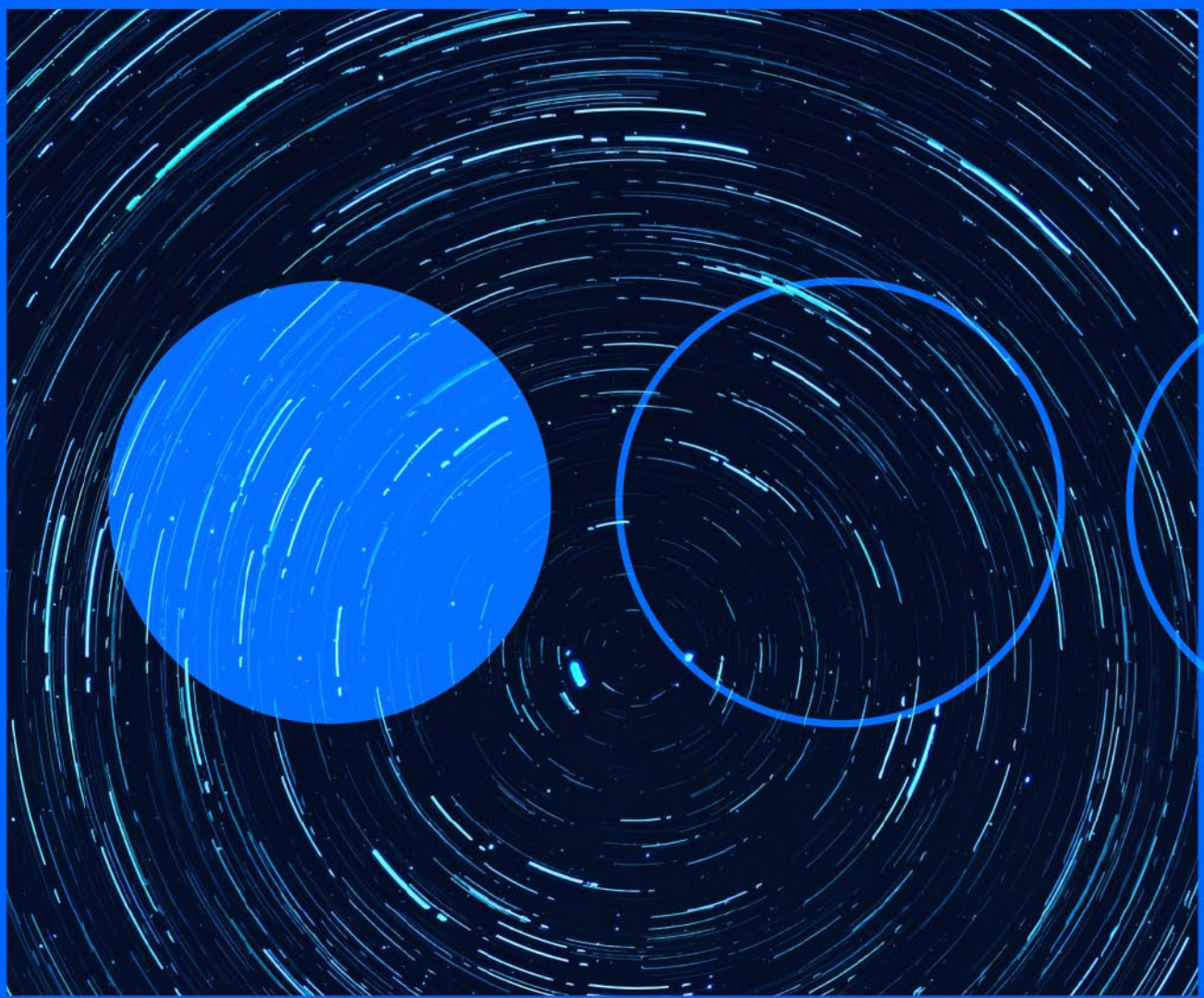
Telefónica Tech

07.10.2022

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

Lazarus targets Dell via new FudModule rootkit

INTERNATIONAL

ESET researchers have reported a new Lazarus campaign targeting a Dell hardware driver using a new rootkit called FudModule. The rootkit uses a technique called bring your own vulnerable driver (BYOVD) to exploit a vulnerability in a Dell hardware driver for the first time. This technique, known as BYOVD, happens when malicious actors load legitimate, signed drivers into Windows that have known vulnerabilities. The campaign, aimed at espionage and data theft, was conducted via spear-phishing from autumn 2021, affecting targets in the Netherlands and Belgium. The malicious emails sent were presented as job offers, and deployed malware loaders (droppers), and customised backdoors. The most notable tool was a user-mode module that gained the ability to read and write kernel memory due to vulnerability CVE-2021-21551. This vulnerability affected a legitimate Dell hardware driver ("dbutil_2_3.sys") and has remained exploitable for 12 years until the manufacturer has issued security updates to fix it.

URL: https://www.welivesecurity.com/2022/09/30/amazon-themed-campaigns-lazarus-netherlands-belgium/

Evolution of the Bumblebee malware

INTERNATIONAL

Checkpoint researchers have published a study highlighting the constant evolution of this malware, which was discovered earlier this year. Checkpoint outlines several features that confirm the constant changes brought about by Bumblebee. These include the input vector used for distribution, most commonly injecting a DLL into an ISO file, however, this has been modified in the past by using a VHD file and has again reverted to ISO delivery via malspam campaigns. As a result, the researchers note the inclusion of checking mechanisms in sandbox environments, to prevent malware analysis. It is also estimated that, until last July, Bumblebee's Command & Control (C2) servers only accepted one infected victim on the same IP address, i.e., if several computers in an organisation accessing the internet with the same public IP are infected, the C2 server only accepted one, but now they can communicate with multiple infected systems on the same network. Finally, the researchers indicate that it is very likely that, depending on the network characteristics of

the infected system, in later stages Bumblebee will deploy stealers or more complex post-exploitation tools such as CobaltStrike.

URL: https://research.checkpoint.com/2022/bumblebee-increasing-its-capacity-and-evolving-its-ttps/

Critical vulnerability in the PHP package repository Packagist

INTERNATIONAL

The Sonar team has published the discovery of a new critical vulnerability affecting Packagist, the official package repository used by Composer, the world's largest PHP package manager. The security flaw, listed as CVE-2022-24828, CVSS of 8.8, allows arbitrary commands to be executed on the server running the Packagist instance. An attacker could exploit this vulnerability to modify the information in existing PHP software packages, even changing the download path of the packages. This type of attack is known as a supply chain attack, one of the most effective techniques. According to the researchers, of the two billion component downloads that are performed with Composer per month, approximately 100 million of these require the metadata provided by Packagist. The vulnerability was fixed immediately in an update in Composer versions 1.10.26, 2.2.12 or 2.3.5

URL: https://blog.sonarsource.com/securing-developer-tools-a-new-supply-chain-attack-on-php/

ProxyNotShell: Bugs and fixes for Exchange vulnerabilities

INTERNATIONAL

The Microsoft team has made publications about the vulnerabilities in Microsoft Exchange Server, classified as CVE-2022-41040 and CVE-2022-41082 although no patches have yet been released to fix these flaws. Pending such patches, Microsoft published a script to apply mitigations based on URL rewriting that, as published by some researchers, could be bypassed. In response, Microsoft corrected these temporary mitigations whose conditions, however, have been called into question again after researcher Peter Hiele demonstrated that one of them, string filtering in URI identifiers, did not consider the character encoding, which made Microsoft's measures do not work. This discovery was confirmed by other researchers, which has led to Microsoft once again having to correct its mitigations. In addition, researcher Kevin Beaumont pointed out that Microsoft's vulnerability disclosures are focused on protecting on-premises servers, leaving out those in hybrid configurations. In the meantime, attempts to scan for systems vulnerable to the flaws, known as ProxyNotShell, have been detected from IPs identified as malicious. Finally, the first attempts to sell exploits for the vulnerabilities via the GitHub platform have begun to be recorded. However, these exploits are turning out to be fake, constituting scam attempts in exchange for high sums of money in cryptocurrencies without the code being used to exploit ProxyNotShell.

URL: https://www.bleepingcomputer.com/news/security/microsoft-updates-mitigation-for-proxynotshell-exchange-zero-days/

Newly published vulnerability in macOS

INTERNATIONAL

Apple software analysis firm Jamf has published details of an investigation by its researcher Ferdous Saljooki on a vulnerability affecting the macOS operating system. The flaw lies in the Archive Utility function, which could allow unauthorised and unsigned malicious applications to run, bypassing all the protections and warnings that Apple usually includes. This is because the Archive Utility does not add the Apple-designed quarantine tag to files when trying to unzip files with two or more folders or subfiles in their root directory. Quarantine tags are normally included by the system when trying to run software that is untrusted or does not give information about its developer and causes it to undergo scanning and the user has to manually authorise it to prevent the installation of unwanted programs. Attackers could execute malicious software without the victim's control due to the absence of these labels. The vulnerability has been given the identifier CVE-2022-32910 and, although it was patched by Apple in bulletins in May and July, it has only become known in the last few days.

URL: https://www.jamf.com/blog/jamf-threat-labs-macos-archive-utility-vulnerability/

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