EUROPOL

Pandemic profiteering

how criminals exploit the COVID-19 crisis

March 2020

FOREWORD

The current crisis is unprecedented in the history of the European Union (EU).

Following the outbreak of the COVID-19 pandemic, Member States have imposed extensive quarantine measures, including travel restrictions, limitations to public life and lockdowns.

However, law enforcement agencies are requested to perform their duties under any circumstances. In many cases, their responsibilities have even been extended to maintain public order and safety and to support health authorities in their work. I would like to thank our frontline health, police and other critical staff for their tireless and relentless work.

Needless to say, this situation also has implications on the internal security of the EU. Criminals have quickly seized the opportunities to exploit the crisis by adapting their modes of operation or developing new criminal activities. Organised crime groups are notoriously flexible and adaptable and their capacity to exploit this crisis means we need to be constantly vigilant and prepared.

Member States' main focus is now on fighting the crisis from a health perspective – it is important that we support their efforts. Crime is a seriously disrupting factor and a diversion from national and EU efforts to ensure the health and safety of citizens. That is why it is relevant to reinforce the fight against crime.

We at Europol are in constant contact with our law enforcement partners across the EU and beyond. During this crisis, more than ever, we must continue to support law enforcement officers in the fight against organised crime and terrorism to enhance the security of European citizens.

The report published today provides an overview of how criminals adapt their misdeeds to the COVID-19 pandemic. It is based on information Europol receives from the EU Member States on a 24/7 basis and intends to support Member States' law enforcement authorities in their work.

CATHERINE DE BOLLE

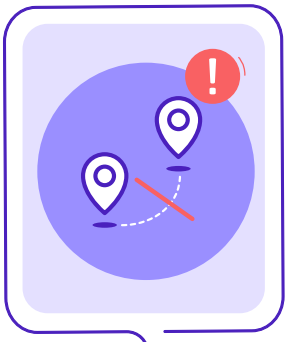
Executive Director, Europol

WHICH FACTORS HAVE AN IMPACT ON CRIME?

The COVID-19 pandemic has forced national governments and the EU to enact various measures to limit the spread of the outbreak, to support public health systems, to safeguard the economy and to ensure public order and safety.

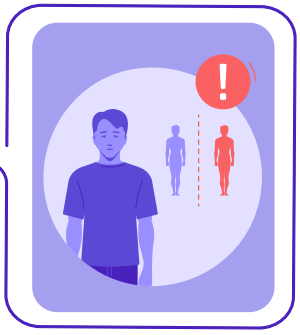
A number of these measures have a significant impact on the serious and organised crime landscape as well as the threat from violent extremists. To understand the impact of the COVID-19 pandemic on the internal security of the EU, it is crucial to identify the factors that prompt changes in crime and terrorism. These factors include:

High demand for certain goods, protective gear and pharmaceutical products



Decreased mobility and flow of people across and into the EU

Limitations to public life will make some criminal activities less visible and displace them to home or online settings

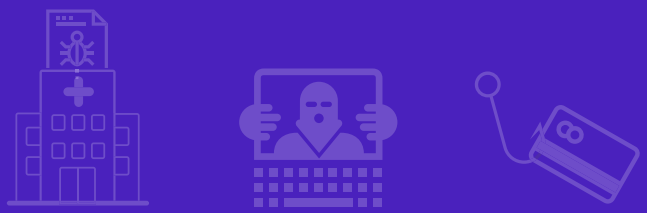


Citizens remain at home and are increasingly teleworking, relying on digital solutions

Increased anxiety and fear that may create vulnerability to exploitation

Decreased supply of certain illicit goods in the EU

CYBERCRIME



KEY FINDINGS

The global pandemic of COVID-19 is not only a serious health issue but also a cybersecurity risk. Criminals swiftly took advantage of the virus proliferation and are abusing the demand people have for information and supplies.

Criminals have used the COVID-19 crisis to carry out social engineering attacks, namely phishing emails through spam campaigns and more targeted attempts such as business email compromise (BEC).

There is a long list of cyber-attacks against organisations and individuals, including phishing campaigns that distribute malware via malicious links and attachments, and execute malware and ransomware attacks that aim to profit from the global health concern.

Information received from law enforcement partners strongly indicates increased online activity by those seeking child abuse material. This is consistent with postings in dedicated forums and boards by offenders welcoming opportunities to engage with children whom they expect to be more vulnerable due to isolation, less supervision and greater online exposure.

The pandemic has an impact on Darkweb operations. Certain illicit goods will become more expensive, as source materials become unavailable. Vendors on the Darkweb offer special corona goods (scam material) at discounts.

OUTLOOK

The number of cyber-attacks is significant and expected to increase further. Cybercriminals will continue to innovate in the deployment of various malware and ransomware packages themed around the COVID-19 pandemic. They may expand their activities to include other types of online attacks.

Cybercriminals are likely to seek to exploit an increasing number of attack vectors as a greater number of employers adopt telework and allow connections to their organisations' systems.

Attack on critical health infrastructure

Cybercriminals carried out a cyber-attack on Brno University Hospital Brno, Czechia amid the COVID-19 outbreak in Europe. Since a state of emergency was declared in Czechia on 12 March 2020, the attack was considered an attack on a critical infrastructure.

The incident prompted the hospital to postpone urgent surgeries and reroute new acute patients to a nearby alternative hospital.

The hospital was forced to shut down its entire IT network during the incident and two of the hospital's other branches, the Children's Hospital and the Maternity Hospital, were also affected.[1]

These types of attack during a public health crisis such as the COVID-19 pandemic are particularly threatening and carry very real risks to human lives.

1 ZDNet 2020, Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak, accessible at https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/

FRAUD

KEY FINDINGS

Fraudsters have been very quick to adapt well-known fraud schemes to target individual citizens, businesses and public organisations.

These include various types of adapted versions of telephone fraud schemes, supply scams and decontamination scams.

The activities of fraudsters will continue to target an increasing number of victims across the EU to exploit anxieties as the crisis persists.

OUTLOOK

Fraud linked to the current pandemic is likely highly profitable for the criminals involved and they will attempt to capitalise on the anxieties and fears of victims throughout this crisis period. A large number of new or adapted fraud and scam schemes can be expected to emerge over the coming weeks and months with the potential for substantial financial damage to citizens, businesses and public organisations.

Criminals have also adapted investment scams to elicit speculative investments in stocks related to COVID-19 with promises of substantial profits.

The emergence of new fraud schemes and a further increase in the number of victims targeted can be expected. Even when the current crisis ends, criminals are likely to adapt fraud schemes in order to exploit the post-pandemic situation.

Supply scams

Businesses seeking to purchase supplies such as protective masks and other equipment are being targeted by scammers.

A Member State's investigation focused on the transfer of €6.6 million from a company to another company in Singapore to purchase alcohol gels and FFP2 and FFP3 masks. The goods were never received.[1]

In another case reported by a Member State, a company attempted to purchase 3.85 million masks and lost €300 000. Similar supply scams of sought-after products have been reported by other Member States.[2]

1, 2 EUROPOL information.

COUNTERFEIT & SUB-STANDARD GOODS

KEY FINDINGS

The distribution of counterfeit and/or sub-standard goods has been a key area of criminal activity in relation to the COVID-19 pandemic.

The sale of counterfeit healthcare and sanitary products as well as personal protective equipment (PPE) and counterfeit pharmaceutical products has increased manifold since the outbreak of the crisis. The advertisement and sale of these items take place both on and offline.

Some developments, such as the distribution of fake corona home testing kits, are particularly worrying from a public health perspective.

OUTLOOK

The sale of counterfeit and/or sub-standard goods on and offline is booming in the pandemic economy. There is particularly high demand for certain types of healthcare and sanitary products (masks, gloves, cleaning products, pharmaceutical products), which has created a substantial market for product counterfeiters, fraudsters and profiteers.

The number of offers of counterfeit and sub-standard good will continue to increase, particularly online. There is a risk that counterfeiters will use shortages in the supply of some goods to increasingly provide counterfeit alternatives both on and offline. This may entail sub-standard or counterfeit foods, hygiene items and other everyday goods.

Criminals take advantage of the high demand in hygiene products driven by the COVID-19 outbreak[1]

Europol supported a global operation to target trafficking counterfeit medicines. Operation Pangea, coordinated by INTERPOL and involved 90 countries worldwide, took place between 3 and 10 March 2020.

The pandemic has opened up a business opportunity for predatory criminals. Authorities around the world seized nearly 34 000 counterfeit surgical masks, the most commonly sold medical product online. Law enforcement officers identified more than 2 000 links to products related to COVID-19.

The results of the operation reveal a worrying increase in unauthorised antiviral medications and the antimalarial chloroquine. Vitamin C, known for its immune-boosting properties, and other food supplements have been seized around the world. Painkillers and antibiotics also represented a significant portion of the seizures.

The operation in numbers

- 121 arrests;
- €13 million in potentially dangerous pharmaceuticals seized;
- 326 00 packages inspected;
- 48 000 packages seized;
- 4.4 million units of illicit pharmaceuticals seized worldwide;
- 37 000 unauthorised and counterfeit medical devices seized (mostly surgical masks and self-testing kits for HIV and glucose monitoring);
- 2 500 links taken down (websites, social media, online marketplaces, adverts);
- 37 organised crime groups dismantled.

Europol supported the operation by facilitating information exchange and providing analytical support.

1 Europol 2020, Criminals take advantage of the high demand in hygiene products driven by the COVID-19 outbreak, accessible at https://www.europol.europa.eu/newsroom/news/rise-of-fake-%E2%80%98corona-cures%E2%80%99-revealed-in-global-counterfeit-medicine-operation

ORGANISED PROPERTY CRIME

KEY FINDINGS

Various types of schemes involving thefts associated with organised property crime have been adapted by criminals to exploit the current situation. This includes the well-known ‘nephew’ or ‘grandchild’ trick and scams involving the impersonation of representatives of public authorities.

Commercial premises and medical facilities are expected to be increasingly targeted for organised burglaries.

The level of activity of criminals involved in organised property crime is expected to further increase during the crisis.

OUTLOOK

The same types of thefts using deception encountered during the COVID-19 crisis have existed before, but criminals have adapted their modi operandi to the current situation. The number of attempts involving these types of thefts and scams is likely to increase across the EU.

While all EU citizens are at risk of being victimised, it appears certain fraud schemes are particularly targeting vulnerable members of society, such as the elderly. Fraudsters also approach victims at home by pretending to be law enforcement or healthcare officials offering testing for COVID-19 and other pretences to enter homes and steal valuables.

Faking and entering

Multiple Member States have reported a similar modus operandi for theft. The perpetrators gain access to private homes by impersonating medical staff providing information material or hygiene products or conducting a 'corona test'.

A Member State reported a case where the perpetrators called the victim to inform them that a relative is infected and in hospital. They claimed that doctors would have to come and take an immediate 'corona test'. These fake doctors came to the victim's home in protective clothing and masks in the middle of the night. The suspects then took an apparent swab sample from the victim's mouth and wiped his forearms with apparent strips of paper to test it. He was then told that the evaluation of the test would take about five hours.

OTHER CRIMINAL ACTIVITIES

KEY FINDINGS

It is difficult to assess the short-term impact of the current pandemic crisis on drug markets, but it is likely to shift supply-demand dynamics and may disrupt illegal supply channels. Some reporting indicates stockpiling of certain drugs by consumers and supply shortages in (pre-)precursors and essential chemicals used in drug production in the EU, which will likely impact on production output and prices. This area requires careful monitoring as supply shortages have the potential to translate into an increase in the number of incidents of drug-related violence between rival suppliers and distributors.

Migrant smuggling has been a key security and humanitarian challenge to the EU over the last five years and remains so during the COVID-19 pandemic crisis. There is likely to be increased demand for services of migrant smuggling networks to enter the EU or to make secondary movements to circumvent the enhanced border control measures currently in place throughout the EU.

There are some concerns that the closure of establishments offering legal sex work may increase the number of incidents of sexual exploitation.

EUROPOL PROVIDES SUPPORT TO LAW ENFORCEMENT PARTNERS DURING THE CRISIS

Europol is ready to support Member State law enforcement authorities and other partners throughout this unprecedented crisis. Europol continues to offer ongoing support in coordinating investigations between different Member States and providing a sophisticated platform for the vital exchange of information.

Crime and terrorism will find ways to continue to operate across borders even in times of border closures and Europol urges our partners to share any pertinent investigations and intelligence to allow us to identify cross-border links.

Europol continues to be the information hub for the exchange of intelligence between Member States and with partner law enforcement authorities. In times of social distancing and remote working, the ability to quickly and effortlessly share information is particularly crucial in carrying on with investigations relying on analytical output.

Europol serves as a platform to exchange intelligence and provides Member States and other partners with solutions such as the European Platform for Experts (EPE). These solutions are highly compatible with remote working and are ideal collaboration tools.

STRATEGIC ACTIVITIES

Providing the Member States' law enforcement authorities and our partners with an up-to-date situational picture is a key priority for Europol during this crisis. To do this, Europol is committing resources to continuous monitoring of the situation and to provide immediate support to Member States if needed.

OPERATIONAL ACTIVITIES

EU Law Enforcement Emergency Response Protocol for Large-Scale Cyber-Attacks

The possibility of a large-scale cyber-attack with serious repercussions in the physical world and crippling an entire sector or society is no longer unthinkable. To prepare for major cross-border cyber-attacks, a European Union Law Enforcement Emergency Response Protocol (EU LE ERP) was adopted by the Council of the European Union in December 2018. The Protocol gives a central role to Europol's European Cybercrime Centre (EC3) and is part of the EU Blueprint for Coordinated Response to Large-Scale Cross-Border Cybersecurity Incidents and Crises.

The EU LE ERP serves as a tool to support EU law enforcement authorities in providing immediate response to major cross-border cyber-attacks through rapid assessment, the secure and timely sharing of critical information and effective coordination of the international aspects of their investigations.

EC3 has regular coordination calls on the cyber impact of COVID-19 with the EU's cybersecurity agency ENISA and CERT-EU, a collection of security experts from EU institutions.

EUROPOL PREVENTION CAMPAIGNS

Europol continues to inform the general public of these scams during the pandemic through preventive social media campaigns. Europol invites countries to work with us on shaping and disseminating these messages.

PANDEMIC PROFITEERING: HOW CRIMINALS EXPLOIT THE COVID-19 CRISIS

This publication and more information on Europol are available on the Internet.

www.europol.europa.eu