The Role of Police Authorities in IPR Enforcement

BOGDAN CIINARU | BANGKOK| 13/09/2019

www.ipkey.eu
OSINT Research and Monitoring Team

- “scanning” the internet (publicly available web-sites) in order to gather information and monitor relevant trends;
- share information and observed trends with national competent authorities;
• facilitate and support the activities of national authorities competent in the field of “tracing the money” related to IP infringements by gathering information, monitoring relevant trends and organising meetings;

• follow trainings to update the technical knowledge of payment providers and asset recovery activities;

• provide technical training and expertise to law enforcement agencies.
• 22-23/02 : Ops meeting
• Exchange of targets between IPR Centre, Europol, MS’s, Interpol, private partners.
• 01/05: 1st call for IPR holders
• 31/08: 2nd call for IPR holders
• 15/11: Deadline for sending final reporting sheet to Europol
• 26/11: Joint press release
Operation In-Our-Sites (IOS)

Participating LEAs

Albania, Austria, Belgium, Bulgaria, Bosnia and Herzegovina, Colombia, Czech Republic, Denmark, France, Greece, Hungary, Hong Kong- China, Ireland, Italy, Netherlands, Peru, Republic of Korea (South Korea), Republic of Moldova, Republic of Serbia, Romania, Slovakia, Spain, Portugal, Ukraine, United Kingdom of Great Britain and Northern Ireland, United States of America, Interpol

Private sector companies

<table>
<thead>
<tr>
<th>Subject IOS IX</th>
<th>2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preparation</td>
<td></td>
</tr>
<tr>
<td>Kick-off-meeting</td>
<td>Jan</td>
</tr>
<tr>
<td>Deadline for 1st call</td>
<td>Feb</td>
</tr>
<tr>
<td>Deadline for 2nd call</td>
<td>Mar</td>
</tr>
<tr>
<td>Final reporting</td>
<td>Apr</td>
</tr>
<tr>
<td>End of operation and joint press release</td>
<td>May</td>
</tr>
<tr>
<td></td>
<td>June</td>
</tr>
<tr>
<td></td>
<td>July</td>
</tr>
<tr>
<td></td>
<td>Aug</td>
</tr>
<tr>
<td></td>
<td>Sep</td>
</tr>
<tr>
<td></td>
<td>Oct</td>
</tr>
<tr>
<td></td>
<td>Nov</td>
</tr>
<tr>
<td></td>
<td>Dec</td>
</tr>
</tbody>
</table>
Operation In Our Sites
Project TransAtlantic VII

This domain name has been seized

Operation In Our Sites-Project TransAtlantic VIII is a coordinated effort by U.S., European, South American and Asian law enforcement agencies targeting websites and their operators that sell counterfeit goods.
PIPCU takes down over 31,000 sites in international Europol operation
27 Nov 2018

This year, the City of London Police’s Intellectual Property Crime Unit (PIPCU) suspended over 31,000 sites as part of Europol’s Operation in Our Sites.
Twelve people, including four in Ireland, arrested in global operation targeting websites selling fake goods

Europol operation takes down 33,600-plus Internet domains selling counterfeit goods


Over 1M Fake Goods Websites in Global ‘Operation in Our Sites’

Over 1 million copyright-infringing website domain names selling counterfeit fake goods were criminally and civilly seized within the past year through the combined efforts of law-enforcement agencies across the world, high-profile industry representatives and anti-counterfeiting associations.

As part of an international operation, Europol’s Intellectual Property Crime Co-ordinated Coalition (IPC3) has seized 33,654 domain names distributing counterfeit and pirated items online. The websites featured items such as counterfeit pharmaceuticals, pirated films and television shows, music, software, electronics and other bogus products. The joint international operation also involved the US National Intellectual Property Rights Coordination Centre* and law enforcement authorities from 26 countries including EU Member States and third parties**, and was facilitated by Interpol.
In Our Sites

- Participants
- Websites seized
- Arrested

<table>
<thead>
<tr>
<th>IOS I</th>
<th>IOS II</th>
<th>IOS III</th>
<th>IOS IV</th>
<th>IOS V</th>
<th>IOS VI</th>
<th>IOS VII</th>
<th>IOS VIII</th>
<th>IOS IX</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>133</td>
<td>1</td>
<td>12</td>
<td>328</td>
<td>0</td>
<td>8</td>
<td>188</td>
<td>6</td>
</tr>
<tr>
<td>10</td>
<td>690</td>
<td>0</td>
<td>292</td>
<td>0</td>
<td>21</td>
<td>999</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>5158</td>
<td>10</td>
<td>10</td>
<td>27</td>
<td>0</td>
<td>10</td>
<td>26</td>
<td>12</td>
</tr>
</tbody>
</table>

36126
<table>
<thead>
<tr>
<th>Types</th>
<th>Countries</th>
<th>Seizures</th>
<th>Arrested</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jewellery and other accessories</td>
<td>133</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Illuminated Phone Case</td>
<td>5</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>Sunglasses</td>
<td>690</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Shoes</td>
<td>188</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>Glasses</td>
<td>5156</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>Wallets</td>
<td>7786</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>29492</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Type of Counterfeit Goods**

- Clothing: 82.99%
- Shoes: 8.66%
- Illuminated Phone Case: 2.52%
- Sunglasses: 0.16%
- Glasses: 0.47%
- Wallets: 0.31%

*Directed by the European Commission, IP Key South-east Asia is implemented by the European Union Intellectual Property Office (EUIPO)*
<table>
<thead>
<tr>
<th>IOS</th>
<th>Seizures</th>
<th>Arrested</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>5</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>II</td>
<td>12</td>
<td>328</td>
<td>340</td>
</tr>
<tr>
<td>III</td>
<td>10</td>
<td>690</td>
<td>700</td>
</tr>
<tr>
<td>IV</td>
<td>17</td>
<td>188</td>
<td>205</td>
</tr>
<tr>
<td>V</td>
<td>19</td>
<td>292</td>
<td>311</td>
</tr>
<tr>
<td>VI</td>
<td>21</td>
<td>999</td>
<td>1020</td>
</tr>
<tr>
<td>VII</td>
<td>27</td>
<td>5156</td>
<td>5423</td>
</tr>
<tr>
<td>VIII</td>
<td>27</td>
<td>7786</td>
<td>8053</td>
</tr>
<tr>
<td>IX</td>
<td>26</td>
<td>33600</td>
<td>34046</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>29492</strong></td>
<td><strong>12</strong></td>
<td><strong>29504</strong></td>
</tr>
</tbody>
</table>
Operation In-Our-Sites (IOS)

This restricted area is meant to be the only point of reference for the exchange of strategic and technical information mainly between Europol and its Private Sector partners in IOS.

IOS follow-up survey is now closed. Please download the report here.

Thank you very much for your kind participation!
DON'T

Profits from counterfeiting fund other forms of serious organised crime like labour exploitation or human trafficking. Stop buying counterfeit goods online. Don't be an accomplice of crime.

90% OFF

WHEN BUYING ONLINE
OPERATION POSTBOX II

- EUROPOL, European Anti-Fraud Office (OLAF) and Belgian Customs
- counterfeit goods – including medicine –, trafficking drugs and endangered animal and plant species (CITES)
- 22 Member States
- first time set-up and use of an international cyber patrol with customs services
In the initial phase of the operation, customs authorities checked mail and courier service packages for prohibited items.

More than 500 packages were seized in Belgium only, followed by Italy with 460 and Ireland with 304 seizures.

OLAF with Europol support provided participants with access to its Virtual Operation Coordination Unit, a secure communication system facilitating intelligence exchange in real time.

An expert cyber patrol which raided both the open web and the dark net, as well as social media sites, in search of the perpetrators of the crimes and deanonymize.
• 2320 seizures
• 50 case files were open
• 30 suspects identified in EU Member States
• The main findings reveal that Asian e-commerce platforms are still responsible for the majority of counterfeit sales.
• Drug trafficking takes place mainly through the Dark Web, where technology is used to keep buyers and sellers anonymous.
OPERATION PANGEA X

- LEA from 123 countries involved
- International week of action (12 – 19 September)
- 400 arrests worldwide and the seizure of more than USD 51 million worth of potentially dangerous medicines
- Websites taken offline and the suspension of more than 3000 online adverts for illicit pharmaceuticals
- 197 police, customs and health regulatory authorities from a record 123 countries
• Social networks are showcases for online vendors, counterfeiters do not show references to business activity such as legal office and V.A.T. number

• The operation Aphrodite focuses on websites and major social networks

• Contact and Sales Channels: Whatsapp, Telegram, Wechat.

• Contact information can be detected in different parts of the profile: e.g. name, image or QR code

• Payment systems and methods of delivery of goods: application of the "follow the money" technique to verify the type of offense (counterfeiting, credit card phishing or other types of fraud)
The complex Universe of the Web: a growing and wide spread threat

<table>
<thead>
<tr>
<th>Social network</th>
<th>Modus operandi</th>
</tr>
</thead>
<tbody>
<tr>
<td>Few pieces/zero stock</td>
<td>Stock up only when negotiations had been concluded</td>
</tr>
<tr>
<td>First contact on social only</td>
<td>Change phone number</td>
</tr>
<tr>
<td>Subsequent contacts on whatsapp</td>
<td>Cooperation with other people</td>
</tr>
<tr>
<td>Cooperation with other people</td>
<td>Expedition through postal system</td>
</tr>
<tr>
<td>No payments with electronic money</td>
<td>Payments with cash upon delivery</td>
</tr>
</tbody>
</table>
B493 Ugreen Ethernet Cable Cat6 Lan Cable UTP CAT 6 RJ 45 Network Cable Patch Cord for Laptop Router RJ45 Network Cable.

**US $24.76**

Color:
- G1
- G2
- G3

Quantity:
- 1
- 2997 pieces available

**Free Shipping** to Romania via China Post Registered Air Mail

Estimated Delivery: 29-51 days

- **Buy Now**
- **Add to Cart**

**60 Day Buyer Protection**
Money back guarantee
Focusing during the investigation on:

- Price
- Profile name
- Labels (hashtag)
- Types and trademarks of the products on sale
- Contact information
- Post
OPERATION APHRODITE

- 15 000 links closed
- 1 000 accounts closed
- 18 online site shut down
- 4.5 million pieces seized (sports articles, medicines, mobile phones, bags, jewellery, sunglasses, clothing, watches, perfumes and cosmetics, illegal IPTV set-top-boxes etc.)
- **24** suspects prosecuted
- Numerous suspects investigated
- Many investigations are still ongoing
• The data returned on particular targets is determined by their privacy Settings

• As most users are negligent, and as the platforms keeps altering its settings, a lot of intelligence is available to the investigators

• To search for people try to identify their closed friends and relations and ask to be part of your network
• Study the suspect’s social media page

• Their Timeline; gather details of the target’s likes, interests, relationships, etc.

• Take note of any personal details if available

• Try to see their most important connections

• See their photos, can contain many useful tips about the suspect

• Click on More and visit the other sections of the target’s profile, gathering intelligence as you go along
• the cases initiated during the previous Aphrodite II, may have generated some developments that will be further developed in Aphrodite III

• through Aphrodite I, it were identified different ways of action in order to achieve better results in the upcoming Aphrodite operation

• we improved our templates and the cooperation with most of the participating private companies developed into an efficient work

• we managed to involve new countries in the operation which achieved great results
- the trade in counterfeit goods will continue to increasingly take place online
- online marketplaces will become even more popular with a wider group of customers.
- the use of social media for advertising counterfeit products is expected to continue in the future
- counterfeit goods that are sold online will continue to be distributed in parcels via postal services
- due to reinforced checks and monitoring of the express freight couriers, counterfeiters may make increased use of postal freight for the labels
- targeting and controlling suspicious shipments in postal freight are a great challenge
• Not a new trend
• Illegal and legal business mixed in same premises
• Offenders usually are technically skilled
• Not necessary a big amount of money to start (only with a computer used as a server or with a big Data-centre for the Big Money)
• Socially accepted (just looking for the best price)
• Spread throughout EU and outside
• Virtual Currencies used for payment
• Two possible “tendencies” identified
Development of new work methodologies:
• significant economic benefits
• high security standards
• customers service (satisfied clients) with:

Constantly renewed contents.
• 24/7 technical support
• Internet “doubts - solving” forum
The Economic Crime and Special Operations Command of the Romanian Police, under the coordination of the General Prosecutor’s Office, and with the support of Europol IPC3 have undertaken the operation

Possible links could be related to Austria (suspects’ bank accounts) and to Italy (where other suspects and criminal activity was developed)
The following assets connected to the criminal activity were seized:

- 350.000 euros from 6 Romanian bank accounts and from an account belonging to a payment processor for online vendors;
- a real estate with its dependencies in a total value of 50.000 euro
- a luxury car with an estimated value of 60.000 euro;
- the servers and the IPTV streaming web domain.
OPERATION DREAM

https://youtu.be/NHHHurbGgKk
The operation was undertaken by:

• Cypriot Police – Intellectual Property Crime Unit;
• Cybercrime Division of the Greek Police;
• The Dutch Fiscal Investigative and Intelligence Service (FIOD);
• The Cybercrime Unit of the Bulgarian Police;
• with the support of Europol’s Intellectual Property Crime Coordinated Coalition (IPC³) and the members of the Audiovisual Anti-Piracy Alliance (AAPA)
Operational results:
• In Cyprus three suspects were arrested and the whole digital infrastructure was closed down;
• In Bulgaria one suspect was arrested, 84 servers and 70 satellite receivers were seized, with decoders, computers and accounting documents;
• Five IP addresses hosted by a Dutch company were deactivated.
The criminal group have offered online illegal television signals from more than 14,000 international points of sale since 2016 based on payed subscriptions.

The signals were sold through a company which designed the application needed to illegally stream films, television series and sport events.

The decoder was sold for EUR 120 and the server to transmit the illegal signal was hosted in France and controlled from the business in Spain.
Following coordination of Europol, on the action day:

- 8 house searches were carried out in Spain;
- six members of the organised crime group were arrested;
- more than 4600 set-top-boxes were seized;
- VC farm identified;
- the online streamed channels were shut down.
The criminal group have offered online illegal television signals for many consumers since 2015.

The signals were sold through set-top-boxes where the OCG installed an illegal IPTV streaming app.
Following coordination of Europol, on the action day:

• 2 experts from Europol were deployed;
• 4 house searches were carried out in Ireland and U.K.;
• six members of the organised crime group were arrested;
• more than 4600 set-top-boxes were seized;
• Six bank accounts and two credit union accounts were frozen under anti-money laundering legislation;
• nine other accounts were part frozen;
• in total more than €1,000,000 were frozen;
• the online streamed channels were shut down;
• media campaign for the consumers.
VC FARM MOVIE
Bulgarian Supreme Prosecutor’s Office of Cassation, police officers from the Bulgarian Cybercrime Department from the General Directorate Combating Organized Crime of the Ministry of Interior IPC3 and the Audiovisual Anti-Piracy Alliance

Europol’s IPC3 supported the investigation on the ground by deploying an analyst and a specialist to Bulgaria equipped with a mobile office.
Five cable operators were illegally intercepting and distributing more than 60 premium TV channels (both foreign and Bulgarian), without the consent of the rights-holders.

The financial damage is estimated to be more than 10 million Bulgarian lev (approximately €5 million). More than 700,000 subscribers received the illegal broadcasted signal from the criminal network.
РН-TV
Лятна промоция IPTV! Предплати и спести!

Купон RN50 - при заплащане над 50 лв. - 5% отстъпка
Купон RN100 - при заплащане над 100 лв. - 10% отстъпка
Купон RN200 - при заплащане над 200 лв. - 15% отстъпка

Купонът се въвежда при предлагащ на услугата IPTV в електронния ни магазин https://my.rn-tv.com

Промоцията възли на 15.05.2019 до 15.09.2019

Directed by the European Commission; © 2019 EU. All rights reserved. Logo: European Intellectual Property Office (EUIPO)
Global piracy problem requires global collaboration from law enforcement, government and industry including:

- Deployment of effective technical measures to protect audiovisual content
- Public education and awareness
- Information gathering and intelligence sharing
- Training for law enforcement, judiciary and government
- Improved (uniform) legislation
- Coordinated cross border enforcement actions
ILLEGAL IPTV

Difficulties for Law Enforcement Agencies (LEA’s) to tackle this:

• Lack of dedicated resources;
• Technical expertise is required (identify the servers, IP addresses, etc.);
• VC as a new payment method;
• Transnationality;
• Cooperation with the private sector;
• Different legal frameworks;
• Prosecution;
• Data preservation timeframe in some countries;
• Awareness for the consumers (viruses and malware).
• Books, games, movies, music

• Distributed via BitTorrent portals, P2P networks, cyberlockers, stream ripping

• Profit generated via digital advertisements

• Phishing attempts or malware distribution

• IPTV – servers located in different countries than those where subscriptions are sold
Thank you for your attention!

Bogdan Cîinaru
Tel.: +31703531750
bogdan.ciinaru@europol.europa.eu
THANK YOU

@IPKey_EU