"Cybercrime During COVID-19 and Major Impact"

Developed For
FCAIT, *i*MSc (IT)

Dissertation Report (Sem – VI)
Submitted For
The Partial Fulfilment Towards
The Degree of
Integrated Master of Science (Information Technology)
***i*MSc (IT)**

By

Nandini Agrawal D	A03
Vidhi Asodariya R	A05
Pallavi Sevak R	A54

Under the Guidance of

Internal Guide
(Prof. Kinjal Patel)
FCAIT, *i*MSc(IT),
Ahmadabad

Faculty of Computer Applications & Information Technology
***i*MSc (IT) Programme, Ahmedabad**

GLS UNIVERSITY

Faculty of Computer Applications & Information Technology

***i*MSc(IT) Programme**

Ahmedabad

CERTIFICATE

This is to certify that

1) Agrawal Nandini Devendrakumar 201901619010003
2) Asodariya Vidhi Rakeshbhai 201901619010005
3) Sevak Pallavi Rajanikant 201901619010051

Students of Semester- VI Integrated Msc (IT) [TY iMSc(IT)], FCAIT, GLS University has/have successfully completed the

Dissertation

On

"Cyber Crimes During Covid-19 Pandemic And Major Impact "

as a partial fulfillment of the study of Third year Semester-VI,

Integrated Master of Science (Information Technology)

[*i*MSc(IT)]

Date of Submission: **30-03-2022**

Prof. Kinjal Patel	Prof. Tripti Dodiya
(Project Guide)	**(Project Co – ordinator)**

Acknowledgement

One moment of gratitude for all the faculty member of GLS University and special thanks goes to Director our Guide Prof. Kinjal Patel to allow this great opportunity to us and for providing us the Authoritative guidance on a wide range of initiatives.

We dedicate this success to the entire team, who helped us in every Possible way to achieve this strength with which we are able to present such an incredible Dissertation.

We are much obliged here to thank all the individuals who have contributed in the field of computer Science and IT. Without all their valuable sources, we would never have reached to this stage.

The project helped learn how to do proper Research and we learned about many new things while doing this project. We got the opportunity to explore something new apart from the course. We would like to thank our family members and friends for always being with us on our sides helping us in every way they can.

Table of Content

Glossary of Important Terms and Abbreviations

DDoS: Distributed Denial of Service

MANET: Mobile Ad Hoc Network

PAN: personal area network

UDP : User Datagram Protocol

TCP SYN: Transfer Control Protocol Synchronize

ICMP : Internet Control Message Protocol

GDELT:The Global Database of Events, Language and Tone

CAMEO :Conflict and Mediation Event Observations

AIC : Akaike Information Criterion

HTTPS : Hypertext Transfer Protocol Secure

URL : Uniform Resourse Locator

DNS : Domain Name System

RBF : Radial Basis Function

UCI : Unique Client Identifier

WHO : World Health Organization

CDC : Centers for Disease Control and Prevention

BCE : Business Compromise Emails

WSN : Sensor Networks

IoT : Internet of Things

RDP : Remote Desktop Protocol

VPN : Virtual Private Network

IOT : Internet of Things

INTERPOL : Intertional Criminal Police Organization

Table Of Figures

Abstract

November 17th, 2019, this date marked the beginning of a long road for what is now known as the COVID-19 pandemic. Which got declared as Corona virus pandemic or COVID-19 by World Health Organization. More than 42,30,70,401 cases of COVID-19 have been found leading to 5 lakhs deaths till February 23, 2022. With every passing day, the number of cases and deaths is expanding.

During this isolation period, various digital applications are needed to ensure a normal life for most of the people. Artificial intelligence, machine learning, data analytics, big data, cloud computing, Internet of things (IoT) and other digital technologies are playing a vital role in managing routine activities through work from home, online education, remote patient treatment, citizen protection, risk communication, and medical supplies. On the downside, various technical threats like online fraud and cyber-attacks are rising and increasing challenges in the COVID-19 pandemic. 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. This pandemic brings out the best but unfortunately also the worst in humanity. With a huge number of people teleworking from home, often with outdated security systems, cybercriminals prey on the opportunity to take advantage of this surreal situation and focus even more on cybercriminal activities. it is global and affects everyone, regardless of their location, race, ethnicity, religion, social origin, gender, disability or income, or any other status. With this report we want to warn individuals, companies, public institutions and other organisations about these criminal activities. The objective of this paper is to explore the available COVID-19 statistics and understand the impacts with technical threats to relief measures caused in the current pandemic.

KEYWORDS

COVID-19, Cyber security, Cyber-attack, Cyber- Crime , Impact , Prevention , Cyber – Bullying , Social Media.

Introduction

Corona virus which is currently being called as COVID-19, first time outbreaks in Wuhan, China at the end of December, 2019 and spread worldwide very rapidly. In the wake of the COVID-19 pandemic, there has been a sharp rise in the use of online technologies to support remote work via cloud computing, high speed data networks, software applications, dynamic databases, the internet, and its web component.[8]

Using telecommuting and video conferencing, these technologies have proven to be supportive in remote office collaboration, work-from-home sessions, online academics, andreligious worships; activities that initially entailed physical clusters of persons at specific locations, time frames, and durations. Within the context of computers and computer networks, an attack is any plan to expose, alter, disable, destroy, steal, or gain unauthorized access.

A cyber-attack is any sort of offensive that targets computer information systems, infrastructures, computer networks, or PC devices the year 2020 will be marked as adistinctively disruptive year, not only for the worldwide health crisis but also for the online life being digitally transformed, as exponential change accelerated at home and work via cyberspace.

There are many purposes of cybercrime act which include financial gain, entertainment, and activist for political or religious purpose and for revenge. The impact of any security attacks may lead to losses in monetary, reputation and even nation sovereignty. The purpose of this paper is to analyze different type of cyber attacks that increased or decreased during the epidemic.

The study demonstrates on how criminals can exploit crisis to achieve different type of cybercrimes. In addition, the research articulates on how lacks of awareness at user level contribute to the increase of cybercrimes.

3. WHAT IS CYBER CRIME?

REASON

Cybercrime first started with hackers trying to break into computer networks. Some did it just for the thrill of accessing high-level security networks, but others did it to gain sensitive, classified material. Eventually, criminals started to infect computer systems with computer viruses, which led to breakdowns on personal and business computers.[9]

Computer viruses are forms of code or malware programs that can copy themselves and damage or destroy data and systems. When computer viruses are used on a large scale, like with bank, government or hospital networks, these actions may be categorized as cyber terrorism. [9]

DEFINITION

Cybercrime is defined as crimes committed on the internet using the computer as either a tool or a targeted victim. It is very difficult to classify crimes in general into distinct groups as many crimes evolve on a daily basis.

Even in the real world, crimes like rape, murder or theft need not necessarily be separate. However, all cybercrimes involve both the computer and theperson behind it as victims; it just depends on which of the two is the main target.

Hence, the computer will be looked at as either a target or tool for simplicity's sake. For example, hacking involves attacking the computer's information and other resources. It is important to take note that overlapping occurs in many cases and it is impossible to have a perfect classification systemCybercrime is defined as crimes committed on the internet using the computer as either a tool or a targeted victim.

3.1 Computer as a Tool:

When the individual is the main target of Cybercrime, the computer can be considered as the tool rather than the target. These crimes generally involve less technical expertise as the damage done manifests itself in the real world. Human weaknesses are generally exploited. The damage dealt is largely psychological and intangible, making legal action against the variants more difficult.

These are the crimes which have existed for centuries in the offline. Scams, theft, and the likes have existed even before the development in high-tech equipment. The same criminal has simply been given a tool which increases his potential pool of victims and makes him all the harder to trace and apprehend.

3.2 Computer as a Target:

These crimes are committed by a selected group of criminals. Unlike crimes using the computer as a tool, these crimes require the technical knowledge of the perpetrators. These crimes are relatively new, having been in existence for only as long as computers have - which explains how unprepared society and the world in general is towards combating these crimes.

There are numerous crimes of this nature committed daily on the internet. There are so many varieties of crimes that are committed on the internet daily; some are directed to the computer while others are directed to the computer users. In this study, we have identified some common crimes committed.

4 TYPES OF CYBER CRIMES

4.1 PHISHING ATTACK

It is one of the easiest forms of cyber-attack for an attacker to carry out; through it, they can invade every important thing of their target's lives. Most of the time, phishing has been witnessed in the wild in emails.[2] More than 900 k threats are there across email, URL and file according to data collected by smart protection network. So It's an attack in which the threat actor poses as a trusted person or organization to trick potential victims into sharing sensitive information or sending them money. Phishers take advantage of fear of the virus and the curiosity to find out information about it such as the number of confirmed cases and mortality, disease symptoms, and possible treatment methods to established successful phishing campaigns. According to APWG report, 267,372 phishing campaigns were reported in H1 of 2020, increasing (19.06%) over 2019 during the same period. These campaigns targeted different sectors such as SaaS/email, financial institutions, payment, and social media.[11]

4.1.1 How phishing attacks work?

Phishing attacks begin with the threat actor sending a communication, acting as someone trusted or familiar. The sender asks the recipient to take an action, often implying an urgent need to do so. Victims who fall for the scam may give away sensitive information that could cost them. Here are more details on how phishing attacks work: [11]

The Sender: In a phishing attack, the sender imitates someone as trustworthy. Depending on the type of phishing attack, it could be an individual, like a family member of the recipient, the CEO of the company they work for, or even someone famous who is supposedly giving something away. Often phishing messages mimic emails from large companies like PayPal, Amazon, or Microsoft, and also banks or government offices.

The message: Under the guise of someone trusted, the attacker will ask the recipient to click a link, download an attachment, or to send money. When the victim opens the message, they find a scary message meant to overcome their better judgement by filling them with fear. The message may demand that the victim go to a website and take immediate action or risk some sort of consequence.

The Destination: If users take the bait and click the link, they're sent to an imitation of a legitimate website. From here, they're asked to log in with their username and password credentials. If they are gullible enough to comply, the sign-on information goes to the attacker, who uses it to steal identities, pilfer bank accounts, and sell personal information on the black market.

4.1.2 EXAMPLES

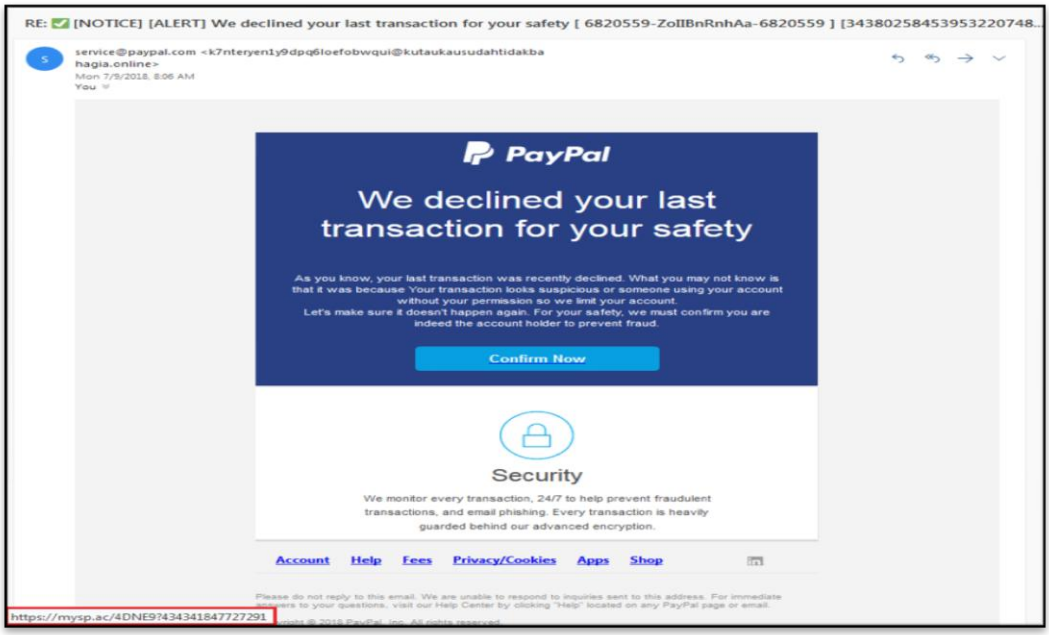
Certain phishing Web sites were being remarked and are now blocked

• adaminpomes[.]com/em/COVID-19/index-2[.]php

• bookdocument[.]in/Covid-19/COVID-19/index[.]php

• glofinance [.].com/continue-saved-app/COVID-19/index[.]php

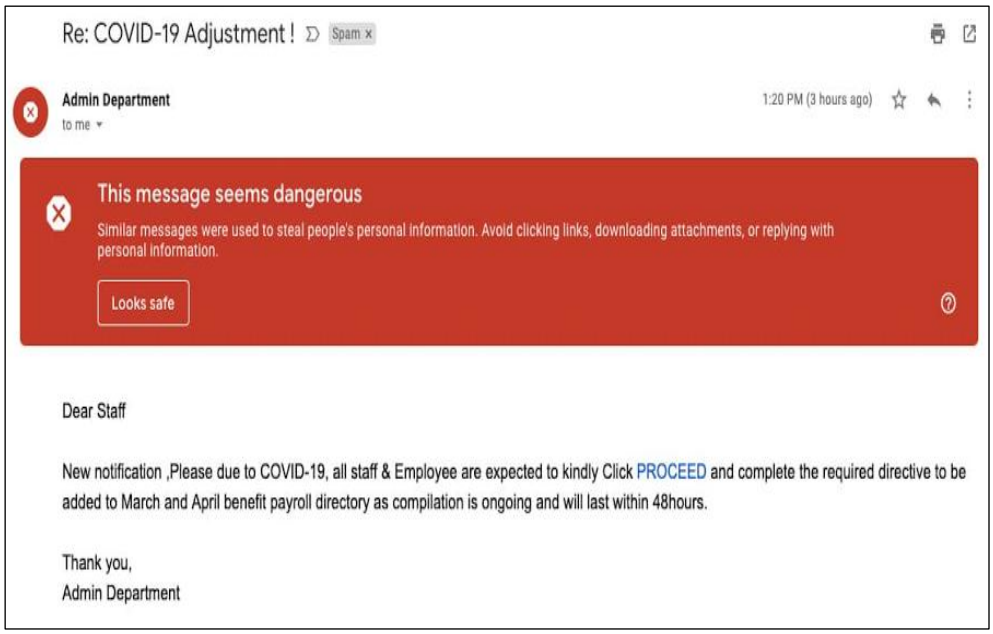
• laciewinking[.]com/Vivek/COVID-19



[Figure 1 Phishing attempt that spoofs a notice from PayPal]

In the Figure 1, a phishing attempt that spoofs a notice from PayPal, asking the recipient to click on the "Confirm Now" button. Mousing over the button reveals the true URL destination in the red rectangle.Victims were deceived by pretending that the message was from the national or global health authorities, governments, offers of vaccines and medical supplies, urging charitable donations related to COVID-19. [11]

Figure 2 presents a phishing email which has been sent to specific employees pretending to be from company management.



[Figure 2: The Phishing E-Mail]

4.2 Email Spam

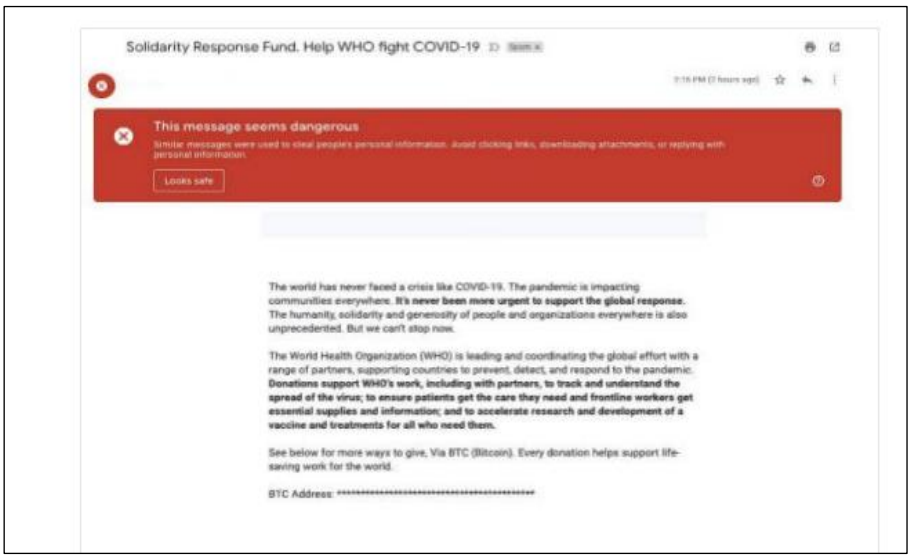
Email is a means of information transfer from any part of the world that is extremely fast and cost effective and can be used from personal computers, smartphones, and other last-generation electronic gadgets.[14]

4.2.1 Usage of email

Despite the increase in usage of other forms of online communication such as instant messaging and social networking, emails have continued to take the lead in business communications and still serve as a requirement for other forms of communications and etransactions.

Emails are used by almost all humans. It is estimated that by the end of 2016, there will be over 2.6 billion email account holders worldwide and it is estimated that nearly half of the world population will be using emails by the end of 2020.

Emails are considered as one of the most used tools, as it is used in phishing campaigns, spear phishing, spamming, spreading fake news, fraud, and Fake donation campaigns . Moreover, emails are considered as the most official communication media between companies and employees, so cybercriminals take advantage of this circumstance to increase their campaigns.



[Figure 3: Example of an email impersonating the world health organization (WHO)]

Figure 3, is an example of an email impersonating the World Health Organization (WHO) intended to request fraudulent donations to COVID-19 patients. Most of the URLs that were registered as a threat belong to phishing scams, such as exploiting people sitting at home and posting offers for a free Netflix subscription on social media App (Facebook or Twitter). The post contains a malicious link; when clicked; the victim will be transferred to a fake Netflix login page designed to capture their login credentials.

They also use websites to promote applications that they claim to protect their users from the Coronavirus. It has been shown that they infect users' devices with a hypothetical virus called: Black NET RAT. This tool adds the affected device to a botnet used for DDoS attacks, stealing the Firefox cookies, saved passwords, and Bitcoin wallets. As discussed, malware threats were detected during the first half of 2020.

A Trojan called QNodeService sent via a fake email shown as tax exemption notice due to COVID-19 from United States government to deceive the victim. Trojans stole the victim's credentials from Chrome and Firefox browsers and managed data on victims' devices.Agari Cyber Intelligence Division reported a Business Email Compromise attack as the intruders took advantage of COVID-19. The attack was carried on by the Ancient Tortoise, a cybercrime organization behind several BEC cases in the past.

This attack is believed to be a series of the previous attacks the group launched earlier. The attackers first target the bank accounts. Then they use the information of the customers and send them emails to change their bank information and payment methods due to the novel coronavirus. The attackers pretend to be from legit organizations or businesses. In the current situation, the business email compromise scams are using coronavirus disease as a tool.

The scam works by convincing or tricking the targets into making transactions to an intruder who shows him/herself as a legit employee working in the same company.The Reports say that there has been a 667% increase in the number of successful email attacks since February 2020 Between March 1 and March 23, over 9000 email attacks were related to COVID-19 compared to 1,188 in February, and just 137 in January (Shi, 2020)

4.2.2 Techniques for Mitigating E-mail Spam

Prior to machine learning techniques, many different technical measures were employed for spam filtering, like - rule-based spam filtering, white lists, black lists, challenge-response (C/R) systems, spam filtering, honey pots, OCR filters, and many others, each with its own merits and drawbacks. Black-lists, white-lists, challenge-response (C/R) systems, etc. are origin-based techniques used by reputation-based filters. As part of awareness activities, organizations should educate their users on the social engineering techniques that are employed to trick users into disclosing information. [14]

Examples of recommendations to avoiding email spam and other forms of social engineering include:

- ✓ Never reply to email requests for financial or personal information. Instead, contact the person or the organization at the legitimate phone number or website. Do not use the contact information provided in the email, and do not click on any attachments or hyperlinks in the email.
- ✓ Do not provide passwords, PINs, or other access codes in response to emails or unsolicited popup windows. Only enter such information into the legitimate website or application.
- ✓ Do not open suspicious emails file attachments, even if they come from known senders? If an unexpected attachment is received, contact the sender (preferably by a method other than email, such as phone) to confirm that the attachment is legitimate.
- ✓ Do not respond to any suspicious or unwanted emails. (Asking to have an email address removed from a malicious party's mailing list confirms the existence and active use of that email address, potentially leading to additional attack attempts.)

[Figure 4: Spam Mail]

4.3 Ransom-ware Attack

Ransomware is a type of malicious software that prevents/ blocks users access to a computer system unless a ransom is paid. Some ransomware might allow access but encrypts sensitive data, victim's files, drives making them inaccessible with demand for a ransom payment to decrypt them in bit coin and other crypto currencies. The rise of ransom ware as a cybersecurity threat is nothing short of spectacular - from its dormant introduction nearly three decades ago, to present day, where ransomware is widespread and has become a serious threat.[17]

Cybercriminals are launching ransomware attacks in hospitals, health centers, education, and public institutions. Since they can't afford to be locked out of their systems because of the current situation, criminals are optimistic that these organizations can pay the ransom. The ransom ware infects the system via email attachments, links, or through working employees whose credentials are already compromised by exploiting a vulnerability in their systems . Cybercriminals are now even offering ransomware-as-a-service on the dark web. A new ransomware named CoronaVirus was uploaded and spread through a fake Wise Cleaner (system optimization software) website. The victims were lured to download the fake setup file from the site. Once the victim installs this malware on their computer, this malware can steal a password, encrypts the data which cannot be unencrypted later on, and also steals information from the system as well.

[Figure 5: Ransom-attack Example]

4.3.1 EXAMPLES

1. UHBVN Ransom ware Attack

Uttar Haryana Bijli Vitran Nigam was hit by a ransomware attack where the hackers gained access to the computer systems of the power company and stole the billing data of customers. The attackers demanded Rs.1 crore or $10 million in return for giving back the data.

2. WannaCry

India was the third worst-hit nation by WannaCry ransomware, affecting more than 2 lakh computer systems. During the first wave of attacks, this ransomware attack had hit banks in India including few enterprises in Tamil Nadu and Gujarat. The ransomware majorly affected the US healthcare system and a well-known French car manufacturing firm.

3. Mirai Botnet Malware Attack

This bot net malware took over the internet, targeting home routers and IoT devices. This malware affected 2.5 million IoT devices including a large number of computer systems in India.This self-propagating malware was capable of using exploitable unpatched vulnerabilities to access networks and systems.

4. Petya

India was one of the top 10 countries to be hit by Petya ransomware. This ransomware attack halted work at one of the terminals of India's largest seaport causing computer lockdown and serious consequences for the country's exports.

5. BSNL Malware Attack

The state-owned telecom operator BSNL was hit by a major malware attack, impacting nearly 2000 broadband modems! 60,000 modems became dysfunctional after the malware attack hit the Telecom Circle.

4.3.2 Proactive Measures to Prevent Ransomware Attacks

As we continue to develop smart cities and smart grid technologies in 2021, the risk of ransomware attacks will stay put as a big challenge for all organizations. Apart from focusing on development and advancement, every industry vertical must understand the crucial role of cyber security.

With the help of these below listed proactive measures organizations can reduce or prevent the constantly evolving ransomware attacks in the future:

Employee Awareness Training:

Cyber threat actors majorly use emails as bait in attempting cyber attacks on an organization and humans being the weakest link tend to easily fall for it. So to avoid and overcome this problem, organizations must educate their employees by making them aware of the prevailing cyber threats. A right security attack simulator and awareness training tool can help in reducing the threat of employee error. Such tools help in mitigating existing cyber risks within the organization and enhance the cyber security posture.

Backup Your Data Separately: The best way to stay proactive is by backing up your data in a separate external storage device but it should not be connected to your computer. Backing up your data will help in securing it from being encrypted and misused by cyber attackers.

Regular Vulnerability Assessment: Basic cyber security hygiene like vulnerability assessment and penetration testing can help in preventing malware like ransomware. With the help of continuous vulnerability assessment, one can find out the exploitable vulnerabilities and fix them before any threat actor discovers it.

Never Click on Unverified Links: Avoid clicking links that are attached in spam emails or on an unfamiliar website. Such links are the bearers of malicious files that badly infect the user's computer when clicked. Moreover, these links are the pathways for ransomware to access the user's system and encrypt or lock confidential data for ransom.

4.3.3 DETECTION TECHNIQUES

[1] Static-based analysis Detection:

The most common type of static analysis, which is commonly used in commercial virus scanners, is referred to as signature analysis. In signature analysis, code string patterns (signatures) are extracted from the target application's code and compared to a repository of known malicious code patterns[17]

[2] Dynamic-based (behavioural) analysis detection:

Dynamic-based analysis detection entails the live monitoring of processes, in order to determine if any are behaving with any malicious intent. Any maliciously behaving process will be flagged as dangerous and terminated.

Suspicious setup Behaviour:

- payload persistence
- Anti-system restore
- Stealth techniques
- Environment mapping
- Network traffic
- Privilege elevation

[3] Machine-learned behavioural-based detection:

A behavioural approach to ransomware detection requires a decision making algorithm that accepts a quantitative behavioural trace of a running process as an input, to output a simple binary decision - yes it is safe/benign or no it is ransomware.

Classification Scheme:

- Real-time operation
- Resource light
- Easily updateable

In recent years, new ransomware have been discovered, including:

Net walker: Created by the cybercrime group known as Circus Spider in 2019, this ransomware allows hackers to rent access to the malware code in exchange for a percentage of the funds that are received.

Dark Side: Dark Side is a recent group that ultimately targets theft and encryption of sensitive data, including backups through RaaS.

Conti: Conti ransom ware uses a double-extortion technique to encrypt data on an infected machine. Attackers from this group usually send a phishing email originating from an address that the victim trusts.

Revel: Also known as Sodden and Sodinokibi, REvil is a ransomware group that has gained a reputation for extorting larger ransom payments than their competitors, as well as promoting underground cybercrime forums.

Since these newer strains of ransomware behave differently today, there is now a need for alternate methods of detection. Recently defenses have begun to harden, including improved heuristics or behavioral analysis, and the use of canary or bait files for earlier detection. Additionally, increased effort needs to be put into predicting and anticipating risks rather than the old "detect and respond" approach.

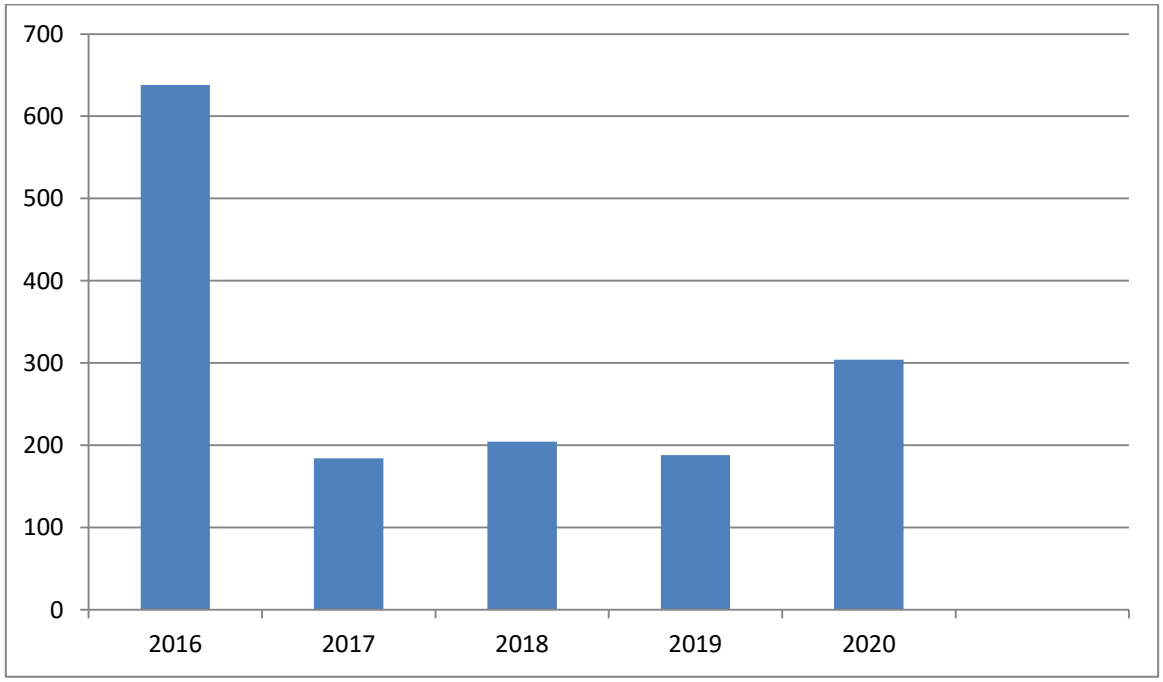
[4] Robust behavioural-based malware detection:

A robust behavioural-based malware detection solution should be one whose performance is invariant to system noise. [17]

This system noise should include general noise introduced by variability in development techniques as well as purposeful noise introduced by obfuscation techniques. 13 labs.mwrinfosecurity.com RansomFlare uses high level behavioural features that have shown to generalise behaviour well even under the presence of obfuscation noise. This is evident when tested against the polymorphic ransomware Virlock, where RansomFlare generates the same behavioural feature set over multiple execution runs of Virlock samples.

Static-based detection is effective against known ransomware, however the continuous influx of new ransomware proves difficult to detect on an acceptable time scale. Furthermore, static obfuscation - particularly in the form of malware factories - is being used to avoid detection of known ransomware.

A more effective ransomware detection scheme is one that has predictive capabilities to make intelligent threat inferences of unknown processes. This can be achieved by treating all running executables as unknowns, where the threat level is continuously updated based on how the executable is behaving. RansomFlare uses such an approach by using dynamic (behaviour) analysis in conjunction with machine learning to provide predictive abilities capable of zero-day ransomware detection.



[Figure 6: Ransom ware attacks during 2016 to 2020]

4.4 DDOS Attack

4.4.1 A Brief History of DDoS Attacks

The first known distributed denial of service attack occurred in 1996 when Panix, now one of the oldest internet service providers, was knocked offline for several days by a SYN flood, a technique that has become a classic DDoS attack. Over the next few years DDoS attacks became common and Cisco predicts that the total number of DDoS attacks will double from the 7.9 million seen in 2018 to something over 15 million by 2023.[23]

4.4.2 Definition

It is an attack that focuses on making computer systems unresponsive and unavailable resulting the running services on those systems unavailable for anyone. Distributed DoS attack is launched from many computers distributed across the internet, Because these attacks come from thousands of machines at once, they are difficult to combat by simply blocking traffic from machines, especially when attackers forge the IP address of attacking computers, making it difficult for defenders to filter traffic based on IP addresses.

Example:

Most of the government and healthcare organizations have seen a rapid increase in the Distributed Denial of Services (DDoS) attack in the current pandemic due to COVID-19. The hackers flood the organizations' websites or systems with fake or bot users to crash the normal functioning of the system and thus interrupt the communication channel.

A recent example of this happened when a DDoS attack targeted the website of the Department of Health and Human Services (DHoS) in the U.S. by flooding millions of users at a time. Distributed Denial of Service (DDoS) attacks in the networks needs to be prevented or handled if it occurs, as early as possible and before reaching the victim.

Dealing with DDoS attacks is difficult due to their properties such as dynamic attack rates, various kinds of targets, big scale of botnet, etc.

Distributed Denial of Service (DDoS) attack is hard to deal with because it is difficult to distinguish legitimate traffic from malicious traffic, especially when the traffic is coming at a different rate from distributed sources. The researchers noted that DDoS attacks increased during the COVID-19 crisis as threat actors exploited the pandemic to execute large and small-sized attacks on various victims, including healthcare, education, and government.

Consequently, the research group witnessed an expanding attack landscape in 2020 caused by the COVID-19 pandemic. The report states that DDoS attacks continue to be the biggest nuisance during the COVID-19 pandemic and in the foreseeable future. Most notably, A10 Networks witnessed an increase in DDoS weaponry by 12% within the second half of 2020.

Rich Groves, Director of Security Research at A10 Networks says that the increase in the number of DDoS weapons and connected devices, the 5G network rollout, and the use of new exploits and malware by attackers, “made it very easy for these IoT devices to be compromised.”5G’s improved internet connection speeds led to increased internet traffic, ultimately leading to an increase in the number of attacks.[23]

A10 report also correlated with Amazon and Google’s observations indicating that DDoS attacks peaked at 2.3 Gbps on amazon web services and 2.5 Gbps on Google’s cloud platform. Akamai also blocked 809 million packets targeting the Akamai platform on June 21, 2020.The high volume of online shopping occasioned by COVID-19 pandemic also led to increased DDoS attacks during the holiday shopping season.

4.4.3 Top DDoS weapons by size include Simple Services Discovery Protocol and SNMP

The team discovered changes in the DDoS weapon choice used by threat actors during the DDoS attacks experienced during the COVID-19 pandemic. The previously-preferred DDoS weapon Portmap dropped in popularity to the third position during the second half of 2020.Simple Services Discovery Protocol (SSDP) became the most preferred DDoS weapon used in 2,581,384 attacks, while SNMP (1,773,694) took the second position. ODNS Resolver (1,706,338) and TFPT (1,409,121) occupied the fourth and fifth positions respectively.

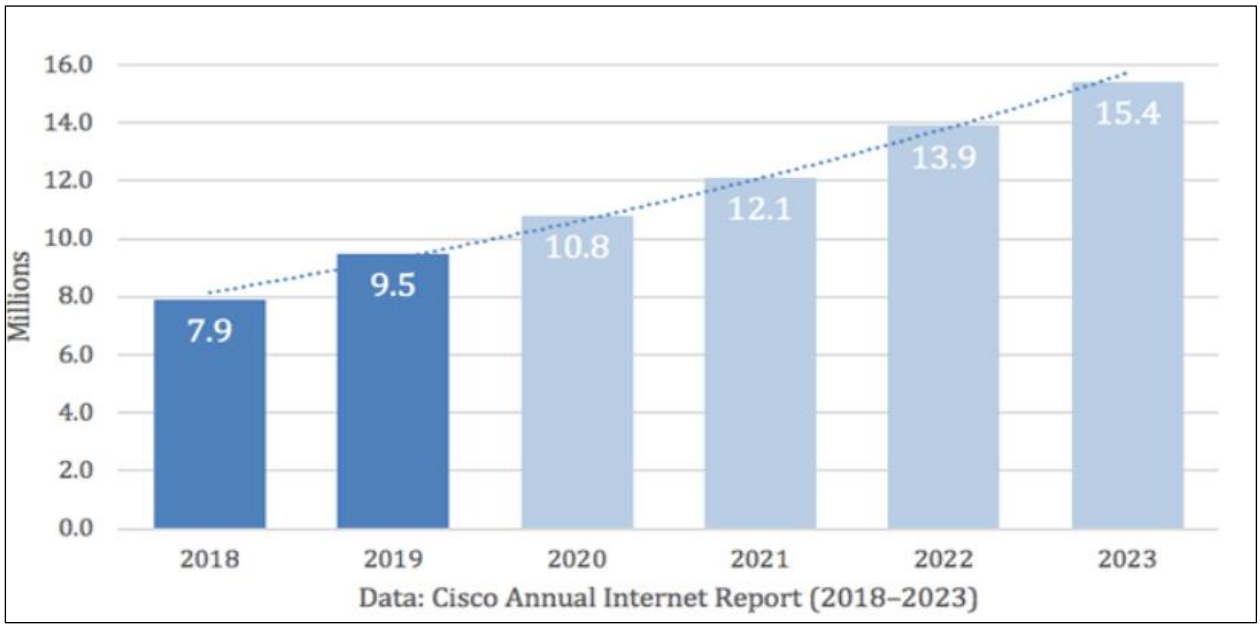
4.4.4 Exponential growth of bonnets witnessed during the COVID-19 crisis

A 10 researchers noted exponential growth in DDoS attacks from botnets located in India. Botnets are compute nodes including routers, IP cameras, servers and computers, IoT devices, etc., infected with malware and used to carry out DDoS attacks.

The report authors noted that botnets "provide the ultimate flexibility to DDoS attackers as they can be sourced from different locations across the globe, depending on the attacker's requirements."

A10 network researchers found 130,000 unique IP addresses exhibiting scanning behavior resembling that of the Mirai botnet in the first two weeks of Sept. 2020. The research tracked a total of 846,700 botnet agents during the period.A leading Indian broadband provider was the single largest contributor of DDoS activity, according to the report. The broadband provider was associated with up to 200,000 unique sources of "Mirai-like" activity at the height of the campaign.

4.4.5 DDOS Attack Example



[Figure 7 Total DDOS Attacks]

1. The Google Attack, 2020

On October 16, 2020, Google's Threat Analysis Group (TAG) posted a blog update concerning how the threats and threat actors are changing their tactics due to the 2020 U.S. election. At the end of the post, the company snuck in a note:

In 2020, our Security Reliability Engineering team measured a record-breaking UDP amplification attack sourced out of several Chinese ISPs (ASNs 4134, 4837, 58453, and 9394), which remains the largest bandwidth attack of which we are aware.

2. The AWS Dodos Attack in 2020

Amazon Web Services, the 800-pound gorilla of everything cloud computing, was hit by a gigantic DDoS attack in February 2020. This was the most extreme recent DDoS attack ever and it targeted an unidentified AWS customer using a technique called Connectionless Lightweight Directory Access Protocol (CLDAP) reflection.

This technique relies on vulnerable third-party CLDAP servers and amplifies the amount of data sent to the victim's IP address by 56 to 70 times. The attack lasted for three days and peaked at an astounding 2.3 terabytes per second.

3. The Mirai Krebs and OVH DDoS Attacks in 2016

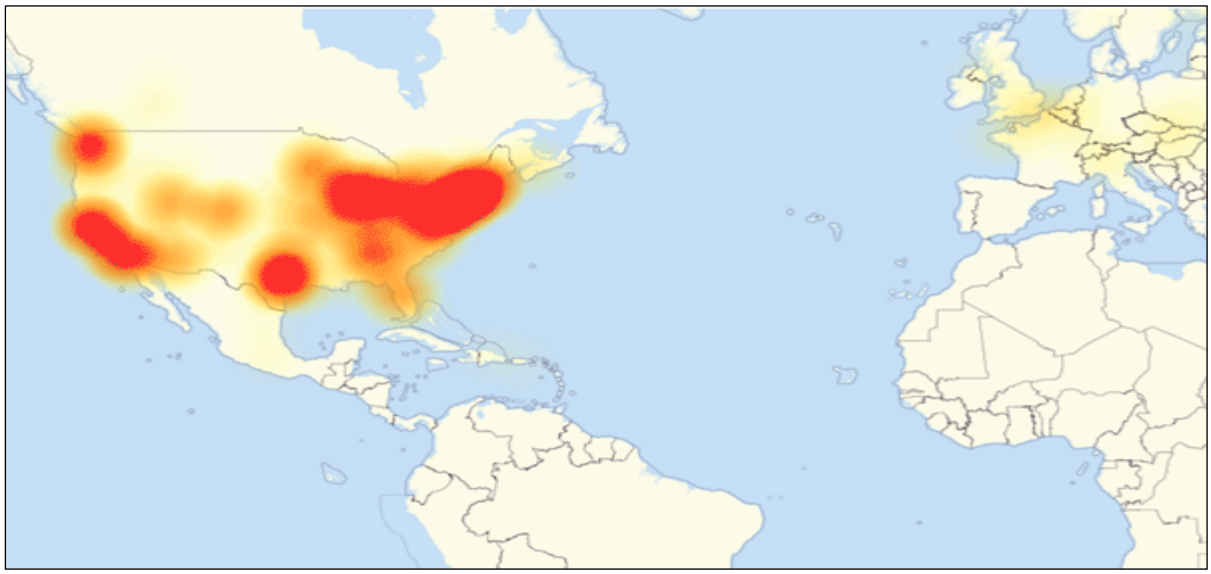
On September 20, 2016, the blog of cybersecurity expert Brian Krebs was assaulted by a DDoS attack in excess of 620 Gbps. Krebs' site had been attacked before. Krebs had recorded 269 DDoS attacks since July 2012, but this attack was almost three times bigger than anything his site or the internet had seen before.

The source of the attack was the Mirai botnet, which, at its peak later that year, consisted of more than 600,000 compromised IoT devices such as IP cameras, home routers, and video players. The Mirai botnet had been discovered in August that same year but the attack on Krebs' blog was its first big outing.

The next Mirai botnet attack on September 19 targeted one of the largest European hosting providers, OVH, which hosts roughly 18 million applications for over one million clients. This attack was on a single undisclosed OVH customer and was driven by an estimated 145,000 bots, generating a traffic load of up to 1.1 terabits per second. It lasted about seven days. But OVH was not to be the last Mirai botnet victim in 2016.

4. The Mirai Dyn DDoS Attack in 2016

Before we discuss the third notable Mirai botnet DDoS attack of 2016, there's one related event that should be mentioned. On September 30, someone claiming to be the author of the Mirai software released the source code on various hacker forums and the Mirai DDoS platform has been replicated and mutated scores of times since.



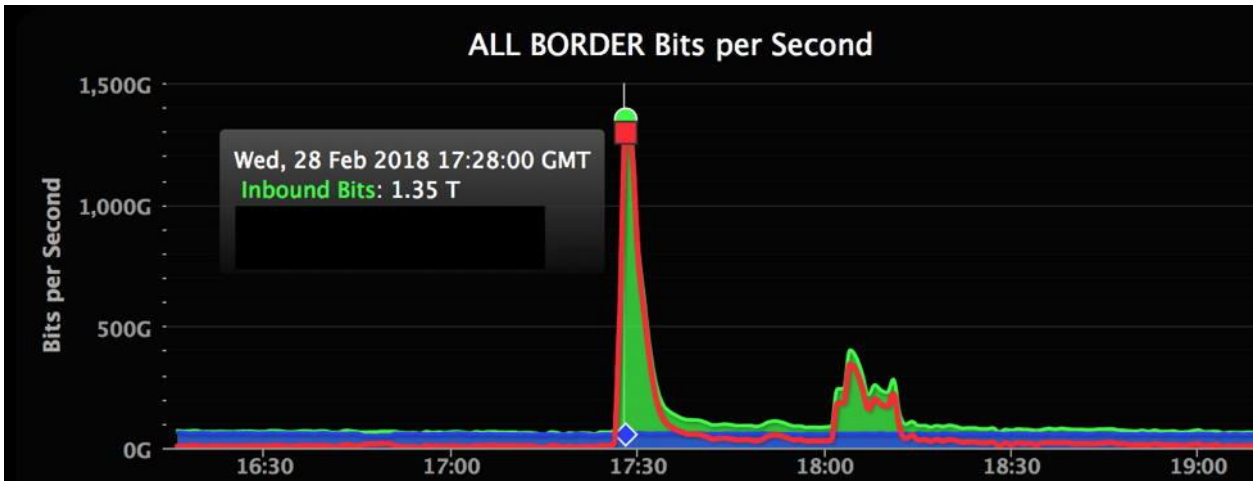
[Figure 8: A map of internet outages in Europe and North America caused by the Dyn cyberattack October 2, 2016 / Source: DownDetector (CC BY-SA)]

On October 21, 2016, a major domain name service (DNS) provider, was assaulted by a one terabit per second traffic flood that then became the new record for a DDoS attack. There's some evidence that the DDoS attack may have actually achieved a rate of 1.5 terabits per second.

The traffic tsunami knocked Dyn's services offline rendering a number of high-profile websites including GitHub, HBO, Twitter, Reddit, PayPal, Netflix, and Airbnb, inaccessible. Kyle York, Dyn's chief strategy officer, reported, "We observed 10s of millions of discrete IP addresses associated with the Mirai botnet that were part of the attack.

5. The GitHub Attack in 2018

On Feb. 28, 2018, GitHub, a platform for software developers, was hit with a DDoS attack that clocked in at 1.35 terabits per second and lasted for roughly 20 minutes. According to GitHub, the traffic was traced back to "over a thousand different autonomous systems (ASNs) across tens of thousands of unique endpoints."



[Figure 9:Chart of the February 2018 DDoS attack on GitHub. Source: Wired]

Figure 7 shows how much of a difference there was between normal traffic levels and those of the DDoS attack.

Even though GitHub was well prepared for a DDoS attack, their defenses were overwhelmed. They simply had no way of knowing that an attack of this scale would be launched. As GitHub explained in the company's incident report: "Over the past year, we have deployed additional transit to our facilities.

We've more than doubled our transit capacity during that time, which has allowed us to withstand certain volumetric attacks without impact to users … Even still, attacks like this sometimes require the help of partners with larger transit networks to provide blocking and filtering."

6. A European Gambling Company, 2021

In February, Akami announced that they had dealt with "three of the six biggest volumetric DDoS attacks" the company has ever recorded. The DDoS attacks were attempts at extortion. The hackers launch a DDoS attack the target can't help but notice and then demand payment not to do it again and at an even greater scale. In this case the threat attack weighed in at 800Gbps.

4.4.6 DoDos Detection:

Improving Accuracy Using Big Data:

The first generation of out-of-band DDoS detection solutions were based on single server software design, mostly running on standalone rack-mounted server appliances.

While far better than nothing, single servers simply don't have the compute, memory and storage resources to track high volumes of traffic data on a network-wide basis.

This is particularly true when attempting to perform dynamic baselining, which requires scanning massive amount of flow data to understand what is normal, then looking back days or weeks in order to assess whether current conditions constitute an anomaly.

Regardless of whether it is deployed on-premises or in the cloud, single server DDoS detection is insufficient to accurately detect today's attacks in a consistently reliable fashion.

By leveraging big data technologies for storing network events as they happen and by accessing this data repository in the cloud, customers can avoid DDoS detection appliances that fail to scale as their on-premise networks grow and/or re-deploy in the cloud, or avoid expensive in-house projects that require ongoing investments or obsolete as open software frameworks change.

4.5 Fake Vaccination

India, known to be the world's largest manufacturer and distributor of vaccines, started its free vaccine roll-outs against COVID-19 on 16 January 2021.[30]

National Expert Group on Vaccine Administration for COVID-19 was formed to overlook collaborations at national, state and district levels.

- COVISHIELD by the Serum Institute of India
- COVAXIN by Bharat Bio tech .
- Sputnik V was later granted EUA in April 2021.

i. In the rising fear of the third wave, there are people receiving fake vaccination in various parts of the country.
ii. INTERPOL had issued warning across its 194 member countries that this arena could be a prime target of criminal networks.
iii. In South Africa, 400 ampules, equivalent to 2400 doses, of fake COVID-19 vaccines were dismantled from warehouse.
iv. When reports of fake Vaccine nation surfaced in the Indian media, the country was shaken.In Mumbai , 2053 people were given fake jabs of the vaccines at nine centres as part of vaccination drives/camps.
v. An entire housing committee was scammed by fake vaccines and one hospital was even sealed for conducting a fake Vaccine nation drive.
vi. A special investigation team was set up by the Mumbai Police which arrested several people.
vii. A similar situation was witnessed in Kolkata, where 800 people were duped with fake jabs.

4.5.1 Vaccination App:

When the CoWIN application (app) was announced to be launched in India as the application that handles registration and creates vaccine schedules, there were already fake CoWIN apps promising people with vaccination.

4.5.2 Issues with App:

After the launch, problems such as discrepancies in the information provided and slot allotments, server issues with freezing and crashing of the app revealed how unprepared the system was to keep up with the increasing user demand.

The app also did not address the estimated 18 million households in India that have no working mobile phones or access to the internet. These loopholes provided an opportunity for fake Vaccinators to target the vulnerable population.

Some fake apps also led to malicious links trying to hack people's banking information. A report from McAfee, a software security company, stated that out of the 13,133,582 COVID-19-related malicious files detected worldwide, 883884 were detected in India alone.

4.5.3 Technique To Target Those Getting Vaccinated

As people post vaccine certificates online, cybercriminals are using sensitive personal information from it to hack into bank accounts and sell data to telemarketing companies.

Fraudsters ask people to register on fake websites dubbed as 'Pradhanmantri Berozgar Bhatta Yojna' through SMS, e-mail or other social media platforms on which victims are required to fill in sensitive details including their credit card information. The hackers then start clearing bank accounts based on the details provided by victims.

Another scam promises Rs 50,000 as a 'coronavirus subsidy' from the World Health Organization.Scamsters have also started targeting people who have received the vaccine by calling them from +91 2250041117. Those who answer the call are asked to press 1 if they have been vaccinated, and if he/she does so, the phone ends up getting hacked.

Officials have clarified that these are fraud calls, and that 1921 is the only official number used by the Government of India for vaccine feedback.

4.5.4 PREVENTION

All vaccines must be delivered from the Central Government vaccine stores.Private vaccine centres could be allowed to purchase vaccines from the government but would still need to ask permission from the state health ministry and the local police so that proper records can be maintained.QR code scan-based batch number registration (identification) in the government website should be made mandatory before opening a vial. QR code scanning can be incorporated into the CoWIN app as well.[30]

Vaccinator training programmes should be run by the government and valid certificates should be verified with the state government department website before enrolling individuals as vaccinators. Patients should get a confirmation message at once and should be advised not to leave the centre until the message is received.CBI coordinates with the INTERPOL and could implement strict law enforcement for perpetrators leading fake vaccination scams More structured and reliable system could streamline the process and prevent vulnerable populations from falling prey.

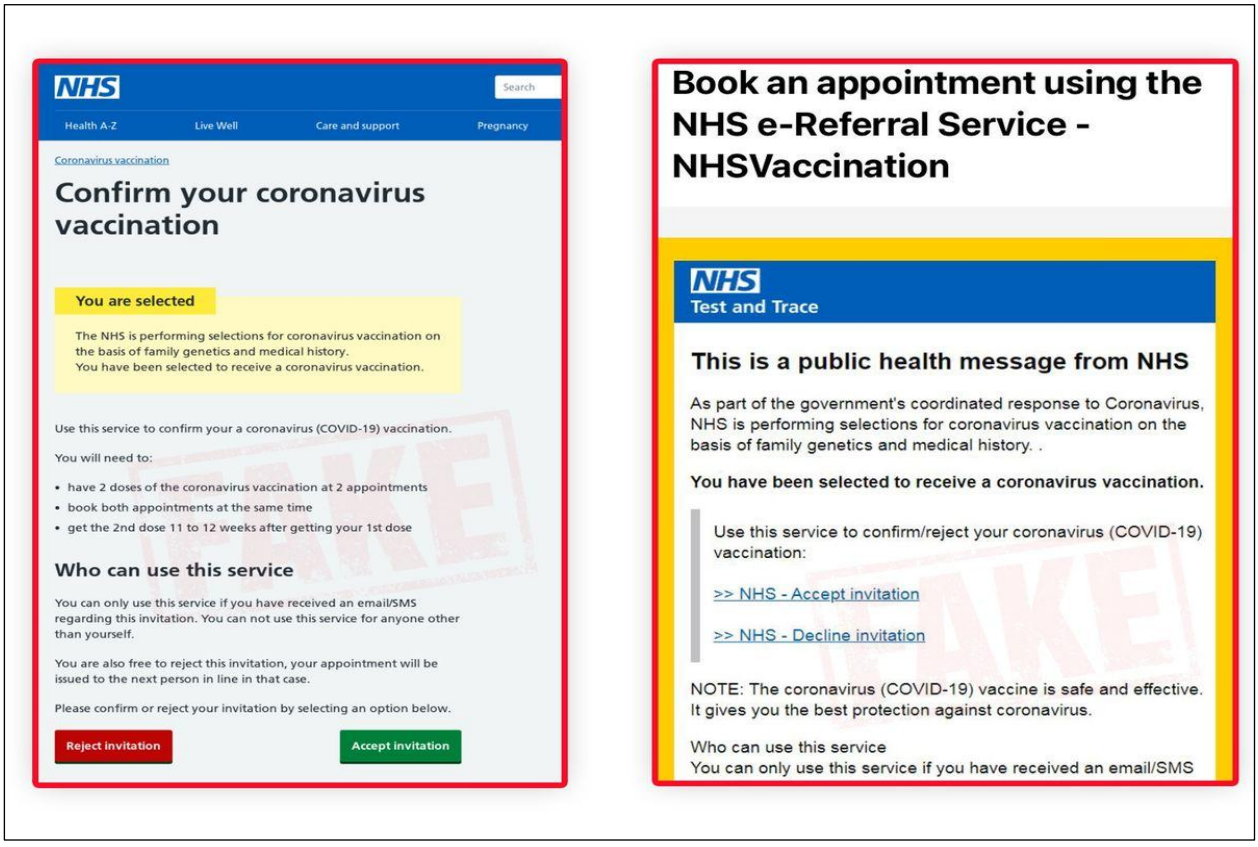
4.5.5 Why Shouldn't You Share COVID Vaccination Certificate Online?

In India, a COVID-19 vaccination certificate includes details such as beneficiary name, age, gender, vaccination date, last 4 digits of Aadhaar card, UHID and beneficiary reference ID—which if shared in public domain is more than enough for cyber criminals to carry out mischievous crimes.

Cyber expert and Internet researcher Sourajeet Majumder told **The Quint** that it can be used by fraudsters to defraud you or can be sold on the dark web for some quick money.

If cybercriminals get hold of your COVID-19 vaccination certificate, they can:

- ✓ Use the data to impersonate you
- ✓ Create fake certificates and sell them online
- ✓ Give your data to telemarketing and health insurance companies to advertise their products
- ✓ Carry out targeted phishing attacks and blackmail you with the information they have
- ✓ Sell your vaccination certificate on the dark web, breaching privacy



[Figure 10: Fake Vaccination]

4.6 FAKE NEWS WEBSITES

At the beginning of the pandemic, South Korea started using the "Corona 100m (Co100)" application, which would signal to mobile phone owners whether there are any people infected with corona virus within 100 meters, giving everyone information not only about the location of infected person, but also reveal the information about the date of infection of that person, their nationality, sex, age and locations that person visited.[30]

The unit for cybercrime security of the Hungarian police has arrested several people for spreading false news since the beginning of February 2020.

When the raid was at first been carried out, The sites that wrote about the coronavirus were closed by the police in Hungary before the official confirmation, after that, they started to monitor the Hungarian online media due to false news related to the coronavirus.

After these, a package of pandemic-related laws passed by the Hungarian Parliament on March 30 gave the government power "to rule by decree indefinitely, bypassing normal parliamentary procedures: the act allows prison terms of one to five years for those who "spread falsehoods or distorted facts" that could alarm the public. These measures were temporary".

On March 19, 2020, the Government of the Republika Srpska decided to ban panic and riots (including presenting and transmitting false news in the media and on social networks) during an emergency situation.This decision was repealed on April 14, 2020

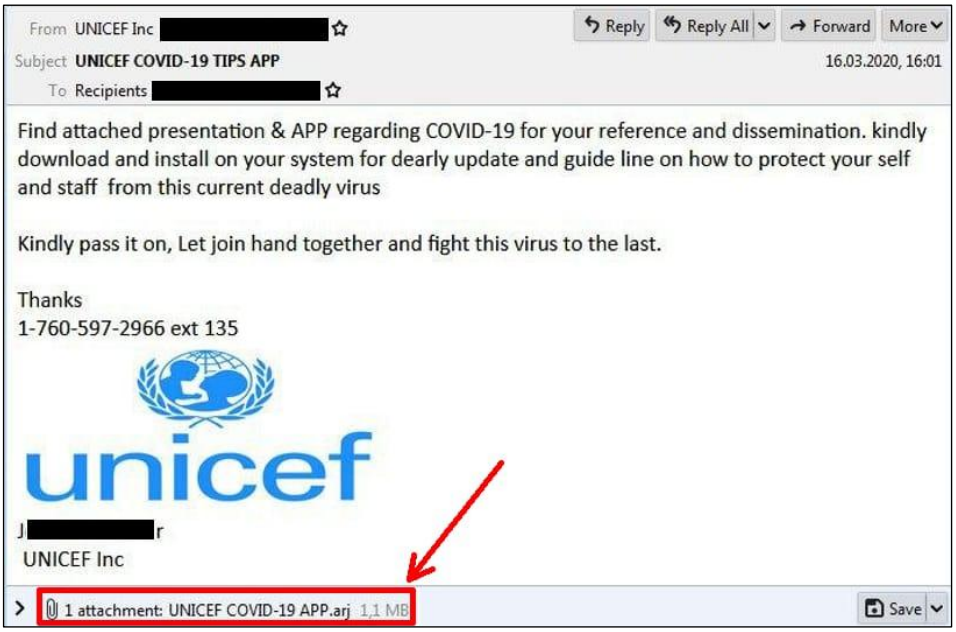
Examples of Fake Links

1. Click here for a cure :

From February 2020, internet users began to receive various emails with the text to receive coronavirus vaccines with one click.

The message was sent by a mysterious medical expert, claiming to have exclusive news of vaccine, which is provided by the Chinese and British governments. [30]

Clicking on the link would be redirected to a website that looks convincing and credible, but it is actually designed to steal the user's personal information and to retrieve all users' login details.



[Figure 11: Refund Fraud E-MAIL]

This way user becomes a victim of identity theft, giving hackers access to all documents and other sites to which the user previously logged in using the same email and password.

The best way to see where the link will actually take you is to hold the mouse cursor over the given link and a real caption of its URL will appear. If it's suspicious, just don't click on it.

2.WHO: Covid-19 tax refund

Agent Tesla Key logger:

Many hacker campaigns present themselves as the World Health Organization, offering users tips on corona virus protection.

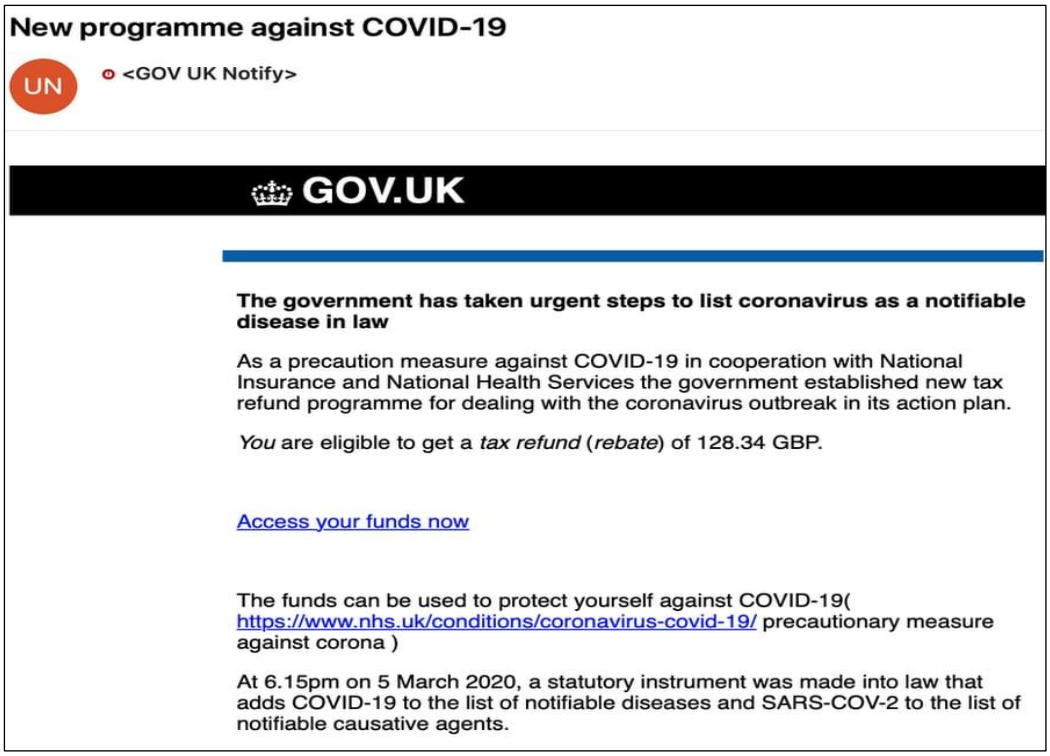
According to analysts, user doesn't receive any useful advice, but their computer becomes infected with malicious software called Agent Tesla Key logger.

Once installed, this malware records everything that is typed on a computer and sends it to attackers, which is a tactic that can provide access to online banking and financial accountTo avoid this, avoid emails like this one from the WHO, cause they are probably fake, instead visit the official website or WHO channels on social networks to get the latest advice.

3.We refunded your tax to help protect you from covid-19" / Little measure that saves

In the UK, as hackers devised an email sent on behalf of the UK tax authorities with a promise that citizens who go to the site given in a sent message, entering personal data and their bank account details, will be able to recover taxes due to covid-19.This variations of the classic "phishing" campaign regarding tax refunds used by cybercriminals.

To avoid this don’t respond to any request sent via e-mail concerning financial transactions, and especially not to enter data on users' bank accounts.



[Figure 12: Fake Refund Policy Example]

4. CDC: Donate here to help the fight

Another fake email collecting donations to work on the development of a coronavirus vaccine, exclusively in bitcoins. Like the WHO, the Centres for Disease Control and Prevention (CDC) has been used to misrepresent numerous different "phishing" campaigns.

The e-mail address looks very convincing, just like the design of the e-mail. This example was reported to malware experts Kaspersky. Kaspersky says it has detected more 513 different files with corona virus in their title, which contain malware.

Attackers in web-phishing use URL-personalization through of include words related with covid or corona virus, such as the following URLs:

covid19mobile.app
covid19-stats.co.za
coronavirusnotalone.com
sars-cov2numbers.com
limpiezascovid.com
coronademic.net
coronavirusalerts.com
coronavirus.technology
coronavirusmedicine.com
covidrule.com

[Table 1: Web-Phising URLs]

The domain-tools portal has a record of 162,364 malicious URLs with word related to the covid-19 pandemic since January to May of year 2020, while security enterprise firm Palo Alto says the increase of malicious URL are 1,300 domains every day.

4.7 CRIMES RELATED TO ROBBERY

As per International Labour Organization (ILO), the global pandemic covid-19 can cause different threats on the population like hunger, unemployment and financial cries. These crises may cause increase in crimes like robbery.

Elaborated the threat of crimes like robbery and discussed some technological preventive measures like Drones, Intelligent CCTV Cameras, Central Command & Control Center and Artificial Intelligent Sensors which can be adopted to stop the robberies during the pandemic as Police will be mostly dealing to ensure check and balance of SOPs developed for stopping spread of corona virus.

When the unemployment rises, the risk of crimes including cybercrimes also rises.

4.7.1 ROBBERY THREATS DURING COVID-19:

In the current situation, face mask is currently mandatory for every individual but it is also an opportunity for robbers to commit robbery without being recognized.

The ideal condition for the robbers to wear face mask, hoodie, hand gloves and everyone will inspire from them as they have followed SOPs and it would be difficult for police to get hands on them without their finger prints and face.

Another factor that cannot be ignored that currently in the world, police and other agencies are called to ensure check and balance on the citizens to not violate the SOPs (Statement of Purpose) developed for lockdown which is an opportunity for criminals to attack on the industries/factories which are left empty as no activities are currently going.

Sr.	Factors	Difficulties
1	Face Mask	Criminals cannot be recognized as everybody wears surgical mask these days.
2	Gloves	Fingerprints of criminals cannot be matched due to usage of gloves.
3	Police	Police is currently busy with general public to urge them follow SOPs

[Table 2:Common Factor]

4.7.2 STATS OF ROBBERY RELATED CRIMES' DURING COVID-19

Robberies are increased by 50% during lockdown, In March, 2020 two men wearing surgical masks robbed three workers in New York and took away $250,000 money which they were transferring from gaming machines to lockers.

Some other robberies involved in which suspects wore surgical masks happened in Washington D.C and North Carolina during the lockdown.

4.7.3 PREVENTION

1. DRONES

Drones can be used to monitor the streets and ensure surveillance during the lockdown.They can be handled manually or through automated system. Drones which have real time video communication and independent capabilities and are equipped with cameras can help police/authorities to control crimes proactively.

2. ARTIFICIAL INTELLIGENT SENSORS

Artificial intelligent sensors which can be placed at random location can help in reduction of crime during the lock down period. When the sensor detects bullets firing or yelling, they start beeping police alarm which can cause criminals to run away for their lives.

3. DIGITAL IMAGE PROCESSING IN CCTV CAMERAS

Digital Image Processing in CCTV cameras with speaking power can also be used to cope with the crimes. Camera detects the face of criminal and start speak his name will cause criminal to run away from crime scene, otherwise it can just start beeping police alarm or some recorded police voice.

4. CENTRAL COMMAND AND CONTROL CENTERS

Central command and control center that have monitor screens and artificial intelligence power can be handy in this critical period. If cameras detect any criminal activity, it starts beeping the alarm in command and control center. By the help of this, crimes like robbery can be prevented during the lockdown period when the countries have a lot of other matters to deal with.

4.8 Cyber Bullying On Children and Youth

The study aimed at exploring the risk s of victi mization of chil dren and youth thro ugh cyberb bullying during the lockdown.A qualitative approach, non-participant observation was utilised. Data was collect ed from three social media platforms which include Facebook,Twitter,and Instagram from posts since the beginning of lockdown. Keywords such as "ama2000s", "2000s" and "90s vs 2000s" wre used to search for content. Facebook groups for "2000s" where most young people engage were also used.

The study found that with the increase of the use of social media among children and youth during the lockdown, most have been victims of cyberbullying. In these platforms where young people engage, most posts and comments carried content which includes sexting, sexual comments on young girls' pictures, trending of videos of school children fighting, and insulting each other. A significant finding was the use of fake accounts to perpetrate cyberbullying. [9]

Several learning institutions responded by moving some of the courses to their online platforms to try and avoid the disruption of the 2020 academic calendar. 'Cyber bullying' may occur through the use of tools such as mobile phones, chat, rooms, emails, instant messaging, and social networking sites by someone or a group of people to harm children and youth.In the search for data on Instagram, the researcher searched for words such as ama the 2000s, funny memes, Mzansi jokes. The results depicted that the use of the internet is still high and has gone higher during the Covid-19 pandemic.This, therefore, placed the question on the risk of the youth and children being victimized through cyberbullying as they use the internet.

The findings show that cyberbullying increased on Instagram during the lockdown period. Under the hashtag 'ama2000'there were more post which included sexual content and insulting comments. The hashtag has 1000+ posts; however, more of these posts were during the lockdown period. In an attempt to explore the risks of victimisation of children and youth through cyberbullying during Covid19 lockdown the study used thematic analysis and six themes were identified. The themes include increased cyberbullying during Covid-19 lockdown, humiliation.

Mkhize and Gopal online violence, post sharing sexual content, harassment, reaction to cyberbullying. The themes were developed based on the research questions and they are discussed below.[40]

4.8.1 Major Factor

1. Humiliation, Harassment

The study found that there were various videos of young teenagers being involved in fights. The videos show teenagers including school learners with school uniforms fighting.

These videos had been shared on different social media platforms which include Facebook Groups and Twitter with more than 2000 views, comments, and shares. Some of these videos were turned into memes to make fun of the teenagers involved in the fights on the video.

2. Online Violence

Online violence was observed to be one of the most common experiences that occur on social media. This involved the use of vulgar language as well as threats, it is another form of cyberbullying that occurs mostly on social media and the internet at large.

Based on the findings, online violence included racism, condoning violence as well as gender-based violence.

3. The use of Fake Accounts

It was found that on all three social media platforms, that is, Facebook, Twitter, and Instagram there were individuals who used fake accounts to pretend to be someone else. This includes using the names and pictures of someone else.

Some people use fake accounts to post or comment on other people’s posts using insults or harassing others.

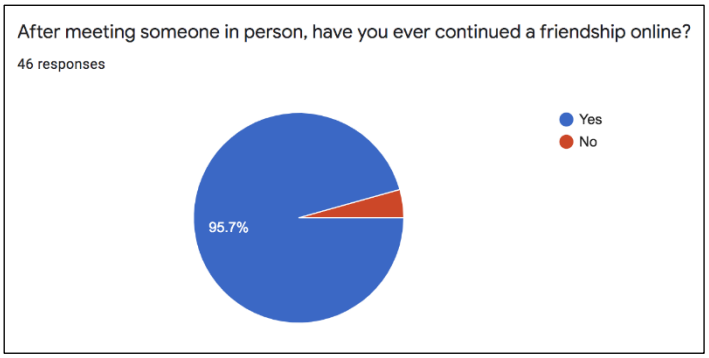
4. Posts Sharing Sexual Content

Sexing was the major finding of this study. Popover and Fine(2016) assert that adolescents were more likely to have seen sexual or violent content online.

On Facebook groups and Instagram posts of half-naked girls were shared. On those posts, comments were responding using sexual messages

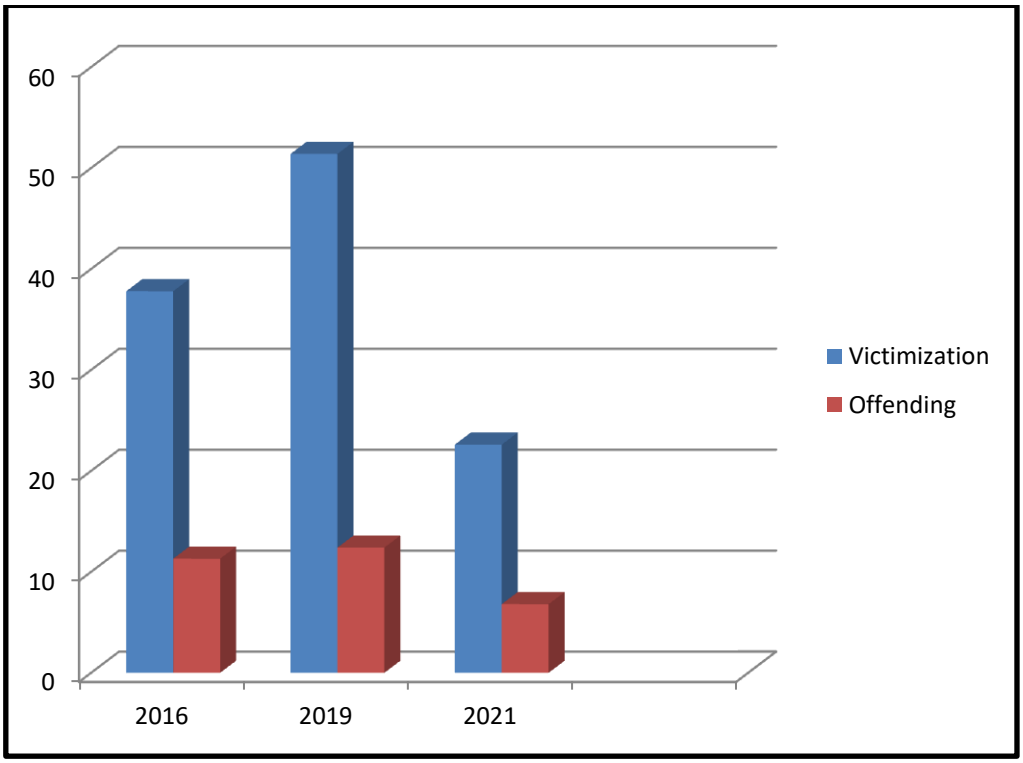
5.Fake online friendship

Developing online friendship over social media (with no real-life familiarity and using the emotional connect to trick you in transferring funds on some pretext such as medical emergency, legal troubles, problems in a foreign country etc.



[Figure 13: Nationally Representative Samples Of U.S 13 To 17 Year Old]

If we focus just on our last three studies, all of which are relatively large (2,500-4,700 participants) nationally-representative samples collected in 2016, 2019, and 2021 using the same methodology and identical instrument, we can evaluate some recent trends in bullying and cyberbullying behaviors over that time period.



[Figure 14: Chart Of Cyber Bullying Impact]

For example, in the spring of 2021, 22.6% of students said they had been bullied at school in the previous 30 days, compared to 51.4% in 2019 and 37.8% in 2016. A similarly steep drop was observed in self-reported school Bullying offending behaviours in 2021. In 2016 and 2019, about 11-12% admitted that they had bullied others at school compared to 6.8% in 2021.In short, school bullying behaviors have undoubtedly dropped during the pandemic.[40]

4.8.2 IMPACT OF CYBER BULLYING

- What makes cyber bullying different from traditional bullying is that the impact of cyber bullying is worse due to the perpetrator being hidden. According to the SAPS (N.d)
- The effects can be devastating on victims of cyber bullying and can include feeling hurt, humiliated, angry, depressed, or even suicidal.
- Research shows that bullied teens are more likely to commit suicide.
- The data was collected from social media posts from the year 2020, to find the most active groups on Face book.
- The most active groups on Facebook included groups such as Ama 2000s which are the groups for young people. On Twitter, the researcher randomly searched for posts under the hash tags used on Twitter during the lockdown.
- The researcher also used the words such as “cyber bullying”, “bullied”, and “cyber bullied” to search for the topics on Twitter that touch on the issue of cyber bullying in South Africa.
- Children and youth face high risks from online predators as they spend more time on the internet during the Covid-19.
- The lockdown put children’s privacy in danger as they spend more time online. They are likely to encounter online risks, including being exposed to child sexual abuse material, or child sexual abuse and exploitation.
- And while sharing images and stories of lockdown and its challenges through social media is a way to stay connected, children’s rights to privacy and protection should not be compromised," (UNICEF, 2020). Some of the tweets shared also expressed concerns about the increase in cyber bullying.

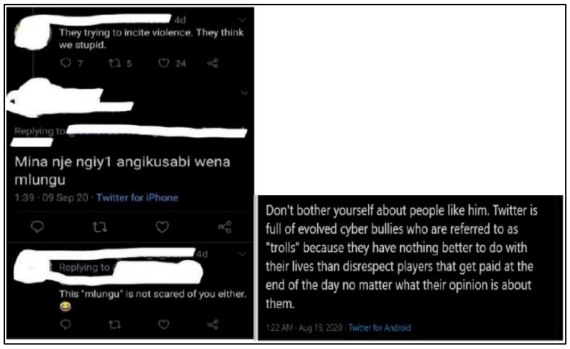
4.9 Social Media

Nowadays, social media is very common thus hackers find it a great opportunity and tend towards the various social media platforms such as Face book and WhatsApp.The scams typically lure victims into free subscriptions such as Netflix premium free account. When the victim clicks on the link, it redirects them to their social media phishing website.[9]

In some cases, it may ask to enter the credentials of their accounts. This way, they either capture their credentials or install malware into their systems, mobile devices, and web browsers to steal information and cookies, and thus, the user becomes a victim.

[Figure 15: Face book Viral Video]

- Picture from a video that trended on Facebook groups used as a meme.
- **(Posted on 14 September 2020)** This picture was used on one of the Facebook groups to make fun of the girls that were fighting and the meme was shared on different groups with 100+ shares on each group and 800+ comments and 500+ reactions. The comments included people sharing their WhatsApp numbers to have the video shared with them.
- In this case, the videos and pictures circulated on social media were of young girls who were video recorded fighting.



[Figure 13: Tweeter]

- Tweets of arguments from Twitter
- **(Tweeted on 09 September 2020 and 19 August 2020).**
- Shows The Online Violence , who explain that it is when someone is purposely using extreme and offensive language and getting into online arguments and fights with someone

[Figure 14: Fake Accounts]

- People identifying and mentioning fake accounts
- **(Posted on 24 July and 22 August 2020; tweeted 23 May 2020)**

4.9.1 Detection

Checking-in at a restaurant, announcing flight details or uploading pictures on social media with a famous place in background are routine activities of social media users, but these activities put people at risk. Alex Merton-McCann from McAfee explains that cyber-casing is a process of using geo-tagged data by criminals. [44]

Eucating users about the risk of sharing location and providing them authority to make informed decisions will help reducing misuse of location data.Credit card fraud has been on rise in past several years, and due to heavy losses, the researcher community is constantly searching for new ways of detection and prevention Credit card transaction screening techniques, such as address verification services (AVS), card verification methods (CVM), personal identification numbers (PIN) and biometrics, are some basic checks, but an effective and economical fraud detection system is the need of the day.

The researcher stresses that the tremendous use of neural network in banking and finance sector shows its success in the field. The need of securing user's information is all time high and needs a proper solution, otherwise breaches will occur constantly.

Cybercrime	Prevention tips	Preventing techniques
Burglary via Social Networking	Do not share location Do not share home address Do not share personal information with friends of friends Limit your connection to only those whom you know Check your privacy setting and control how others can tag you Limit your app permissions	Techniques: Time series approach, random forest based model , multi-layer perceptron, self-organising map, rule induction, genetic algorithms and case based reasoning
Credit Card Fraud	Continuous surveillance of vaults Regular and severe material accounting Employee log that touches critical material to sign for it Apply two-person rule to access critical property Encourage employee attention to security Seek security buy-in	Monitoring anomalies Techniques: address verification service (AVS), card verification value (CVV), decision tree, neural network, k-means clustering, hidden Markov model, and genetic algorithm
Cyber Intrusion and Data Breaches	Design and conduct end-user awareness campaign Create and enforce the computer security policy Keep data only as long as you need it Prepare an incident response plan Deploy intrusion detection and preventions system Make routine vulnerability assessment.	Verification and validation Personal identification number (PIN) Techniques: Petri net-based encryption, address verification service (AVS), card verification method (CVM), common vulnerability and exposure database (CVE).

[Table 3]

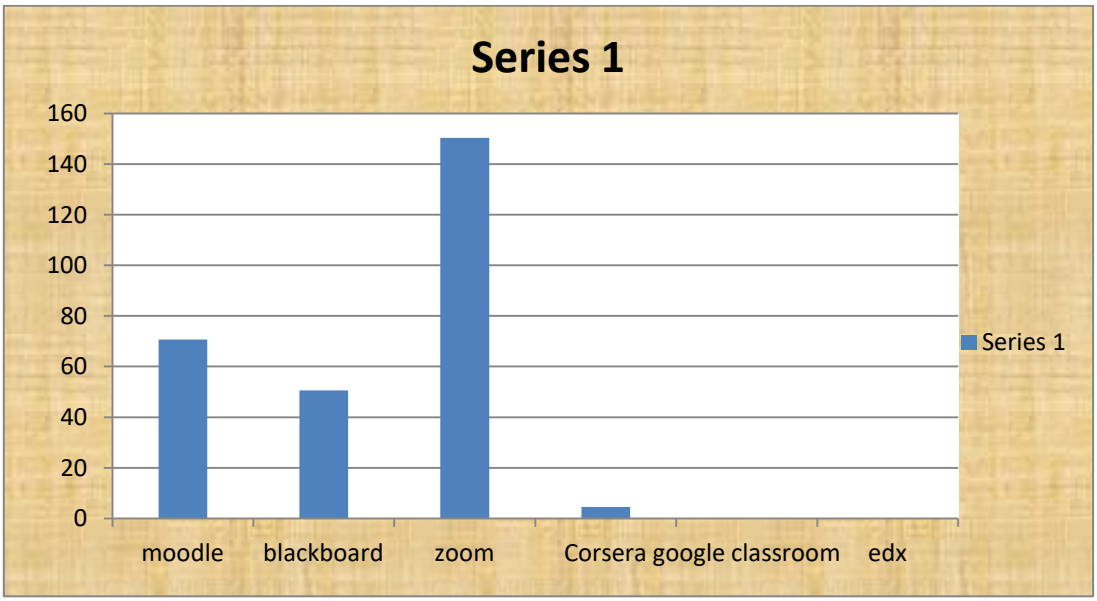
4.10 Online education

1. Zoom meeting

Many sectors, such as industries, education, have shifted online. Cybercriminals have evolved their criminality to exploit the social, legal and psychological nuances associated with COVID19. School-age children, both the new and more frequent users of the Internet, are being proactively targeted by online sex offenders.

To sign up for the applications, the consumers have to agree to some terms and conditions, which include their privacy and security data collection. A recent consumer report analysed the privacy policies of these applications such as Google Meet, Microsoft Team, and Zoom and concluded that they are collecting more data than people realize , which is alarming. [44]

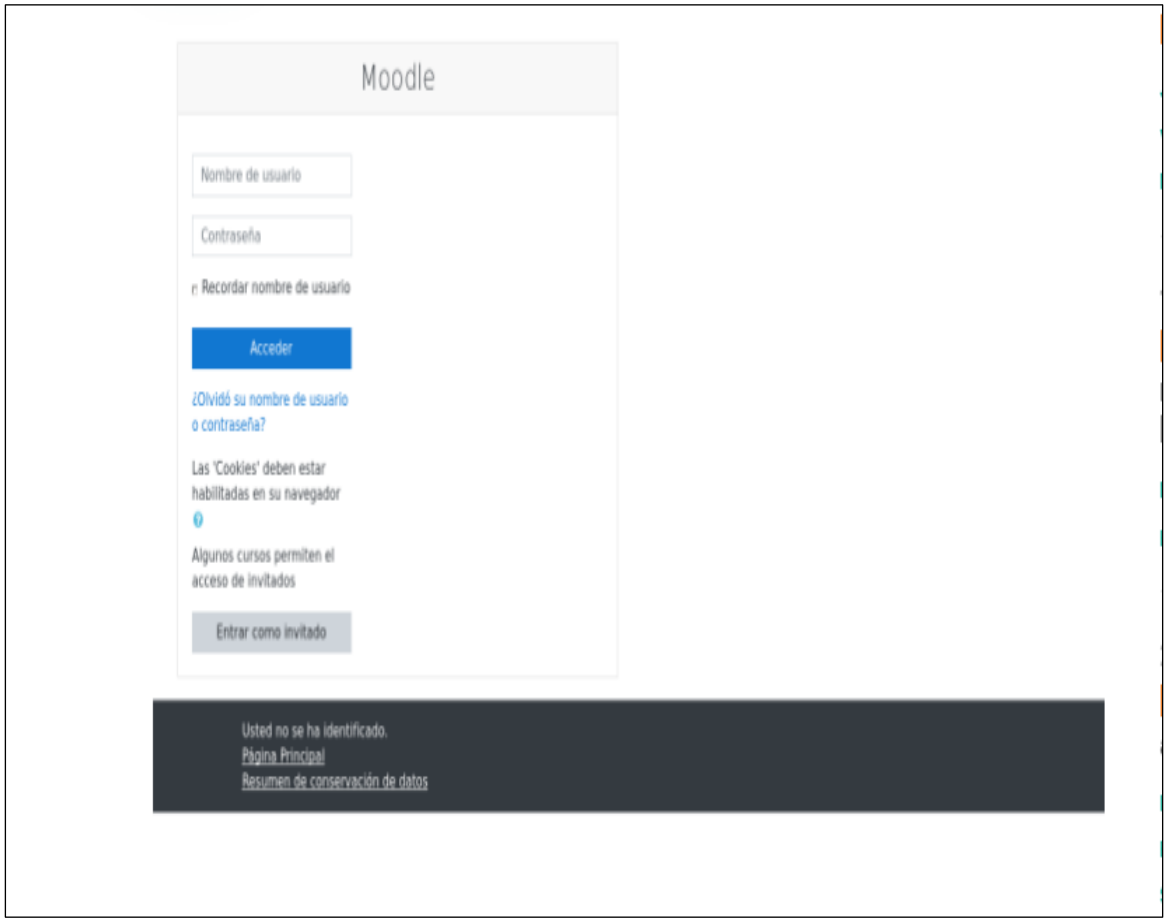
This includes offenders seeking to groom1 and sextort2 individual children, through to broader infiltration in online classes 3 now referred to as “Zoom-bombing”. As large numbers of people turn to video-teleconferencing (VTC) platforms to stay connected in the wake of the COVID-19 crisis, reports of VTC hijacking (Zoom-bombing) are emerging nationwide..



[Figure 15 Online Education]

From January to June 2021, the number of unique users that encountered various threats distributed via the platforms specified in the methodology section of this report was 820.The most popular lure was Moodle, with Blackboard and Zoom being the second most popular.

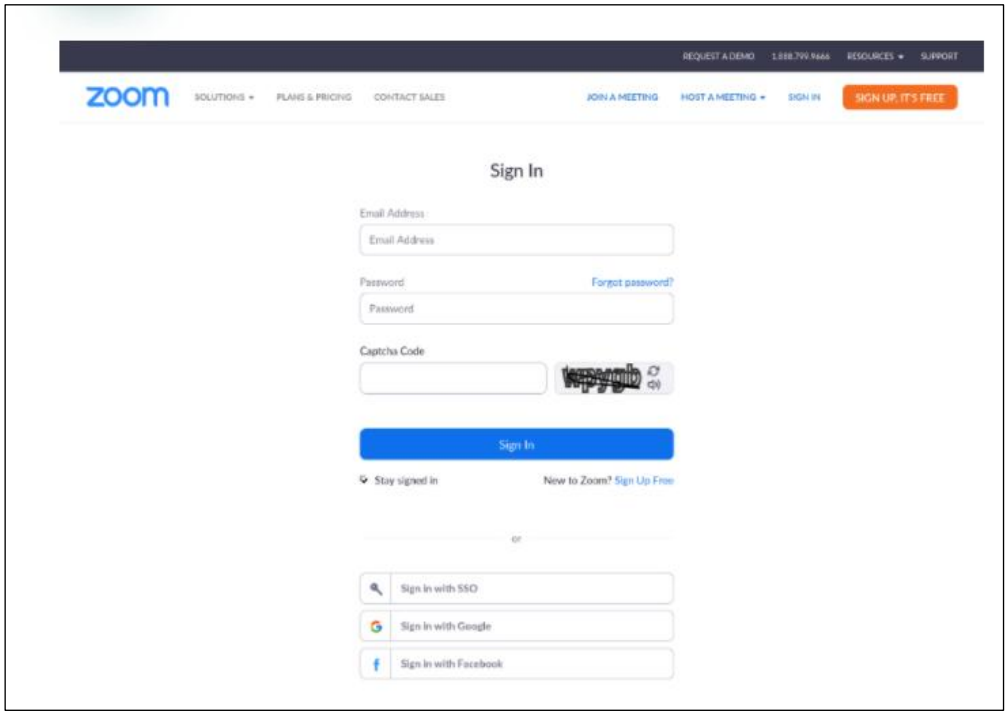
Most universities also have their own platforms where students and faculty can login to access important resources and various academic services.This past spring, some attackers went so far as to target specific universities by creating phishing pages for their individual academic login pages.



[Figure 16: Fake login page for Moodle]

The most widely used online conferencing tool Zoom now faces a massive backlash in terms of privacy and safety, as security experts, privacy advocates, lawmakers, and the FBI are warning that Zoom's default settings are not adequately secure. In addition to this, recently, many countries have started monitoring the locations and other details of their citizens and visitors cell phones to locate specific cities and districts where a significant number of the people infected are residing.

Zoom-bombing has the potential of compromise systems and generate lack of privacy. Zoom-bombing not only affected educational institutions, US government entities mentioned that they were victims of attacks during meetings. Attackers have taken advantage of the increased in the use of video conferencing tools for teleworking or tele-education, to send malicious emails using references of video conferencing tools.



[Figure 17: Fake login page for Zoom]

In other hand, a high school in Boston- Massachusetts report intrusions on on-line class using the teleconferencing software Zoom,which includes Maine, Massachusetts, New Hampshire, and Rhode Island, two schools in Massachusetts reported the following incidents:

In late March 2020, a Massachusetts-based high school reported that while a teacher was conducting an online class using the teleconferencing software Zoom, an unidentified individual(s) dialed into the classroom. This individual yelled a profanity and then shouted the teacher's home address in the middle of instruction.

A second Massachusetts-based school reported a Zoom meeting being accessed by an unidentified individual. In this incident, the individual was visible on the video camera and displayed swastika tattoos. As individuals continue the transition to online lessons and meetings, the FBI recommends exercising due diligence and caution in your cybersecurity efforts. [44]

The following steps can be taken to mitigate teleconference hijacking threats:

- Do not make meetings or classrooms public. In Zoom, there are two options to make a meeting private: require a meeting password or use the waiting room feature and control the admittance of guests.
- Do not share a link to a teleconference or classroom on an unrestricted publicly available social media post. Provide the link directly to specific people.
- Manage screensharing options**.** In Zoom, change screensharing to "Host only."
- Ensure users are using the updated version of remote access/meeting applications. In January 2020, Zoom updated their software.
- In their security update, the teleconference software provider added passwords by default for meetings and disabled the ability to randomly scan for meetings to join.
- Lastly, ensure that your organization's telework policy or guide addresses requirements for physical and information security.
- However, as long as online learning continues to grow in popularity, cybercriminals will attempt to exploit this fact for their own gain.
- That means educational organizations will continue to face a growing number of cyber risks – into this fall and beyond. Fortunately, engaging – and secure – online academic experiences are possible.
- Educational institutions just need to review their cyber security programs and adopt appropriate measures to better secure their online learning environments and resources.

4.11 Malicious Domains, Malicious Websites

Ever since the beginning of the outbreak of the COVID-19 pandemic, attackers acted quickly to exploit the confusion, uncertainty and anxiety caused by the pandemic and launched various attacks through COVID-19 themed malicious domains.

Malicious domains are rarely deployed independently, but rather almost always belong to much bigger and coordinated attack campaigns. Thus, analyzing COVID-themed malicious domains from the angle of attack campaigns would help us gain a deeper understanding of the scale, scope and sophistication of the threats imposed by such malicious domains.

We collected data from multiple sources, and identify and characterize COVID-themed malicious domain campaigns, including the evolution of such campaigns, their underlying infrastructures and the different strategies taken by attackers behind these campaigns.Our exploration suggests that some malicious domains have strong correlations, which can guide us to identify new malicious domains and raise alarms at the early stage of their deployment.

The results shed light on the emergency for detecting and mitigating public event related cyber attacks. [9]

4.11.1 Technique

Custom malicious domains refer to the domains registered by attackers which are not well known and remain active for a short period of time to avoid detection. This design is mostly used for broadly distributed infections rather than targeted ones.There has been an increase in websites that claim to be applications that are supposed to protect users from COVID-19, such as They mentions that their application, called "Corona antivirus," has been developed by scientists at Harvard University. But in reality, installing this application infect the system with a malware called BlackNET RAT. Which enables the system to work as an boatnet , can help to launch a DDoS attack, upload some remote files, execute malicious scripts, collect browser cookies and passwords and harvest keystrokes. www.coronavirusmedicalkit.com This fraudulent website is issued by the United States Department of Justice. It is alleged that the web site provides WHOapproved vaccine kits for COVID-19. In Reality , valid COVID-19 vaccines approved by the WHO are not yet available in the market. The fake website asks for US$ 4.95.

4.11.2 Crimes

List of Blackbaud breach victims tops 120

The UK's National Trust has joined a growing list of education and charity organisations to have had the data of their alumni or donors put at risk in a two-month-old ransomware incident that occurred at US cloud software supplier Blackbaud.According to the BBC, the Trust, which operates hundreds of important and historical sites across the country, including natural landscapes and landmarks, parks, gardens and stately homes, said that data on its volunteers and fundraisers had been put at risk, but data on its 5.6 million members was secure.

The organisation is conducting an investigation and informing those who may be affected. As per the UK's data protection rules, it has also reported the incident to the Information Commissioner's Office, which is now dealing with a high volume of reports, including Black bauds.[51]

1. IT services company Cognizant warns customers after Maze ransom ware attack

Cognizant has warned that a cyber attack by the Maze ransomware group has hit services to some customers.The IT services company, which has a turnover of over $16bn and operations in 37 countries, said the attack, which took place on Friday 17 April, had caused disruption for some of its clients. Cognizant, which supplies IT services to companies in the manufacturing, financial services, technology and healthcare industries, confirmed the attack in a statement on Saturday 18 April.

2 .Phishing scam targets Lloyds Bank customers

Customers of Lloyds Bank are being targeted by a phishing scam that is currently hitting email and text message inboxes.Legal firm Griffin Law has alerted people to the scam after being made aware of about 100 people who have received the messages.The email, which looks like official Lloyds Bank correspondence, warns customers that their bank account has been compromised.

It reads: "Your Account Banking has been disabled, due to recent activities on your account, we placed a temporary suspension untill [sic] you verify your account."

3. Coronavirus now possibly largest-ever cyber security threat

The total volume of phishing emails and other security threats relating to the Covid-19 coronavirus now represents the largest coalescing of cyber attack types around a single theme that has been seen in a long time, and possibly ever, according to Sherrod DeGrippo, senior director of threat research and detection at Proofpoint.

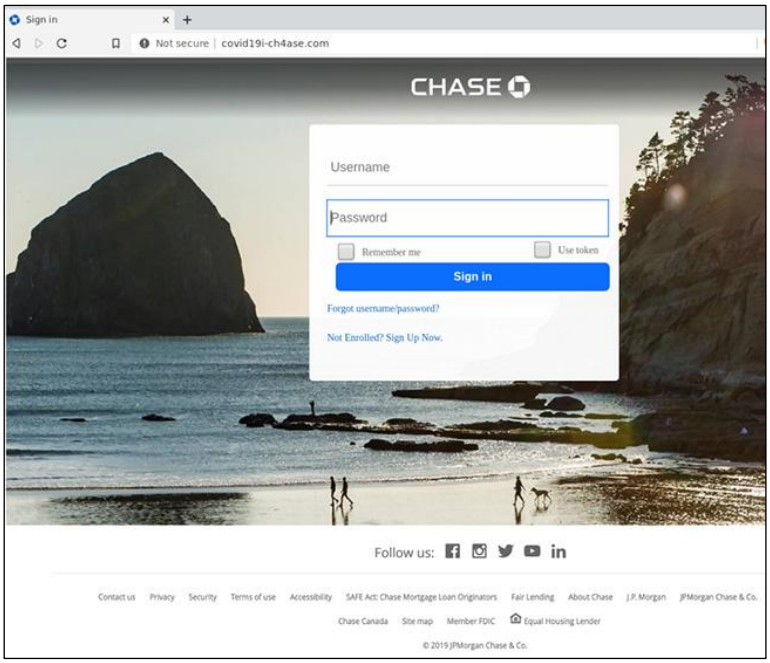
To date, Proofpoint has observed attacks ranging from credential phishing, malicious attachments and links, business email compromise, fake landing pages, downloaders, spam, and malware and ransomware strains, all being tied to the rapidly spreading coronavirus.“For more than five weeks, our threat research team has observed numerous Covid-19 malicious email campaigns, with many using fear to try to convince potential victims to click,” said DeGrippo.[51][9]

4. Cyber gangsters hit UK medical firm poised for work on coronavirus with Maze ransom ware attack

Cyber gangsters have attacked the computer systems of a medical research company on standby to carry out trials of a possible future vaccine for the Covid-19 coronavirus.

The Maze ransom ware group attacked the computer systems of Hammersmith Medicines Research, publishing personal details of thousands of former patients after the company declined to pay a ransom.

The company, which carried out tests to develop the Ebola vaccine and drugs to treat Alzheimer’s disease, performs early clinical trials of drugs and vaccines.



[Figure 18]

In Figure, the threat actor was sending phishing messages 'from' Chase with some form of messaging about the bank's COVID-19 response, making it seem plausible to users that their bank may have set up a dedicated page related to the virus.

4.11.3 DETECTION

A typical technique to measure the level of similarity of two time series is to calculate the distance between them. To determine whether a domain produces similar time series every day, we calculate the Euclidean Distance between every pair of time series of a domain.

Euclidean Distance is a popular distance measuring algorithm that is often used in data mining. We first need to break the local time series produced for each domain into daily time series pieces.

Each day starts at 00:00 am and finishes at 23:59 pm. Assuming that a domain has been queried n days during our analysis period, and di, j is the Euclidean Distance between ith day and jth day, the final distance D is calculated as the average of (n − 1) ∗ (n−2)/2 different distance pairs, as shown in the following formula:

$$D = (Xn\ i=1\ Xn\ j=i+1\ di,j\ )/((n - 1) * (n - 2)/2)$$

4.1 SPEARD OF MISINFORMATION

Misinformation has started to spread in various media, including traditional media, websites, social media which had the most significant impact on spreading misinformation and fake news more quickly. The increasing spread of misinformation and disinformation will continue to confuse the public and undermine the scientific response.

Cybercriminals are taking advantage of COVID-19 and the new reality it has imposed: telecommuting hitting peak levels and huge amounts of information — and misinformation circulating the Internet. Scammers are ramping up their activities as they try to maximize ill-gotten gains.

As the world responds to the COVID-19 pandemic, we face the challenge of an overabundance of information related to the virus. Some of this information may be false and potentially harmful .Inaccurate information spreads widely and at speed, making it more difficult for the public to identify verified facts and advice from trusted sources, such as their local health authority or WHO.However, everyone can help to stop the spread. If you see content online that you believe to be false or misleading, you can report it to the hosting social media platform.

4.12.1 Misinformation about COVID-19

1. 5G Narrative

Although viruses cannot be spread through wireless technology, theories associating 5G wireless technologies with COVID-19 have proliferated and led to more than 70 cell towers being burned in Europe (predominantly the United Kingdom) and Canada.

2. Gates Vaccine Narrative

Between February and April 2020, varied conspiracies linking Bill Gates to COVID-19 (e.g., as a pretext to embed microchips in large portions of the global population through vaccination) were the most ubiquitous of all conspiracy theories. Among other direct consequences, a non-government organization that became linked with this theory ended up calling the US Federal Bureau of Investigation for help after being targeted online.

3. Laboratory Development Narrative

Research indicates that COVID-19 is a zoonotic virus (see papers published in February by Chinese scientists and in March by a group of scientists from the US, United Kingdom, and Australia). However, officials in both the US and China have accused the other country of purposefully developing COVID-19 in a laboratory, often with the implication of military involvement.

4.12.2 CRIMES

The WHO has offered a WhatsApp service to refute fake news, but unfortunately the rapid, viral spread of disinformation on social networks has been so widespread that we have in fact witnessed the appearance of attitudes harmful to health.In some cases, patients refused to take ibuprofen or other anti-inflammatory drugs because of the erroneous idea that they could increase the chances of getting infected with the coronavirus. Misleading information about treatment for COVID-19 has resulted in an increasing number of vitamin D abuse and even mass poisoning from methanol intake. [55]

After the lockdown, in countries where social distancing and the use of face masks were mandated, news of correlation between cancer and mask coverings appeared on social networks.The lockdown and consequent social distancing has resulted, especially in those residing in highly infected areas, in a posttraumatic stress syndrome (PTSD) characterized by anxiety, sleep disturbances, distress. Misinformation and fake news contributed to the onset of PTSD and headline stress disorder cases .

The consequences of these disorders have not only had effect in the peak infection phase but will also have future repercussions. The historical importance of the COVID-19 pandemic is such that, also in the future, COVID-19-related news will be published cyclically in the mass media and on social networks. Poor quality information may in the future amplify anxiety to the state of panic especially in the event of a new wave of infections; people will relive the moments of the first phase of the peak of COVID-19 and will return to look for information to safeguard their health and that of their loved ones.

The rapid evolution of the COVID-19 pandemic has not permitted immediate and certain scientific data. Considering this, the need therefore arises that, especially in the event of pandemics, doctors must provide the public only with evidence-based information in a simple and shared way in order to avoid misinterpretation and misunderstanding.

Better coordination between the medical community, governments, and the mass media is therefore needed to avoid the spread of disinformation through different channels, limiting the dissemination of fake news and thereby better engaging the general public to adhere to correct guidelines.

4.12.3 DETECTION:

The spread of information or misinformation in online social networks is context specific and studies have revealed topics such as health, politics, finances and technology trends are prime sources of misinformation and disinformation in different contexts to include business, government and everyday life.

Methods using machine learning and Natural Language Processing (NLP) techniques exist to automate the process to some extent.

However, because of the semantic nature of the contents, the accuracy of automated methods is limited and quite often require manual intervention.

The amount of data generated in online social networks is so huge as to make the task computationally expensive to be done in real time. We analysed the literature on cognitive psychology to understand the process of decision making of an individual.

An individual is seen to make decisions based on cues of deception or misinformation he obtains from the social network.

4.13 Day – TO – Day Life Crimes:

1. Online shopping and auction fraud:

The Home Office defines this category as “fraud attributable to the misrepresentation of a product advertised for sale through an internet auction site or the non-delivery of products purchased through an internet auction site.”This fraud was chosen as one of the individual fraud types for two reasons. On one hand, as illustrated by its name, the internet plays an essential role in its commission.[55]

On the other hand, it was considered that online shopping and auction fraud is a crime that should affect both individuals and organizations, thereby permitting comparisons between them.

2. Dating fraud:

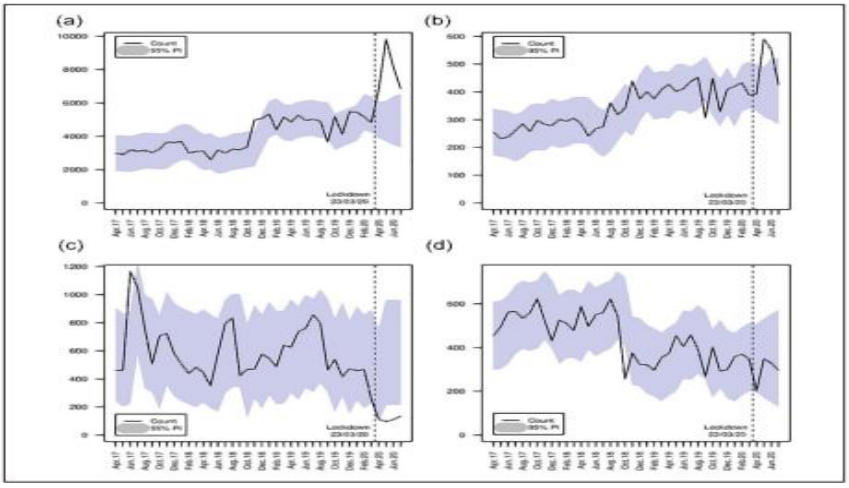
In this type of fraud “the intended victim is befriended on the internet and eventually convinced to assist their new love financially by sending them money for a variety of emotive reasons.” This was also requested because the internet plays an essential role in its commission, especially when the typical physical places for meeting a potential partner, such as pubs or nightclubs, are closed or restricted during lockdown.

3. Ticket fraud:

This category “involves the victim purchasing tickets remotely e.g., over the phone or internet.” Data on this fraud were solicited because although often cyber-enabled, the opportunity to commit ticket fraud is created by the desire to carry out activities in the physical world. This crucial link to the physical world allows analysis of the connection between activities in physical space and crime in cyberspace.

4. Door-to-door sales and bogus tradesmen fraud:

This is one of the only crimes in the Action Fraud data that they consider not cyber-enabled and that is committed in relatively large numbers (more than 1,000 cases per year)



[Figure 19: As a,b,c,d]

[ARIMA forecast and actual count of four fraud types in the United Kingdom, April 2017 to July 2020]

Online shopping fraud	95 % PI
Dating fraud	95 % PI
Ticket fraud	95 % PI
Door-to-door fraud	95 % PI

[Table 4]

Above figure visualizes the range of values forecast from the historical series as well as the known count rates for the four individual fraud types analyzed in this research.

First, **Figure (a)** shows a steep increase in recorded online shopping and auction fraud in March, April and May 2020 that is far beyond the values that would be expected 95% of the time in accordance with the ARIMA prediction intervals. The number of recorded offenses then dropped back down in June and July but remained outside the range of predicted values

Figure (b) indicates a similar trend with regard to dating fraud: a pronounced increase immediately subsequent to the introduction of lockdown measures in the United Kingdom. However, in contrast to online shopping fraud, this is followed by what appears to be a return to the less steep historical upward trend in June and July.

In Figure (c) we can discern that the trend for ticket fraud is the inverse of that observed for the previous two fraud types. Ticket fraud appears to have a seasonal pattern, with higher levels of recorded crime in spring and summer than in winter and autumn in the 3 years prior to 2020. However, recorded ticket fraud during the first months of the COVID-19 pandemic was reduced to close to zero. In April, May, June, and July 2020, it was below the prediction interval and far below the numbers recorded in the spring and summer of 2017, 2018, and 2019.

Finally, as shown in **Figure (d),** door-to-door frauds were on a downward trend from April 2017. This trend appears to have continued during the pandemic with a notable drop in April 2020; however, the reduction in this fraud type was within the prediction interval forecast by the ARIMA model.

Thus, based on the analysis of these four individual fraud types, the null hypothesis with regard to H2 is not rejected because even though the cyber-enabled online shopping fraud and dating fraud did increase, ticket fraud, which is also cyber-enabled but dependent on events that take place in physical spaces, decreased.

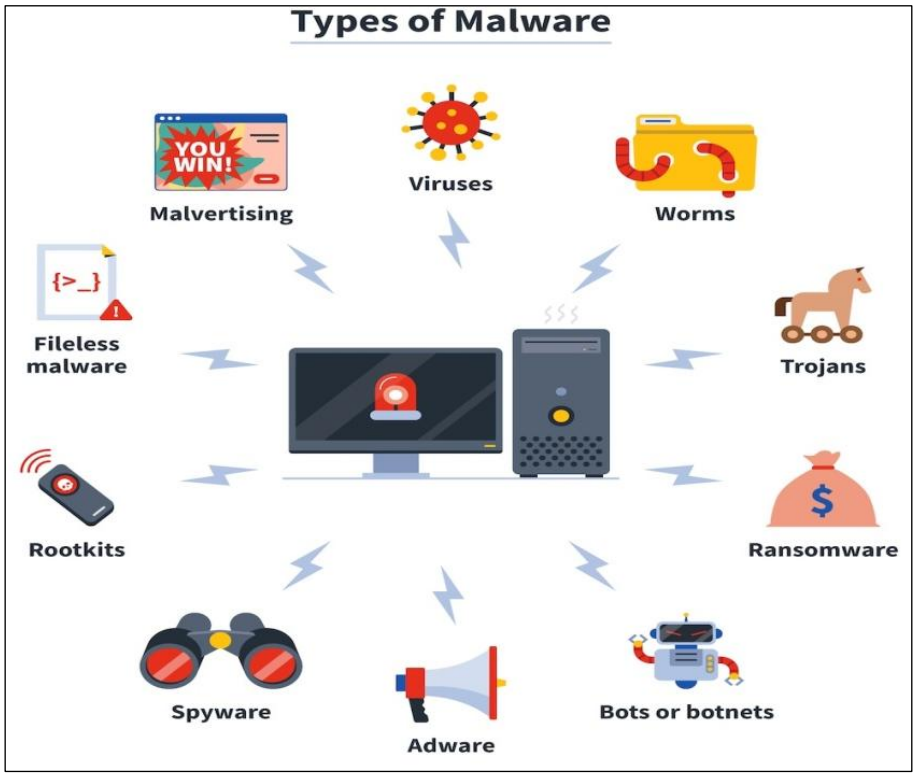
As such, it appears not all cyber-enabled frauds have been affected in the same manner by the mobility restrictions associated with the pandemic. Furthermore, the decline in door-to-door sales fraud identified in this study follows the pre-COVID downward trend and the variability during the first months of the pandemic is not beyond the 95% prediction interval.

However, that the opportunity structures for fraud are nuanced and that the reductions in offline routine activities during the pandemic are associated with disparate effects on distinct cyber-enabled fraud types. As we have seen, less offline retail activity appears related to more online activity and, consequently, more online shopping fraud. On the contrary, less ticket-related offline leisure and transport activities led to a decrease in ticket fraud.In this sense, ticket fraud provides an interesting example of online opportunity structures being affected by offline changes in routine activities; it demonstrates how a decline in activities in the physical world can also reduce opportunities for cyber-enabled frauds.

4.14 MALWARE

Malware is derived from the terms malicious software. Hackers develop malicious software to infect and gain access to the victim computer without the user's consent.There are different types of malware they are spyware, ransomware, viruses, adware, worms, Trojan horses, or any other kind of malware program that can get into the system.[9]

Malware, also known as malicious code, refers to a program that is covertly inserted into another program with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the confidentiality, integrity, or availability of the victim's data, applications, or operating system. Malware is the most common external threat to most hosts, causing widespread damage and disruption and necessitating extensive recovery efforts within most organizations.



[Figure 20: Types Of Malware Attack]

4.14.1 Malware incident handling :

1. Keystroke Loggers:

A keystroke logger monitors and records keyboard use. Some require the attacker to retrieve the data from the host, whereas other loggers actively transfer the data to another host through email, file transfer, or other means.

2. Root kit:

A rootkit is a collection of files that is installed on a host to alter its standard functionality in a malicious and stealthy way. A rootkit typically makes many changes to a host to hide the rootkit's existence, making it very difficult to determine that the rootkit is present and to identify what the rootkit has changed.

3. Web Browser Plug-Ins:

A web browser plug-in provides a way for certain types of content to be displayed or executed through a web browser. Malicious web browser plug-ins can monitor all use of a browser.

4. E-Mail Generators:

An email generating program can be used to create and send large quantities of email, such as malware and spam, to other hosts without the user's permission or knowledge.

5. Attacker Toolkits:

Many attackers use toolkits containing several different types of utilities and scripts that can be used to probe and attack hosts, such as packet sniffers, port scanners, vulnerability scanners, password crackers, and attack programs and scripts.

4.14.2 Malware Incident Prevention

This section presents recommendations for preventing malware incidents within an organization. The main elements of prevention are policy, awareness, vulnerability mitigation, threat mitigation, and defensive architecture.[61]

Ensuring that policies address malware prevention provides a basis for implementing preventive controls. Establishing and maintaining general malware awareness programs for all users, as well as specific awareness training for the IT staff directly involved in malware prevention– related activities, are critical to reducing the number of incidents that occur through human error. Expending effort on vulnerability mitigation can eliminate some possible attack vectors .

Implementing a combination of threat mitigation techniques and tools, such as antivirus software and firewalls, can prevent threats from successfully attacking hosts and networks. Also, using defensive architectures such as sandboxing, browser separation, and segregation through virtualization can reduce the impact of compromises..When planning an approach to malware prevention, organizations should be mindful of the attack vectors that are most likely to be used currently.They should also consider how wellcontrolled their hosts are (e.g., managed environment, non-managed environment); this has significant bearing on the effectiveness of various preventive approaches.

In addition, organizations should incorporate existing capabilities, such as antivirus software deployments and patch management programs, into their malware prevention efforts. However, organizations should be aware that no matter how much effort they put into malware incident prevention, incidents will still occur (e.g., previously unknown types of threats, human error).

For this reason, organizations should have robust malware incident handling capabilities to limit the damage that malware can cause and restore data and services efficiently.

4.14.3 TECHNIQUES

[A] Repackaging Malware: authors repackage the popular applications of Android official market, Google Play, and distribute them on other less monitored third party app-store. Repackaging includes the disassembling of the popular benign apps, both free and paid; append the malicious content and reassembling of app .This process of repackaging is done by reverseengineering tools. During repackaging, malicious authors change the signature of repackaged app and so the app seems new to the antimalware. TrendMicro report have shown that 77% of the top 50 free apps available in Google Play are repackaged .

[B] Drive By Download : It refers to an unintentional download of malware in the background. Drive by download attacks occur when a user visit a website that contains malicious content and injects malware into the victim‟s device without the user‟s knowledge. Malware developers use Android/NotCompatible which is one of the drive-by download app.

[Figure 21: Malware families seen in 2015]

[C] Dynamic Payloads Malwares:

They penetrate into Android devices through dynamic payload technique. They encrypt the malicious content and embed it within APK resources. After installation, the app decrypts the encrypted malicious payload and executes the malicious code. Some malwares, instead of embedding payload as resource, download the malicious content from remote servers dynamically and are not detected by static analysis approach .

[D] Stealth Malware Techniques:

On Android device malware scanners cannot perform deep analysis because of the availability of limited resources such as battery. Malware developers exploit these hardware vulnerabilities and obfuscate the malicious code to easily bypass the antimalware. Different stealth techniques such as key permutation, dynamic loading, native code execution, code encryption and java reflection are used to attack the victim‟s device.

1. CovidLock, 2020

Fear in relation to the Coronavirus (COVID-19) has been widely exploited by cybercriminals. CovidLock ransomware is an example.This type of ransomware infects victims via malicious files promising to offer more information about the disease.The problem is that, once installed, CovidLock encrypts data from Android devices and denies data access to victims.To be granted access, you must pay a ransom of USD 100 per device.

2. Locker Goga, ransomware, 2019

Locker Goga is a ransomware that hit the news in 2019 for infecting large corporations in the world, such as Altran Technologies and Hydro. It’s estimated that it caused millions of dollars in damage in advanced and targeted attacks.Locker Goga infections involve malicious emails, phishing scams and also credentials theft.Locker Goga is considered a very dangerous threat because it completely blocks victims’ access to the system.

4.14.3 TYPES OF MALWARE

Virus

Viruses are a subgroup of malware. A virus is malicious software attached to a document or file that supports macros to execute its code and spread from host to host. Once downloaded, the virus will lay dormant until the file is opened and in use. Viruses are designed to disrupt a system's ability to operate. As a result, viruses can cause significant operational issues and data loss.

Worms

Worms are a malicious software that rapidly replicates and spreads to any device within the network. Unlike viruses, worms do not need host programs to disseminate. A worm infects a device via a downloaded file or a network connection before it multiplies and disperses at an exponential rate. Like viruses, worms can severely disrupt the operations of a device and cause data loss.

Trojan virus

Trojan viruses are disguised as helpful software programs. But once the user downloads it, the Trojan virus can gain access to sensitive data and then modify, block, or delete the data. This can be extremely harmful to the performance of the device. Unlike normal viruses and worms, Trojan viruses are not designed to self-replicate.

Spyware

Spyware is malicious software that runs secretly on a computer and reports back to a remote user. Rather than simply disrupting a device's operations, spyware targets sensitive information and can grant remote access to predators. Spyware is often used to steal financial or personal information. A specific type of spyware is a keylogger, which records your keystrokes to reveal passwords and personal information.

Adware

Adware is malicious software used to collect data on your computer usage and provide appropriate advertisements to you. While adware is not always dangerous, in some cases adware can cause issues for your system.

Adware can redirect your browser to unsafe sites, and it can even contain Trojan horses and spyware. Additionally, significant levels of adware can slow down your system noticeably. Because not all adware is malicious, it is important to have protection that constantly and intelligently scans these programs.

Ransom ware

Ransom ware is malicious software that gains access to sensitive information within a system, encrypts that information so that the user cannot access it, and then demands a financial payout for the data to be released. Ransomware is commonly part of a phishing scam. By clicking a disguised link, the user downloads the ransomware. The attacker proceeds to encrypt specific information that can only be opened by a mathematical key they know. When the attacker receives payment, the data is unlocked.

Fileless malware

File less malware is a type of memory-resident malware. As the term suggests, it is malware that operates from a victim's computer's memory, not from files on the hard drive. Because there are no files to scan, it is harder to detect than traditional malware. It also makes forensics more difficult because the malware disappears when the victim computer is rebooted. In late 2017, the Cisco Talos threat intelligence team posted an example of fileless malware that they called DNSMessenger.[58]

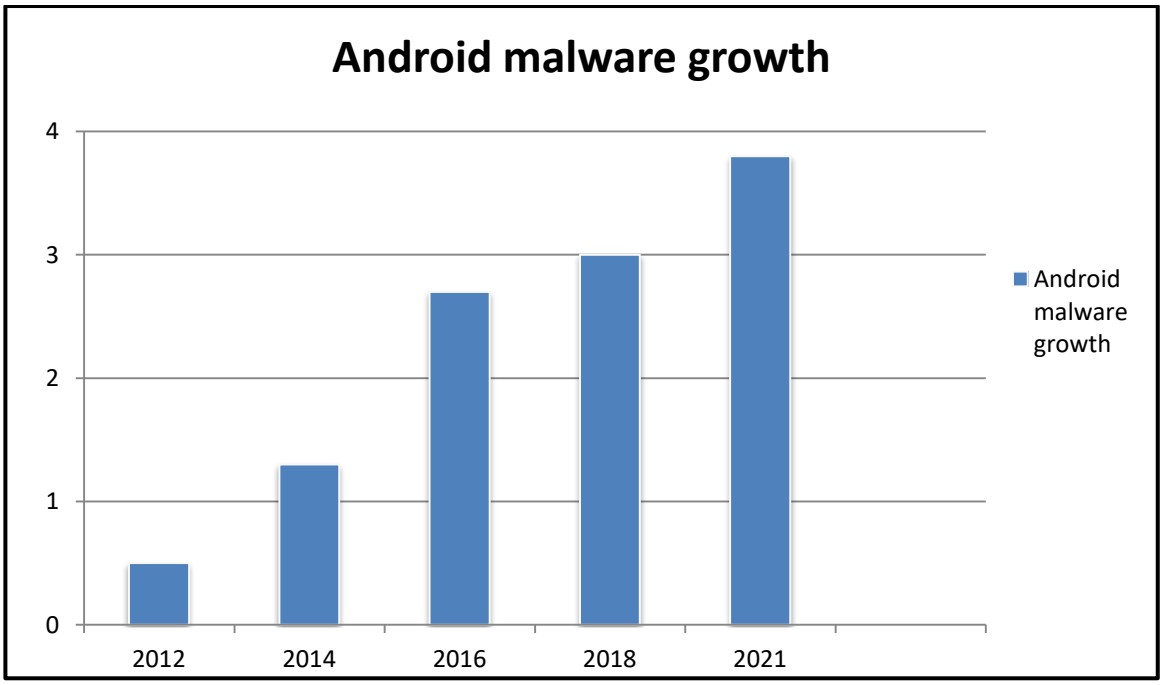
Malware types	Threats percentage
PUAs	50%
Adware	27%
Trojans	22%
Riskwares	11%
SMSsenders	7%
Downloaders	3%

[Table 5: TOP ANDROID MALWARE TYPES IN 2015]

4.14.4 Dark Herring malware on millions of Android device

There are hundreds of malware techniques identified which attack the Android platforms in several ways such as sending messages without the victim‟s knowledge and deleting them by itself, sending user‟s private information to some other server and many more. So there is a great need to protect user‟s data from these malwares.

This ever increasing malware threats have forced the Android antimalware industry to develop the solutions for mitigating malicious app threat on Android smartphones and other Android devices. Two main approaches are used for this purpose: Static approach and Dynamic approach. Antivirus programs use any of these approaches to protect the mobile systems from the malware attacks. They detect the malicious apps and notify the user about such apps and take measures to remove these malwares. With the increasing number of threat level, the antivirus detection rate has also increased. As a result of threat & malware, and protection mechanism offered by Android antimalware programs, the overall risk situation of Android users is difficult to assess.



[Figure 22]

Wide range of malwares has been detected and the number of malwares is increasing every year. According to TrendMicro, malwares have increased to 7.10 million in first half (1H) of 2015. Above Figure shows the increased number of Android malwares over the years. The behavior of different malware families is provided in subsequent sections.

5. Literature Survey

No	Research Paper Name	Publishing Company/ Author Published Date	TECHNIQUE	CRIME
1	Cybercrimes during COVID -19 [1]	April 2021	1] COVID 19 As Phishing Bait 2] Rise of Ransomware 3] Spread of Misinformation	1] URLs registered 2] Black NET 3] Trojan
2	Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic[2]	2020	1] Zoom Meetings 2] DDOS Attack 3] Malicious Domains	1] Flooding the organizations' 2] corona virus-themed Win locker 3] Using domain spoofing 4]Making free subscriptions
3	Malware Incident Prevention and Handling [3[	July 2013	1.Maze ransomware attack 2.Phishing scam 3. largest-ever cyber security threat 4.Cyber gangsters hit UK medical	Organizations should develop and implement an approach to malware incident prevention.
4	A Surge in Cyber-Crime during COVID-19[4]	October 15-19, 2018	1.Worldwide spending on cybersecurity 2. businesses experienced phishing. 3. business leaders feel	Measure the level of similarity of two time series is to calculate the distance between them.
5	Fake COVID-19 vaccination Fraud in India[5]	26 August, 2021	1] South Africa, 2] In India, Mumbai 3] In China 4] In Kolkata,	register on fake websites dubbed as ‘Pradhan Mantri Berozgar Bhatta

6	A behavioural-based approach to ransom ware detection2017[6]	2017	1.Healthcare Ransomware 2.BRENNTAG 3. COLONIAL PIPELINE	1.Static-based analysis detection: Dynamic-based 2.analysis
7	Detecting Covid-19 chaos driven phishing/malicious URL attacks by a fuzzy logic and data mining based intelligence system[7]	2021	1.Ransom ware attacks 2.Malicious domains 3. Phishing 4.Intelligence architecture	The URL of the site is taken from the browser address bar in the chrome extension's content script. The data will then be sent to the web service.
8	Cyber bullying Perpetration: Children and Youth at Risk of Victimization during Covid-19 Lockdown[8]	February , 2021	1 Humiliation, Harassment 2. Online Violence 3.The use of Fake Accounts 4.Posts Sharing Sexual Content	1.Denigration 2.Flaming 3.Impersonation Outing and Trickery
9	Android Malware Detection & Protection[9]	February 2016	Dark Herring malware on millions of Android devices	A concept of hybrid antimalware is presented which will address the limitations of existing static and dynamic approaches.
10	Detection of cyber security issues in digital healthcare[10]	April , 2019	The research found that 86 percent involved phishing and/or smishing; 65 percent involved malware; 34 per cent involved financial fraud	It is generated a questionnaire to collect data on the topic of corona virus causes a rise in cyber-crime.).

11.	Cyber Security and Privacy Protection During Coronavirus Pandemic[11]	2021	1] Abuse of medical data 2]Illegal Control 3]Fake news website	1](Co100) App : Signals the phone owners 2]The msg having exclusive news 3] Campaigns pretending 4] Hackers devised an email
12.	Cyber security attacks on smart home during covid-19[12]	February 09,2022	phishing attack,Malware ,Ramsom ware,Online meeting ,hijacking ,Zoom-bombing ,Fake apps	1.Fake Login Email Screen 2.Geographic location 3.BabyShark 4. Rammit 5. Pizd

Cyber crime which is considered as the illegal activity committed on the Internet is now a big threat to the nation. Now a day's number of internet users is increasing rapidly. As the use of Internet is increasing by which any information can be accessed easily from anywhere, so various illegal activities basing upon the internet are also increasing. A report McAfee estimates that the annual damage to the global economy is at $445 billion; however, a Microsoft report shows that such survey-based estimates are "hopelessly flawed" and exaggerate the true losses by orders of magnitude. Approximately $1.5 billion was lost in 2012 to online credit and debit card fraud in the US. In 2016, a study by Juniper Research estimated that the costs of cybercrime could be as high as 2.1 trillion by 2019. The majority of cyber crimes are centered on forgery, fraud and phishing. India is the third most targeted country for phishing attack after the US and the UK.

Many people can access this social networking site through iPhone, AndroidPhone, Tab, Laptop or other electronic gadgets. They can expertise their profile through posting any comment, uploading a photo, text or scrap posting, uploading of music and video in their profile to make the profile more attractive in front of their Facebook friends. By this site, users may choose to communicate through various digital objects are connected with friends who are far away from them.. In 2015, nearly 2500 million users are available in India. However, the maximum part of users is covered by teenagers inIndia. Impact of Facebook has a Social Networking Site (SNS)

6. Data and Analysis

We explore the cybercrime landscape with these cybercrime facts and statistics. The numbers will give you an idea of how widespread cybercrimes are in an increasingly digital and connected world.

Among the 13 crimes measured, the top two most worrisome for Americans are cybercrimes. 72% feared computer hackers accessing their personal, credit card, or financial information, and 66% worry about identity theft. (Gallup, 2020)

Each year since 2001, the monetary damage caused by cybercrime has been increasing exponentially. It already reached around $4.2 billion in 2020. That number does not include damages from unreported cases. (IC3, 2020)

The United States suffered the most high-profile cyber-attacks with 156 separate incidents between May 2006 and June 2020. (SecurityBrief, 2020)

Germany, India, Australia, and the United Kingdom have all been targets of significant attacks in the last 14 years as well. (SecurityBrief, 2020)

These attacks on different countries included assaults on defense agencies, government and federal systems, and prominent tech companies. (SecurityBrief, 2020)

4.83 million DDoS attacks were recorded in the first half of 2020. (Help Net Security, 2020)

Data breach gets our attention when we read about billions of personal user information stolen from large companies. In truth, a data breach can happen to companies big or small and can involve data theft of thousands of records.

In January 2019 alone, 1.76 billion records were leaked from various data breaches around the world. (IT Governance, 2019)

In the first three quarters of 2020, there were 2,953 reported breaches across the globe. It was a 51% decrease compared to the same period in 2019. (RiskBased Security, 2020).

However, a staggering 36 billion records were exposed by the end of September 2020, making it the worst year on record in terms of data breaches. (Risk Based Security, 2020)

70% of workers said that remote work due to COVID-19 would increase the cost of a data breach. (IBM, 2020). The average cost of a data breach on remote work is about $137,000 per attack. (IBM, 2020)

Remote desktop protocol (RDP) attacks increased by 400% during the onset of the COVID-19 pandemic from March to April of 2020. (Kaspersky, 2020)

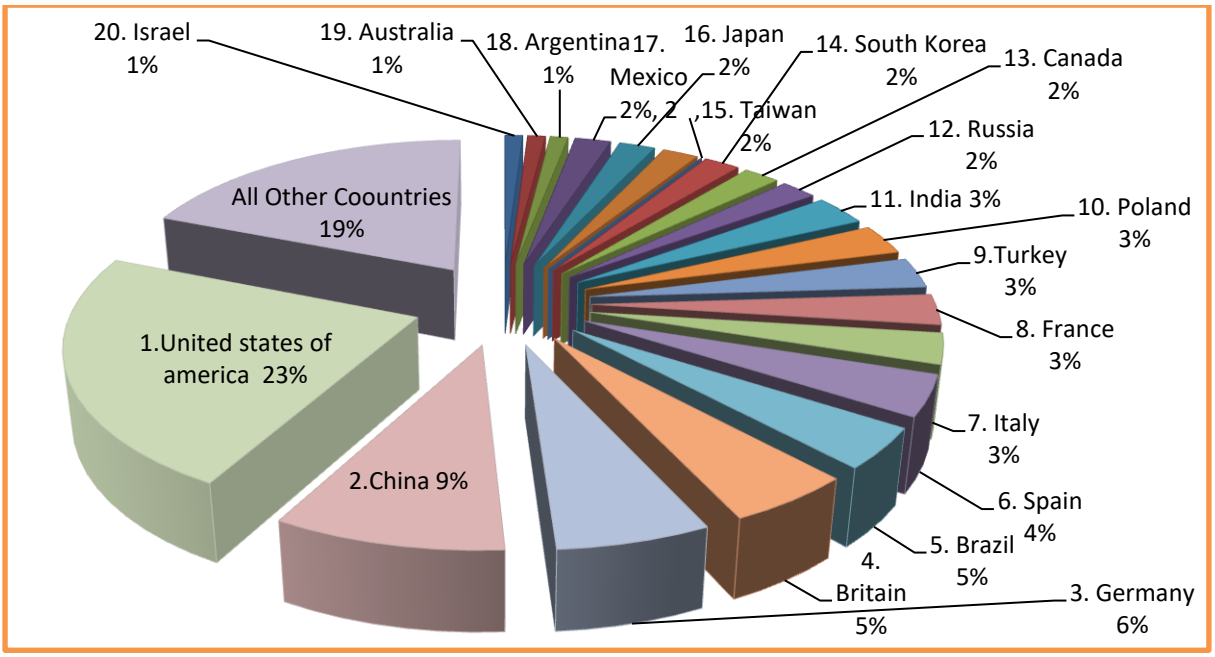
In 2020, it takes an average of 280 days to identify and contain a data breach. (IBM, 2020)45% of breaches are done through hacking. (Verizon, 2020) It is followed by errors at 22%, social attacks at 22%, malware at 17%, misuse by authorized users at 8%, and physical actions at 4%. (Verizon, 2020)

72% of data breach victims are large businesses. (Verizon, 2020)Additionally, 28% of victims are small enterprises. (Verizon, 2020).Often, external actors (70%) and organized criminal groups (55%) are behind the data breaches. (Verizon, 2020)However, a small percentage of the perpetrators have involved business partners (1%) and multiple attackers (4%). (Verizon, 2020)

98% of Internet-of-Things (IoT) devices are unencrypted, which exposes confidential data to attacks. (SecurityBrief, 2020).51% of threats in the healthcare industry are coming from imaging devices. (SecurityBrief, 2020). Additionally, 72% of virtual local area networks in the healthcare industry mix IT assets and IoT devices, which allows malicious software to spread rapidly through various end-user devices. (Security Brief, 2020)

A large number of attacks use web applications at 43%. (Verizon, 2020)

7. Results and Discussions

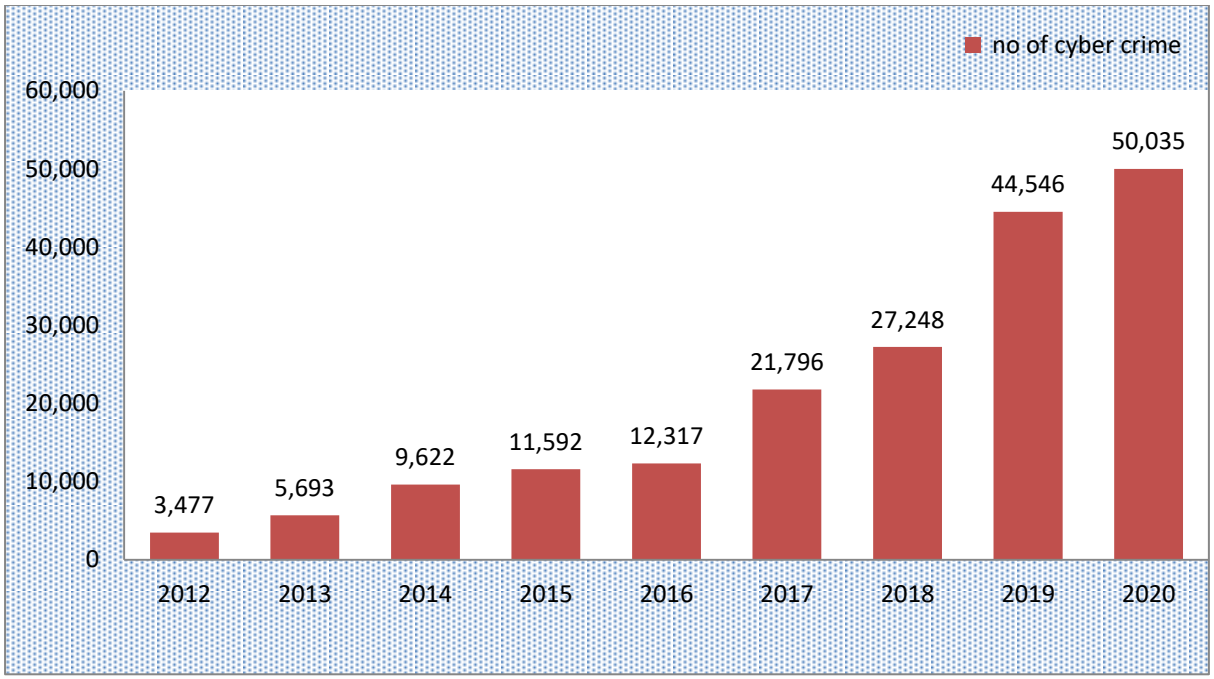


[Figure 23: Cyber Crime Rate in Different Countries]

Symantec has ranked 20 countries that face, or cause, the most cybercrime. In compiling such a list, Symantec was able to quantify software code that interferes with a computer's normal functions, rank zombie systems, and observe the number of websites that host phishing sites, which are designed to trick computer users into disclosing personal data or banking account information. [9][10][12]

Symantec was also able to obtain data including the number of bot-infected systems which are those controlled by cybercriminals, rank countries where cyber attacks initiated and factor in the a higher rate of cybercrime in countries that have more access to broadband connections.

The highest rate of cybercrime was found to be in the United States which may mainly contribute to the broad range of available broadband connections, which are those that allow uninterrupted internet connectivity



[Figure 24 Cyber Crime Rate in India]

It was estimated that in 2017, consumers in India collectively lost over 18 billion U.S. dollars due to cyber crimes. However, these were estimates based only on reported numbers. In a country like India, it is highly likely that the actual figures could be under-reported due to a lack of cyber crime awareness or the mechanisms to classify them.

- Country has registered 107% of CAGR in the number of Cyber Crimes registered in last few years.
- 3,477 Cyber Crime cases were registered in 2012.
- 50 percent in the next few years, reaching 12,317.
- The statistics of 2020 stupor people as it shows the unexpected increase, making the count of cyber crime cases reach 50,035. Surprisingly,
- In 2016 the number of cases registered under Cyber Crime laws increased by more than 100% to 27,248.

8. CONCLUSION

The analyses indicate clear and noticeable increase in cyber-attacks and cybercrimes at the peak of COVID-19 epidemic worldwide. Due to the imposition of bans by governments and the stay at homes, which led to an increase in the use of the Internet and thus the exploitation of cybercriminals to increase their campaigns. The everyday routine activities of millions of individuals have moved from physical to online environments, and opportunities for crime appear to have shifted towards cyber-dependent or cyber-enabled crime.While it may be lucky for some businesses, in serious cases, the data that are compromised might heavily affect the organization and customers and therefore leads the company to be unable to continue on normal operations. A new age of cyber awareness as companies now send their employees to work from home with limited security. Virtual private networks (VPNs) and servers will play a significant role in cyber security of the future. Not only are many companies across the world going to work from home models, thousands of work-from-home companies are now springing up and are facing similar problems. Cyber criminals are all too aware of the limited security that individuals can provide at home. New challenges for the work-at-home individuals include finding simple yet secure solutions for cyber security.

Future Direction

In the future, cyber security will be developed with the integration of the latest technologies, such as Artificial Intelligence, Blockchain, Internet of Things, and much more. This is proven when 61% of the enterprises say, according to Forbes in 2019, that they are unable to detect data breach without the help of Artificial Intelligence. Traditional services can be expensive and risky, but with Blockchain, any transaction or trade processes within asset management are shown to be highly secure and more efficient as there is no room for error with Blockchain. With enormous amounts of data being generated day by day, Big Data can be riskier than ever. Professionals can work on their way to research and utilize machine learning to protect these data.

All in all, while all these threats may sound like a totally new challenge to the next generation of security professionals, all these may only be achievable when these new technologies are firmly implemented in our daily lives. As for the current situation, every user should start taking baby steps of protecting your own personal data before it is compromised by unauthorized users.

9. Reference

1. https://www.researchgate.net/publication/350972842[1]
2. https://www.techrxiv.org/articles/preprint/Ten_Deadly_Cyber_Security_Threats_Amid_COVID-19_Pandemic/12278792/files/22624319.pdf[2]
3. https://journals.sagepub.com/doi/10.1177/10439862211027986 [3]
4. https://www.scirp.org/journal/paperinformation.aspx?paperid=34631https://www.scirp.org/journal/jis/[4]
5. http://dx.doi.org/10.6028/NIST.SP.800-83r1[3]
6. https://scholar.google.com.pk/
7. https://www.researchgate.net/publication/345372297 https://www.researchgate.net/publication/345372297_A_Surge_in_Cyber-Crime_during_COVID-19[4]
8. https://crimesciencejournal.biomedcentral.com/articles/10.1186/s40163-021-00162-9
9. https://pmj.bmj.com/[5]
10. https://www.researchgate.net/publication/322129882
11. http://labs.mwrinfosecurity.com/[6]
12. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3830792
13. https://www.sciencedirect.com/[7]
14. https://www.researchgate.net/publication/349735062[8]
15. https://doi.org/10.1080/0960085X.2020.1771222
16. https://www.researchgate.net/publication/297591972[9]
17. https://www.researchgate.net/
18. https://yis.univie.ac.at/index.php/yis/article/view/2783[10]
19. https://doi.org/10.15308/Sinteza-2021-158-164[11]
20. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9210363[12]

10. Appendices

Cybercrime is a global plague that is combated by law enforcement throughout the world. Countries have suffered estimated billions in damages and been forced to update their legal structure to address this new form of crime. Cybercrime has led to the creation of new positions within law enforcement, new units in police departments, and new specialties for lawyers. With traditional forms of crime, a person generally violates a law within a single jurisdiction. Cybercrime is different from other crime because a single offense can cross multiple jurisdictions even cross the globe itself. This scope has created legal and logistical problems that need to be addressed, forced cooperation between law enforcement throughout the world, and made obvious the need for governments to work together.

Unfortunately, although the need is there, many governments have failed or fallen short of the objective to effectively deal with cybercrime. In this appendix, we look at the special issues involved with international investigations and the problems that relate to them. We will see how laws differ from one nation to another, the cooperative efforts between countries to combat cybercrime, and how jurisdictional and other obstacles can prevent cybercrimes from ever being prosecuted.

It Provides the Web site addresses for reference material available on the Internet. The Web sites provide information on laws governing other countries, law enforcement Web sites, and background materials that are useful when investigating computer-related crimes on an international scale.