UNODC
United Nations Office on Drugs and Crime

COVID-19 RESPONSE

COVID-19: Cyber Threat Analysis

United Nations Office on Drugs & Crime
Middle East and North Africa
Assessment & Actions

An overview of current MENA online criminal trends linked to the pandemic and how to circumvent and protect against these relentless attempts at deceiving and defrauding victims.

Produced by the Cybercrime Program at the Regional Office for the Middle East and North Africa (ROMENA)

May 10th 2020

COVID-19: Cyber Threat Analysis

Introduction

November 17th, 2019, this date marked the beginning of a long road for what is now known as the COVID-19 pandemic.[1] Little we could have suspected that we would embark on a global crisis that would challenge all levels of society and all known industrial, commercial and residential sectors of the world. This modern time pandemic has produced new challenges that we have come to expect in times of crisis. The 2004 Tsunami in Asia and the 2010 Earthquake in Haiti are clear examples of how human behavior reacts to crisis that has shaken the world.[2]

Whenever a new crisis emerges, different criminal actors are the first to jump on the occasion to exploit unsuspecting victims in times of fear, uncertainty and doubt. These exploits take multiple forms, from the physical to the digital world. History has taught us that the most efficient method to initially counter these threats is through prevention and awareness towards all levels of corporate and personal life.

The pandemic brings an elevated challenge in this regards that was rarely seen in the past; it is global and affects everyone, regardless of their location, race, ethnicity, religion, social origin, gender, disability or income, or any other status. Even though certain groups are more at risk, those circles of risk could extend to reach our families, friends and coworkers. Considering this context, criminals are out to capitalize on these fears. This paper will focus on addressing the digital aspect of those threats and how to prevent falling further into the victimization caused by this pandemic.

Perspective of the Digital Threat[3]

In a single 24-hour period, April 14th to April 15th 2020:

170,387 Spam emails were found to contain "corona" or "COVID" in the subject line.

19,694 unique IP addresses were used to send those emails.

8,391 unique email domains were used to send those emails.

583 of those emails were found to send an infected attachment. If clicked on, the attacker could take full control of the victim's computer.

This is a single day, and a focus on a single type of threat. It is now easy to imagine the global impact that this can culminate into.

Table of Contents

What are the main threats?

This report will focus on the widely used threats that are plaguing the digital world within this crisis and the new challenges this brought to the cyberspace. It is still early to determine the efficiency of those attacks, but they can be devastating. Nevertheless, we must keep in mind that most of these attacks target anyone using online technology and will exploit their emotions to victimize them. Here is an overview of the different attacks that are witnessed daily and a brief explanation of their inner mechanics and objectives.

Malicious Campaigns

Phishing Emails

Email is and will continue to be the biggest threat vector for individuals and organizations. Cybercriminals have long used major and widely publicized events in phishing campaigns to enhance the efficiency of their attacks, and the current pandemic is no exception.

Several dark web malicious websites are advertising COVID-19 Phishing Email Kits using an infected email attachment disguised as a map of the virus's outbreak for various prices that can range from 150$ up to 1000$. Cybercriminals purchasing these "kits" can then use them to start their email campaigns targeting anyone from individuals to large scale organizations. These infections are made possible by unpatched operating systems and the infected attachment will exploit the weaknesses of the computer it is visualized on.

Different themes are being used in those emails to enhance the click rate of the campaign. It can be anything from reports on the pandemic to health advice from official government sources. Once clicked on, these viruses can include a variety of damages to a system that can range from ransomware, keyloggers and other types of personal information gathering.

They will also advertise the sale of facemasks or other products linked to the Corona Virus outbreak in an effort to both extract a maximum of information from the computer system, it has now infected, along with the possibility of gathering credit card information in the event that an unsuspecting victim purchases fake medical supplies.

Criminals are sending waves and waves of these campaigns that can include over 150,000 to 175,000 emails sent at a time. Multiple campaigns are witnessed daily. Most of these campaigns will include malware which takes advantage of unsuspecting victims to gather personal credentials that can be used in many types of criminality.

The current volume of coronavirus-related email lures, by far, represents the highest number of attacks the Cyberspace has witnessed.

Did you know?

Cybercriminals are currently using the Covid-19 wave to create and exploit infection concerns. But this phenomenon isn't new to the Cyberspace. Cybercriminals have long used fake HIV test results to target healthcare, insurance and pharmaceutical companies globally.

HIV/AIDS PANDEMIC (AT ITS PEAK, 2004-2012)
Death Toll: 32 million
Cause: HIV/AIDS

HIV/AIDS has truly proven itself as a global pandemic, killing more than 32 million people since 1981. Between 2004 and 2012 the annual global deaths from HIV/AIDS dropped from 1.7 million to 770 000.[4]

The online attacks related to HIV/AIDS has already been eclipsed in comparison to the amount of campaigns that want to exploit the Coronavirus panic.

These campaigns serve as a reminder that health-related baits did not begin and will not halt with the latest Coronavirus-themed attacks that we are witnessing. They are operating within a consistent strategy as assailants would perceive the utility of the health-related alarm factor. Often, cybercriminals will attempt to personalize the emails sent within their campaign to ensure the curiosity of the receiver is triggered. The personal information indicated in the email may have been acquired from a public source or previous illicit actions.

If you receive one of those emails, do not open it, especially if you are not expecting any results to be emailed to you. Instead, contact your doctor or health professional directly to discuss results or use a follow-up appointment for any tests that you may have undergone.

This will ensure that you do not fall victim to any potential cyber-campaigns.

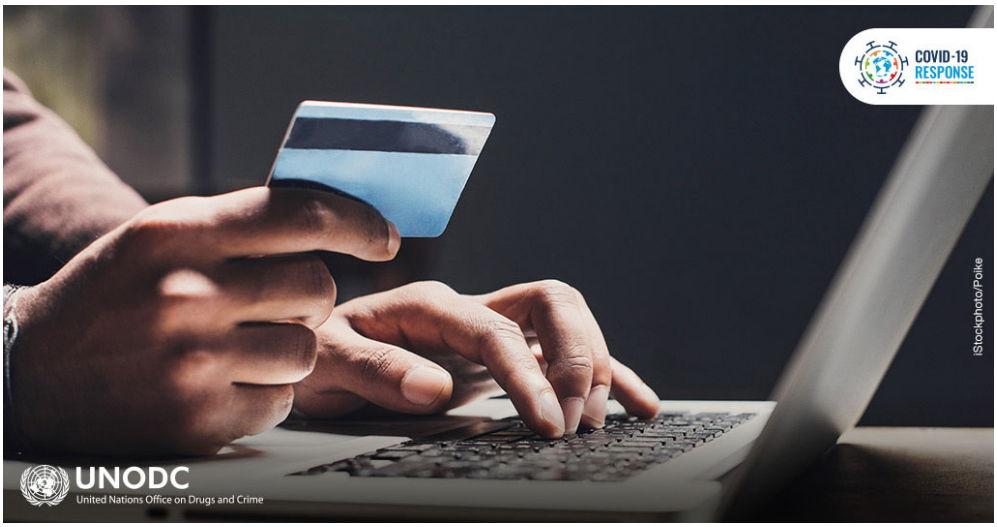
Malicious Domains

New websites are being registered to disseminate information related to the pandemic. However, many of them will also be traps for unsuspecting victims. For the past six weeks, hundreds of domains related to COVID-19 have been registered daily. While some of them are genuine and provide accurate information without ill-intentions, a large portion of them are malicious in nature. As of the end of March 2020, more than 9,000 domains were registered with the Corona Virus theme.

These malicious websites have a wide variety of attacks at their disposal. Here are a few of those attacks:

Impersonating an official website

The National Cyber Security Centre (NCSC) in the United Kingdom (UK) has reported that cyber criminals have impersonated the US Center for Disease Control (CDC), creating domain names like the CDC's web address to request passwords and even bitcoin donations to fund a fake vaccine.[5]

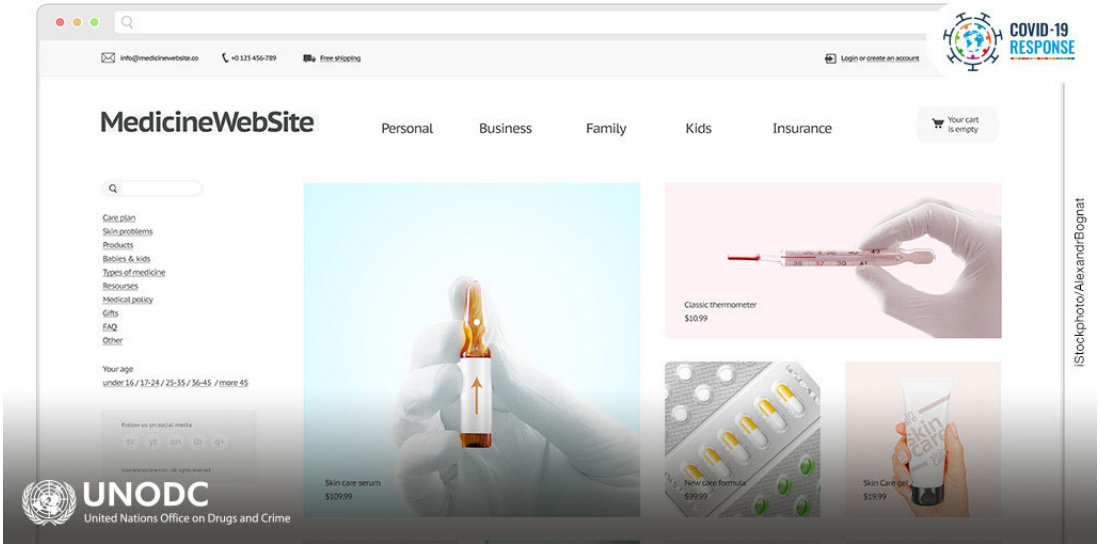


Spreading Malware

Many of these domains will create webpages that are loaded with various malwares designed to exploit the weaknesses of specific operating systems. These malwares can steal credentials of any kind; credit card numbers, banking data, sensitive browser data and export the acquired information for criminal usage. This malicious software can also gather cryptocurrency wallets, take unauthorized control of webcams, gather device information and install a keylogger which will record everything that is typed using the keyboard of the infected system.

Fake campaigns

Websites will also advertise a multitude of services and products and often will request the assistance of the general population to do so. As an example, a website will ask users to donate their computing power to dedicate it towards COVID-19 research, only to deliver information-stealing malware in return.[6] In simple terms, computing power donation is the act of allowing another person/entity to use the processing power of your computer or device so they can perform calculations or other tasks using your hardware. Keep in mind that in this specific scenario, the donation of computing power is only a pretext to ensure they will steal your data.



Disinformation

The concepts of misinformation and disinformation are not new. Evidently, the current situation has made it easy to spread this across all social platforms. A very large portion of internet users are confined in their homes and are using the internet in a heightened capacity which enables misinformation to be posted, re-posted and added upon across any media.

The techniques used are very complex and can take many forms. In fact, every single technique discussed in the present document can be combined as they are all inter-linked.

For example, an employee from a large and prominent international organization receives a phishing email and the person falls into the trap by clicking on the link or opens the attached content. This action has triggered the rest of the chain that will enable the cyber campaign to become much more efficient. The attacker now has access to a multitude of accounts that the unsuspecting victim owned. The criminal can use these accounts to launch further email phishing attacks or can start posting disinformation from the social

media of a well-respected person within the international community. This will add credibility to the false information being spread across different platforms. This is just a simple example that could become quite complex and far stretching beyond normal limits if the attacker is determined into achieving his goals.

What are the objectives of disinformation?

There are many definitions of this concept. Usually the intention is to mislead in order to damage an agency, entity, or person, and/or gain financial or political advantage. It can also be used for sensationalism, dishonesty, or outright fabricated headlines to increase readership. In an era where the number of followers or readers can become a source of financial gain, we can easily understand the reasons behind the efforts deployed for misinformation in the recent years. Regarding this specific pandemic, as it is on every headline across the world, the creators of disinformation are running malicious and covert campaigns by creating stories and misguidance across every sector and every social platform to attain their objective.

There are websites that are trying to investigate misinformation related to COVID-19.[7] In a little over a month, more than 50 articles have been debunked and proven false. It has become exceedingly difficult to keep up with the amount of misinformation related to the current situation. Considering this, it has become more important than ever to ensure that the source of the information is verified, credible and corroborated before any action is undertaken in relation to the news.

Social Media Enhanced Usage

As more people rely on social media for information, for communication with their friends and family, for work, for online shopping and more, the use of all social media has grown exponentially as a result of the COVID-19 crisis. As highlighted below, statistics are now showing this increase and it helps us understand the impact that malicious campaigns cited above could have in the current context. This enables cybercriminals to have a wider base of potential victims to reach within their relentless attempts at defrauding individuals or entities.

The below statistics have been gathered from a survey of more than 25,000 consumers in 30 markets and it was conducted from March 14th to March 24th, 2020.[8]

The application WhatsApp has seen a 40% increase in usage overall. Initially it jumped 27% in usage at the very beginning of the crisis. During the mid-phase of the pandemic, that number reached 41% and finally for countries already in the later phase of the pandemic, WhatsApp usage has jumped by 51%.

In specific countries, the usage can even represent a much higher value. For example, WhatsApp usage in Spain was up to 76%.

However, this application is not alone in its enhanced usage; the study found that Facebook, Instagram, WeChat and Weibo also witnessed a 40% increase in their interaction time.

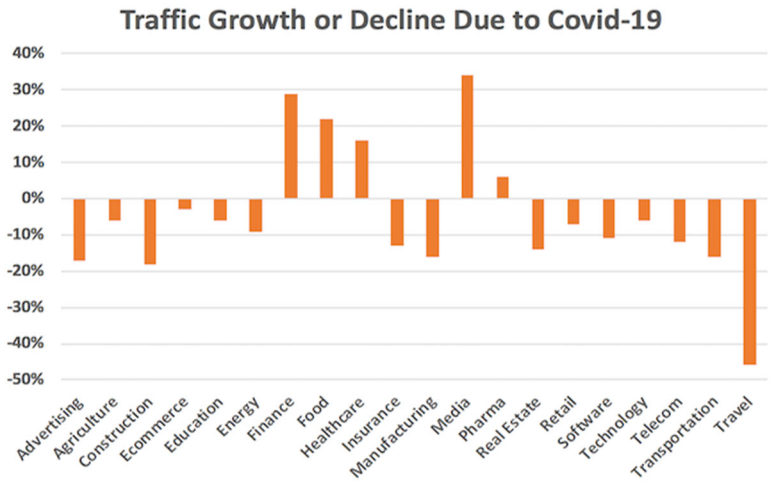


Table 1 ([9])

Most importantly, consumers reported they did not trust their social media platforms for critical news related to COVID-19, despite the increasing usage rates of those applications worldwide. This information is highly commendable and directly shows that the general user base is aware that fake news and misinformation are rampant within these mediums.

National news channels and government agency websites have been considered as better options, with most survey respondents, identifying them as a "trustworthy" source of news and information. Social media platforms, meanwhile, were only considered "trustworthy" by 11% of consumers.[10]

One of the most prominent statistical outcomes resulting from the media usage is the increase of group calls time, which jumped to more than 1,000% during the last month, as reported by Facebook Messenger. This indicates that a large portion of the world are upholding social distancing correctly.

Percent Change in Average Monthly In-Home Data Usage by Device

2019 VS. 2020 - GIGABYTES RECEIVED

	CONNECTED TV	GAMING CONSOLE	PC/MAC	PHONE	SMART SPEAKER	STREAMING BOX/STICK	TABLET	GRAND TOTAL
JAN	26%	6%	-3%	21%	7%	24%	18%	16%
FEB	22%	12%	-5%	27%	-4%	21%	15%	16%
MAR*	27%	12%	-4%	34%	30%	24%	12%	18%

comscore

Source: Comscore Total Home Panel Custom Reporting.
*March compares same 17-day period for both 2019 and 2020

Table 2

Average Daily In-Home Data Usage by Device

GIGABYTES RECEIVED

SUN/MON/TUES PERIOD	CONNECTED TV	GAMING CONSOLE	PC/MAC	PHONE	SMART SPEAKER	STREAMING BOX/STICK	TABLET	GRAND TOTAL
MARCH 17-19, 2019	2.6	3.0	1.4	0.7	0.1	3.9	0.4	12.0
MARCH 15-17, 2020	3.6	4.4	1.6	1.0	0.1	5.4	0.6	16.6
PERCENT CHANGE	37%	48%	15%	53%	44%	38%	33%	38%

comscore

Source: Comscore Total Home Panel Custom Reporting

Table 3

COVID-19 Regional Impact[xi]

(as of April 21st, 2020)

Total Cases

143,317

Total Deaths

6,651

Total Tests Performed

1,992,420

COVID-19 World Impact

(as of April 21st, 2020)

Total Cases

2,529,707

Total Deaths

174,683

Total Tests Performed

22,130,676

Regional Perspective

In context with cyberattacks, the North African and Middle East region is not spared. Cybercriminals are exploiting the fact that authorities are currently occupied to ensure the pandemic does not spiral into an uncontrollable situation. The attackers are taking advantage that governments have reassigned key personnel to ensure the health crisis remains under control. This section will highlight different events that occurred in the region since the beginning of this worldwide pandemic.

MENA cyberspace risks

Banking and Governments Infrastructure

Several events have occurred in the past weeks targeting banking and government infrastructures across the region. As the service has been limited due to numerous curfews across multiple countries of the region, cybercriminals have stepped in to launch various attacks against this critical infrastructure.

While not all attacks are successful, some have allowed cybercriminals to defraud victims in a moment where everyone's savings is becoming important. In some cases, authorities have managed to identify the suspects and official investigations are underway.

Social Media

During this crisis, as people are confined in their homes, many use social media for entertainment and to have fun. Cybercriminals have shifted their attention to several applications used widely in the region to launch various attacks. For example, on April 15th, 2020, the popular application Tiktok, which usage in the region has grown exponentially in the past few weeks, has witnessed several weaknesses exploited by cybercriminals where unapproved and unauthorized videos would be added onto victims account without their knowledge. It is important to note that several regional organizations are using this application and it could lead to misinformation about COVID-19.

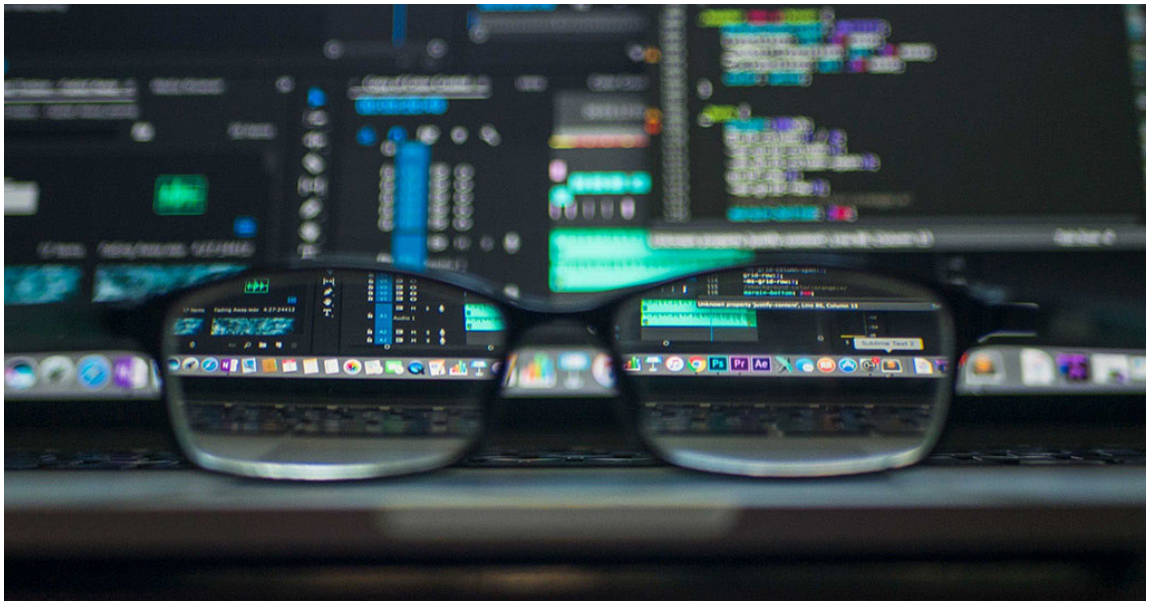
Videoconferencing exploits

While most countries of the region are under curfew, several organizations have enabled their employees to work from home to assist the authorities in reducing the burden of the health sector regarding corona infections. These businesses, however, must still proceed with conducting their activities and have shifted to online applications to entertain meetings and other activities required by their own mandates.

Hence, cybercriminals are always on the lookout for opportunity to exploit different aspects of the online community. As an example, an application used to hold meetings, various conference calls and training became popular since most countries began practicing social distancing. A weakness in the application allowed attackers to take complete control of a session. The cybercriminal could intercept audio and video of everyone within the meeting and could also inject unsolicited content during the conference or training. It goes without saying that these meetings potentially contained confidential information that was then leaked or used in different criminal manners afterwards.

Phishing Campaigns

As it was previously indicated in this document, phishing emails have been a part of life since the late 1990's and the current crisis has only seen an influx of these attacks. In the MENA region, several attacks of this kind have taken place across all industries, local, regional or international. Due diligence has become more important than ever as we all rely on information that is posted online, and we must ensure that the data that we are working on or visualizing is the correct one.



UNODC's Regional Response

The Cybercrime Regional Program is currently engaging in a multitude of technical assistance activities across the region. UNODC's cybercrime experts are responding to the high demand from counterparts regarding this thematic by providing them with the proper equipment, training and counsel.

As the current situation is a challenge for all levels of governments, activities and equipment to be provided have been adjusted to match the current reality and to address the immediate needs of the various regional ministries implicated in the crisis that is shaking the world.

Many risks await governments with the specific attacks indicated in the current document. Data theft, misleading information to the general public, reduced trust, reputational issues are only a few of these risks that could become a reality to any entity. Therefore, a response to these attacks is mandatory. This will ensure to minimize the impacts generated by the cybercriminals in their quest to disrupt public trust and achieve financial gain.

Future plans

The Cybercrime MENA Program has different activities and procurement planned for the following months that will strengthen countries' capacities to respond more efficiently to the COVID-19 crisis from a Digital World's perspective.

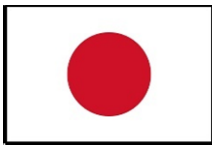
This response can take the following forms:

- Enhanced Cybersecurity for the Critical Infrastructures at the country level.
- Development of Standard Operating Procedures to ensure a proper digital response.
- Procurement of internationally recognized training for first responders and government officials.
- Procurement of digital forensics equipment to ensure proper investigation of various cyber-attacks in the current context.
- Assessment of needs and regional coordinated assistance response.
- Cybercrime investigations specialized interventions to prevent further attacks.
- Digital Forensics response to various crime scenes or data tracking.
- Legislative review and counsel.
- International Cooperation assistance.
- Social Media Awareness campaign on specific pandemic issues.

In the current time, there is an immediate need for these activities to assist countries in ensuring the response is leveled across the world.

As evidently indicated by UNODC's Cybercrime Global Program initiative, "*Now is not the time to de-invest in specialist cybercrime law enforcement. The capability and capacity to counter cybercrime are vital components for protecting Critical National Infrastructure, keeping children safe online, empowering industry, securing hospitals and supporting economic recovery from COVID-19.*"[11]

UNODC Cybercrime team at ROMENA extends its gratitude to the European Union, Government of Japan, Kingdom of Norway and the United States of America who's support has made the efforts aforementioned possible.

The content of this publication is the sole responsibility of UNODC ROMENA and do not necessarily reflect the views of the countries mentioned.

Contributors

The main contributors of the present report are part of UNODC's Cybercrime program at the Regional Office for the Middle East and North Africa.

Mr. Patrick BOISMENU, patrick.boismenu@un.org
Counter-Cybercrime Advisor to the MENA Region and Program Coordinator

Mr. Moustafa ELBANNA, mostafa.elbanna@un.org
Cybercrime MENA Regional Program Officer

Mr. Sadok BEN REJEB, sadok.benrejeb@un.org
Cybercrime National Program Officer in Tunisia

Ms. Nada FARRAG, nada.farrag@un.org
Cybercrime MENA Regional Program Administrative Associate

Referenced Material

1. Dweepobotee Brahma, Sikim Chakraborty and Aradhika Menokee, *The early days of a global pandemic: A timeline of COVID-19 spread and government interventions*, (2 April 2020)
2. UNODC MENA Regional Programme, *COVID-19: How to stay safe from cybercriminals exploiting the pandemic* (March 2020)
3. RiskIQ, *RiskIQ i3: COVID-19 Daily Update* (15 April 2020)
4. UNAIDS, Fact Sheet - World AIDS Day 2019 (1 December 2019)
5. National Cyber Security Centre United Kingdom, *Cyber experts step in as criminals seek to exploit Coronavirus fears (16 March 2020)*
6. Jeremy H, Axel F and Proofpoint threat insight team, *New RedLine Stealer Distributed Using Coronavirus-themed Email Campaign* (16 March 2020)
7. Jane Lytvynenko, *Here's A Running List Of The Latest Hoaxes Spreading About The Coronavirus* (24 March 2020), Jane Lytvynenko, *Here Are Some Of The Coronavirus Hoaxes That Spread In The First Few Weeks* (2 March 2020)
8. Sarah Perez, *Report: WhatsApp has seen a 40% increase in usage due to COVID-19 pandemic* (26 March 2020)
9. Neil Patel, *What The Coronavirus (COVID-19) Means For Marketers* (15 April 2020)
10. Worldometer, *COVID-19 CORONAVIRUS PANDEMIC* (21 April 2020)
11. UNODC Global Programme on Cybercrime, *CYBERCRIME AND COVID19: Risks and Responses* (14 April 2020)