

EUROPEAN CYBERCRIME CENTRE (EC3)

Emmanuel KESSLER

WHICH ROLE AS A COOPERATION HUB ?
WHICH ACHIEVEMENTS ?
WHICH E-GOVERNANCE & CHALLENGES ON CYBERCRIME ?

The image shows the Europol logo, which consists of the word "EUROPOL" in a stylized, white, sans-serif font. The letter "O" is replaced by a graphic of a hand holding a torch. The logo is set against a dark blue background with a yellow and white diagonal stripe below it.

Europol Unclassified – Basic Protection Level

EC3 - WHO ARE WE ?...a cooperation hub at EU level.



January 2013

- ✓ Cyber Threats and Trends
- ✓ Capacity Building
- ✓ Prevention & Awareness
- ✓ Internet Governance
- ✓ Outreach

- ✓ Transnational Payment Fraud
- ✓ Cyber-Dependent Crimes
- ✓ Child Sexual Exploitation
- ✓ Dark Web team



- ✓ Digital Forensics
- ✓ Document Forensics

2023 ACHIEVEMENTS, ...FROM YEARS OF OPERATIONS, LESSONS LEARNT FOR BETTER COORDINATION

PRIVATE SECTOR



JOINT CYBERCRIME ACTION TASK FORCE/J-CAT



2013

Europol
Operational
Centre 24/7

EC3 CYBER
INTELLIGENCE

EC3
OPERATIONAL
UNIT



J-CAT – EC3
International Ransomware
Response Model (IRRM)

2021



2016

NOMORERANSOM.ORG



Digital IT Lab



Advanced on-the-
spot forensic support

Europol operations against ransoms: the 2023 overview...

<https://www.europol.europa.eu/media-press/newsroom>

TAKEDOWN OF RAGNAR LOCKER RANSOMWARE GANG

Operation Talpa

OCT 2023

Ragnar Locker Ransomware Gang

International investigation led by the French National Gendarmerie, together with law enforcement authorities from the Czechia, Germany, Italy, Japan, Latvia, the Netherlands, Spain, Sweden, Ukraine and the United States of America, supported by Europol and Eurojust.

Results:

- A significant arrest of the main perpetrator made in France on Oct 16th.
- Searches were conducted in Czechia, Spain and Latvia.
- 5 Suspects were interviewed in Spain and Latvia in the following days.
- Ransomware's infrastructure was also seized in the Netherlands, Germany and Sweden.
- The associated data leak website on Tor was taken down in Sweden.

EUROPOL

Europol Unclassified - Basic Protection Level

TAKEDOWN OF MALWARE FOR HIRE

Operation Parker

FEB 2023

Core members ransomware criminal group targeted

Operation by German and Ukrainian police, supported by Europol, the Dutch Police (Politie) and the US FBI.

ECJ's support:

- Information exchange
- 3 experts deployed in Germany on the action day
- Analytical support: cryptocurrency, malware, decryption and forensic analysis

Results:

- Raided house of a German national
- Electronic equipment seized
- Ukrainian suspect interrogated
- 2 locations searched in Ukraine

DoppelPaymer ransomware

- Used since 2018 to attack organisations and critical infrastructures.
- Used a unique tool that compromised defence operations by terminating the security-related processes of the attacked systems.
- Distributed through phishing/teams including malicious attachments.
- Double extortion scheme, used a leak website launched by the criminals in 2020.
- The DoppelPaymer attacks were enabled by the specific **LockBit** malware.

EUROPOL

Europol Unclassified - Basic Protection Level

TAKEDOWN OF MALWARE FOR HIRE

Operation 5th Element

NOV 2023

International collaboration leads to dismantlement of ransomware group in Ukraine amidst ongoing war

The ransomware gang is behind high-profile attacks that created losses of hundreds of millions of euros

The investigation benefited from funding from the European Multi-Disciplinary Platform Against Criminal Threats (MPACT).

Results:

- 30 properties searched
- Ringleader arrested and 4 accomplices detained

Participating countries: NO, FR, NL, UA, DE, CH, USA, EUROPOL, EUROJUST

The individuals under investigation are believed to be part of a network responsible for a series of high-profile ransomware attacks against organisations in 71 countries.

These cyber actors are known for specifically targeting large corporations, effectively bringing their businesses to a standstill. They deployed **LockerGoga**, **MegaCortex**, **HIVE** and **Dharma ransomware**, among others, to carry out their attacks.

EUROPOL

Europol Unclassified - Basic Protection Level

RANSOMWARE-AS-A-SERVICE

OP Dawnbreaker

HIVE ransomware

JAN 2023

Shutdown of HIVE infrastructure marketplace extorting millions in ransom

ECJ's support:

- Information exchange
- 4 experts deployed on the spot on the action day
- Analytical support: cryptocurrency, malware, decryption and forensic

Results:

- International operation led by Germany, Netherlands and U.S. involving authorities from 13 countries
- About EUR 120 million saved thanks to mitigation efforts
- Decryption keys free of charge

Ransomware-as-a-Service / Double Extortion Model

- Criminals copied the data and then encrypted the files.
- They asked for a ransom to both decrypt the files and to not publish the stolen data on the Hive Leak Site.

Modus Operandi

HIVE ransomware was used to target businesses and critical infrastructure sectors, including government facilities, manufacturing, information technology and healthcare (1 hospital in Germany)

EUROPOL

Europol Unclassified - Basic Protection Level

LAW ENFORCEMENT COOPERATION TAKEDOWN

Operation EndGame

Qakbot botnet

SEPT 2023

Cross-border judicial cooperation takes down large botnet infrastructure Qakbot

Eurojust and Europol aided cross-border judicial cooperation with law enforcement from France, Germany, Italy, The Netherlands, Romania, UK, and the US for this operation.

Results:

- Coordinated international law enforcement effort led to the takedown of Qakbot infrastructure
- Nearly EUR 8 million seized in cryptocurrencies

Europol facilitated information exchange, coordination, and provided analytical support.

Qakbot

The malware victimised more than 700 000 computers in almost 30 countries, with at least EUR 54 million paid in ransoms since 2007.

Distributed via spam emails with malicious attachments/links.

Stole financial data and login credentials and allowed for further infections like ransomware and made infected computers part of a botnet.

EUROPOL

Europol Unclassified - Basic Protection Level

TAKEDOWN OF CHIPMIXER

Operation Atlas

takedown Chipmixer

MARCH 2023

One of the darkweb's largest cryptocurrency laundromats washed out

The investigation was also supported by Belgium, Poland and Switzerland.

Results:

- Takedown of the platform infrastructure
- 4 servers seized
- EUR 44 million in Bitcoins seized
- 7 TB of data seized

ChipMixer (Unlicensed)

Available on the clear and on the darkweb.

Specialised in mixing/cutting trails related to virtual currency assets = anonymising where the initial funds originated.

Criminals have illegally obtained money → Deposited into 'mixers' to disguise origins → Crypto exchanges → Funds into a fiat currency → Laundered money available for criminals

EUROPOL

Europol Unclassified - Basic Protection Level

EUROPOL

OPERATION CRONOS

CORE COUNTRIES

AUSTRALIA, CANADA, FRANCE, GERMANY, JAPAN, NETHERLANDS, UNITED KINGDOM, UNITED STATES, SWEDEN, SWITZERLAND

PARTICIPATING COUNTRIES

FINLAND, NEW ZEALAND, POLAND, UKRAINE

E-GOVERNANCE

TRANSPPOSITION OF ARTICLE 28
OF THE NIS2 DIRECTIVE ?

COOPERATION BETWEEN
LEA & REGISTRIES AND
REGISTRARS

ACCESS PLATFORM&TOOLS
FOR LEA

RELIABILITY OF DATA SETS

GETTING
INFORMATION
ON DNS and
IPV4/IPV6

THE « THICK
WHOIS »

Thank you for your attention

@EC3EUROPOL on X
EC3Partners@europol.europa.eu

www.europol.europa.eu

