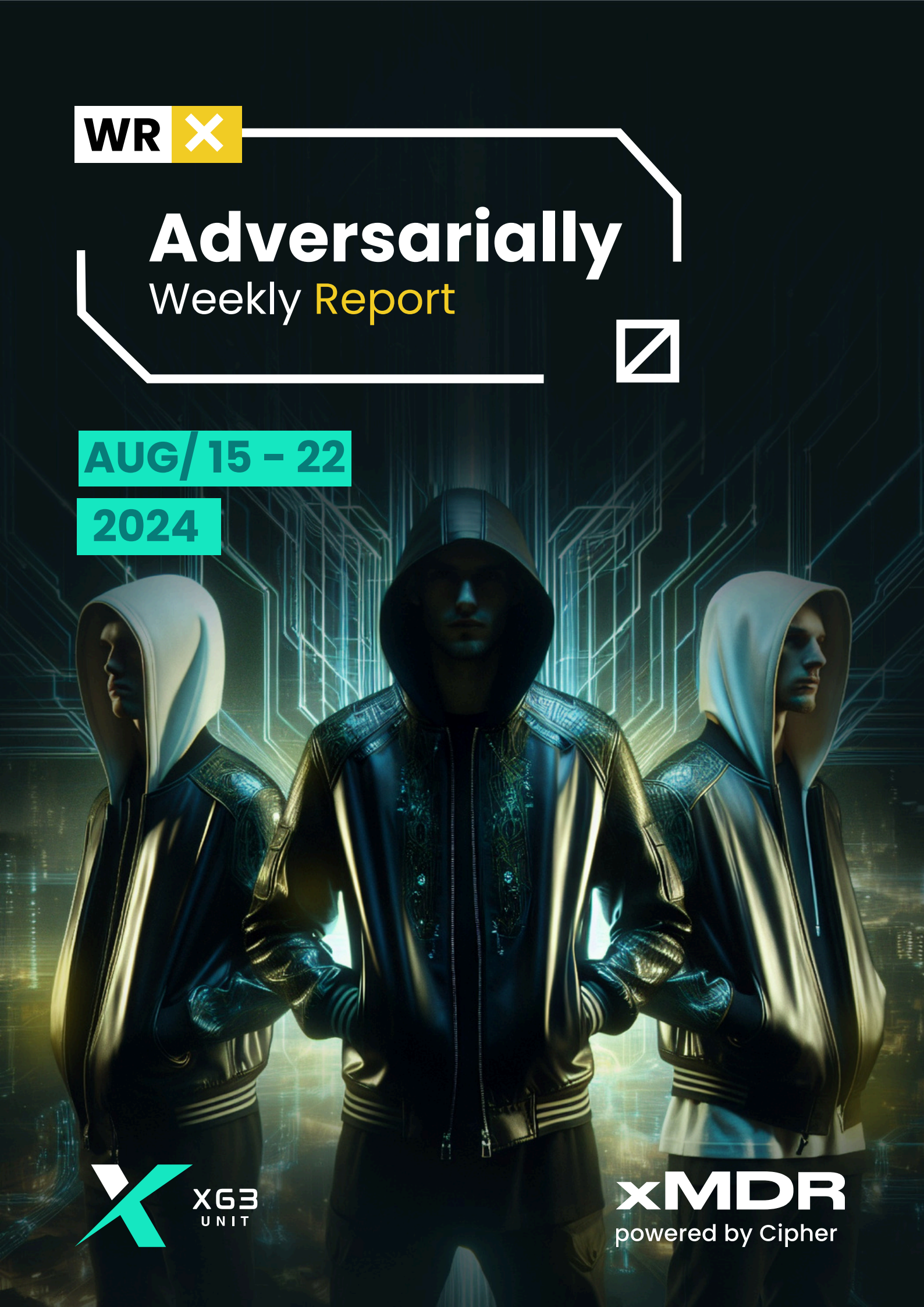
WR X

Adversarially

Weekly Report

AUG/ 15 - 22

2024



XG3 UNIT

xMDR

powered by Cipher

ADVERSARIALLY
weekly report
Aug 15 - 22, 2024

XG3 UNIT

Adversary of the Week

Hazelnut Cosmos Taurus

Type: Individual

Countries:

Maturity:

Sectors: Finance

Activity: Cybercrime

TTPs: Exploit Public-Fancing Application

Chive Cosmos Taurus

Type: Individual

Countries:

Maturity:

Sectors: Education

Activity: Cybercrime

TTPs: Exploit Public-Fancing Application

Ransomhub

Type: Group

Countries:

Maturity:

Sectors: All

Activity: RaaS

TTPs: 35

ADVERSARIALLY
weekly report
Aug 15 - 22, 2024

XG3 UNIT

Global

- The hacktivist group **HackNet** has carried out several DDoS attacks on the website of the **Kiev City Blood Centre**. This kind of attacks are quite dangerous as paralysing such centres can have serious health consequences.

- A **phishing campaign** carried out by **TA453** has been detected, in which they attempt to lure the target into interacting with a benign email to generate conversation and trust and then click on a malicious follow-up link. This campaign is **distributing** a malware **toolkit** called **BlackSmith**, which in turn distributes a **trojan** called **AnvilEcho**.

- **D4RK S!DEZ** group has allegedly launched cyber attacks against **Ufone**, a reputed Pakistani Internet provider. The group claims that nearly **200k IPs were affected** and several domains suffered from the attack.

- Cybersecurity researchers have detected a **large-scale campaign** that managed to attack and extort money from several organisations using cloud systems. The attackers created a clever tactic to **exploit environment variable (.env) files** exposed on cloud infrastructures. These files contained sensitive data such as access codes to different software and services, allowing the attackers to gain unauthorised access to the victims' systems, through which they further infiltrated the networks.

- The Ukrainian Computer Emergency Response Team (CERT-UA) has detected a series of **malicious email attacks** that could originate **from UAC-0020**, a threat actor group linked to the Luhansk People's Republic. These emails include a link that redirects to the download of a malicious file that **installs** components of the **Spectr** software.

- A rather unusual **backdoor** called **Msupedge** has been detected in an attack targeting a university in Taiwan. This backdoor has one notable feature and that is that it **communicates with a command and control (C&C) server via DNS traffic.** The intrusion at the university could apparently have been due to the exploitation of vulnerability CVE-2024-4577.

- **National Public Data** claims to have suffered a **data breach** and suggests that the **leaked information** could contain private data such as name, email address, phone number, social security number and postal addresses. It was discovered that there were **134 million unique email** addresses in one version of the leaked database.

ADVERSARIALLY
weekly report
Aug 15 - 22, 2024

Spain & Latam

- **Chive Cosmos Taurus** has allegedly sold through the Breach forum a Fortinet access for a Spanish company in the education sector with a revenue of $40M. The sale was made for $200.

- **Slategray Cosmos Taurus** sells on Breachforum a database with 27.6 million WhatsApp users' mobile numbers with their name on their WhatsApp account.

- **Tuftsblue Cosmos Taurus** sells on Breachforum a database of a Spanish telephone company with information on 29,000 customers. The leaked information contains private data such as names, surnames, ID number, address, bank account number and others. The selling price is 5000$.

- **Hazelnut Cosmos Taurus** offers on Breachforum a database of the Spanish company Avatrade, a financial broker that deals with foreign exchange from all over the world. The database reportedly contains more than 313k lines of private customer information.

- **Ticklemepink Cosmos Taurus** sells 7,200 credit cards from various South American countries such as Argentina, Brazil and Uruguay on Exploit. The sale is in bidding format starting at $25,000.

- **Lightseagreen Cosmos Taurus** claims on a dark web forum to have compromised the website of the police station of Adepoldo, Brazil.

ADVERSARIALLY
weekly report
Aug 15 - 22, 2024

XG3 UNIT

Vulnerabilities & Exploits

- **CVE-2024-38193** is a Bring Your Own Vulnerable Driver (BYOVD) flaw, which serves as a kernel entry point for the Winsock API. It is currently **being exploited by Lazarus.** With successful exploitation, attackers can **gain system-level privileges**, including the highest privilege on the Windows system, known as SYSTEM access, allowing them to execute untrusted code.

- A critical security flaw **(CVE-2024-5932)** in the popular **GiveWP WordPress plugin** has left over **100,000 websites vulnerable** to remote code execution and unauthorized **delete critical files from the server.** The vulnerability in question is a PHP Object Injection (POI) flaw that can be triggered through the deserialization of untrusted input, specifically via the 'give_title' parameter in the GiveWP plugin.

- The vulnerability, identified as **CVE-2024-28000,** has a CVSS **score of 9.8** found in the **LiteSpeed Cache plugin** for WordPress has been actively exploited, with over 30,000 attack attempts blocked in just the last 24 hours. This is a critical **privilege escalation vulnerability**, and allows attackers to spoof their user ID and log in as an administrator, giving them full control over the affected WordPress site. With administrative access, attackers can upload malicious plugins, modify site content, steal data and further compromise site security.

- **SolarWinds** has issued an urgent security advisory for its Web Help Desk (WHD) software, warning of a **critical hardcoded credential vulnerability** listed as **CVE-2024-28987**. The flaw allows **unauthorized remote access** to critical internal functions, enabling attackers to potentially disrupt operations, steal sensitive data, or escalate their attacks within the targeted network.

ADVERSARIALLY
weekly report
Aug 15 - 22, 2024

XG3 UNIT

⚠️ Warning of the week

- A BYOVD flaw exploited by Lazarus could give attackers SYSTEM access on Windows. Time to update and patch before Lazarus takes your system for a joyride. Remember, SYSTEM access should be reserved for you, not for a sneaky BYOVD exploit.

- The GiveWP plugin has developed a giving spirit—but not in a good way. Over 100,000 WordPress sites are exposed to remote code execution. Patch that PHP Object Injection flaw before your generous site ends up donating admin control to attackers!🌐⚠️

- LiteSpeed Cache has a heavy problem—a privilege escalation flaw with over 30,000 attack attempts blocked in 24 hours. Patch up fast or risk giving attackers full admin control. Don't let them turn your WordPress site into their personal playground. 📄🔓

- SolarWinds' WHD has hardcoded credential issues that make unauthorized remote access a breeze. Patch now before attackers disrupt your operations or steal sensitive data. A help desk should solve problems—not invite them.🛡️🔍

ADVERSARIALLY
weekly report
Aug 15 - 22, 2024

XG3 UNIT

Ransomware

Total Victims = 114 (-8)

- Spain - **0** (-2)
- Latam - **3** (-2)
- WorldWide - **111** (-4)

The king is...

Data of the week

Top Countries

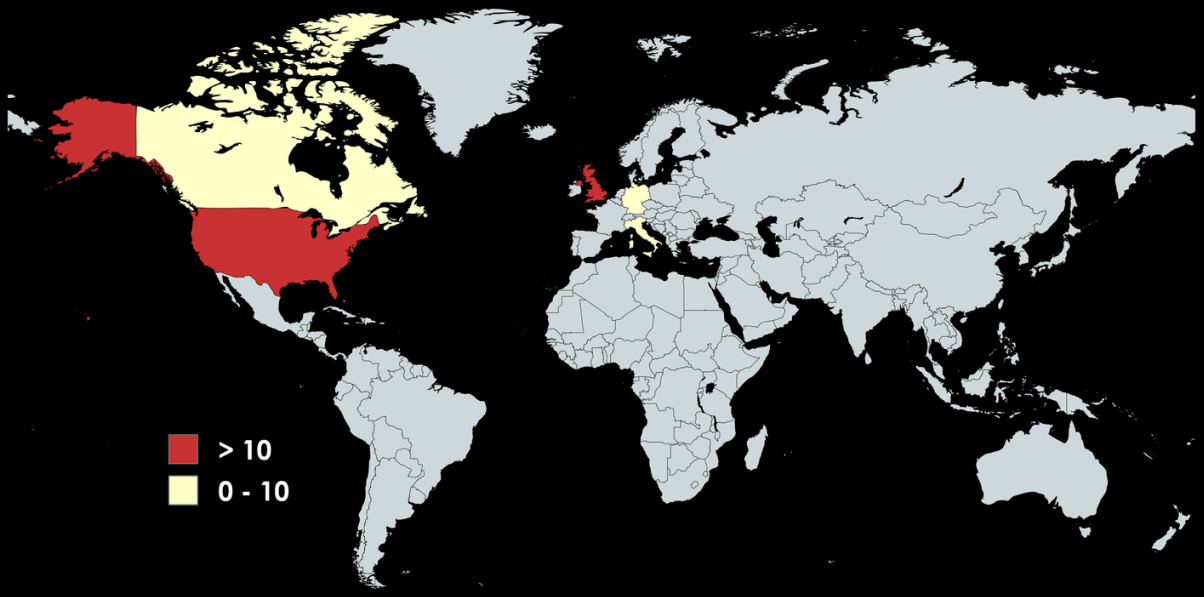
- USA - **43** (-14)
- GBR - **14** (+9)
- ITA - **7** (+4)
- DEU - **3**
- CAN - **3**

Top Sectors

- Manufacturing - **20** (-1)
- Technology - **14** (-3)
- Finance - **10** ☆
- Healthcare - **10** (-2)
- Engineering - **8** ☆

Top Groups

- Ransomhub - **26** (-1)
- Helldown - **8** (-2)
- Play - **7** (-2)
- Qilin - **7** ☆
- Cloak - **5** ☆



Victims

- **Ransom Victim:** imobesidade.com.br | Group: ransomhub | Sector: Healthcare | Country: Brazil
- **Ransom Victim:** Prefeitura do Jaboatão dos Guararapes | Group: qilin | Sector: Government Administration | Country: Brazil
- **Ransom Victim:** tiendasmacuto.com | Group: BrainCipher | Sector: Commerce | Country: Venezuela

ADVERSARIALLY
weekly report
Aug 15 - 22, 2024

XG3 UNIT

Top MITRE TTP covered:

- Command & Scripting
- Phishing for Information
- User Execution
- OS Credential Dumping
- Impair Defenses

Data added to Digital Adversary in the last week

TTP'S 27

Top Most Relevant

- Command and Scripting Interpreter
- System Information Discovery
- Financial Theft

Threat Actors 8

Top Most Relevant

- Palegoldenrod Cosmos Taurus
- LigthSalmon Cosmos Taurus
- Gold Cosmos Taurus

xMDR

ADVERSARIALLY

weekly report

Aug 15 - 22, 2024

xMDR
powered by Cipher