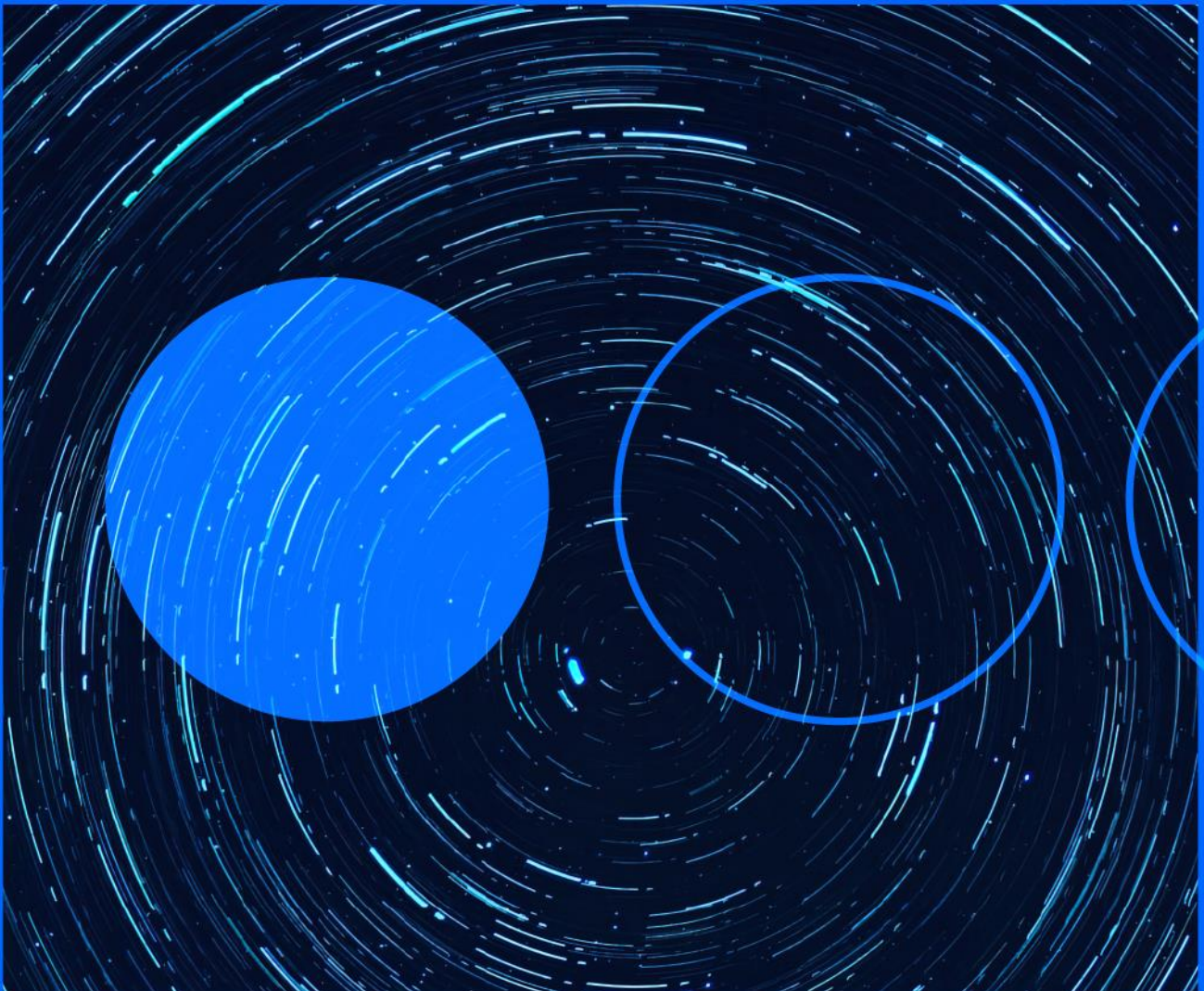







22.07.2022

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



Lightning Framework: new malware targeting Linux environments

INTERNATIONAL

Researchers at Intezer have published information about a new type of malware targeting Linux environments, which they have named Lightning Framework. While the researchers have not located a complete sample and some details of the malware are still unknown, some of its characteristics have been analysed. It is an advanced malware that installs itself on the victim's system via a downloader that will download all its modules and plugins. From there, the malware impersonates the GNOME password manager to connect to a polymorphic Command & Control server and download more components. Other features include the manipulation of timestamps and process IDs, the creation of a script with the name "elasticsearch" to create persistence and the implementation of a backdoor by creating its own SSH server. According to Bleeping Computer [1], Lightning Framework is the latest in a growing wave of malware variants attacking Linux systems, following recent detections of OrBit, Symbiote, BPFDoor and Syslogk.

[1] <https://www.bleepingcomputer.com/news/security/new-lightning-framework-linux-malware-installs-rootkits-backdoors/>

URL: <https://www.intezer.com/blog/research/lightning-framework-new-linux-threat/>



Cisco fixes multiple vulnerabilities

INTERNATIONAL

Cisco has released security patches to fix 45 vulnerabilities (three critical, one high and 41 medium) affecting various products. Three of the patched flaws, listed as CVE-2022-20857 CVSS 9.8 [1], CVE-2022-20858 CVSS 9.8 [2] and CVE-2022-20861 CVSS 9.8 [3], affected the Cisco Nexus Dashboard datacentre management solution and could allow an unauthenticated remote attacker to execute arbitrary commands and perform actions with root or administrator privileges. Another high-severity flaw, listed as CVE-2022-20860 CVSS 7.4 [4], is also highlighted in the SSL/TLS implementation of Cisco Nexus Dashboard that could allow an unauthenticated remote attacker to alter communications by intercepting traffic in man-in-the-

middle attacks. While these flaws are not known to be actively exploited, Cisco is urging users of affected devices to apply the patches as soon as possible.

[1] <https://nvd.nist.gov/vuln/detail/CVE-2022-20857>

[2] <https://nvd.nist.gov/vuln/detail/CVE-2022-20858>

[3] <https://nvd.nist.gov/vuln/detail/CVE-2022-20861>

[4] <https://nvd.nist.gov/vuln/detail/CVE-2022-20860>

URL: <https://tools.cisco.com/security/center/publicationListing.x?>



Luna: new ransomware targeting Windows, Linux and ESXi

INTERNATIONAL

Kaspersky security researchers have discovered a new ransomware family based on the Rust programming language, named Luna, on a ransomware forum on the dark web. This new ransomware appears to have the ability to encrypt devices running various operating systems, including Windows, Linux and ESXi systems. According to Kaspersky experts, at this stage Luna appears to be a simple ransomware in development and, for the time being, limited to command-line options only. However, its encryption scheme is unusual, combining the Diffie-Hellman elliptic curve X25519 secure key exchange, using Curve25519 with the Advanced Encryption Standard (AES) symmetric encryption algorithm. Furthermore, the trend of using a cross-platform language such as Rust denotes the trend of cybercriminal gangs developing ransomware capable of targeting multiple operating systems, without much effort and adaptation for each target. According to the research, there are no known data on possible victims of this ransomware family, as its operators have only recently been discovered and their activity is still being monitored.

URL: <https://securelist.com/luna-black-basta-ransomware/106950/>



Atlassian fixes critical flaw in encrypted Confluence credentials

INTERNATIONAL

Atlassian has released a security update that fixes a critical encrypted credential vulnerability in Confluence Server and Data Center that could allow unauthenticated remote attackers to log into vulnerable servers. The encrypted password is specifically added after installation of the Questions for Confluence application (versions 2.7.34, 2.7.35 and 3.0.2) for an account with the username disabledsystemuser, which is designed to assist administrators with the migration of application data to the Confluence cloud. The disabledsystemuser account is created with an encrypted password and is added to the confluence-users group, which allows viewing and editing all non-restricted pages within Confluence by default. Exploitation of this vulnerability, classified as CVE-2022-26138 [1], would therefore allow an attacker to log in and access any page to which the confluence-users group has access. So far, no active exploitation of this flaw has been observed, and Atlassian claims that this application, which helps improve internal communications, is reportedly installed on

more than 8,000 Confluence servers. To patch this bug, it is recommended to upgrade to the fixed versions (2.7.38 or higher to 3.0.5), or disable or delete the disabledsystemuser account, as uninstalling the Questions for Confluence application would not be enough.

[1] <https://www.cve.org/CVERecord?id=CVE-2022-26138>

URL: <https://confluence.atlassian.com/doc/questions-for-confluence-security-advisory-2022-07-20-1142446709.html>



CloudMensis: New malware targeting macOS

INTERNATIONAL

ESET researchers have discovered a new malware that is being used to implement backdoors and exfiltrate information on macOS devices. The malware was first detected in April 2022 by the ESET team and has been named CloudMensis. One of its most notable features is the use of cloud storage services such as DropBox, Yandex Disk or pCloud to communicate with its command and control (C2) servers. CloudMensis also manages to execute code on the target system and obtain administrator privileges to execute a second, more functional phase that collects information such as email attachments, screenshots, document exfiltration, keystrokes and other sensitive data. Similarly, it is currently unknown how it is distributed and what the infection vector is, as well as who the end targets of this malware would be and the threat actor to attribute this activity to.

URL: <https://www.eset.com/int/about/newsroom/press-releases/research/eset-research-discovers-new-threat-to-mac-users-cloudmensis-spies-on-them-in-targeted-operation/>

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



2022 © Telefónica Cybersecurity & Cloud Tech S.L.U. All rights reserved.

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.