

EUROPOL

EC3 - European Cybercrime Centre

EUROPOL CAPACITIES AND EFFORT SUPPORTING LAW ENFORCEMENT AGAINST CYBERCRIME

Emanuele Iovini

E-Governance Specialist

Prevention & Outreach team

RIPE90 – Lisbon – 13 May 2025

A large, white, stylized Europol logo is mounted on a dark blue building facade. The logo features a stylized 'E' with a yellow and orange graphic element. The word 'EUROPOL' is written in a bold, sans-serif font, slanted upwards from left to right. A yellow horizontal line runs across the bottom of the logo area.

Europol Public Information

EC3: Who are we?

The **European Cybercrime Centre (EC3)** was set up by Europol to strengthen the law enforcement response to cybercrime in the EU and thus to help protect European citizens, businesses and governments from online crime



Together in the fight against **cybercrime**

- Established in **2013**
- Involved in many high-profile operations
- Hundreds of operational-support deployments
- **Operational, strategic, analytical and forensic support to Member States' investigations**
- Each year, EC3 publishes the Internet Organised Crime Threat Assessment (**IOCTA**), its flagship strategic report on key findings and emerging threats and developments in cybercrime

Europol Organizational Structure

- 01 – Operational Centre
- 02 – European Serious and Organized Crime Centre
- 03 – European Cybercrime Centre (EC3)**
- 04 – European Counter Terrorism Centre
- 05 – European Financial Economic Crime Centre

Head of EC3

Knowledge

Prevention & Outreach
Policy & Development

Digital Support

Forensic Support
Cyber Intelligence Support

Operations (O3)

AP Cyborg **HIGH TECH CRIMES**
AP Terminal **PAYMENT FRAUD**
AP Twins **CHILD SEXUAL ABUSE**
AP Dark Web **DARK WEB**

Joint Cybercrime
Action Taskforce **J-CAT**

ESTE DOMINIO HA SIDO BLOQUEADO

A través de la cooperación internacional en la operación KAERB se ha llevado a cabo una serie de acciones coordinadas para dismantlar los servicios cibercriminales de una organización que operaba en 5 países.

Las fuerzas de seguridad y policiales han intervenido bases de datos y otra información relacionada con este dominio.

Cualquiera que opere o haya utilizado estos servicios cibercriminales está sujeto a investigación y procesamiento.

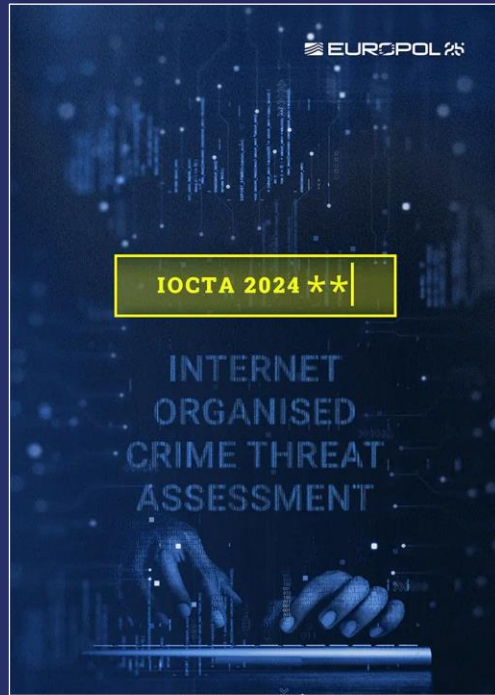
Si tiene información para denunciar sobre actividad cibernética criminal de este dominio, contáctenos:



EUROPOL

IOCTA 2024 **

INTERNET ORGANISED CRIME THREAT ASSESSMENT



THIS DOMAIN HAS BEEN SEIZED

Through the international cooperation of Operation Endgame, a series of coordinated actions to dismantle cybercriminal services has been carried out.

Law enforcement agencies have seized databases and other information relating to this domain. Anyone operating or using these cybercriminal services is subject to investigation and prosecution.

If you have information to report about cyber criminal activity on this domain, please contact us:

operation-endgame.com
contact@operation-endgame.com




THIS WEBSITE HAS BEEN SEIZED

OPERATION PhishOFF

METROPOLITAN POLICE

This domain has been seized by the Federal Bureau of Investigation (FBI) and the United States Secret Service (USSS) pursuant to a seizure warrant obtained by the United States Attorney's Office for the Western District of Pennsylvania under the authority of 18 U.S.C. §§ 981, 982, and 1030, as part of a law enforcement action taken in parallel with the United Kingdom's Metropolitan Police Service (MPS), and other international law enforcement partners.

International law enforcement continues to work collectively against cybercrime, wherever and however it is committed.




<https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024>

/// How does international cooperation look like?

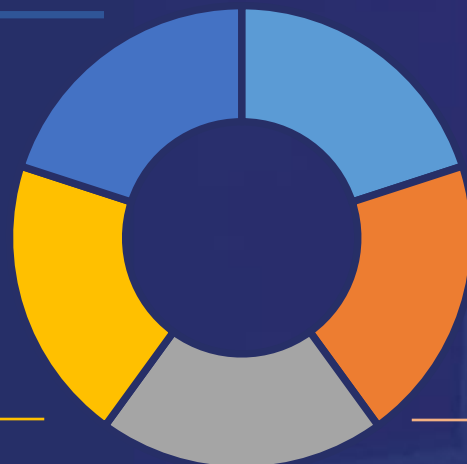


- In the lead of the investigation
- Owners of the data shared
- Coordinate and implement the Operational Action plan



SIENA:

- Cross-check operational data
- Analytical support and deconfliction
- Coordinate sprints, video calls and meetings
- **Large File Exchange (LFE)**
- **Virtual Command Post (VCP)**
- Command post: support live activities



EUROJUST

Judicial cooperation:

- European Arrest Warrants
- European Investigation Orders
- Mutual Legal Assistance

Organizes coordination meetings



European Multidisciplinary Platform Against Criminal Threats (EMPACT)

Multiannual Plan to fight against organized at EU level

- Funding operational sprints
- Funding resources



- J-CAT is a 24/7 permanent taskforce of cyber liaison officers, operating from Europol headquarters together with the European Cybercrime Centre (EC3)

EC3 Advisory Groups



23 MEMBERS
AG Service Providers



26 MEMBERS
AG Financial Services



28 MEMBERS
AG Internet Security

/// EC3 Advisory Groups

Fostering **closer cooperation** between law enforcement and key partners from the public and private sector

Goals:

- Establish and deepen trusted relationships
- Provide expert advice to EC3
- Agree on joint strategic and operational initiatives in the fight against cybercrime



EC3 Advisory Groups

Missions for the AGs members

- Support operations
- Threat assessment
- Policy discussion
- Capacity building
- Awareness support
- Participation in EC3 events

/// Operation Talent

Europol-supported operation led by German authorities



January 2025

Overview of the operation

- Law enforcement from **eight countries**
- Takedown of the two largest cybercrime forums in the world: “**cracked.to**” and “**nulled.io**”
- **2 arrests**
- 7 properties searched
- 17 servers and over 50 electronic devices seized
- EUR 300 000 of cash and cryptocurrencies seized
- **12 domains seized** along with other associated services (hosting + financial processor)

/// Operation Talent

The platforms nulled.to and cracked.io



- More than **10 million users** and EUR 1 million of profit
- Marketplace for illegal goods and **Cybercrime as a Service (CaaS)**
- Quick entry point in the cybercrime scene
- Platforms working as one-stops shops
- Hosting service **StarkRDP** - promoted and run by the suspects)
- Financial processor **Sellix**

/// Operation Talent

The platforms nulled.to and cracked.io



- Associated services: **stolen data, login credentials malware, hacking tools**
- Also Offered **AI-based tools** and **scripts** to:
 - Automatically scan for security vulnerabilities
 - Optimize attacks
 - Advanced phishing techniques, using AI to create more personalized and convincing messages

/// Operation Talent

Europol role in supporting the investigation



- Bringing relevant partners together **for cross-border cooperation and joint action:**
- Joint Cybercrime Action Taskforce (**J-CAT**) hosted at Europol HQ:
- Main Country: Germany + Australia, France, Greece, Italy, Romania, Spain, USA

/// Operation Talent

Europol operational support to the investigation



- Providing **Analytic** and **forensic** support
- Action day with **analyst deployed on the spot** to work with German investigators
- Act as **broker of the law enforcement knowledge**, providing a hub through which Member States can connect and benefit from one another's Europol's expertise
- Operational sprints

/// The importance of WHOIS/IP in investigations

Cooperation is an essential aspect in investigations

- Finding the **real location** of a server
- Identifying the real **“User”**
- Finding **who holds/own the data** consenting:
 - Freeze/Seize/Takedown +
 - Lawful interception of connections/packets (when possible)
- Obtaining **copies** of the servers
- Monitoring illicit activity

/// The importance of WHOIS/IP in investigations

Cooperation is an essential aspect in investigations

- Addressing the real owner/holder directly - **Evade hopping** through different SPs
- Starting investigations **faster**
- Enabling **local “low value” investigations** which are hampered by lack of data
- Finding connection between servers -> **Discover/Assess the whole criminal infrastructure**



Regulations related to E-Governance

- 1) Directive on measures for a high common level of cybersecurity across the Union (**NIS 2 Directive**) (art. 28)
- 2) EU Electronic Evidence legislative package:
Regulation (EU) 2023/1543 - Directive EU 2023/1544
- 3) **Second Additional Protocol to the Budapest Convention on Cybercrime**
- 4) Regulation (EU) 2022/2065 - **'the Digital Services Act' (DSA)**

Mentions:

- 5) Clarifying Lawful Overseas Use of Data Act– CLOUD Act
- 6) European Union Artificial Intelligence Act

/// Regulations' common aspects

1. Establishing a **legal/reference contact** for LEAs/Judicial Authorities/Legitimate access seekers
2. Maintain accurate and up-to-date information about registrant/users
3. Having data management and retention policies (based on local law)
4. Being ready to answer in **short time** (8 hrs for emergency requests)
5. Having **backup strategies**
6. Building mechanism to **retrieve data** in a fast and reliable way
7. Building **cooperation procedures** with LEAs and trusted flaggers
8. Monitoring **illicit activities**

Law enforcement Challenges

The traditional law enforcement approach does not work. There is several challenges when it comes to investigation, identification and prosecution.



Encryption

Encryption of online transmissions prevents monitoring by law enforcement agencies. Widespread use of end-to-end encryption in communications makes it hard to for LE to operate.



Anonymity

Legal or regulatory protections for personal privacy also present barriers to law enforcement in online environments as they prohibit government actions that violate privacy.



High Volume/ Low value crime

High volume and low value crime poses a challenge to law enforcement due to it's less noticeable nature.



Challenges of public- private partnerships

Cooperation with the private sector is vital in combating cybercrime as the private sector holds much of the evidence of cybercrime. In addition to that they often also provide and maintain much of the tools used to navigate cyberspace



Cross-Border Jurisdiction

Challenges associated with national legal frameworks and overlapping jurisdictions result from the fact that the online environment extends beyond borders



Tracing Communication & Payments

The technological barriers associated with monitoring online activity include the hardware and software protective systems that people use to prevent unauthorized access to personal data through the Internet.

Law enforcement Challenges

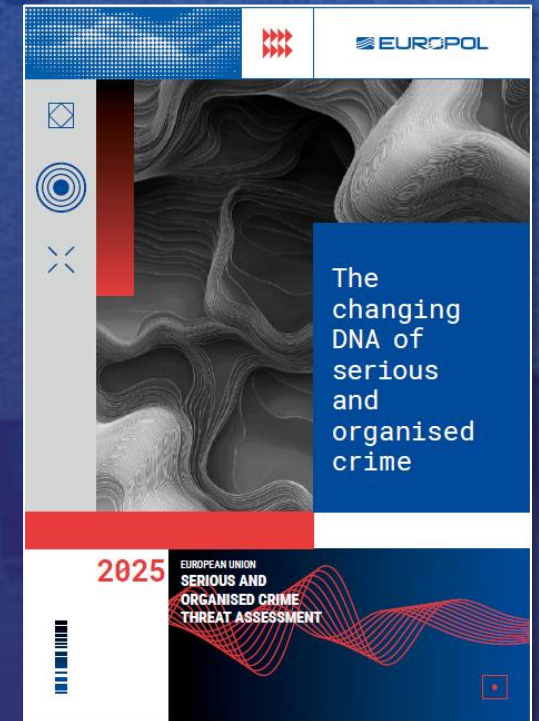
The traditional law enforcement approach does not work. There is several challenges when it comes to investigation, identification and prosecution.

New technologies

- Blockchain
- AI
- Quantum computing

*“Artificial intelligence has transformed the modern world with unprecedented speed and impact. Indeed, the very qualities that make AI revolutionary - **accessibility, versatility, and sophistication** - have made it also an attractive tool for criminals.”*

<https://www.europol.europa.eu/publication-events/main-reports/changing-dna-of-serious-and-organised-crime>



Thank you for
your attention

Questions?

 **EUROPOL**

www.europol.europa.eu

