International Journal of Science and Research (IJSR)
ISSN: 2319-7064
ResearchGate Impact Factor (2018): 0.28 | SJIF (2019): 7.583

Cyber Crime during COVID-19

Adv Purva Saini

Abstract: ***"KARLO DUNIYA MUTHHI ME" these are the true words across the world with the arrival of internet. Internet has become one of the integral part of our daily life. Cybercrime, or computer-oriented crime, is a crime that involves a computer and a network. A crime where a computer is the object of the crime or is used as a tool to commit an offense is cybercrime. Cybercrime is evolving and growing in response to the COVID-19 pandemic. COVID-19 is the infectious disease caused by the most recently discovered coronavirus. This new virus and disease were unknown before the outbreak began in Wuhan, China, in December 2019. COVID-19 is now a pandemic affecting many countries globally.[1]The world is focused on the health and economic threats posed by COVID-19, cyber criminals around the world undoubtedly are capitalizing on this crisis.[2]. The COVID-19 pandemic has forced organisations.***

Keywords: Cyber crime, COVID-19, pandemic, CISA, FINRA, DFS, HIPAA

1. Introduction

Over the past few years, that has been a couple of other pandemics. At this point in time there are still other ongoing pandemics with regards to the Middle East Respiratory Syndrome (MERS) and HIV/AIDS. Ebola is the most recent pandemic which has been deemed as being under control.[3] The term under is under control. Ebola cases still occur and the last outbreak has been reported on the 1st of August 2018. [4] At this point in time, the last confirmed case of Ebola was recorded on the 17th of February 2020, and thus the classification of under control can be used.[5]

Today the world's population is effected by coronavirus. And one third of the population is in coronavirus lockdown. millions of office workers are working from home. These workers attending meetings using tele-working arrangements and accessing non-public data online – sometimes via home computers and private devices. The lockdown increases the scope for criminals to exploit vulnerabilities and commit financial crime.[6]

1.1 Concept of COVID-19

Coronaviruses are a large family of viruses which may cause illness in animals or humans. In humans, several coronaviruses are known to cause respiratory infections ranging from the common cold to more severe diseases such as Middle East Respiratory Syndrome (MERS) and Severe Acute Respiratory Syndrome (SARS). The most recently discovered coronavirus causes coronavirus disease COVID-19.[7]

COVID-19 is the name given by the World Health Organization (WHO) on February 11, 2020 for the disease caused by the novel coronavirus SARS-CoV-2. It started in Wuhan, China in late 2019 and has since spread worldwide. COVID-19 is an acronym that stands for coronavirus disease of 2019.[8] "COVID-19! How can I protect myself and others" is based on the UN Sustainable Development Goals and aims to help young people understand the science and social science of COVID-19.[9]

1.2 Concept of Cyber Crime

The criminals of the twenty first centuary rely on internet and the advanced technology largely for any information required by them to further their criminal intentions. Cyber criminals have evolved their criminal activities to making them profitable. Term "cyber crime "is frequently used in 21st century knowledge society and is created by the combination of two words cyber and crime. The term cyber denotes the cyber space i.e. the virtual space and means od informational space modeled through computer, in which various objects or symbol images of information exist.

However the term crime refers to a social or economic phenomenon and is as old as the human society. Crime is a legal concept and has punishment under law. Crime is a legal wrong that can be followed by criminal proceedings which may result onto punishments.

Cybercrrime is defined as crimes committed on the internet using the computer as either a tool or a targeted victim. Cybercrime is a term for any illegal activity that uses a computer as its primary means of commission. It is an offence that is committed against individuals or group of individuals with a criminal motive or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such as internet.

Levin's case[10] is among the first high- profile cases of hacking for criminal gain. Vladimir a member of a Russian crime ring, succeeded in hacking into citibank's network and stealing confidential information of Citi bank's customers. Using the customer passwords and codes, Vladimir transferred approx. $3.7 million without the banks knowledge or concent.IN 1998 the American court found him guilty and handed Vladimir a three year sentence and ordered him to restitute $240000 to citibank.

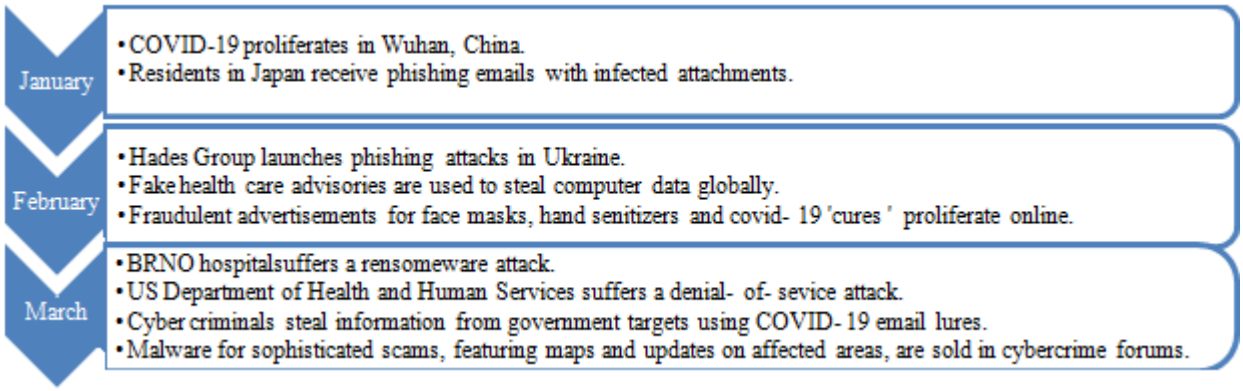
1.3 Effect of COVID-19 on cybercrime

From our Cyber Intelligence Centre, we have observed a spike in phishing attacks, Malspams and ransomware attacks as attackers are using COVID-19 as bait to impersonate brands thereby misleading employees and customers. This will likely result in more infected personal computers and phones. Not only are businesses being targeted, end users who download COVID-19 related applications are also being tricked into downloading ransomware disguised as legitimate applications. Organisations should take proactive steps by advising their staff and customers to be more vigilant and cautious especially when opening links, emails

or documents related to the subject COVID-19. Organizations should ensure their detection and alerting capabilities are functional while keeping an eye on the impact of having many remote workers.[11]

Palo Alto Networks' Regional Vice President for India & SAARC Anil Bhasin said:"Cyber-criminals have been exploiting fears around the COVID-19 outbreak to conduct email scams, phishing and ransom ware attacks. These emails and messages entice users to open malicious attachments by offering more information related to the COVID-19 situation but contain malicious files masked under the guise of links, pdf, mp4 or docx file.[12]
Some Cyber attacks during the pandemic:-[14]

Trishneet Arora, Founder & CEO of TAC Security noted that the low-security standards of home Wi-Fi systems are a serious threat for the cybersecurity sector at the moment with data of millions of people at stake. He observed that the role of cyber security companies at this moment is more critical than ever. It is essential at this moment to monitor baseline behaviours and any anomalous cyber activity should be looked into in real-time basis.[13]



Cybercrime is the greatest threat to every company in the world, and one of the biggest problems with mankind. The impact on society is reflected in the Official Cybercrime Report, which is published annually by Cybersecurity Ventures.[15]The International Criminal Police Organization (Interpol) recently issued a global threat assessment on crime and policing to its 194 member countries.

Security officials in the United Kingdom and United States have issued a joint statement urging individuals and organisations to maintain a heightened level of security and advising them about threats connected to email and message scams that appear to have come from trusted sources (eg the World Health Organisation) and offer medical supplies or treatment to fight the pandemic, or advertise fictitious solidarity initiatives.[16] The statement paid particular attention to cybercriminal actions directed at exploiting vulnerabilities in software and remote working tools, including video conferencing software. According to law enforcement agencies, the main aim of Covid-19-related cyber crime is to steal personal information, induce the download of malicious software, commit fraud or seek illegal gains.

Guidance and published information:-

Some federal and state agencies and industry groups have issued guidance and published information on these threats and recommendations.[17]These are:-

1) The Cyber Security and Infrastructure Security Agency (CISA) published an alert to employers stating that telework options require an enterprise virtual private network (VPN) solution to connect employees to an organization's information technology network. (Mar 13, 2020)
2) The Financial Industry Regulatory Authority (FINRA) published an information notice encouraging firms and their associated persons to take appropriate measures to address increased cyber vulnerabilities and protect customer and firm data on company and home networks as well as mobile devices. (Mar 26, 2020).[18]
3) New York's Department of Financial Services (DFS) issued guidance to regulated institutions in the virtual currency space. DFS urges businesses to implement a preparedness plan to manage the risk of disruption to services and operations in light of the COVID-19 outbreak. (Mar 10, 2020)
4) the Health Insurance Portability and Accountability Act (HIPAA) should review two pieces of guidance from the U.S. Department of Health and Human Services: (1) a bulletin (Feb 2020) addressing application of the HIPAA Privacy Rule in the context of the COVID-19 outbreak, and (2) a notice (Mar 23, 2020) regarding enforcement of HIPAA rules against health care providers in connection with the good faith provision of telehealth during the COVID-19 nationwide public health emergency.
5) California's Attorney General rejected industry requests to postpone the effective date of the state's new data privacy law, the California Consumer Privacy Act (CCPA), which is currently set for July 1, 2020.
6) CISA issued an advisory memorandum (Mar 28, 2020) for state, local, and tribal authorities and their industry partners to assist in the identification of essential workers in seventeen critical infrastructure sectors in light of the COVID-19 pandemic.
7) CISA published a warning to individuals to remain vigilant for scams related to COVID-19. These include emails with malicious attachments or links to fraudulent websites to trick victims into revealing sensitive

information or donating to fraudulent charities. (Mar 6, 2020)

8) The Federal Bureau of Investigation (FBI) issued a public service announcement warning that it has seen a rise in COVID-19-related fraud schemes from scammers trying to steal money or personal information. (Mar 20, 2020)
9) The Federal Trade Commission (FTC) is hosting a page dedicated to helping consumers avoid coronavirus scams, including how to handle robocalls, online offers for vaccinations and home test kits, and how to identify fraudulent emails about government stimulus checks and public health information.
10) The Department of Justice (DOJ) has created a page outlining its efforts to detect, investigate, and prosecute wrongdoing related to fraud schemes and COVID-19.
11) Individual United States Attorney's Offices have also launched efforts to protect residents, such as the Virginia Coronavirus Fraud Task Force.
12) The Consumer Financial Protection Bureau (CFPB) published an informational guidance for consumers regarding the rise of COVID-19 related fraud schemes.
13) Individuals who believe they are a victim of a scam or attempted fraud involving COVID-19 can report it to the National Center for Disaster Fraud Hotline at 866-720-5721 or via email to disaster@leo.gov. Individuals who believe they are the victim of an internet scam or cyber-crime should report it to the FBI's Internet Crime Complaint Center at 804-261-1044 or ic3.gov.
14) A joint advisory published today *(8th April)* by the UK's National Cyber Security Centre (NCSC) and US Department of Homeland Security (DHS) Cyber security and Infrastructure Agency (CISA) shows that cyber criminals and advanced persistent threat (APT) groups are targeting individuals and organisations with a range of ransomware and malware.[19]

2. Conclusion

The COVID-19 pandemic is an unequalled global challenge to all of society The Covid-19 crisis provides a environment for financial crime to the cyber criminals in his favour. Criminals are exploiting vulnerabilities opened up by the Covid-19 lockdown, increasing the risks of cyber attacks, money laundering (ML) and terrorist financing (TF). Authorities have highlighted the need for (i) drawing attention to these crimes so that financial institutions and the general public are better informed; (ii) extra vigilance with respect to increasing and evolving risks; and (iii) active sharing of information between the public and private sectors, and within and between jurisdictions.

COVID-19 will change our lives forever with new work styles, new cyber security issues, new proposed policies, personal hygiene and so on. The fight against COVID-19 is not just for the organisation, employee or customer but a joint effort from everyone. It is also obivious that Post COVID-19, all the organizations, agencies and industrial groups will need to rethink and amend their cyber risk management measures and make new provisions.

References

[1] https://www.who.int/emergencies/diseases/novel-coronavirus-2019/question-and-answers-hub/q-a-detail/q-a-coronaviruses
[2] https://www2.deloitte.com/ng/en/pages/risk/articles/covid-19-impact-cybersecurity.html
[3] World Health Organization. Ebola virus disease. Accessed: 20 March 2020. URL:/
[4] EJ Sirleaf and R Panjabi. Accessed: 20 March 2020. URL: https://time.com/5806459/five-key-lessons-from- ebola-that-can- help-us-win-against-coronavirus-everywhere/16 F Mouton and A de Coning
[5] Medecins SANS Frontieres. DRC Ebola outbreaks - Crisis update - March 2020.
[6] https://www.bis.org/fsi/fsibriefs7.pdf
[7] https://www.who.int/
[8] https://www.goodrx.com/blog/what-does-covid-19-mean-who-named-it/
[9] https://www.who.int/emergencies/diseases/novel-coronavirus-2019/events-as-they- happen
[10] United states v. Levin(1982)ECR 1035
[11] https://www2.deloitte.com/ng/en/pages/risk/articles/covid-19-impact-cybersecurity.html
[12] (http://timesofindia.indiatimes.com/articleshow/74860142.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst
[13] (http://timesofindia.indiatimes.com/articleshow/74860142.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst.
[14] https://globalinitiative.net
[15] https://www.researchgate.net/publication/340443250_Corona_Virus_COVID-19_Pandemic_and_Work_from_Home_Challenges_of_Cybercrimes_and_Cybersecurity
[16] https://media.cert.europa.eu/cert/moreclusteredition/en/securityboulevarde65efcacb6cd9bf31080185461c6e720.20200404.en.html.
[17] https://www.natlawreview.com/
[18] https://www.finra.org/rules-guidance/key-topics/covid-19
[19] https://www.ncsc.gov.uk/news/security-agencies-issue-covid-19-cyber-threat-update