CYBERCRIME

Introduction

There are lots of cybercrime activities that take place on the dark net. It has offered a breeding ground for many cybercriminals, and the results of these are slowly being witnessed. Cyberattacks are increasingly becoming more effective and also more challenging for authorities to trace where data and money stolen by cybercriminals disappear to. This is because of the structuring of the underground economy on dark nets. There are different types of actors in an attack, and each of these has been specializing and advancing their techniques. The actors responsible for creating exploits and malware have become better at it. Those that deal with money muling have also become quicker and better at ensuring that the proceeds from attacks are less traceable. When the efforts from the different actors that form a cyberattack today are combined, the end result is an advanced attack that is difficult to stop and equally challenging to investigate. This chapter will mainly focus on familiarizing you with the categories of cybercrimes, the cybercrime activities that take place on the dark net, and the new value chains that have made cyber attackers to be more effective. It will cover this in the following topics:

- Cybercrime and its categories
- Cybercriminal activities through the dark net
- Data exfiltration
- Monetization of cybercrime
- Malware-as-a-service and money laundering.

Cybercrime and Its Categories

The commonly used definition of cybercrime is a crime that involves the use of a computer and/or a network for illegal reasons. These could include fraud, identity theft, or copyright violation among other reasons. Cybercrime has been happening on the surface net for a long time. However, the increasing popularity of the dark net has given cybercriminals a more secure space that they can operate

from. The main challenge that cybercriminals seek to avoid is trails of their criminal activi-ties leading back to them. This is because if they are traced, they can be arrested and face criminal charges and probably serve long sentences. The dark net provides an almost ideal platform for cybercriminals to carry out their activities. There are several categories of cybercrimes, and these are as listed below.

Computer Fraud

This involves the misrepresentation of facts to cause someone to do or to refrain from doing something, thus leading to a loss. It is a popular type of cybercrime and has seen many people and organizations fall victim. Computer fraud involves the falsification of data through either entry of falsified data or the entry of unau-thorized instructions. It may also involve the alteration, destruction, suppres-sion, or theft of online transactions. Lastly, it may also involve the manipulation or deletion of stored data. There has been an increase in these types of illegal activities which have translated to millions of dollars lost annually. The follow-ing are the most reported computer fraud incidents by both individuals and organizations.

Business Email Compromise

This is a high-profile scam that is generally targeted at businesses. The scam is ideal when the business has partners in foreign countries to whom funds are regularly electronically sent. The scam begins with the compromise of a business email account of a high-ranking organizational employee. When the email has been compromised and is in the hands of the attackers, they will study the type of communication that the executive employee handles. In most cases, they will send an email to the accounts or finance department requesting the next payments for certain companies to be paid through new overseas bank accounts. With this instruction, hackers can create a cash cow where employees will periodically send huge amounts of money as payments to their foreign suppliers or business partners while the amounts go to hackers (Figure 5.1).

An example of such an attack was on a company called Ubiquiti Networks. Hackers created a spoofed email account of a high-ranking staff member and instructed the accountants to be sending payments to suppliers through new over-seas bank accounts. By the time that the scam was realized, the company had lost

close to $44 million. It is, therefore, an elaborate scam that is currently in use by hackers and has been proven to be effective (Figure 5.2).

Data Breach

This is another common type of computer fraud. It is where data is leaked or spilled from a purportedly secure storage. Sensitive information ends up in the hands of hackers who either release it publically or use it as ransom to get paid a certain amount. One of the biggest data breaches for a renowned company is that of the email provider company called Yahoo. Yahoo has repeatedly been a victim of data breach where it is reported that hackers have had access to sensi-tive information about millions of Yahoo's users. Surprisingly, the attack has not occurred once to the company hinting that the hackers may be working closely with an insider or have been on Yahoo's systems for a significant period of time. Another significantly big hack was that of Republican National Committee's (RNC) voter data in the United States. RNC was compromised and the data of over 200 million Americans breached by the attackers. This was as a result of data being stored insecurely on Amazon S3 bucket. Uber has also been a victim of a data breach though the managers handled the incident quite loosely. It is reported that a hacker was able to breach the company and steal data of 57 million users. Some executives paid the hacker a significant amount of money to silence the hacker. In the end, this attempt to conceal the hacker rather than to deal with it came into the limelight and some executive employees were fired. The US White House has already banned the use of Kaspersky products on government comput-ers after the popular antivirus maker was caught up within the traps of computer fraud. Kaspersky has been reported to have been hacked by Russian hackers to help them pull out data from a laptop owned by a contractor to the NSA that was using the antivirus. In this specialized attack, the hackers are said to have used the program's ability to access any file on a computer's hard drive to steal. This attacker showed the extent to which insecurity had gone to if an antivirus program could be used for data breaches. Another data breach that involved an unlikely perpetrator was that reported by WikiLeaks. According to the popular expose network, the US CIA had a database of exploits that it could use to track

From all these attacks, it can be noted that there has been an increase in sophis-tication and effectiveness. One would think that big companies such as Yahoo

would be invincible by attackers since they must have state-of-the-art security systems guarding their networks. However, it has been proven by hackers that data breaches can affect anyone and there are very many ways for them to conduct the breaches. This makes data breaches one of the most feared types of cybercrime and can affect just about anyone.

Denial of Service

Denial-of-service (DoS) attacks are considered part of computer fraud since they are done to purposefully suppress or prevent normal processes or transactions, thereby leading to losses. DoS attacks involve the interruption of access to systems or networks due to an overwhelming amount of illegitimate requests being sent to servers. This type of an attack has become one of the most feared by organiza-tions since it comes unannounced and is hard to stop once it has started. The main culprits behind the attack are botnets which have recruited thousands of devices that send huge amounts of requests to organizational servers. In 2016, an unlikely victim of distributed denial of service (DDoS) was a domain name resolving com-pany called Dyn. The attack was executed by a botnet of 100,000 devices that continuously sent requests to the company at an estimated rate of 1 Tbps. The attack was a bold one since it was targeted at a company that directly influences internet performance since it is responsible for translating domain names into IP addresses (Figure 5.4).

With the attack on Dyn, several websites could not be accessed since their names were not able to be resolved. The attack served as a wakeup call to all other companies that had looked down upon the capabilities of determined attackers. Another DDoS attacker was against an investigative reporter called Brian Krebs whose website was taken down by a massive attack that peaked at 620 Gbps effectively putting the site offline. The significance of this attack was the sheer amount of force that was used against the investigative reporter. The attack was attributed to a Mirai botnet which had scanned devices connected to the web and infected thousands of them with malware to force them to participate in DDoS attacks. Lastly, for 2016 attacks, there was a wave of DDoS attacks against Russian banks whereby a botnet of approximately 24,000 computers was reported to be behind the attack. The attacks were targeted at five banks, and the attacks lasted over 2 days. However, it is reported that the attacking botnet was not able to take the websites offline. In 2017, there was a reported 915 increase in DDoS

attacks. This was due to the increased adoption of Internet of Things (IoT) devices. IoT devices have been plagued with insufficient security, thus making them ideal targets for hackers wishing to get very many devices to recruit to their botnets. The attack on many organizations has been in an effort to either take them offline or to distract the organizations while a data breach takes place (Figure 5.5).

Email Account Compromise

This is quite similar to the discussed business email compromise. However, this type of an attack is not constrained to businesses only. It can be targeted at the gen-eral public and even to people that least expect to be targeted. Compromised email accounts belonging to professionals are used and the aim is to manipulate other people into sending money or sensitive information to the attackers. Individuals working in financial institutions, real estate, and law brokerage firms are likely targets by the attackers for the purpose of obtaining the email accounts. The attack-ers will pretend to be the professionals and continue on to engage with clients and request for payments or some favors. The accounts are compromised through pass-word guessing or through social engineering techniques. The hacker can use the compromised email to target clients, friends, and relatives or perform transactions under the pretense of being the real owners of the account.

Malware

The malware was exhaustively covered in Chapter 4 where it was said to be mali-cious software that is broadly categorized into three classes: viruses, worms, and Trojans. These programs are created to alter, manipulate, or destroy systems and data. Some types of malware, especially the ones that are considered to be exploits, are used to open an avenue for attacks. Malware has increasingly been used at the core of most cybercrime activities. Malware can easily be installed onto unsecured

• In Q3 2017, organizations experienced an average of 237 DDoS attack attempts per month, equal to eight per day. -Corero Network Security, 2017

• In Q3 2017, monthly DDoS attack attempts increased 35% over Q2, and 91% over Q1. -Corero Network Security, 2017

• The growing availability in DDoS-for-hire services and the proliferation of unsecured Internet of Things (IoT) devices has led to the increase in DDoS attacks in 2017. -Corero Network Security, 2017

devices and then be used to commit other crimes such as data theft. There are malware that automatically download onto a device once the user visits a certain page. It is difficult for the user to tell when his or her device has been infected without an antivirus program. Malware can not only steal data but can maintain an open communication channel between the hackers and the victim machine. The hackers can monitor everything that a user does for a long period before executing their attacks. In the previous chapter, there was a highlight on the new value chains of the underground malware economy. There was a particular value chain whereby when attackers were targeting businesses and financial institutions, they would compromise the machines and keep monitoring the infected devices for long. Once they were familiar with the systems that the targets were using, they would proceed to execute the last bit of the attack. This is the bit where they would use the systems on the infected devices to do either authorize transactions to their accounts or to create transactions to transfer money to their accounts.

Phishing

This is a form of computer fraud that involves the use of emails to manipulate people into sending money or sensitive information to cybercriminals. The normal phishing attack is hardly targeted at specific people since the same phishing email is sent to multiple recipients. The most common pattern of such attack is the claim by the sender to be from a legitimate company, and certain information or creden-tials are required from the recipient. Another variation of phishing attacks is where the recipients are deceived of having won lotteries or some competitions and they are required to give some information or part with a certain amount to claim their prize. A more advanced form of phishing is spear phishing which is quite different from normal phishing by the fact that the email is highly customized according to the recipient. The attacker will have some foreknowledge about the recipient and thus will know exactly where to target them. For instance, an attacker could create an email resembling that of the HR of a company and then use the email to manip-ulate the target into giving out their tax information or their sensitive information. It will not appear as inappropriate for the HR to request some personal information and so the target will most likely send it over. Phishing has been advancing with time and has incorporated

technology into it. Whereas traditional phishing emails featured grammatical errors, spelling mistakes, and obviously faked emails, a new set of attackers has come up. These attackers create high-quality emails. There are tools that can clone websites, and all the attacker has to do is to play around with the domain name they will use to host the fake website. The attacker can then send a phishing email to the target informing them that there is a problem with their account with a certain company and they need to log in to solve the problem by clicking on a provided link. Upon clicking the link, the target will be directed to the clone website and will be prompted to log in using a similar interface as is on the legitimate website. When the target logs into the account, the credentials are sent to the attackers and the target will be taken round in circles being told to provide more personal information to authenticate himself or herself into the account (Figure 5.6).

Phishing has been a very effective attack of late with attackers duping many people with the new techniques that they are using. There have been PayPal phish-ing attacks where users are told that their PayPal accounts have a problem that needs to be resolved and thus they are required to immediately log in to through a provided link. The link would go to a cloned site, provide the targets with the normal PayPal login page and then they would enter their credentials. After doing so and submitting the information, the cloned website would take the user through a series of steps where they would continually be requested to give out a bit more of personal information. At the end of the attack, the target would have given out so much information such that they would be at the mercy of the attackers. PayPal acknowledged the attack and sent emails to all its users on how to prevent them-selves from falling victim. Another successful wave of phishing attacks took place in the 2017 tax-filing season for US citizens. Hackers used the opportunity where people were in a rush to complete filing their taxes to defraud them. They would create emails purported to be from the Internal Revenue Service (IRS) requiring the recipients to either send out information or to send out some monies. The ring of phishers was, later on, tracked to India and the mastermind arrested. This was after Americans had lost millions of dollars to them. The same attack can be rep-licated just about anywhere else in the world using the same techniques and tech-nologies that the attackers used.

The effectiveness of phishing attacks has definitely been noted by hackers. They are therefore capitalizing on this technique of reaching a large number of people but using minimal resources. There have been many other attacks just as effective as the two described above. In Qatar, it was estimated that 1 of each 25 citizens had been hit by over 93,000 phishing attempts in just 3 months of 2017. In Czech, there was a fake campaign purporting to be by the country's postal service. The fake campaign urged people to download an app for their postal services. However, they were downloading a malicious app that turned out to steal their banking informa-tion. In the same year, companies in over 50 countries were fooled into download-ing a pdf file on energy solutions. The pdf file had a malware injected into it and would infect any device that it was opened in. Amazon has seen the same fate as PayPal after hackers sent phishing emails claiming that there were some items on discount on the e-commerce site. When they clicked on items in the email, they would proceed to log into a clone site, but when they clicked on the discounted products, they would be told that the items were no longer available. However, the information that they would have already given the hackers would be used to attack them in future. There were very many other phishing attempts sent to organiza-tional employees. From a security survey done to a sample of organizations world-wide, it was estimated that 75% of all organizations had received phishing emails in 2017. This estimate shows that phishing is making a great come back and they were increasingly becoming successful. Moreover, the survey showed that the impacts of phishing were malware infections, compromised accounts, and data loss.