WR X

Adversarially

Weekly Report

SEP 26 - 3 OCT

2024

XG3 UNIT

xMDR
powered by Cipher

ADVERSARIALLY

weekly report

Sep 26 - 3 Oct, 2024

XG3 UNIT

Adversary of the Week

Orangepeel Cosmos Taurus

Type: Individual

Countries: 🇵🇪

Maturity: 🟩⬛⬛

Sectors: Sport

Activity: Cybercrime

TTPs: Exploit Public-Fancing Application

Kimsuky

Type: Group

Countries: 🌍

Maturity: 🟧🟧⬛

Sectors: Government, Defense, Energy

Activity: Cybercrime

TTPs: 55

RansomHub

Type: Group

Countries: 🌍

Maturity: 🟥🟥🟥

Sectors: All

Activity: RaaS

TTPs: 30

ADVERSARIALLY

weekly report

Sep 26 - 3 Oct, 2024

Global

- Authorities have identified **Aleksandr Viktorovich Ryzhenkov,** a key **member** of the **Evil Corp** group and an **affiliate** of the **LockBit** ransomware. Ryzhenkov, also known as 'Beverley', has been linked to more than 60 LockBit ransomware exploits and is accused of attempting to extort $100 million from victims. This expose came about through **Operation Cronos,** a joint law enforcement effort.

- **Z-Pentest** group has claimed responsibility for a **cyberattack** on a **water treatment plant** in Arkansas City, USA. The threat actors allegedly forced the plant's hydraulic systems into manual control, causing operational disruptions and highlighting vulnerabilities in critical infrastructure.

- The North Korean APT group, **Sparkling Pisces aka Kimsuky**, has been linked to new malware tools, **KLogEXE** and **FPSpy**, as uncovered by cybersecurity researchers. KLogEXE is a **stealth keylogger**, while FPSpy is an **advanced backdoor** capable of executing commands and data theft, underscoring Kimsuky's evolving cyber espionage capabilities.

- A **new variant** of the **Octo banking malware**, called **Octo2**, has been identified by cybersecurity researchers. Targeting **European banks** in countries like Italy and Poland, Octo2 enhances remote access and anti-detection capabilities, enabling full device takeovers and fraudulent transactions. Its sophisticated obfuscation techniques make it a serious threat to mobile banking users.

- **Storm-0501** is ramping up ransomware attacks **targeting hybrid cloud environments**. Using sophisticated tactics, including vulnerabilities in on-premises servers, the group **deploys** ransomware like **Embargo** to exploit cloud networks. Organizations face severe risks from data breaches, credential theft, and financial losses.

- North Korean hackers from the group "**Kimsuky**" have **targeted Diehl Defence**, a German **arms company,** using fake job offers and a spoofed website. The **cyber-espionage campaign** aimed to **steal sensitive defense data.** Kimsuky operates on behalf of North Korea's military intelligence to gather confidential information.

- **Agence France-Presse (AFP)**, a global media giant, was **hit by a cyberattack**, **disrupting its IT systems** and news delivery services to clients. AFP's teams, with France's cybersecurity agency ANSSI, are investigating and working to mitigate the attack. **No details on the perpetrators or attack method** were provided.

- **GorillaBot**, a massive **botnet** with **300,000 infected devices,** has become a leader in DDoS attacks. It targeted **200,000 entities** across **113 countries,** hitting sectors like **universities, government, telecoms,** and critical infrastructure. With support for major CPU architectures, it issued over **300,000 attack commands in 24 days,** severely impacting China, the U.S., and Canada.

Spain

- **Abyss** hacking group claims to have breached **Spanish mining company Tolsa**, reportedly exfiltrating **5.1 TB of sensitive data.** As of now, Tolsa's website is down, adding credibility to the group's claim. Abyss has issued a ransom deadline of October 3, 2024, putting Tolsa under pressure to respond. This incident highlights ongoing risks of large-scale ransomware attacks targeting critical industries.

- **Mediumvioletred Cosmos TaurusX** claims to have leaked a database belonging to **Barcelona Experts,** allegedly containing **38,000 lines of sensitive information**. The data includes user details, internal messages, system configurations, etc. The breach raises concerns over the potential exposure of personal and organizational data.

- **CyberDragon group** claims to have hacked **Plataforma Fénix,** a single sign-on platform used by the **Royal Spanish Football Federation (RFEF).** Allegedly, the group has obtained **passports and other sensitive documents** from over a hundred users, including team representatives.

- The **Catalonia Waste Agency (ACR)** suffered a **ransomware attack** this past weekend, primarily affecting its **Waste Document Management System (SDR)**. While internal systems were impacted to a lesser extent, contingency measures were swiftly implemented, allowing services and waste transport in Catalonia to continue without disruption. The Catalonia Cybersecurity Agency is collaborating with ACR to mitigate the attack's effects and restore system integrity. An **investigation is ongoing.**

- **Mutua Madrileña** has fallen victim to a **cyberattack** targeting its home **insurance customer database,** potentially exposing personal data of thousands of clients. The **breach** occurred via an **external provider** and the company is proactively informing affected customers. In addition has notified relevant authorities, including the Spanish Data Protection Agency.

- The FBI has revealed that a **Chinese malware**, part of the **"Raptor Train" botnet**, has **infected 2,000 devices in Spain.** This botnet has compromised over 260,000 network devices globally, including routers and IoT devices, and is primarily used for DDoS attacks and network infiltration. While the main targets are in the U.S. and Taiwan, Spain accounts for 0.8% of the affected devices.

Latam

- **Unbleachedsilk Cosmos Taurus** offers on Breachforum The leaked Batcom Telecom database, which exposes sensitive information of 28,000 customers and 300 users, including personal data, login credentials and API files. The compromised data includes names, contact details, identification numbers and account credentials.

- **Upsdellred Cosmos Taurus** claimed to have breached the system of the municipality of Moreno, Argentina, accessing sensitive government data.

- **Orangepeel Cosmos Taurus** offers at BreachForum a data breach at Citibank Peru has exposed sensitive information on more than 100,000 people. The leaked data includes names, surnames, ID numbers, email addresses, dates of birth and home addresses, raising significant privacy concerns for affected customers.

Vulnerabilities & Exploits

- Multiple **critical vulnerabilities** have been discovered in **CUPS** (Common Unix Printing System), exposing Linux, BSD, Solaris, and Chrome OS to remote attacks. Exploits, such as **CVE-2024-47177,** allow unauthenticated attackers to execute arbitrary commands by manipulating printer URLs. Over 75,000 hosts are publicly exposed on the internet.

- Multiple **critical vulnerabilities** have been discovered in **PHP**, impacting versions prior to 8.1.30, 8.2.24, and 8.3.12. These flaws include **log tampering (CVE-2024-9026)**, **arbitrary file inclusion (CVE-2024-8927)**, and **data integrity issues (CVE-2024-8925)**. Exploitation of these vulnerabilities could lead to system compromise, unauthorized access, and hindered incident response.

- A critical flaw, **CVE-2024-28987,** was discovered in **SolarWinds Web Help Desk**, exposing 827 instances to potential attacks. Hardcoded credentials in the software allow attackers to modify help desk tickets and access sensitive data. A PoC exploit has been released, urging organizations to apply SolarWinds' latest hotfix to prevent unauthorized access.

- A **critical** flaw, **CVE-2024-47070,** has been discovered in the authentik Identity Provider, allowing attackers to **bypass password authentication** by manipulating the X-Forwarded-For HTTP header. With a **CVSS** score of **9.1,** this vulnerability poses significant risks to organizations using affected versions, **enabling unauthorized access to user accounts.**

- A newly discovered vulnerability, dubbed the **"Perfect" MITM attack,** allows attackers to **intercept and decrypt SSL traffic from Gmail** while maintaining the legitimate certificate chain, making detection impossible. Despite **affecting** over **1.5 billion users,** Google has downplayed the issue, raising concerns about the vulnerability's potential for exploitation.

- **Zimbra** recently released a critical patch for **CVE-2024-45519,** a severe vulnerability in its postjournal service. This flaw allows unauthenticated attackers to **execute arbitrary commands** on affected systems.

- A severe **unauthenticated remote code execution (RCE)** vulnerability, affecting all **GNU/Linux systems,** has been discovered by researcher Simone Margaritelli. With a **CVSS** score of **9.9,** the flaw allows attackers to execute arbitrary code remotely. Despite industry acknowledgment, no fix is available yet.

⚠ Warning of the week

- CUPS might handle your printing, but these new vulnerabilities are no small matter. With CVE-2024-47177 allowing remote command execution, your system could be the one doing the attackers' dirty work. Patch those Linux, BSD, Solaris, or Chrome OS systems fast before your servers start freelancing for hackers!

- PHP is cracking under pressure! With vulnerabilities like log tampering and file inclusion, patch to the latest versions ASAP. Unless, of course, you enjoy surprise visitors having full access to your system logs and files. PHP's vulnerabilities aren't waiting, so neither should you.

- Hardcoded credentials in SolarWinds? It's like leaving your front door open with a sign that says, 'Help yourself!' Apply the hotfix immediately to lock the door before hackers start rewriting your help desk tickets... with malicious intent.

- With CVE-2024-47070, attackers could bypass your passwords faster than a coffee break! Fix this X-Forwarded-For header issue before they get unauthorized access, or your identity provider might be providing identities... to the wrong people.

- MITM attacks are no longer 'perfect' when you patch them! Despite Google's downplay, this vulnerability could intercept your SSL traffic undetected. So, before your inbox starts reading like a public diary, ensure your Gmail and SSL protections are rock solid.

- Zimbra's postjournal service has a critical flaw that lets attackers run commands without even logging in. Update your systems quickly, or you might find someone else's fingerprints all over your data... and they didn't even need a key.

- An unauthenticated RCE in GNU/Linux? Yikes! With a 9.9 CVSS score, this flaw is nearly perfect for attackers. While we wait for a fix, consider tightening your security posture—because the only 'remote' thing you want on your system is your own control.

ADVERSARIALLY
weekly report
Sep 26 - 3 Oct, 2024

XG3 UNIT

Ransomware

Total Victims = 141 (+22)
- Spain - **2** (+1)
- Latam - **7** (+1)
- WorldWide - **132** (+20)

The king is...

Data of the week

Top Countries

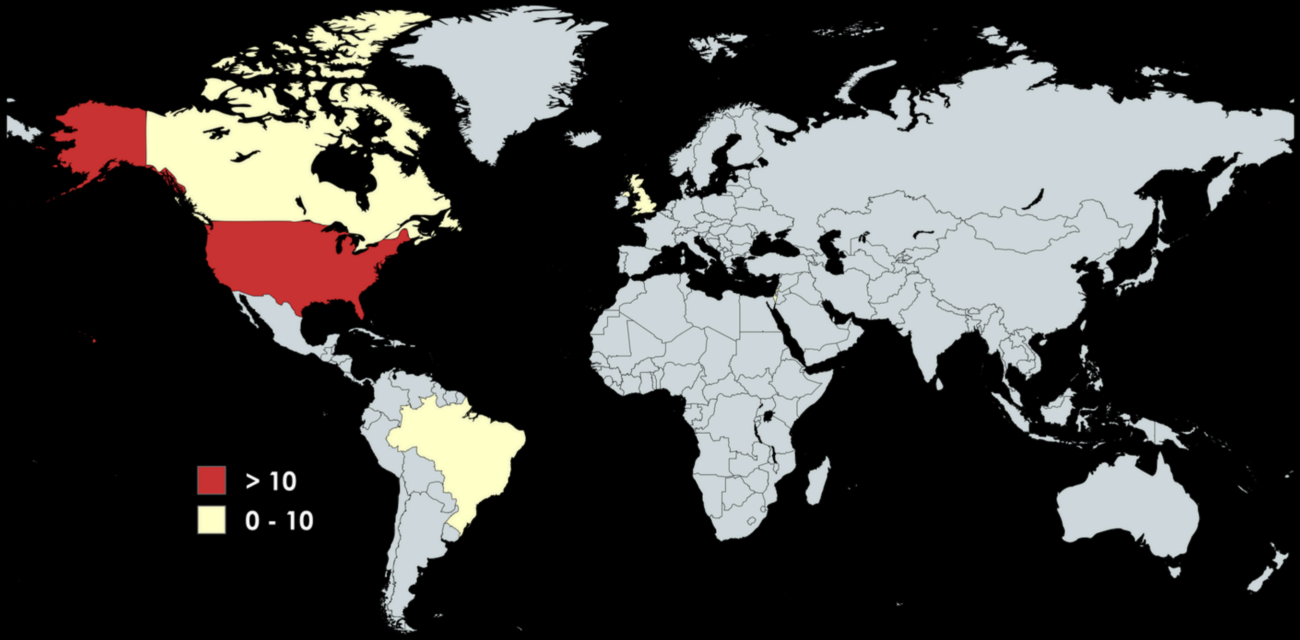
- USA - **58** (+1)
- CAN - **8** (+1)
- BRA- **6** (+1)
- GBR- **6** (+1)
- ISR - **4** (☆-2)

Top Sectors

- Technology - **31** (+20)
- Manufacturing - **25** (+4)
- Finance - **9** (+2)
- Healthcare - **8** (-2)
- Consulting - **6** ☆

Top Groups

- Ransomhub - **15** (+3)
- Play - **12** ☆
- Lockbit3 - **10**☆
- Nitrogen - **9** ☆
- Meow - **9** ☆



Victims

- **Ransom Victim:** FoccoERP | Group: trinity | Sector: Technology | Country: Brazil
- **Ransom Victim:** marthamedeiros.com.br | Group: madliberator | Sector: Design | Country: Brazil
- **Ransom Victim:** TOTVS | Group: blackbyte | Sector: Technology | Country: Brazil
- **Ransom Victim:** nfe.fazenda.gov.br | Group: killsec | Sector: Government | Country: Brazil
- **Ransom Victim:** appweb.usinacoruripe.com.br | Group: ransomhub | Sector: Technology | Country: Brazil
- **Ransom Victim:** www.vbrlogistica.com.br | Group: ransomhub | Sector: Transportation | Country: Brazil
- **Ransom Victim:** Corantioquia | Group: meow | Sector: Administration | Country: Colombia
- **Ransom Victim:** decalesp.com | Group: blacksuit | Sector: Technology | Country: Spain
- **Ransom Victim:** tolsa.com | Group: abyss | Sector: Manufacturing | Country: Spain

ADVERSARIALLY

weekly report

Sep 26 - 3 Oct, 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 **55**

Top Most Relevant

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

Threat Actors **1**

Top Most Relevant

- Akira

Tools **3**

Top Most Relevant

- LaZagne
- RClone
- AdFind

xMDR

ADVERSARIALLY

weekly report

Sep 26 - 3 Oct, 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.