12/12/2019

***CyberCrimes and DarkWeb***

Techncal Writing report

**SAIFULLAH KHAN Roll Num: 1802012**

**Submitted to: ifran nadeem**

# Abstract

The coin has two sides, we can see the first one directly because it is visible to everyone but to see the other side of the coin we had to flip it. Same is the case in today’s world. Our society has two types of people.  Some people use the advance technology for good reasons such as to make easiness for other individuals like online banking, online trading, and so many things that decrease the working time as compared to the past. While other types of people use the same technology for crimes like online money frauds, hacking, password cracking, and different attacks on websites, databases, servers and other information centers.

As the world is growing, a lot of inventions are taking place in the field of information technology. These inventions are really helpful in modern life. Like computers make computation easy and so on. But on the other side the notorious people take advantage of it. Like they use “parrot security” operating system for hacking. They use “Kali linux” for different types of penetrations on websites. They use different advance application for stealing users data across the network. So they use computer as a crime machine and these types of crimes are called Cyber Crimes. These types of activities are committed on “Dark web”.

Things become more interesting when “Super computer” came into play. These are giant computers that can perform such tasks that other computers cannot does. They make research extremely fast such space research. But as we stated that coin have two faces, these giant computers can be used for illegal activities such as cyberattacks on different agencies (as a Cyber weapon). Like attacks on Iran nuclear plants. That virus was designed on a high-tech super computer named stuck net virus the most powerful weapon.

**Table of Contents**

[Abstract 1](#_Toc27056855)

[Introduction 4](#_Toc27056856)

[Research (Work) 5](#_Toc27056857)

[Cyber Crime 5](#_Toc27056858)

[Types of Cybercrime 5](#_Toc27056859)

[Trojan: 7](#_Toc27056860)

[Viruses: 9](#_Toc27056861)

[STUXNET Computer virus: 11](#_Toc27056862)

[Denial of server attack: 12](#_Toc27056863)

[Ransomware attacks 14](#_Toc27056864)

[ Locky 15](#_Toc27056865)

[ Bad rabbit 15](#_Toc27056867)

[ WannaCry 16](#_Toc27056869)

[ Crypto Locker 16](#_Toc27056871)

[ Golden Eye 16](#_Toc27056873)

[Dark Web 16](#_Toc27056875)

[Silk Road 18](#_Toc27056876)

[Results: 20](#_Toc27056877)

[Conclusion: 21](#_Toc27056878)

[Refrences: 22](#_Toc27056879)

# Introduction

               Cyber Crimes can be defined as the act that can take place to steal information when the computer is used as a target (victim) or as a weapon.

Cyber Crimes has many shapes depending on the goals and skills of attacker person/group. I.e. there are thousands of ways a hacker can get access to your computer. If they group is highly skilled the attack can be destructive, on the other hand if the group is not highly skilled there is a possibility you can stop the hacker attack.

So we cannot quit the use of these modern technology in order to avoid Cyber Crimes nor we can leave them as it is. There for different laws are made to protect these types of hazards but still “Hackers” find a lot of ways to commit such activities.

This report will cover some aspects of Cyber Crimes, how it happens on Dark web and how they can be dismantled.

So any illegal activity that involves computer for stealing data falls within Cyber Crime.

# Research (Work)

## Cyber Crime

“Offences that are done by individuals or group of individuals with illegal goal/motive to damage reputation of victim or to make loss to victim maybe directly or indirectly using modern technology such as networking, communication(including private chat rooms, emails, social media groups etc.)”.

Source: (Moore, R. (2005) "Cybercrime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing)

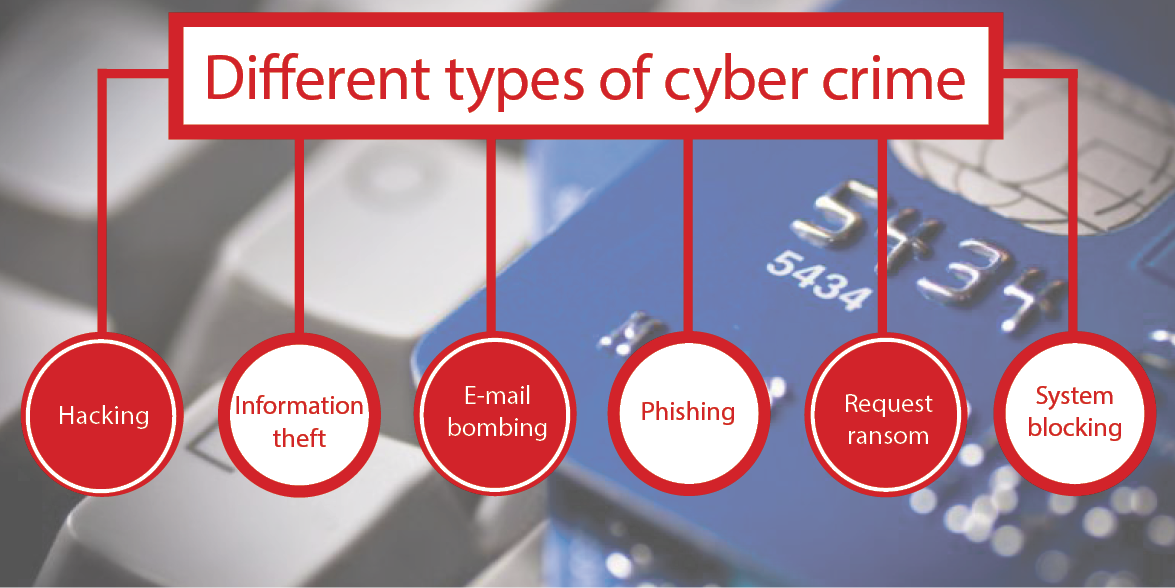
Cybercrime have two broad categories:

*Computer as a target*: In this case computer is used to attack other computers networks

Like hacking, malware attacks, Trojan horse attack, DDos attack.

*Computer as a weapon:* The computer is used as a weapon to commit real world crimes such Cyber Terrorism, some IPR violation, stealing credit card data and so many other.

### Types of Cybercrime



#### Unauthorized access:

Unauthorized access is when an anonymous person gains access to a server, website, database, service, using someone else account or a fake account. This task can be done by numerous ways such as flooding (over traffic) the target user account by access attempts, and so many others ways.

Unauthorized access can also occur when an individual get access to a server where the access is not allowed and he/she gets access by some illegal ways, also be the part of this crime.

In today’s world there are millions of cases where unauthorized person get access to people accounts. It has been estimated that in every 3 seconds 1 ID has been stolen.

#### Hacking:

Hacking is a very broad word. It covers nearly all types of cybercrimes including small password hacking up to huge server’s attacks. Hacking was first demonstrated by magician john Nevil Maskelyne in 1903. He hijacked a public demonstration of Marconi’s telegraph. He also involves in gaining unauthorized access to its computer system.

The biggest hackers attack in history is “STUXNET” virus attack on Iran nuclear power plants. STUXNET consist of three parts 1. WORM\_STUXNET 2. LNK\_STUXNET 3. RTKT\_STUXNET.

Five biggest hacks of all time: [1]

* 1. The viruses that corrupt Iran nuclear power plant computers.
* 2. The hacker that who disappear whole US armory (system).
* 3. The first cyber war that causes destruction on large scale including businesses.
* 4. Bitcoin's attacks also known as Bitcoin’s Monday attack.
* 5. [LulzSec costs Sony $171 million](https://www.alphr.com/security/1000560/the-five-biggest-hacks-of-all-time/page/0/5" \l "PlayStationNetwork" \o "PlayStationNetwork)

### Trojan:

Trojan is also called Trojan horse virus. These are malicious software’s that can take control of your device and perform the work for which it was designed.

But the main property of Trojan which make it different from other malicious software’s is “Spy”. Once Trojan is being installed on your device it takes all the files to the Hackers.

#### Parts of Trojan:

There are two main parts of Trojan.

1. Client Part

This is that part of Trojan which is used to communicate with the server (victim) for receiving information (data). You can call it a remote control part of Trojan, because hackers use it to control the different functions of Trojan in user system.

1. Server Part

This is the active part of Trojan that is send over network to the target system. It is wrapped by some advertisement or any other Aids so that to compelled user to click on it. Once it is installed it take control of the system and generate different ports for connection with the “Client part”.

*Way of action:*

Once the Trojan is installed on user computer it activate all the parts and the first task is to remain undetected in computer so that anyone does not know about it (antivirus system). Then it start reading all the system files and start capturing it , in order to send it to the attacker (client).

When it get complete information about the system it activates the communication part (Linker\_Trojan) and become ready to send the data to the place from where it was launched. Some Trojans are designed to remain in the system for many years due to different reasons.

Some advance Trojans horse viruses destroy the user’s data completely when it time in the system completed or the required goal of hacker is achieved.

*Types of Trojans:*

* Backdoor Trojan.
* Distributed Denial of servers attack Trojan.
* Downloader Trojan.
* Fake AV Trojan.
* Game-thief Trojan.
* Infostealer Trojan.
* Remote access Trojan.
* Rootkit Trojan.
* Trojan banker.
* Trojan IM.
* Ransom Trojan.

#### Trojans malware attacks:

1. *Emotet Banking Trojan.*

After a long time emotet activity become very familiar and increased in the end year 2017. It has been recorded that about 2000 percent increase occurs in these activity by causing financial lose (stealing financial information).

*Source (Symantec 2018 internet security threat report).*

1. *ZeuS or Zbot attack.*

The source code of this Trojan is released in year 2011 when it was used to steal the PIN’s code of user for banking system. So it is called banking Trojan. It records the key pressing sequence when you want to log in into your account and steal it.

1. *Rakhni Trojan attack.*

This virus was found in 2013. It is used to carry ransomware to the target computers but now a days it is used by “cryptojacker” that allows the hacker to use the infected computers for mining of cryptocurrency.

In 2017 the increase in the cryptocurrency mining was 3400 percent.

Source (*Symantec 2018 internet security threat)*

### Viruses:

“A computer virus is a malicious program or computer code that insert or attaches itself with other useful computer program, replicates itself, executes and spread to all the connected computer network”.

It can also be defined that a piece of code that alter the normal execution of the computer programs and damage the computer environment.

Computer viruses are similar to the biological viruses in some features like replicating itself, infected other nearby networks, and remain undetected etc. but the way it differ from biological virus is stealing information and performing required functions. Computer virus is powerful weapon in current era of science and technology because all the information is stored, shared and access online that give us advantage to perform extra work in less time.

We can take example of lecture delivering methods in universities where a common system is provided for one lecture hall so every professor, that want to show his lecture slides/works, have to access his account and he will find his stuff instead to bring his own laptop and after that he founds that there no compatible connection cable for his laptop or power issues may arises. So online data bases helps us.

But hacker can also use these new technologies for their illegal desires, like they can send you an email and it contain a virus file, upon clicking it will take your all work to the hacker.

The very first virus was “Creeper virus” was send over ARPANET that has the ability to replicate itself. It was written by Bob Thomas in 1971 in BBN technologies.

Source ( Thomas Chen; Jean-Marc Robert (2004). [*"The Evolution of Viruses and Worms"*](https://web.archive.org/web/20130809004515/http:/vxheaven.org/lib/atc01.html). Archived from [*the original*](http://vxheaven.org/lib/atc01.html) on 2013-08-09*. Retrieved 2009-02-16*.).

Parts of computer virus

Computer virus have some complex kinds of search algorithms that identifies and locates new target files/program and it also have the ability to replicate itself to that program which was identified as a target.

* *Infection mechanism*

The infection mechanism of any virus is very complex and designed so that anti-viruses program cannot detect it. The first thing that a virus do after entering into a system is to remain undetected and for this reason it sleeps the anti-virus system.

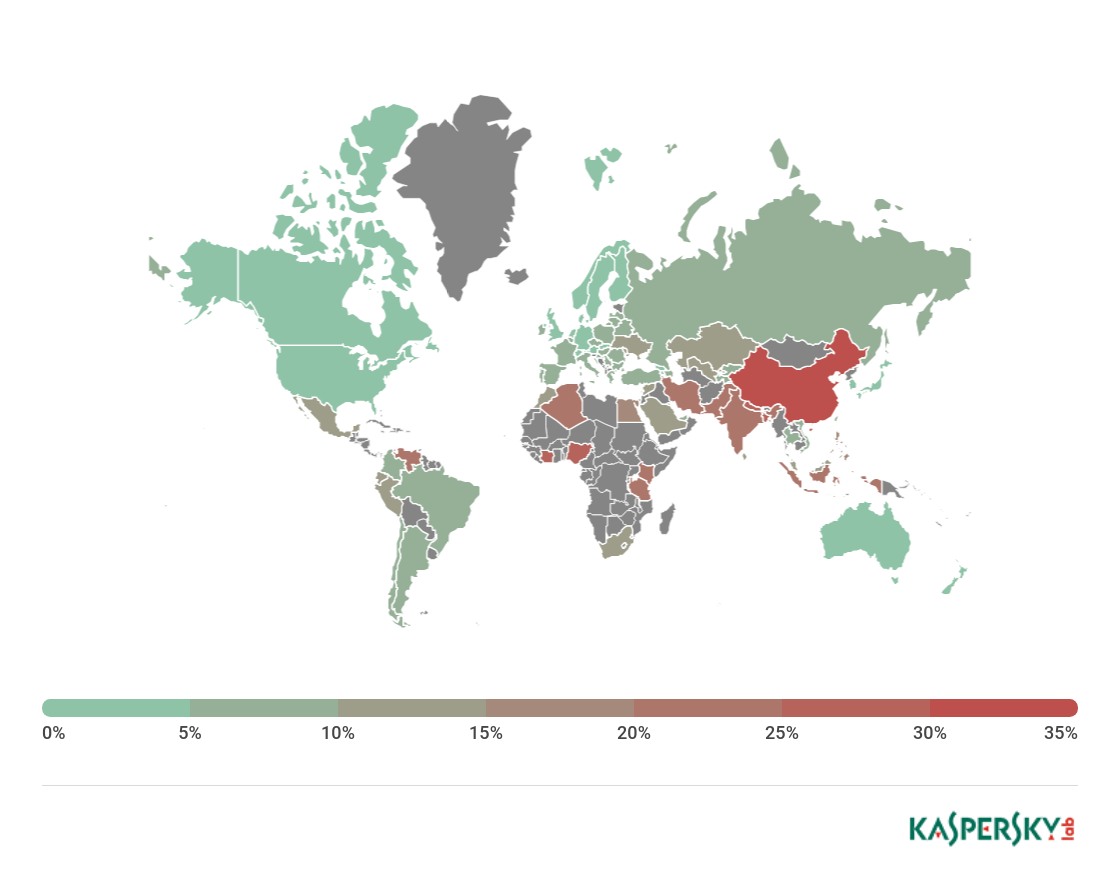
* *Trigger*

It is also called “logic bomb”. Trigger is already compiled/ready file of virus that is can be active at any time when the condition is suitable or the required event is happening. It function is to activate and run the main “payload” of virus.

* *Payload*

It is the main body of the virus that contain the actual purpose of the virus (payload consist of coding that can perform the main task). Once the payload is activated it start the corrupting the files or may perform other malicious activity. The activation of payload slow down the computer speed/processer speed because the virus is consuming these resources for their own purpose. So these activity is noticeable.

*This picture showing Infected countries*



### STUXNET Computer virus:

Stuxnet computer virus is first discovered in 2010 when it was used against Iran nuclear program. Stuxnet targets the SCADA system that is used to control the PLCs, GUIs, and other high power processing system on industrial level for productions. PLCs generally allows automation of processes such as electromechanical for machinery in industries.

Stuxnet interrupt with the PLCs and take control of centrifuges that is used in the purification of Uranium (U238).

*Stuxnet has three main part:*

* Worm

The worm executes all the routine that is closely related to the activation and attack of main payload (main body).

* Link File

Link file generally executes all the .exe files of virus to perform activity and is responsible for the propagation of the virus into all system (spread copies).

* Rootkit

The rootkit is sensitive part of stuxnet that is responsible to prevent the detection of virus by anti-virus system and also to hide the activities when the payload is activated.

### Denial of server attack:

*Denial of server is an attack carried out to shut-down the targeted system/machine, which make it unreachable for legitimate users. The request that is send to the target server triggers a crashing situation for the server.*

Denial of server attack is generally achieved by flooding the bandwidth of any server that is responding to the request.

The hackers first creates thousands of virtual users using some infected system and then start sending request to the server with no return IP addresses or wrong IP addresses (because of virtual clients). That process continues until the server become unable to respond to any legitimate user/request and become crashed.

Using denial of server attack the data is not stolen but the server crashed for some time may be longer depending on the strength of sever.

Popular floods attack are:

* Buffer overflow attack
* ICMP flood
* SYN flood

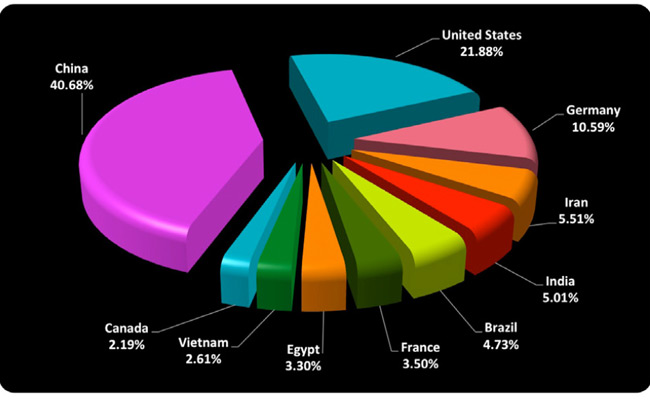
Flooding Example: fig



Just look into the figure, Here every user (fake) wants to access the server and it over rides the responding limit of the server that causes it to shut-down.

Every year thousands of DDos attacks occurs on different servers located in different countries. Some are destructive while some are least. But the main point is can we stop it? The answer is no! we cannot stop it because it is unpredictable to say where the attack is going or where it to be!

Percentage of DDos attack:



### Ransomware attack

Ransomware attack is one of the most familiar attack that is used by the cybercriminals in order to hold people to ransom.

Ransomware attack can target an individual or an organization. Ransom malware is entered into the system using infected USBs, emails, through internet, drive-by download, or any other links. Once the computer system is attack/infected by any type of ransom the user data is encrypted (hacker’s demands money in any digital currency) or the user is locked out-side the system preventing the users to access his system.

Today’s thousands of ransomware attack occurred over different organizations and the millions of money is demanded to relock their data.

#### Types of ransomware

* Crypto ransomware

Crypto ransomware are used by cyber thieves to encrypt data on the user computer with a strong and unique key and leave a message so that the user pay them money and get their files back.

* Locker ransomware

Locker ransomware is used not for encrypting data but it locked down the user outside the system and thus is unable to access their system.

#### Example of ransomware attacks

### Locky

### Locky was first seen in 2016 attacked by a group/organization of hackers that has the ability to lock more than 160 types of files as a target. Locky spreads itself by using different ways such as spam email having infected attachments, and other tricks to trap the user to install it. This method of transfusion is called phishing. Locky targets such types of files that is used by the engineers, graphic designers, programmers and testers.

### Bad rabbit

### Bad rabbit is used against insecure websites to infect it. When the users visit these websites, without knowing that these websites are attacked by hackers, they are infected. It is transmitted by drive-by method.

### WannaCry

### WannaCry was first seen in 2017 when it was leaked by a hacker group called “Shadow broker group”. It is created by USA agency named NSA (National security agency). This ransomware was designed to attack and to exploit some OS vulnerability such as Windows (an easy target). It is reported that WannaCry affects 230,000 computers every year.

### Crypto Locker

### Crypto locker was first seen in 2007. It uses infected emails method to spread over networks of computers. This malware first finds the valuable files and encrypt it in order to demand for money to unlock it. It infect over 500,000 computers every year.

### Golden Eye

### Golden eye was first seen in 2017 when it was used against Iran nuclear program. This malware force the Chernobyl nuclear plants worker to check the radiation level inside the reactor manually (using tools physically without automatically) because they have been locked to do it using their Windows PCs.

## Dark Web

The word “Dark-web” pointed towards an online content that is highly encrypted and is not stored/indexed by search engines that we use normal. It mean every day we search different data using search engines like google, yahoo, Bing etc that find our desired data but the data/content which dark-web holds cannot be search on these conventional search engines because the searching and data storing techniques are quite different from each other.

Fig: *Showing difference between Deep and Dark net*



Dark web is actually the down layer of deep web. That covers a wide range of information which is invisible to regular internet browsing activities.

There are specific tools (browsers) that is used to access and search data on dark web like “torr” aka the onion route. Once you access to dark web there are different websites that provides online market place for purchasing of drugs, illegal weapons, private chat rooms, target killers, contain highly important financial and private data.

Now a question arises that when they buy or sell something illegal they have to pay money for it and so there account can be tracked? The answer is interesting … No! It cannot be. Because they uses their own currency known as “Bitcoin”. Bitcoin is untraceable currency that be used for purchasing and selling of any illegal goods using Dark-web.

Size of Dark web Economy

Economist reported that Drug dealing activity on dark-web ranges from 17 million dollars (in 2012) to 180 million dollars (in 2015), reported in year 2016. But these are just estimations as no one knowns what is going on in dark-web. So the exact economy size is much larger than this estimation because there is major selling weapons that contributes to a greater extent.

Regulators of Dark-web

Regulators of the dark web are struggling to ensure the dark web activity and to make it stable. After the most familiar online drug market was shut down by the US agency FBI known as “Silk Road”. But after the shutting down of Silk Road, Silk Road version2 was popped up, unfortunately FBI and Europol also shut it down in around 2012. Silk Road version3 came into play in 2012 after some months.

## Silk Road

Silk Road was launched in 2011, and was designed by American “Ross Ulbricht”. He uses the two master keys of that time one is “tor browser” for anonymity and other is “Bitcoin”, the untraceable currency. The tor browser help him in untracking the routes of traffic over the internet.

His words “Everyone has the right to buy and sell what he want so long that he doesn’t hurt anyone else”.

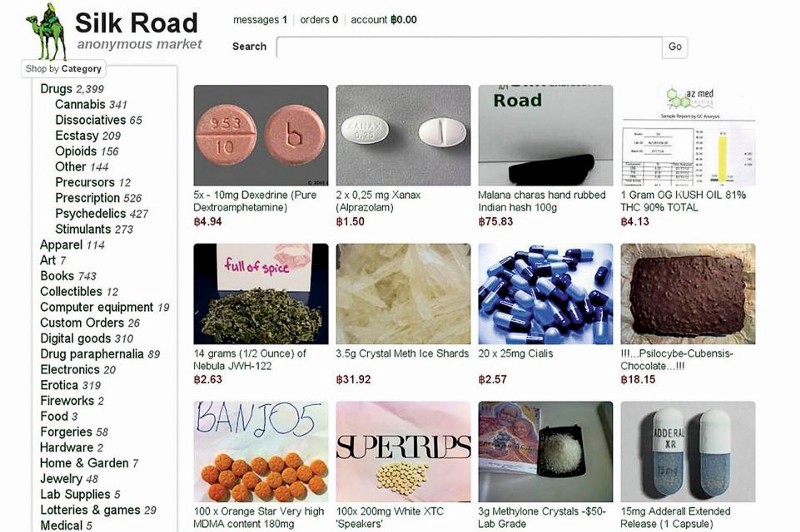
Ross Ulbricht picture



Silk Road was used as an online market for selling and buying drugs. In early days the seller have to buy an account during in auction but later on a fixed price was selected for it. The venders of Silk Road was spread in around 10+ countries and they provides goods to more than 10,000+ customers in a day.

In year May 2013, Silk Road was shut down by the FBI because they found the address of the Silk Road servers located in the Ice land (in the capital of Iceland).

After some months Silk Road v2 was online but FBI again shut it down and in 2014 Silk Road v3 become online.



A picture of Silk Road

## Results:

Studying all these Cyber crimes and their different method of action and their properties take us to the point that it is impossible to stop all kinds of cyber crimes. According to a report (NSA, 2016) 180 million $ loss occurs every year to the cyber related company due to these Cyber Crimes.

If we think about the very first computer virus it was not as much dangerous as the current viruses but it is the Human mind that make it so advance which make it unstopble.

Due to these risk more than 87% of computer users uses different anit-virus system (applications), but still 56% users are at risk and they are facing security problems like their data is hacked, they have spyware in their systems and so many others. But only 18% or less viruses, Trojans and other harmful apps are removed by these security software.

Now if relay on these percentage we can say that these security softwares is unable to stop these Crimes! But it is wrong. All the softwares are made by Humans and we always left some bottle nick in codes (programs) so that the hacker find it and get in from their.

It is reported that more than 90% usage of internet is Dark net. So the normal internet we use is used only 10-12% that is quit confusing! The answer is a wide range of people from normal people to Governament employees and security experts as well as Intelligence and Police uses it for different reasons.

## Conclusion:

After this research and analysis of disserent CyberCrimes and Darknet, it is clear that every Online computer is at risk because the network contain millions of computers and it is strongly possible that a lot computers are infected and the virus is spread from this computers into so many because of internet connection.

Some precautions that might help us to stay safe

* Always update you firewall.
* Regularly check your anti-virus system.
* Donot download anything from unknown site.
* Donot click on pop us from browsers.
* Always scan emails.
* If you encountered with a virus immediately logout from all your accounts and delete your data.
* Always keep a backup for data.
* Use trusted applications only.
* Always scan USBs devices.

## Refrences:

1. (<https://www.alphr.com/security/1000560/the-5-biggest-hacks-of-all-time>)

2. (<https://www.investopedia.com/terms/d/dark-web.asp>)

3. (<https://www.investopedia.com/terms/d/dark-web.asp>)

4. (Wikipedia: <https://en.wikipedia.org/wiki/Stuxnet> )

5. [Silk Road (marketplace) - Wikipedia](https://en.wikipedia.org/wiki/Silk_Road_(marketplace))

6. [How the founder of the Silk Road made millions on his illegal startup on the Dark Web - TechRepublic](https://www.techrepublic.com/article/how-online-marketplace-silk-road-became-the-craigslist-for-illegal-drugs/)

7. [When A Dark Web Volunteer Gets Raided By The Police : All Tech Considered : NPR](https://www.npr.org/sections/alltechconsidered/2016/04/04/472992023/when-a-dark-web-volunteer-gets-raided-by-the-police#mainContent)

8. [What is a Botnet Attack – Definition | Akamai](https://www.akamai.com/us/en/resources/what-is-a-botnet.jsp)

9. [The Silk Road: A Story of Bitcoin, Drugs, and the Dark Web](https://blockexplorer.com/news/silk-road-timeline-bitcoin-drugs-dark-web/)