Cyber Crimes: What an Engineer Can Do. . .?

*Note: This report created with some reference and discuss about present cyber-crime should not be used

1st Joyshree Sarkar
dept. CSE
United International University (UIU)
Dhaka, Bangladesh
jsarkar181169@bscse.uiu.ac.bd

2nd Md. Saiful Islam
dept CSE
United International University (UIU)
Dhaka, Bangladesh
mislam181292@bscse.uiu.ac.bd

3rd Minhajul Arefin Fahim
dept. CSE
United International University (UIU))
Dhaka, Bangladesh
mfahim181238@bscse.uiu.ac.bd

Abstract—Cybercrime is a crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target. Cybercrime may harm someone's security and financial health. Cybercrime, also called computer crime, the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy. Cybercrime, especially through the Internet, has grown in importance as the computer has become central to commerce, entertainment, and government. Because of the early and widespread adoption of computers and the Internet in the United States, most of the earliest victims and villains of cybercrime were Americans. By the 21st century, though, hardly a hamlet remained anywhere in the world that had not been touched by cybercrime of one sort or another. There are many types of cybercrime in the world. Some of cybercrime are given below

Index Terms—component, formatting, style, styling, insert

I. INTRODUCTION

Cybercrime is a crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target. Cybercrime can harm a

person's financial health and safety. Cybercrime, also known as computer crime, the use of a computer as an instrument for illegal purposes, such as fraud, trafficking in child pornography and intellectual property, identity theft or invasion of privacy. Cybercrime, especially over the Internet, has grown in importance as the computer has become a central part of commerce, entertainment, and government. Due to the early and widespread adoption of computers and the Internet in the United States, most of the early victims and villains of cybercrime were Americans. In the 21st century, however, there was hardly a village left in the world that had not been affected by some form of cybercrime. There are many types of cybercrime around the world. Some of the cybercrimes are described below.

Identify applicable funding agency here. If none, delete this.

II. DEFINITION OF CYBER CRIME

Cybercrime is any criminal activity that involves a computer, a network device, or a network. While most cybercrimes are carried out with the aim of generating profit for cybercriminals, some are carried out against computers or devices directly to damage or disable them, while others use computers or networks to spread malware, illegal information, pictures or other material. Some cybercrimes do both, that is, they target computers to infect them with a computer virus, which then spreads to other machines and sometimes entire networks.

One of the main effects of cybercrime is financial; Cybercrime can include many types of criminal activity for profit, including ransomware attacks, email and internet fraud, and identity fraud, as well as attempted theft of financial accounts, theft of credit cards, or other card information. of payment. Cybercriminals can also target an individual's private information as well as corporate data for theft and resale. With many workers moving into remote work routines due to the pandemic, cybercrime is expected to increase in frequency in 2021, making backup data protection particularly important.

III. REASONS FOR CYBER CRIME

1. Lack of security assistance

Very few people know the simplest steps to increase cybersecurity. Furthermore, most do not have easy access to the resources they need, when they need them. Take the passwords. It is known that the stronger your password, the more secure your account will be.

In 2019, 23 million online accounts still used the password "123456". 71 of the accounts are protected by passwords used on various websites. Our password habits must change.

The best time to inform people about the strength of their passwords is when they create accounts. Simple information like" how long it will take to break the password" or" if a known data breach has already occurred" can significantly improve the strength of passwords at the setup stage.

2. System vulnerabilities When cybercriminals spot a weakness, they pounce on it. This is why system vulnerabilities can be so dangerous.

In January 2020, American software developer SolarWinds was the target of a cyber-attack. Cybercriminals exploited a

vulnerability in company software after employees shared details of the system failure online. The attackers managed to steal the administrative credentials of an account holder.

Minimizing the threat of such attacks requires a combined reactive and preventive approach. In addition to having the proper security software and the proper network settings, it is important to keep your software up to date. This means installing software updates and patches as soon as they are available, as they can fix vulnerabilities.

3. Assess the risk Criminals want us to underestimate the risk of cyberattacks. The more we underestimate, the easier it becomes for them. Unfortunately, everyone's ability to calculate risk is low!

Take the example of car accidents and plane crashes. Statistically, flying is much safer than driving. However, up to 1 in 6 people are afraid of flying, while few people worry about driving their cars every day.

Quirks like the ones above make it difficult for humans to calculate risk. What we call the normality bias makes us think that the future will be like the present. In other words, we cannot calculate the risk of a cyber-attack, so we conclude that such a risk probably does not exist. But the risk of a cyber-attack is very real. In fact, it is a risk that increases every day. To reverse this trend, we must start protecting ourselves online. Ordinary people need to know the risks, as well as the basic preventive measures they can take to stay safe.

IV. TYPES OF CYBER CRIME

1.Hacking
2.Virus dissemination
3.Logic bombs
4.Email bombing and spamming
5.Web jacking
6.Software Piracy

A. 1. Hacking

Simply put, hacking is an act committed by an intruder by gaining access to the computer system without authorization. Hackers are basically computer programmers, who have advanced knowledge of computers and generally misuse that knowledge for devious reasons. They are usually tech enthusiasts who have expert-level skills in a particular software or language. As for the reasons, there could be several, but the most common are quite simple and can be explained by some human tendency such as greed, fame, power, etc. Some people do this just to show their expertise, ranging from relatively harmless activities like modifying software to perform tasks that are beyond the creator's intention, others simply want to cause destruction.

B. Virus dissemination

Viruses are computer programs that attach to or infect a system or files and tend to travel to other computers on a

network. They interrupt the operation of the computer and affect the stored data, either by modifying it or deleting it completely. Unlike viruses," worms" do not need a host to cling to. They simply replicate themselves until they consume all available memory on the system. The term" worm" is sometimes used to refer to self-replicating" malware." These terms are often used interchangeably in the context of hybrid virus / worms that dominate the current virus scenario." Trojans" differ from viruses in the way they spread. They masquerade as a legitimate file, such as an email attachment from a so-called friend with a very credible name, and they do not spread. The user may also unknowingly install a program infected with a Trojan horse through unwanted downloads while visiting a website, playing online games, or using Internet applications. A Trojan horse can cause damage similar to other viruses, such as stealing information or hampering / disrupting the functioning of computer systems.

C. Logic bombs

A logic bomb, also known as" slag code," is a piece of malicious code that is intentionally inserted into software to perform a malicious task when triggered by a specific event. It is not a virus, although it generally behaves the same. It is stealthily inserted into the program where it remains inactive until specified conditions are met. Malware, like viruses and worms, often contains logic bombs that fire at a specific payload or at a predefined time. The user of the software is unaware of the payload of a logic bomb and the task it performs is undesirable. Program codes that are programmed to run at any given time are called" time bombs." For example, the infamous" Friday the 13th" virus, which only attacked host systems on specific dates; It" exploded" every Friday of the thirteenth of the month, causing the system to slow down.

D. Email bombing and spamming

Email bombardment is characterized by the sending of large volumes of emails to a destination address by an attacker, resulting in the blocking of the victim's email account or mail servers. The message is meaningless and is too long to consume network resources. Pointing multiple accounts on a mail server can have a denial of service impact. Spam filters can easily detect these frequently arriving messages in your inbox. Email bombing is typically done by botnets (private computers

connected to the Internet whose security has been compromised by malware and under the control of the attacker) as a DDoS attack

E. Web jacking

Web hijacking takes its name from ”hacking”. Here, the hacker takes control of a website fraudulently. It can modify the content of the original site or even redirect the user to another similar fake page controlled by him. The website owner no longer has any control and the attacker can use the website for his own selfish interests. There have been reports that the attacker demanded a ransom and even posted obscene material on the site.

F. Software Piracy

Thanks to the internet and torrents, you can find almost any movie, software, or song from any source for free. Internet piracy is an integral part of our lives that we all contribute to, consciously or not. In this way, the profits of the resource developers are reduced. It’s not just about using someone else’s intellectual property illegally, but also passing it on to your friends, further reducing the income they deserve.

V. CASE STUDY

A. Phishing scam targets Lloyds Bank customers:

Lloyds Bank customers are being targeted by a phishing scam that is currently affecting email and text message inboxes. The legal department alerted people after 100 people received the messages. The email, which looks like an official message from Lloyds Bank, alerts customers that their bank account has been compromised. It says: “Your bank account has been deactivated, due to recent activity on your account, we have placed a temporary hold until [sic] verifies your account. Every time someone tries to verify, they are scammed by phishing.

B. Coronavirus now possibly largest-ever cyber securitythreat:

Based on the covid-19 concept, phishing scams by cyber attackers have increased a lot. The attacker is sending emails, messages or links to people about coronavirus awareness, but unfortunately people are falling for this phishing scam. The total volume of phishing emails and other security threats linked to the Covid-19 coronavirus now represents the largest amalgam of cyberattack types around a single topic that has been seen for a long time, and possibly never, according to Sherrod De Grippe. , senior director. investigation and detection of threats in Proofpoint. To date, Proofpoint has observed attacks ranging from spoofing, malicious attachments and links, compromised work emails, fake landing pages, downloaders, spam, and strains of malware and ransomware, all related to the rapid spread of the coronavirus. . “For more than five weeks, our threat investigation team has

C. Cyber gangsters demand payment from Travelex after Sodi-nokibi attack:

The computer files of the Travelex company have been compromised by one of the most sophisticated ransomware attacks known as Sodinokibi, which shuts down its computer systems on New Year’s Eve. This happens when many of your belongings were on vacation. Foreign exchange firm Travelex is faced with requests for payment to decrypt critical computer files. The attackers demanded a 6-digit amount to provide decryption tools that will allow you to recover the contents of files on your computer network that have been encrypted by the virus.

D. List of Blackbaud breach victims tops 120:

The UK National Trust has joined a growing list of educational and charities where the data of their former students or donors has been put at risk in a ransomware incident that occurred at the US cloud software provider. Blackbaud. According to the BBC, the Trust, which manages hundreds of important and historic sites across the country, including natural landscapes and monuments, parks, gardens and stately homes, said data on its volunteers and fundraisers had been put at risk, but the data on its 5.6 million members was safe. The organization investigates and informs those who may be affected. In accordance with UK data protection regulations, he also reported the incident to the Information Commissioner’s office, which now handles a large volume of reports, including from Blackbaud

E. Cyber gangsters hit UK medical firm poised for workoncoronavirus with Maze ransomware attack:

Cyber gangsters have attacked the computer systems of a medical research company that is currently working on a possible future vaccine against COVID-19. The Maze ransomware group attacked the computer systems of Hammersmith Medicines Research and was able to reveal the personal details of many former patients after the company refused to pay what the attacker requested. The company, which has conducted trials to develop the Ebola vaccine and drugs to treat Alzheimer’s disease, is conducting the first clinical trials of drugs and vaccines. This tragedy is shameful and damages our morals and ethics. This incident is so unethical and the attackers should be ashamed of what they did.

F. Travelex hackers shut down German car parts companyGe-nia in massive cyber-attack:

The criminal group responsible for the cyberattack which has been disrupting major banks and the Travelex exchange chain for more than three weeks has launched what has been called a" massive cyber-attack". The parts group, which employs 4,300 people in seven countries, said today the attack would have far-reaching consequences for the company, which has been forced to shut down its IT systems and fire staff home. him. The century-old company, which is headquartered in Attendorn, said in a statement on its website that it would take weeks or months before its systems were fully operational.

G. Cosmetics company Avon offline after cyber attack

The cosmetics company Avon remains offline for more than a week after a ransomware attack on its computer systems. The attack affected the back-end systems used by its famous sales representatives in several countries other than the UK, including Poland and Romania, which are now back online. After that, people could no longer order from the company. Avon disclosed the breach in a notification and sharing commission on June 9, 2020, alleging that it suffered a" cyber incident" in its IT environment that disrupted systems and affected operations.

VI. RESULT

A. Alert

- Ransomware and Malware is the most powerful attack in this time
- Every person and organization must be alert for this type of attack.
- Never save the password on device

B. Protected

- If we use firewall we can protect our data 56
- Using Multi vector for DDOs attack
- Use real time protection "ON" in the device
- Use Encryption System for transfer data or save Data

VII. CONCLUSION

- Cybercrime is not limited to countries; an attempt could be conducted from any part of the world. It is fearful to see cyber wars as the easiest way to carry out sabotaging rather than wars such as cold war. it's a cold war which any hacker can do by using any device and its impact is more effective than chemical and biological wars, terrorist wars or jihadist attacks. Law enforcement agencies around the world are working together to stop this activity in order to ensure safety and

VIII. FUTURE WORK

- Ransomware protection
- Malware protection
- How to make a fireball system for protect to PC

IX. REFERENCE

- Dr. K. Kiran Kumar HOD, Department of Computer Science Engineering Chalapathi Institute of Engineering Technology Guntur, Andhra Pradesh, India
- The Rise in Cybercrime and the Dynamics of Exploiting the Human Vulnerability Factor Dr. Nabie Y. Conteha *, Malcolm D. Royer b a Department of Computer Information Systems, College of Business Public Administration Southern University at New Orleans, 6801 Press Drive, Suite 108, New Orleans, Louisiana 70126, USA Department of Cyber Security and Information Assurance, Graduate School of MGT and Technology University of Maryland University College Adelphi, Maryland, USA a Email: nconteh@suno.edu b Email: malcolm.d.royer@gmail.com
- Harman deep Singh Brar, Gulshan Kumar," Cybercrimes: A Proposed Taxonomy and Challenges", Journal of Computer Networks and Communications, vol. 2018, Article ID 1798659, 11 pages, 2018. https://doi.org/10.1155/2018/1798659
- Term Paper on The Nature of Cyber Crime and Cyber Threats: A Criminological Review Ashraful Mozid 1 Nelufer Yesmen 2 1Department of Criminology and Police Science, Mawlana Bhashani Science and Technology University, Santosh, Tangail -1902, Bangladesh