Cyber Security: Malware Used By Hackers

Today’s use of technology has drastically changed since the 1970s since the first computer was released. Well, the year is 2020 and almost everything is done on the computer or a cell phone. In 2018, 84% of households in the U.S. owned a computer and in the same year, 765 million people were hacked or experienced data breaches. The use of cybersecurity, it's mainly used to protect software from hackers. Cyber Hackers mainly search for vulnerabilities in a companies software, and attempt to download malware which is the main focus is to destroy or Botnets that have the same focus as malware. A key point in time for cybersecurity was in the 1970s when the first computer virus was discovered.

Mathematician John von Neumann was the first to predict the idea in the 1940s, but it took 30 years for someone to create a computer virus. During the age of Arpanet which was the earliest form of the internet. In 1971 a few users on the network were surprised to see on their screens “ I am the creeper, catch me if you can.” Who or what is the creeper? Well, the creeper was a worm and it was a type of computer virus that has the ability to replicate itself and make it spread to other systems. Bold, Beranek and Newman were the creators of the creeper. Time has changed and other hacking software don't display messages, they are ought to take information and possibly use them against you. Fast Forward to 1983, MIT was granted US Patent 4,405,820 for a “cryptographic communications system and method.” This introduced the RSA algorithm, which was the first public-key cryptosystem. Cryptography is the bedrock of modern cybersecurity, which is the art of writing or solving codes. In this world, there are two types of people, the good and the evil. This carries in with the Cyber Security world, there are the people who will hack for the purpose of something good and the people who will hack for the purpose of being dishonorable. On the day October 1, 2003, the infamous group that is still known to this day, Anonymous. The group does not have a leader and represents many online and offline community users. All together they exist as an anarchic, digitized global brain. They have been linked to numerous high-profile incidents. Anonymous claims that their main cause is protecting citizens' privacy. One of the biggest hacking incidents was “ Operation Aurora.” This was announced by google on January 12, 2010, when they had a major breach on its infrastructure in China. At first, Google initially thought the attackers' goal was to find access to Gmail accounts that are owned by Chinese human rights activists. Later, analysts discovered that the true intent of the hacking was to identify Chinese intelligence operatives within the U.S. who may have been on watch lists for American law enforcement agencies. Also, the attacks hit 50 other companies in the internet, finance, technology, media, and chemical sectors. One of the reasons this operation happened was, these hackers were able to find vulnerabilities in google’s security systems.

Throughout the hacking process, they always look for a vulnerability. What is a vulnerability you might ask? A vulnerability is a weakness in a product that can allow an attacker to compromise the integrity, availability, or confidentiality of the product. For example, imagine your client’s software connects outsiders on their networks to any inner workings of the operating system without any restrictions or limited access, the user is potentially inviting attackers to cross over and rewrite the codes that help keep the information protected. Some of the more common vulnerabilities consist of: missing authorization, download of codes without integrity checks, software that is already infected with a virus, and the most common is having a weak password.

Another example of a vulnerability is a link. You may think why is a link considered a vulnerability? Well a twitch streamer, TimTheTatMan opened up a link that was sent through a donation. Tim proceeded to open the link and everything seemed normal. Well the person who sent the link to the twitch streamer, was able to put a sticky note on the desktop that addressed " Hi!" So the question is what proper procedures can you do to prevent incidents like these? There are many possibilities that secure any vulnerability in your system. Companies tend to have an abundance of protection services, such as Web protection with managed antivirus,MailProtection, patch management and backup to offer clients complete protection from every security angle. Ways to help prevent vulnerabilities if you are not protected by things such as those stated. You can always block users from visiting suspected and confirmed unsafe websites or applying web bandwidth checks. These are just two effective ways that help keep you safe from any vulnerabilities. Some statistical facts that help elaborate the idea of vulnerabilities are that the U.S., U.K, and China are more vulnerable to smart home attacks since most of these smart home devices are connected through an external network. If that router doesn't have decent security protection, this is opening up your home to a cyber attack. Criminals are finding new ways to exploit these vulnerabilities. Overseas in Japan, they had reported that they had lost over $530 million due to hacking, this had to do with their cryptocurrency. All these incidents are due to these hackers finding some type of vulnerability to hack into the system and do whatever they please. With the technology on the rise, it also leads to the rise of cybercrimes and as of right now we are expected to cost $6 Trillion by 2021. In 2015 the figure was $3 Trillion. With viruses, they can be obtained via external or internal. Such as if you download something sketchy off a website that is an external threat. If you put a USB drive into your computer it can access many things since it has gone through with ease past the firewall. The USB thumb drive method is the most common, since purchasing a thumb drive is very inexpensive, very small, and can store a lot of data. With the hackers they were able to develop targeted malware, this is known as the Conficker worm. The Conficker worm can automatically execute upon connecting with a live USB port. That isn't the worst thing, the worst thing is the default operating system is configured to allow most programs including malicious ones to run automatically. To put this in perspective this is the equivalent of everyone in your neighborhood having an electric garage door opener and being able to use it to open everyone else's garage doors. This is just one of many threats that can oppose damage through the inside. Even our smartphones are full-functioning computers, they have wifi connectivity, multithreaded operating systems, and vast application support. These devices are capable of posing the same threats we've seen with notebooks and thumb drives. Not only do they pose the same threats as notebooks, they also have the potential to elude traditional data-leak prevention solutions. To summarize vulnerabilities, there are endless possibilities on finding a distinct way to breach and steal a person's personal information. Vulnerabilities can be accessed externally or internally. Just like vulnerabilities, malware has similar intent which can also be payload in a number of different ways.

Although there are many cybercriminals they also are becoming more sophisticated in their own methods with malware. Which is a collective name for malicious software variants, which can include viruses, ransomware, and spyware. These consist of codes developed by cyberattackers, they were specifically designed to cause extensive damage to the data and systems or try and attempt to gain unauthorized network. Malware is usually delivered in the form of a link or file over an email which requires the user to click on the link or open the file that executes the malware. The question is what does malware actually do? Well, its payload can happen in many different ways. Some of the common types of malware are different in many ways. The first common type is a virus, these viruses attach their malicious code to clean and

they wait for an unsuspecting user to execute them. The virus is one of the more common ones, although ransomware aka scareware comes with a heavy price to pay. Ransomware has the ability to lock down on networks and lockout any users until some type of ransom is paid. This method has targeted some of the biggest organizations in the world today, with expensive results. Carrying out a ransomware attack requires some help. For example, imagine the big trojan horse outside of troy is the ransomware hanging in your inbox, and the link inside is the greek soldiers, which is the trojan. It is hidden within something and disguises itself as legitimate software. With the trojan, it acts discreetly, by breaching security by creating backdoors that give other malware variants easy access. This leads to another type of malware that sometimes we can't even see. Spyware, as its name suggests, it is coded to spy on what a user is doing. They hide in the background on a computer, with this type of malware, will collect information without the user even knowing. Botnets help malware with everything, the pure purpose of the botnet is giving a network of computers infected by the malware are controlled remotely by criminals, most of the time for financial gain or sometimes to launch attacks on websites or networks. If your computer were to be infected with malware and part of a botnet, it can communicate and receive instruction about what it's supposed to do from "command and control." All of these botnets are designed to harvest data, such as passphrases, social security numbers, credit card numbers, you name it. All of the data obtained is used for nefarious purposes, such as identity theft, credit card fraud, spamming, and malware distribution. Each type of malware has its own unique way of causing havoc, it relies on the user action of some kind. How does malware spread? They usually can be delivered through an email or an executable file. Links like those are where trojans tend to disperse themselves and hide. Computers are not the only ones that are vulnerable to these attacks. Cell phones are vulnerable to attacks too. For some instances, malware can even be sent through text messages or social media. Now that there is an understatement of what malware is and the different types. Some procedures that are used to protect your system from malware, the two areas to consider are protective tools and user vigilance. Protective tools are the easiest to implement, the reason is that it is simply the best in class protective software that can manage itself and update itself. It's always a good idea to keep temptations low when something says " check out this cool website" or sometimes out of fear when a message pops up like " install this antivirus software immediately." Things like these can be very deceiving and keeping temptations lower will save your personal information. One of the biggest ways to prevent malware is EDUCATION. This is the key to ensuring users are aware of the risk of malware and what they can do to prevent any attack. Sometimes this can include user policies and if they are in the right place and having the right anti-malware solutions constantly monitoring your networks, emails, and other activities that could put your organization/yourself at risk. The cyber security industry is on the rise and is looking for people that have the ability/skills to work around the field. It all starts with the history, knowing the vulnerabilities, and the different kinds of malware.

Technology has been on the rise and continues to develop better and bigger things. With that on the rise, it also leads to the rise of cybercrimes. We are expected to have $6 trillion in cybercrime attacks by the year 2021. With the use of cybersecurity, it's mainly used to protect software from hackers. Cyber Hackers mainly search for vulnerabilities in a companies software, and attempt to download malware which is the main focus is to destroy or Botnets that have the same focus as malware and help it in some way.