ISSUE 8: March 2016 - December 2016

Europol's European Cybercrime Centre (EC3)

The EC3 Bulletin

1 | A word from the Head of EC3
STEVEN WILSON

After nearly a year at Europol, the vibrant rhythm and the new challenges make me feel that 2016 has passed quicker than any of my previous 30 years in policing.

My initial impressions of the European Cybercrime Centre (EC3) as a dynamic, highly motivated workforce have been constantly reaffirmed by the efforts of staff on a multitude of tasks and operations throughout the year.

I outlined some key objectives upon arrival, in particular providing a greater level of support to the other business areas of Europol and sharing our skills and knowledge to further their investigations through cyber tactics. I am glad to see that this concept is being implemented.

One such example is the development of a response to the growing challenge of the supply of criminal commodities through marketplaces on the darknet. While we have identified the significance of these hidden services to all forms of criminality, there are particular challenges arising from the supply of firearms that must be addressed by Law Enforcement. The technical support of EC3 to all of the operations department is vital to adequately address this challenge.

Moreover, the EC3 digital and document forensics team has been providing training to many Europol staff, allowing them to capture key evidence on the ground. This ongoing enhancement of basic cyber skills will continue to be a priority throughout Europol as our society becomes increasingly digitised.

In terms of cooperating with non-law enforcement partners, the work done with our Advisory Groups is highly significant, including the launch of a new group focused on Communications Providers. We are in the process of streamlining them, setting up new objectives and meaningful deliverables across sectors, whilst retaining the most active members and bringing in companies and individuals with fresh perspectives.

Our Focal Points (FPs) have continued to deliver excellent results and major global operations, with significant impact on criminality targeting a range of sectors worldwide. Among others, the following has been highlighted in this bulletin:

- FP Terminal has supported a multitude of operations against ATM skimming organised criminal groups, two major global airline action events, an action on ATM malware gangs, two significant money muling initiatives with prevention campaigns, and new initiatives on e-Commerce.

- FP Twins has coordinated a strong commitment from 24 countries to come together for two weeks, pooling expertise in order to identify children under live abuse. Their work has led to children having been rescued already, with preparatory work done to aid the identification of many more.

Moreover, their involvement in leading complex transnational cases is driving innovative investigation tactics.

- FP Cyborg, Cyber Intel and J-CAT have tackled some of the most challenging cases seen in cyber yet. The recently completed Operation Avalanche is just one of many examples of the global investigation and coordination role they provide.

In Strategy we were sorry to lose Olivier Burgersdjik as Head of Business Area. He played a key role in setting up and steering EC3 and we wish him all the best in his new challenges within the organisation, where he will be leading the implementation of the Integrated Data Management Concept (IDMC). At the same time we welcome his replacement, Philipp Amann, who has already proved his abilities as former team leader of Strategy & Development. It says much of the professionalism of the staff that despite significant shortages they have continued to deliver highly important products such as the IOCTA 2016, and have managed a multitude of safety and media campaigns. Moreover, they have delivered what is in my opinion the most impressive Public Private Partnership I have seen to date in cyber: No More Ransom. This partnership with the Dutch Police, Kaspersky Lab and Intel Security has quickly reached global significance – a clear testimony to the difference that our work makes in ensuring a safer online environment for all.

We hope to see staff increases in 2017, in order to help us cope with the major expansion in EC3's responsibilities and allow us to continue to support the EU Member State fight against cybercrime, payment card fraud and online child sexual exploitation.

I hope you enjoy this last bulletin of 2016, a reflection of our work over the past months. I also hope the upcoming holiday season will allow you to spend some quality time with your families, recharging batteries that in many cases must be close to empty.

I am extending my personal thanks to all EC3 stakeholders for your outstanding efforts this year and I am already looking forward to an even better 2017!

Steven Wilson
Head of EC3

> *"My initial impressions of the European Cybercrime Centre (EC3) as a dynamic, highly motivated workforce have been constantly reaffirmed by the efforts of staff on a multitude of tasks and operations throughout the year.'*

> *"I am extending my personal thanks to all EC3 stakeholders for your outstanding efforts this year and I am already looking forward to an even better 2017!'*

2 | EC3 Operations

Second Victim Identification Task Force

In April 2016, the second Victim Identification Task Force (VIDTF II) conducted two weeks of intense work at Europol's headquarters in The Hague to identify victims of child sexual abuse and exploitation. Together with Europol, top experts from more than 10 EU Member States, Third Countries and INTERPOL joined forces to identify victims of child sexual abuse and exploitation. At this stage seven children have been identified as a result of actions taken after VIDTF II.

Outcome

Together with its partners, Europol's co-ordinated effort in the fight against online sexual exploitation and victimisation of children has yielded over 250 sequences of child sexual abuse images and video files, which have been uploaded to the INTERPOL hosted International Child Sexual Exploitation Database. Additions were made to more than 300 existing sequences. Furthermore, Europol has distributed intelligence packages to several countries to assist in the identification of

DID YOU KNOW?

Experts from Austria, Croatia, Denmark, Estonia, France, Germany, Italy, Spain, Sweden, the Netherlands, Romania, and the UK worked with their counterparts from Australia's AFP and Task Force Argos, Canada and US FBI and ICE, in an unparalleled collaborative effort.

These actions will ensure that many more victims have a better chance of being identified and are made safe from child sexual abuse. A number of investigations are well advanced and should soon lead to positive outcomes for more victims.

2 | EC3 Operations

Operation PLUS ULTRA II

In May 2016, Europol supported the Spanish Guardia Civil in their operation Plus Ultra II. The action against offenders in EU Member States was facilitated by Europol through the transfer of information on targets and checking of connections to known online activity. Intelligence packages were distributed on 23 targets within the EU, and investigations are ongoing.

The initial notification to the Guardia Civil came from the U.S. National Centre for Missing and Exploited Children (NCMEC). Europol works closely with NCMEC and U.S. Immigration and Customs Enforcement (ICE) in distributing to date more than 30 000 such notifications to 19 countries in the EU enriched with data from Europol's own databases.

FINDING

Notable behavioural patterns seen from the offenders in the cases targeted by Operation Plus Ultra II include organising to make access to child abuse easier amongst themselves, and using Privacy and Proxy (P&P) services and other measures to conceal their identities.

2 | EC3 Operations

Operation Daylight

A Europol coordinated operation targeting those responsible for distributing child sexual abuse material has led to 611 intelligence packages being disseminated through Europol to Member States and Associated Countries.

This EMPACT operational action has resulted in 207 criminal investigations being opened among these countries, and 75 persons being arrested or convicted at this point.

The action was planned and executed by law enforcement agencies across the European Union and focussed on those distributing child sexual abuse material using online networks. Those networks continue to be a primary source for persons with a sexual interest in children who seek child sexual abuse and exploitation material online.

Europol received intelligence from Switzerland in an action planned under the EMPACT framework for 2015, and distributed intelligence packages through its secure systems to Member States and Third Countries. The resulting police actions, investigations and prosecutions are ongoing in many of the countries, with results still being reported.

EMPACT, the European Multidisciplinary Platform Against Criminal Threats, is the EU's mechanism for delivering operational actions and strategic planning against different crime threats.

2 | EC3 Operations
ATM skimming networks dismantled

Main results

24 people arrested

18 house searches

EUR 50 000 seized

Electronic devices, computers, mobile phones and evidence found in a criminal laboratory used for manufacturing skimming devices sized

47 individuals identified involved in various activities within the criminal group, such as producing and installing skimming devices, payment card falsification, illegal financial transactions, and money laundering

Europol capabilities and services used

- Suspects identification
- Organisation of operational meetings
- Analytical support and expertise
- Information exchange

On 9 November 2016, the Romanian Police and Prosecutor's Office dismantled a large Organised Criminal Group (OCG) specialised in payment card fraud.

Modus Operandi

The criminals had been travelling across several EU Member States, installing skimming devices at ATMs (Automated Teller Machines) and self-service fuel stations, to copy the magnetic strip data from payment cards. The data was consequently used to produce fake payment cards with which cash was withdrawn in non-EU countries such as Nepal, the Philippines, Taiwan and the United States.

The 24 arrested are also suspected of establishing/supporting an organised criminal group, illegal software and hardware operations, payment card falsification, fraudulent financial transactions, and money laundering.

Key Factor **Close police cooperation on the global level and the direct support of American Express.**

During an operation run simultaneously in Europe and Asia with the support of Europol's EC3, 29 arrests took place in Malaysia and 76 throughout Europe. The Organised Crime Group's leaders were arrested, and two illegal production sites of high quality credit cards were dismantled.

The investigation spanned from the end of 2015 to the spring of 2016 in Malaysia and 14 European countries: Austria, Belgium, Switzerland, Czech Republic, Germany, Denmark, Spain, France, Croatia, Italy, Luxembourg, the Netherlands, Norway and UK.

Modus Operandi

The OCG was established in Malaysia with its members committing payment fraud crimes all over the world. High quality counterfeit credit cards were manufactured in different locations and subsequently used by individuals to purchase high value goods, mainly at electronic stores and duty-free shops at airports.

The credit card production sites used sophisticated equipment to ensure that counterfeits would not be recognised as such by merchants.

Main results

105 people arrested

Multiple house searches

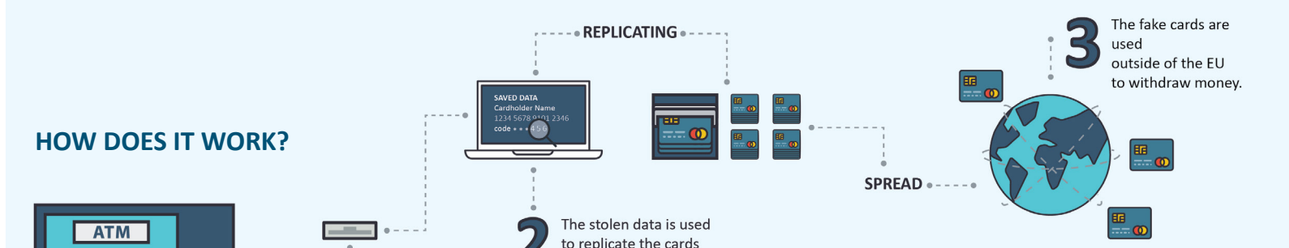
3 000 counterfeit payment cards seized

fake passports, cameras, jewellery and substantial amounts of money in cash seized

Europol capabilities and services used

- Organisation of operational meetings in Europe and Asia
- Analytical support
- Analysis of the seized data/equipment

EUR 5 million estimated loses



On 14 April 2016, the Italian Carabinieri, in close cooperation with Europol, successfully disrupted an international criminal group responsible for large-scale ATM skimming, forgery of documents and money laundering.

Modus Operandi

The primary modus operandi of the criminal network, composed mainly of Romanian nationals, was to harvest financial data from ATMs in Italy, Denmark and the UK using ATM skimming devices. This data was then used to create fake payment cards, which were used to withdraw large amounts of cash from ATMs in Indonesia and Belize.

On 18 May 2016, the French Gendarmerie of Pau, in close cooperation with the Investigative Unit of the Italian State Police of Imperia and Europol's EC3, disrupted an international criminal group responsible for large-scale ATM skimming and money laundering.

Modus Operandi

The criminal network was composed mainly of French-Italian nationals and their primary modus operandi was to harvest financial data from ATMs, with the help of ATM skimming devices, in different areas of France. The compromised card data, which was used to create fake payment cards, was stored on a cloud server managed by the members of the criminal organisation. These fake cards were used to withdraw large amounts of cash from ATMs outside the European Union (Asia and the US).

On 6 September 2016, the Italian Polizia Postale e delle Comunicazioni – in close cooperation with the Romanian DIICOT, the General Inspectorates of the Romanian Police and Gendarmerie, and Europol – disrupted an international criminal group responsible for large-scale misuse of compromised payment card data, prostitution and money laundering.

Modus Operandi

Composed mainly of Romanian nationals, the criminal network used ATM skimming devices which allowed them to compromise ATMs, as well as phishing techniques, to perform a high volume of fraudulent transactions in the area of Milan and Monza (Italy). To secure the exchange of sensitive information among the members of the criminal group, they used a digital version of the pizzino, a slip of paper used by the Italian Mafia to communicate, on encrypted internet-based communication services.

Main results

16 people arrested in Italy

Multiple house searches

Micro camera bars, card readers, magnetic strip readers and writers, computers, phones, flash drives and plastic cards ready to be encoded seized

Europol capabilities and services used

- Suspects identification
- Organisation of operational meetings
- Analytical and forensic support
- Exchange and cross-check of intelligence

EUR 1.2 million estimated loses

Main results

9 people arrested in France

Multiple house searches

Micro camera bars, card readers, magnetic strip readers and writers, computers, phones and flash drives, two hand guns, five vehicles and thousands of plastic cards ready to be encoded seized between France and Italy

Europol capabilities and services used

- Suspects identification
- Organisation of operational meetings
- Analytical and forensic support
- Exchange and cross-check of intelligence

> EUR 0.5 million estimated loses

Main results

14 people detained, 7 arrested in Italy and Romania

Multiple house searches

Micro camera bars, card readers, magnetic strip readers and writers, computers, phones and flash drives, several vehicles and thousands of plastic cards ready to be encoded seized in Romania and Italy

Europol capabilities and services used

- Deploiment of mobile office
- Organisation of operational meetings
- Analytical support and expertise
- Exchange and cross-check of intelligence

EUR several hundred thousand estimated loses

Global Airline Action Days

Two international law enforcement operations against airline fraud took place on 15-16 June and 10-15 October 2016 respectively

DID YOU KNOW?
The airline industry is estimated to lose over one billion dollars per year as a result of fraudulent online purchases of flight tickets.

They were organised through coordination centres at Europol in The Hague, INTERPOL Global Complex for Innovation in Singapore, and Ameripol in Bogota, and were supported by Canadian and US law enforcement agencies.

Participation

Representatives from airlines, online travel agencies, payment card companies, Perseuss and the International Air Transport Association (IATA) worked together with experts from Europol's EC3 to identify suspicious transactions and provide confirmation to law enforcement officers deployed in the airports. Eurojust provided support throughout the action days, together with the European Border and Coast Guard Agency (Frontex), which assisted in the detection of identity fraud, fake documents and irregular migration.

These global actions were part of a larger operation, named CICONIA ALBA, the third EU-wide Joint Action Days taking place under the EMPACT framework. The intelligence-led operational actions taking place in the framework of this operation cover several crime areas, whilst focusing on key criminal hotspots and infrastructure in the EU and beyond.

Read more about CICONIA ALBA here.

Crime facilitator

Although such global actions target fraudsters suspected of purchasing plane tickets online using compromised credit cards, fraudulent online transactions are highly lucrative for organised crime, and often facilitate more serious criminal activities including illegal immigration, trafficking in human beings, drug smuggling, and terrorism.

TIP!

Passengers should take care when purchasing airline tickets online, and be cautious of deals that are 'too good to be true'.

Know the crime: airline ticket fraud

The use of compromised credit card details is an increasingly prominent crime, with tens of thousands of criminal complaints filed in many EU countries. An increase in Card-Not-Present (CNP) fraud is apparent across almost all sectors; the purchases of physical goods, airline tickets, car rentals and accommodation with compromised cards has seen a significant increase throughout the EU. Airline companies are among the most affected by CNP fraud.

Law enforcement is now tackling this international phenomenon on a daily basis in close cooperation with the private sector. This has enhanced the trust between all involved parties, and will continue to inflict damage to the criminals involved in airline ticket fraud.

Global actions against online fraudsters in the airline sector

The coordinated Global Airport Actions targeted criminals suspected of fraudulently purchasing plane tickets online using stolen or fake credit card data.

Main results

	15-16 JUN 2016	10-15 OCT 2016
People detained, denied boarding, and questioned by police	140	193
Suspicious transactions reported	252	350
Airlines involved	74	75
Airports involved	130	189
Countries involved	43	43

The International Air Transport Association (IATA) took part in the actions, providing important fraud intelligence from its database

Austria, Bulgaria, Croatia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, United Kingdom.

Australia, Brazil, Canada, Colombia, Hong Kong, Indonesia, Malaysia, Mexico, New Zealand, Nigeria, Philippines, Qatar, Singapore, Thailand, United Arab Emirates, United States of America.

Austria, Belgium, Bulgaria, Croatia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, United Kingdom.

Australia, Brazil, Canada, Colombia, Ecuador, Hong Kong, Indonesia, Malaysia, Mexico, New Zealand, Nigeria, Panama, Philippines, Qatar, Singapore, Thailand, United Arab Emirates, United States of America.

Europol deployed specialists and equipment to locations across Europe

A dedicated team of analysts working from the **Europol operational centre** provided live access to centralised criminal intelligence databases

Aim of the actions

Target the criminal online services offering credit card credentials and fake plane tickets

Protect consumers from being duped by these criminal enterprises

Coordination centres:

INTERPOL Singapore

USA

EUROPOL / EC3 The Hague (NL)

AMERIPOL Bogotá (Colombia)

Canada

Actions against e-Commerce fraud

On 14 and 15 November 2016, the Finnish National Bureau of Investigation, the Spanish Guardia Civil, the British West Midlands Regional Cyber Crime Unit together with the Royal Canadian Mounted Police and with the support of Europol's EC3 teamed up in a cross-continental joint action day aimed at breaking down an international CNP fraud network. The operation took place simultaneously in Canada, Finland, Spain and the United Kingdom and resulted in 15 arrests.

Modus Operandi

Initiated by the Finnish authorities, the investigation uncovered that the members of the OCG had in their possession more than 6 000 credit card details, which they had used to attack more than 170 e-merchants with fraudulent activities exceeding EUR 1 million.

After making the first purchase using the stolen credit card information, the criminal network uploaded and sold the data on a website available on the deep web with the purpose of it being re-used by other criminals.

This transnational operation is particularly important as the OCG was very active in their attempts to recruit new members of a young age, as well as providing them with the technical skills needed to perform this illegal activity.

EC3 contributed to the success of the investigation by producing analytical reports and hosting earlier this year an operational meeting at Europol's headquarters in The Hague.

Main results

- **15** people arrested
- **6 000** credit card details identified
- **170** e-merchants attacked
- losses of **EUR 1 million**

Europol capabilities and services used

- Operational coordination
- Operational support
- Analytical reporting

"Payment card fraud against online shops is considered as high profit and low risk criminal activity, with losses for the European sector exceeding EUR 1 billion per year. Investigative measures are very complex due to the virtual and international dimensions of this crime. Cyber fraud is a top priority for Europol and law enforcement agencies across the European Union.'

Noting the steady increase of credit and debit card payment and online fraud, Europol's EC3 has stepped up its efforts to support large-scale cross-border investigations targeting online fraudsters.

In October 2016, 42 criminals were arrested for online fraud activities, ordering high-value goods from online shops with stolen credit card information. The individuals had performed more than 3 000 illegal online transactions through which they had purchased items worth a total of EUR 3.5 million.

Law enforcement authorities from Austria, Finland, France, Greece, Ireland, the Netherlands, Portugal, Romania, Spain, and the United Kingdom, supported by Europol, teamed up in a coordinated joint action against those criminal networks, targeting the locations where illegally purchased goods had been delivered.

Europol coordinated this operation with direct assistance from payment card schemes, banks, logistic companies and e-merchants. EC3 specialists were also deployed in the Member States with mobile offices to offer on-the-spot support to national authorities.

A large number of packages from online shops was intercepted and 120 locations were searched, using information that had been previously submitted by e-merchants, the payment industry and logistic companies. The house searches led to seizures of high-value goods, including electronic appliances, smartphones, tablets, watches and clothing.

The investigative measures also revealed that the suspects might have been involved in other forms of crime, such as ID fraud, phishing, cyber-attacks, romance fraud, the illegal use of stolen passports, illegal immigration, money laundering, and terrorism. Several new investigations have been initiated as a result of this operation.

This was the first European-wide action on e-Commerce fraud. By working together and utilising Europol's unique capabilities, law enforcement authorities from Member States were able to piece together 3 000 individual fraud investigations in to 40 international cases. Merchants and banks contributed extensively to these investigations.

Main results

- **42** people arrested
- **120** locations searched
- **3 000** illegal online transactions
- losses of **EUR 3.5 million**

Links to other forms of crime

ID fraud, phishing, cyber-attacks, romance fraud, the illegal use of stolen passports, illegal immigration, money laundering, and terrorism.

Europol capabilities and services used

- Operational coordination
- Operational support
- Networking power
- Strategic analysis
- Exchange of information – SIENA
- Operational analysis

DID YOU KNOW?

This operation followed the successful Europol-supported action led by the United Kingdom's Dedicated Card and Payment Crime Unit (DCPCU) in June 2016. Eleven people were arrested in a joint operation between DCPCU and Visa Europe, which proactively targeted remote purchase fraud. The operation saw the banking industry and retailers share live data for the first time.

Information shared by the involved organisations was used to target individuals suspected of using stolen card details to purchase high value goods. Items seized by officers included a cinema system, computers, mobile devices, designer clothes, kitchen equipment, gaming goods, and two machetes. The total value of fraudulent activity was more than EUR 280 000.

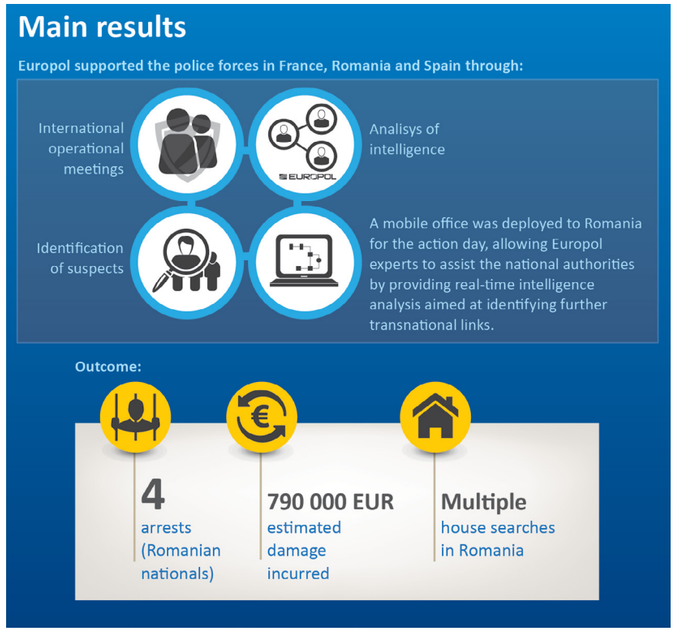
The operation is a practical continuation of the work of the e-Commerce Working Group, a private-public partnership network established in 2013 with the key stakeholders, including the Merchant Risk Council, a network of 450 e-merchants.

Physical attacks on ATMs

On 6 April 2016, the Romanian National Police and the Directorate for Investigating Organised Crimes and Terrorism (DIICOT), in cooperation with the French Police and Gendarmerie Nationale and the Spanish Policia Nacional, disrupted a criminal network responsible for physical attacks on ATMs throughout Europe. Supported on-the-spot by Europol experts, the operation was preceded by extensive criminal investigations coordinated by Europol and Eurojust.

Modus Operandi

Active in France and other European countries in 2014-2015, the criminal network's modus operandi involved the use of sledgehammers and angle-grinders to attempt to open ATMs.



Operation Avalanche

On 30 November 2016, after more than four years of investigation, the Public Prosecutor's Office Verden and the Lüneburg Police (Germany) in close cooperation with the United States Attorney's Office for the Western District of Pennsylvania, the Department of Justice and the FBI, Europol, Eurojust and global partners, dismantled an international criminal infrastructure platform known as 'Avalanche'.

The Avalanche network was used as a delivery platform to launch and manage mass global malware attacks and money mule recruiting campaigns. It has caused an estimated EUR 6 million in damages in concentrated cyber-attacks on online banking systems in Germany alone. In addition, the monetary losses associated with malware attacks conducted over the Avalanche network are estimated to be in the hundreds of millions of euros worldwide, although exact calculations are difficult due to the high number of malware families managed through the platform.

The global effort to take down this network involved the crucial support of prosecutors and investigators from 30 countries. As a result, 5 individuals were arrested, 37 premises were searched, and 39 servers were seized. Victims of malware infections were identified in over 180 countries. Also, 221 servers were put offline through abuse notifications sent to the hosting providers.

On the action day, Europol hosted a command post at its headquarters in The Hague. From there, representatives of the involved countries worked together with Europol's EC3 and Eurojust officials to ensure the success of such a large-scale operation.

"The operation marks the largest-ever use of sinkholing to combat botnet infrastructures and is unprecedented in its scale, with over 800 000 domains seized, sinkholed or blocked.'

DID YOU KNOW?

What made the 'Avalanche' infrastructure special was the use of the so-called double fast flux technique. The complex setup of the network was popular amongst cybercriminals because of this technique offering enhanced resilience to takedowns and law enforcement action.

Download the double fast flux infographic here.

In addition, Europol supported the German authorities throughout the entire investigation by assisting with the identification of the suspects and the exchange of information with other law enforcement authorities. Europol's cybercrime experts produced and delivered analytical products.

The criminal groups have used the Avalanche infrastructure since 2009 for conducting malware, phishing and spam activities. They sent more than 1 million e-mails with damaging attachments or links every week to unsuspecting victims.

The investigations commenced in 2012 in Germany, after an encryption ransomware (the so-called Windows Encryption Trojan), infected a substantial number of computer systems, blocking users' access. Millions of private and business computer systems were also infected with malware, enabling the criminals operating the network to harvest bank and e-mail passwords.

With this information, the criminals were able to perform bank transfers from the victims' accounts. The proceeds were then redirected to the criminals through a similar double fast flux infrastructure, which was specifically created to secure the proceeds of the criminal activity.

The loss of some of the network's components was avoided with the help of its sophisticated infrastructure, by redistributing the tasks of disrupted components to still-active computer servers. The Avalanche network was estimated to involve as many as 500,000 infected computers worldwide on a daily basis.

The successful takedown was supported by INTERPOL, the Shadowserver Foundation, Registrar of Last Resort, ICANN and domain registries. Several antivirus partners provided support concerning victim remediation.

Malware campaigns that were distributed through this network include around 20 different malware families such as goznym, marcher, matsnu, urlzone, xswkit, and pandabanker.

The money mule schemes operating over Avalanche involved highly organised networks of "mules" that purchased goods with stolen funds, enabling cyber-criminals to launder the money they acquired through the malware attacks or other illegal means.

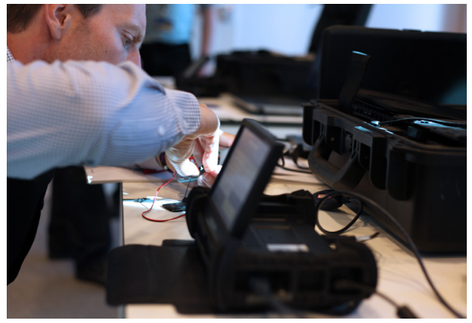
2 | EC3 Operations
EC3 Forensic Laboratory

Though the EC3 Laboratory has been busy supporting major cases in 2016 ranging from advanced cyber cases to major counter terrorism investigations, it managed to deliver several forensic extraction training courses for mobile devices.

Being a major challenge for EU law enforcement, mobile devices remain a difficult area of examination. Europol delivers on the spot support in this field but the growing demand from the Member States demanded a major enhancement of the internal capabilities. Important hardware and software resources have been invested towards this key mission and more than 60 Staff have been trained and certified in the different units of Europol to be sure the support given is as close as possible to the needs of investigations and also as forensically relevant as possible. Strict methods and policies have been implemented to ensure top quality of the reports delivered.

Examination of a several thousands of phones, tablets and GPS devices have been delivered by Europol directly at the point of arrest or on the crime scene bringing quality evidence to courts in a timely manner.

Examination of a several thousands of phones, tablets and GPS devices have been delivered by Europol directly at the point of arrest or on the crime scene bringing quality evidence to courts in a timely manner.



2 | EC3 Operations
Technical workshop on decryption

With the support of EC3 and other law enforcement authorities from the EU, the JRC is exploring new forensic techniques to improve password recovery processes in full compliance with the EU regulatory framework.

On 6 and 7 June 2016 in Ispra, Italy, Europol's EC3 and the European Commission's Joint Research Centre (JRC) jointly organised a technical workshop on best practices relating to decryption in law enforcement. The workshop took place in the framework of an EC3-JRC collaboration on fighting cybercrime, terrorism and organised crime.

With the support of EC3 and other law enforcement authorities from the EU, the JRC is exploring new forensic techniques to improve password recovery processes in full compliance with the EU regulatory framework.

Several Member States shared best practices and techniques leading to successful investigations. In particular, advanced mathematical modelling supported by machine learning processes was discussed in order to ensure higher success rates of decryption during investigations.

3 | Prevention & Awareness
No More Ransom

www.nomoreransom.org

On 25 July 2016, Europol, the Dutch National Police, Intel Security, and Kaspersky Lab joined forces to launch No More Ransom, a new step in the cooperation between law enforcement and the private sector to fight ransomware together. Ransomware is a type of malware that locks the victim's computer or encrypts their data, demanding them to pay a ransom to regain control over the affected device or files.

NO MORE RANSOM!

The initiative set up on online portal aimed at informing the public about the dangers of ransomware, how it works, and how to protect themselves. The portal contains 160 000+ keys to help victims recover data that has been locked by cybercriminals and offers the option to report a crime, directly connecting with Europol's overview of national reporting mechanisms.

The project has been envisioned as a non-commercial initiative, aimed at bringing public and private institutions under the same umbrella.

Public-Private cooperation

Since the successful launch of the initiative, law enforcement agencies from a further 22 countries have signed up to fight ransomware together with the private sector.

The new members are: Austria, Bosnia and Herzegovina, Bulgaria, Croatia, Colombia, Denmark, Finland, France, Hungary, Ireland, Italy, Latvia, Lithuania, Malta, Portugal, Romania, Singapore, Slovenia, Spain, Switzerland, and the United Kingdom.

The project's objectives are supported by Eurojust, the European Commission, CERT-EU and eu-LISA (the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice)

INTERESTED?
nomoreransom@europol.europa.eu

Initial results

Until now, over 6 000 people have successfully managed to decrypt their devices without having to pay the criminals, by using the main decryption tools on the platform (CoinVault, Rakhni, WildFire and Shade). This has deprived cybercriminals of an stimated couple of million Euros in ransoms.

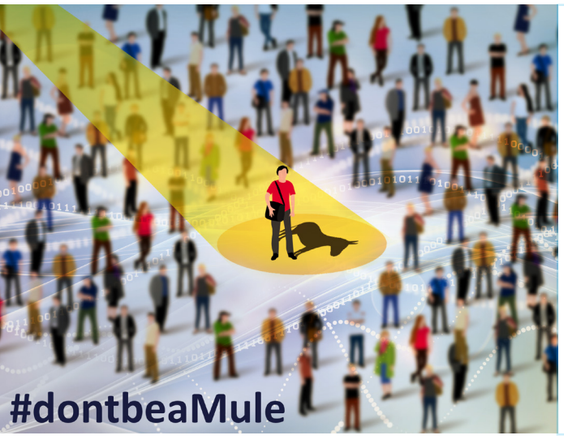
The more law enforcement agencies and private sector partners work together, the more decryption tools can be created and made available. More than 30 partners from private sector and the CERT community joined in December this year, with Bitdefender, Check Point, Emsisoft and Trend Micro bringing to the portal new and valuable decrytion tools to reinforce the service provided to victims.

Latest developments

- New decryption tools
- Portal available in other languages than English
- Enlargement to partners from private sector

"Ransomware is a top threat for EU law enforcement: almost two-thirds of EU Member States are conducting investigations into this form of malware attack, and the number of victims is increasing. While the target is often individual users' devices, corporate and even government networks are affected as well.'

European Money Mule Action(s) - EMMA



Money mules are individuals recruited by criminal organisations to receive and transfer illegally obtained money between bank accounts and/or countries. Through the money mules, the criminals gain access to the stolen goods or funds without revealing their identity.

The recruited individuals may be willing participants, however some are unaware that their actions foster the cycle of criminal activity. Money mules may also help perpetuate other crimes beyond money laundering as the stolen money might go towards funding other forms of organised crime, such as drug dealing and human trafficking.

The European Money Mule Actions (EMMA) are operational projects under the flag of EMPACT Cybercrime Payment Fraud Operational Action Plan, designed to combat online and payment card fraud. EMMA is modelled after a Dutch example successfully employed in recent years in the Netherlands. These actions build upon the effective partnership between the police, the prosecution and the banking sector at the national as well as the international level.

From all reported money mule transactions in the scope of these operations, 90-95% were linked to cyber-enabled criminal activity.

This successful multisectoral model against money muling combines the operational efforts to identify and arrest the mules with a multilingual prevention campaign in all the participating countries in order to raise awareness about this criminal phenomenon both to the international, as well as the national audiences.

The operatios were supported by Europol's EC3, Eurojust and the European Banking Federation (EBF).

Awareness material in 13 languages!

Read more about money muling on our dedicated webpage.

Main results

	EMMA 1 Operational week: 22-26 Feb. Awareness week: 1-4 Mar.	EMMA 2 Operational week: 14-18 Nov. Awareness week: 22-25 Nov.
participating countries	8 Belgium, Denmark, Greece, the Netherlands, Portugal, Romania, Spain and UK (with further support from Moldova)	17 Bulgaria, Croatia, France, Germany, Greece, Hungary, Italy, Latvia, Moldova, the Netherlands, Poland, Portugal, Romania, Spain, UK, Ukraine and USA (FBI and Secret Service)
money mules identified	700	580
suspects interviewed	198	380
people arrested	81	178
supporting banks	70	106

#MobileMalware

Mobile devices such as smartphones or tablets have become ingrained in our daily lives. Technology which was once only found on desktop computers can now be carried in the palm of one's hands. Yet as the popularity of these devices explodes, the appetite of cybercriminals targeting these devices has grown too. The risk of mobile malware is real: hackers can steal money and sensitive information, use these devices as bots and even spy on your activities. Unfortunately, most people have not realised the importance of protecting their mobile devices from such attacks.

To raise awareness among users, Europol's EC3 led a joint Mobile Malware Awareness Campaign as part of the European Cyber Security Month 2016.

Over the course of one week (from 24 to 28 October), 22 EU Member States (Austria, Belgium, Croatia, Cyprus, Czech Republic, Hungary, Ireland, Italy, France, Germany, Greece, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovenia, Spain, and the United Kingdom), 3 non-EU countries (Colombia, Norway and Ukraine) and 2 EU agencies (ENISA and eu-LISA) in cooperation with numerous public and private partners raised awareness about this criminal phenomenon and its consequences. The range of activities included press conferences, school lectures, educational workshops and training courses, online quizzes, and live chats on social media.

This was accompanied by a massive communication campaign via social media channels and national law enforcement websites.

DON'T MISS IT!

To help people better protect their mobile devices from cybercrime, Europol's EC3 has developed awareness-raising materials available for public download in 20 languages**.** It provides an overview of the threat and key vulnerabilities of the mobile devices. A set of tips explains how to securely perform everyday activities such as downloading apps, internet banking, and connecting to WI-FI, whilst showing individuals how to avoid becoming a victim of mobile ransomware.

As Europol's 2016 Internet Organised Crime Threat Assessment shows, mobile malware features firmly in law enforcement investigations in 14 European countries.

Over 45 partners from the internet security industry, financial institutions, national Ministries, and CERTs (Computer Emergency Response Teams) supported this campaign at national level.

EUROPEAN CYBER SECURITY MONTH

October 2016 was the European Cyber Security Month, which started with a kick-off event in Brussels hosted by the European Banking Federation. Representatives from the EU public sector, national co-ordination teams, and the banking industry gave insights into the month long campaigns. Europol's EC3 chaired a dedicated panel on mobile malware, together with leading IT and banking security specialists.

Read more about how to stay protected from mobile malware on our dedicated webpage.

This awareness campaign was part of the EMPACT Operational Action Plan 2016 of the Cybercrime sub-priority of Cyber Attacks. The campaign was coordinated by Europol with the close support of the Cyber Crime Division of the Hellenic Police.

3 | Prevention & Awareness

Mock Retail Cyber Hack Excercise

On 1 December 2016, Europol's EC3 hosted a Mock Retail Cyber Hack exercise in cooperation with MasterCard, intended to simulate a cyber-attack on European merchants. The event focused on providing first-hand experience to merchant customers and their acquirers in order to understand the steps to follow in case of a cyber-attack and to raise awareness of the issue.

The initiative brought together representatives from law enforcement, the retail industry, banking sector, forensic investigation field, Dutch Electronic Crimes Task Force (ECTF) and Dutch Computer Emergency Response Team (CERT).

Since cybercriminals are increasingly targeting European merchants, Europol's EC3 considers collaborations such as this an efficient approach to promote best practices in dealing with cyber-attacks, as well as familiarising the affected parties with all the actors involved at each step of the investigation.

The Mock Retail Cyber Hack also aims at creating a network of trusted contacts to facilitate information exchange regarding rising cyber threats. The simulation seeks to iron out the inconsistencies in order to ensure that the e-Commerce environment becomes more secure.

Through this training, participants learned:

- what their particular role is and who can provide assistance and advice in case a cyber hack occurs;
- how to deal with threats such as infiltration to the payment system or denial of service (DoS) attacks.

In general, they benefited from tailored briefings from industry and law enforcement experts concerned with mitigating, investigating and assisting in the event of a cyber hack.

Read more about young cybercriminals on our dedicated webpage.

Awareness material in 8 languages!

3 | Prevention & Awareness

Operation TARpit

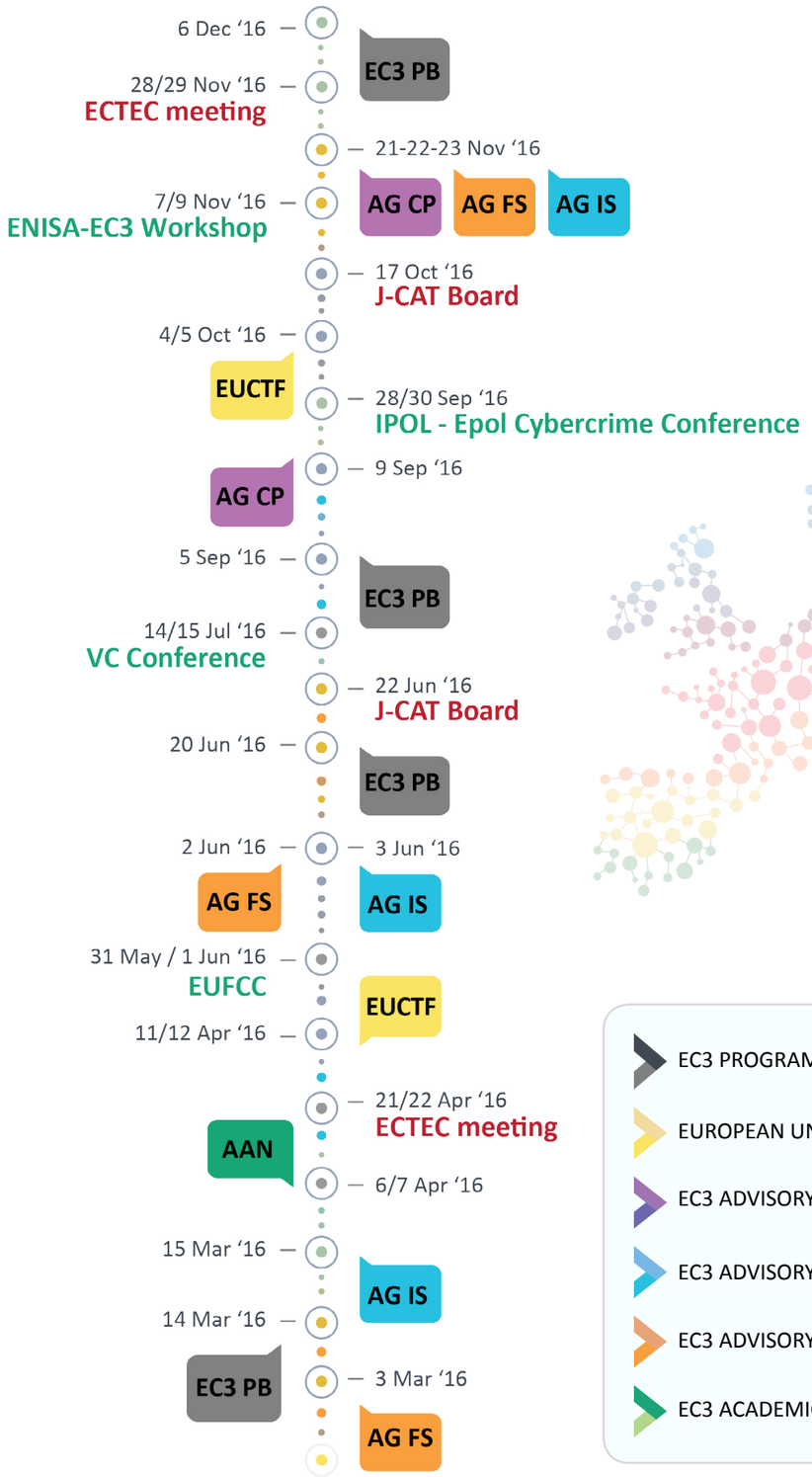
From 5 to 9 December 2016, Europol and law enforcement authorities from 13 countries carried out a coordinated action targeting users of Distributed Denial of Service (DDoS) cyber-attack tools.

The individuals arrested, mainly young adults under the age of 20, are suspected of paying for stressers and booters services to maliciously deploy software to launch DDoS attacks, which flood websites and web servers with massive amount of data, leaving them inaccessible to users.

This operation was followed by a prevention campaign to raise awareness of the risk of young adults getting involved in cybercrime. These teenagers often have a skill set that could be put to a positive use. Skills in coding, gaming, computer programming, cyber security or anything IT-related are in high demand and there are many careers and opportunities available to anyone with an interest in these areas.

4 | Strategy and Outreach

EC3 Governance & Advisory meetings



- EC3 PROGRAMME BOARD (PB)
- EUROPEAN UNION CYBERCRIME TASKFORCE (EUCTF)
- EC3 ADVISORY GROUP ON COM. PROVIDERS (CP)
- EC3 ADVISORY GROUP ON INTERNET SECURITY (IS)
- EC3 ADVISORY GROUP ON FINANCIAL SERVICES (FS)
- EC3 ACADEMIC ADVISORY NETWORK (AAN)

4 Strategy and Outreach

Internet Governance: Preventing the criminal abuse of the Internet Infrastructure

EC3 represents and promotes the views of the European law enforcement community in the global discussion on the governance of the Internet, which takes place in the framework of different Internet Governance organisations such as ICANN, RIPE, IETF and others. EC3 participates in the development of new policies, standards and norms adopted by those organisations in order to support the ability of law enforcement organisations to investigate, prevent, attribute and disrupt unlawful activity online and to reduce the criminal abuse of the global internet infrastructure, in particular the Domain Name System (DNS) and the Internet Protocol (IP) addresses. In 2016 EC3 has focused its efforts on improving accountability in both in the Domain Name System (DNS) and in the IP space.

ICANN and the DNS WHOIS

As one of the funding members of the Public Safety Working Group (PSWG) of ICANN - the organisation which operates the Internet's DNS and accredits generic top-level domain (gTLD) name registrars - EC3 was appointed to represent the law enforcement community in a policy development process whose aim is to replace the DNS WHOIS database.

The DNS WHOIS is a publicly available directory containing the contact details of all registered domain name holders (registrants). Anyone who needs to know who is behind a domain name can find this information in the database. The WHOIS is a critical element of online accountability and accurate DNS WHOIS information is essential to investigate and attribute abuse and unlawful activity online. It is used by a multitude of stakeholders such as intellectual property and trademark owners to identify owners of websites infringing their trademarks, consumer protection authorities tracking down websites selling counterfeited products, but also law enforcement authorities who use the WHOIS to get information on individuals involved in criminal activities based on the abuse of the domain name system such as distributing malwares, conducting spam campaigns or controlling botnets.

However, despite a number of ICANN contractual obligations to ensure accurate WHOIS information, bad actors have found many ways to register domain names anonymously and registrars (companies selling domain names to individuals) do not always validate and authenticate clients registering new domains in the WHOIS.

This activity is directly relevant for the work of EC3 operations department. In one of the latest operations coordinated by EC3 - Operation Avalanche - LEA took down of a large criminal infrastructure used to conduct malware, phishing, spam and money laundering campaigns. The infrastructure was very difficult to track because it relied on an evasion technique called "fast flux" which is used to quickly move domain names from a set of computers to another one. Those domains are not only registered for malicious purposes but the fast flux technique could be prevented if registrars would do better authorisation and authentication of clients making those rapid changes - which are typical of the fast flux technique.

As one of the funding members of the Public Safety Working Group (PSWG) of ICANN - EC3 was appointed to represent the law enforcement community in a policy development process whose aim is to replace the DNS WHOIS database.

Globally coordinated initiative with the 5 RIRs

In 2016, EC3 has also launched a new initiative aiming at the five Regional Internet Registries (RIRs) and in particular RIPE NCC which manages the allocation and registration of IP addresses and autonomous system (AS) numbers in Europe, Central Asia and the Middle East.

RIPE maintains the RIPE database which contains contact information on ISPs which hold and allocate IP addresses. The RIPE database is publicly available and it is an essential tool for investigators because it helps to identify the owner of IP addresses that is abused to carry out fraud, malware distribution or spam. However, the databases maintained by the five RIRs are often inaccurate which leads to severe delays in investigations.

Europol and the FBI have therefore launched a globally coordinated initiative to improve the accuracy of these databases. In order to influence the process, EC3 has attended meetings of the RIPE community in May and in October to present different cases of investigations hindered by the inaccuracy of the information provided in these databases. Other LEA agencies around the world have engaged with their respective RIRs.

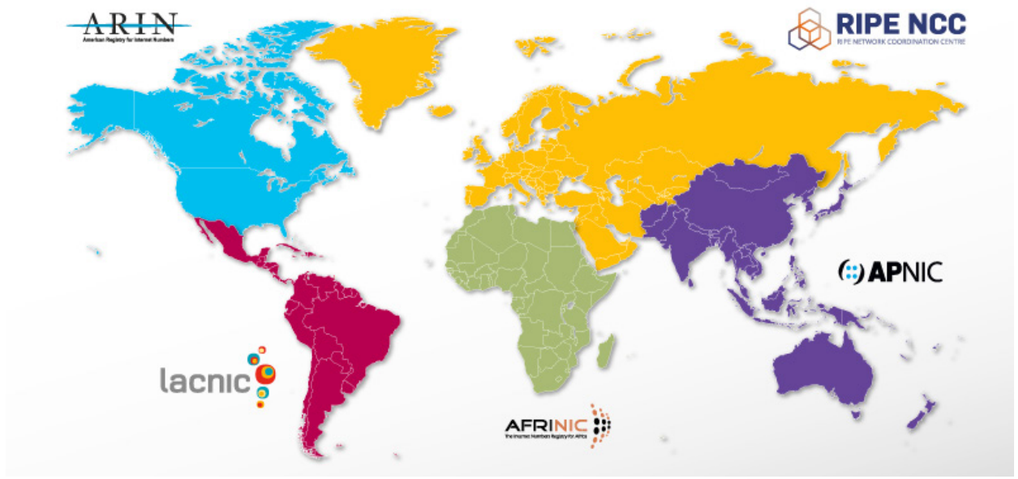
The Costa Rican Police presented at LACNIC in September 2016 while the Sri Lankan police attended APNIC. The FBI and the Canadian Police presented a case study at ARIN and the Mauritius Police and the African Union spoke at AfriNIC.

DID YOU KNOW?

In 2017, EC3 will present a proposal to change the policy of the RIPE community and other partner organization will do the same around the globe. They will then actively work to get those changes adopted by the respective communities. In order to further improve the cooperation with RIPE EC3 concluded a Memorandum of Understanding in December 2016.

Improving accountability mechanisms in the field of Internet Governance

These efforts to improve the adoption of a policy frameworks that prevent the abuse of the most important critical internet infrastructure will continue in 2017. Improving accountability mechanisms in the field of Internet Governance contribute to discourage criminals by making it more costly and more difficult to carry out cybercrime.



The role of public - private partnerships EC3's Advisory Groups

EC3 used this opportunity to revise the terms of reference for the groups with a view to making them even more action- and result driven.

The EC3 Programme Board identified the need for establishing Advisory Groups to provide guidance and support.

Public -private partnerships are at the heart of the successful response to the challenges and threats posed by cybercrime, which call for close cooperation across various sectors and at multiple levels to share relevant intelligence in a lawful manner, pro-actively exchange best practices, knowledge and expertise, and plan and execute joint action. This is reflected in the 2013 communication by the Programme Board of Europol's European Cybercrime Centre (EC3) which identified the need for establishing Advisory Groups to provide guidance and support the work of EC3 in general.

The first two groups were established in the areas of Financial Services and Internet Security. Since their establishment, the members of the AGs and EC3 have created an environment that is characterised by trust, mutual respect and recognition for the importance of a complementary and cooperative approach in the fight against cybercrime. This has resulted in several strategic and tactical products as well as initiatives that have benefited from the support by the AGs. This year a third group was established, focussing on the cooperation between law enforcement and Communication Providers.

In addition to the three AGs, EC3 also maintains a cybercrime prevention network and an academic advisory network.

EC3 used this opportunity to revise the terms of reference for the groups with a view to making them even more action- and result driven.

The idea behind it is to maximise the impact of the investments by the members and EC3 into these partnerships and to leverage the personal commitment and networking power that the members offer. An important step in achieving this was to deepen the involvement of EC3 Operations which has been essential in identifying concrete projects and activities for 2017 and beyond. These planned activities, which have been synchronised across the various groups to the extent possible and also consider the EMPACT OAPs for next year, have been specified in separate work plans and linked to concrete delvierables. This will help to not only manage expectations but also channel resources and efforts most effectively.

4th INTERPOL-Europol Cybercrime Conference

"Cybercrime remains a real and innovative threat. It evolves over the years and so does the cooperation between Europol and INTERPOL - to look at ways of combating the criminals together. The joint Cybercrime Conference is a yearly milestone. We look back to learn the most pressing threats and trends, and then forward to identify how to keep citizens, business and governments protected."

Steven Wilson, Head of EC3

Under the theme "Solutions for Attribution", some 200 delegates from 56 countries shared best practices and identified ways to overcome technical, operational and strategic hurdles faced by law enforcement when investigating cybercrime and cyber-enabled crimes. Focus was put particularly put on financial crime, terror-related activities and child sexual abuse.

Next edition: 27 to 29 September 2017, at Europol's headquarters in The Hague.
Theme: *To be announced.*

Cyber specialists from law enforcement, the private sector and academia met in Singapore from 28 to 30 September 2016 to address the challenges of identifying those responsible for crimes committed in cyberspace.

Topics such as ransomware and bulletproof hosting were also at the top of the conference agenda.

Enhanced private-public partnerships, the reshaping of information sharing agreements and the further development of regionally-focused capacity building programmes were identified as key areas for future efforts.

INTERPOL-EUROPOL CYBERCRIME CONFERENCE
28-30 SEPTEMBER 2016
SINGAPORE

Conference conclusions:

1. Law enforcement agencies and private sector companies to consider and find **solutions to address respective constraints when investigating cybercrime**;

2. **Supporting user-focused initiatives** such as 'No more ransom', a multi-stakeholder project which aims to help victims of ransomware retrieve their encrypted data without paying their attacker;

3. INTERPOL and Europol to **support existing entities in their establishment of regional cyber centres** via capacity building and information sharing.

The 2016 Internet Organised Crime Threat Assessment (IOCTA), the annual report on the cybercrime threat landscape prepared by Europol's EC3, was officially announced at the conference and released to the public afterwards.

3rd Virtual Currencies Training

Virtual currencies and other emerging instruments supported by blockchain and distributed ledger technology bring innovation and have the potential to revolutionise how public and private sectors are providing their services. The more these services are deployed and create value, the more they will be the target of malicious activities by criminals. This presents particular challenges for judicial investigations; the fast growing and emerging characteristics of these technologies can jeopardise the prosecutions of such types of cybercrime.

The third edition of the Virtual Currencies Training was held on 14 and 15 July 2016. The training was organised by Europol's Cybercrime Centre (EC3) at Europol headquarters in The Hague, following the success of the previous two editions. The event brought together over 90 experts from various regions of the world. Most participants were representatives from law enforcement authorities, in particular from EU Member States, but several US law enforcement agencies, the Swiss Police Cybercrime Division, and the Royal Canadian Mounted Police also took part. Furthermore, there were leading experts from several commercial and non-for-profit organisations that are active in the field of facilitating the lawful use of virtual currencies.

The aim of the conference was to further strengthen the fight against the abuse of virtual currencies for criminal transactions and money laundering. Experts from law enforcement and the private sector shared their insights regarding criminal trends, and the latest techniques used by criminals and terrorists to hide their financial tracks – how they cash out criminal proceeds using Bitcoins and various other digital currencies. The latest cutting-edge technology solutions for tracing blockchain transactions in criminal investigations were presented, and best practices and law enforcement techniques were shared.

The conference addressed the latest trends in compliance, presented by the Financial Crimes Enforcement Network (FinCEN), and the invited virtual currency exchangers demonstrated their best practices in implementing Anti Money Laundering policies and mechanisms, as well as risk-based approaches to suspicious transactions.

The event offered opportunities for closer cooperation and new partnerships to prevent and fight cybercrime and money laundering, as well as facilitate asset recovery.

On 28 June 2016 in Brussels, Europol's European Cybercrime Centre (EC3) and the European Commission's Joint Research Centre (DG JRC) jointly organised a workshop on Virtual Currencies, in the context of the fight against fraud and counterfeiting of non-cash means of payments.

The workshop brought together participants from the Commission, academia, industry, and EU law enforcement with the objective of analysing emerging cases of fraud and counterfeiting, targeting Virtual Currencies and evaluating their possible contribution to the revision of the 2001 Council Framework Decision (2001/413/JHA). This was in order to enable an effective and solid prosecution of such new type of criminal activities.

Conference on privacy and security online

On 19-20 May 2016, Europol in cooperation with the European Institute of Public Administration organised a conference on privacy in the digital age of encryption and anonymity online. The event provided an opportunity to have an open, inclusive and transparent debate amongst different view holders, with the aim of finding a way to strike the right balance between freedom and security online.

The conference saw participation from different organisations such as the European Data Protection Supervisor, the Europol Joint Supervisory Body, the EU Agency for Network and Information Security (ENISA), Eurojust, Amnesty International, the EastWest Institute, and many others from a broad range of professional backgrounds, representing private industry, academia, privacy advocates, and law enforcement.

In several high-level discussion panels and workshops, lively discussions took place on the polarising challenges around privacy versus security online, and the need to protect citizens' privacy whilst giving law enforcement the means to investigate crime. There was a general consensus that the availability and use of encryption and anonymity technologies is not only important and legitimate in many circumstances, but also essential to a secure and safe cyberspace.

One of the main themes conveyed at the conference was the challenge that encryption and anonymity online presents for law enforcement. Whilst there is a clear support for strong encryption, and the opposing of any technical solution that would weaken security in cyberspace for everyone, it was made clear that the criminal abuse of these technologies must be addressed. This abuse seriously impedes on law enforcement's ability to protect citizens from criminal and extremist behaviour, and to then bring those responsible to justice.

Read here the ENISA-Europol joint statement on lawful criminal investigation that respects 21st Century data protection.

3rd EU Financial Cybercrime Coalition

On 31 May and 1 June 2016, the third conference of the EU Financial Cybercrime Coalition (EUFCC) was hosted at Europol with the aim of further strengthening the cooperation between EU law enforcement and the financial sector.

Participation at this annual event has grown steadily in time, so that by its third iteration in 2016, more than 150 professionals in total attended – approximately two thirds represented financial institutions from 20 EU Member States, and 5 were Non-EU Cooperation Partners.

The Members of the EC3 Advisory Group on Financial Services were an integral part of the organisation and the success of the EUFCC conference. The presentations at the conference provided an overview of the most pertinent threats affecting banks and payment systems, and those that might impact upon them in the future.

Conclusions

- Operational successes were highlighted; new financial sector/law enforcement cooperation structures were shared with participants as examples of best practice for developing modern partnerships between these two sectors.
- The event resulted in several proposed initiatives aimed at enhancing the sharing of intelligence to further improve and better target international law enforcement cooperation.
- Based on the positive feedback received, EC3 will continue to support the organisation of EUFCC conferences in the future.

5th ENISA-EC3 Workshop between CSIRTs and law enforcement agencies

"Close cooperation and information sharing between Law Enforcement and the CSIRT community is the best way to ensure a safer cyberspace for European business and private citizens. This joint workshop is intended to explore better ways of working together to collectively tackle the cyber threat.'

Steven Wilson
Head of EC3
Europol

On 7 and 8 of November 2016, on the occasion of the fifth ENISA/EC3 Workshop EU Law Enforcement Agencies (LEAs) and their CSIRT (Computer Security Incident Response Team) counterparts convened at Europol's headquarters in The Hague for a two-day workshop focusing on "Information: From Taxonomy to a Sharing Mechanism".

Goal

The main purpose of this year's workshop consisted of fostering better cooperation between national/governmental CSIRTS and EU Law Enforcement agencies, with the aim of establishing a network able to discuss topics of interests to both law enforcement investigators and CSIRT operators alike, such as information exchange and policy elements affecting the activities of both sides.

Cooperation

In 2014, Europol and ENISA signed a strategic cooperation agreement aimed at facilitating the exchange of knowledge and expertise, as well as the cooperation between the two agencies in order to offer support to EU Member States in tackling cybercrime.

Strategic meeting on Payment Card Fraud

On 22-23 March 2016 Europol's EC3 and ASEANAPOL, with the cooperation of INTERPOL and the support of the Romanian National Police and the Royal Malaysian Police, organised the second strategic meeting on Payment Card Fraud (PCF) in Kuala Lumpur, Malaysia.

This two-day meeting brought together 25 law enforcement officers from the EU Member States Bulgaria, Germany, Greece, Romania, and the United Kingdom with their counterparts from the ASEANAPOL community, which included Brunei, Cambodia, Indonesia, Malaysia, Myanmar, Philippines, Singapore, Thailand, and Vietnam, to discuss cooperation in preventing and combating this type of crime. The private sector was represented by the European ATM Security Team (EAST), which provided the law enforcement community with a comprehensive overview of the ATM fraud and its migration to Asia.

The aim of this event was to increase awareness among experts about all types of non-cash means of payment, including card skimming, ATM malware, internet fraud, and e-Commerce fraud.

New and unreported modus operandi recently detected by different investigative units were shared between experts, and cases involving European criminals active in Asia were discussed, which resulted in the elaboration of operational plans for coordinated actions in the close future.

A third meeting will take place in Bangkok (Thailand) on 13-14 December 2016.

The aim of this event was to increase awareness among experts about all types of non-cash means of payment, including card skimming, ATM malware, internet fraud, and e-Commerce fraud.

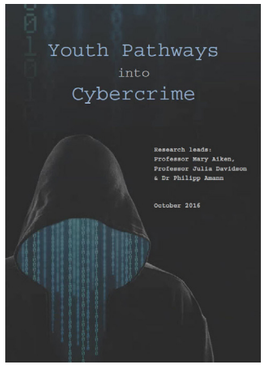
DID YOU KNOW?

On 8 November 2016, during the 85th INTERPOL General Assembly organised in Bali, the Deputy Director Operations at Europol, Wil van Gemert, and the Executive Director of the ASEANAPOL Secretariat, Brigadier General Yohanes Agus Mulyono signed a Letter of Intent aimed at strengthening the cooperation between the two organisations, providing mutual support, as well as facilitating the exchange of best practices and expertise in their areas of interest.

"Cooperating closely with ASEANAPOL will allow the agency to gain a better understanding and mitigate in a more efficient manner security threats present or originating from the region'

Wil van Gemert
Europol

5 What's new?
Youth Pathways into Cybercrime



After 11 months of initial research, this white paper by Europol, Middlesex University and UCD Geary Institute for Public Policy was published in October 2016.

Paladin Capital Group funded the project, which was led by Professor Mary Aiken and Professor Julia Davidson with the support of Europol's EC3.

The research draws together existing, recent evidence on online behaviour and associations with criminal and antisocial behaviour amongst young people. Specifically, it was designed to explore the trajectories and pathways that lead to 'cyber-criminality' through a series of mixed-methodological endeavours and the integration of theoretical frameworks across criminology and psychology, including cyberpsychology and computer science.

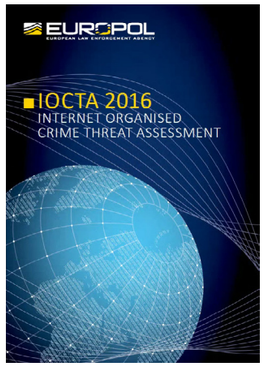
It highlights the implications for youth who engage in criminal hacking behavior, for parents/caregivers of those youths, and for persons involved in related matters of policing and practice. It provides key recommendations for policy and training, along with multi-disciplinary prevention, intervention, and deterrence measures.

The report concludes with recommendations for further research to examine addictive type behaviors associated with youth hacking, along with collaboration between, and proactive work with, industry, educators, and reformed young hackers to develop a prototype educational awareness program that can be piloted and evaluated in schools.

INTERESTED?

Download it here.

5 What's new?
IOCTA 2016



Europol's 2016 Internet Organised Crime Threat Assessment (IOCTA) is produced by the European Cybercrime Centre (EC3) at Europol. It informs decision-makers at strategic, policy and tactical levels in the fight against cybercrime, and focuses on three crime areas: cyber-attacks, child sexual exploitation online and payment fraud.

The 2016 IOCTA provides a predominantly law enforcement-focused assessment of the key developments, changes and emerging threats in the field of cybercrime over the last few years. It is based on contributions by EU Member States and the expert input of Europol's staff, which has been further enhanced and combined with input from Europol's partners in private industry, the financial sector and academia.

A key role for the IOCTA is to inform priority setting for the operational action plans in the framework of the European Multidisciplinary Platform Against Criminal Threats (EMPACT).

The 2016 IOCTA identifies an expanding cybercriminal economy exploiting our increasingly internet-enabled lives and low levels of digital hygiene.

Informed largely by Europol's law enforcement and cooperation partners, the report identifies eight main cybercrime trends and provides key recommendations to address the challenges.

READ MORE?

Download the PDF document.

Access the IOCTA online version.

THE EIGHT MAIN CYBERCRIME TRENDS:

1 Crime-as-a-Service

The digital underground is underpinned by a growing Crime-as-a-Service model that interconnects specialist providers of cybercrime tools and services with an increasing number of organised crime groups. Terrorist actors clearly have the potential to access this sector in the future.

2 Ransomware

Ransomware and banking Trojans remain the top malware threats, a trend unlikely to change for the foreseeable future.

3 The criminal use of data

Data remains a key commodity for cyber-criminals. It is procured for immediate financial gain in many cases but, increasingly, also acquired to commit more complex fraud, encrypted for ransom, or used directly for extortion.

4 Payment fraud

EMV (chip and PIN), geo-blocking and other industry measures continue to erode card-present fraud within the EU, but logical and malware attacks directly against ATMs continue to evolve and proliferate. Organised crime groups are starting to manipulate or compromise payments involving contactless (NFC) cards.

5 Online child sexual abuse

The use of end-to-end encrypted platforms for sharing media, coupled with the use of largely anonymous payment systems, has facilitated an escalation in the live streaming of child abuse.

6 Abuse of the Darknet

The Darknet continues to enable criminals involved in a range of illicit activities, such as the exchange of child sexual exploitation material. The extent to which extremist groups currently use cyber techniques to conduct attacks are limited, but the availability of cybercrime tools and services, and illicit commodities such as firearms on the Darknet, provides opportunity for this to change.

7 Social engineering

An increase of phishing aimed at high value targets has been registered by enforcement private sector authorities. CEO fraud, a refined variant of spear phishing, has become a key threat.

8 Virtual currencies

Bitcoin remains the currency of choice for the payment for criminal products and services in the digital underground economy and the Darknet. Bitcoin has also become the standard payment solution for extortion payments.

5 What's new?
Update on the Virtual Global Taskforce (VGT)

Representatives from Europol's EC3 attended the VGT Board of Management meeting, held on 28-30 November 2016 in Bern (Switzerland) lead by the UAE Ministry of Interior, the current Chair of the Virtual Global Taskforce.

Goal

To face crime on the international level and to set up coordinated actions to eliminate child abuse material from the internet worldwide.

In 2017, Europol will host the winter meeting of the VGT group

During the sessions, several topics related to child protection were discussed, among others:

- abuse and online exploitation,
- combating violation of child rights,
- developing mechanisms of joint work,
- enhancing international cooperation to fight against the dangers facing the children.

The meeting was an opportunity for the governments, law enforcement agencies, concerned institutions and civil society organizations to meet and agree on tangible actions and establish international trans-border cooperation networks acting as a strong alliance to deter offenders.

Both the Management and Advisory Board discussed a number of issues on the agenda including voting for the joining of the a new private sector member, the growing concern of live distant child abuse, current operations and the proposal of undercover operations, enhancing the current website, and addressing capacity building in the Philippines.

In addition, members of the private sector joined the meeting and discussed the joined efforts to combating remote child abuse online and their contribution to tackling this crime, based on their area of expertise.

The VGT was established in 2003 to combat online child abuse and has now grown to have 13 country members and 19 private sector members. It aims to disassemble child sexual exploitation networks on the internet, coordinate undercover investigations about cybercrimes, exchange and develop intelligence information and identify victims.

Visit their website to read more.

"Holding this meeting reflects the awareness of the governments worldwide that the internet is becoming widely misused to exploit and abuse children which is a crime and a global problem that knows no borders. Resolving this problem requires coordinated and serious international actions"

Major General Dr. Nasser Lakhrerbani Al Nuaimi

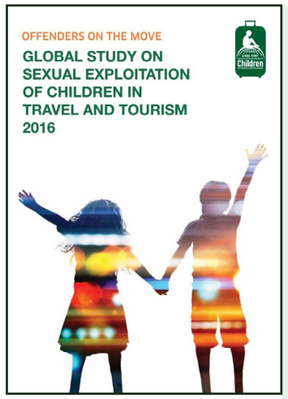
5 What's new?
Update on ECPAT's initiatives

ecpat LUXEMBOURG

01

The Global Study on Sexual Exploitation of Children in Travel and Tourism was released on 12 May 2016 by ECPAT International, marking the 20th Anniversary of the First World Congress against commercial sexual exploitation of children.

The report aims to raise awareness and to spur action from governments, the tourism industry and civil society organisations to end the sexual exploitation of children in travel and tourism (SECTT). This study, funded by the Dutch Government and overseen by the members of the ECPAT High-Level Global Taskforce, contains contributions from the global ECPAT Network, partners and experts, including Europol's European Cybercrime Centre, as well as other law enforcement agencies, governments and universities.



Click here to read the full report.

Key findings

- The Global Study has collected and analysed qualitative and quantitative information on the SECTT in all regions of the world, including case studies and good practices.
- The findings from 9 regional reports (East Asia, Europe, Latin America, Middle East and North Africa, North America, The Pacific, South Asia, Southeast Asia and Sub-Saharan Africa) reveal similarities, such as an increased diversification of travel and tourism infrastructure and the increased use by offenders of mobile technologies, while also highlighting challenges that are specific to each region.
- Some of the key findings of the study include the need for a broader view on SECTT given its spread, and the need for a clear global definition of SECTT that would be mirrored within national legislations.
- The report emphasises the need for cross-sectoral partnerships and aligned approaches in SECTT prevention and interventions, recommending that partners across sectors around the world should come together to push for effective laws, strong enforcement, the end of impunity for offenders, and the better protection of children.

02

On 14 June 2016, a Global Interagency Working Group, which Europol participated in, released the 'Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse' in Geneva, Switzerland.

The guidelines aim at overcoming the language barriers that exist between law-makers, child protection agencies, media, and civil society groups, due to the use of different terminology and definitions of concepts.

The absence of a common language has caused confusion, which has undermined global efforts to protect children. The so called 'Luxembourg Guidelines' can help in strengthening collaboration between these sectors in order to jointly stop child sexual exploitation.

The Luxembourg Guidelines offer guidance on how to navigate the lexicon of terms commonly used relating to sexual exploitation and sexual abuse of children.

They aim at building consensus on key concepts in order to strengthen data collection and cooperation across agencies, sectors and countries.

The guidelines are available to all major child protection agencies and organisations worldwide as well as to law-makers and the media.

www.luxembourgguidelines.org

TERMINOLOGY AND SEMANTICS
Interagency Working Group on Sexual Exploitation of Children

Click here to read the guidelines.

5 What's new?

Europol and Trend Micro release comprehensive overview of ATM malware

On 12 April 2016, Europol's European Cybercrime Centre (EC3) and the security software company Trend Micro have announced the release of their latest joint report, "ATM Malware on the Rise", which offers a comprehensive overview of the ATM malware threat and the specific malware types in circulation.

With more than three million ATMs across the globe and the total number of cash withdrawals averaging around EUR 8.6 billion per year, ATMs are an attractive target for criminal attacks. Through the use of specially designed malware, attackers no longer need to use traditional safe cracking methods to empty an ATM's money safe.

In this report, Trend Micro and Europol highlight the increasing sophistication of cybercriminals in terms of how attacks are planned and orchestrated, using both new methods and techniques in conjunction with well-known attack vectors.

Audience

This report has been released to a closed audience consisting of law enforcement authorities, financial institutions and the IT security industry.

5 What's new?

The 22nd Annual Training Programme

On 17-19 May 2016, the 22nd Annual Training Program was held in Tallinn, Estonia.

The annual event was organised by the Europe, Middle East and Africa (EMEA) Chapter of the International Association of Financial Crimes Investigators (IAFCI).

The three day training provided knowledge about new forms of financial fraud, lessons learned from investigations, and ideas to enhance future cooperation. More than 50 officers attended the training, with speakers from the Dedicated Card and Payment Crime Unit (DCPCU) in the United Kingdom, Finnish National Bureau of Investigation, Antwerp Police Department, the NATO Cooperation Cyber Defence Centre of Excellence (CCDCOE), and Europol. Moneygram, Verifone and Skype were amongst the representatives from the private sector.

DID YOU KNOW?

The IAFCI is a world-wide non-profit organisation, which brings law enforcement, banking institutions, and retail and service members together, in order to join forces against financial fraud. The neutral environment that IAFCI provides enables the sharing of information relating to financial fraud, fraud investigation and fraud prevention methods. Due to its 4 000 members, who are all a part of a network of highly skilled, motivated and committed experts from the public and private sector, IAFCI is an influential association within the field of financial fraud. Europol is represented through the many Europol staff members that are members of the IAFCI network.

Visit their website to read more.

5 What's new?

Update on Europol's training courses

01 **Second Europol Training Course on Payment Card Fraud Forensics and Investigations:** From 11 to 15 July 2016, at the Spanish National Police Academy in Ávila, Spain.

The training focused on the forensic examination of skimming devices, payment card and ATM malware forensics, as well as investigative techniques to target criminal networks responsible for international payment fraud incidents.

There were a total of 59 participants from law enforcement, the private sector and academia, representing 29 countries including a number of EU Member States, Australia, Colombia, Norway, and Turkey.

The majority of participants were experts in forensically examining skimming equipment and electronics, and investigators in payment fraud. During the course, they took part in specific sessions that included card-not-present and card-present fraud modus operandi, trends and threats for investigators, as well as tools for payment card analysis. The course provided common sessions, workshops, and networking events with the private sector, including S21sec, Verifone, Trend Micro, Santander Group, and Visa.

The course was supported by a number of companies who led workshops related to ATM malware. The banking sector, merchants including airlines and fuel card companies, the European ATM Security Team, ATM manufacturers, and POS companies were present and shared their expertise and capabilities in supporting law enforcement work. Participants also visited the 'Financial City Santander', where they had the opportunity to attend workshops and panels on improving preparation for new ATM malware threats among law enforcement.

02 **17th Europol Training Course on Combating the Online Sexual Exploitation of Children on the Internet:** Concluded on 21 October 2016, at the LAFP-NRW Police Academy in Selm, Germany.

This ten-day course provided training for 65 representatives from EU Member States, non-EU States (Albania, Australia, Canada, Colombia, Israel, the Former Yugoslav Republic of Macedonia, Moldova, New Zealand, Norway, Serbia, Switzerland, Ukraine and the United States), Europol and INTERPOL. Principally aimed at law enforcement investigators, the course was also attended by a prosecutor from one of the Member States.

The training was delivered by police trainers from Europol, Belgium, Czech Republic, Denmark, France, Italy, New Zealand, Portugal, and one from Ireland on behalf of INHOPE. All participants had extensive knowledge and experience in investigating and combating the sexual abuse of children online.

The training follows the European Cybercrime Centre's (EC3) approach to cybercrime and its training ethos. The approach is collegial, with expert trainers and investigators working in the field of child sexual exploitation coming together to network and exchange experiences. The main objective of this annual course is to enhance the expertise of those working in this crime area in the EU and beyond, so that they are better able to investigate and dismantle child sex offender networks on the Internet, with the rights and safety of the children involved being a priority.

In addition to lectures, ranging from perpetrator psychology and the latest online investigation techniques to international cooperation, the course programme included a wide range of hands-on exercises with the intention of aligning law enforcement investigation standards.

Since the first course took place in 2000, approximately 800 law enforcement officers and members of the judiciary from EU Member States and from countries around the world have been trained.

5 What's new?

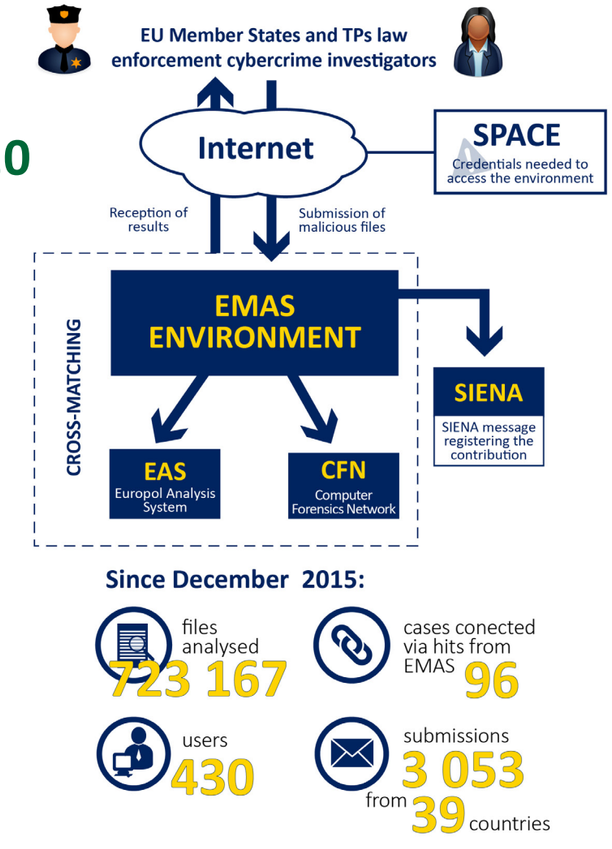
Update on EMAS 2.0

Europol Malware Analysis Solution (EMAS) is a dynamic, automated malware analysis solution, which executes malware samples submitted by investigators from European Union Member States (MS) and Third Parties (TP) in a tightly controlled sandbox environment. EMAS was launched in December 2015 and is accessible through the Europol Platform for Experts (EPE).

EMAS allows users to submit malicious files for automated analysis from anywhere on the internet, to have their malware samples cross-checked with Europol databases and to receive the results back almost instantly.

Key factors

- The solution is free to use;
- The added value is represented by cross-checking malware related entities with all the information available in the Europol databases and generating additional investigative links;
- EMAS submissions are considered official contributions to Focal Point Cyborg and follow the data handling rules and regulations that govern Europol's information system.



EMAS is constantly maintained, updated and developed by Europol. New features are implemented to improve EMAS with a focus on the changes suggested by the users as this would result in an improved experience for them, better tailored to the investigative needs.

1st EMAS Workshop 2016

Within the framework of the 2016 Operational Action Plan (OAP) of the EMPACT Priority Cybercrime Attacks, the Strategic goal 1.4 has been set up "to identify links and support Member States investigations in relation to current malware attacks by making use of the Europol Malware Analysis Solution". The Strategic goal was to be achieved with extending to all MS and TP with Operational Agreement the access and increasing the usage of EMAS.

Against this background, FP Cyborg organised and delivered the 1st EMAS Workshop on 25 and 26 October 2016 at Europol's Headquarters.

More than 37 participants, police officers from EU MS and TP, attended the workshop that aimed to showcase in detail all EMAS functionalities and emphasize the added value of using EMAS in investigations.

Agenda

- malware investigation best practices,
- overview of EMAS space on EPE,
- EMAS – past, present and future,
- practical sessions on EMAS interface, uploading samples and reporting,
- EMAS auto-crossmatch and graphical visualization,
- EMAS as international case generator,
- EMAS analytics and integration with Europol databases,
- discussion on future developments and functionalities needed.

PHOTO CREDITS

Cover Image © Europol © Shutterstock | **Background image** © Europol © Shutterstock | **Page 2** © Europol | **Page 3** © Europol © INTERPOL | **Page 4** © Shutterstock | **Page 5** © Europol © Shutterstock | **Page 6** © Europol | **Page 7** © Europol | **Page 8** © Shutterstock | **Page 9** © Europol | **Page 10** © Shutterstock © Europol | **Page 11** © Europol | **Page 12** © Europol | **Page 13** © Europol | **Page 14** © Europol © Shutterstock | **Page 15** © Europol © NMR | **Page 16** © Shutterstock | **Page 17** © ECSM © Europol | **Page 18** © Europol | **Page 19** © Europol © Shutterstock | **Page 20** © ICANN | **Page 21** © RIR © Shutterstock | **Page 22** © Shutterstock | **Page 23** © INTERPOL © Shutterstock | **Page 24** © Shutterstock | **Page 25** © Shutterstock | **Page 26** © Kabuntu | **Page 27** © Shutterstock | **Page 28** © Youth Pathways into Cybercrime © Europol | **Page 29** © Europol | **Page 30** © VGT © Shutterstock | **Page 31** © ECPAT | **Page 32** © Shutterstock | **Page 33** © Shutterstock | **Page 34** © Europol | **Back Cover** © Europol | **Background image** © Shutterstock

HAPPY HOLIDAYS

AND

BEST WISHES

FOR 2017

EUROPOL
EC3 | European Cybercrime Centre

Website: www.europol.europa.eu/EC3
Facebook: www.facebook.com/Europol
Twitter: @EC3Europol
YouTube: www.youtube.com/EUROPOLtube