Technical innovation can be harnessed for social good, but just as readily for nefarious ends. This is truer of cybercrime than of perhaps any other crime area. And cybercriminals are also getting more aggressive. That's why Europol and its partner organisations are taking the fight to them on all fronts.

Cybercrime is an EMPACT priority for the policy cycle from 2018 to 2021: the aim is to fight cybercrime, by (1) disrupting the criminal activities related to attacks against information systems, particularly those following a Crime-as-a-Service business model and working as enablers for online crime, (2) combating child sexual abuse and child sexual exploitation, including the production and dissemination of child abuse material, and by (3) targeting criminals involved in fraud and counterfeiting of non-cash means of payment, including large-scale payment card fraud (especially card-not-present fraud), emerging threats to other non-cash means of payment and enabling criminal activities.

According to the most recent Internet Organised Crime Threat Assessment (IOCTA) , cybercrime is becoming more aggressive and confrontational. This can be seen across the various forms of cybercrime, including high-tech crimes, data breaches and sexual extortion.

Cybercrime is a growing problem for countries, such as EU Member States, in most of which internet infrastructure is well developed and payment systems are online.

But it is not just financial data, but data more generally, that is a key target for cybercriminals. The number and frequency of data breaches are on the rise, and this in turn is leading to more cases of fraud and extortion.

The sheer range of opportunities that cybercriminals have sought to exploit is impressive. These crimes include:

- using botnets—networks of devices infected with malware without their users' knowledge—to transmit viruses that gain illicit remote control of the devices, steal passwords and disable antivirus protection;
- creating "back doors" on compromised devices to allow the theft of money and data, or remote access to the devices to create botnets;
- creating online fora to trade hacking expertise;
- bulletproof hosting and creating counter-anti-virus services;
- laundering traditional and virtual currencies;
- committing online fraud, such as through online payment systems, carding and social engineering;
- various forms of online child sexual exploitation, including the distribution online of child sex-abuse materials and the live-streaming of child sexual abuse
- the online hosting of operations involving the sale of weapons, false passports, counterfeit and cloned credit cards, and drugs, and hacking services.

High-tech crimes

Malware, or malicious software, infiltrates and gains control over a computer system or a mobile device to steal valuable information or damage data. There are many types of malware, and they can complement each other when performing an attack.

- A **botnet** (short for robot network) is made up of computers communicating with each other over the internet. A command and control centre uses them to send spam, mount distributed denial-of-service (DDoS) attacks (see below) and commit other crimes.
- A **rootkit** is a collection of programmes that enable administrator-level access to a computer or computer network, thus allowing the attacker to gain root or privileged access to the computer and possibly other machines on the same network.
- A **worm** replicates itself over a computer network and performs malicious actions without guidance.
- A **trojan** poses as, or is embedded within, a legitimate programme, but it is designed for malicious purposes, such as spying, stealing data, deleting files, expanding a botnet, and performing DDoS attacks.
- A **file infector** infects executable files (such as .exe) by overwriting them or inserting infected code that disables them.
- A **backdoor/remote-access trojan (RAT)** accesses a computer system or mobile device remotely. It can be installed by another piece of malware. It gives almost total control to the attacker, who can perform a wide range of actions, including:
  - monitoring actions
  - executing commands
  - sending files and documents back to the attacker
  - logging keystrokes
  - taking screen shots
- **Ransomware** stops users from accessing their devices and demands that they pay a ransom through certain online payment methods to regain access. A variant, police ransomware, uses law enforcement symbols to lend authority to the ransom message.

- **Scareware** is fake anti-virus software that pretends to scan and find malware/security threats on a user's device so that they will pay to have it removed.
- **Spyware** is installed on a computer without its owner's knowledge to monitor their activity and transmit the information to a third party
- **Adware** displays advertising banners or pop-ups that include code to track the user's behaviour on the internet

The response:

PURSUING CYBERCRIMINALS ON ALL FRONTS

With such a range of activities being pursued with such inventiveness, the response of Europol and its partners must itself be comprehensive, dynamic and relentlessly innovative. And it is.

First, there's the institutional response. In 2013 Europol set up the European Cybercrime Centre (EC3) to bolster the response of law enforcement to cybercrime in the EU and help protect European citizens, businesses and governments.

Each year the EC3 issues the aforementioned Internet Organised Crime Threat Assessment (IOCTA), which sets priorities for the EMPACT Operational Action Plan in the areas of cybercrime that are the focus for that year.

The EC3 also hosts the Joint Cybercrime Action Taskforce (J-CAT). Its mission is to drive intelligence-led, coordinated action against key cybercrime threats through cross-border investigations and operations by its partners.

These institutional arrangements have led to notable successes at the operational level, including:

- the coordination of a joint operation, including private-sector partners to target a botnet, Ramnit, that had infected millions of computers around the world;
- coordination with Eurojust in an operation targeting large-scale malware attacks that originated in Ukraine and that were being investigated by a number of agencies — an operation that led to tens of arrests and continues to supply evidence that supports other cybercrime investigations;
- an operation targeting a major cybercriminal forum engaged in trading hacking expertise, malware and botnets, Zero Day Exploits, access to compromised servers, and matching partners for spam campaigns and malware attacks.

NUMBER OF ITEMS FOUND: 540

SEARCH

TYPE

Article/Story, Event, How-To Guide, Landing Page, Multimedia, News/Press Release, Operation, Page, Publication/Document

TARGET GROUP

SEARCH

CLEAR ALL

CRYPTOCURRENCY EXPERTS MEET AT EUROPOL TO STRENGTHEN TIES BETWEEN LAW ENFORCEMENT AND PRIVATE SECTOR

NEWS/PRESS RELEASE

18 ARRESTED IN THE UK AND ROMANIA FOR €20 MILLION FAKE TRAIN TICKET SCAM

NEWS/PRESS RELEASE

27 May 2019

GLOBAL TASKFORCE CLOSE TO IDENTIFYING THREE VICTIMS OF CHILD SEXUAL ABUSE

NEWS/PRESS RELEASE

22 May 2019

MULTI-MILLION EURO CRYPTOCURRENCY LAUNDERING SERVICE BESTMIXER.IO TAKEN DOWN

NEWS/PRESS RELEASE

16 May 2019

THE GOZNYM CRIMINAL NETWORK - HOW IT WORKED

PUBLICATION/DOCUMENT

16 May 2019

GOZNYM MALWARE: CYBERCRIMINAL NETWORK DISMANTLED IN INTERNATIONAL OPERATION

NEWS/PRESS RELEASE

08 May 2019

DEEPDOTWEB SHUT DOWN: ADMINISTRATORS SUSPECTED OF RECEIVING MILLIONS OF KICKBACKS FROM ILLEGAL DARK WEB PROCEEDS

NEWS/PRESS RELEASE

03 May 2019

DOUBLE BLOW TO DARK WEB MARKETPLACES

NEWS/PRESS RELEASE

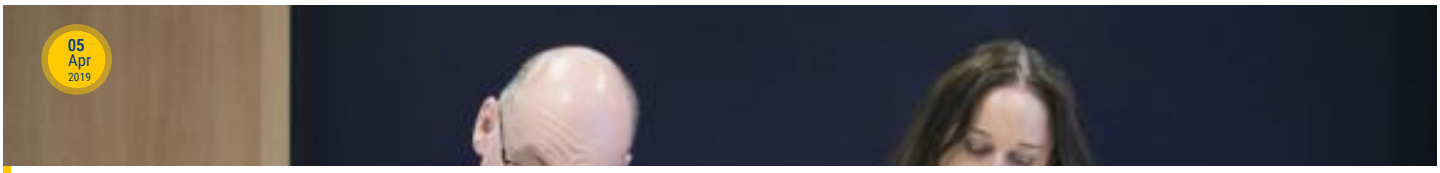
09 Apr 2019

WELCOME ON BOARD! POLAND AND SWEDEN JOIN THE JOINT CYBERCRIME ACTION TASKFORCE TO HELP FIGHT THIS BORDERLESS THREAT

NEWS/PRESS RELEASE

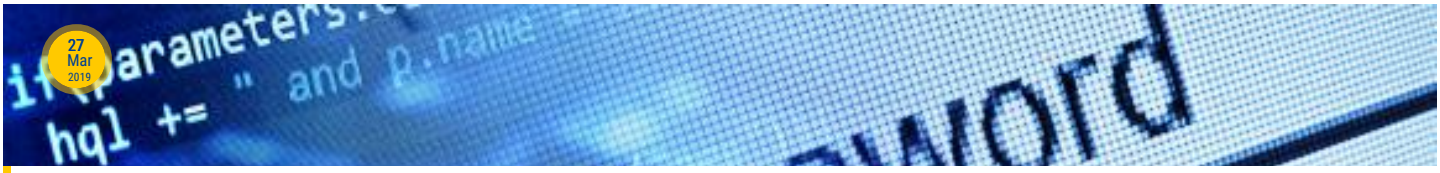
FINAL WHISTLE FOR AN ILLEGAL SPORTS BETTING NETWORK IN PORTUGAL

NEWS/PRESS RELEASE



EUROPOL AND MRC EUROPE JOIN FORCES IN THE FIGHT AGAINST E-COMMERCE FRAUD

NEWS/PRESS RELEASE



EUROPOL TEAMS UP WITH INDUSTRY EXPERTS TO COMBAT PHISHING

NEWS/PRESS RELEASE

« FIRST ‹ PREVIOUS 1 2 3 4 5 6 7 8 9 ... NEXT › LAST »

Source URL: https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime?t=&ct%5Barticle%5D=article&ct%5Bevent%5D=event&ct%5Bguide%5D=guide&ct%5Bpanel%5D=panel&ct%5Bmultimedia%5D=multimedia&ct%5Bnews%5D=news&ct%5Boperation%5