

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 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

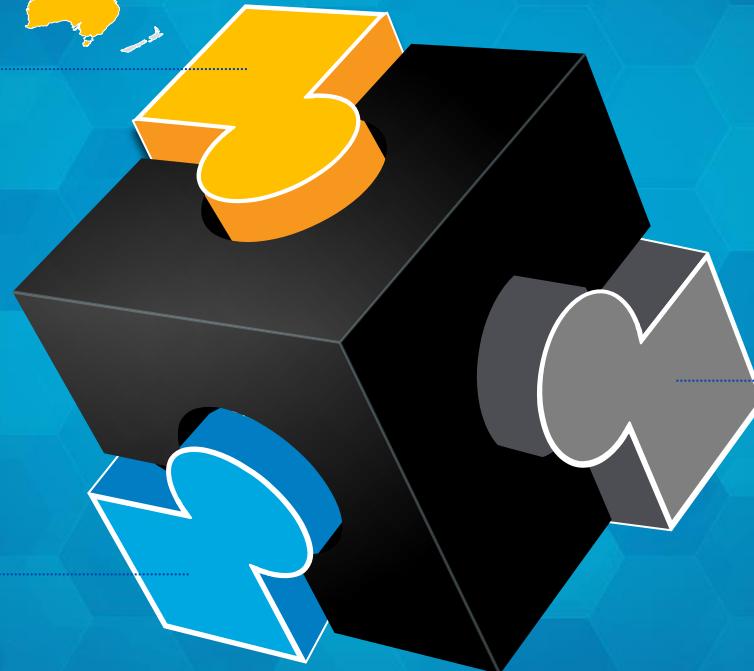


External Cooperation

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.

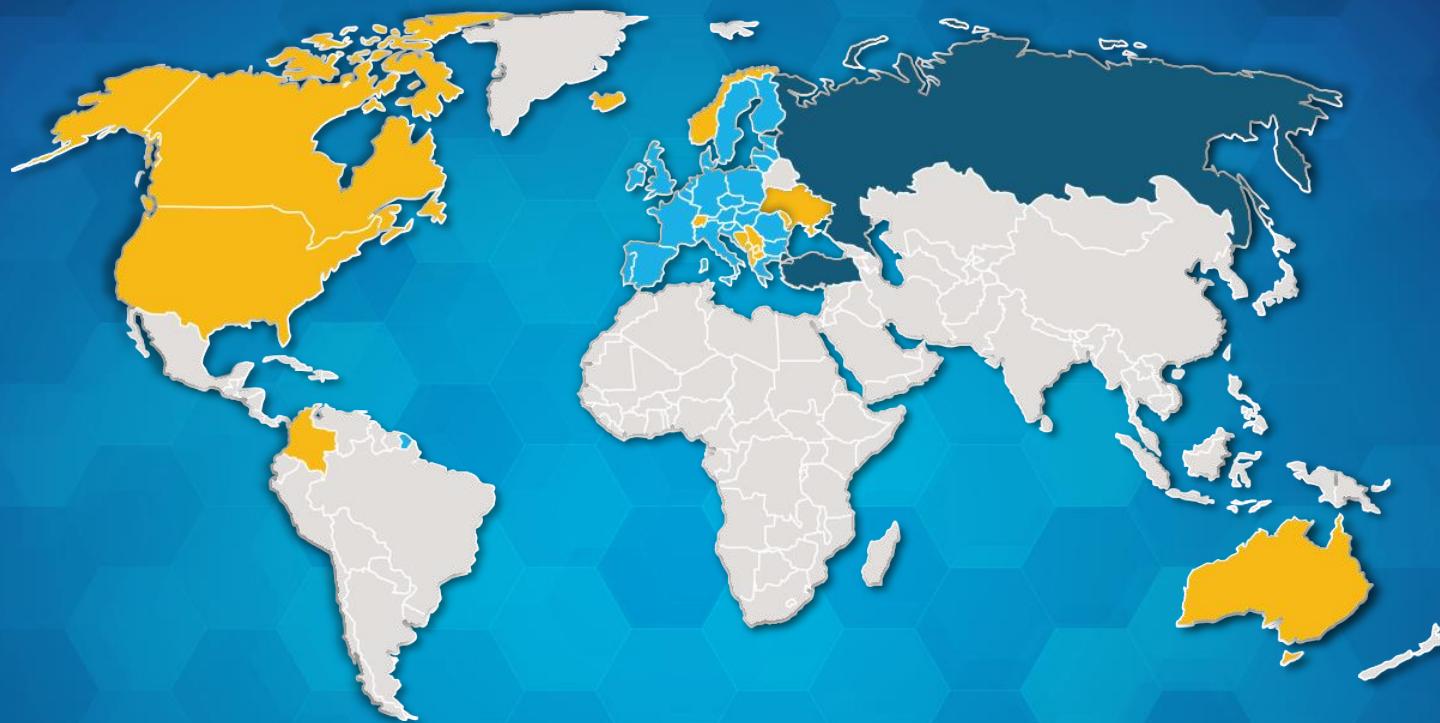


Europol Liaison Officers in:

- Interpol IGGI
- 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

Chairmanship: **Germany**



Vice-Chairmanship: **US FBI**

Identification
of pri-

Intervention

Investigative
nities

JOINT CYBERCRIME **J-CAT** 2.0 ACTION TASKFORCE

Attachment Schemes with Law Enforcement and Private Sector

High-Tech Crimes

Online Child Sexual Exploitation

Payment Fraud

Cross-Crimes Factors Facilitating Cybercrime

EC3 Advisory Groups

Communication Providers



Programme Board



Financial Services



Internet Security





- 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

Critical infrastructures and information systems

Cyber Attacks

AP CYBORG

Cyber Intelligence Team

Organized groups generating
large criminal profits

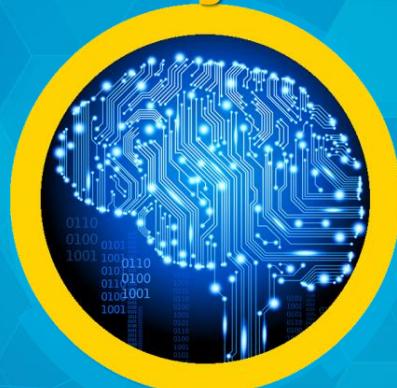
Payment Card Frauds

AP TERMINAL

Serious harm to the victims

Child Sexual Exploitation

AP TWINS



EUROPOL
EC3 | European Cybercrime
Centre

EC3 OPERATIONS



Operations AVALANCHE & ANDROMEDA



- 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**

**Awareness
raising and
prevention**

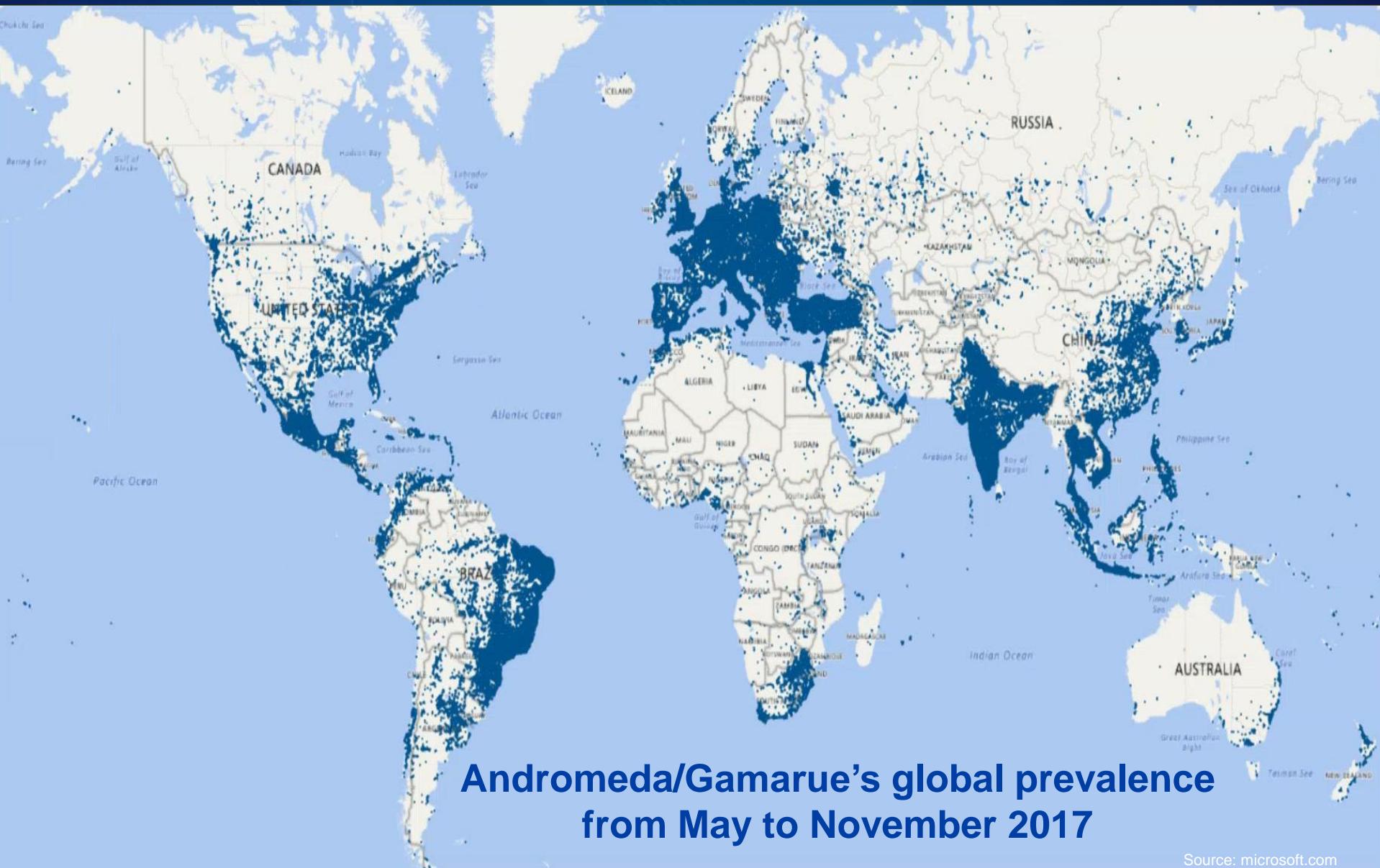
**39 servers
seized in
13 countries
221 servers
taken offline**

**Victim
remediation
in 189
countries**

**64 TLDs
+832k
domains in
26 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



Source: microsoft.com

- 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

- 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



Operation BAKOVIA: Action Day



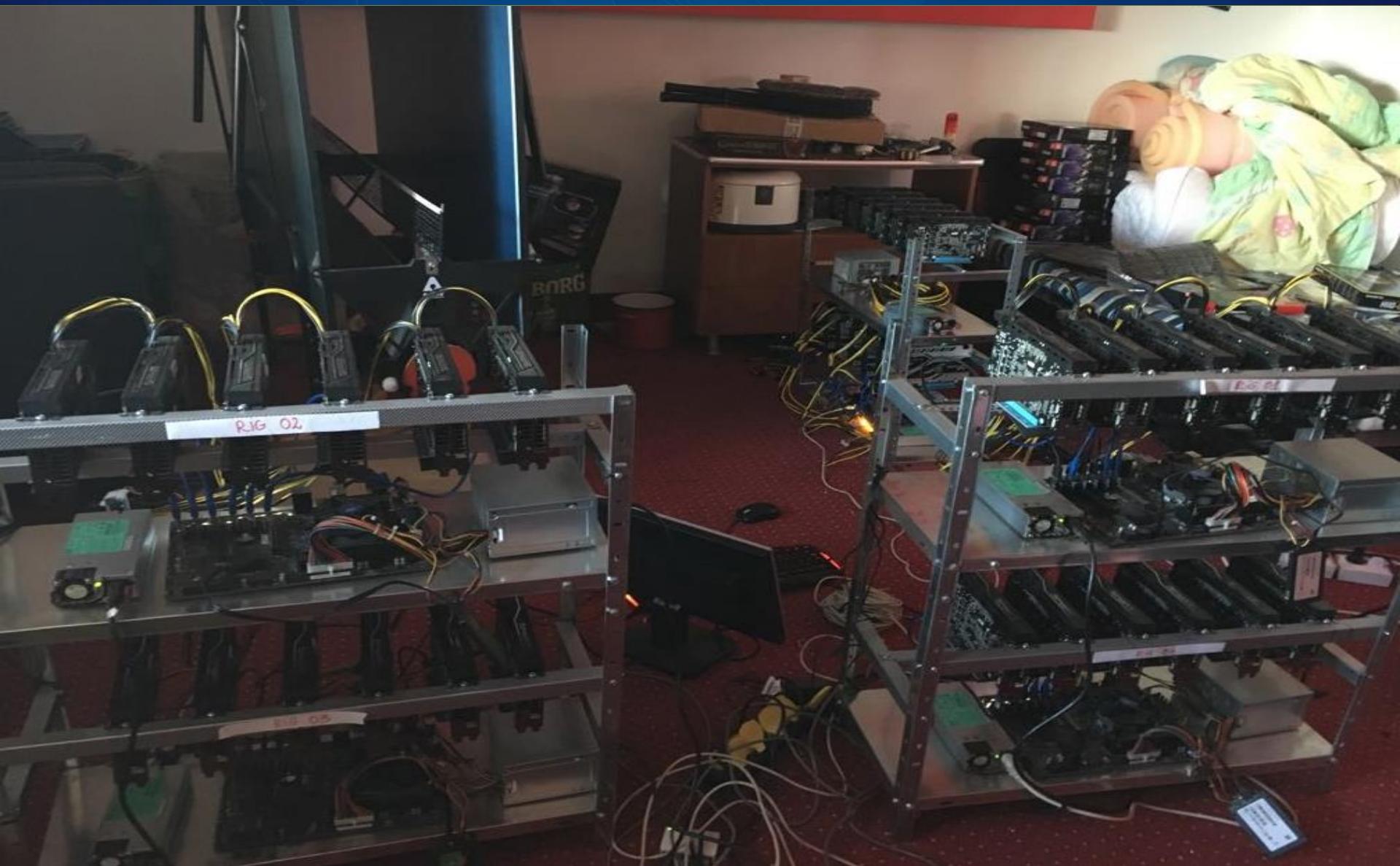
Operation BAKOVIA: suspects arrested



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?

The screenshot shows the homepage of Nomoreransom.org. At the top left is a red ribbon banner with the text "Winner SC Magazine EDITOR'S CHOICE AWARD". The top navigation bar includes links for "Crypto Sheriff", "Ransomware: Q&A", "Prevention Advice", "NO MORE RANSOM", "Help", "Partners", and "About the Project". A language selector shows "English".

The main content area features five large, numbered circular icons:

- 01** **109 Partners** (with a "Partners" link)
- 02** **Website available in 26 languages** (with a "Website" link)
- 03** **>28 000 devices successfully decrypted** (with a "Decryption Tools" link)
- 04** **Prevention is possible. Following our security advice can help you to avoid becoming a victim of ransomware.** (with a "Prevention" link)
- 05** **2017 SC Magazine Editor's Choice Award** (with a "SC Magazine" link)

In the center is a graphic of a document with a padlock and a dollar sign, indicating encrypted files.

On the right side, there are two download buttons:

- A red button labeled "DOWNLOAD" for the "Tool made by Kaspersky Lab".
- A blue button labeled "DOWNLOAD" for the "Tool made by Elevenpaths".

At the bottom, the URL "Nomoreransom.org" is displayed in large yellow text, along with the text "Europol Unclassified - Basic Protection level".

Keeping in touch



SPACE
SECURE PLATFORM
FOR ACCREDITED
CYBERCRIME EXPERTS

EUROPOL
EC3 | European Cybercrime
Centre

3,460 Active Users

55 Online
sub-communities



@EC3Europol

By understanding the stages of a [#cyberattack](#), you reduce its impact on your organization

ncsc.gov.uk/



Survey

User Education

Train all users to consider what they include in publicly available documents such as social media profiles. Encourage them to be aware of the risks from discussing work-related topics on social media, and the potential of being targeted by phishing emails.

Who might be attacking you?

Open Criminals interested in making money through cyber crime, or terrorist groups with political motives. Industrial competitors and foreign intelligence services interested in gathering economic advantage for their country. Hackers who find breaking into computer systems an enjoyable challenge. Hackers who wish to attack companies for political or ideological motives. Employees, or those who have learned how to do it by accident, or through malice.

TIPS & ADVICE

Use and understand wireless security, such as Wi-Fi networks, physical software, peer-to-peer sharing websites and removable storage devices, potential ways for your device to be infected with malware.

Keep your devices, operating systems and all software up-to-date.

Install and keep up-to-date firewalls, antivirus updated on your devices.

Back up the data stored on your computer regularly, on a separate storage device and offsite.

Think before you click on links and like/share without knowing their true origin and avoid clicking on suspicious links from unknown sources.

Open received files, software and apps from trusted sources.

Never use your laptop to process messages received through email, social networks or instant messaging tools, unless from a known and safe source.

RETWEETS 17 LIKES 10



Let's make Europe safer



Follow us: **@EC3Europol**

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