EUROPOL'S EUROPEAN CYBERCRIME CENTRE (EC3)

Latest challenges on cyber-threats and cyber crisis

Emmanuel KESSLER
Head of Prevention&Outreach

1

Which Ec3 capacities against cyberthreats ?

JCAT/DSU/Law enforcement emergency response protocol /IRRM…

2

Which threats from our windows ?

IOCTA 2023 is coming !

3

Which activities? Which operations ?

Short examples of achievements : Hive, Power off, Raidforum…

4

Which new challenges and expectations in the way forward ?

AI, going dark, E-evidence, NIS2,…

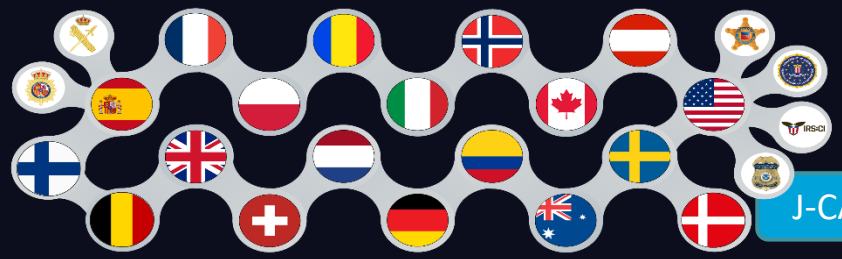
1

WHICH PERMANENT CAPACITIES ?

EUROPOL EC3 European Cybercrime Centre

SECURED COMMUNICATION NETWORK & CAPACITIES - SIENA

Extension of the EUROPOL mandate (June 2022)



J-CAT

Europol Operational Centre 24/7

EC3 CYBER INTELLIGENCE

EC3 OPERATIONAL UNIT

PRIVATE SECTOR

Internet Security

Financial Services

Communication Providers

EU AGENCIES AND MAJOR STRATEGIC PARTNERS

Digital IT Lab

Advanced on-the-spot forensic support

EU MEMBER STATES LAW ENFORCEMENT AUTHORITIES

EUCTF European Union Cybercrime Taskforce

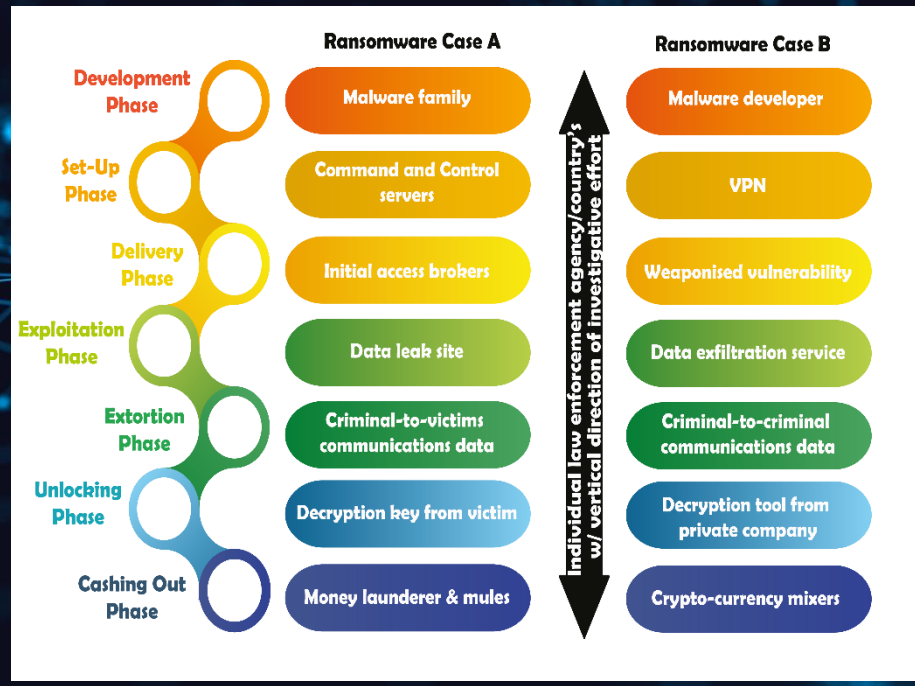
1

other tools and approaches… Rethinking the kitchen !

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

No More Ransom

Law Enforcement Emergency response Protocol



Which latest trends ??

2

Ransomware as a service

Re-victimisation in malware attacks

Increasing demand for criminal services, Initial access brokers

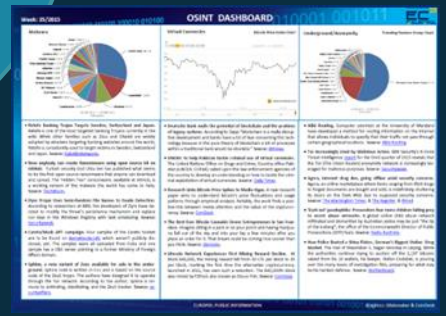
Data theft

DDOS attacks

Social engineering

Abuses of legitimated services

Increased maturity of cybercriminal



GoldDust : an emblematic cooperation example

On 4 November 2021, Romanian authorities arrested two individuals suspected of cyber-attacks deploying the Sodinokibi/REvil ransomware.

The suspects are allegedly responsible for 5.000 infections, which in total pocketed half a million euros in ransom payments.

Operation GoldDust involved 17 countries, Europol, Eurojust and INTERPOL.

The arrests follow the joint international law enforcement efforts of identification, wiretapping and seizure of some of the infrastructure used by Sodinokibi/REvil ransomware family, which is seen as the successor of GandCrab.

3

VPNLab.net – Disrupting criminal capacities !

In 2022, law enforcement authorities took action against the criminal misuse of VPN services as they targeted the users and infrastructure of VPNLab.net.

The VPN provider's service was being used in support of serious criminal acts such as ransomware deployment and other cybercrime activities.

Law enforcement authorities seized the 15 servers that hosted VPNLab.net's service, rendering it no longer available.

EUROPOL EC3 European Cybercrime Centre | JOINT CYBERCRIME J-CAT ACTION TASKFORCE

3

Targeting the criminal ecosystem by Shuting down an illegal marketplace and seizing its infrastructure

Forum's administrator
& 2 accomplices arrested

Coordinated by Europol to support independent investigations of the United States, United Kingdom, Sweden, Portugal and Romania

RaidForums - operation Tourniquet

500 000+ users

Considered one of the world's biggest hacking forums

Sold access to database leaks belonging to a number of U.S. corporations.

Information included: **cards, bank account numbers and routing information, usernames and associated passwords**

3

OPERATION POWER OFF – SEIZING CRIMINAL INFRA

GLOBAL CRACKDOWN AGAINST DDoS SERVICES

International operation with 8 services from US, UK, Netherland , Germany, Poland

7 ADMINISTRATORS ARRESTED

HIVE Ransomware

Shutdown of HIVE infrastructure marketplace extorting millions in ransom

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

EC3's support:

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

EUROPOL EC3 European Cybercrime Centre | JOINT CYBERCRIME J-CAT ACTION TASKFORCE

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.

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

Operation **Parker**

3

2 high-value ransomware targets hit

Operation led by Germany and Ukraine, with support of Europol, Netherlands and U.S.

Results:

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

EC3's support:

- Information exchange
- 3 experts deployed in Germany on the action day
- Cryptocurrency, malware, decryption and forensic analysis

DoppelPaymer ransomware

- Used since 2019 to attack **organisations** and **critical infrastructures**.
- Used a **unique tool** that compromised defence organisms by terminating the security-related process of the attacked systems.
- Distributed through **phishing/spam** including malicious attachments.
- **Double extortion scheme**, used a leak website launched by the criminals in 2020.

4

Current & next challenges for LEA

Artificial intelligence

High volume of crime/ reporting

Cross-border jurisdiction

Anonymity of criminals

Tracing payments

Tracing communication

Thank you for your attention

EUROPOL

EC3Partners@europol.europa.eu

www.europol.europa.eu