Telefónica
Tech

04.11.2022

Cyber threats weekly briefing 2022

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

Vulnerabilities fixed in new OpenSSL version

INTERNATIONAL

The new 3.0.7 version of OpenSSL, announced last week by the developers of the project, was made public this past Wednesday.

The expectation around this version was high because, initially, it was going to patch a critical vulnerability in the software, the first of this severity since 2016. In the end, yesterday’s release includes fixes for two vulnerabilities considered to be of high importance, thus lowering the initial criticality announced.

The vulnerability that had raised the highest alert is CVE-2022-3602, a buffer overflow flaw in the certificate verification process that requires a certificate authority (CA) to have signed a malicious certificate or the application to continue the verification process without a valid path. While an attacker could trigger the flaw via a malicious email address, many platforms already incorporate protections to prevent such attacks.

The second vulnerability fixed, also with high criticality, CVE-2022-3786, is also a buffer overflow in the same process, but based on the length of the email address.

URL: https://www.openssl.org/news/secadv/20221101.txt

Emotet campaign returns after five months of inactivity

INTERNATIONAL

The research team Cryptolaemus, which specialises in the study of the Emotet malware, has announced on Twitter that the operators of the popular malware have returned to malicious actions after five months of inactivity. In particular, an Emotet infection campaign has been detected via email distributing malicious Excel files. To bypass Mark-of-the-Web (MoTW) protection, the mail instructs the potential victim to copy the Excel file to the Templates folder, which will allow it to be opened outside the protected mode and thus execute the macros that will download the malware onto the target computer. The Emotet malware is then downloaded as a DLL file into random folders created in the path %UserProfile%\AppData\Local. According to the available data, this reactivation campaign is reportedly having a global impact, distributing its malicious files in several languages.

URL: https://twitter.com/Cryptolaemus1/status/1587792659275448320

Use of Raspberry Robin in complex infection chains

INTERNATIONAL

Microsoft researchers have recently reported new discoveries concerning the Raspberry Robin malware. Based on their analysis, this malware is being marketed as a method to gain access to victims' systems to subsequently install other malware or carry out other post-exploitation activities. During the summer, Raspberry Robin has been used to install the FakeUpdate malware by malicious groups close to EvilCorp, and has even been observed in infection chains of the Lockbit ransomware. More recently, Raspberry Robin is reportedly being used to deploy other malware such as IcedID, Bumblebee, and Truebot. Likewise, Microsoft has observed its use by the FIN11/TA505 group, which is using it together with Truebot to deploy Cobalt Strike beacons and infect their victims with the Clop ransomware, thus allowing this group to abandon phishing as the initial vector of the chain of infection. It should be noted that, according to Microsoft, nearly 3,000 devices from 1,000 different organizations have been affected in some way by Raspberry Robin in the last month.

URL: https://www.microsoft.com/en-us/security/blog/2022/10/27/raspberry-robin-worm-part-of-larger-ecosystem-facilitating-pre-ransomware-activity/

Google fixes a 0-day vulnerability for Chrome

INTERNATIONAL

Google has released an update for Chrome that fixes a 0-day vulnerability that has a public exploit. The vulnerability, identified as CVE-2022-3723, was discovered by researchers at Avast and involves a type confusion issue in V8, the JavaScript engine in Chrome that would be triggered by receiving datasets marked both trusted and untrusted. Successful exploitation of the vulnerability would allow a remote attacker to manipulate data on the victim's system and escalate privileges. It is recommended to update the browser as soon as possible, to version 107.0.5304.87 on Mac and Linux and 107.0.5304.87/88 on Windows.

URL: https://www.malwarebytes.com/blog/news/2022/10/update-chrome-now-and-fix-a-vulnerability-with-an-existing-exploit-for-it

RomCom RAT launches campaign via KeePass and SolarWinds fakes

INTERNATIONAL

Researchers at BlackBerry Threat Research have discovered a RomCom RAT (Remote Access Trojan) campaign with new access vectors. According to the BlackBerry team, RomCom has cloned the official download pages of several widely used software products such as the network monitor SolarWinds, the password manager KeePass or the PDF file reader Reader Pro. RomCom has copied the original HTML to reproduce it on domains with typos that give the appearance of veracity to these malicious URLs. In fact, in the case of SolarWinds along with the infected file the user will be redirected to the official SolarWinds registration page to be contacted by legitimate customer support in order to avoid suspicion on the part of the victim. In the pieces of malware analysed, the file "setup.exe" has been observed executing the file "hlpr.dat", which contains the dropper that installs RomCom. This campaign is spread through phishing techniques, SEO poisoning and social engineering.

URL: https://blogs.blackberry.com/en/2022/11/romcom-spoofing-solarwinds-keepass

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.