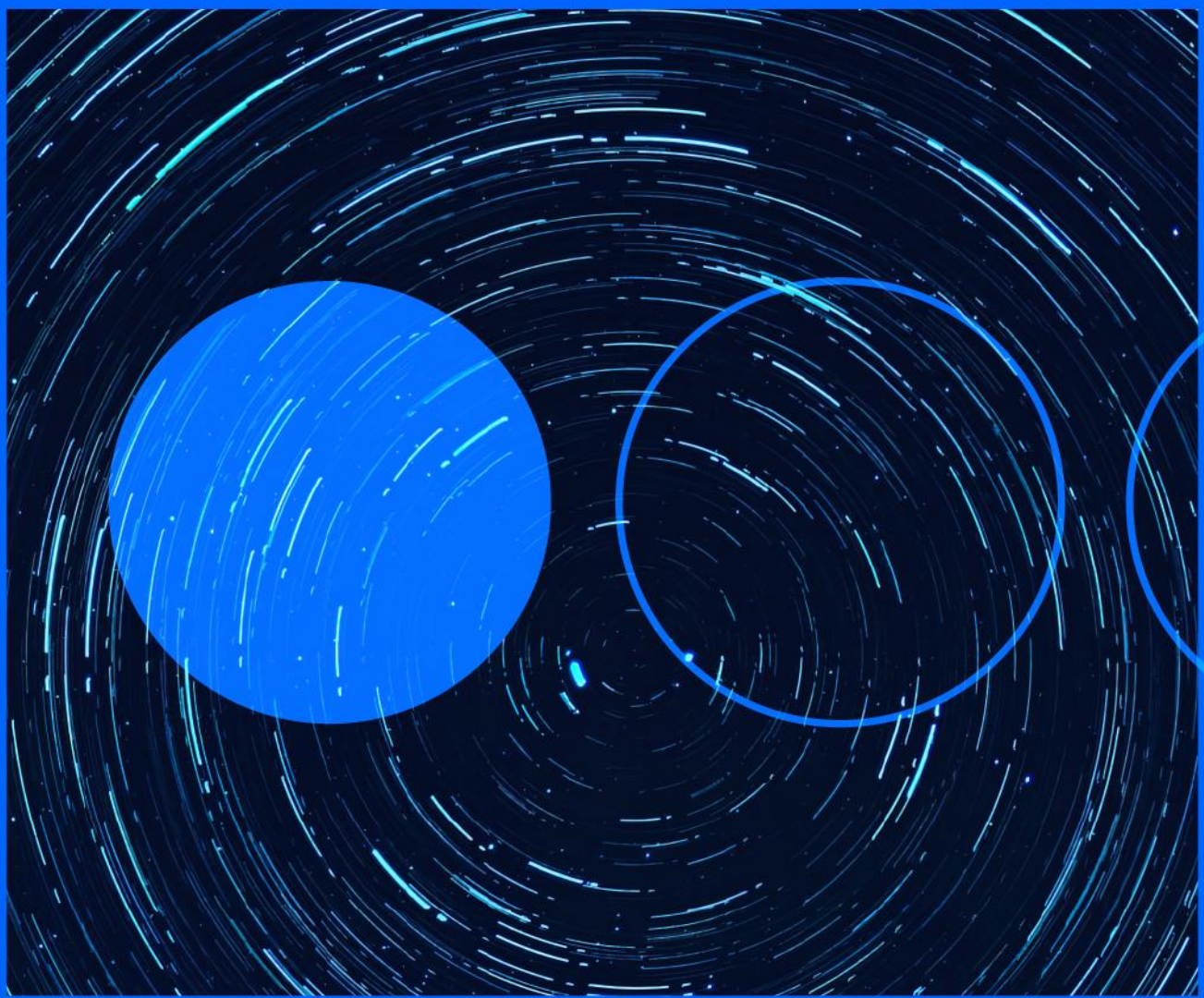
Telefónica Tech

05.08.2022

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

Possible link between Raspberry Robin malware and Evil Corp infections

INTERNATIONAL

The Microsoft Threat Intelligence Center (MSTIC) team has published new information about the Raspberry Robin malware, first detected by the Red Canary team in September 2021 [1]. The main method of spread associated with this family is via infected USB devices, and one of its main features is the use of QNAP NAS devices as Command & Control (C2) servers. In their update, Microsoft experts reportedly discovered that Raspberry Robin, in more advanced stages, is deploying the FakeUpdates malware, traditionally linked to the DEV-0206 actor, on infected networks. However, once FakeUpdates is successfully distributed, the activity observed leads to actions that have traditionally been linked to those carried out by DEV-0243 (Evil Corp) prior to its ransomware infections. In terms of impact, it is worth noting that this malware is reported to have been detected in hundreds of organisations across a multitude of industries.

[1] https://redcanary.com/blog/raspberry-robin/

URL: https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/#DEV-0206-DEV-0243

VMware critical security advisory

INTERNATIONAL

VMware has issued a critical security advisory (VMSA-2022-0021) reporting ten recently detected and patched vulnerabilities. These include a critical vulnerability discovered by VNG Security researcher Petrus Viet and listed as CVE-2022-31656 with a CVSSv3 of 9.8. It is an authentication bypass vulnerability that affects local domain users and could allow an unauthenticated attacker to gain administrator privileges. Regarding the rest of the vulnerabilities, six of them have been catalogued with a "significant" risk (CVE-2022-31658, CVE-2022-31659, CVE-2022-31660, CVE-2022-31661, CVE-2022-31664, CVE-2022-31665, CVE-2022-31665), CVE-2022-31665) and three with "moderate" risk (CVE-2022-31657, CVE-2022-31662, CVE-2022-31663), including remote code execution, privilege escalation and cross-site scripting (XSS) bugs, among others. These bugs affect VMware Workspace ONE Access (Access), VMware Workspace ONE

Access Connector (Access Connector), VMware Identity Manager (vIDM), VMware Identity Manager Connector (vIDM Connector), VMware vRealize Automation (vRA), VMware Cloud Foundation, and vRealize Suite Lifecycle Manager products. While VMware is urging that the patches be implemented as soon as possible, it should be noted that no active exploitation has been detected so far.

URL: https://www.vmware.com/security/advisories/VMSA-2022-0021.html

Vulnerabilities in Apache HTTP Server

INTERNATIONAL

Multiple vulnerabilities have been discovered in Apache HTTP Server affecting versions prior to 2.4.54. A remote attacker could exploit some of these vulnerabilities to trigger a denial-of-service condition, disclosure of confidential information, cross-site scripting (XSS), or circumvention of security restrictions on the target system. The vulnerability catalogued as CVE-2022-31813 [1] stands out for having a CVSSv3 of 9.8 and its exploitation would allow the evasion of IP-based authentication control by not sending, under certain conditions, X-Forwarder-* headers. It should also be noted that these bugs affect many products that use the Apache server, such as IBM [2] or F5 [3], and it is therefore recommended that Apache HTTP Server is updated as soon as possible following the vendor's instructions.

[1] https://nvd.nist.gov/vuln/detail/CVE-2022-31813

[2] https://www.ibm.com/support/pages/node/6595149

[3] https://support.f5.com/csp/article/K21192332

URL: https://httpd.apache.org/security/vulnerabilities_24.html

Remote code execution vulnerability in DrayTek routers

INTERNATIONAL

The Trellix Threat Labs team has detected an important remote code execution vulnerability affecting DrayTek routers. Exploitation of the vulnerability, tracked as CVE-2022-32548 - CVSSv3 10.0 [1], would allow the execution of attacks that do not require user interaction, as long as the device's management interface is configured for network services. If successful, the attacker would gain access to the device's internal resources, completely compromise the device, and even launch attacks within the LAN from the device's own default configuration. The flaw affects the Vigor 3910 along with 28 other DrayTek models that share the same code base and has been patched by the company. Trellix has also published a video [2] detailing the process of exploiting this vulnerability, so it is recommended not to expose the administration interface to the Internet, reset passwords and update the software of the affected devices to the latest version.

[1] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-32548
[2] https://youtu.be/9ZVaj8ETCU8

URL: https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/rce-in-dratyek-routers.html

RapperBot: new botnet targeting Linux systems

INTERNATIONAL

Fortinet security researchers have discovered a new botnet, called RapperBot, that specifically targets Linux systems. This new malware is reportedly based on the original source code of the Mirai botnet but is notable for having unique features that are rare in this type of malware, such as its own Command & Control (C2) protocol. Also unlike Mirai, RapperBot focuses on using brute-force techniques to access SSH servers instead of Telnet, launching tests on lists of credentials downloaded by the malware from its own resources. If it succeeds in gaining access to the server, the bot adds a new SSH key and creates a Cron task that re-adds the user every hour in case an administrator discovers the account and deletes it. It is currently unknown what RapperBot's main purpose may be, as its authors have kept its DDoS functions limited. However, the addition of persistence and detection evasion mechanisms indicate that the botnet's operators may be interested in initial access sales to ransomware actors.

URL: https://www.fortinet.com/blog/threat-research/rapperbot-malware-discovery

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