53rd TF-CSIRT & FIRST Regional Symposium Europe

European Cybercrime Centre

Álvaro Azofra, Sara Marcolla

EUROPOL/EC3

Hamburg, 5 February 2018
Welcome to Europol!
“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 common interest covered by a Union policy.”

More than 1000 staff
200 Europol Liaison Officers
Around 100 crime analysts
Supporting over 40 000 international investigations each year.
New Regulation, ongoing successes

External Cooperation
Operational and Strategic Agreements with Third Parties.

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

Private-Public Partnerships
Improved strategic and tactical relationship with partners from Academia and Private Sector.
EU wide reach

Europol Liaison Officers in:

• Interpol IGCI
• Interpol IPSG
• Washington DC
Third party Cooperation

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)

Chairmanship: Germany  
Vice-Chairmanship: US FBI

Identification of priorities  
Investigative opportunities

INVESTIGATION

Attachment Schemes with Law Enforcement and Private Sector

Operating from 2023

High-Tech Crimes
Online Child Sexual Exploitation
Payment Fraud
Cross-Crimes Factors Facilitating Cybercrime

Europol Unclassified - Basic Protection level
EC3 Advisory Groups

Communication Providers
- Telenor
- Orange
- Nedelijk ICT
- KPN
- GSMA
- Etno
- PT
- Vodafone
- Telefónica
- BT
- Tele2
- TIM
- RIPE NCC
- Ericsson
- Belgacom
- Digitus

Programme Board
- CEPOL
- European Commission
- ENISA
- EUROJUST
- CERT-EU
- EUCF
- European Union Cybercrime Taskforce
- Consilium
- INTERPOL

Financial Services
- Betaalvereniging Nederland
- Western Union
- UBS
- EBF
- Booking & Payments Federation Europe
- Bitpay
- Circle
- ING
- CitiBank
- AIB Lab
- Erste Bank
- Danske Bank
- MasterCard
- American Express
- Visa
- Raiffeisen Bank International
- Barclays
- European Central Bank
- Euromoney

Internet Security
- FireEye
- Check Point
- Cisco
- McAffee
- Symantec
- S21sec
- Trend Micro
- Bitdefender
- CrowdStrike
- Palamoot
EC3: machinery at work

- Stakeholder management
- Outreach
- Prevention
- Strategic Analysis
- Forensic Analysis
- Internet Governance
- Policy Engagement
- Training
- Communication
EC3 Cyber Intelligence Team

• 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

Critical infrastructures and information systems

Cyber Attacks

Cyber Intelligence Team

Organized groups generating large criminal profits

Payment Card Frauds

AP TERMINAL

Serious harm to the victims

Child Sexual Exploitation

AP CYBORG

AP TWINS

Europol Unclassified - Basic Protection level
Operations AVALANCHE & ANDROMEDA

Europol EC3

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

- 5 arrests in 4 countries
- 37 searches in 7 countries
- 39 servers seized in 13 countries
- 221 servers taken offline
- 64 TLDs +832k domains in 26 countries
- Awareness raising and prevention
- Victim remediation in 189 countries
• **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

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

Source: microsoft.com
Operation ANDROMEDA

- Andromeda associated with 80 malware families:
  - Petya (ransomware)
  - Cerber (ransomware)
  - Troldeh (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.
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

Notitia criminis
Intelligence
Investigation
Coordination
Action day
Operation BAKOVIA

FBI investigation 2014

Cerber & Dharma
RO

UK Server NCA

RaaS Darkweb

Dutch NHTCU investigation 2015

Malicious email with CTB-locker

Server wiretap in Netherlands

CTB-locker & Cerber RO

USSS investigation 2017
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

- 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?

- **109 Partners**
- **2017 SC Magazine Editor’s Choice Award**
- **Website available in 26 languages**
- **>28,000 devices successfully decrypted**
- **54 free decryption tools available**

Nomoreransom.org
Let’s make Europe safer

Follow us: @EC3Europol

sara.marcolla@europol.europa.eu
alvaro.azofra@europol.europa.eu