Scientific Voyage
Vol. 1, No. 3,
Page 47-54 (2020)

SCIENTIFIC VOYAGE
ISSN: 2395-5546

GCECT
Publication
Jul.-Sep.

An overview of cybersecurity risks during the COVID-19 pandemic period

Soumit Chowdhury [1], Soumya Mukherjee [2], Saranya Naha Roy [3], Rashed Mehdi [4] and Rishav Banerjee [5]

Department of Computer Science and Engineering, Government College of Engineering and Ceramic Technology, Kolkata 700010, West Bengal, India

Abstract. The COVID-19 pandemic has affected lives of billions of people around the world. The pandemic has and will continue to transform and shape the digital world. New measures are being taken to cope with social distancing norms prevalent around the world. Booming telecommuting, dependence on e-services, virtual events, movement of infrastructure to clouds have become common. All these changes have severe security implications. This paper analyses how people can be affected from the cybersecurity aspect. It highlights some of the most common methods by which people can be manipulated into revealing information resulting in loss/theft of money and/or intellectual properties. It also spells out some common measures that can be taken to dispel much of the risks. Overall, this presented study has tried to highlight most of the potential threats in the digital platform with specific supporting data. Additionally, the paper also focuses on some effective mechanisms to handle these critical issues especially in this pandemic situation of COVID-19.

***Keywords*:** Cybersecurity; COVID-19 pandemic; phishing; cybercrime

1. Introduction

The COVID-19 pandemic has affected life in an unprecedented way. Throughout the world, governments have issued directives for hospitals and other health care facilities to take more precautions and ramp up their resources, for businesses and schools to close, and for individuals to maintain safe social distancing or quarantining if necessary. Digital trade is slowly picking up pace to fill up the void left due to the absence of marketplace trade. After a brief government-imposed hiatus, e-commerce is slowly making its way and is expected to grow much more over the upcoming few months. E-wallets and electronic transactions are gaining traction much more than ever. Medical practitioners are using tele-health services to treat non-critical patients. These have contributed to the need for a digitally connected world that requires transfer of sensitive information. Unfortunately, unscrupulous persons have jumped to the occasion and are using this opportunity to the fullest extent for their benefit. While no one can predict how long the corona virus effects will last, all of us can educate ourselves and take action to protect our identities and wallets.

Main objectives which this report focuses on are as follows:

- 1. Cybercrimes have become a serious threat during this situation as the majority of communications are being done online. Thus, the report aims to discuss the different types of cyber threats in order to spread awareness among the masses.
- 2. The report also focuses on different effects and consequences of the cyber attacks based on previous records, reports and surveys in order to make a concrete understanding of the present situation of the risks associated with cyberspace.

----

[1] E-mail: *joy_pinu@yahoo.co.in*
[2] E-mail: *soumyamukherjee@mail.com*
[3] E-mail: *saranyanaharoy@gmail.com*
[4] E-mail: *rashedmehdi42@gmail.com*
[5] E-mail: *rishav16ban98@gmail.com*

- 3. The report also discusses different methodologies that can be employed to prevent and protect the digital infrastructure of the country and the masses against these cyber attacks.

2. Cybercrime

Cybercrimes are criminal activities carried out by hackers, a group of hackers, organizations, or are often covertly state-sponsored that target computers or a group of computers connected to a network. Cybercriminals are often extremely skilled. They know ins and outs of the systems they are hacking and use advanced techniques that are used to evade security mechanisms in place. Some studies show that due to the government-imposed lockdown and social distancing rules, many criminals have gravitated towards organized cybercrimes [1]. Most commonly cybercrimes are organized for monetary benefits, while others have political or personal motives [2]. Cybercrimes are broadly divided into a couple of categories:

(i) *Crimes that target networks or devices:* Malwares like virus, rootkits and DOS attacks,

(ii) *Cybercrimes that use devices to participate in criminal activities:* Phishing emails, cyberstalking and Identity Theft.

2.1 Cybercrime Methods

In order to protect oneself from cybercrime, one must need to know about the different ways in which computers can be compromised and privacy infringed. In this section, we discuss a few common techniques employed by the cyber criminals and will give a comprehensive idea of the loop-holes in networks and security systems, which can be exploited by attackers, and also their possible motives for doing so.

2.2 DDOS Attacks with botnets

DDoS stands for Distributed Denial of Service. This type of attack is used to bottle an online server with traffic that is much larger than the capacity it is designed for. This causes the service to become unavailable for legitimate users. Botnets are used for such attacks. These botnets are compromised computers that are remotely controlled by hackers and are used to perform all kinds of malicious activities including DDoS attacks by sending spam traffic.

2.3 Phishing and social engineering

This type of cybercrime is most common and is becoming increasingly popular during the work-from-home era. This type of attack involves the cybercriminals sending out dubious email attachments or links that redirect to malicious domains. Often proven social engineering techniques are used to trick users into revealing their secret information via these spam emails. Often cybercriminals would pose as customer service agents and gain your confidence by professional behavior. Later they would trick the user into revealing passwords or OTPs or access codes. These would enable the criminals to gain take control of your accounts and sell them online for monetary gains. A special type of phishing technique is spear phishing. These are specifically made to trick employees of an organization holding key access points, into revealing information. Extensive social engineering techniques are employed to gather background details about the employee such that the phishing emails can be designed to look as legitimate as possible. Verizon's report [3] in 2020 showed that 86% breaches were financially motivated, 22% of data breaches involved with a phishing email. As per a report by Google, there have been 18 million malware and phishing emails each day in April alone, with 240 million other spam mails each day [4].

2.4 Data Theft/ Online Identity Theft

In this type of cybercrime, the attackers employ a variety of techniques to gain access to the target's confidential information such as Personally Identifiable Information, financial information or even medical information. This information can be then used by hackers to conduct tax or insurance fraud, participate in criminal activities by opening a phone/internet account in the victim's name, claim government benefits or perform other imposter scams. In view of the pandemic situation, identity theft is quickly becoming a headache for people working from home. Statistics [5] shows that children and seniors are most likely to fall for identity theft. Malicious fraudsters target users' identity by setting up fake websites related to Covid19, spoofed government and health organization, fake job postings or sending mails related to miracle cures, free check-up or government aids.

Other cybercrimes include spam, data breaches, fraud, cyberstalking, cyberbullying and harassment, child predation, cyber extortion, social blackmail, stock market manipulation, cyber-espionage, attacks on critical infrastructure and information systems, and cyberterrorism.

Tools that are used to commit cybercrime without the victim's knowledge are called crimeware. They are intended to yield financial or other benefits to the attacker. Trojans, viruses, bots, keyloggers, backdoors, e-skimming, spyware, ransomware, scareware, adware, worms, malicious code, and denial-of-service are major examples of crimewares [6].

The following info-graphics demonstrate how the cybercrime rates have increased year-on-year basis:

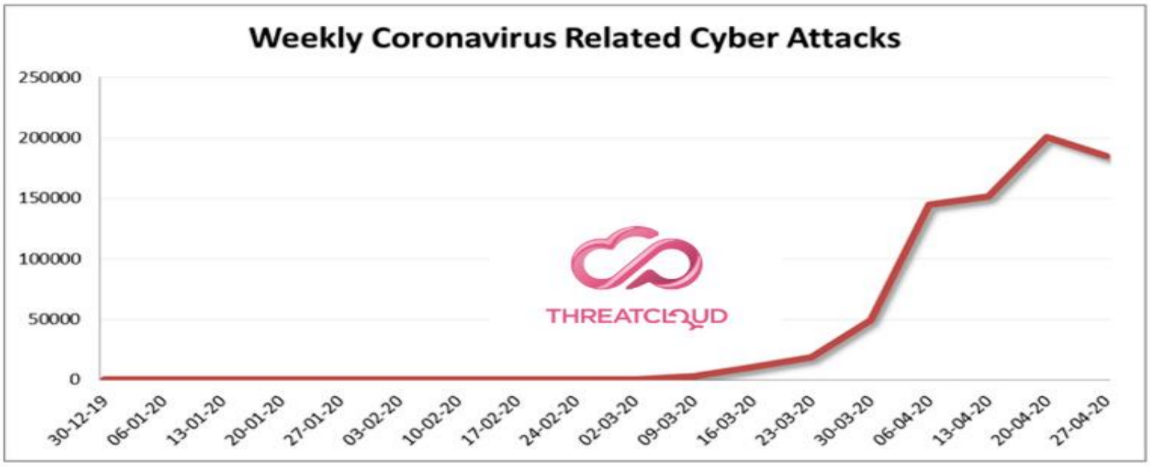
Table 1: Cyber-dependent crime and online fraud record in May 2019 and May 2020

	Count in May 2019	Count in May 2020	Relative Change (%)
Computer virus/malware/spyware	742	648	-12.67
Denial of Service attack	14	18	28.57
Hacking – Server	24	25	4.17
Hacking – Personal	270	479	77.41
Hacking – Social media and emails	939	1,449	54.31
Hacking – PBX/Dial Through	9	7	-22.22
Hacking combine with extortion	313	251	-19.81
Online fraud – Online shopping and auction	5,619	8,482	50.95
All cybercrimes	7,930	11,359	43.24

Table 2: Cyber-dependent crime and online fraud record in May 2019 and May 2020 [1]

		Count in May 2019	Count in May 2020	Relative Change (%)
Cyber-dependent crimes	Individuals	2.300	2,643	14.91
	Organization	260	222	-14.62
Online fraud – online shopping and auction	Individuals	5.408	8,220	51.99
	Organization	194	250	28.87
All cybercrimes	Individuals	7.708	10,863	40.93
	Organization	454	472	3.96

The following graph shows how the cyberattacks have varied with time since the start of this year [7].



3. Cybersecurity risk scenarios

Unlike regular crime, cybercrime is happening every moment in a large scale and the victims are totally unaware of it, until it's too late for them to realise. Any person can simply be doing whatever he/she usually does online, and without any warning, cybercrime can strike. This section tries to explain the most common scenarios that are vulnerable to cyber-attacks and some precautionary measures that one should always keep in mind while using the internet.

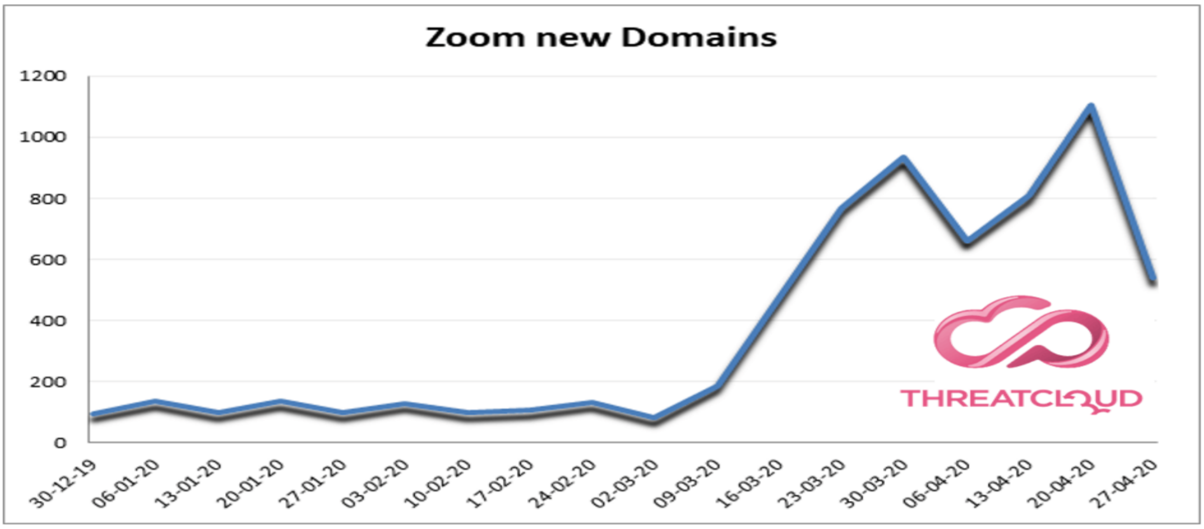
3.1 Risks at Work-from-home

The pandemic has forced the majority of employees to work from remote. Thus, they aren't working within the organization's secure perimeter. Often company leaders and higher-level staff need to access extremely sensitive information that could be accessed only from the workplace systems. Remote access to such computers or connections to those via Virtual Private Networks would be a huge risk for the security and integrity of a company. To prevent attack from cybercriminals, always-on-surveillance and real-time risk analysis of threats and breaches are needed. In this regard CERT-In, the country's nodal agency to counter cyberattacks has issued important advisories to protect people from cyberattacks [8,9].

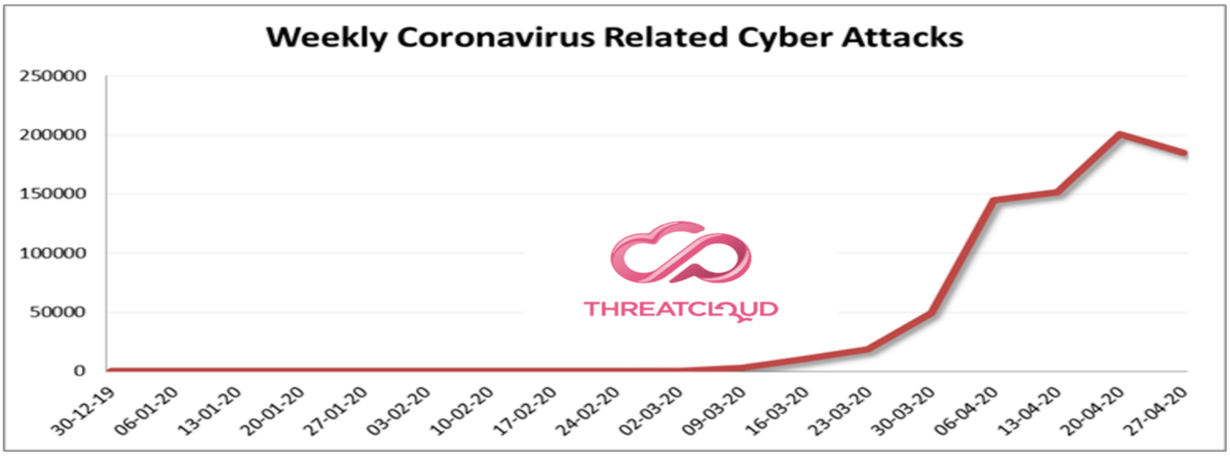
According to a research by Metova [10], as many as 18% of the participants replied that their employers did not have clear security and password guidelines. Another 31% believed work-from-home was less secure than working from the office. Video conferencing has become an integral part of the present WFH times. As many as 76% of all respondents in the Metova's survey responded that they were using video conferencing as part of their daily routine. Insecure network or compromised computers may lead to snooping by third party entities. Often common video conferencing apps may have an unpatched zero-day vulnerability, which may leave them susceptible to attacks. Some important points to keep track of are:

- Security Settings: By default, most video-conferencing apps require passwords to enter a video conference and the host's permission to let the user in, to prevent video bombing. Thus, all users should be made aware of when & how to use them. Hackers can exploit bugs or unattended user permissions to make recordings causing data leakage.
- Phishing: Apps like Slack, Microsoft Teams, and Zoom have messaging components that can be used by attackers to deliver phishing links.

As per a report by Checkpoint Research [11], since the beginning of the year, more than 1700 new domains were registered out of which 4% have been found to contain suspicious characteristics. New phishing websites have been spotted for every leading communication application, including the official classroom.google.com website, zoom, Microsoft teams, slack and others.



- Encryption: Often conferencing app vendors offer features such as automatic transcription, recording, facial recognition, real-time background replacement, noise reduction, echo cancellation, or audio mixing. These require the video stream to be decrypted to separate audio and video data to perform the mentioned activities. The data is usually sent to the vendor's server over encrypted channels. However, the data must travel through many private and public networks to reach its destination. If an attacker gains access anywhere in the path of this data stream, he can record and broadcast corporate secrets and intelligence. Thus, it is necessary to check if the vendor offers a high level of encryption like AES 128 bit or AES 256 bit.
- Post-video archiving: Often meeting metadata is required to be stored for record and future references. Information like these are extremely sensitive, thus need to be stored in secured and air-gapped networks. It is not recommended to store these types of data in personal computers as they can be vulnerable to malware [12].



Based on the joint survey by ISSA and ESG [13], a few important statistics can be noted:

a) 39% of respondents claim that they were very prepared to secure WFH devices and applications while 34% were prepared. 27% were underprepared.

b) 48% say that WFH has impacted the security team's ability to support new business applications/initiatives. Thus, the workloads of the members of the security team have increased.

c) An important consideration is that 70% report that they don’t know or don’t believe that this crisis will lead to cybersecurity becoming a higher priority. Only 30% say that cybersecurity will be a higher priority.

A couple of measures can be taken place to ensure security:

- Use of Cloud: Cloud-based security and platform services reduce the deployment time of the product. Also, cloud-based products are dynamically scalable. Cloud-based secure virtual desktop services give IT professionals remote access to employees' systems, including files and the network. Secure-edge, cloud-based data leakage prevention, and threat-protection controls can help safeguard an organization's critical assets. Moreover, cloud-based managed detection and response services can be extended to remote workplaces.
- Additionally, companies that use secure remote access technology can give remote employees private access (without a VPN) to enterprise applications and systems. Firms can also use privileged access management (PAM) services to allow special remote access to their IT and application administrators. Multi-factor authentication services including biometric and text-based methods enable stringent risk-based access to internal applications that are opened for remote access.

3.2 Risks in online trade and e-commerce

Following government restrictions on social distancing & lockdown, thousands of businesses had to close. Many physical stores, especially small businesses are likely to shut down. Certain fraudsters are setting up websites that mimic well-known retailers both in the URL as well as the look and feel of the websites. They offer essentials supplies at bargain prices which lures unsuspecting customers. The orders are faked and the fraudsters siphon out the payment information entered in those pages. Many businesses such as restaurants are dependent upon mobile applications to run in times of lockdown. Modified and malware infected apps downloaded from non-standard app stores can invite security risks. E-wallets and electronic methods of payment have become important as more and more customers are looking up to these as a solution to contactless payment. Unfortunately, UPI based payment fraud is rising in India, which stems mostly from inadequate knowledge among the masses about the proper usage of the same.

Organizations and individuals need to be aware of a lot of things during this period. A few important points are being highlighted here.

- Sales and distribution of goods: Prices of goods can be manipulated online causing artificial inflation. Similarly, the prices of shares and bonds can be influenced by hoarding.
- Fake websites: Fake websites selling goods at impossible pricing or requiring to pay the amount upfront may attract customers. Most of the time fraudsters disappear without delivering the goods.
- Adequate system audits: Both the consumer as well as business need to monitor, scan, and patch their devices from security vulnerabilities regularly to prevent bugs and exploits especially zero-day vulnerabilities.
- Education about e-payment methods: There has been tremendous growth in e-banking for the last few years due to the sustained push by the government. Proper education about performing transactions is needed for the mass to adapt to it. While the individuals are responsible, it should be the duty of banks and UPI providers to educate the user much more information actively through interactive mediums to engage the user.

3.3 Risks affecting businesses and enterprises

Business Email Compromise (BEC) [14] is one of the preferred methods via which fraudsters can compromise a company. They rely heavily on social engineering tactics to source useful information in order to trick their victims. Email accounts of executives or high-level employees, having the authority to control finance or involved with wire transfer payments are sourced from the internet via company websites, job posting portals like LinkedIn, Glassdoor or via social sites. The fraudsters then spoof the emails and send in emails to the unsuspecting employees that impersonate the CEO or similar highly ranked executives. This is popularly called as ‘CEO imposter Scams’. These emails may contain phishing links, word documents containing macro viruses or keyloggers that enable them to carry out fraudulent transfers. This can result in hundreds of thousands of dollars in losses.

A few cautious practices can prevent such scams [15]:

- Setting up of multi- user approval system that verifies the transaction via order id and approval from finance officers and managers.
- Approval of any changes to vendor payment information and funds request from the concerned people over phone.
- Avoiding transmission of account information, transaction id and other similar sensitive information via email.

Ransomware are a family of malware that demands ransom by restricting the access to the critical organizational data by encrypting them. They work by taking advantage of security vulnerabilities and make the systems unusable until a payment is made. Ransomware has been a problem for businesses even before the corona virus hit. Phishing mails and fraudulent websites are the major distributors of ransomware. Malware and ransomware themes with corona virus have been rampant in the first half of 2020 [16]. It is always advised by anti-virus vendors to not to pay the ransom as there is no guarantee that the files will be decrypted. The largest ransomware attack in history was the infamous WannaCry which hit some of the largest organizations of the world in May 2017. A report published in April 2020 by VMware Carbon Black noticed how ransomware attacks grew 148% on global organisations with the finance industry being heavily targeted [17]. Ransomware samples have risen by 72% in the pandemic period [18]. Regular security audit, application of security patches and upgrading to the latest software are the primary steps that should be followed to resist ransomware attacks.

4. Conclusion

The paper is an attempt to promote educational awareness regarding the most common threats looming in digital platforms during the pandemic period. It discusses the attacks that are gaining popularity during COVID-19 pandemic period. Attacks such as DDoS are mainly centered to disrupt the functioning of an organization resulting in huge loss of the revenue. The organization should always keep a plan ready in case of a DDoS attack and should always monitor its network if there is lack of performance. Attacks such as phishing, coupled with social engineering, are generally designed keeping individuals in mind and mostly try to extract money or to gain access to the personal computers of the victim. Identity theft is also one of the most common attacks. This paper also discusses various vulnerable situations which people are exposed to while working from home or exploring an e-commerce site to buy something and discusses various points to keep in mind in such situations. Finally, we see the various risks of the business enterprise and some precautionary measures to prevent from being a victim.

The work is one of the few papers relevant to this pandemic affected period that focuses on discussion about how the security risks have evolved to take maximum advantage of this situation. This study is done primarily keeping people in mind that have lesser knowledge about the various cyber-threats and the risk they pose to an individual or to an organization. By giving an insight into the motives behind such attacks and various vulnerable situations that a hacker tries to exploit to perform treacherous activities, one can be aware of the ways that lead to cyber-crime. Furthermore, it discusses some basic yet important points to keep in mind while surfing the net or while working remotely on a public network so that cyber-attacks can be avoided. As the security landscape evolves more study on this context can be done.

References:

1. D. Buil-Gil, F. Miró-Llinares, A. Moneva, S. Kemp and N. Díaz-Castaño, *Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK,* European Societies, DOI: 10.1080/14616696.2020.1804973.
2. NYU School of Professional Studies, *Cyberpower and Global Security;* https://www.sps.nyu.edu/homepage/academics/courses/GSCC1-GC1015-political-cybercrime.html.
3. Verizon , *2020 DBIR Summary of Findings| Verizon Enterprise Solutions;* https://enterprise.verizon.com/resources/reports/dbir/2020/summary-of-findings.
4. K. Lyons, *Google saw more than 18 million daily malware and phishing emails related to COVID-19 last week;* https://www.theverge.com/2020/4/16/21223800/google-malware-phishing-covid-19-coronavirus-scams.
5. M. Mott, *Brain Changes as Trust Rises With Age;* https://www.nih.gov/news-events/nih-research-matters/brain-changes-trust-rises-age, Dec 2012.
6. A. Emigh , *The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond* [J. Digit. Foren. Prac. **1** (2006) 245]; DOI: 10.1080/15567280601049985.
7. ThreatCloud , *Coronavirus cyber-attacks update: beware of the phish;* https://blog.checkpoint.com/2020/05/12/coronavirus-cyber-attacks-update-beware-of-the-phish.
8. CertIN, *Coronavirus pandemic (COVID 19) based Cyber Attacks;* https://www.cert-in.org.in/s2cMainServlet?pageid=PUBADV01&CACODE=CICA-2020-2710.
9. CertIN, *Cert-In Advisory CIAD-2020-0008;* https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES02&VLCODE=CIAD-2020-0008.

10. Metova, *Infographic: 1000+ Respondents on Working from Home Due to COVID-19;* https://metova.com/infographic-work-from-home-covid-19.
11. Checkpoint , *COVID-19 Impact: Cyber Criminals Target Zoom Domains;* https://blog.checkpoint.com/2020/03/30/covid-19-impact-cyber-criminals-target-zoom-domains.
12. S. Gode , *Video Conferencing Security Issues and Opportunities;* https://www.unifysquare.com/blog/video-conferencing-security-issues-and-opportunities.
13. J. Oltsik, *The Life and times of Cybersecurity professionals 2020* (A joint report by ISSA-ESG , July 2020).
14. Trend Micro,*Business Email Compromise (BEC);*https://www.trendmicro.com/vinfo/us/security/definition/business-email-compromise-(bec).
15. S. Gressin,*CEO imposter scams: Is the boss for real?* https://www.ftc.gov/news-events/blogs/business-blog/2016/05/ceo-imposter-scams-boss-real , May 16,2016)
16. Trend Micro , *Developing Story: COVID-19 Used in Malicious Campaigns;* https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains.
17. J. Treinen and P. Upatham, *Amid COVID-19, Global Orgs See a 148% Spike in Ransomware Attacks; Finance Industry Heavily Targeted;* https://www.carbonblack.com/blog/amid-covid-19-global-orgs-see-a-148-spike-in-ransomware-attacks-finance-industry-heavily-targeted.
18. SkyBox Security , *2020 Vulnerability and Threat Trends Report;* https://lp.skyboxsecurity.com/WICD-2020-07-WW-VT-Trends_Reg.html.