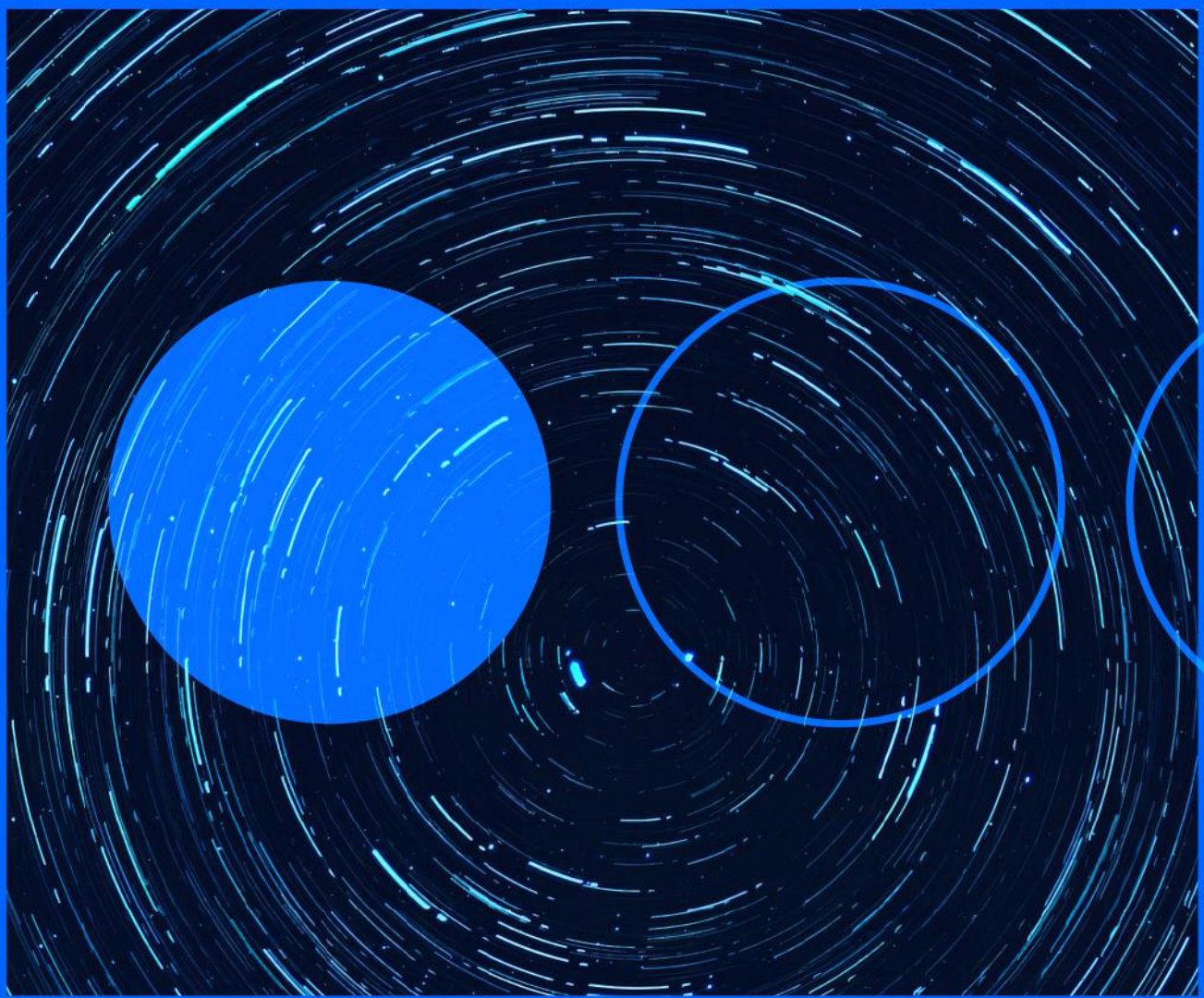
Telefónica Tech

24.03.2023

Cyber threats weekly briefing 2023



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

HinataBot: new botnet dedicated to DDoS attacks

INTERNATIONAL

Researchers at Akamai have published a report stating that they have identified a new botnet called HinataBot that has the capability to perform DDoS attacks of more than 3.3TB/s. Experts have indicated that the malware was discovered in mid-January, while being distributed on the company's HTTP and SSH honeypots. HinataBot uses exfiltrated user credentials to infect its victims and exploits old vulnerabilities in Realtek SDK devices, CVE-2014-8361, Huawei HG532 routers, CVE-2017-17215, and/or exposed Hadoop YARN servers. Once the devices are infected, the malware executes and waits for the Command & Control server to send the commands. Akamai warns that HinataBot is still under development and that it could implement more exploits, and thus expand its entry vector to more victims and increase its capabilities to carry out attacks with a greater impact.

URL: https://www.akamai.com/blog/security-research/hinatabot-uncovering-new-golang-ddos-botnet

CISA issues eight security advisories on industrial control systems

INTERNATIONAL

CISA has recently issued a total of eight security advisories warning of critical vulnerabilities in industrial control systems. These new vulnerabilities affect several products from different companies such as Siemens, Rockwell Automation, Delta Electronics, VISAM, Hitachi Energy y Keysight Technologies. The most significant of these vulnerabilities are those affecting the Siemens brand, of which three warnings have been collected affecting its SCALANCE W-700 assets, RADIUS client of SIPROTEC 5 devices and the RUGGEDCOM APE1808 product family, with a total of 25 vulnerabilities with CVSSv3 scores ranging from 4.1 to 8.2. As a

result, due to their impact, the warnings for Rockwell Automation's ThinManager ThinServer equipment stand out, with one of its three bugs having a CVSSv3 of 9.8, as does the InfraSuite Device Master asset from Delta Electronics, for which a total of 13 vulnerabilities have been reported.

URL: https://www.cisa.gov/news-events/alerts/2023/03/21/cisa-releases-eight-industrial-control-systems-advisories

Mispadu: banking trojan targeting Latin America

INTERNATIONAL

Researchers at Metabase Q Team have published a report on an ongoing campaign targeting banking users in Latin American countries using the Mispadu trojan. According to Metabase Q Team, the trojan has been spread through phishing emails loaded with fake invoices in HTML or PDF format with passwords. Another strategy involves compromising legitimate websites looking for vulnerable versions of WordPress to turn them into its C2 server and spread malware from there. According to the research, the campaign started in August 2022 and remains active, affecting banking users mainly in Chile, Mexico and Peru. In November 2019, ESET first documented the existence of Mispadu (also known as URSA), a malware capable of stealing money and credentials, as well as acting as a backdoor, taking screenshots and logging keystrokes.

URL: https://www.metabaseq.com/mispadu-banking-trojan/

Critical vulnerability in WooCommerce Payments fixed

INTERNATIONAL

Researcher Michael Mazzolini of GoldNetwork reported a vulnerability in WooCommerce Payments this week, which has resulted in a security update being forced to be installed. The vulnerability does not yet have a CVE identifier, although it has been assigned a CVSSv3 criticality of 9.8, being a privilege escalation and authentication bypass vulnerability, which could allow an unauthenticated attacker to impersonate an administrator and take control of the online retailer's website. It should be noted that no active exploitation has been detected so far, although Patchstack has warned that since no authentication is required for exploitation, it is likely to be detected in the near future. The affected versions range from 4.8.0 to 5.6.1, and the vulnerability has been fixed in version 5.6.2.

URL: https://developer.woocommerce.com/2023/03/23/critical-vulnerability-detected-in-woocommerce-payments-what-you-need-to-know/

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