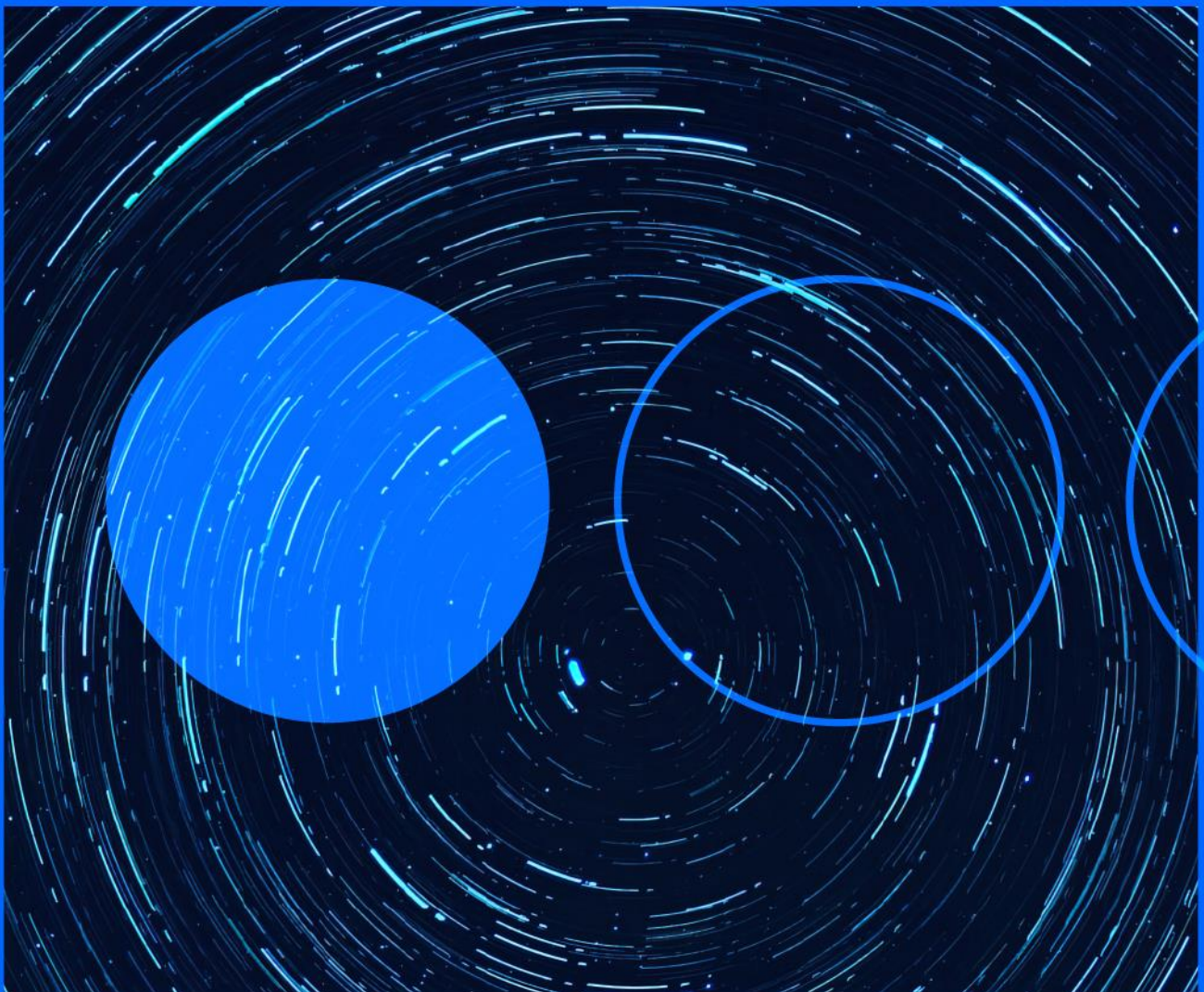







03.02.2023

Cyber threats weekly briefing 2023



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



LockBit Green: new LockBit variant

INTERNATIONAL

Researchers at vx-underground have recently detected that a new ransomware variant, called LockBit Green, is being used by the LockBit ransomware handlers. This new variant would be the third one used by the group, after its inception with Lockbit Red, and its subsequent evolution to LockBit Black (also called LockBit 3.0). Several [researchers](#) have analysed the available samples of LockBit Green and found that this new variant is based on Conti's source code. Based on their analysis, they note that the ransom note used is that of LockBit 3.0, and that the .lockbit extension is no longer used, but a random one, when encrypting files on the victim's system. The [PRODAFT](#) team has also shared Indicators of Compromise (IoCs) and a Yara rule for the new variant.

URL: <https://twitter.com/vxunderground/status/1618885718839001091>



GitHub revokes compromised Desktop and Atom certificates

INTERNATIONAL

Github has taken the decision to revoke a number of certificates used for its Desktop and Atom applications after they were compromised in a security incident in December. According to the company itself, the unauthorised access in December did not affect the platform's services, however, a group of certificates were exfiltrated as a result. These certificates are password-protected, and so far, no malicious use of them has been detected. The removal of these certificates will invalidate GitHub Desktop for Mac versions 3.0.2 to 3.1.2 and Atom versions 1.63.0 to 1.63.1. Users of these versions are advised to upgrade to the latest version in the case of Desktop and revert to earlier versions in the case of Atom. The changes will take effect on 2 February.

URL: <https://github.blog/2023-01-30-action-needed-for-github-desktop-and-atom-users/>



PoC available for KeePass vulnerability

INTERNATIONAL

KeePass has recently discovered a vulnerability in its software for which a PoC has already been released. The flaw, identified as [CVE-2023-24055](#), allows threat actors with write access to a system to alter the XML configuration file and inject malware to export the database with users and passwords in plain text. When a user accesses KeePass and enters the master password to open the database, the export rule is triggered in the background and the content is saved in a file that is accessible to attackers. While [KeePass described the issue in 2019](#) without describing it as a vulnerability, users are requesting that the product include a [confirmation message](#) before exporting or being able to [disable the feature](#). Bleeping Computer recommends ensuring that unprivileged users do not have access to any application files and creating a [configuration file](#).

URL: <https://www.bleepingcomputer.com/news/security/keepass-disputes-vulnerability-allowing-stealthy-password-theft/>



Two new vulnerabilities in CISCO devices

INTERNATIONAL

Researchers at Trellix have warned of two vulnerabilities in Cisco devices. The first, identified as CVE-2023-20076 and with a [manufacturer's](#) CVSS of 7.2, would allow an unauthenticated attacker to remotely inject commands into various devices. The second bug, so far identified with Cisco bug ID CSCwc67015, would allow an attacker to remotely execute code and overwrite existing files. While both bugs were originally identified in Cisco ISR 4431 routers, they would affect other devices as well: 800 Series Industrial ISRs, CGR1000 Compute Modules, IC3000 Industrial Compute Gateways, IOS-XE-based devices configured with IOx; IR510 WPAN Industrial routers and Cisco Catalyst Access points (COS-APs). Cisco has reportedly released security updates for the first vulnerability mentioned, and researchers urge affected organisations to upgrade to the latest firmware version available, and to disable the IOx framework if it is not needed.

URL: <https://www.trellix.com/en-us/about/newsroom/stories/research/when-pwning-cisco-persistence-is-key-when-pwning-supply-chain-cisco-is-key.html>



Lazarus campaign against energy and healthcare companies

INTERNATIONAL

WithSecure has published extensive research on the latest campaign by the APT Lazarus, allegedly backed by North Korea. The campaign has been named "No Pineapple!" and in it the group has managed to steal 100GB of data from medical research, engineering and energy companies, among others. According to WithSecure, Lazarus exploited vulnerabilities [CVE-2022-27925](#) and [CVE-2022-37042](#) in Zimbra to place a webshell on the victims' mail server. Once inside the system they used various tools such as the Dtrack backdoor and a new version of the GREASE malware, which abuses the PrintNightmare vulnerability. WithSecure was able to attribute the campaign to Lazarus, in addition to repeating TTPs associated with the group, because it discovered that the webshells communicated with an IP located in North Korea.

URL: <https://labs.withsecure.com/content/dam/labs/docs/WithSecure-Lazarus-No-Pineapple-Threat-Intelligence-Report-2023.pdf>

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.