EUROPOL
EC3 | European Cybercrime Centre

@EC3Europol

53rd TF-CSIRT & FIRST Regional Symposium Europe

European Cybercrime Centre EUROPOL

Álvaro Azofra, Sara Marcolla
EUROPOL/EC3

Hamburg, 5 February 2018

Welcome to Europol!

EUROPOL
EC3 | European Cybercrime Centre

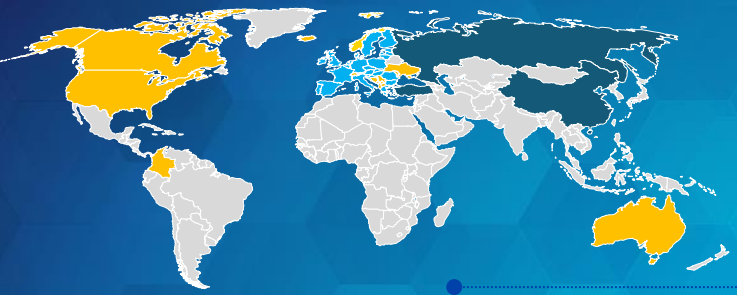
European Police Office

EUROPOL EC3 European Cybercrime Centre

"Europol shall support and strengthen action by the competent authorities of the Member States and their mutual cooperation in preventing and combating serious crime affecting two or more Member States, terrorism and forms of crime which affect a

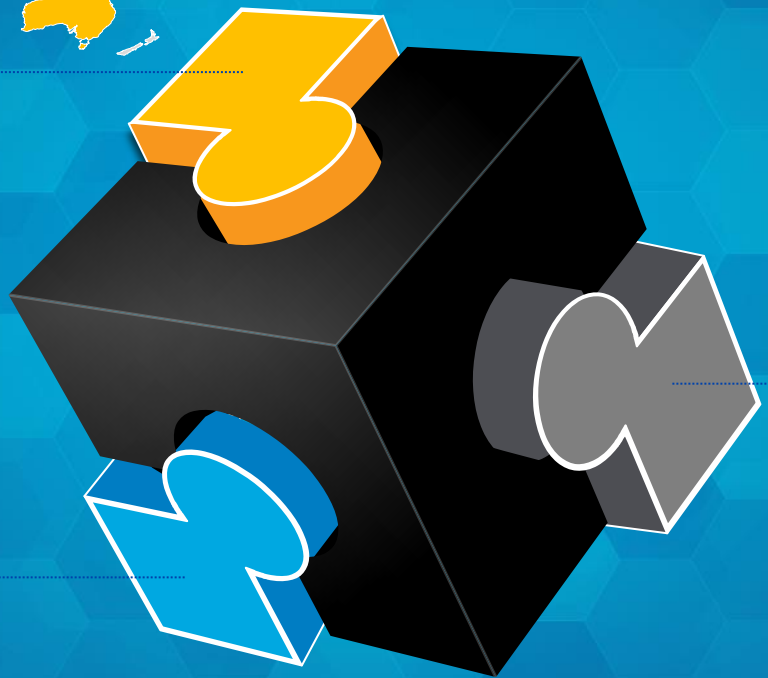
New Regulation, ongoing successes

EUROPOL EC3 European Cybercrime Centre



External Cooperation

Operational and Strategic Agreements with Third Parties.



Private-Public Partnerships

Improved strategic and tactical relationship with partners form Academia and Private Sector.

European Commission

EU Policy Cycle

Stakeholder representing Law Enforcement in the Security Strategy of the EU and other policy making initiatives.

EU wide reach

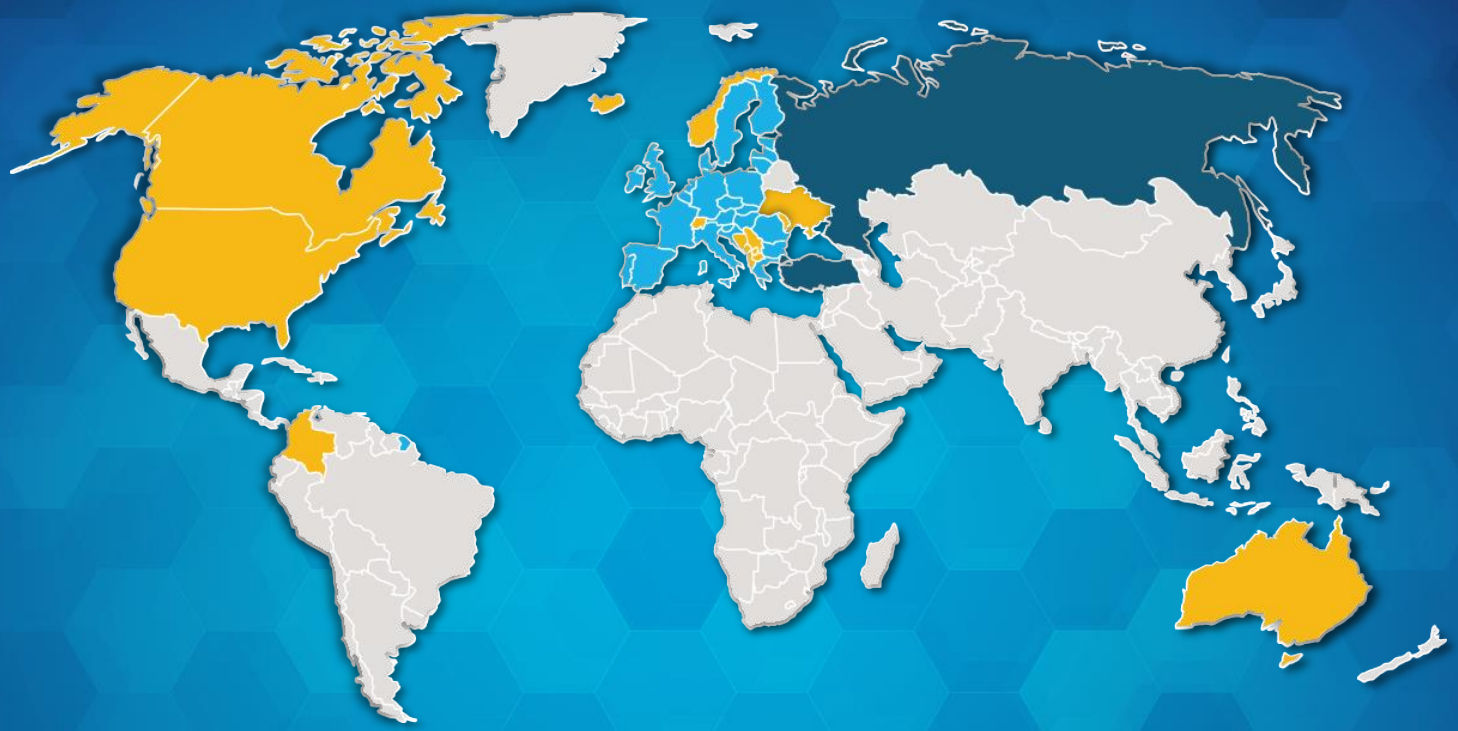
EUROPOL EC3 European Cybercrime Centre

Europol Liaison Officers in:

- Interpol IGCI
- Interpol IPSG
- Washington DC

Third party Cooperation

EUROPOL EC3 European Cybercrime Centre



28 EU Member States

Operational Agreements: Albania, Australia, Canada, Colombia, Eurojust, Former Yugoslav Republic of Macedonia, Moldova, Montenegro, Iceland, Interpol, Liechtenstein, Monaco, Norway, Serbia, Switzerland, Ukraine, United States of America

Strategic Agreements: Bosnia and Herzegovina*, CEPOL, ECB, ECDC, EMCDDA, ENISA, FRONTEX, OHIM, OLAF, Russia, UNODC, World Custom Organisation

Joint Cybercrime Action Taskforce (J-CAT)

EUROPOL EC3 European Cybercrime Centre

Chairmanship: Germany

Vice-Chairmanship: US FBI

Identification of pri

Investigative nities

JOINT CYBERCRIME ACTION TASKFORCE

J-CAT 2.0

Attachment Schemes with Law Enforcement and Private Sector

Operating from EC3

High-Tech Crimes

Online Child Sexual Exploitation

Payment Fraud

Cross-Crimes Factors Facilitating Cybercrime

EC3 Advisory Groups

EUROPOL EC3 European Cybercrime Centre

Communication Providers

Programme Board

Financial Services

Internet Security

EC3: machinery at work

EUROPOL
EC3 | European Cybercrime Centre

EC3 Cyber Intelligence Team

EUROPOL EC3 European Cybercrime Centre

- Analytical hub: collection + process + analysis.
- Disparate intel feeds: public, private and open sources
- Identify emerging threats and patterns
- Support other EC3 teams
- NO surveillance & NO infiltration

EC3 Cybercrime Operations

EUROPOL EC3 European Cybercrime Centre

Critical infrastructures and information systems

Cyber Attacks

AP CYBORG

Cyber Intelligence Team

Organized groups generating large criminal profits

Serious harm to the victims

Payment Card Frauds

AP TERMINAL

Child Sexual Exploitation

AP TWINS

EUROPOL EC3 European Cybercrime Centre

EC3 OPERATIONS

EUROPOL EC3 European Cybercrime Centre

Operations AVALANCHE && ANDROMEDA

EUROPOL EC3 European Cybercrime Centre

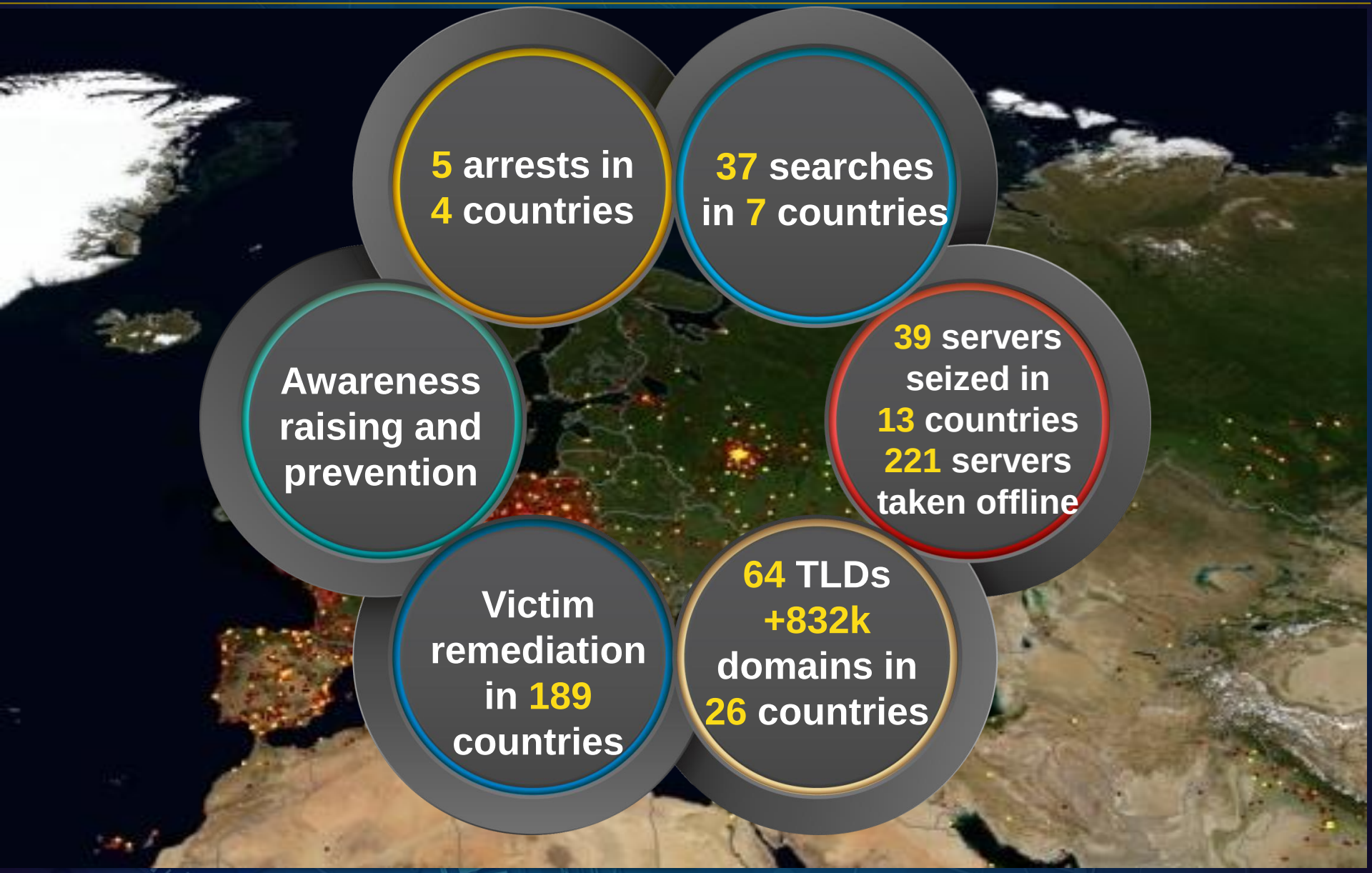
- *Notitia criminis*
- Intelligence
- Investigation
- Coordination
- Action day

Operation AVALANCHE

- Avalanche: infrastructure for malware delivery && cyberattacks && Money mule recruitment campaigns.
- 20+ malware families.
- 180+ countries affected.
- €6M in monetary losses (just in Germany).
- After 4 years of investigation, time for action.

Operation AVALANCHE - Nov 2016

EUROPOL EC3 European Cybercrime Centre

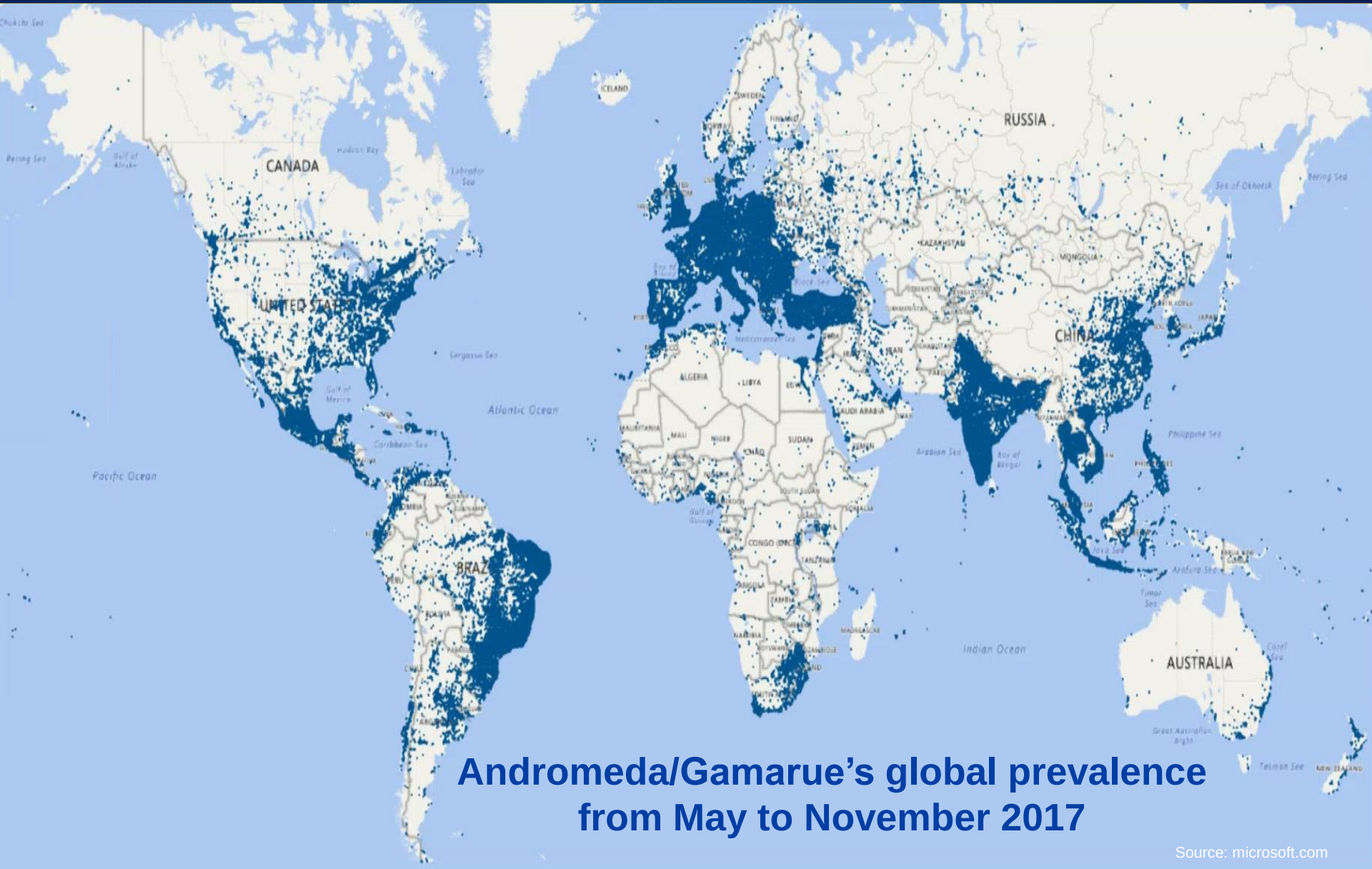


Operation ANDROMEDA

- Andromeda (AKA Gamarue) was part of the Avalanche infrastructure.
- Excluded from Avalanche takedown.
- Provided as modular criminal kit: bot builder, keylogger, rootkit, formgrabber, teamviewer…
- Q3+Q4 2017 detected/blocked in **+7M** machines.

Operation ANDROMEDA

EUROPOL EC3 European Cybercrime Centre



Andromeda/Gamarue's global prevalence from May to November 2017

Source: microsoft.com

Operation ANDROMEDA

EUROPOL EC3 European Cybercrime Centre

- Andromeda associated with 80 malware families:
  - **Petya (ransomware)**
  - **Cerber (ransomware)**
  - **Troldesh (ransomware)**
  - **Ursnif (info-stealing and banking trojan)**
  - **Carberp (info-stealing and banking trojan)**
  - **Fareit (info-stealing and DDoS malware)**
  - **Kasidet (worm and DDoS malware)**
  - **Lethic (spam bot)**
  - **Cutwail (spam bot)**
  - **Neurevt (click-fraud malware)**
  - **Ursnif (click-fraud malware)**
  - **Fynloski (backdoor)**
- +1 200 C2 domains && IP addresses
- 464 distinct botnets

Operation ANDROMEDA – Nov 2017

- International partners took action against Andromeda infrastructure.
- First 48 hours of sinkholing, 2 Million unique Andromeda victim IP addresses captured (Microsoft).
- House search and arrest of a suspect in Belarus.

Operation AVALANCHE && ANDROMEDA

EUROPOL EC3 European Cybercrime Centre

- Global joint effort collapsed the entire criminal network.
- Avalanche: globally 55 % of Avalanche victims still infected today.
- Both operations still ongoing, more actions will come.

Operation BAKOVIA

EUROPOL EC3 European Cybercrime Centre

- *Notitia criminis*
- Intelligence
- Investigation
- Coordination
- Action day

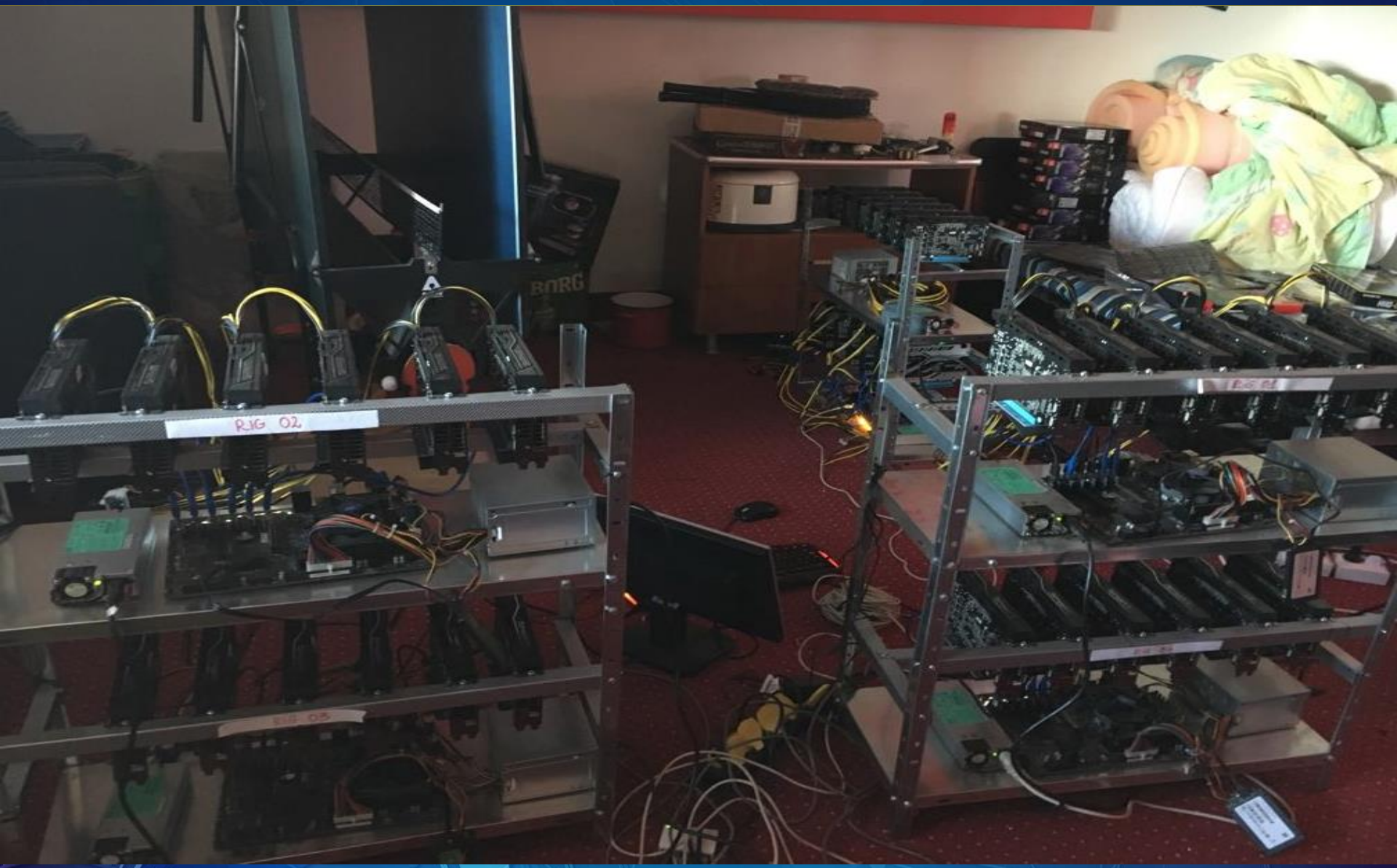
Operation BAKOVIA

Operation BAKOVIA: Action Day

Operation BAKOVIA: suspects arrested

Operation BAKOVIA: seized material

Operation BAKOVIA: currency mining infrastructure



Operation BAKOVIA: currency mining infrastructure

Operation BAKOVIA: takeaways

EUROPOL EC3 European Cybercrime Centre

- Global joint effort ended with the **arrest** of the main suspects.

- 3 suspects arrested in RO from CTB-Locker.
- 2 suspects arrested in RO from Cerber.

Cybercrime investigation → **International coordination**

How can you contribute further?

Nomoreransom.org

Keeping in touch

EUROPOL EC3 European Cybercrime Centre

SPACE

SECURE PLATFORM FOR ACCREDITED CYBERCRIME EXPERTS

EUROPOL EC3 European Cybercrime Centre

3,460 Active Users

55 Online sub-communities

@EC3Europol

More than **10,200** followers

EUROPOL

EC3 | European Cybercrime Centre

Let's make Europe safer

Follow us: **@EC3Europol**

sara.marcolla@europol.europa.eu

alvaro.azofra@europol.europa.eu