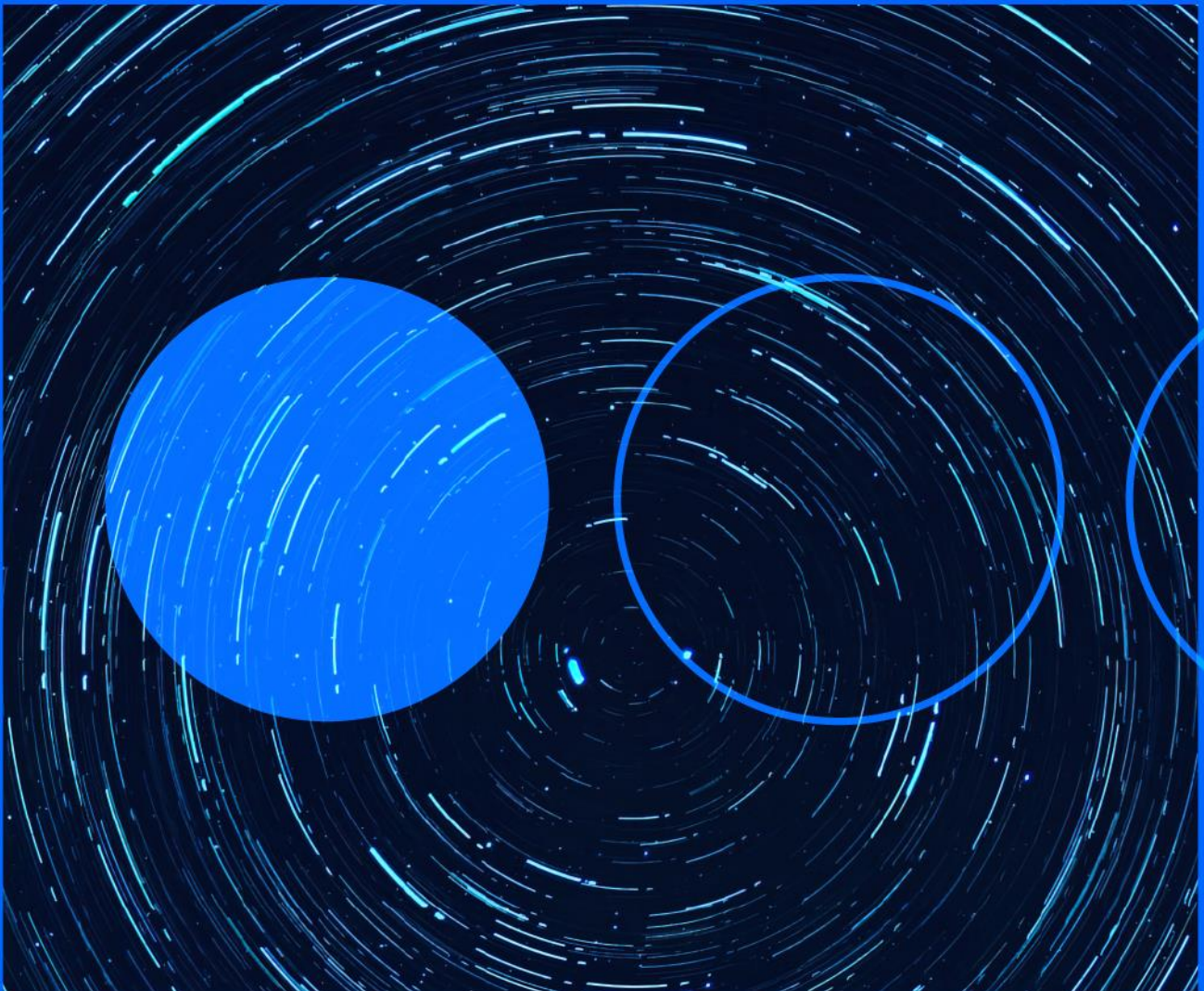







10.03.2023

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

FBI and ICISA Launch Advisory to Combat Royal Ransomware

INTERNATIONAL

The FBI and ICISA launched the [#StopRansomware: Royal Ransomware](#) Cyber Security Advisory on 2 March to help combat this type of ransomware by disseminating TTPs and IOCs. Many companies in different [critical infrastructure sectors](#) such as industry, telecommunications, healthcare, education, among others, have been breached with this ransomware variant since September 2022. The FBI and CISA believe that Royal uses its own file encryption software, disabling antivirus when gaining access to a system and leaking data before finally deploying the ransomware. They then demand ransoms of between one and eleven million dollars in Bitcoin and in the note they leave victims a .onion site for contact. Organisations are advised to implement the recommendations and mitigations in the advisory to prevent these attacks.

URL: <https://patchstack.com/articles/psa-houzez-theme-unauthenticated-privilege-escalation-vulnerability-exploited-in-the-wild/>

Hiatus: worldwide campaign against business routers

INTERNATIONAL

The Lumen Black Lotus Labs team has identified an active campaign targeting business routers. The campaign, which has been named "Hiatus", has been active since July 2022, targeting end-of-life DrayTek Vigor 2960 and 3900 routers with an i386 architecture. The entry vector is currently unknown, but once the router has been compromised, the threat actors implement a bash script that downloads and executes two malicious binaries: HiatusRAT and a variant of tcpdump for capturing packets. According to the researchers, at least 100 victims have been detected and have become part of the botnet of the malicious actors, mostly located in Europe, North America and South America. Lumen Black Lotus Labs estimates that the threat actors kept the campaign at low infection levels in order to evade detection by not attracting as much attention.

URL: <https://blog.lumen.com/new-hiatusrat-router-malware-covertly-spies-on-victims/>



SYS01stealer: new infostealer targeting critical infrastructures

INTERNATIONAL

The research team at Morphisec has published a report on a new infostealer targeting critical government infrastructures which they have named SYS01stealer. The malicious actors behind this threat specifically try to target corporate Facebook accounts by using Google ads and fake Facebook profiles that provide download links promoting games, adult content, software, but are actually malicious. It is worth noting that once the victim downloads the .zip file, and it is executed, the file will proceed to perform a DLL sideload inside the victim's system. Experts point out that SYS01stealer's goal is to steal browser cookies and exploit authenticated Facebook sessions to exfiltrate information from the victim's Facebook account. The malware can also upload files from the infected system to the Command & Control server and execute commands sent by it.

URL: <https://blog.morphisec.com/sys01stealer-facebook-info-stealer>



PoC of polymorphic malware using Artificial Intelligence

INTERNATIONAL

Researchers at Hyas have built a proof-of-concept for polymorphic malware generation using an Artificial Intelligence language model. The software created, which they have named BlackMamba, is a polymorphic keylogger with the ability to modify its code during execution, and without the use of Command & Control (C2) infrastructures. BlackMamba uses a benign executable to communicate with the OpenAI API during execution, which provides it with the malicious code necessary to collect the user's keystrokes. Whenever the malware executes, this capability is re-synthesised, allowing it to evade security solutions. According to the researchers, their analysis with a well-known EDR solution yielded no detection of the malware. The exfiltration of the data collected by the malware in this test is done via Microsoft Teams, which it accesses with the stolen credentials.

URL: <https://www.hyas.com/blog/blackmamba-using-ai-to-generate-polymorphic-malware>

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.