

WR



Adversarially

Weekly Report



SEP 5 - 12

2024



xMDR
powered by Cipher

Adversary of the Week



Dimgrey Cosmos Taurus

Type: Individual

Countries:  


Maturity: 

Sectors: E-commerce

Activity: Cybercrime

TTPs: Exploit Public-Fancing Application



BlindEagle aka APT-C-36

Type: APT

Countries:  

Maturity: 

Sectors: Insurance

Activity: Cybercrime

TTPs: 23



RansomHub

Type: Group

Countries: 

Maturity: 

Sectors: All

Activity: RaaS

TTPs: 35



Global

- **GigtoGig**, a UK employment agency, **discovered a misconfigured Amazon AWS S3 bucket** belonging to GigtoGig. The breach **contained** more than **100,000 workers' passports, over 17,000 work permits**, as well as visas and resumes. With this information, all workers are at **risk of** being impersonated, **phishing** attacks, **scams**, etc.
- More than **35,000 of Macron's emails** have been **leaked** by **Russian state agents**. This leak was published just before the French elections.
- **Mediumvioletred Cosmos Taurus**, a member of the **CyberNiggers** group, sells on BreachForum several databases with a total of **20 gigabytes** of source code, private keys, credentials, API keys, projects, employee data, threat reports, T-Mobile virtual machine logs, documents and much more from **cybersecurity consulting** firm **CapGemini**.
- **Deutsche Flugsicherung**, Germany's state-owned air traffic control company, has been the **victim of a cyber attack**. The incident **affected** the company's administrative IT **infrastructure**, but air **traffic control** operations were **not affected**.
- **Avis**, a US **airport car rental company**, has **suffered** a major **cyber-attack**. More than **400,000 customers** have had their **personal information compromised**, including full names, dates of birth, emails, phone numbers, credit card details and driving licence numbers. The most affected customers have been in the state of Texas.



Spain & Latam

- The **APT group BlindEagle** has increased its **attacks** on the **insurance** sector in **Colombia**, using **BlotchyQuasar**, a variant of QuasarRAT. Through phishing emails **masquerading as DIAN**, it **steals** critical **financial information**, as well as logging keystrokes and monitoring banking services.
- New **phishing campaigns** using known **banking trojans** such as **Mekotio**, **BBTok** and **Grandoreiro** are targeting **Latin American** countries with new scams. They mainly target sectors such as **manufacturing, retail and financial services** and impersonate official business communications or law enforcement agencies.
- **Dimgrey Cosmos Taurus X** offers a database of the e-commerce company Temu with confidential customer information from many countries including Brazil, Mexico, Chile, Colombia, Peru and Uruguay.
- **Medusa** has **attacked** the **Cortefiel** group in Spain. It has breached more than **700GB of information**, including data on more than 3,000 employees.
- The **City Council of San Lorenzo del Escorial** has been the **victim** of a cyber-attack and **450GB of confidential information** has been leaked and is on **sale for \$45,000**.
- The **Pontifical University of Salamanca** has suffered a **cyber-attack**. Among the **personal data** that could have been affected are name and surname, email, telephone number, degree, employment status, although there is **currently no record of the exfiltration of data** or the publication of the attack on the dark web.
- **Lookiero**, an online personal shopping service has experienced a **security breach**, reportedly resulting in the **personal information** of almost **5 million users being breached**. The database is contained in a **4.11 GB** downloadable .csv file, containing **sensitive information** such as usernames, encrypted passwords, physical addresses and payment-related data such as credit card details and Facebook access tokens.



Vulnerabilities & Exploits

- **CVE-2024-40766**: A recently patched vulnerability is being **actively exploited**. The flaw, which originally reportedly only affected SonicOS admin access, has been confirmed to **affect** the **SSLVPN feature of the firewall** as well. Cybersecurity researchers have detected that affiliates of the **Akira ransomware** are **exploiting** this vulnerability **to compromise SSLVPN user accounts on SonicWall appliances**.
- Two serious vulnerabilities, identified as **CVE-2024-37288** and **CVE-2024-37285**, are **affecting** the popular open source data visualisation and analysis platform **Kibana**. Attackers can exploit the **first vulnerability with a CVSS of 9.9** by creating malicious YAML payloads, leading to **remote code execution**. The **second with a CVSS of 9.1**, allows attackers to **execute arbitrary code** if they possess specific Elasticsearch index privileges and Kibana privileges.
- **HAProxy** disclosed that vulnerability **CVE-2024-45506** affecting its load balancing and proxy software is being **actively exploited**. It is a vulnerability with CVSS **7.5** and under certain conditions, it can **cause an endless loop**, leading to a system crash and a **remote denial of service (DoS) attack**.
- A series of critical vulnerabilities have been uncovered in **Veeam Backup & Replication**, potentially exposing organizations to unauthorized access, remote code execution, and data breaches. The **most severe** vulnerability (**CVE-2024-40711, CVSS 9.8**) allows unauthenticated attackers to **execute code remotely**, granting them full control over the affected system. **Others vulnerabilities impact** various aspects of Veeam Backup & Replication, including **Multi-Factor Authentication (MFA) bypass**, sensitive information disclosure and **Local Privilege Escalation (LPE)**.
- **Siemens**, a global industrial automation giant, has disclosed a **critical heap-based buffer overflow vulnerability** in its User Management Component (UMC). The vulnerability, identified as **CVE-2024-33698** and assigned a CVSS score of **9.3**, could allow an **unauthenticated remote attacker to execute arbitrary code** on affected systems, potentially leading to severe consequences.
- **Windows** has disclosed **2 zero-day** vulnerabilities, **CVE-2024-38226 and CVE-2024-38217**, which are being **actively exploited**. These allow attackers to **bypass essential security protections** in Windows, such as the Office macro and Mark of the Web (MoTW).

Warning of the week

- **Akira** ransomware is slipping through SonicWall's SSLVPN like it's an open door. Patch up this vulnerability fast or risk handing your credentials to ransomware affiliates. Your VPN should protect you, not invite cybercriminals over for tea.
- **Kibana's** visualizations are stunning—until attackers exploit these critical flaws to execute remote code. Patch your system before they turn your data dashboards into their own playground. Because no one likes a hacker creating art with your system.
- **HAProxy** may be great at balancing traffic, but this flaw could lead to an endless loop of denial. Patch quickly, or you'll find yourself stuck in a system-crashing loop. Avoid the infinite frustration—no one wants a traffic jam on their network.
- Backup plans are great—until someone exploits a Veeam flaw and takes control. Patch this remote code execution vulnerability before attackers restore themselves into your systems. Keep your backups safe and out of hacker hands, especially with MFA bypasses lurking.
- **Siemens'** User Management Component has a heap overflow issue, allowing attackers to execute code remotely. Patch now or risk an industrial-sized problem. No one wants their automation systems hijacked—especially not by someone else managing user access.
- **Windows' latest zero-days** are bypassing macros and MoTW protections like it's 1999. Keep your systems updated before attackers exploit these flaws and make themselves at home in your documents. Patch fast, because you don't want hackers marking your files!

ADVERSARIALLY

weekly report

Sep 5 - 12, 2024



Ransomware

Total Victims = **104** (-38)

- Spain - **2** (+1)
- Latam - **2** (-2)
- WorldWide - **100** (-37)

The king is...



Data of the week

Top Countries

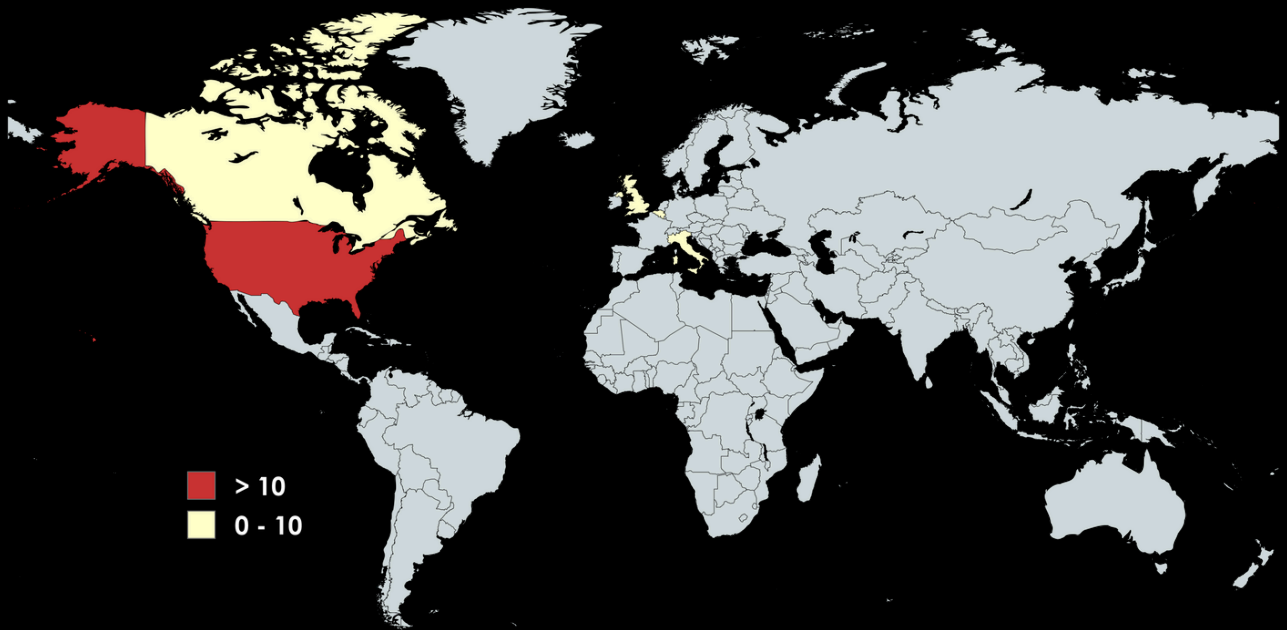
- USA - **42** (-23)
- GBR - **7** (+1)
- CAN - **6** (-7)
- BEL - **6** ☆
- ITA - **3** ☆

Top Sectors

- Manufacturing - **21** (-9)
- Technology - **14** (+3)
- Education - **9** ☆
- Finance - **9** (-1)
- Healthcare - **7** ☆

Top Groups






- Ransomhub - **22** (-10)
- Bianlian - **8** ☆
- Play - **8** (-3)
- Qilin - **8** ☆
- Cicada3301 - **8** ☆



Victims

- Ransom Victim:** rhp.com.br | Group: lockbit3 | Sector: Healthcare | Country: Brazil
- Ransom Victim:** Imetame | Group: akira | Sector: Energy | Country: Brazil
- Ransom Victim:** Grupo Cortefiel | Group: medusa | Sector: Commerce | Country: Spain
- Ransom Victim:** inorde.com | Group: ransomhub | Sector: Technology | Country: Spain

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 **90**

Top Most Relevant

- Command and Scripting Interpreter
- Data Encrypted for Impact
- Ingress Tool Transfer



Threat Actors **2**

Top Most Relevant

- RansomHub
- Cicada3301



Tools **1**

Top Most Relevant

- FudModule

xMDR

ADVERSARIALLY
weekly report
Sep 5 - 12, 2024

xMDR
powered by Cipher

LEGAL NOTICE: PROHIBITION OF DISTRIBUTION, USE OR SHARING WITHOUT AUTHORIZATION This document (hereinafter, "the Document") is the exclusive property of Prosegur Ciberseguridad S.L. (hereinafter, "the Owner"). The Owner possesses all intellectual property rights associated with the Document, including, among others, copyright and property rights. Access to this Document is granted only to parties authorized by the Owner for the specific purpose of confidential evaluation.

Any distribution, reproduction, unauthorized use, disclosure or sharing of the Document, in whole or in part, with third parties without the prior and express written authorization of the Owner is strictly prohibited. Any unauthorized use of the Document will constitute a violation of the Owner's intellectual property rights and may result in legal action. Access and use of this Document are subject to the terms and conditions established by the Owner. Any authorized party that receives the Document must comply with the restrictions and obligations established by the Owner.

Any questions or requests for authorization for distribution, reproduction or use of the Document should be directed to the Owner.

Failure to comply with these restrictions may have legal consequences. By accessing or using the Document, you accept and acknowledge the terms of this legal notice.