Cyber Crimes: What an Engineer Can Do…?

Md Saiful Isalm ***Joyshree Sarkar***

Sreeja Dey ***Supti Saha***

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 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.

1. Hacking

In simple words, hacking is an act committed by an intruder by accessing computer system without permission. Hackers are basically computer programmers, who have an advanced understanding of computers and commonly misuse this knowledge for devious reasons. They're usually technology buffs who have expert-level skills in one particular software program or language. As for motives, there could be several, but the most common are pretty simple and can be explained by a human tendency such as greed, fame, power, etc. Some people do it purely to show-off their expertise – ranging from relatively harmless activities such as modifying software to carry out tasks that are outside the creator's intent, others just want to cause destruction.

2. Virus dissemination

Viruses are computer programs that attach themselves to or infect a system or files, and have a tendency to circulate to other computers on a network. They disrupt the computer operation and affect the data stored – either by modifying it or by deleting it altogether. "Worms" unlike viruses don't need a host to cling on to. They merely replicate until they eat up all available memory in the system. The term "worm" is sometimes used to mean self-replicating "malware". These terms are often used interchangeably in the context of the hybrid viruses/worms that dominate the current virus scenario. "Trojan horses" are different from viruses in their manner of propagation. They masquerade as a legitimate file, such as an email attachment from a supposed friend with a

very believable name, and don't disseminate themselves. The user can also unknowingly install a Trojan-infected program via drive-by downloads when visiting a website, playing online games or using internet-driven applications. A Trojan horse can cause damage similar to other viruses, such as steal information or hamper/disrupt the functioning of computer systems.

3. Logic bombs

A logic bomb, also known as "slag code", is a malicious piece of code which is intentionally inserted into software to execute a malicious task when triggered by a specific event. It's not a virus, although it usually behaves in a similar manner. It is stealthily inserted into the program where it lies dormant until specified conditions are met. Malicious software such as viruses and worms often contain logic bombs which are triggered at a specific payload or at a predefined time. The payload of a logic bomb is unknown to the user of the software, and the task that it executes unwanted. Program codes that are scheduled to execute at a particular time are known as "time-bombs". For example, the infamous "Friday the 13th" virus which attacked the host systems only on specific dates; it "exploded" every Friday that happened to be the thirteenth of a month, thus causing system slowdowns.

4. Email bombing and spamming

Email bombing is characterized by an abuser sending huge volumes of email to a target address resulting in victim's email account or mail servers crashing. The message is meaningless and excessively long in order to consume network resources. If multiple accounts of a mail server are targeted, it may have a denial-of-service impact. Such mail arriving frequently in your inbox can be easily detected by spam filters. Email bombing is commonly carried out using botnets (private internet connected computers whose security has been compromised by malware and under the attacker's control) as a DDoS attack.

5. Web jacking

Web jacking derives its name from "hijacking". Here, the hacker takes control of a web site fraudulently. He may change the content of the original site or even redirect the user to another fake similar looking page controlled by him. The owner of the web site has no more control and the attacker may use the web site for his own selfish interests. Cases have been reported where the attacker has asked for ransom, and even posted obscene material on the site.

6. Software Piracy

Thanks to the internet and torrents, you can find almost any movie, software or song from any origin for free. Internet piracy is an integral part of our lives which knowingly or unknowingly we all contribute to. This way, the profits of the resource developers are being cut down. It's not just about using someone else's intellectual property illegally but also passing it on to your friends further reducing the revenue they deserve.

Case Study of 2020

1. Cyber gangsters demand payment from Travelex after Sodinokibi attack:

Foreign exchange company Travelex is facing demands for payment to decrypt critical computer files after it was hit by one of the most sophisticated ransomware attacks, known as Sodinokibi, which disabled its IT systems on New Year's Eve. The company, which has operations in 70 countries, has faced days of disruption after criminal hackers penetrated its computer networks and delivered a devastating attack timed to hit the company when many of its staff were on holiday. According to security specialists, criminals are demanding a six-figure sum to supply Travelex with decryption tools that will allow it to recover the contents of files across its computer network that have been encrypted by the virus.

2. List of Blackbaud breach victims tops 120

The UK's National Trust has joined a growing list of education and charity organizations 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 organization is investigating 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 Blackbaud's.

3. 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 until [sic] you verify your account.”

4. 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 De Grippe, 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 De Grippe.

5. Cyber gangsters hit UK medical firm poised for work on coronavirus with Maze ransomware 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 ransomware 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.

6. Cosmetics company Avon offline after cyber attack

Parts of the UK website of Brazilian-owned cosmetics and beauty company Avon remain offline more than a week after an alleged ransomware attack on its IT systems. The attack is understood to have impacted the back-end systems used by its famous sales representatives in multiple countries besides the UK, including Poland and Romania, which are now back online. This has left people unable to place orders with the company. Avon disclosed the breach in a notification to the US Securities and Exchange Commission on 9 June 2020, saying it had suffered a “cyber incident” in its IT environment that had interrupted systems and affected operations.

7. Travelex hackers shut down German car parts company Genia in massive cyber-attack

The criminal group responsible for the cyber-attack that has disrupted high-street banks and the foreign currency exchange chain Travelex for more than three weeks has launched what has been described as a “massive cyber-attack” on a German automotive parts supplier. Parts

manufacturer Gedia Automotive Group, which employs 4,300 people in seven countries, said today that the attack will have far-reaching consequences for the company, which has been forced to shut down its IT systems and send staff home. The 100-year-old company, which has its headquarters in Attendorn, said in a statement posted on its website that it would take weeks or months before its systems were fully up and running.

8. Carnival cruise lines hit by ransomware; customer data stolen

Cruise ship operator Carnival Corporation has reported that it has fallen victim to an unspecified ransomware attack which has accessed and encrypted a portion of one of its brand's IT systems – and the personal data of both its customers and staff may be at risk. Carnival, which like the rest of the travel industry has been stricken by the Covid-19 pandemic – it also operates Princess Cruises, owner of the ill-fated Diamond Princess, which found itself at the Centre of the initial outbreak – reported the incident to the US Securities and Exchange Commission on 17 August. In its form 8-K filing, the company said the cyber criminals who accessed its systems also downloaded a number of its data files, which suggests it may be at imminent risk of a double extortion attack of the sort perpetrated by the Maze and ReVIL/Sodinokibi groups.

9. Law firm hackers threaten to release dirt on Trump

The cyber-criminal gang behind the ReVIL or Sodinokibi ransomware attack on New York celebrity law firm Grubman, Shire, Meiselas and Sacks (GSMS) have doubled their ransom demand to $42m and threatened to publish compromising information on US president Donald Trump, according to reports. In a statement seen by entertainment news website Page Six, the Sodinokibi group – which has also gone by the name Gold Southfield – said they had found "a ton of dirty laundry" on Trump. The threat reportedly reads: "Mr Trump, if you want to stay president, poke a sharp stick at the guys [GSMS], otherwise you may forget this ambition forever. And to you voters, we can let you know that after such a publication, you certainly don't want to see him as president. The deadline is one week."

10. IT services company Cognizant warns customers after Maze ransomware 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.