MOTIVES BEHIND CYBERCRIMES

Bharath Janardan

Student,
School of Computer Science & Engineering,
Lovely Professional University, Phagwara, Punjab, India.

Abstract: Computer and mobile network usage has been increasing for the past few decades, and along with it, the number of illegal cyber activities has also been increasing. To deal with cyber-attacks, it is necessary to understand the motives behind them. The purpose of this research is to study the various motives of a cyber-criminal. Some of the motives have a similarity between them, but others differ significantly.

***Index Terms* - cybercrime, hackers, attackers, target, motive, internet**

I. INTRODUCTION

The development of Information and Communication Technology has affected the conventional lifestyle of the people. The number of personal computers, mobile phones, tablets and other technologies which use the internet has been increasing steadily. Websites, web pages, and internet hosts are sources of clients. These clients provide a lot of information online including their personal information. All this information can get to the hands of cyber-criminals if not secured properly. This is where cybersecurity plays its part. With an increasing number of clients, more and more cybercrimes are prone to happen. Cybercrimes can happen on different scales and from different motives. Identifying the motive behind the attack can help the policy-makers decide on what countermeasures will be effective to prevent further illegal activities[7]. The following section will list the possible motives behind the cybercrimes. The list may not contain all possible motives but will contain several of them.

II. MOTIVES BEHIND CYBER CRIME

2.1 Political Motive

2.1.1 Sabotage

The entire world is using the internet and devices using the internet as a medium for the transmission of data. With the introduction of the Internet of Things (IoT), as the name suggests, physical objects are embedded with sensors. All of these technologies facilitate people. But these technologies facilitate hackers as well. Hackers can tweak the algorithm or code used in these devices which may go unnoticed. With the tweaked code, hackers can sabotage the device. On a large scale, they can sabotage a company or a business. For example, the attacker can target a bank and tweak some code in their ATM which can disrupt the transaction process to give the wrong output. Such an act would compromise the trustworthiness of the bank in the minds of the customers and would affect the loyalty of the customers to the bank.

2.1.2 Espionage

Espionage is not something new to the world. Spies were already a thing since the medieval period to get information anonymously. Even kings used to have spies who travel to other kingdoms and gain important information. With the change in time, spies also evolved, and now we have to deal with bigger challenges under the name "Cyber Espionage". Cyber espionage is the act of gaining unauthorized access to a server, with a motive of getting hands-on sensitive data using proxy servers. The hacker can target the government, the military infrastructure, and other governmental organizations. The threat actors are usually state-affiliated or nation-states who aim for strategic advantage. In 2019, Chinese and Iranian hackers were aggressively attacking the US government agencies to steal information to influence the citizens or to derange the critical infrastructure in the US. Cybersecurity experts believe that this attack was the result of Trump's withdrawal from the Iran nuclear deal and the trade war with China[1].

2.1.3 Propaganda

This is again something which has existed since time unknown. Cyber propaganda is the act of spreading fake news to the audience to compromise the target. We ourselves may have experienced when people have tried to spread fake news about us to create a bad image of us in the minds of our friends or family. With the development of technology and the introduction of social media, spreading fake news just got a thousand times easier. All it takes is to have a social media account, gain some followers, and start spreading the message. To facilitate this attack, there are many tools available on the internet. For example, some tools can be used by the attacker to gain fake followers and paid likes to make the news seem more legit to whoever reads it. The main objective of the attacker is to create a bad image and to defame the target. An example of cyber propaganda would be the spread of fake news about the beverage product Frooti in India, allegedly contaminated with the blood of an HIV-positive employee which has been circulating for quite some time[2].

2.1.4 Protest

Protesting is the act of showing objection, disapproval, or dissent towards an idea or action.

Protest against a political action is the most common protest. The conventional form of protests like riots, public speeches, letters of opposition, group pr mass petitions may be effective within a state or within a country. But what if the entire world come to know about the situation and support the protesters? That is where cyber protesting comes into action. With the greatest technology ever in people's hands -the internet, they can spread the word all over the world within hours or even minutes. The attackers want the whole world to support them against whoever the target is. The target can be the government and government officials of a country, a company, or anybody who is trying to force action on the public.

2.2 Emotional Motive

2.2.1 Boredom

When people are hit with boredom, they tend to do activities to get out of it. Normally, people go for an outing, play games, do some sports activities or just hang out with friends. But when a hacker is hit with boredom, things get tedious for cybersecurity officers. Hackers try to exploit systems are servers just to get out of boredom and this may be an individual hacker or a group of boredom-struck hackers. The satisfaction a hacker gets once he/she successfully compromises the target is like winning a trophy. According to the www.cyberghostvpn.com website, the number of phishing cases has been rising since March of 2020, one of the reasons being the coronavirus pandemic causing boredom amongst hackers.

2.2.2 Hate

We can never predict the actions of a person whose mind is filled with hatred. He/she may even resort to violence. Nowadays, people started using the internet as a medium to publicize their hate towards a person or a group of persons. The attacker may put hate speeches online or may bully the target through social media comments or posts. The attacker may also spread fake news about the target. By doing this, the attacker hopes to get more support from other online users and try to psychologically weaken the target. According to the Indian Express, Maharashtra Police has filed more than 400 cases of cybercrime linked to COVID-19 and related issues during the pandemic, out of which a large portion of them pertain to hate speeches and attempts to give a communal angle to the pandemic.

2.2.3 Revenge

People always have the fear of losing their privacy online. Attackers know this and they take advantage of it to take revenge on their target. Revenge can be by exposing the personal information of the target on the internet, revealing private data of the target to the public, or the worst form of revenge-revenge porn. Revenge porn is the act of publishing sexual acts of the target online.

2.3 Ideological Motive

2.3.1 Freedom of Information

In the cyber world, people who think that the internet is a public place and all the information it contains should be accessible to the users, are many. They want that all information be accessible to everyone for free so they can study, modify, and improve it. So, the attacker(s) target private information and make it public. However, according to their ethics, one should not exploit the information to harm anyone. But this ideology is against the law. An unauthorized person should not have access to confidential data.

2.3.2 Religious Beliefs

Different people have different beliefs regarding their religion. People have all the right to believe in whichever religion they prefer. But some people believe that their religion is superior to others. Not only do they believe that they want to spread their ideology to the world. Thus, they carry out cyber-attacks to promote their religion. They spread propaganda or stage protests. The most common targets of these attackers are corporate websites which they vandalize with religious messages.

In the UK, according to the BBC, the rise in religious hate crimes rose by 40% from 5,949 in 2016-17 to 8,336 in 2017-18[3].

2.3.3 Terrorism

According to the Federal Bureau of Investigations, "The CSIS has defined it (cyber terror) as the use of computer network tools to shut down critical national infrastructures or to coerce or intimidate a government or civilian population". The number of cases of cyber terrorism has been increasing for a long time and is still on the rise. The amount of money the government and large corporations lose because of system breaches are millions. The cybercriminals plan and execute security breaches to gather sensitive data from the servers. This data may then be used by the criminals to blackmail the targets for financial gain.

2.4 Financial Motive

Financial gain is the most common motivation for cybercrimes. In this digital era, hackers have many domains into which they can hack and gain access. One such domain is the financial domain or banks. Since banking services are made available through the internet, hackers have many opportunities ranging from intercepting online transactions to directly hacking into the target's bank accounts. A hacker may also impersonate banks to trick firms and individuals. One of the common attacks is ransomware where the attacker hacks into the system/server/website and demands money from the target if they want it to function again.

The introduction of bitcoins has facilitated the attackers to demand bitcoins instead of currency since bitcoin transactions cannot be tracked. One of the most famous ransomware attacks is WannaCry ransomware which propagated from 12th of May

2017 to 15th of May 2017 which affected more than 200,000 computers across 150 countries causing billions of dollars' worth of damages[4].

2.5 Personal Motive

2.5.1 Self-Amusement

We have all been in situations where we think we were probably going to mess things up, but somehow manage to perform well and get amused by ourselves. This self-amusement boosts our confidence in believing in ourselves and we continue putting ourselves in that vibe. This is the same case with hacking skills. People start with beginner-level hacking and when they find themselves triumphant, they move to the next level. This may finally lead to them being a skillful hacker. However, they might not know the ethics of hacking and go the wrong way.

2.5.2 Intellectual Challenge

When you love doing something and you get really good at it, you look for a challenge so that by completing it, you feel like you have accomplished something in your life and be proud of it. Hackers enjoy the intellectual challenge of finding out vulnerabilities in software systems and exploiting it to achieve clever outcomes. This type of hackers may not harm organizations but rather warn them about the vulnerabilities of the system. However, many other hackers who exploit the vulnerabilities and cause damage to the organization. Pirated software is an example of this type of hackers who crack the original versions of the software and provide it to the public, which will bring loss to the developers.

2.5.3 To Prove Technical Proficiency

Many people in this world want to prove their skills to the world. Some of them use social media public stages to demonstrate their skills. They want people to acknowledge their skills. Some hackers also have this desire to be acknowledged by others for their technical skills. They hack into systems and websites and make some pranks to get the attention of people. Most of them won't harm the target, for their purpose is just to attract attention towards themselves. These hackers may get this motivation by taking up challenges from friends. There are even famous companies like Google who offered $1 million to people who could hack its Pixel 3 and Pixel 4 phones[5].

2.6 Commercial Motive

2.6.1 Trade Secrets/Intellectual Property Theft

This kind of attack deals with stealing intellectual properties like trade secrets, copyrights, patents, etc. Out of these, copyrights and trade secrets are the ones that are frequently stolen. Generally, the stolen data are sold to rival companies for money. This may result in huge losses for the company that created it. Earlier, it was difficult to spy and steal data because it needed a lot of physical labor, money, and was time-consuming. But in this digital era, these works can be done by a single person from his/her home. One of the most common examples is piracy. These days, pirated copies of movies, software, and video games are available on the internet from the day of release[8]. Both piracy and downloading pirated copies are considered illegal.

2.6.2 Attack Against Competitors

Nowadays, there is tough competition in almost all domains. Let it be business, education, job, gaming, and whatever domain you name. To compete with rivals, you have to work hard and be consistent in all aspects. In the case of business, innovation and creativity are two of the most important traits you must have to compete. To bring down the competitor, companies hire hackers to hack into their competitor's network and steal critical data like blueprints, research and development plans, and trade secrets. By getting hands-on such data, a company can plan their future in such a way that their product will have more demand in the future. Or, they may even copy the rival's ideas and implement them before they do. This can cause millions of losses for the rivals including their market value.

2.7 Exploitation Motive

2.7.1 Child Pornography

Images and videos of children (below 18 years of age) involved in sexual activities are traded around the clock. These videos and images are sold to pedophiles. In addition to this, attackers may use it to blackmail the family of the children involved in the sexual act for money. There are many laws in different countries against child pornography. A large portion of those who purchase child pornography is child molesters themselves. The abusers use information systems and online video chatting websites to lure children into engaging in sexual activities. They also arrange meetings with children to perform sexual activities with them. In India, the IT Act (Section 67-B) says that whoever 'collects, seeks, browses, downloads' child pornography is an offender[6].

2.7.2 Harassment

This type of attack includes cyberbullying, hate crimes, cyberstalking, and other forms of online harassment. Attackers try to annoy, provoke, threaten, or cause the target mental distress. The attacker resorts to this type of attack mostly because of a grudge towards the target. The attacker may use social media to propagate hate speeches about the target. The punishment for committing such crimes can be jail time and fines. In addition to this, the convict may be court-ordered for psychological counseling.

III. CONCLUSION

Information systems provide a wide variety of resources to which people are attracted. The number of users connected to online services is increasing day by day with the availability of the internet and smart devices at low costs. This creates a large attack surface for cybercriminals who can basically target anyone connected to the internet. These cybercriminals may be motivated by political, emotional, ideological, financial, personal, commercial, and exploitation motives. Computers, information systems, and the internet are being used by people of all ages. Studies have proven that juveniles and young adults use computers more than other age groups and are most likely to commit cybercrimes. Young people when working on information systems face many challenges which they take on. Some of these challenges may earn them profit in some way or another. Personal satisfaction and financial gain are the most common motives behind their cybercrimes. Since they take on challenges, they are most likely to be involved in online adventures, stalking or stalked, exploiting or exploited, hacking, or hacked. To summarize, the motives for cybercrimes vary greatly from each other but they may have great similarities in what they are trying to achieve. The attackers will be satisfied with whatever part he had in the attack. With more and more digitalization in progress, the number of cybercriminals tends to increase. Knowing the motives for cybercrimes can help in deciding the penalty for illegal activities and to eliminate such potentialities in the future.

REFERENCES

[1] Nicole Perlroth, “Chinese and Iranian hackers renew their attacks on U.S. companies” (Feb 18, 2019) The New York Times. [Online]. Available: https://www.nytimes.com/2019/02/18/technology/hackers-chinese-iran-usa.html

[2] Brett M. Christensen, “HOAX-‘Frooti HIV contamination warning’” (May 22, 2014). HOAX slayer website. [Online]. Available: https://www.hoax-slayer.net/hoax-frooti-hiv-contamination-warning/

[3] The BBC news website. [Online]. Available: https://www.bbc.com/news/uk-45874265

[4] The Wikipedia Website. [Online]. Available: https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

[5] Thomas Brewster, “Google will pay you $1 Million if you can hack its phones” (Nov 21, 2019) . Forbes Website. [Online]. Available: https://www.forbes.com/sites/thomasbrewster/2019/11/21/google-bug-bounty-hits-1-million-if-you-can-hack-its-phones/?sh=7f61df677978

[6] R.K. Vij, “India must review its law on child pornography and address gaps” (Aug 02, 2020). Outlook Website. [Online]. Available: https://www.outlookindia.com/website/story/opinion-india-must-review-its-law-on-child-pornography-and-address-gaps/357863#:~:text=The%20IT%20Act%20(Section%2067,child%20pornography%20is%20an%20offender.&text=The%20POCSO%20Act%20punishes%20only,be%20made%20a%20criminal%20offence.

[7] Li, Xingan. (2017). A Review of Motivations of Illegal Cyber Activities. Criminology & Social Integration Journal. 25. 110-126. 10.31299/ksi.25.1.4.

[8] M. Sai Krupa, “India: Cyber Theft of Intellectual Property” (Mar 14, 2018). Mondaq Website. [Online]. Available: https://www.mondaq.com/india/trademark/682548/cyber-theft-of-intellectual-property