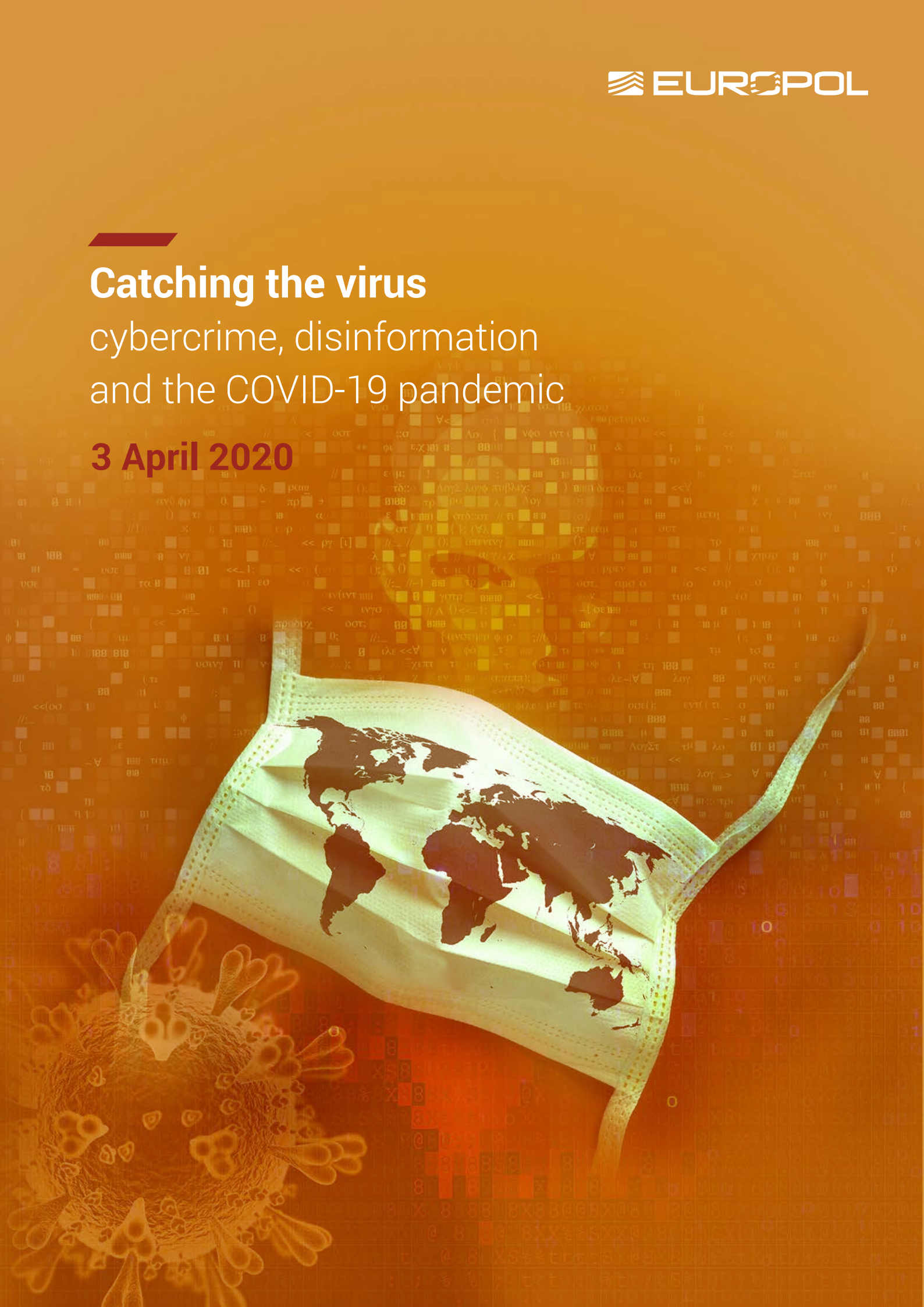
EUROPOL

Catching the virus

cybercrime, disinformation and the COVID-19 pandemic

3 April 2020



FOREWORD

This pandemic brings out the best but unfortunately also the worst in humanity. With a huge number of people teleworking from home, often with outdated security systems, cybercriminals prey on the opportunity to take advantage of this surreal situation and focus even more on cybercriminal activities. With this report we want to warn individuals, companies, public institutions and other organisations about these criminal activities. I would also like to draw special attention to the most vulnerable among those victims; I am very concerned about the rise of child sexual abuse online. Europol is investing resources and capacities to support Member States in countering cyber-dependent crime during this difficult situation.

CATHERINE DE BOLLE
Executive Director, Europol

INTRODUCTION

Cybercriminals have been among the most adept at exploiting the COVID-19 pandemic for the various scams and attacks they carry out. With a record number of potential victims staying at home and using online services across the European Union (EU) during the pandemic, the ways for cybercriminals seeking to exploit emerging opportunities and vulnerabilities have multiplied.

Europol has been monitoring the impact of the COVID-19 pandemic on the cybercrime landscape since the beginning of the current crisis and can present an updated threat picture and assessment of potential further developments in this crime area. The threat from cybercrime activities during the crisis is dynamic and has the potential to increase further. Europol is investing resources and capacities to continue to support EU Member States and other partner law enforcement authorities to counter threats during this difficult situation.

The findings of this report are mainly based on contributions to Europol from Member States and Europol's partner countries.

Europol supports national law enforcement authorities in the international coordination of cyber-related cases by connecting the investigations, facilitating information exchange, operational analysis and forensic services.

Europol's European Cybercrime Centre (EC3) is specialised in supporting the prevention and investigation of cyber-attacks, child sexual exploitation, payment fraud and the online trade of illegal commodities through the dark web, becoming a cybercriminal information hub and a platform for cooperation with the private sector and the cybersecurity community.

KEY FINDINGS

- The impact of the COVID-19 pandemic on cybercrime has been the most visible and striking compared to other criminal activities.
- Criminals active in cybercrime have been able to adapt quickly and capitalise on the anxieties and fears of their victims.
- Phishing and ransomware campaigns are being launched to exploit the current crisis and are expected to continue to increase in scope and scale.
- Activity around the distribution of child sexual exploitation material online appears to be on the increase, based on a number of indicators.
- The dark web continues to host various platforms such as marketplaces and vendor shops to distribute illicit goods and services.
  - After an initial fluctuation in sales via the dark web at the beginning of the crisis in Europe, the situation stabilised throughout March 2020.
  - Vendors attempt to innovate by offering COVID-19 related products.
  - Demand and supply dynamics for some goods are likely to be affected if product scarcity occurs via distributors on the surface web.
- Criminal organisations, states and state-backed actors seek to exploit the public health crisis to make a profit or advance geopolitical interests.
  - Increased disinformation and misinformation around COVID-19 continues to proliferate around the world, with potentially harmful consequences for public health and effective crisis communication.

RANSOMWARE

Ransomware is a type of malicious software criminals use to take files on a device hostage by encrypting the data and subsequently refusing access to them. To regain access to the files, the victim needs to pay the criminal a ransom. Generally, perpetrators request such a payment in the form of bitcoin or some other virtual currency. The primary focus therefore is on financial gain.

In recent years, criminals have focused their attacks on organisations. As many organisations suffer disruption to business when they cannot access their files, criminals have a relatively high likelihood of receiving the payment. Normally, criminals focus their attacks on high-value data or assets within organisations that are especially sensitive to downtime—so the motivation to pay a ransom is consequently very high. Hospitals are such an example, since downtime for a hospital could potentially lead to loss of life. Other examples include government agencies, universities and organisations within the manufacturing sector.

Ransomware is also offered on the dark web as a ransomware-as-a-service product. During the COVID-19 pandemic, most reports to Europol has related to previously known ransomware families, which suggests the involvement of established criminals continuing their business. However, new ransomware families have also continued to frequently appear during the pandemic.

To carry out a ransomware attack, criminals need to gain access to the system of their victim. This can be achieved through social engineering techniques such as phishing attacks. When the victim clicks on a link or opens a malicious email, the perpetrator can execute their strategy by infecting the device.

How has the COVID-19 pandemic changed the way criminals use ransomware?

The types of criminals exploiting the COVID-19 pandemic online were also active in the area of cybercrime before. However, some are believed to have intensified their activities and are actively recruiting collaborators to maximise the impact of their attacks or schemes.

The period between the initial infection with ransomware and the activation of the ransomware attack is shorter. Criminals do not wait for the ideal moment to launch the attack but try as soon as possible.

DISTRIBUTED DENIAL-OF-SERVICE

Only a slight increase in the number of distributed denial-of-service (DDoS) attacks has been observed following the outbreak of the COVID-19 pandemic. However, it is expected that will be an increase in the number of DDoS campaigns in the short to medium term. Due to a significant increase in the number of people working remotely from home, bandwidth has been pushed to the limit, which allows perpetrators to run 'extortion campaigns' against organisations and critical services and functions. DDoS is an accessible type of crime with limited barriers to entry because it is cheap and readily available.

MALICIOUS DOMAIN NAME REGISTRATION

Following an initial spike in the domains registered related to the words 'corona' and 'COVID', the current figures indicate that this appears to have stabilised. These registered domain names form the backbone for many criminal operations.

OUTLOOK

Ransomware has been the most dominant cybercrime threat over the last several years. The current crisis is unlikely to change that dynamic. The pandemic may multiply the damaging impact of a successful attack against certain institutions, which reinforces the necessity for effective cyber-resilience. The number of phishing attempts exploiting the crisis is expected to continue to increase. However, we also expect a greater number of inexperienced cybercriminals to deploy ransomware-as-a-service. Not all of these campaigns will result in successful attacks due to the lack of experience and technical skills of the criminals.

CHILD SEXUAL EXPLOITATION

While the entirety of online child sexual exploitation material (CSEM) cannot be measured directly, there are several indicators that can be used to assess the scope of online CSEM and whether there is an increase in the production and/or distribution of material. Europol will be monitoring the specific indicators below in the upcoming weeks to assess the impact of the COVID-19 crisis on online child sexual exploitation and support investigations.

1) The number of referrals from NCMEC/NCECC[1]

There does not appear to be a significant increase in the number of referrals. However, this may be due to decreased manual moderation of platforms because of teleworking, latency in the reporting period, and the use of automatic systems to detect content online rather than a decrease in availability of CSEM.

2) Information from national law enforcement authorities on the number of searches being carried out online for CSEM

Countries have reported an increase in the number of attempts to access illegal websites featuring CSEM blocked in their filters.

3) The number of reports from the public to law enforcement or other institutions (hotlines)

Spain has noted a significant increase in the number of complaints submitted by the public about CSEM online since the beginning of March 2020 (Figure 1)[2]. From February to March 2020, there was an increase of 100 complaints compared to the previous month. Over more than three years, the number of monthly reports was higher on only two previous occasions.

Denmark has reported an increase in the number of attempts to access illegal websites featuring CSEM. The growth, from 18 sites searched to 55, represents a three-fold increase from one week to another. This is an indication of increased online offender activity or at least demand for CSEM online[3].

4) The nature or volume of new posts on online forums dedicated to child sexual exploitation compared to established baselines

Isolated and 'bored' offenders are stating their increasing interest in image trading. In some countries, there has been an increase in adult offenders attempting to initiate contact with children via social media.

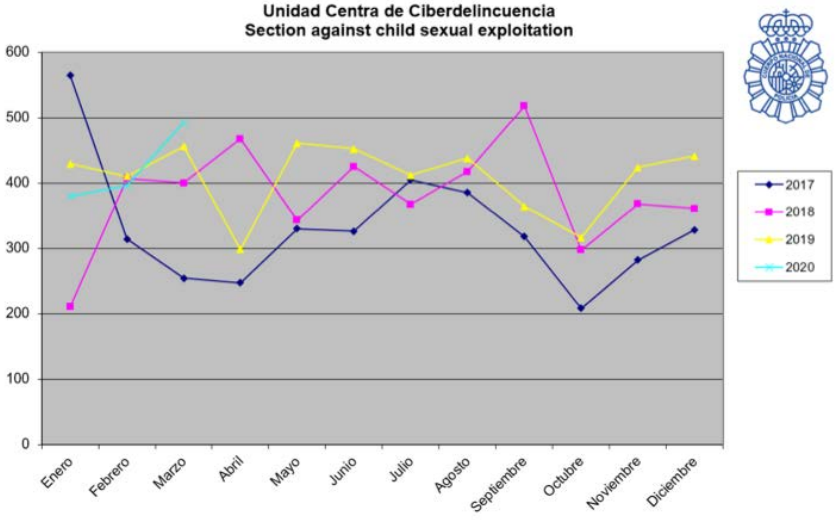


Fig. 1: Number of complaints submitted by the public about the presence of CSEM online 2017-2020. **Source:** Spanish National Police, March 2020.

1 NCMEC – National Center for Missing and Exploited Children (USA), NCECC – National Child Exploitation Crime Centre (CA). Referrals are made on online platforms for CSEM detected on their networks.
2 Contribution to Europol: Spain.
3 Contribution to Europol: Denmark.

5) Conversations between criminals on forums

Discussions about the COVID-19 pandemic are already appearing on child sexual exploitation boards on the dark web. Users there indicate their anticipation that children are going to be spending an increased amount of time online, with references made to the Omegle application. Other users indicate they will have more time to download available material.

Excerpts of discussions posted on CSEM boards on the dark web

1

hello now with this quarantine almost worldwide you think that there will be more children on omegle there will be people taking it out Packs you who think there will be new materials that will go up in boystown there will be more children who without the need to enter omegle suddenly take out pack by fb or by other media suddenly do not upload it by boystown maybe they viralise it in groups you think it will be true all this or not

Source: *Dark web (translated from original.* ***Note:*** *'packs' here is understood to refer to new CSEM. The translation has respected original grammar and punctuation).*

2

As many will know, many countries are alert with the issue of coronavirus. but on the other hand, imagine.... being locked up at home all the time. those who have a child at home or well some of them are taking them at home and spend more time with their children. hahaha I would like to have that situation

Source: *Dark web*

6) Number of detected connections from which CSEM has been downloaded over peer-to-peer file-sharing networks

Spain, for example, has reported a 25% increase between the weeks commencing 17 March and 24 March, as illustrated in Figure 2. Other countries have also reported similar trends.

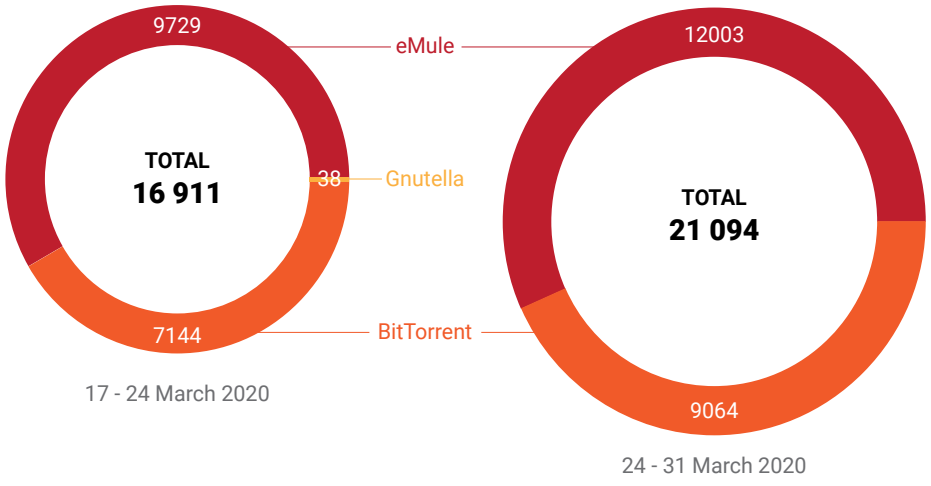


Fig. 2: Detected IPs from which CSEM have been downloaded in Spain from weeks commencing 17 March and 24 March 2020.
Source: Spanish National Police, April 2020

OUTLOOK

Offenders are likely to attempt to take advantage of emotionally vulnerable, isolated children through grooming and sexual coercion and extortion.

Children allowed greater unsupervised internet access will be increasingly vulnerable to exposure to offenders[4] through online activity such as online gaming, the use of chat groups in apps[5,] phishing attempts via email, unsolicited contact in social media and other means.

Adults working remotely subsequently are not as able to supervise their children's internet activity or actively engage with them offline to effectively monitor for signs of stress, isolation and loneliness. Adults working remotely will be more vulnerable to phishing attempts to discover their personal information and that of their family which could then be used by offenders against them and their children.

Children could be more exposed, through less secure online educational applications, to unwanted attention from adults or identification of their personal information[6].

Children may be more inclined towards self-production of CSEM for exchange with peers or to send to others including adults depending on various factors.

4 DailyCaller 2020, Porn And Predators: Activists Warn Of Internet Dangers For Kids During Coronavirus Crisis, accessible at https://dailycaller.com/2020/03/28/porn-predators-internet-coronavirus-children/

5 TechCrunch 2020, Report: WhatsApp has seen a 40% increase in usage due to COVID-19 pandemic, accessible at https://techcrunch.com/2020/03/26/report-whatsapp-has-seen-a-40-increase-in-usage-due-to-covid-19-pandemic/

6 Mercury News 2020, 'Zoom-bombing' on the rise: Hijackers invade videoconferences for work, school, FBI says, accessible at https://www.mercurynews.com/2020/03/31/coronavirus-zoom-bombing-hijackers-videoconferences/

The impact of the COVID-19 crisis on the dark web is still developing. After an initial fluctuation in sales via the dark web at the beginning of the crisis in Europe, the situation stabilised throughout March 2020[7].

Alternative platforms such as social media, instant messaging and secure communications applications are also likely to be increasingly used to facilitate the distribution of illicit goods, including drugs, online[8].

New opportunities

The COVID-19 crisis has provided new business opportunities, such as offering COVID-19 related products. Vendors are also providing discounts on their goods as a means of promoting business in what remains a competitive market. Masks and test kits are the most frequently encountered items offered via marketplaces or vendor shops. Although the intention may purport to be good, this is an easy way to sell fake, counterfeit or poor quality articles anonymously.

The sale of these items is most prevalent on the anonymisation platform Tor but is also evident on another decentralised privacy orientated platform, Openbazaar. Openbazaar is promoting their mobile app Haven as an option to sell COVID-19 related articles.

Only a small number of sales of these items have been recorded so far on the dark web, probably due to availability of similar goods on the surface web and the wider customer base not being traditional dark web users. This has the potential to change if items become more costly and scarce and customers then seek to source them from elsewhere.

CSEM also continues to be distributed via dark web platforms and there are signs of increasing activity around this criminal domain on the dark web during the duration of the COVID-19 pandemic.

7 Contribution from the European Monitoring Centre for Drugs and Drugs Addiction (EMCDDA).

8 Contribution from the European Monitoring Centre for Drugs and Drugs Addiction (EMCDDA).

Demand

The users of dark web marketplaces, vendor shops and other platforms include both individual citizens and criminal groups seeking to obtain illicit products.

The technical barriers to entry are minimal and the dark web is freely accessible to anyone with basic understanding of online technologies.

OUTLOOK

So far, there has not been a notable increase in the number of users buying illicit goods online. However, changes in supply and demand can be expected.

For drug-related items, the outlook will depend largely on supply chains. If it becomes more difficult for users to obtain certain drug choices, addicts might try to obtain their products through alternative methods. This could involve methods that will reduce social distancing and increase risk to public health.

For COVID-19 related items the demand will likely continue to mirror products sought after on surface web platforms. Scarcity on surface web platforms runs the risk of pushing customers to seek out alternative offers on the dark web.

HYBRID THREATS: DISINFORMATION AND INTERFERENCE CAMPAIGNS


Many Member States have reported problems with respect to the spread of disinformation during the current crisis. Hybrid threats are broad and complex attacks on governance. A wide range of measures applied in hybrid campaigns include cyberattacks and disinformation, disruption of critical services, undermining of public trust in governmental institutions and exploiting social vulnerabilities.

Disinformation and misinformation around COVID-19 continue to proliferate around the world, with potentially harmful consequences for public health and effective crisis communication. Some state and state-backed actors seek to exploit the public health crisis to advance geopolitical interests, often by directly challenging the credibility of the EU and its partners.

DISINFORMATION

The spread of disinformation or fake news is a key fixture of the hybrid threat landscape. Users become vulnerable and receptive to disinformation and fake news due to the paradoxical oversaturation with available information combined with a perceived lack of trustworthy sources of news that reinforce some of the users' preconceived notions and believes.

Several institutions keep track of misinformation and fake news about COVID-19, publishing regular updates debunking such claims. The World Health Organization (WHO) keeps track of false claims about COVID-19 on its website, which is regularly updated. It focuses on claims made about the nature of the virus and potential cure and prevention measures[9].

The European External Action Service (EEAS) provides regular updates on the current trends and insights into disinformation activities[10].

The spread of fake news and disinformation is in many cases not considered a criminal offence. The spread of disinformation can originate from a variety of actors, including cybercriminals seeking financial gain and state actors.

9 World Health Organization 2020, Coronavirus disease (COVID-19) advice for the public: Myth busters, accessible at https://www.who.int/emergencies/diseases/novel-coronavirus-2019/advice-for-public/myth-busters

10 EEAS 2020, EUvsDiSiNfo, accessible at https://euvsdisinfo.eu/

CYBERCRIMINALS

Both seasoned cybercriminals and opportunistic individuals spread disinformation in order to benefit from it in different ways. However – not including individuals who derive satisfaction from misleading people – the ultimate aim is always to obtain profit.

Some individuals simply seek to obtain direct financial gain through digital advertisements, as engagement with fake news messages about COVID-19 can be very high. The number of new websites related to COVID-19 has soared in recent weeks.

Another strategy to profit financially from the COVID-19 crisis is to spread fake news about potential cures for the virus or effective prevention measures. In some cases, these messages are relatively harmless, although they may give individuals a false sense of security. However, such messages can also help criminals seeking to sell items that they claim will help prevent or cure COVID-19.

According to the EEAS, state actors also spread disinformation, seeking to sow distrust and destabilise governments. Violent extremists and terrorists are also using the pandemic to spread their message.

OUTLOOK

The spread of disinformation and misinformation around COVID-19 has potentially harmful consequences for public health and effective crisis communication. On a broader level, coordinated disinformation campaigns can feed distrust in the ability of democratic institutions to deliver effective responses to the current situation. Criminal organisations, state and state-backed actors seek to exploit the public health crisis to advance geopolitical interests.

CATCHING THE VIRUS – CYBERCRIME, DISINFORMATION AND THE COVID-19 PANDEMIC

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

www.europol.europa.eu