CO325

ASSIGNMENT 1

JAYATHUNGA W.W.K.
E/19/166

I.

Introduction

Protecting digital assets is fundamental to cybersecurity. These assets can include vital infrastructure data and private, sensitive information. Preventing unwanted access, modification, or destruction of these assets is the aim.[1]
Cyberattacks are a persistent concern in the digital world. Usually, one or more of the following goals are the focus of these attacks:[2]

I. ***gaining access to sensitive information:***
This could involve private information like credit card details, social security numbers, or trade secrets. Once obtained, this data may be sold on the black market, utilized for fraudulent purposes, or exploited to obtain an unfair advantage over competitors.

II. ***Information alteration:***
A cyberattacks objective may occasionally be to change data rather than steal it. This could entail altering financial documents, faking data to yield false conclusions, or vandalizing websites to disseminate propaganda or false information.

III. ***Information destruction:***
A few cyberattacks have the intent of erasing systems or data. This could include erasing important data, employing software exploits to physically harm devices, or utilizing Distributed Denial of Service (DDoS) assaults to interrupt services.

IV. ***Extortion of money:***
A ransomware attack is one type of hack that encrypts data and demands payment in exchange for the decryption key.

Cybersecurity uses a multifaceted strategy to defend against various threats:

I. ***Technology:***
   This refers to the instruments used to safeguard systems and networks, such as firewalls and antivirus programs.

II. ***Processes:***
   This includes developing and adhering to security-related protocols, such as routinely patching and updating software, backing up data, and keeping an eye on network activity.

III. ***People:***
   This entails educating users on how to spot and steer clear of possible dangers, such phishing emails.

To put it briefly, cybersecurity is an essential component of our digital life that entails people, technology, and procedures cooperating to safeguard our virtual environment.

<u>**The Importance of Cybersecurity**</u>[2]

In the current digital era, the significance of cybersecurity cannot be emphasized. The Internet of Things (IoT), cloud computing, and smart device proliferation have all significantly increased the potential surface area for cyberattacks.

- ***Smart Devices:***
  As our reliance on smartphones and other smart home appliances grows, they also present potential ports of entry for cyberattacks. These gadgets frequently have access to our home or workplace networks and hold sensitive information.

- ***Cloud Computing:***
  By offering scalable and adaptable resources via the internet, cloud computing has completely changed the way businesses run. But when information is handled and kept on distant computers, it opens the door for hackers to target it. One of the main concerns in cybersecurity is making sure cloud environments are secure.

- ***IoT:***
  The term "Internet of Things" (IoT) describes a network of actual physical objects, including cars, appliances, and other goods, that are implanted with sensors and software to allow them to communicate and share data via the internet. IoT has a lot of advantages, but it also greatly expands the number of possible attack points for cybercriminals.

Because it guards against theft and destruction to all types of data, cybersecurity is essential. Sensitive information, personally identifiable information (PII), protected health information (PHI), personal information, data related to intellectual property, and information systems used by the government and business sectors are all included in this. These data are vulnerable to theft or alteration by cybercriminals in the absence of strong cybersecurity safeguards, which could cause serious harm to one's finances and reputation.

Furthermore, data protection is not the only aspect of cybersecurity. It also has to do with guaranteeing the availability and integrity of IT systems. Cyberattacks have the potential to interfere with regular business activities, resulting in downtime and lowering output.

Cybersecurity is critical in a society where we do more and more business and personal transactions online. In an increasingly interconnected world, it's about securing our digital safety, maintaining our privacy, protecting our data, and defending our social and economic well-being.

Types of Cyber Threats[1]–[3]

I. ***Malware:***
A portmanteau of "malicious software," malware includes a wide range of destructive software programs, such as viruses, worms, ransomware, and spyware. Malicious software is usually installed on a network through a vulnerability that is created when a user clicks on a link or email attachment that poses a risk. Once installed, malware can lead to a number of issues, such as data theft and system breakdowns.

II. ***Phishing:***
A sort of cybercrime in which a perpetrator contacts a victim via text, phone, or email while pretending to be a trustworthy organization in an attempt to trick them into divulging personal information. Passwords, bank account and credit card information, and personally identifiable information may be among them. After that, the data is utilized to get access to crucial accounts, which increases the risk of identity theft and financial loss.

III. ***Man-in-the-Middle (MitM) Attacks:***
In a Man-in-the-Middle (MitM) attack, an imposter or eavesdropper enters the conversation between two parties. This gives the attacker the ability to listen in on conversations between two people who think they are speaking with each other directly and perhaps change or intercept such conversations. Attacks of this kind have the potential to steal confidential data or disseminate false information.

IV. ***Denial-of-service (DoS):***
Designed to bring down a computer or network and prevent authorized users from using it. DoS attacks achieve this by transmitting information that causes a crash or by overloading the target with traffic. Because of this, the system is unable to process valid requests, so depriving authorized users of their access to the system.

Understanding these dangers is the first step in defending against them, as they each pose a serious risk to cybersecurity. Furthermore, it's critical to remember that these are only a handful of the numerous varieties of cyberthreats that exist in the modern world. The field of cybersecurity is always changing, and new threats appear on a regular basis. As a result, sustaining a solid defense depends on always aware and alert.

Cybersecurity Best Practices[1]–[4]

I. ***Educate every employee:***
Our IT department is not the only one in charge of cybersecurity. A cybercriminal may be able to gain access to our network through any employee who utilizes a computer or mobile device. As a result, it's critical that each employee is aware of the dangers and how to help lower them. This includes receiving instruction on how to spot phishing emails and steer clear of them, setting strong passwords and changing them on a regular basis, and the dangers of utilizing public Wi-Fi networks for work-related activities. Frequent updates, reminders, and training sessions can help to keep this information current and relevant.

II. ***Patch promptly:***
Software companies frequently provide updates to address vulnerabilities in their products. We can defend our network from attacks that take use of these vulnerabilities by quickly implementing these patches. This necessitates setting up a method to keep an eye out for fresh patches, evaluate how applicable they are to our program, and promptly apply them. Tools for automated patch management can facilitate and expedite this procedure.

III. ***Install firewalls:***
According to preset security rules678, a firewall is a hardware or software that watches over and regulates incoming and outgoing network traffic. By obstructing harmful traffic and limiting unwanted access to our network, it serves as a barrier between our internal network and the outside world678. Every device that connects to our network, including servers, desktop computers, and mobile devices, needs to have a firewall enabled.

IV. ***Organize for unforeseen events:***
A cybersecurity crisis could still happen even with the finest safeguards in place. A disaster recovery strategy equips our company to handle such an event with proficiency. In the event of a cyberattack or data breach, this plan should specify what has to be done. It should include instructions on how to isolate compromised systems, remove the threat, retrieve lost data, and resume regular operations. The strategy is tested and updated on a regular basis to guarantee that it stays effective as our company and the threat landscape change.

Strong cybersecurity strategies are based on these best practices. But since cybersecurity is a dynamic, multifaceted industry, it's critical to keep up with emerging threats and security protocols. Seek guidance from a cybersecurity expert or company for more detailed recommendations catered to the requirements and conditions of our company.

Conclusion[1]–[3]

The significance of cybersecurity in the digital age cannot be emphasized. There is a greater chance of cyber dangers as we depend more and more on digital platforms for communication and business.

Governments, corporations, and individuals all have a part to play in preserving cybersecurity. This is due to the interconnectedness of our digital world's security. One compromised system may cause breaches in other systems that are linked. As a result, it is the duty of everyone who handles data or uses digital systems to practice proper cybersecurity.

Even with the constant threats, there are ways to drastically lower the likelihood of a cyberattack. This entails combining the application of appropriate security tools with the adoption of sound security practices. Using secure passwords, updating software, exercising caution when visiting links or downloading data, and staying informed about the most recent cyberthreats are a few examples.

Furthermore, stopping assaults is not the only aspect of safeguarding digital systems. It also entails preparing a strategy for handling attacks when they happen. This entails putting mechanisms in place to recognize and eliminate risks, recover lost data, and resume regular operations.

In summary, cybersecurity is a societal problem in addition to a technological one. It necessitates appropriate attitudes and actions in addition to the appropriate technology. The goal is to establish a culture of security in which everyone is aware of the dangers and knows how to keep others and themselves safe. Ultimately, we are all better secure the more systems we secure.

2. The vicissitude of Cyber Crime Threat Landscape: The past, present and the future[2], [3], [5]–[9]

The term "cybercrime," which first appeared in the digital era, describes a broad range of malevolent actions carried out online and using digital means. As technology becomes more and more ingrained in our daily lives, cyber threats have become more complex and expansive. Cybercriminals are always coming up with new ways to take advantage of digital systems, which is why attack techniques keep changing. Technology is evolving at a quick pace, giving cybercriminals more and more tools at their disposal to carry out their evil deeds, which is what is driving this progress. Ransomware assaults and data breaches are only two examples of the varied and frightening world of cybercrime. In light of this, it is essential to comprehend these dangers' characteristics and evolutionary trajectory in our increasingly digital environment. The struggle against cybercrime is dynamic and never-ending, necessitating constant attention to detail and adjustment to the constantly shifting terrain of online threats.[2]

[1], [5]–[7], [9]–[11]Cybercrime is a dynamic and constantly changing phenomena that encompasses a wide range of destructive behaviors carried out through digital devices and the internet. Technology breakthroughs and shifts in online behavior are what fuel this ongoing evolution. As our connection to the digital world grows, the decisions we make in this virtual space can have a big impact on the real world. Quick to take advantage of these developments, cybercriminals are always coming up with new ways to attack targets in order to carry out their nefarious schemes. This illustrates the complexity of our digital culture, where choices made in the virtual world can have a significant impact on the real world, ranging from significant interruptions of vital services to compromises of personal data. Comprehending the ever-changing landscape of cybercrime is vital for formulating efficacious approaches to counter these hazards and safeguard our virtual environment.

It is true that the development of cybercrime might be compared to a game of cat and mouse, in which players are constantly changing their strategies to outwit one another. Cybercriminals create creative ways to get around cybersecurity experts' latest defenses, which are meant to safeguard digital systems and data. Significant progress has been made in both offensive and defensive cyber capabilities as a result of this dynamic and continuous conflict. This loop is further fueled by the speed at which technology is developing, giving both sides access to an ever-expanding toolkit. This ongoing change emphasizes how intricate the cybersecurity environment is and how important it is to maintain constant awareness, creativity, and adaptation in the face of changing threats. In this digital cat and mouse game, we can only expect to keep one step ahead by this unrelenting quest of security and resilience.

Since its inception, the environment of cybercrime has experienced tremendous changes. Cybercrime in the early days of the internet was comparatively easy to commit and consisted of things like spreading viruses and email frauds. However, the complexity and scope of cybercrime have increased along with technological advancements. Cybercriminals now use a wide range of advanced tactics, such as ransomware, phishing, hacking, and distributed denial-of-service (DDoS) attacks.

The danger picture is expected to grow increasingly more complicated as we move forward. Cybercrime is finding new ways to operate as a result of emerging technology like artificial intelligence, machine learning, and the Internet of Things (IoT). In addition, as our society becomes more digitally advanced, we become more susceptible to these dangers.

When seeking to give a thorough history of cybercrime, looking at its causes, present situation, and possible developments in the future. We can create more effective defenses against these changing threats and better plan for the future by knowing the history and current state of cybercrime. We all have a shared responsibility to combat cybercrime, and our best chance of securing the digital world is by working together. Together, let's set out on this adventure to investigate cybercrime's past, present, and future.

Cybercrime began to emerge in the 1940s, not long after the first digital computer was invented. Because there was restricted access to these enormous electronic devices during this time, cyberattacks were essentially nonexistent. When computer pioneer John von Neumann conjectured that computer programs could reproduce in 1949, the theory behind computer viruses was first made public.

The term "phone phreaking" first appeared in the late 1950s, signifying the subcultural and technological origins of hacking. In order to avoid paying long-distance charges and make free calls on the network, telecom engineers could operate remotely thanks to "phreaks" that took advantage of certain protocols. Though it eventually stopped in the 1980s, this practice helped pave the way for digital technologies.

To expound further, the origins of cybercrime may be found in the 1940s with the introduction of the Electronic Numerical Integrator and Computer (ENIAC), the first digital computer. This machine was essentially impervious to cyberattacks because it was not connected to any network and was solely utilized for military and scientific purposes.

In 1949, prominent computer scientist John von Neumann established the theoretical basis for computer viruses12. His idea of a self-replicating program is credited with inspiring the development of contemporary computer viruses12. This concept, which was ground-breaking at the time, has had a significant influence on the growth of cyberthreats. The idea of a program that could replicate itself within the host system, like to a biological virus, was effectively born out of Von Neumann's hypothesis. The self-replication mechanism seen in many modern computer viruses is what drives their operation. This idea has been developed and modified over time, resulting in the wide variety of malicious software that is available today. As a result, von Neumann's groundbreaking research has had a long-lasting impact on cybersecurity, influencing how we perceive and respond to cyberthreats.

"Phreaking" is a term for a type of hacking that first appeared in the late 1950s. It involves using phone network manipulation to make anonymous or free calls. By taking use of the protocols that let telecom experts work remotely on the network, this was accomplished. The "phreaks" circumvented the billing systems by using a variety of strategies, such as producing particular tones to operate the phone switches.

Despite being against the law, this behavior was motivated by curiosity and a desire to learn how the telephone network operated. It drew a group of enthusiasts who exchanged knowledge and methods, giving rise to the hacking subculture.

In the 1980s, phone phreaking rapidly decreased as more secure phone networks were introduced and technology shifted to digital platforms. But because it showed how to take advantage of weaknesses in communication networks, it had a big influence on how cybercrime developed.

More complex types of cybercrime have emerged as a result of the principles acquired from phone phreaking being applied to the digital sphere. With our growing reliance on digital technology, the danger landscape of cybercrime is predicted to get more intricate and difficult to navigate.

Since computers and the internet have become essential to government, business, and entertainment, cybercrime has become more significant in today's world. Hacking, phishing, and the deployment of malicious software, such as ransomware, are the most frequent cyberthreats. Cybercriminals typically don't need a lot of technical knowledge in order to take advantage of human flaws.

Cybercrime poses a wide range of complex and varied dangers today. From more complex techniques like distributed denial of service (DDOS) assaults, pandemic-related phishing, ransomware attacks, and mobile malware, they span from hacking of social media and email passwords, phishing attacks, and the dissemination of harmful software.

Let's examine these dangers in more detail, Hacking is the act of gaining unauthorized, frequently malevolent, access to networks or systems. Hackers may utilize compromised machines for additional assaults, disrupt networks, or even steal confidential data. Attackers can deceive people into divulging private information, like credit card numbers or passwords, by posing as reputable organizations through the practice of phishing. Phishing attacks frequently take the shape of phony emails or internet pages.[9]

Spyware, ransomware, worms, viruses, and other dangerous software are examples of malicious software. These programs have the ability to compromise networks, steal confidential data, and interfere with system operations. Distributed Denial of Service, or DDOS, assaults include flooding a server, network, or service with traffic, making it sluggish or unusable. This can be used to bring down websites or interfere with their operation.[9]

Phishing attempts relating to pandemics have increased since the start of the COVID-19 pandemic. Attackers deceive people into disclosing personal information or downloading harmful software by sending out emails or messages purporting to provide information or assistance regarding the pandemic. In a ransomware attack, the victim's files are encrypted by malware, and the attacker demands a fee to unlock them. Financial damage as well as major disruptions may result from these attacks.

Mobile malware has grown to be a serious threat as smartphones and other mobile devices are used more frequently. These assaults may entail taking use of mobile devices to steal confidential data or to serve as launching pads for other attacks.

Future cybercrime is expected to be influenced by a number of major developments. The estimated total cost of data breaches by 2024 is $5 trillion. This enormous sum is anticipated to come from a 70% anticipated increase in cybercrime and a spike in fines brought on by data protection regulations.

Cybercrime is expected to be significantly impacted by artificial intelligence (AI) in the future. AI will be targeted for attacks and turned into a weapon as it gets more widely used. It is anticipated that cybercriminals would use AI to carry out sophisticated cyberattacks. Cybercriminals can use AI to create malware more quickly, automate attacks, and increase the efficacy of social engineering and frauds by using deep fakes and AI-powered voice synthesis that sounds human. Artificial Intelligence is playing a major part in the increasingly perilous cyber threat scene.

As technology becomes more and more ingrained in our daily lives, cyber threats have become more complex and expansive. Cybercriminals are always coming up with new ways to take advantage of digital systems, which is why attack techniques keep changing. Technology is evolving at a quick pace, giving cybercriminals more and more tools at their disposal to carry out their evil deeds, which is what is driving this progress. Ransomware assaults and data breaches are only two examples of the varied and frightening world of cybercrime. In light of this, it is essential to comprehend these dangers' characteristics and evolutionary trajectory in our increasingly digital environment. The struggle against cybercrime is dynamic and never-ending, necessitating constant attention to detail and adjustment to the constantly shifting terrain of online threats. In this digital cat and mouse game, we can only expect to keep one step ahead by this unrelenting quest of security and resilience.

In conclusion, attackers are always coming up with new strategies and tactics, making cybercrime a dynamic and complex field. It's critical that people and organizations remain aware of these risks and take the necessary precautions to keep themselves safe. This entails creating strong, one-of-a-kind passwords, updating software and systems, being wary of opportunistic emails or messages, and utilizing trustworthy security tools.

[3], [4], [8], [12], [13]The significance of cybersecurity in an increasingly digital future cannot be emphasized. While there are many advantages to the rapid growth of technology, there are also new risks and weaknesses that can be taken advantage of by cybercriminals. As a result, it is crucial that we continue to be watchful and proactive in our cybersecurity efforts.

We also need to acknowledge that cybersecurity is a shared duty including corporations, governments, and consumers, rather than solely being the responsibility of individuals or organizations. To establish a safe and secure digital environment, cooperation is needed. This entails putting in place strong security measures, informing the public about the dangers, and encouraging a cybersecurity-aware culture.

Moreover, our defenses and strategies need to change along with the cyber threat scenario. This entails keeping up with the most recent patterns and advancements in cybercrime, funding R&D to create fresh security solutions, and taking a proactive and flexible approach to cybersecurity.[9]

In the end, combating cybercrime necessitates a sustained effort and constant attention to detail. But if we band together and make the most of technology, we can make everyone's digital life safer and more secure. Cybercrime may have an unclear future, but we can meet these difficulties head-on and come out stronger if we are prepared and resilient. Let's keep working toward a time where technology advances society and fosters wealth rather than acting as a destructive weapon.

3.

a) Threat actors use the organized criminal model known as "cybercrime-as-a-service," or "CaaS," to offer other individuals their instruments, knowledge, and services. It basically amounts to the commodification and commercialization of cybercrime, making it possible for people with little technical knowledge to commit cybercrime.

Making as much money as possible is every cybercriminal's main objective. Thus, the next logical step toward achieving this objective was the creation of the CaaS model. CaaS, as a coordinated action, results in higher income with less work. Hackers are now offering their expertise and tools to anyone who is willing to pay for them or share the profits.

CaaS is increasing at a rate that keeps up with any successful organization, which is bad news for all online users, business owners, and IT specialists alike. The range of possible outcomes is equal to the variety of attacks that can occur. A few of these include data theft, user surveillance, and blackmail, which leave the victims with nothing but damaged reputations and empty wallets.

If they are willing to pay for it on the dark web, anyone can utilize CaaS to engage in cybercrime. Hackers no longer require advanced coding knowledge or the ability to create harmful software on their own. They might be the "clients" of a more skilled cyberthief. The provider offers a ready-to-launch cyberattack after doing all the necessary preparations.

Many different types of cybercrimes can be carried out with CaaS. A few examples of potential threats include ransomware, phishing, social engineering, malware, distributed denial of service (DDoS), and financial fraud.

Similar to a real firm, a cloud-based application service provider is extremely well-organized. In order to create the products and services they are selling, engineers, managers, and developers are involved. Tech support agents may even be included to assist customers in comprehending all of the technical specifications of the "product". Additionally, a few CaaS models provide hosting services for assault launchers.

Money mules are typically also engaged. Their objective is to transfer the profits to several accounts until all parties become "clean" and there is no trace of the funds. For their attacks, cybercriminals can rent cyberweapons by the hour, day, or month. Also, there is a wide range in pricing, with the most basic kits costing only a few dollars and the most expensive ones costing hundreds of dollars.

For sixty dollars a day, for instance, you may rent a DDoS booter. However, the $84,000 Maze Ransomware Kit is among the priciest ransomware kits available on the dark web. Cybercrime-as-a-service will help you recover your hijacked social media account. This $300 service is aimed against Facebook, Instagram, WeChat, TikTok, and Twitter.[14], [15]

b) Large enterprises worldwide are becoming increasingly concerned about targeted attacks. These well-thought-out attacks move through six stages, each of which illustrates how an attacker gets deeper into their target. Intelligence gathering, points of entry, command and control, lateral movement, asset/data finding, and data exfiltration are the six phases of a targeted attack.

   Information on the targeted target is gathered during the first stage, known as intelligence gathering. In spite of the fact that the onslaught is already under way, this phase never ends. Information gathered from within the network can enhance the effectiveness of any current attacks.

   Spear phishing emails have been the typical method employed by points of entry to penetrate the networks of their intended targets. Although there are still ways to accomplish this, attackers have introduced new techniques. Among these options are watering hole assaults, which target websites that the target company or industry frequently visits.

   There are various causes behind the increase in targeted attacks. The economics is one of the causes. The global economic outlook is nevertheless beset by challenges. All industries are being impacted by supply chain problems, energy crises, and inflation. The entire cost of cybercrime will rise due to inflation as the costs of prevention and remediation rise.

   The growth of malware-as-a-service is another factor. Businesses, governments, people, and organizations in almost every industry have been afflicted by ransomware. Threat actors can now more easily than ever obtain potent ransomware tools. Criminals can conduct attacks that cost businesses millions of dollars even with only rudimentary technical knowledge.

   Targeted assault trends are also on the rise due to geopolitical strife. Attacks sponsored by states and motivated by politics are already on the rise as a result of growing geopolitical tensions.

   The loss of financial data is the most frequent consequence of targeted attacks. More focused attacks have resulted from the emergence of hacktivism and the growing ambitions of cybercriminals to make bigger profits. Targets are frequently chosen by criminals based on their anticipated capacity to pay a high ransom rate. Depending on the type of business they have infected, ransoms can range from tens of thousands to millions of dollars.[1], [5]–[7], [10], [16]

c) In the digital world, targeted ransomware assaults are becoming more and more common. These are well-thought-out, phased attacks that demonstrate the progression of attackers within their targets. The phases comprise asset/data discovery, lateral movement, command and control, information gathering, points of entry, and data exfiltration.

It is anticipated that ransomware assaults would become increasingly more difficult in the future. Today's cybercriminals are capable of launching ransomware attacks on businesses, organizations, and even governments, causing unimaginable devastation. Ransomware has changed considerably over time, growing more potent. Ransomware is obviously appealing to thieves because it's a pretty easy technique that can do a lot of damage with little effort.

It is anticipated that ransomware will continue to pose a threat. Cybercriminals have countless ways to take advantage of holes in contemporary technology. One good example is the increasing usage of Internet of Things (IoT) devices, which are perfect targets for cybercriminals since many of them have inadequate security features and are improperly configured.

More needs to be done, even while corporate IT teams are making every effort to counter the threat posed by ransomware attacks and hackers. This also applies to common sense precautions, particularly with regard to Internet of Things devices, where default settings should be altered right away, stronger passwords should be used, and undesired services should be turned off as soon as feasible.

It appears reasonable to predict that ransomware will continue to become more of an issue in the future. The loss of financial data is the most frequent consequence of targeted attacks. More focused attacks have resulted from the emergence of hacktivism and the growing ambitions of cybercriminals to make bigger profits. Targets are frequently chosen by criminals based on their anticipated capacity to pay a high ransom rate. Depending on the type of business they have infected, ransoms can range from tens of thousands to millions of dollars.[3], [5], [16]

d) A sort of cyberattack known as "form jacking" occurs when hackers insert malicious JavaScript code into an online form, usually one that requests money. That malicious code gathers the payment card number along with other customer data, such as name, address, and phone number, when a site user submits their payment card information and clicks submit.

Form jacking is a technique used to steal credit card numbers and other data from payment forms that are accessible on website checkout pages. The malicious JavaScript code is what gathers the data supplied by a website user on an e-commerce payment page when they enter their payment card details and click "submit." The cybercriminals have installed malicious JavaScript code that can gather data, including phone numbers, home and business addresses, payment card information, and more. The data is subsequently moved to the attacker's servers after it has been gathered.

Cybercriminals seeking to make quick money find form jacking to be a very alluring alternative due to its discretion and lack of user interaction. When they add JavaScript code to the intended website, an assault starts. Keep in mind that it typically targets third-party code and appears as a supply chain attack rather than the website itself. After the malicious code is installed, all information provided by the user on the form that they submit to the website is likewise sent to the attacker. There's no indication that anything is wrong because the transaction proceeds normally after the user presses "Submit" or an analogous button. Because of this, it might be challenging for users and website owners to identify form jacking until it's too late.

The practice of form jacking has increased recently. According to Symantec's 2019 ISTR report, on average 4,800 websites per month were found to have been infected by form jacking code. Symantec stopped an astounding 37 million form jacking attempts in 2018.[11], [17]

e) One important development in the field of cybersecurity is crypto jacking. It involves exploiting the Central Processing Unit (CPU) power of victims' devices to mine cryptocurrency covertly by installing coin miners without the victims' knowledge. Because of how common this tendency is, Symantec wrote a research report on it that offers information and analysis on this cybersecurity risk.

The last quarter of 2017 saw a spike in the prevalence of crypto jacking, which was accompanied by a rise in the price of cryptocurrencies, such as Monero, which is mostly mined by CPU miners. The space occupied by browser-based coin miners saw the biggest spike in activity. The number of crypto jacking incidents peaked in December 2017, when Symantec prevented over 8 million instances. In July 2018, there were just under 5 million crypto jacking events prevented, despite a modest decline in activity from the previous month.

Device slowing, overheated batteries, higher energy usage, gadgets becoming useless, and decreased productivity are the main consequences of crypto jacking. Businesses who are billed based on CPU utilization may incur increased expenditures as a result of cloud crypto jacking.

To mine cryptocurrency, computer programs known as coin miners are employed. Digital currencies made with computer programs and processing power are called cryptocurrencies. The most well-known cryptocurrency is called Bitcoin, but mining it using a computer is not possible—specialized equipment is needed. Monero is the cryptocurrency that is mostly mined on desktop PCs.

An executable file must be downloaded and run on your computer in order to mine coins with file-based mining. Scripting languages are used to create browser-based coin mining, which occurs inside a web browser. When a website contains a coin-mining script, the users' computer resources will be used to mine cryptocurrency while they are on the website.

It is not against the law to mine coins, and many people opt to mine coins for personal gain by running files or scripts on their computers. As long as users are informed that their CPU resources will be utilized to mine cryptocurrency while they are on the website, coin mining is a legitimate alternative to advertising on certain websites. The issues occur when users are unaware that their computers are being used to mine cryptocurrencies or when hackers install coin miners covertly on victims' PCs or Internet of Things (IoT) devices without the victims' knowledge (a practice known as "crypto jacking").[11], [18]

f) In the constantly changing digital landscape, cloud attacks are a serious concern. On-premises apps, storage, and private clouds endure while Software-as-a-Service (SaaS) application consumption soars and workloads progressively shift to Infrastructure as a Service (IaaS) platforms like AWS and Azure. Existing security paradigms are being challenged by this hybrid IT environment, which makes things more complex and leaves enterprises struggling to keep up.

In addition to offering a roadmap for upcoming security requirements, Symantec's first Cloud Security Threat Report (CSTR) gives insightful information about the difficulties facing cloud security today. According to the survey, businesses are storing data across several environments, which causes problems with visibility in these cloud workloads. Remarkably, 93% of survey participants said it was difficult to keep track of all cloud workloads. The cloud's quick deployment times and decentralized architecture aggravate this problem by amplifying human mistake and introducing weaknesses that hackers can take advantage of. According to the paper, in order for enterprises to adjust to this new reality, their security strategies may need to be realigned or even completely redesigned.

Because of the cloud's decentralized structure and ability for quick deployment, human mistake is magnified, opening up opportunities for hackers to take advantage of. The majority of firms are not keeping up with the development of new cloud apps in relation to their cloud maturity, which is a serious worry, according to the report. Remarkably, 73% of participants say that inexperienced security measures, including using personal accounts and not using multi-factor authentication (MFA) or data loss prevention (DLP) services, were to blame for at least one cloud issue. This demonstrates how urgently businesses must improve their security procedures and adjust to the changing cloud environment in order to lessen these risks.

According to the report, in order to adapt their security strategies to this new reality, firms should realign and, in some cases, reimagine them. Comprehending the ways in which threat vectors are evolving in the cloud is essential for updating your security program and strategy as needed. The research helps enterprises adjust to the new realities of increasing cloud risks by offering insights and information about this cybersecurity danger.[1], [6], [10], [11]

g) A supply chain attack, sometimes referred to as a value-chain or third-party attack, is the process by which an attacker gains access to a system or network by taking advantage of flaws in third-party software or services. Because they prey on trustworthy connections and take advantage of the access provided by outside partners or suppliers, these attacks are very sneaky.

Large enterprises and government buildings are among the many targets that supply chain assaults represent a serious threat to. Because they target trusted connections and take use of the access provided to outside providers or partners, these assaults are especially sneaky because they take advantage of flaws in third-party products or services.

Commercial software products are one avenue through which these attacks might be launched. An attacker can access a multitude of targets if they are able to breach the integrity of a software company's system or product. Because it maximizes the attacker's potential impact by allowing them to penetrate several systems through a single port of entry, this approach is especially successful.

Apart from proprietary software, open-source supply chains pose a substantial danger. Anyone can help design a program because open-source development is collaborative in nature. Although this transparency is one of the advantages of open-source software, it may also be used by adversaries to introduce security holes into open-source programs.

Another avenue via which supply chain attacks might occur is from foreign sources. These risks may manifest when software products incorporate harmful code that the creator was ordered to add by a hostile actor or government agency. The worldwide scope of supply chain threats and the necessity of strong international collaboration and cybersecurity standards are highlighted by this assault technique.

Supply chain attacks can have serious repercussions, such as reputational harm and monetary loss. Thus, it is essential to comprehend and reduce the risks related to supply chain threats in order to maintain safe digital infrastructures.

Supply chain attacks can have serious repercussions, such as reputational harm and monetary loss. In Target's infamous 2013 attack, for example, a threat actor gained access to an HVAC contractor and used that information to breach Target's systems.

Strong security measures are necessary to prevent supply chain assaults. These methods include employing data loss prevention (DLP) services, multi-factor authentication (MFA), and supplier security due diligence for both new and current vendors. Maintaining safe digital infrastructures is critical as the digital world changes, and recognizing and reducing the risks associated with supply chain threats is essential.[2], [3], [5], [7], [9], [11], [17]–[19]

h) Hackers are increasingly targeting critical infrastructure, such as transportation networks, water supply, pipelines, electricity grids, and even hospitals. Due to their necessity for continuous operation, these infrastructures are attractive targets for hackers, whether they are nation-state-sponsored hacking organizations seeking to cause havoc or ransomware groups seeking to profit. The seriousness of these dangers is highlighted by the recent cyberattack on South Staffordshire Water, a UK utility that supplies drinking water to more than 1.6 million people. The corporation reported that "a criminal cyber-attack" had caused damage to its corporate IT networks. The event raises serious concerns because, despite the company's assurances, the attackers were unable to access the industrial systems that control the chemicals in the water. What may have happened if the cybercriminals had been able to encrypt the networks that control water supplies?

   This event acts as a sobering reminder of the possible repercussions of such strikes. The ramifications may be disastrous if hackers were to take over the systems that control water supplies. This could seriously endanger public health not just by interrupting the water supply but also by giving the attackers the ability to alter the water's chemical composition. This emphasizes how urgently strong security measures are required to defend vital infrastructure against these kinds of attacks.

   Indeed, water corporations are not the only ones who face the threat of cyberattacks. Targeted industries also include finance, petroleum, food, transportation, and the food industry. These sectors frequently rely on antiquated systems that are unable to fend off contemporary threats. These sectors urgently need to upgrade and fortify their cybersecurity safeguards because the antiquated nature of these systems leaves them especially open to cyber assaults.

   Recognizing this expanding concern, the US Cybersecurity and Infrastructure Security Agency (CISA) released a warning regarding the rise in malicious cyber activities. The US Water systems, networks, and devices' information technology and operations are the particular focus of this endeavor. The notice serves as a clear reminder of how constantly changing cyber dangers are and how important it is to maintain constant watch and take preventative action to safeguard vital infrastructure. It emphasizes how crucial it is to keep up with the most recent cybersecurity threats and put strong security measures in place to protect important systems and data.

   These attacks can have serious repercussions, such as harm to one's reputation or financial loss. Thus, sustaining safe digital infrastructures requires an awareness of and commitment to reducing the risks associated with attacks on vital infrastructure.[2], [3], [5]–[7], [9], [10], [12], [18]–[20]

i) Cyberattacks known as Internet of Things (IoT) attacks take use of flaws in IoT devices to obtain sensitive data without authorization. Devices, networks, data, and people may all be compromised by these assaults. Cybercriminals can take control of an automated or IoT system, shut it down, or launch an IoT attack to steal data.

Devices connected to the Internet of Things (IoT) are especially susceptible to many types of network assaults, such as denial of service (DDoS), phishing, spoofing, and data theft. These assaults have the potential to take advantage of IoT device weaknesses, posing a major risk to cybersecurity. An effective attack, for example, may result in ransomware infestations, in which malicious software encrypts data and demands a fee to unlock it. Sensitive information can potentially be accessed and taken by unauthorized parties in significant data breaches. Businesses may suffer greatly from these occurrences, which frequently need for significant human and financial resources to resolve. Data recovery, system maintenance, bolstering security precautions, and reputational damage mitigation are all possible steps in the recovery process. In order to stop these kinds of assaults, it is imperative that businesses put strong security measures in place for their IoT devices.

Internet of Things (IoT) devices are connected by wireless connections, which present a huge attack surface with several access points that hackers can take advantage of from a distance. This is made worse by the fact that a lot of IoT devices lack strong security features because they are made for basic functions. This makes these gadgets simple pickings for online thieves. These devices' simplicity combined with their interconnectedness creates a special cybersecurity issue. It is similar to a house with lots of windows and doors but simple, easily picked locks. In order to guard against potential cyber threats, it is therefore essential that both manufacturers and consumers give high priority to implementing robust security mechanisms in IoT devices, even though these devices may seem simple.

The notorious Mirai botnet, which turned Internet of Things equipment like cameras and routers into a network of remotely controlled bots, or "zombies," is one example of an IoT attack. Then, strong DDoS attacks were launched using this botnet.

Strong security procedures, such as encrypting communications, upgrading and patching devices on a regular basis, and changing default passwords, are necessary to prevent IoT assaults. The need to put in place strong security measures to guard against these changing dangers grows along with the number of IoT devices.[2], [3], [6], [7], [10], [11], [21]

j) With mobile devices becoming an integral part of many people's lives, the mobile landscape is changing quickly. This evolution concerns not just the gadgets in se, but also their applications. For example, mobile learning methods in higher education have increased significantly. Over time, both the ownership of mobile devices by students and their attitudes toward mobile learning have evolved. The COVID-19 pandemic has affected students' ownership and use of mobile devices for educational purposes.

But the danger landscape also changes in tandem with the mobile landscape. Mobile malware poses a serious risk to both individual and corporate security. Malicious software created expressly to target mobile devices—such as tablets and smartphones—with the intention of obtaining personal information is known as mobile malware. Mobile malware is becoming more common even though it isn't as widespread as malware that targets traditional desktops since many businesses now permit employees to access corporate networks using their personal devices, which could introduce unexpected hazards into the environment.

cybercriminals employ a variety of tactics to infiltrate mobile devices. Ransomware, a type of malware, encrypts a user’s data and demands a ransom for its release. Bank Trojans masquerade as legitimate banking apps to steal financial information. Cryptocurrency mining malware, or crypto jacking, covertly uses a device’s resources to mine cryptocurrency. Remote Access Tools (RATs) provide hackers with control over a device, enabling them to steal data or install additional malware. Advertising click fraud generates illegitimate clicks on online ads, which can lead to financial losses and the spread of malware. Each of these threats poses a unique risk to mobile devices and necessitates specific preventative measures.

Strong security measures are required to guard against these changing dangers, and this need is only going to increase as the number of mobile devices increases. It is essential to comprehend how threat vectors are changing in the context of mobile devices in order to adjust your security program and strategy as needed. This entails keeping up with the most recent cybersecurity threats, putting robust security policies into place, and regularly checking and updating security measures as necessary. In this quickly changing digital ecosystem, ensuring the security of mobile devices is a dynamic process that calls for alertness and proactive steps.[2], [3], [5]–[7], [10]–[12]

References

[1] “Cloud Security Threat Report (CSTR) Volume 1 | Adapting to the New Reality of Evolving Cloud Threats Executive Summary,” 2019.

[2] “acr2018final”.

[3] C. Point Software, “Cyber Security Report 2020.”

[4] “Norton Cyber Security Insights Report 2016 CONTENTS.”

[5] “Sophos 2023 Threat Report Maturing criminal marketplaces present new challenges to defenders Sophos X-Ops.”

[6] “Internet Security Threat Report Internet Security Threat Report CONTENTS,” 2016.

[7] “ISTR Internet Security Threat Report Volume 23.”

[8] N. by Symantec, “2017 Norton Cyber Security Insights Report - Global Results,” 2018.

[9] T. Hunter Team and S. Endpoint Security, “The Threat Landscape in 2021 (White Paper),” 2021.

[10] “Internet Security Threat Report ISTR,” 2017.

[11] “ISTR Internet Security Threat Report Volume 24 |,” 2019.

[12] B. SophosLabs, “Navigating cybersecurity in an uncertain world.”

[13] “NORTON CYBERSECURITY INSIGHTS REPORT.”

[14] “cybercrime-as-a-service-caas-explaned”.

[15] “cybercrime-as-a-service”.

[16] D. O’brien, J. Dimaggio, and H. Giang Nguyen, “An ISTR Special Report TARGETED RANSOMWARE.”

[17] C. Wueest, “An ISTR Special Report FORMJACKING: How Malicious JavaScript Code is Stealing User Data from Thousands of Websites Each Month.”

[18] “Internet Security Threat Report ISTR Cryptojacking: A Modern Cash Cow An ISTR Special Report |,” 2018.

[19] “FE DE R A L B U RE A U O F I N VE S TI G A TIO N.” [Online]. Available: www.ic3.gov,

[20] “FE DE R A L B U RE A U O F I N VE S TI G A TIO N.” [Online]. Available: www.ic3.gov

[21] “Cyber Safety Insights Report Global Results,” 2019.