Cybercriminal Mindset

Tariq I Musaji

30th July 2023

Introduction

Cybercrime is any criminal activity in the cyberspace that targets a computer, individual, or network for either disruptive purposes or for financial gain. These nefarious activities include identity theft, phishing, and ransomware attacks among others. The digital world is rapidly growing, and so are the numbers of cybercriminals present in it. Technological advancement has led to the advancement of the techniques and of the equipment that is used for malicious ends. According to Hashim & Medani (2021), nearly 30,000 websites are hacked each day. Yet, 1 in 10 businesses in America are not insured against cyber-attacks. In 2021, 50% of internet users in America had their online accounts breached. In 2022, 39% of organizations in the UK reported facing a cyber-attack. While, in America 53.35 million people were affected by cybercrime in the first half of 2022. To handle this problem effectively, one must understand the mindset of cyber criminals. Hence, the primary purpose of this discussion is to reveal the mindset of these hackers; the different categories of hackers; thinking; persona and personality traits. What is the impact of hacking on society and how may AI help aid the malicious activities of cyber criminals?

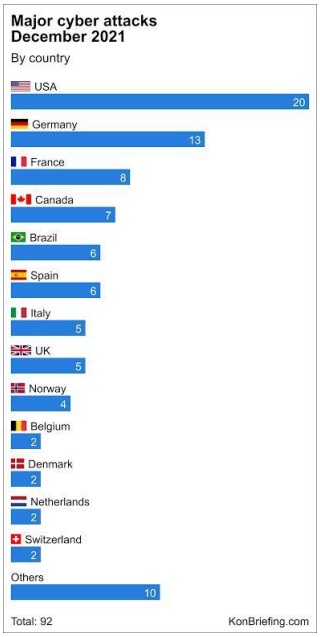
What motivates hackers?

There are a variety of factors that motivate cybercriminals. These include personal satisfaction, financial gain, and even ideological or political objectives. But the most significant motivator is financial gain (Hashim & Medani, 2021). According to Mansfield -Devine (2018), businesses with valuable data are the top targets of hackers. The more expensive the data, the

higher the chance of becoming a target. This is also true for companies who have a large quantity of assets or money that can be stolen, such as bank account information or credit card numbers. Victims of cybercrimes may face guilt, worry, and anger following their experience. Velu & Beggs (2019) advise that victims of cybercrime must carry out security precautions, discuss their experience with their loved ones, and book an appointment with a mental health professional to help deal with their emotional distress.

What do hackers think?

It is also important to understand the mindset of hackers. According to Velu & Beggs (2019), hackers are frequently driven by an urge to prove their mastery and to test the limits of networks and systems. They are frequently asking themselves: "how can I exploit this?", "how can



I break this?", "how can I change this according to my wish and cause utmost damage?". On the other hand, cybersecurity teams are constantly trying to provide protection. Petrov & Quinn (2017) state that having an employee with an adversarial mindset can be an effective critical thinking tool that may drastically enhance an organization's cyber security by pre-emptively identifying and removing vulnerabilities.

Facebook

It is predominately believed that a business, which has more employees, and more money would have more security. Facebook holds these in vast quantities, but its data breach history during the last decade shows that the company has yet to develop a safe platform that users may trust. Those thinking that 2021 would be smooth sailing year were disappointed by the massive Facebook hack on April 3rd. Facebook's lapse in 2021 caused an exposure of the personal details of nearly half a billion Facebook users including their names, phone numbers, birthdays, and locations. Facebook confirmed the security breach but said it occurred due to a security issue in 2019 that the company had already fixed. However, this justification was not satisfactory to many Facebook users. The information had been leaked, and the impact on the users would be ongoing with 30 million Facebook accounts hacked in America alone (Savor & Douglas, 2016). People cannot discern easily if their accounts were amongst those hacked, with every user having a 20% chance of being hacked if their account information was part of the stole data. Even though these breaches have affected users' privacy, the likelihood that individuals would want to stop using such a popular platform is rather small. Closing a Facebook account may not be preferable, but there are steps that one may take to secure personal accounts, even on platforms with imperfect security. The use of stronger system generated passwords generated on a user's phone may be one answer.

Yahoo

With 227.8 million users, it is safe to say that Yahoo is still a key player in the online world in 2023. According to Trautman & Ormerod (2016), Yahoo first revealed details about its security breach in September 2016 wherein 500 million Yahoo users' data was stolen by hackers back in late 2014. Eight million of these hacked accounts belonged to users in the UK. Yahoo knew about the intrusion but did not realize the extent of their security lapse. In July 2016, while inquiring into a different data breach, Yahoo revealed data of 200 million Yahoo customers' accounts were available for sale on a website on the darknet. The information broker appeared to be a hacker with the nickname 'Peace.' The same individual was believed to be responsible for the data previously stolen from LinkedIn and Myspace. In November 2016, Yahoo learned about its second breach. Law enforcement agents began sharing stolen information with Yahoo, which a hacker provided to these agents. Although the hackers did not see the entire data, only accessing a small sample. Yet, Yahoo only revealed its second cyber-attack after the third data breach, which occurred in February 2017 when hackers stole data from one billion users. This more recent attack was different from the first two.

NHS Cyberattacks 2017

One of the most famous ransomware attacks occurred in the spring of 2017. On Friday 12th May 2017 the NHS stood still for many days because of the 'WannaCry' outbreak. A cyber-attack that affected GPs, hospitals, and surgeries all over England and Scotland. Even though the NHS was not the only target, the worldwide cyber-attack highlighted NHS security weaknesses and led to the cancellation of many operations and appointments alongside the absurd relocation of many of those in emergency centers. NHS Staff had to use pen, paper, and their mobile devices as the primary systems of NHS including their telephones were affected. The 'WannaCry' outbreak affected more than 200,000 computers in more than 150 countries (Martin & Martin, 2017).

The ransomware used in the attack is referred to as 'WannaCry'; it was primarily carried out via emails which prompted the user into releasing malware when they opened attachments on their systems in a technique known as phishing. Once a computer has been affected by a cyberattack, its files become encrypted and computer tasks are closed so that no one can access those files anymore. Finally, the attacker asks for payment so that the computer-user can regain access to their computer, usually in either crypto-currency or Bitcoins. The NHS was not prepared for a national cyber-attack, and so was uncertain as to who would lead the response. The issue the NHS faced was that communications like emails were either removed or infected meaning that it was difficult to control the spreading of the ransomware.

Categories of Hackers

Rawal & Manogaran (2022) state that hackers often exploit vulnerabilities to achieve unauthorized access to computers and networks, yet systems hacking is not always illegal or for malicious purposes. Hacking involves applying information technology skills to solve a specific problem. There are different types of hackers, and some hacking activities are helpful as they reveal programming deficiencies which enables developers to improve software quality. According to Rawal & Manogaran (2022), there are three general categories of hackers: black hat, white hat, and grey hat. Black hat hackers are those that illegally access computer systems with malicious objectives. When a black hat hacker sees a security vulnerability, they try to exploit it frequently by installing dangerous malware such by implanting a virus like a Trojan horse. These hackers are often responsible for ransomware attacks designed to breach data systems or to extort financial gains. **However, white hat hackers are ethically** safe hackers who identify and fix the vulnerabilities in security systems. They hack computer systems with an organization's permission

to reveal system weaknesses. This allows an organization to fix and heighten the overall security of their computer systems. Many cybersecurity professionals began their career as black hat hackers. However, the significant role played by ethical hacking is still largely misunderstood, as one may see in a recent case of ethical hacking in Germany. Grey hat hackers fall in between the above two categories. They may not have malicious or criminal intent, but neither do they have the consent or prior knowledge of those whose computer systems they hack into. Nevertheless, when they reveal weaknesses (e.g., zero-day vulnerabilities), they tell the owner of the computer system rather than manipulating them. Nevertheless, grey hat hackers may ask for payment in exchange for providing all the information they discover.

Although nearly all hackers fall into one of the categories mentioned above, there are some more types and sub-types of hackers. Green hat hackers are "green" in that they lack the technical skills and experience of expert hackers; they depend mostly on social engineering techniques and phishing to break into security systems. Blue hat hackers are white hat hackers that a company hires to help enhance its security systems through penetration tests. Red hat hackers, who are also called vigilante hackers, are those that take aggressive actions to fight back against black hat hackers. They put maximum effort into stopping the evil guys and may even take matters into their hands. Red hat hackers carry out full-scale attacks on the servers of cyber-attackers and cyber-criminals to gain access to their resources with the intention of defeating them.

Traits and Personas of Hackers

The most apparent personality traits of hackers are their high-consuming curiosity, intelligence, and intellectual abstraction. Most hackers can retain and reference huge amounts of

complex detail. Hence, someone with the above traits, with even mild to moderate analytical intelligence, can become an effective hacker. It is largely believed that black hat hackers primarily intend to gain money, yet this is not true for all these hackers. More than the lust for money, black hat hackers love the challenge, in fact Collier & Clayton state that hackers find repetitive work to be the most boring part of hacking (2021). They get more happiness out of a successful hack than engaging in repetitive work for instance selling credit cards numbers for money. The satisfaction of a victorious hack keeps cybercriminals motivated to undertake the next challenge. The thrill of the quest to break the walls of cybersecurity protection is their utmost reward. Hacking involves complex techniques and a mathematical and methodical mind. Further, successful black hat hackers are also extremely creative, with the skill to think beyond boundaries.

Many activities of hackers are crimes. These include accessing a network without permission, robbery, and identity theft. This is not a harmless activity; individuals may consequently face a serious and relatively long-term prison sentence. Despite this, hackers are determined to experience the thrill, even if this means spending the rest of their lives in jail. According to research, whether hackers crack digital security with good or bad intentions, they demonstrate deceitful, manipulative, cynical, exploitative, and insensitive traits (Collier & Clayton, 2021).

What Lessons Have Been Learned as a Society?

Hackers have a very profound impact on society, with the younger generation showing a great interest in hacking. Although ethical hacking is not dangerous, it is still crucial to understand what ethical hackers do for the interest of society. These days the internet has made it easier to connect every computer to the whole world, which makes computers vulnerable to attacks from cybercriminals. Thus, students are now studying security courses to learn about hacking and its

applications. Those who learn such skills are employed in the highest-paying jobs later in life. However, students may get attracted to gaining control of other's computer systems through hacking. Therefore, it is important to teach students that hacking for unethical purposes is not good. Ethical hacking can have a positive impact on businesses in society. As we have seen, information and technology advancements have meant businesses' data tends to be stored on computer systems. This means that most companies now carry out their business transactions electronically. Therefore, students must learn ethical hacking to fulfill the demands of today's businesses and become competitive in the current job market.

In society, more and more people are using auctions and shopping websites to buy things. These e-commerce websites give away good rewards as well as discounts. Ethical hacking provides government organizations and businesses to identify and prevent problems caused by cyber-criminals primarily attempts made to steal significant data. Currently, cyber-attacks have become more serious and more frequent. Recent cyber-attacks, involving NotPetya malware and WannaCry ransomware, have taught society some important lessons about improving cyber-security defenses and about the importance of doing so.

Attacks involving WannaCry ransomware occurred in Blaster in 2003 and Sony in 2014. According to Shin & Son (2017), regular patching and the use of firewalls may prevent these attacks. WannaCry weaknesses were exposed nearly two months prior to the attack.

Many companies are full of IT professionals but are still vulnerable to cyber-attacks. According to Hamsley & Fisher (2018), the NotPetya cyber-attacks target organizations without the appropriate patch to fight the Microsoft vulnerability (SMB-1). According to McMahon & Williams (2017) companies may apply the Microsoft patch MS17-010 to prevent such a vulnerability. Even after the application of patches, no anti-virus software or firewall is flawless.

Therefore, saving important data in a different location beyond the network is advisable for instance: cloud storage; the use of remote servers and even USB sticks.

If a computer system is affected by a cyber-attack, it is important to immediately report the incident and take the proper action at once. According to Cong & Harvey (2023), firm participation and rapid incident reporting helped stop the WannaCry spread soon after the attacks began. Some governments have issued warnings for acts of ignorance where cyber-attacks have failed to be reported within three days.

Furthermore, paying ransom money gives no guarantee that all the files will be retrieved following a cyber-attack. The email service (Posteo) instantly stops an email used for Bitcoin receipt, which preventing it from being used in any further communication. Additionally, paying ransom money will likely motivate cybercriminals to keep attacking the systems instead of aiding the recovery of the files. Cyber-attacks are clear reminders to take preventative measures to protect computer systems and their data. It is getting more difficult to ignore cyber-related risks, as individuals continue to see attacks emerge and spread across the global network.

How to prepare for social engineering and malware attacks

Each year, social engineering attacks occur by using more and more complex techniques. Technology continues to develop, and its advancement in fields such as machine learning and Artificial Intelligence (AI), like deepfake technology, will further increase social engineering risks.

Social engineering involves the psychological strategies scammers use to motivate people to click on compromised links or divulge sensitive data. There are many forms of social engineering, including phone calls, emails, and text messaging. These attacks take undue advantage of users' helplessness, fears, and curiosity to trick them into sharing information such as social security

numbers, bank account details, or login credentials. In most cases, they redirect users to websites which result in drive-by unprotected downloads alongside phishing attacks.

The below strategies set the basis for securing computer networks from phishing. By making some extra efforts it is possible to further enhance enterprise cybersecurity. For example, one may use a password manager to enable users to generate and manage login credentials for each website while minimizing the effect of potential information breaches. By doing so, only one password will be compromised, and victims can instantly generate a new password. Another way is by enabling two-factor authentication, which serves as a first line of defense against cybercriminals trying to get access to credentials. Furthermore, it is also suggested to use privacy-centric search engines and browsers. One may also find it effective to research and use the security tools owned by smaller technology companies. Moreover, it is recommended that one uses encrypted email or messaging programs when sharing any sensitive information. If a user does experience a phishing attack, it is suggested to file a complaint with the Internet Crime Complaint Center of Federal Bureau of Investigation (FBI). Companies can also train their workforce by employing cybersecurity tactics such as instituting cyber education programs and simulated phishing attacks.

Role of AI in Cybercriminal Activity

Many technology professionals are enthusiastic about the potential of Artificial Intelligence. However, cybercriminals too are also ready to apply this new technology to assist them in their adversarial endeavors. AI is an incredible innovation, but it may also become cause for concern. According to Jaber & Fritsch (2021), cybercriminals may use Artificial Intelligence to write malware, with malware being the malicious programs hackers use to hack computer programs. Cybercriminals are often looking for ways to crack password and get access to private

data. A malicious actor may use different techniques to crack passwords with AI offering a new and fruitful way for these individuals to crack passwords.

Social Engineering is a cybercrime tactic that affects many victims every week. It has become an increasingly troublesome problem in every part of the world. Social engineering occurs through manipulation wherein victims are led to fulfilling the attacker's demands; often it occurs without the victim even realising what has happened. Hackers must find software vulnerabilities to hack software programs, with such software vulnerabilities frequently occurring because of bugs in the software's code. When a person fails to update a software program or if any bug goes unpatched, these vulnerabilities may pose a serious risk. AI can be used to analyze stolen data. Often malicious actors are ready to pay huge amounts, if data is valuable enough. Thus today, as data is increasingly being considered as a valuable asset, we see that it is being frequently sold on the dark web. This places individual’s data in an increasingly vulnerable position.

Data is usually stolen in small fragments, especially when the target of the attacker is an individual victim. Nevertheless, larger data breaches can lead to the theft of larger databases. At this stage, the hacker must evaluate what information in this database is more useful. AI can help in selecting which data holds the most value, by streamlining and cutting down the time it takes for a hacker to evaluate what data holds the maximum value. This is a key example of how AI is not only useful but also poses a potential threat. Like many other kinds of technology, A I have been, and will continue to be exploited by cybercriminals. With AI continuously updating its features, one must wait and see how cybercriminals will be able to use such technology for their attacks in the future. Yet, Artificial Intelligence, is in essence related to learning and may help us combat cybercrime, for instance one day it may become convenient to use an AI-powered tool to

secure valuable and sensitive data. Cybersecurity organizations must play their role to fight AI related threats.

References

Cong, L.W., Harvey, C.R., Racette, D. and Wu, Z.Y., 2023. *An anatomy of crypto-enabled cybercrimes* (No. w30834). National Bureau of Economic Research.

Hashim, A., Medani, R. and Attia, T.A., 2021, February. Defences against web application attacks and detecting phishing links using machine learning. In *2020 international conference on computer, control, electrical, and electronics engineering (ICCCEEE)* (pp. 1-6). IEEE.

Hemsley, K. and Fisher, R., 2018. A history of cyber incidents and threats involving industrial control systems. In *Critical Infrastructure Protection XII: 12th IFIP WG 11.10 International Conference, ICCIP 2018, Arlington, VA, USA, March 12-14, 2018, Revised Selected Papers 12* (pp. 215-242). Springer International Publishing.

Jaber, A.N. and Fritsch, L., 2021, November. COVID-19 and global increases in cybersecurity attacks: review of possible adverse artificial intelligence attacks. In *2021 25th International Computer Science and Engineering Conference (ICSEC)* (pp. 434-442). IEEE.

Mansfield-Devine, S., 2018. The best form of defence–the benefits of red teaming. *Computer Fraud & Security*, *2018*(10), pp.8-12.

McMahon, E., Williams, R., El, M., Samtani, S., Patton, M. and Chen, H., 2017, July. Assessing medical device vulnerabilities on the Internet of Things. In *2017 IEEE international conference on intelligence and security informatics (ISI)* (pp. 176-178). IEEE.

Petrov, V. and Quinn, R., 2017. *An Analysis of Sheila Fitzpatrick's Everyday Stalinism: Ordinary Life in Extraordinary Times: Soviet Russia in the 1930s*. Macat Library.

Rawal, B.S., Manogaran, G. and Peter, A., 2022. Hacking for Dummies. In *Cybersecurity and Identity Access Management* (pp. 47-62). Singapore: Springer Nature Singapore.

Savor, T., Douglas, M., Gentili, M., Williams, L., Beck, K. and Stumm, M., 2016, May. Continuous deployment at Facebook and OANDA. In *Proceedings of the 38th International Conference on software engineering companion* (pp. 21-30).

Shin, J., Son, H. and Heo, G., 2017. Cyber security risk evaluation of a nuclear I&C using BN and ET. *Nuclear Engineering and Technology*, *49*(3), pp.517-524.

Trautman, L.J. and Ormerod, P.C., 2016. Corporate directors' and officers' cybersecurity standard of care: The Yahoo data breach. *Am. UL Rev.*, *66*, p.1231.

Velu, V.K. and Beggs, R., 2019. *Mastering Kali Linux for Advanced Penetration Testing: Secure your network with Kali Linux 2019.1–the ultimate white hat hackers' toolkit*. Packt Publishing Ltd.