Catching the virus – cybercrime, disinformation and the COVID-19 pandemic

INTELLIGENCE NOTIFICATION

01 APRIL 2020

Releasable to Europol strategic partner countries, agencies and institutions, EU Commission, General Secretariat of the Council

Contents

Introduction

Criminals active in the area of cybercrime 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 EU during the pandemic, the attack vectors 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 area of criminality. The threat from cybercrime activities during the crisis is dynamic and has the potential to incease further. Europol and particularly EC3 are investing resources and capacities to continue to support MS and other partner law enforcement authorities to counter threats during this difficult situation.

Key findings

- The impact of the COVID-19 pandemic on cybercrime has been the most visible and striking in comparison to other criminal activities.
- Criminals active in the domain of cybercrime have been able to adapt quickly and capitalise on the anxieties and fears of their vicrims.
- Phishing and ransomware campaigns are being launched to exploit the current crisis and are expected to continue to increase in scope and scale.
- Most reporting to Europol relates to previuosly known ransomware families. However, new ransomware faimilies also continue to appear with frequency during the pandemic.
    - The period between the initial infection with ransomware and the activation of the ransomware attack is shorter now than previously seen. Criminal do not wait for the ideal moment to launch the attack but try as soon as it is possible
- Only a slight increase in the number of DDoS attacks has been observed following the outbreak of the COVID-19 pandemic in Europe.
- Activity around the distribution of child sexual exploitation material (CSEM) online appears tp be on the increase, based on a number of indicators including:
    - The number of detected connections from which CSEM have been downloaded over Peer-to-Peer File Sharing Networks
    - The volume of new posts in online forums dedicated to CSE compared to established baselines and conversations between criminals in forums (qualitative)
    - The number of reports from the public to law enforcement or other institutions (hotlines)
- The dark web continues to host various platforms such as marketplaces and vendor shops used for the distribution of illicit goods and services.
    - After an initial fluctuation in sales via the dark web following the beginning of the crisis in Europe, the situation has been stabilising through March 2020.
    - Vendors attempt to innovate by offering COVID-19 related products.
    - Demand and supply dynamics for some goods are likely to be impacted if product scarcity occurs via distributors on the surface web.
- Increased disinformation and misinformation around COVID-19 continue to proliferate around the world, with potentially harmful consequences for public health and effective crisis communication.
    - Coordinated disinformation campaigns seek to frame vulnerable minorities as the cause of the pandemic and to fuel distrust in the ability of democratic institutions to deliver effective responses.
    - Both criminal organisations, state and state-backed actors seek to exploit the public health crisis to advance geopolitical interests.

Cyber-dependent crime

Ransomware

> Ransomware is a type of malicious software criminals use to take the 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 Bitcoins or some other virtual currency. The primary focus therefore is on financial gain.

Throughout the last years, criminals have focused their attacks on organisations. Since many organisations suffer a business disruption when they cannot access their files, criminals have a relatively high likelihood of receiving the payment. The concept as Big Game Hunting (BGH) sees criminals focusing 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 actually potentially lead to loss of life. Other examples include government agencies, universities and organisations within the manufacturing sector.

In the IOCTA 2019, Europol reported how investigators cited over 25 individual identifiable families of ransomware. Several of these featured more prominently in law enforcement reporting, including the various versions of Dharma/CrySiS, ACCDFISA, GlobeImposter, and Rapid. GandCrab, Locky, and Curve-Tor-Bitcoin-Locker also featured prominently in EMAS submissions.

Ransomware is also offered on the dark web as a ransomware-as-a-service (RaaS) product. GandCrab was an example of RaaS.[1] The main distinction between RaaS and other ransomware attacks is the target. Perpetrators of RaaS have low skills as they are renting the service through an underground forum and will most likely target 'low-hanging fruit.'

During the COVID-19 pandemic, most reporting to Europol relates to previuosly known ransomware families, which suggests the involvement of known actors continuing with their business. However, new ransomware faimilies also continue to appear with frequency 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

[1] The Post 2020, Post-GandCrab, Cybercriminals Scouring the Dark Web for the Next Top Ransomware, accessible at https://threatpost.com/post-gandcrab-cybercriminals-scouring-the-dark-web-for-the-next-top-ransomware/147476/

phishing attacks. When the victim clicks on the link or opens a malicious email, the perpetrator can execute his strategy by infecting the device.

Since criminals request payment in cryptocurrency, the ultimate destination of the funds is difficult to identify as cryptocurrencies are more difficult to trace in comparison to traditional forms of payment.

Ransomware: attacks on hospitals and other critical infrastructure during the COVID pandemic

Considering the crucial function of hospitals and medical facilities during a pandemic, a successful ransomware attack on one of these facilities is a primary source of concern. On 13 March 2020, the Brno University Hospital, the second biggest hospital in Czechia, suffered a ransomware attack. The hospital hosts one of the largest COVID-19 testing facilities in the country and had to cancel certain medical interventions and relocate patients to other hospitals.

Europol has received several request to support investigations involving similar criminal groups also involved in ransomware attacks. In one case, a criminal group tried to extort a MS' national health authority demanding 2 BTC in order to avoid DDoS attacks on hospitals.

What is different in terms of the ransomware modus operandi during during the COVID pandemic?

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

The nationalities of suspects engaged in cybercrime targeting the EU during the pandemic are largely the same as before and include national of various countries of Eastern Europe with Ukraine and Moldova featuring prominently.

The period between the initial infection with ransomware and the activation of the ransomware attack is shorter. Criminal do not wait for the ideal moment to launch the attack but try as soon as it is possible. They are aware that in times of crisis the pressure on certain infrastructure is particularly high and that victims are more likely to pay the ransom in order to regain control over their systems. While it is possible that the ransoms demanded as part of attacks may increase in the future, however, currently ransoms demanded during the COVID-1 pandemic remain moderate.

DDoS

Only a slight increase in the number of 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 over the short- to mid-term. Due to a significant increase in the numbers of people working remotely from home, bandwidth has been pushed to the limits, which provides an opportunity for perpetrators to run 'extortion campaigns' against organisations and also critical services/functions.[2] DDoS is an

[2] Security Alliance 2020, TLP AMBER:CIISI-EU ONLY

accessible type of crime with limited barriers to entry, because it is cheap and readily available.

Croatia reported a DDoS attack on an authentication server of a university network which allowed students to continue to study remotely due to COVID-19.

Malicious domain name registration

Following an initial spike in the domains registered related to the words “Corona” and “Covid”, the current figures indicate that the development appears to have stabilised (Fig.1&2). These registered domain names form the backbone for many criminal operations.

Our provider has a ranking system (associated to risk) and only counting domains since 01/01/2020 with a risk score above 50 points, we have (until 28/03/2020, included) a total of 83.356 domains:

- 48.467 domains with the word “corona”
- 35.069 domains with the word “covid”

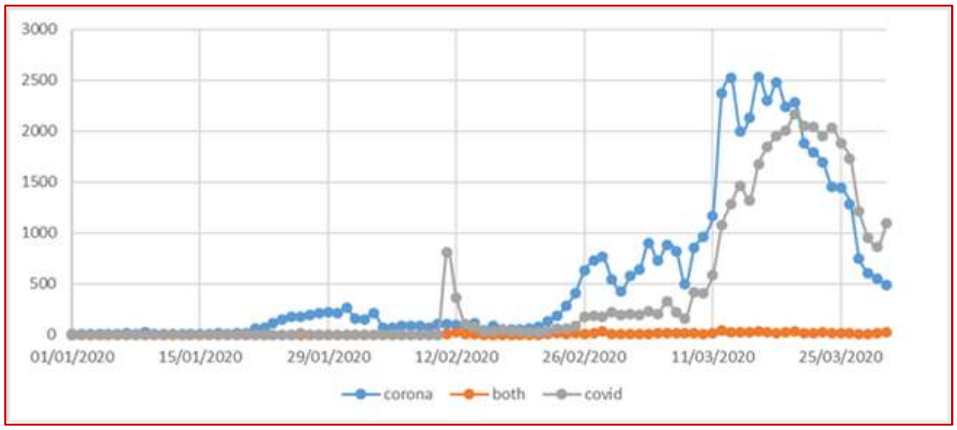


Figure 1. Number of domains registered per day

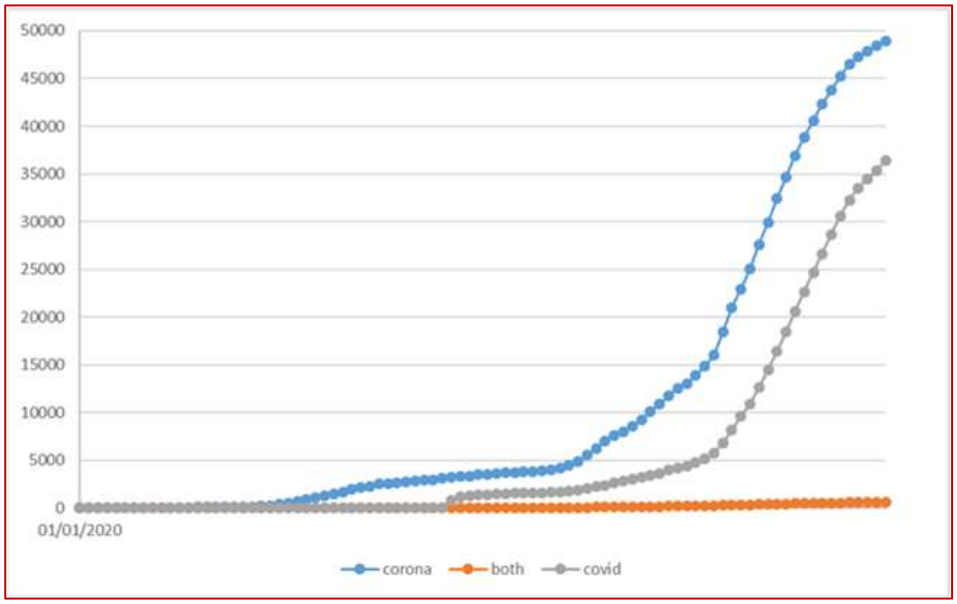


Figure 2. Total number of domains registered

Below is an example to illustrate how criminals abuse domains. This fake government website lures users with the promise of aid or relief. The domain uk-covid-19-relieve[.]com imitated a legitimate "gov.uk" sites and tries to collect personal information and bank account credentials.

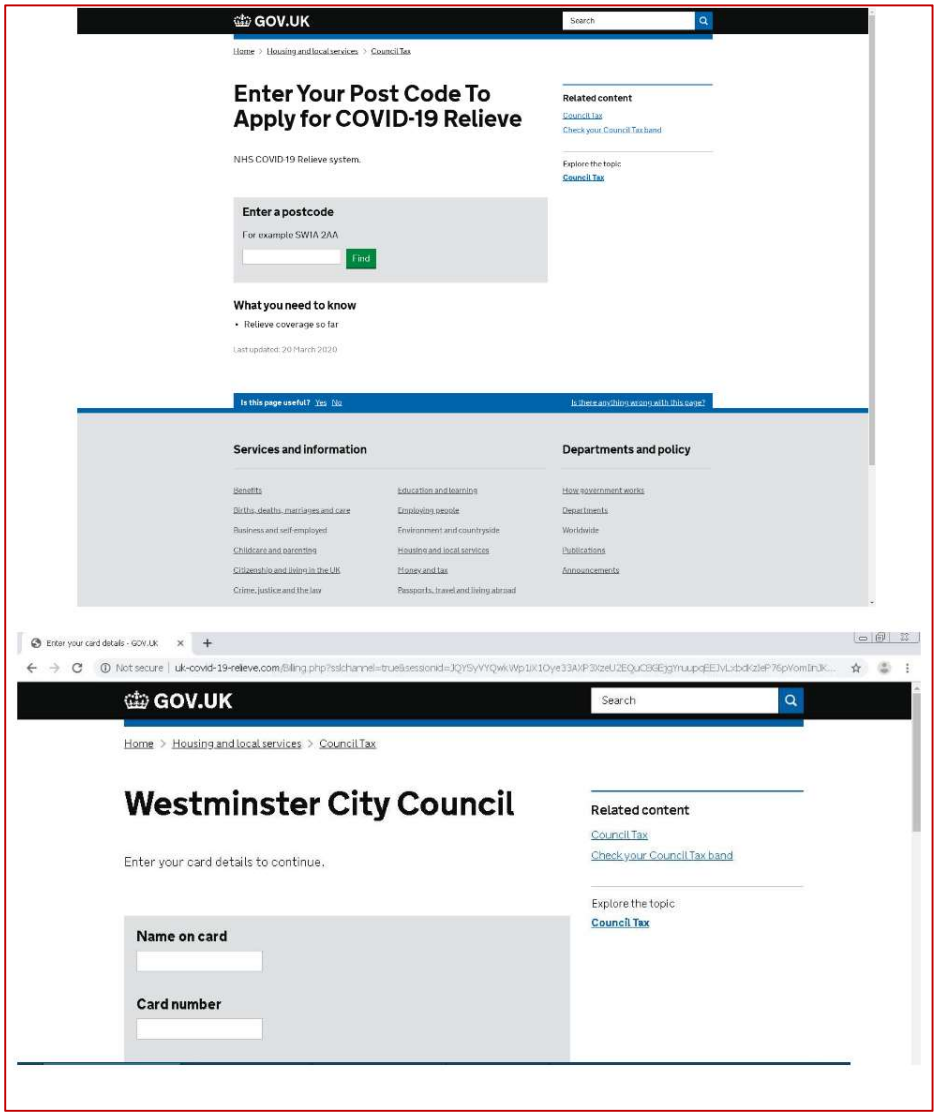


Figure 3. Example of malicious domain registration used to phish for user information.

Source: TrendMicro 2020, Developing Story: COVID-19 Used in Malicious Campaigns, accessible at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains

Outlook

Ransomware has been most dominant cybercrime threat over the last several years. The current crisis situation is unlikely to change that dynamic. The pandemic situation may multiply the damaging impact of a successful attack against certain institutions, which reinforces the necessity for effective cyber-resilience.

Certain groups claimed to have reduced their activity duringh the crisis. However, considering the number of perpetrators active in the scene and the ease with which RaaS attacks can be carried out, Europol does not anticipate a decrease in the level of threat.

The number of phishing attempts exploiting the crisis is expected to continue to increase. We expect a greater number of inexperienced cybercriminals deploying RaaS. However, not all of these campaigns may result in successful attacks due to the lack of experience and technical skills of the criminals.

Child Sexual Exploitation (CSE)

While the totality 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 these specific indicators in the upcoming weeks to assess the impact of the COVID-19 crisis on online CSE and support investigations.

1) Number of Referrals from NCMEC/NCECC[3]

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 due to teleworking, latency in the reporting period, and the use of automatic systems to detect content online rather a decrease in availability of CSEM. NCMEC is expected to provide a situational overview shortly.

2) Information from national law enforcement authorities on the number of searches being carried out online for CSEM from countries which have implemented content prevention/blocking/reporting

So far, one MS, Denmark, has reported and increase in the number of attempted accesses to illegal websites featuring CSEM. The growth was an increase to 3 times the number of sites searched from one week to another, from 18 to 55. This is an

[3] NCMEC – National Centre for Missing and Exploited Children (USA), NCECC – National Child Exploitation Coordination Centre (CA) referrals are made by online platforms for CSE content detected in their networks.

indication of increased online offender activity or at least demand for CSE content online.[4]

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

Spain noted a significant increase in the number of complaints submitted by the public about CSEM online since the beginning of March 2020 (Fig.3).[5] From February to March 2020, there was an increase of 100 complaints on the previous month. Over a period of more than three years, the number of monthly reports was higher only on two occasions.

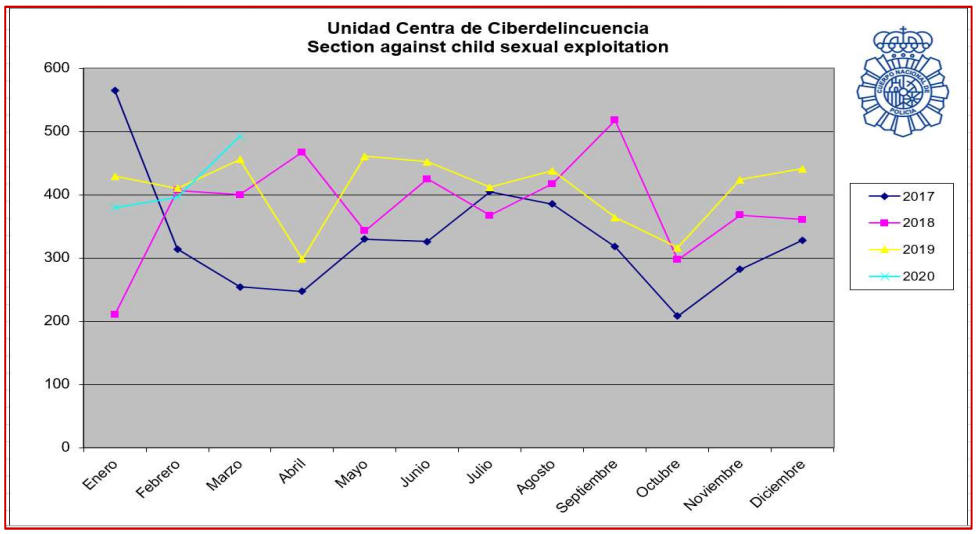


Figure 3. Number of complaints submitted by the public about the presence of CSEM online 2017 – 2020

Source: Police National Spain, March 2020.

4) Volume of new posts in online forums dedicated to CSE compared to established baselines

Isolated and "bored" offenders are stating their increasing interest in image trading. Child profiles are experiencing a greater number of attempts to initiate contact by adult offenders in some countries.

5) Conversations between criminals in forums (qualitative)[6]

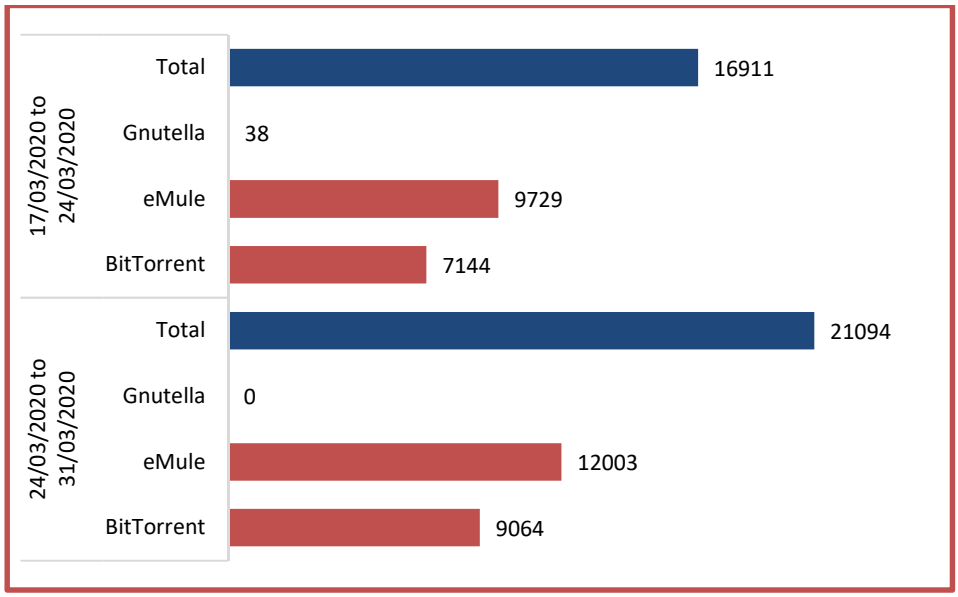
[4] Contribution to Europol: Denmark.
[5] Contribution to Europol: Spain

[6] Europol Monitoring [AP Twins]

Discussion about the COVID-19 pandemic are already appearing on CSE boards on the darkweb (Fig. 4). 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.

6) Number of detected connections from which CSEM have been downloaded over Peer-to-Peer File Sharing Networks

In this Spain has also reported a 25% increase between the week beginning the 17th of March and the week beginning the 24th of March as illustrated below:



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[7] through online activity such as online gaming, the use of chat groups in apps[8], phishing attempts via email, unsolicited contact in social media and other means.

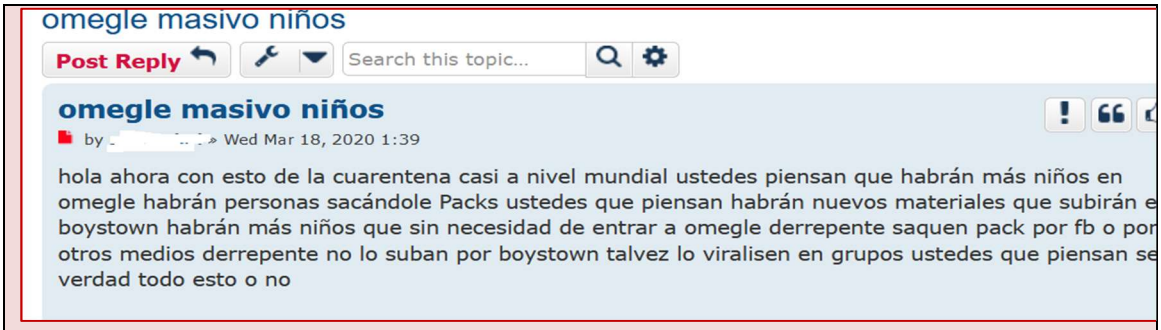
[7] DailyCaller 2020, Porn And Predators: Activists Warn Of Internet Dangers For Kids During Coronavirus Crisis, accessible at https://dailycaller.com/2020/03/28/porn-predators-internet-coronavirus-children/
[8] TechCrunch 2020, Report: WhatsApp has seen a 40% increase in usage due to COVID-19 pandemic, accessible at https://techcrunch.com/2020/03/26/report-whatsapp-has-seen-a-40-increase-in-usage-due-to-covid-19-pandemic/

Adults working remotely will be less able to supervise their children's internet activity and actively engage with them offline to effectively monitor for signs of stress, isolation and loneliness. Adults working remotely will be more vulnerable to phishing attemtps to discover their personal information and that relating to 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.[9]

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.

Figure 4. Examples of online conversations among suspected offenders



TEXT:

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 viralize it in groups you think it will be true all this or not

Source: Boystown (a dark web site)

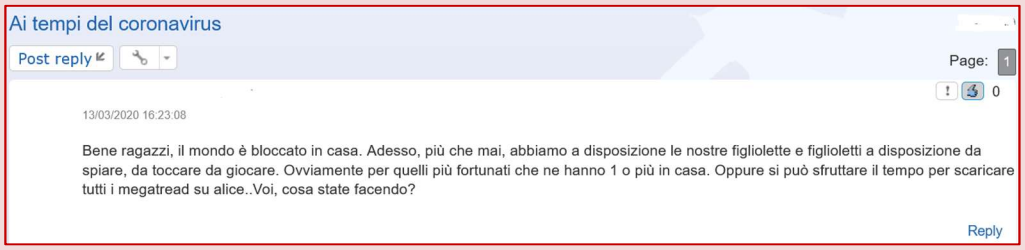
(Note on translation: Packs here is understood to refer to "new CSE material". It can be difficult to make proper English translations of online posts because they don't always follow rules for proper grammar etc.)

[9] 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/

TEXT:

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: Boystown (a dark web site)



TEXT:

Well guys, the world is locked in the house. Now, more than ever, we have our little boys available to be spied on, to be touched to be played. Obviously for the luckier ones who have 1 or more at home. Or you can take the time to download all the megatreads on alice.You, what are you doing?

Source: AliceInWonderland

Dark web

The impact of the COVID-19 crisis on the dark web is still developing. After an initial fluctuation in sales via dark web following the beginning of the crisis in Europe, the situation has been stabilising through March 2020.[10]

Europol's monitoring of the dark web indicated that some vendors are also concerned over increased scrutiny of parcels due to infection reduction processes and increased delays. Some vendors are warning their customers of delays in shipping or have changed their shipping policies to restrict shipping to their own country).[11] There are complaints of some customers that vendors are not reshipping orders if they are not delivered or only reshipping orders within their own countries.

Alternative platforms such as social media, instant messaging and secure communications applications are likely to be increasingly used to facilitate the distribution of illicit goods, including drugs, online.[12]

New opportunities

The COVID-19 crisis has provided new business opportunities such as offering COVID-19 related products. Vendors are also providing discount offers 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 with full anonymity.

The sale of these items dominates on Tor but is also evident on another decentralized privacy orientated platform Openbazaar. Openbazaar are promoting their mobile app Haven as an option to sell COVID-19 related articles.

Only a small number of sales for these items have been recorded so far on the dark web, probably due to availability of like 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.

Also seen on the dark web are advertisements for vaccines and even infected blood and saliva. For the latter, it is assessed the advert was a scam. The dark web criminal community also condemned this and a related post was removed from publication on DREAD, one of the most frequently used forums on the dark web.

[10] Contribution by the European Monitoring Centre for Drugs and Drugs Addiction (EMCDDA)
[11] Contribution by the European Monitoring Centre for Drugs and Drugs Addiction (EMCDDA)
[12] Contribution by the European Monitoring Centre for Drugs and Drugs Addiction (EMCDDA)

Through manual scanning of the dark web marketplaces, Europol identified adverts offering the anti-malarial drug Chloroquine, which is under assessment as an effective medicine for the treatment of COVID-19 patients. At the time of writing several vendors are offering this product on White House market, Empire Market and Dark Bay. However, it is anticipated Chloroquine will also be offered via other markets shortly. At present, the number of listings and of sales is slowly increasing, but still low.

Unsurprisingly, the scale of compromised credit cards and data traded on the dark web has increased in line with fraud developments elsewhere. Carding vendors are announcing special rates and offer high-value credit cards due to the COVID-19 pandemic. The criminal community consider COVID-19 crisis an opportunistic time for carding in the belief people are loading money into their accounts, and criminals are encouraging each other to take advantage of the situation.

CSE 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.

The website darknetlive.com is keeping a record of posts about the impact of corona virus on vendor and marketplace activity: darknetlive.com/corona.

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 on supply chains and country restrictions. 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

This section focuses on the concept of hybrid threats specifically in connection to the spread of disinformation and fake news. 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.[13]

Disinformation and misinformation around COVID-19 continue to proliferate around the world, with potentially harmful consequences for public health and effective crisis communication. In the EU and elsewhere, coordinated disinformation campaigns seek to frame vulnerable minorities as the cause of the pandemic and to fuel distrust in the ability of democratic institutions to deliver effective responses. 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 European Union and its partners.

The European External Action Service (EEAS) provides a taxonomy to highlight different aspects of hybrid threats related to possible actors and behaviour (Fig.5).

	Problem	Diagnosis
Actor	Individual	Is it a person acting in private capacity?
	Nonstate actor	Is it a private or nongovernmental organization?
	Political actor	Does it act on behalf of a recognized political entity?
	Foreign state	Is it a government agency or proxy?

[13] Contribution to Europol.

Behavior	Transparency Dependency Authenticity Infrastructure Intent	Is the actor disguising their identity or actions? Are they acting on behalf of another? Are illegitimate communication techniques used? Is there evidence of backend coordination? Does the behavior suggest a malign intent?
Content	Truthfulness Narratives Synthetic Expression Harm	Is the content verifiably untrue? Does content align with known disinformation narratives? Is the content manipulated? Is the content reasonable self-expression? Is the content harmful?
Distribution	Organic Semi-organic Inorganic Targeting Scale	Is virility commensurate with content and public interest? Does virility suggest an inauthentic boost? Is virility mostly automated/ inauthentic? Is content tailored or microtargeted to individuals? Does the scale indicate an operation or campaign?
Effect	Climate of debate Trust / reputation Freedoms Public health Public safety Election integrity Nat'l security	Is it issue-based e.g. false information, polarization, trolling? Is it target-based e.g. false rumors, hack & leak, forgeries? Is it denying e.g. expression, political deliberation? Does it threaten health wellbeing or medical safety? Does it threaten physical wellbeing or public order? Does it dissuade from vote, undermine result? Does it threaten territorial integrity?

Figure 7.
Source: James Pamment, Carnegie Endowment for International Peace

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 over-saturation with available information combined with a perceived lack of trustworthy sources of news that reinforce some of the users' preconceived notions and believes.

Several reliable institutions keep track of misinformation and fake news about COVID-19, publishing regular updates debunking such claims. The World Health Organisation (WHO) keeps track of false claims about COVID-19 on its website, which is regularly updated. It focusses on claims related to the nature of the virus and potential cure and prevention measures.[14]

The European External Action Service (EEAS) provides regular updates about the current trends and insights into disinformation activities.[15]

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.

Cybercriminals

Both seasoned cybercriminals and opportunistic individuals spread disinformation in order to benefit from it in different ways. However, except for 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 the last couple of weeks.

Another strategy to gain financially from the COVID-19 crisis is to spread fake news about potential cures or effective prevention measures for the virus. In some cases, these messages are relatively harmless, although they might 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.

State actors[16]

State actors also spread disinformation, seeking to sow distrust and destabilise governments.

Russia

Pro-Kremlin media and social media channels particularly focus on Russian aid delivered to Italy, proclaiming that "Russia is helping Italy and the EU is not". The message appears to resonate with domestic EU audiences: several videos are

[14] 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
[15] EEAS 2020, EUvsDiSiNfo, accessible at https://euvsdisinfo.eu/
[16] Source: European External Action Service (EEAS)

circulating on Instagram in Italian showing individuals swapping the EU flag for the Russian flag, or displaying Russian military vehicles on Italian streets. Pro-Kremlin sources also depicted the Chinese "global project" as superior to the EU.

The news outlet Sputnik, under the direct control of the Russian government, has been particularly active in spreading disinformation about COVID-19. This includes a range of messages that COVID-19 is fake, spread by NATO, designed to kill elderly Italians, or created by the US.[17] The last message has also been propagated by China.[18]

For example, the article by Sputnik Belarus which was aimed at a Russian audience (originally written in Russian language) made very specific claims both supporting their own narrative of the Corona virus being man-made as well as anticipating counter-claims on the Corona virus having an ecological origin. Sputnik Belarus published an article on the 22 of January 2020, which describes how the 'new' Chinese Corona virus was likely created in NATO bio labs in China. They accused NATO of researching the human genome to make a virus targeting specific "races". The article "quoted Japanese media" which allegedly reported that this new virus only infects Chinese people, and that the virus was created to create a specific political and economic situation in the region. The article also cautioned against claims that the virus originated from ecological circumstances.[19] Other disinformation news caught by euvsdisinfo.eu include how COVID-2019 was created by a US based laboratory in 2015.[20]

Disinformation further propagates conspiracy theories in cyberspace. In March fondsk.ru published material in Russian claiming that the Corona virus pandemic is a "substitute to a world war" set forward by the "ruling elite" in an attempt to further their own "capitalist" economic interests.[21] Another aspect is propagating that COVID-19 is fake and that deaths in Italy are not due to the Corona virus, rather the fear atmosphere related to it is a politically motivated move destroying smaller businesses and "instilling a deep state hegemony".[22]

China

While Chinese state-controlled media and social media channels did not target the EU as directly, they strongly promoted the idea that the Chinese model is superior in tackling COVID-19, while highlighting global expressions of gratitude for Chinese aid delivery, including in Italy. Experts argue that besides crafting a better international image, China's overall propaganda goal is to maintain social stability at home. To this

[17] EEAS 2020, EUvsDiSiNfo – Disinformation can kill, accessible at https://euvsdisinfo.eu/disinformation-can-kill/
[18] Guardian 2020, 'American coronavirus': China pushes propaganda casting doubt on virus origin, accessible at https://www.theguardian.com/world/2020/mar/12/conspiracy-theory-that-coronavirus-originated-in-us-gaining-traction-in-china
[19] EEAS 2020, EUvsDiSiNfo, accessible at https://euvsdisinfo.eu/report/a-new-chinese-coronavirus-was-likely-elaborated-in-nato-biolabs/
[20] EEAS 2020, EUvsDiSiNfo, accessible at https://euvsdisinfo.eu/report/covid-2019-was-created-by-the-us-in-2015/
[21] EEAS 2020, EUvsDiSiNfo, accessible at https://euvsdisinfo.eu/report/the-coronavirus-pandemic-is-the-ruling-elites-alternative-to-a-world-war/
[22] EEAS 2020, EUvsDiSiNfo, accessible at https://euvsdisinfo.eu/report/covid-19-is-a-fake-its-a-political-move-to-install-hegemony/

end, the Chinese Communist Party also continues to spread disinformation and conspiracy theories about the origins of COVID-19.

With respect to efforts taken by Chinese government supported tactics used on Twitter, the nexus with respect to cybercrime related activities also becomes apparent according to EU- CERT. EU-CERT recently reported on the modus operandi of hijacking accounts of users from around the world to have them post propaganda and disinformation about the coronavirus outbreak.[23] The information originates not directly from EU-CERT or law enforcement but from a group of investigative journalists in the US.

At the same time, generating fake Twitter accounts also occurs as part of a coordinated campaign, through automatically using a repository of fake profile photos and usernames. Both of these tactics demonstrate a resemblance with cybercriminal activities, but are in this case used for a different purpose. [24]

Extremist content online

Violent extremists and criminals are using the pandemic to spread their message. Currently, it appears that the COVID-19 pandemic is a campaign in the making for terrorist groups in particular IS and Right – Wing oriented groups. One should expect terrorists to further exploit the situation and promote their incitement to terrorist acts in the coming weeks.

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. Both criminal organisations, state and state-backed actors seek to exploit the public health crisis to advance geopolitical interests.

[23] ProPublica 2020, How China Built a Twitter Propaganda Machine Then Let It Loose on Coronavirus, accessible at https://www.propublica.org/article/how-china-built-a-twitter-propaganda-machine-then-let-it-loose-on-coronavirus

[24] EU-CERT 2020, COVID-19 Pandemic - Report of 01 April 2020