ADVERSARIALLY weekly report

Feb 15 - 22 , 2024

by XG3 UNIT

cipher
a Prosegur company

xMDR

ADVERSARIALLY

weekly report

Feb 15 - 22, 2024

XG3 UNIT

Adversary of the Week

Rose Cosmos Taurus

Type: Individual

Countries: 🇲🇽

Maturity: 🟩⬛⬛

Sectors: Education

Activity: Cybercrime

TTPs: Leak of confidential information

Turla

Type: APT

Countries: 🇪🇺 🇨🇳 🇺🇸

Maturity: 🟧🟧⬛

Sectors: Goverment, Education, Finance, IT

Activity: Information theft and espionage

TTPs: 46

LockBit 3.0

Type: APT

Countries: 🇺🇸 🇪🇺

Maturity: 🟥🟥🟥

Sectors: All

Activity: RaaS

TTPs: 41

Global

- **Shanghai Anxun Information Company** data breach reveals alleged **spying on NATO countries and Asian governments**. It mentions **spyware** with capabilities such as **RAT and data collection**, versions for various operating systems and **injectable WiFi devices**. In addition, there are products designed to spy on Chinese social networks and devices with "TOR" type functions.

- An **iOS-targeted Trojan** called **GoldPickaxe.iOS** has been discovered. The Trojan **collects facial profiles, identity documents and intercepts SMS.** To exploit the stolen biometric data of users, this malware **creates deepfakes using AI** face-sharing services.

- **Battery manufacturer Varta**, with a presence in 45 countries, has **suffered a cyber-attack** that has **paralysed its battery production** and administrative processes. The company doesn't yet know the extent of the damage caused.

- **Ukrainian police** have **arrested** an unknown **cybercriminal** who **distributed trojanised software** through his own websites, using it to carry out a campaign of cyberattacks, **gaining access to bank accounts of US and Canadian users and then selling it on the dark web.**

- The **FBI has dismantled** a **bootnet comprised of Ubiquiti Edge OS routers infected with Moobot malware**, which was **controlled by Military Unit GRU 26165, also tracked as APT28 or Fancy Bear**. Threat actors made use of Moobot to deploy their own customised malicious tools, reusing the botnet to turn it into a cyber-espionage tool.

- **Charming Kitten** has been linked to a campaign of attacks **targeting Middle Eastern** policy experts and **distributing the BASICSTAR backdoor**.

- The **APT group Turla** has been detected **using** a new **backdoor TinyTurla-NG** against **non-governmental** organisations in **Poland**.

- The **creator** of the **ransomware Kryptina, Corlys**, has **published** all the **documentation and code for his ransomware free** of charge so that anyone can use it in their attacks. This is yet another tool for threat actors to successfully carry out their attacks.

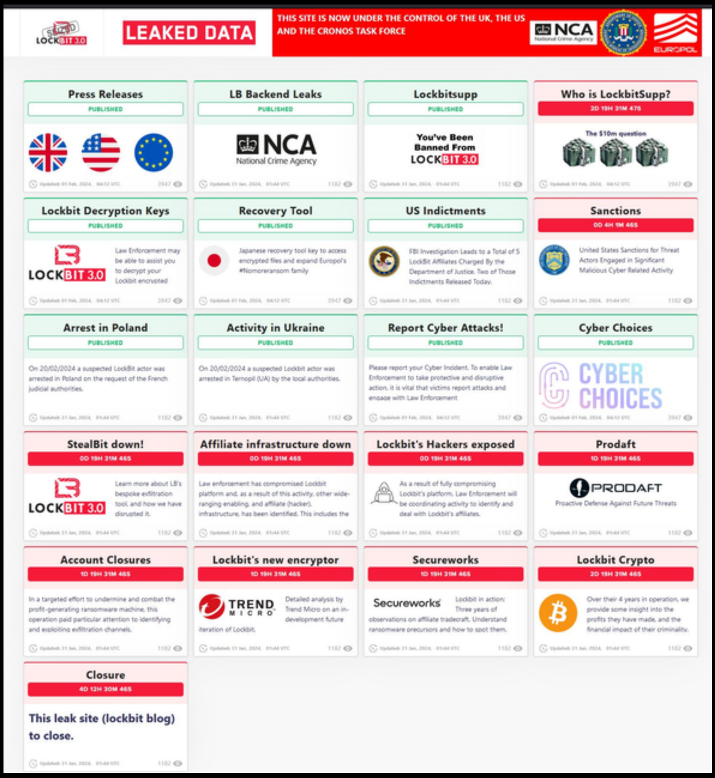
Operation Cronos, the end of LockBit?

A cooperative operation between the **FBI, the UK's National Crime Agency (NCA), EUROPOL** and other countries in Europe and Asia has **disrupted** the structure of the **LockBit ransomware** group and **taken down 22 TOR sites** associated with the group.

Operation Cronos, involving **law enforcement agencies from 11 different countries**, has **seized 11,000 domains** associated with LockBit and **arrested two members** of the group in Poland and Ukraine.

Apparently, the **FBI has made use of the PHP vulnerability listed as CVE-2023-3824**, which occurs when loading Phar. Checking for insufficient length causes a stack buffer overflow, which **can cause memory corruption or allow remote code execution (RCE).**

Having taken control of LockBit's main TOR site, the **authorities have published** in a humorous tone various **statements, decryption tools and threat feeds.**



THIS SITE IS NOW UNDER THE CONTROL OF THE UK, THE US AND THE CRONOS TASK FORCE

Press Releases
PUBLISHED
Updated: 01 Feb, 2024, 04:12 UTC 3947

LB Backend Leaks
PUBLISHED
NCA National Crime Agency
Updated: 31 Jan, 2024, 01:44 UTC 1182

Lockbitsupp
PUBLISHED
You've Been Banned From LOCKBIT 3.0
Updated: 31 Jan, 2024, 01:44 UTC 1182

Who is LockbitSupp?
2D 19H 31M 47S
The $10m question
Updated: 01 Feb, 2024, 04:12 UTC 3947

Lockbit Decryption Keys
PUBLISHED
LOCKBIT 3.0
Law Enforcement may be able to assist you to decrypt your Lockbit encrypted
Updated: 01 Feb, 2024, 04:12 UTC 3947

Recovery Tool
PUBLISHED
Japanese recovery tool key to access encrypted files and expand Europol's #Nomoreransom family
Updated: 01 Feb, 2024, 04:12 UTC 3947

US Indictments
PUBLISHED
FBI Investigation Leads to a Total of 5 LockBit Affiliates Charged By the Department of Justice. Two of Those Indictments Released Today.
Updated: 31 Jan, 2024, 01:44 UTC 1182

Sanctions
0D 4H 1M 46S
United States Sanctions for Threat Actors Engaged in Significant Malicious Cyber Related Activity
Updated: 31 Jan, 2024, 01:44 UTC 1182

Arrest in Poland
PUBLISHED
On 20/02/2024 a suspected LockBit actor was arrested in Poland on the request of the French judicial authorities.
Updated: 31 Jan, 2024, 01:44 UTC 1182

Activity in Ukraine
PUBLISHED
On 20/02/2024 a suspected Lockbit actor was arrested in Ternopil (UA) by the local authorities.
Updated: 31 Jan, 2024, 01:44 UTC 1182

Report Cyber Attacks!
PUBLISHED
Please report your Cyber Incident. To enable Law Enforcement to take protective and disruptive action, it is vital that victims report attacks and engage with Law Enforcement
Updated: 01 Feb, 2024, 04:12 UTC 3947

Cyber Choices
PUBLISHED
CYBER CHOICES
Updated: 01 Feb, 2024, 04:12 UTC 3947

StealBit down!
0D 19H 31M 46S
LOCKBIT 3.0
Learn more about LB's bespoke exfiltration tool, and how we have disrupted it.
Updated: 31 Jan, 2024, 01:44 UTC 1182

Affiliate infrastructure down
0D 19H 31M 46S
Law enforcement has compromised Lockbit platform and, as a result of this activity, other wide-ranging enabling, and affiliate (hacker). infrastructure, has been identified. This includes the
Updated: 31 Jan, 2024, 01:44 UTC 1182

Lockbit's Hackers exposed
0D 19H 31M 46S
As a result of fully compromising Lockbit's platform, Law Enforcement will be coordinating activity to identify and deal with Lockbit's affiliates.
Updated: 31 Jan, 2024, 01:44 UTC 1182

Prodaft
1D 19H 31M 46S
PRODAFT
Proactive Defense Against Future Threats
Updated: 31 Jan, 2024, 01:44 UTC 1182

Account Closures
1D 19H 31M 46S
In a targeted effort to undermine and combat the profit-generating ransomware machine, this operation paid particular attention to identifying and exploiting exfiltration channels.
Updated: 31 Jan, 2024, 01:44 UTC 1182

Lockbit's new encryptor
1D 19H 31M 46S
TREND MICRO
Detailed analysis by Trend Micro on an in-development future iteration of Lockbit.
Updated: 31 Jan, 2024, 01:44 UTC 1182

Secureworks
1D 19H 31M 46S
Secureworks
Lockbit in action: Three years of observations on affiliate tradecraft. Understand ransomware precursors and how to spot them.
Updated: 31 Jan, 2024, 01:44 UTC 1182

Lockbit Crypto
2D 19H 31M 46S
Over their 4 years in operation, we provide some insight into the profits they have made, and the financial impact of their criminality.
Updated: 31 Jan, 2024, 01:44 UTC 1182

Closure
4D 12H 30M 46S
This leak site (lockbit blog) to close.
Updated: 31 Jan, 2024, 01:44 UTC 1182

Illustration 1. Authorities publication on the Lockbit's TOR site

Spain & Portugal

- The **Mossos d'Esquadra's corporate mailbox** has suffered a cyberattack in which cybercriminals have **accessed private documents** with sensitive information about the agents. As a result of the incident, an investigation has been opened and the affected officers have been notified.

LATAM

- Actor **Regal Cosmos Taurus** sells access to a database of the Universidade Federal de Santa Catarina and access to a panel. The data would cover the years 2002 to 2024.

- Actor **Rose Cosmos Taurus** claims to have hacked into a subdomain of the Instituto de Educación Superior Tecnológico Público Chota.

Vulnerabilities & Exploits

- Vulnerability **CVE-2020-3259**, which could **allow** an attacker to **retrieve** the **contents** of an affected device's memory and **affects Cisco Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD)** software, has been found to be **exploited by the Akira ransomware** group.

- A **critical bootloader vulnerability** has been detected in Shim listed as **CVE-2023-40547** that affects almost **all Linux distributions**. It consists of a flaw that could result in the **bypassing of a secure boot** and allow actors to take near-total control of the compromised host.

- Critical Vulnerabilities CVE-2024-22245 and CVE-2024-22250 Pose Ongoing Threats in Deprecated EAP. **CVE-2024-22245** exposes systems to authentication relay attacks. In this scenario, attackers can manipulate domain users into relaying service tickets for arbitrary Active Directory Service Principal Names (SPNs). **CVE-2024-22250**, this vulnerability enables an attacker to hijack privileged sessions within the EAP.

- **Update:** Threat actor **Winter Vivern** has been **linked** to a new **cyber-espionage campaign** that made use of cross-site scripting (XSS) **vulnerabilities** in **Roundcube's webmail servers** to target over 80 organizations. These entities are primarily located in Georgia, Poland, and Ukraine.

⚠️ Warning of the week

- Did you hear about **GoldPickaxe.iOS**? Looks like they're getting creative in the world of iPhone virus! Keep your secrets safer by enabling two-factor authentication and protect your phone as if it were the last slice of pizza at a party.

- Warning! **Scammers handing out trojanised banking software** and selling account access on the dark web. Use strong passwords, keep an eye on your banking movements as if you were a secret agent and, for the love of burgers, don't click on anything online!

- Have you seen Charming Kitten's latest exploit with their **BASICSTAR backdoor**? Don't let them lure you in and keep your defences stronger than your coffee in the morning. Update your software as fast as memes go viral.

- **Shim for Linux issues**! Update now and keep your boot safe from thieves. Don't let your system be the afterparty for cybercriminals!

ADVERSARIALLY weekly report

Feb 15 - 22, 2024

XG3 UNIT

Detections by Risk

Top 5 Weekly Rules Added/Updated by Adversary Rule Risk:

- Enumerating domain admins with net group **(73.0)**
- Suspicious binary download from Powershell, network request **(72.5)**
- Hashcat activity detected **(70)**
- Possible windows lolbin masquerading - name too similar **(65.5)**
- Mimikatz memssp log file detected **(62.5)**

🟥	90-100	*Rules with all or some of these features: Critical attack techniques, sophisticated adversaries, trending Mitre TTPs, relevant CVE scores*
🟧	70-90	*Rules with all or some of these features: High attack techniques, severe adversaries, trending Mitre TTPs, high CVE scores*
🟨	50-70	*Rules with all or some of these features: Medium attack techniques, risky adversaries, trending (or not) Mitre TTPs, medium CVE scores*
🟢	0-50	*Rules with all or some of these features: Low attack techniques, not related to any adversaries, trending (or not) Mitre TTPs, low CVE scores*

Top MITRE Covered

- Account Discovery
- Command and Scripting Interpreter
- Ingress Tool Transfer
- Unsecured Credentials
- MasqueradingSyy

Adversary Trends

Actors	Set Tools	Vulnerabilities
Volt Typhoon	GoldPickaxe	Php / CVE-2023-3824
APT28	GoldDiggerPlus	Vmware / CVE-2024-22245
Kimsuky	Backmydata	Liferay / CVE-2024-26269
APT29	GoldKefu	Liferay / CVE-2024-25603
Storm-1567	GoldPickaxe.iOS	Liferay / CVE-2024-25147

ADVERSARIALLY
weekly report
Feb 15 - 22, 2024

XG3 UNIT

Ransomware

Total Victims = 80 (-44)

- Spain - **0** (-4)
- Latam - **8** (+3)
- WorldWide - **72** (-43)

The king is...

Data of the week

Top Countries

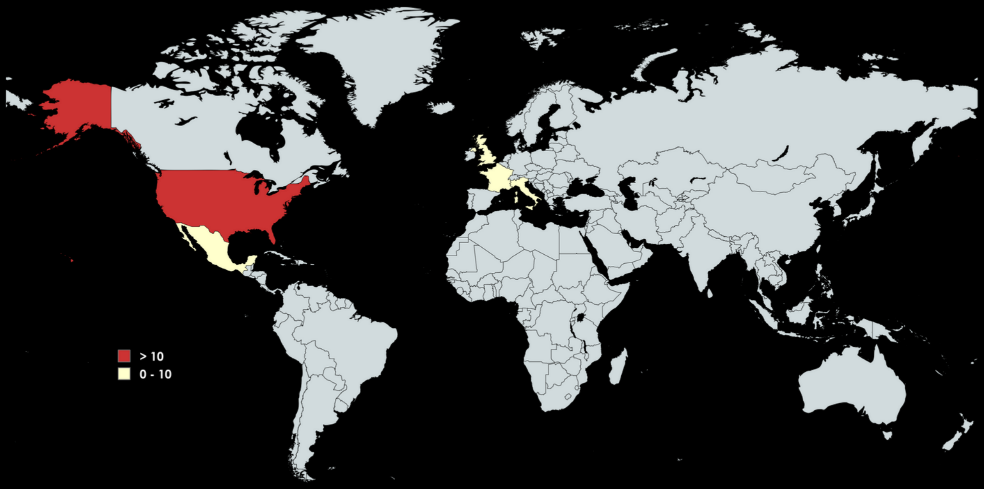
- USA - **34** (-19)
- FRA - **5**
- GBR - **4** (-2)
- MEX - **3** ☆
- ITA - **3** ☆

Top Sectors

- Industrial - **18** ☆
- Services - **16** (-11)
- Other - **7**
- Transport - **4** ☆
- NGO - **4** ☆

Top Groups

- Lockbit - **16** (-32)
- Hunters - **15** (-1)
- Play **9** ☆
- ALPHV - **5** (-7)
- Trisec - **4** ☆



Victims

- **Ransom Victim:** Conseguros | Group: Qilin | Sector: Services | Country: Guatemala
- **Ransom victim:** FALCO Electronics | Group: Trigona | Sector: Industrial | Country: México
- **Ransom victim:** América Móvil | Group: Trigona | Sector: Telecom | Country: México
- **Ransom victim:** Grupo Bimbo | Group: Medusa | Sector: Food | Country: México
- **Ransom victim:** Tiete | Group: Hunters International | Sector: Transport | Country: Brasil
- **Ransom victim:** Tormetal | Group: LockBit | Sector: Industrial | Country: Chile
- **Ransom victim:** Sitrack | Group: LockBit | Sector: Technology | Country: Chile
- **Ransom victim:** Champion Cargo Agent | Group: LockBit | Sector: Transport | Country: Colombia

xMDR

ADVERSARIALLY

weekly report

Feb 15 - 22, 2024

cipher

a Prosegur company

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.