Fall 2022

Malware Detection and Prevention

Dwight Thomas Watson
Murray State University, dwatson0972@gmail.com

Malware Detection and Prevention

By
Dwight Watson

Project submitted in partial fulfillment of the
requirements for the
Bachelor of Integrated Studies Degree

Murray State University
November 30, 2022

Abstract

Malware first appeared in 1971, before broadband internet even existed. The first variations began with people just testing what they could do and were not malicious. Eventually, that time came to an end once cybercriminals began to realize that they could wreak havoc and profit from creating malware. Almost at the same time, cybersecurity was created to help combat these viruses and malicious attacks by cybercriminals. This project paper will dive into the technical issues that arise from malware detection and prevention. It starts with defining malware and goes over the history of malware from its birth to today. Then this paper will list all of the different variations of malware and the processes they execute to break into systems and propagate. Next, it goes over the different variations of malware defenses, starting with antivirus software. The paper will define antivirus software and how it functions as well as provide a history. Then it will dive into cryptographic defenses to define, provide history, and explain the methods employed by cryptography. Finally, it will go over firewalls explaining how they function and their history. Malware will never cease to exist, so it is highly important to consider what computer and network technologies you should employ to protect yourself. This paper isn't just to dismiss malware but to help people understand better how these technologies can work to prevent malware attacks both during and before the attack even happens.

Key Words: Malware, Antivirus Software, Cryptography, Firewall, Key, Cipher, Gateway

Table of Contents

Introduction

The rise and growth of the internet has also in turn caused a rise and growth in the level of threats posed against electronic systems. Cybercriminals who employ these threats try their hardest to trick or scam people into disclosing or destroying personal and professional secrets and data. These threats come in the form of specific malware programs and social techniques. The main purpose of these threats is to break into an electronic system and allow cybercriminals to have full access to the system and then proceed to go through files, access any local devices, and even execute programs. The term “computer virus” is understood by all, even among children. Everyone knows this term as a malicious item regardless of location, age, or background. They know how it affects technology used daily by people such as computers, mobile devices, game consoles, and applications. This shows how integrated technology is in our society and how heavily we rely on it. Thus, the need to protect them against digital threats is a necessity. People need to understand the significance of the threat that malware programs can pose to everyone’s security.

Despite the increased use of antivirus software, the creation and distribution of malware programs has also steadily risen. According to Laka (2022), the number of reported malware has increased significantly over the years and reached over 1.3 billion in 2021 from only being in the 100 million in 2012. This paper aims to educate people about exactly what malware is and the methods that can be used to detect and prevent malware. This includes antivirus software, malware detection and prevention systems, and administrative methods. Many of these provide a good defense against malware, but can also be difficult to set up and employ. Thus, many people who don’t understand technology or find it too difficult end up not even bothering with protecting themselves from any type of attack. By the end of this paper, anyone should fully

understand malware and its threats and how to properly protect themselves from all types of attacks.

Definition of Malware

Malware is defined as “any code added, changed, or removed from a software system to intentionally cause harm or subvert the intended function of the system” (Namanya et al., 2018). This program then tries to break into the computer to cause damage or hold personal information hostage to make a profit. Malware can access computers, servers, cell phones, and networks without the user ever knowing about it. Malware is mostly broken down into two categories. The first is your regular viruses and Trojan horses, which usually trick a user into clicking or downloading software or a file that looks normal to them but ends up allowing the virus onto their computer. The other category is software that either forcefully or secretly enters the user's computer. With this, when the user does detect something wrong, it is already too late. Arce (2018) references a cybercrime survey completed by the Ponemon Institute. They characterized malware as the costliest of all attack vectors compared to malicious insiders, DDoS attacks, malicious code, and botnets (p. 1). With malware having such large effects on companies and individuals, many tech companies have begun to market their products as having some form of security added to help promote their brand.

History of Malware

The 1970s

The first malware to appear in our history was in 1971. This was before the internet that we use today existed. The Advanced Research Projects Agency Network was working on connecting computers together remotely in 1967. They finally succeeded in the year 1969 and a year after that, the Network Control Program was created. The Network Control Program was

the first network transport layer that allowed data to be transferred from one computer to another (Saengphaibul, 2022). In1971, people could get their hands on the first microprocessor, the Intel 4004. This CPU was being made to be commercially used and to be affordable. This allowed computers to become a much bigger market and thus more of a security risk. That same year, the first virus was born. This virus was given the name "The Creeper." This virus, which acts more like a worm, was first created by an engineer named Bob Thomas (Saengphaibul, 2022). "The Creeper" made its way through the Advanced Research Projects Agency Network and would display the message "I'm the creeper, catch me if you can!" Now this very first virus wasn't intended to be malicious. This was simply done to see if it could spread to different computers using the Advanced Research Projects Agency Network.

The 1980s

1982

Almost all non-technical people like to say that "Macs can't get viruses." Unfortunately, for them, Saengphaibul (2022) states that the first computer virus found in the wild in 1982, dubbed "Elk Cloner," was designed to specifically target Apple II computers. According to Saengphaibul (2022), this virus was written by a fifteen-year-old who liked to write these types of programs to play pranks on his friends. The “Elk Cloner” would try to spread when a computer disk began to run. While hiding in memory, the virus would search around for an

uninfected floppy disk. When the disk boots for the fiftieth time, the virus will present a poem to the unlucky user:

Elk Cloner: The program with a personality

It will get on all your disks

It will infiltrate your chips

Yes, it's Cloner!

It will stick to you like glue

It will modify RAM too

Send in the Cloner! (Saengphaibul, 2022)

1986

The first virus recorded for a PC was in 1986. Computers during this time were still underdeveloped and most were not connected to the internet because it wasn't accessible to the public until 1989. At this time, the government and universities mostly use the internet. Still, in 1986, the first PC virus called "Brain" started to spread. Milosevic (2013) tells us that "Brain" originated in Pakistan and was created by two brothers, Amjad Farooq Alvi and Basit Farooq Alvi. They developed the virus to try to warn people that they were using a pirated copy of the medical software they had developed. This virus was not malicious but spread so well using floppy disks that it was known worldwide. The brothers ended up getting calls from many companies around the world asking how they did it. Another virus that came after "Brain" was the "Omega" virus. The virus was named because it would write the omega symbol on the computer display. According to Milosevic (2013), it would infect the boot sector of the computer

but wouldn’t do much until Friday the 13th came around, and then, it would not allow the computer to boot up.

1988

In 1988 it was when the first worm was created called the “Morris” worm. This was another non-malicious creation that was just being tested to see if self-replication was possible. This worm had many firsts within it. According to Saengphaibul (2022), this worm exploited vulnerabilities in programs and services and even checked to see if an infection already existed on the machine. The creator, Robert Morris, was worried that the worm would be easily stopped, so he made it have a very persistent behavior. The issue began because self-replication could not be stopped and thus caused devices to overload and make them inert, creating a denial-of-service that spread quickly. According to Milosevic (2013), Morris was the first person to be convicted under the Computer Fraud and Abuse Act. He ended up becoming a successful entrepreneur and was given tenure at the Massachusetts Institute of Technology (Saengphaibul, 2022).

1989

People saw their first ransomware attack in 1989 when the internet was made publicly available. The ransomware known as the "AIDS Trojan" didn't spread using the internet but spread using the physical mail service. In this mail were infected floppy disks that were sent to AIDS researchers with a questionnaire on AIDS. When the researchers booted the disk for the ninetieth time, the ransomware would begin to alter file names and hide them. Then it would demand $189 to have a yearly lease and $385 for a lifetime one. The ransomware would ask for users to send money via money orders, cashiers' checks, or bankers' drafts to a PO Box in Panama. According to Saengphaibul (2022), the AIDS Trojan was created by Dr. Joseph Popp, who stated that the reason he created the ransomware was so that he could donate any funds he

received towards AIDS research. When the ransomware was analyzed by forensics, they discovered that the key to unlocking the files was "Dr. Joseph Lewis Andrew Popp Jr."

The 1990s

1990

In 1990, a virus named “Casino” was released. Milosevic (2013) tells us that the malware program would copy the file allocation table to memory and then delete the original. After that, it will display a slot game to the user. They needed to match three of the correct signs and had three chances to have it happen otherwise if they restarted the machine the file allocation table would be lost and the computer would not boot up. However, if the user did get lucky enough and wins, then the malware program would copy back the file allocation table and the computer could be used normally.

1992

In 1992, a virus named “Michelangelo” was created. This virus lived in the boot sector and attacked DOS partitions. The virus was coded using Assembly language and was also spread employing floppy disks (Saengphaibul, 2022). The virus was named “Michelangelo” because it was created to have a time bomb inside it with instructions to launch on March 6, which is Michelangelo’s birthday (Milosevic, 2013). Once the virus had been discovered, the media began warning users not to turn on their computers on that day or to change the date on the computer to the next day. Another malware program released in 1992 was named “Walker.” This virus wasn’t malicious and just displayed Walker walking from side to side on the screen.

Another very similar virus was named “Ambulance” and that one had an ambulance driving from side to side making the noises of an ambulance as well (Milosevic, 2013).

1994-95

In 1994-95, the internet started to become a bigger attraction, and companies like AOL, CompuServe, and Prodigy came out. This year also saw the first phishing attacks get created. On AOL, a bot would send out messages to people requesting that they verify account information and that there was something wrong with billing or another type of issue. The only way a user could keep conversing with the bot was if they needed to input their account information for username and password. Once they did this, their information was taken and used by a program called AOHell that would sell the information to users to set up free credit cards (Saengphaibul, 2022). Also, in 1995, the first macro virus named “Concept” was created according to Milosevic (2013). The malware was spread employing the sharing of documents between users on either PC or Macintosh computers. Once the document is opened it will copy itself onto any newly created documents. Milosevic (2013) also tells us that the “Laroux” malware was the first Microsoft Excel macro virus.

1998

In 1998, the very first mail virus was released, named “Happy99” (Milosevic, 2013). This was spread as an attachment in an email that was executable. In 1998, spam filters didn’t exist yet and so email was allowing executables to be sent. Once the user runs the attachment, the

screen will display fireworks and, in the background, the malware program will begin copying the attachment and sending mail to the user's contacts.

1999-2000

In 1999-2000, during the height of Y2K, causing panic around the globe, the first botnet malware was created. The botnet was spread using Internet Relay Chat. The first botnet was called EarthLink Spam because it sent out huge amounts of spam. Saengphaibul (2022) tells us how the EarthLink Spam botnet made up 25% of all the email spam during that time, which was around 1.25 billion emails. Also, this year saw the GTbot come out. This botnet spreads in the same way as the EarthLink Spam botnet. The GTbot didn't send out spam, but instead sent out denial-of-service attacks.

The 2000s

2000

In 2000, while the first botnet had come out, the use of worm malware was increasing. One worm named the "I LOVE YOU" worm became so big that it was brought to the media because of how quickly it could propagate. This worm used email to spread an infected attachment with the title "LOVE-LETTER-FOR-YOU.vbs.txt." Once a person opens up the attachment, the worm will get into their Outlook contacts and begin emailing more people while pretending to be them. These emails would also have the infected attachment and it just snowballed because with the worm using the contacts and pretending to be the person they infected, people would trust these emails. Milosevic (2013) tells us that this virus caused 5.5 billion dollars in financial damage around the world. Another malware program named "Code Red" also came out in 2000. "Code Red" was another type of worm, and according to Milosevic

(2013), it was the first intentionally written worm. This malware program spread like all other worms and was also good at hiding from defense mechanisms.

2001

In 2001, the release of the malware worm named “Nimda” occurred. This worm was similar to the “Code Red” worm where it would also scan the network and spread. The difference, according to Milosevic (2013) was that “Nimda” would scan all IP addresses while “Code Red” would only scan the public IP. With this difference, the worm could infect private networks and even infect hosted websites to display downloads of files that were also infected.

2003

In 2003, most of the world was now connected to the internet employing a broadband connection. With there being so much connectivity to different systems, worms became a big deal. When August 11, 2003, came around, the worm “Blaster” had been let loose. Users at work and home were surprised when their systems began showing the “Blue Screen of Death” and then rebooted. No one knew, however, that they were hit with the Blaster worm. Saengphaibul (2022) tells us how the Blaster worm was to target a remote procedure call vulnerability in Microsoft Windows XP and 2003 operating systems to spread. The worm was meant to create an SYN flood attack on windowsupdate.com to not allow systems to obtain updates. Microsoft was lucky because the designer of the worm used the wrong domain since Microsoft used windowsupdate.microsoft.com. The worm had a bug in the code that created a buffer overflow and this led to a denial-of-service occurring. Milosevic (2013) tells us that it disabled several

systems, such as Air Canada being forced to land planes and a US train company named CSX to stop running.

2005

In 2005, the world began to see the birth of cybercrime. Malware before this time was mostly used by people messing around with each other, or they were just intrigued by what they might be able to do with it. When the malware called “Mytob” and “Zotob” came out, it changed a lot of things. These malware programs were combinations of worms, backdoors, and botnets, and they caused a lot of issues for people. They exploited vulnerabilities in antivirus software and blocked sites.

According to Saengphaibul (2022), these malware programs were so disruptive that they shut down the operations of one hundred organizations and even disrupted CNN enough that the anchor, Wolf Blitzer, had to announce that Lou Dobbs would not be able to come onto the air. This year also saw the first-ever Rootkit. This malware program was created by Sony Entertainment and was named “SONY BMG Rootkit” which was made to protect the copyright of their publications (Milosevic, 2013). SONY wanted to be able to detect and disable copying of their property and decided to use this Rootkit. Milosevic (2013) tells us that when a CD was inserted into a CD player nothing would occur, but if it was inserted into a computer then it would install the Rootkit and hide among sys. The malware program would then control how a person accessed music and if they tried to copy anything then the Rootkit would stop it. When the Rootkit was finally discovered it was a scandal for SONY. The director of global sales at SONY BMG, Thomas Hesse, stated “Most people, I think, don’t even know what a rootkit is, so

why should they care about it?" (Milosevic, 2013). This caused a large impact on SONY's image and after a lawsuit was filed SONY ended up giving refunds and free music downloads.

The year 2005 also saw the rise of spyware and hijacked search results. A malware program named "CoolWebSearch" was the first to hijack search results on Google and instead show search results that the cybercriminal wanted them to see. The malware program was created to take clicks away from Google and was spread employing drive-by download or adware. According to Saengphaibul (2022), the malware program was so difficult to remove that volunteers created programs such as "CWS Shredder" to be able to remove the malware for free.

2007

In 2007, a similar malware program named "BayRob" was launched that would hijack search results on eBay. The malware program wasn't discovered until a woman located in Ohio had purchased a car on eBay for a few thousand dollars, but the vehicle never showed up. Police discovered that the car was never listed and that her system was infected with malware that was showing her fake listings. The FBI and Symantec bided their time until the cybercriminals finally made a mistake which led to their arrest in 2016 (Saengphaibul, 2022).

The 2010s

2010

2010 brought about nation-state cyber weapons. The first one found named "Stuxnet" was a malware program employed to attack Industrial Control Services systems, which were mostly supervisory control and data acquisition systems. Stuxnet targeted industrial centrifuges of nuclear plants to force them to over-spin and create a meltdown. The malware program initially attacked places in Iran but ended up spreading all over the world. According to

Saengphaibul (2022), the NY Times in 2012 confirmed that it was the United States and Israel who had developed Stuxnet.

2011-12

In 2011-12, more modern ransomware began to start. The name of one ransomware program was “Reveton.” This ransomware appeared to be made by a cybercriminal organization. “Reveton” made use of looking professional and by using geolocation information it would provide a lock screen that would display a local law enforcement agency that gave them instructions on how they needed to pay to be able to unlock their computer.

2013

In 2013, a ransomware program named “CryptoLocker” came out that required payment in the form of Bitcoin. The price for the person to decrypt their computer was two Bitcoins, which back in 2013 was anywhere from $13 to $1,100 (Saengphaibul, 2022). Since then, many other ransomware programs have been created and employed in attacks. Also, in 2013, the rise of state-sponsored attacks was occurring. An attack named “DarkSeoul” was employed to attack the Korean broadcaster SBS and banks located in South Korea. This attack employed using a malware program named “Jokra” which would attack a master boot record and overwrite it. According to Saengphaibul (2022), the attack is thought to have been done by “Lazarus” which is a group in North Korea that also attacked Sony Corporation in 2014 for creating the movie “The Interview” that mocked North Korean leader Kim Jong Un.

2015

In 2015, some of the first browser lockers and fake technical support scams began appearing. These malware programs acted similarly to ransomware where they caused users to be alarmed and call a fake support number that went to cybercriminals or pay in cryptocurrency

to have the system no longer infected with malware. Saengphaibul (2022) tells us that these malware programs are employed using JavaScript on legit websites and would cause the browser to lock up and be unusable and display warnings of malware or threats to pay; otherwise, the system would be lost. One version of this was a malware program that would display a fake "Blue Screen of Death" that would convince the user something was wrong. The display would also have a number to call that stated it was Microsoft technical support but was instead a cybercriminal asking for remote privileges into the system to cause further damage.

2016

In 2016, the world saw the release of the first Internet of Things botnet malware program. The malware program was named "Mirai" and was the first to attack "Internet of Things" devices, primarily routers, on a network and would cause a "Distributed Denial of Service" (Saengphaibul, 2022). Most "Internet of Things" devices are neglected, meaning they are not updated regularly because many of them are firmware updates that require taking the device offline. The botnet took advantage of that and the fact that people don't always change the generic username and password of their "Internet of Things" devices. This led to the botnet being able to propagate very easily in very little time and thus made it very difficult to defend against because the attacks began flooding in from everywhere.

2017

In 2017, it was brought to light in the "ShadowBrokers" leak that the United States National Security Agency was creating highly sophisticated malware and how it worked. This was disastrous because it allowed cybercriminals to make use of the malware programs that were developed. The tools and exploits that had been leaked and stolen were known as "Fuzzbunch" and one piece of malware programming inside of it named "DoublePulsar" was a backdoor

attack that employed the “EternalBlue” exploit that was a zero-day exploit saved to be able to target Microsoft’s Server Message Block protocol (Saengphaibul, 2022). This then led to the creation and spread of the “WannaCry” and “Petya/NotPetya” ransomware attacks that caused shutdowns of manufacturing facilities around the world. Originally the leak was blamed on Russia, but so far there hasn’t been any clear proof to place the blame.

2018

In 2018, the “XMRig” application was created for a cryptocurrency named “Monero.” The application itself was not a malware program, but cybercriminals could use the application on other people’s infected systems and take the data to make money. They would target machines that had high CPU power and were remotely exploitable because a lot of these systems were not regularly updated due to carelessness or laziness, thus making them perfect targets for cybercriminals to use (Saengphaibul, 2022).

2019

In 2019, the world saw the birth of “Ransomware as a Service” which is where a cybercriminal would write a ransomware code and then sell the code to other cybercriminals who would employ the ransomware to users around the world making a profit for themselves and the creators. One such “Ransomware as a Service” group known as “GandCrab” was the first to create this type of business. Saengphaibul (2022) tells us how the “GandCrab” group wanted to distance itself from the actual attacks that were carried out and try to generate more revenue. The group would take a cut of anywhere between 25% and 40% for each successful attack carried out by one of their buyers. After a few months of doing this, the group announced its retirement

stating that they had already profited two billion dollars but were also probably having issues with authorities (Saengphaibul, 2022).

Types of Malware

Trojan Horse

Trojan horses are a type of malware that cannot propagate on their own. These malware programs rely on a person to open or download files that are infected to infect the machine and spread. Trojans are created to look as if they are legitimate files or attachments. Laka (2022) explains that the most popular trojan is a fake antivirus program that will pop up and claim that you have been infected by a virus and that you need to download and run a program to clean the computer. This of course allows the trojan access to your computer and any personal information it may contain. Another type of trojan is one that is combined with a spyware program. This is called remote-access trojans. This malware program, once downloaded onto a computer, can then look through the information on the computer but worse yet, can even turn on a computer's webcam and microphone so that they can take a video of the victim in their own house.

Virus

Viruses are another type of malware programming that cannot propagate on their own. These malware programs employ .exe files that they are attached to. Like Trojan horse malware, they need someone to download and run an application that they have not taken the time to make sure is legit or safe. According to Laka (2022), computer viruses are less common than they used to be in the past, and they currently only make up about 10% of all malware in existence. Viruses are not easily removed from a computer and it usually requires an antivirus to be able to try to remove them. Viruses also, once running, begin to employ most of a computer's resources,

which can cause it to freeze up like a DDoS attack. Some viruses, depending on the complexity of the code, can modify copies of themselves to help them better spread (Namanya et al., 2018).

Worm

Worms are different from Trojan horses and viruses in that they can self-propagate. This allows the malware program to spread without the need for a person to download or open an attachment. Worms employ emails and storage devices to spread through the network to other computers. They also consume a lot of bandwidth and processing capabilities from the computer by continuously scanning and causing the computer to become unstable and crash (Namanya et al., 2018). This means that if a person at a business opens an unsecured email or connects to a random storage device they find without scanning, it could then infect an entire business or corporate network. Laka (2022) states that one of the best-known computer worms was known as Stuxnet and was employed to cause damage to Iran's nuclear programs by targeting supervisory control and data acquisition systems.

Ransomware

Ransomware is a malware program that infects a host or network and holds the system captive while requesting a ransom from the owner of the system or network (Namanya et al., 2018). Then the malware program notifies the owner of the computer that they are required to pay a ransom fee to receive the decryption key and have access to their files again. Laka (2022) explains that ransomware is split into two different types: locker ransomware and crypto-ransomware. The former doesn’t encrypt files on the computer and instead makes it lockdown to be inaccessible. This type of ransomware is a bit easier to deal with since if you can just remove the malware program then you can access your files again. Alternatively, if you can’t remove the malware program, then you can remove the storage device and put it into another computer.

Crypto ransomware, however, is more difficult to deal with. This type of ransomware does encrypt all of the files on the computer, which makes it impossible to get access back to the files even after the ransomware has been removed. This type is more effective because it forces a person to either pay the ransom to obtain the decryption key or use a backup, which will mean any data after the backup date will be lost. Unfortunately, even if you do pay the ransom, there is no guarantee that you will receive the decryption key needed to unlock the files. According to Laka (2022), a quarter of ransomware victims pay the ransom demanded, and out of those, 30% do not end up receiving their decryption key. They have then lost both the money they paid for and the files that are still encrypted.

Fileless Malware

Fileless malware was created to counteract the increased use of anti-virus software. According to Laka (2022), fileless malware does not use a file system and can avoid signature-based detection methods. Since the malware performs in this way, it makes it increasingly difficult to detect and prevent because it can directly access the memory of a computer and circumvent the storage device altogether. This type of malware program employs tools and programs that are already on the computer to begin its attack. These tools are Windows Management Instrumentation and Powershell. Windows Management Instrumentation became a largely used exploit when Stuxnet was created that could access Virtual Machine detection, data theft, and code execution. The program Powershell became popular because it was capable of script execution that could circumvent anti-virus detection software.

Adware

Adware is a malware program that is not designed to do any damage to a computer or person but instead is designed to display ads to the person using the computer in the hopes of

making a profit from them clicking on the ads. Even though adware doesn't try and damage a computer itself, there are versions of adware that will take a person using the computer to a website against their will and try to get them to download programs that contain another type of malware program that could cause damage to the computer. Often, adware is something that is wrapped up with a free program installed that the person downloading it doesn't realize is there. Laka (2022) explains how hard it is to measure security threats caused by adware and how the community is still debating over treating adware as a type of malware program. On mobile devices, many applications employ ads as their primary source of income and usually include adware in their free application download.

Malvertising

Malvertising is a malware program where cybercriminals have accessed an exploit in adware for a company. Companies use adware for their revenue and do not realize that their adware is being used to spread malware. Since it is spread this way, people are less likely to realize that they might be opening themselves up for a malware attack. According to Laka (2022), only a handful of users apply the same level of caution to ads displayed on legitimate and trusted websites. Cybercriminals can employ this type of malware program to redirect a person to a less protected website or even infect the browser directly.

Cryptojacking

Cryptojacking is a newer type of malware program. Since the rise of cryptocurrencies, people have become more invested in them. Some people employ computers or miners to find cryptocurrency and these systems take up a lot of resources and power. Cryptojacking is where a cybercriminal wants to make a profit from cryptocurrency but doesn't want to purchase the equipment or power to do so. Instead, they infect another person's system and employ it to mine

for them. The owner of the miner doesn't notice that they have been infected and won't be directly harmed but this does put more of a strain on the system's resources and will eventually decrease the capability of the system to mine for a cryptocurrency (Laka, 2022).

Spyware

Spyware is a type of malware program that's goal is to remain hidden on a machine and be employed for long periods. Spyware is used to try and collect personal and financial information and provide that to a cybercriminal who can exploit that information however they want. This malware program runs its function without the person infected ever noticing it happening. Laka (2022) tells us that spyware is often used in a type of reconnaissance phase for more sophisticated attacks to be more effective. Spyware can be used to access all types of systems such as webcams and microphones so that the cybercriminal can watch and listen to you inside of your home to then blackmail you.

Rootkits

Rootkits is a type of malware program that employs a set of tools to avoid detection from the infected system. Namanya et al. (2018) tell us how these tools are extremely advanced and complicated programs that are written to hide within legitimate processes on the computer that have been infected and because of that they are very invasive and almost impossible to remove. These Rootkits can take complete control over a computer system and obtain administrative privileges. Since these malware programs are so good at evasion, they make antivirus software ineffective in detecting and removing them, so it requires more of a manual effort to deal with

them. Some good ways to manually check are tracking computer systems' behavior for abnormal activities, storage dump analysis, and system file signature scanning (Namanya et al., 2018).

Keyloggers

Keyloggers are a type of malware program where the software is designed to watch and log anything that is inputted into the computer's keyboard (Dadkhah et al., 2014). They are also capable of taking an image from a user's computer and sending it through email. Cybercriminals use many different types of programming languages to make keyloggers. There have been multiple ways for preventing keyloggers from being made, but they are not always reliable. The best way to fight against them is to have up-to-date antivirus software that will be able to successfully detect and prevent them. Dadkhah et al. (2014) tell us, though, that there are keyloggers that exist that are named undetectable keyloggers that can pose an even greater threat.

Bots

Bots are a type of malware program that is designed to complete certain operations that it has been given. According to Namanya et al. (2018), the word bots come from robots that were created to administer chat channels of Internet Relay Chat. Some bots are used for legal purposes, but bots created by cybercriminals are made to create botnets. A botnet is defined as a network of host computers that are controlled by an attacker or botmaster (Namanya et al., 2018). This is essentially a computer becoming infected and being taken control of so that the bot can access any computers connected to the infected one. Then it will infect and take control of those creating a botnet. Namanya et al. (2018) tell us how bots are normally used as spambots to create DDOS attacks, webspiders to scrape server data, or distribute malware onto download

sites. To help defend against these, the CAPTCHA test was created to keep bots out and make sure that the user is human.

Mobile Malware

Mobile malware is a type of malware program that is used to infect mobile phones. These are new types of malware since smart mobile phones haven't been around for a long time. Wu et al. (2014) tell us about six types of mobile malware: User accesses a site, downloads malware, downloads fake security software, malware transfers funds, SMS malware, and QR code malware. The user who accesses a site is the type of mobile malware when a user enters their information onto a site, whether that be registering, logging in, or updating account information. If there is mobile malware on the phone then it can use this information to lock a user out and access their account. The download malware type of mobile malware is when an unsuspecting user downloads malware by accident from non-legitimate sites or even the play store. This type of mobile malware, once downloaded, can affect the mobile device by keeping it from booting up properly, causing the battery to drain quicker than normal, taking complete control of the mobile phone, and accessing the user's data.

The download fake security software type of mobile malware is when a user attempts to secure their phone to prevent malware but accidentally downloads a fake antivirus that is mobile malware in disguise. The mobile malware also disables any other type of antivirus on the mobile phone, thus making it extremely difficult to remove. According to Wu et al. (2014), fake antivirus software is one of the biggest threats to mobile devices. Cybercriminals implant mobile malware into legitimate software and, like ransomware, force the user to pay money to fix the mobile phone. The malware transfer funds type of mobile malware is where a cybercriminal employs the information taken from a user logging onto some type of financial platform and

taking funds from them. A lot of times the cybercriminal will empty the user's bank account. The issue became more difficult to fix when the information was sent out employing a mobile phone (Wu et al., 2014). SMS malware is like a phishing email where a random message is sent to the user's mobile device asking them to click on links and input their information. Mobile SMS is one of the most used functions on a mobile device (Wu et al., 2014). The QR code malware type of mobile malware is when a user scans a QR code and does not realize that the image has links to sites that contain hidden malware in them. These sites can then download malware onto the user's mobile device without them ever knowing.

Malware Mechanisms

Modifying Registry Keys

The registry in a computer is a main part of the Windows operating system. The registry is a type of hierarchical database that is divided into hives. This database is used extensively by administrators and can be a helpful tool. Since it has so much power in what it can do, cybercriminals take advantage of it to perform attacks. Rothman (2017) tells us how a growing tactic among cybercriminals is to use registry keys to store and hide next-step code for malware to employ after it has been dropped onto a computer system. Also, this malware makes use of Windows administrative tools to complete its tasks, thus making it difficult to detect with regular antivirus software. The malware could query the Windows registry to figure out if there are any remote access tools installed on the computer such as TeamViewer, VNC, or Terminal Services.

Then the malware program could employ these as tools to increase its spreading capability and locate more valuable information.

Run/RunOnce Keys

When a malware program has already infected a computer, it will employ persistence mechanisms to guarantee that resources are available. The malware program will create shortcuts into the startup folder of a computer causing Windows to launch the program every time a user logs onto the computer. According to Rothman (2017), if this method of persistence is successful, then the malware will continue to execute its code to make sure advertisement sites are hit, command and control servers are beaconed, or to constantly try to have the user click on popup windows that could be for any number of purposes.

BootExecute Key

When a computer starts up, a process known as the Session Manager is the first one to start. With it starting before the Windows Subsystem started, it can't use the standard Windows API functions and so it applies the native API instead. Doing this makes the configuration manager subsystem boot the hives in the registry. Langendorf (2013) tells us that the Session Manager will load any programs that it finds in this registry key and that the only one that should be in there is "autocheck autochk*" which runs an auto-check during the boot process. Thus, if you see other entries that shouldn't be there then they are more than likely malware programs that have been inserted into the BootExecute key process and will start every time the computer is booted.

Keys Used by WinLogon Process

The WinLogon process is the final step when reading the disk hives, which occur while loading a user's settings during login. Like the BootExecute key, the WinLogon keys can be

manipulated to run malware programs each time a user logs into a computer. Uroz and Rodriguez (2019) explain that the system program that is launched by the WinLogon process is “userinit.exe” and is maintained in a registry key value. Since the registry keys can be changed with high enough privileges, the programs in the WinLogon process can be changed as well to be used by cybercriminals.

Startup Folder

The Startup folder is a special Windows folder that contains all the programs and application shortcuts that are to be launched during the startup process on a computer (Uroz & Rodriguez, 2019). This folder acts like run keys where it has two separate types of configurations by having different root folders. One folder is employed when the user logs in with that account and the other is employed for all users, no matter who logs into the computer. The level of privileges that the programs in these folders have is equal to the level of the user that is signed in.

Services

Windows services are background programs that do not need user interaction (Uroz & Rodriguez, 2019). These services are started when specific conditions are met. Services are normally employed by device drivers for them to communicate with hardware in the computer. Windows services are required to implement functions that are given by the Service Control Manager, which is the process in Windows that controls managing the stopping and starting of services. Services are also executed by employing administrative privileges which are also needed when a user creates a new service for the computer.

Browser Helper Objects

Browser Helper Objects are DLL files that work as plugins for the Internet Explorer browser and they need to register themselves as a COM server placing their CLSID in the

Windows registry (Uroz & Rodriguez, 2019). When a computer boots up, Internet Explorer starts all of the registered Browser Helper Objects so that the extensions can begin to interact freely. Remember that the privileges needed to edit the Windows registry are those of the administrative level. The privilege level that the Internet Explorer browser has is the same as the user who started the program.

AppInit DLLs

AppInit DLLs are a Windows feature that allows any DLL to be loaded into the address space of any application with a user interface, which is an application that loads "user32.dll" (Uroz & Rodriguez, 2019). Thus, this feature can be employed by cybercriminals to make it so that the DLL is loaded with all the interactive applications that are opened. This feature is also located inside of the Windows registry and has a value that contains all of the DLLs, that are to be loaded, full paths. Once again this requires administrative privileges to change, but the permissions for any executions are inherited from the specific applications that start the specific DLL needed.

File Extension Hijacking

The file extension hijacking attack consists of changing the default program associated with certain file extensions, such as .txt, .docx, .pdf, etc., to a different program (Uroz & Rodriguez, 2019). Because of this, the malware program will be launched whenever the user opens this type of file. The list of programs and their file extension associations are kept in the

Windows registry. This also requires the administrative level to change and the programs that have been launched by the user only have the privileges of that user.

DLL Hijacking

DLL hijacking attacks are when a cybercriminal takes advantage of the DLL search order done by Windows (Uroz & Rodriguez, 2019). The search that Windows conducts to find the necessary DLL dependencies starts with searching inside the working directory. If the DLL needed isn't found there, it will move on to a search inside the system directory. If it still hasn't been found it will move on to the 16-bit directory then to the Windows directory, then the current directory, then finally the directory that is defined within the PATH environment variable. According to Uroz and Rodriguez (2019), the problem lies with the fact that any of the legitimate DLLs in these directories can be switched out with an infected DLL and thus will be loaded anytime a program needs that specific dependency DLL loaded.

Antivirus Software

Definition of Antivirus Software

Antivirus software is a security measure and protection tool that is used against malware with the job of scanning, detecting, and preventing them (UK Essays, 2022). Antivirus software is a program that should be installed on all computers and networks because of the need to prevent malware from infecting and spreading. These programs provide tools that give real-time, on-access, and on-demand protection of personal information on a computer. There are many types of antivirus programs and they can work differently from each other. The antivirus software could be installed as a standalone program or it could be wrapped into a bundle of

programs. There is antivirus software for multiple versions of operating systems such as Windows 32 and 64-bit, Linux, and Mac.

Once the antivirus program has been installed onto a computer, it will begin tracking all of the activity that is happening within the system by viewing files that are being accessed, transferred, or stored to or from storage devices both within and outside the computer. Even files that have been downloaded from the internet will be scanned by the antivirus program to guarantee their safety. UK Essays (2022) tells us that if any type of suspicious activity is detected by the antivirus program, then it will automatically remove the file or stop the processes that are potential risks to your computer system, contacts, or other computers and devices in and on your network. There are several types of methods of detection that antivirus programs employ to identify malware, but the most utilized type of detection method is called heuristic analysis and is performed using traditional signature-based virus detection. However, Newman (2022) tells us how the main weakness of virus signatures as a protection method is the antivirus's inability to detect novel threats and that the advancement of cyber threats relying only on signatures has become an antiquated way of providing protection.

Key Performance Indicators

Key performance indicators are used to determine the performance and effectiveness of antivirus software (Patil, 2014). With there being so many different types of antiviruses as well as different types of malware, it has become necessary for a way to be able to grade antivirus software to help determine which one is best for your needs. Different key performance indicators include virus definition updates, antivirus upgrades, on-access scanner, on-demand scan, scheduled scanning, auto-clean infected file scanning, scanning of compressed files, file sharing shield, email shield, heuristic analysis, IM shield, script shield, web shield, antivirus

technical support, and password protected settings. With all of these key performance indicators, we can be at ease with the antivirus software that we decide to utilize.

Virus Definition Update

Since people use the internet daily to download files that could be a type of malware program, it is best if everyone installed antivirus software on their devices. This software needs to be able to perform virus definition updates, which are updates that are installed on a person's electronic device so that the antivirus software is up to date with the latest malware threats (Patel, 2014). With the updated information, the antivirus software is then able to watch out for the new malware it has been given information on. The only time this isn't effective is for zero-day malware programs that are so new that there is no virus definition update to install yet.

Antivirus Upgrades

There are many free types of antivirus software available to install, but many of them are limited in their abilities. Sometimes it is necessary to upgrade an antivirus software to a version that can include a feature or ability that is needed by yourself or a company. Also, antivirus software can provide upgrades at no additional cost that come as an update to the program itself and not just a virus definition update (Patil, 2014).

On-Access Scanner

The on-access scanner is a feature of antivirus software that is used to scan files and folders as they are being accessed to be able to identify a malware infection (Patil, 2014). For the on-access scanner to work correctly, the scanner must run constantly in the background of the

computer. It does employ more resources for its use, but it is a fair trade for constant security running on your devices.

On-Demand Scan

The on-demand scan feature of antivirus software is similar to that of the on-access scanner. However, the on-demand scan isn't running constantly but instead is used to scan certain folders and files of a drive whenever you need to (Patil, 2014). This is normally employed when someone has suspicions that there may be a malware program on their device or located in certain folders or files. Once the scan has been completed, the antivirus software will notify the user that all is good or provide a list of discovered malware programs.

Scheduled Scanning

Scheduled scanning is as the name implies when a user schedules the antivirus software to scan the computer. The user can assign a certain time of day to scan or even specific days of the week or month. The user can also tell the antivirus program to scan automatically whenever the device is restarted before the operating system comes up (Patel, 2014).

Auto Clean Infected File Scanning

Auto-clean infected file scanning is a feature of antivirus software that scans any type of removable storage devices, such as USB flash drives or external hard drives (Patel, 2014). This feature is a good way to secure your device from someone walking up and plugging in a storage device without your knowledge. Some cybercriminals employ the usage of removable storage

devices that contain malware programs capable of launching automatically once inserted into the system or when a device restarts, a removable storage device can take over the computer.

Scanning of Compressed Files

When needing to send large files that an email provider doesn't support, it can be helpful to compress the files into a folder to make it a size that the email provider will accept. When receiving a compressed folder, it is difficult for a user to determine what is contained in the compressed folder or if it is infected with malware. The scanning of compressed files feature of antivirus software is a way to extract and scan the files of the folder in multiple layers of compression (Patel, 2014). Most antivirus software with this feature can support a large variety of different types of compression and encoding formats.

File Sharing Shield

File sharing shield is an antivirus software feature that is similar to the scanning of compressed files where when a file is downloaded from any type of common file-sharing program it is then scanned for any type of malware program (Patel, 2014). People fall prey to infected files that are downloaded from the internet either because they are unaware of the danger or because they do not have the necessary protection employed to detect and prevent any threats posed to their system.

Email Shield

An email shield is a feature of antivirus software that acts like a mail server where it scans incoming and outgoing emails between users and systems and will detain and quarantine any messages deemed to be carrying malware programs harmful to the user or their systems

(Patel, 2014). This feature helps defend against emails containing harmful attachments or phishing scams.

Heuristic Analysis

Heuristic analysis is an antivirus software feature that is employed to take unknown or suspicious objects and evaluate them by simulating the behavior they would conduct within a secure and safe virtual computer environment (Patel, 2014). With this feature, the antivirus software can detect a malware program that hasn't yet been included in the antivirus software's database.

IM Shield

IM shield is a feature of antivirus software that works somewhat the same way as scanning compressed files and file sharing shield, where it will scan any file that is downloaded by an instant messenger or chat program (Patel, 2014). When chatting with people inside online chat rooms or over instant messenger programs, you don't always know who the person is on the other end. They could end up being cybercriminals, that are attempting to get you to download a file they have sent over messenger. The IM shield will scan these files and alert the user if there is anything malicious contained within.

Script Shield

The script shield feature in antivirus software helps detect and prevent malware scripts from running on a user's computer without their knowledge. This feature can detect and prevent scripts that come from the internet remotely and also scripts from other sources via web pages that have been saved to the local disk or within the browser's cache file (Patel, 2014). Scripts can

be inside of many different file types and written in many different programming languages, and having up-to-date antivirus software with a script shield will help protect against these threats.

Web Shield

The web shield feature of antivirus software is similar to that of the script shield. This feature helps defend your system from malware programs while you browse the internet and will detect and block any known or unknown potential threats that may come from the internet via hacked websites that are infected with malware scripts (Patel, 2014). While browsing the internet, some sites can have adware which we discussed earlier that can reroute your browsing to harmful sites filled with malware.

Antivirus Technical Support

The antivirus technical support feature that comes with antivirus software includes a team of experts on the antivirus software and will support users by verifying that the antivirus software is up to date, making sure the system is not infected with any viruses or malware programs, and guarantee the system is secured (Patel, 2014). Many antiviruses include this type of support and they are usually available around the clock.

Password Protected Setting

The password-protected setting in antivirus software is where the software itself is protected by a certain password that the user will be required to enter when attempting to activate the antivirus software or trying to gain access to certain sensitive parts of the software (Patel, 2014). With this extra layer of security, it makes it more difficult for a cybercriminal to attempt

to disable antivirus software to prevent it from detecting any malware they are trying to attack the system with.

History of Antivirus Software

Early Days of Antiviruses

According to UK Essays (2022), there are many competing claims for the innovator of the first antivirus product but the first publicly documented removal of a computer malware program in the wild was done by Bernd Robert Fix in 1987. He created a fix that was used to counter the Polish MKS virus named “Vienna”. That same year, a company from Germany named G Data Software AG created and released the first antivirus software that was employed on Atari ST computers and then followed that up with the “Ultimate Virus Killer 2000.” (Terekhov, 2019). Also, in 1987 the company McAfee, Inc. was founded and by the end of the year would have released the first version of their antivirus software named “VirusScan”. When the “AIDSTEST” virus toolkit came out in 1988, the antivirus “AntiVir” was also released by another German company named Avira. A Czech cybersecurity company named Avast would also release its version of an antivirus software known as “Avast Antivirus” and one of the first virtual private networks called “Avast SecureLine VPN”. That same year, the antivirus program “V1” was released by its creator, Dr. Ahn Chul Soo from South Korea. In 1990, the Computer Antivirus Research Organization was created to research and study malware (Terekhov, 2019). In 1991, the company Symantec released the well-known antivirus software “Norton AntiVirus” and the Dutch cybersecurity company AVG Technologies was founded and created the antivirus

software known as “AVG AntiVirus” in the year 1992. Then, near the end of the 1990s, nineteen different antivirus programs were available.

Terekhov (2019) tells us how in 1988 the antivirus software “Kaspersky Anti-Virus” created by Kaspersky Lab, was the only one that could detect and remove the “Chernobyl” malware virus that was released in Taiwan by a student at Tatung University. Some of the contributors to the early creation of antivirus software and programs were Fred Cohen, Peter Tippett, John McAfee, Eugene and Natalya Kaspersky, Alan Solomon, Vesselin Bontchev, Ross Greenberg, and Erwin Lanting. UK Essays (2022) tells us how before the internet was widespread, the malware was usually spread using floppy disks with malware on them and that antivirus software was used but wasn’t updated often, so it was forced to check executable files and boot sectors of floppy disks. When the internet became more commonly used by people, malware began to spread through it instead.

Next-Generation Antivirus Software

With the constant advancement of malware, cybercriminals are creating the simple processes of the past where antivirus programs used to detect malware are no longer good enough to combat the newest threats. Cybersecurity teams and cybercriminals are still constantly battling it out by creating new malware and new antivirus software. Because of this, people need to be more proactive and less reactive in detecting and preventing malware attacks. Cybersecurity teams have developed what is called next-generation antivirus software. Newman (2022) explains how traditional antivirus software of the past would protect against threats that could be seen and how next-generation antivirus software can protect against a whole group of behaviors that a malware program exhibits. Old antivirus software employs people to watch out

for malware programs, but with the number of systems available and malware becoming more intricate cybersecurity needs to change its ways.

Next-generation antivirus software employs what is called predictive analytics and is driven by machine learning and artificial intelligence to be able to detect and prevent malware programs (Newman, 2022). Machine learning and artificial intelligence are way better than just relying on people. With these tools, an antivirus program will be able to identify and tag the virus as well as anything that is part of that family of viruses. Also, next-generation antivirus software learns about how the virus works and the objectives it has so that it can protect against them in the future. In 2005, a company in Finland named F-Secure created an anti-rootkit tool named “BlackLight”. It was the first cybersecurity company to do this. In 2008, McAfee released a new addition to their “McAfee VirusScan” software named “Artemis”. This was a cloud-based antivirus software, and in 2011 AVG created its cloud-based software named “Protective Cloud Technology” (Terekhov, 2019).

Creation of EDR and XDR

After antivirus software had begun to use machine learning and artificial intelligence, a new type of protection arrived called endpoint detection and response. According to Newman (2022), endpoint detection and response was created by Anton Chuvakin of Gartner in 2013 and since then has been a prerequisite of today’s cybersecurity software. Endpoint detection and response is a method of analyzing the behaviors of what is happening on an endpoint, which is anything from a laptop, desktop, mobile phone, or tablet. While doing this, it creates investigations across utilities and detects and prevents actions and malware from cybercriminals. Eventually, endpoint detection and response further evolved and created extended detection and response which took the focus from just looking at endpoints and instead tracking an entire

network system (Newman, 2022). With extended detection and response, cybersecurity can have more of a holistic view of possible malware attacks across a large area of technology devices, thus cutting out the intermediary and providing an improved version of protection, detection, and response capacity.

Types of Antivirus Software

Antivirus software is divided into four different levels of value, which are free, paid, suites, and premium suites. The difference between the four is the features that are available to the user, with free having the least number of features and antivirus premium suites having the greatest number of features. According to Thomas and Nachamai (2017), free antivirus software provides bare-bones, low-level protection that only scans for malware and can perform automatic virus scans. Most free antivirus software doesn't offer any additional protection or technical support. Paid antivirus software is in the middle between free and suite. This provides additional features such as parental controls and identity theft protection, which are good security tools that are not offered in free versions.

Suite level of antivirus software contains more features than paid level such as firewalls and system performance tools (Thomas & Nachamai, 2017). Some popular antivirus software out there are Norton, McAfee, Bit Defender, Avira, and Avast. Norton is known for its feature of running updates every ten to fifteen minutes, so the software is up to date with the latest threat signatures. McAfee includes a firewall feature that helps prevent cybercriminal attacks and protects against spyware and viruses. Bit Defender has a greater ability to defend a computer from spyware, viruses, and rootkits. The software also has an anti-phishing service feature. Avira created Avira Protection Cloud, which employs information from the internet to improve the detection of threats and employs less power from the computer. Avast is one of the most popular

antivirus software available and has the greatest market share for malware applications. The free version of Avast includes a ton of features for users to employ such as Avast Passwords, anti-spyware, streaming update, Secure HTTPS scanning, Home Network Security scanner, Site Correct, Do Not Track, anti-malware, Smart Scan, Rescue Disk, anti-phishing, and Software Updater (Thomas & Nachamai, 2017).

Cryptographic Defenses

Definition of Cryptographic Defenses

Cryptography is defined as the science of secret writing (Maqsood et al., 2017). The word cryptography derives from the Greek words kryptos, which means hidden, and graphein, which means writing (Naser, 2021). Cryptography has been around since 1900 B.C. during the time of the Egyptians. Kessler (2022) tells us that some experts argue that cryptography came about after the creation of writing. Cryptography performs a critical part in making sure there are secure communications from one device to another. With how unsecure the internet and other networks are, cryptography is a necessity within data and telecommunications. Encryption and decryption are the main functions of cryptography at a basic level (Maqsood et al., 2017). When diving deeper into cryptography, the five main functions of cryptography are Privacy/Confidentiality, Authentication, Integrity, Non-repudiation, and Key Exchange (Kessler, 2022).

Privacy/Confidentiality is the function of making sure that no others can read a message except for the specific receiver. Authentication is the function of having to prove your identity to be authorized. Integrity is the function of promising the intended receiver that the message they have received has not been changed from the original. Non-repudiation is the function of

providing proof that the person who sent the message is the actual person and no other. Key Exchange is the function where crypto keys are exchanged between the sender and receiver.

Cryptography starts using unencrypted data known as “plaintext” and then encrypts the data into what is called “ciphertext” that will then be decrypted back to the “plaintext” (Kessler, 2022). Some other functions of cryptography are Forward Secrecy, Perfect Security, and Deniable Authentication. Forward Secrecy is a feature that defends old encrypted sessions from attacks regardless if the server that the session is on has been compromised. This is performed by having separate keys for each session.

Perfect Security is a system that is known to be unbreakable, and also the “ciphertext” does not show any information on the “plaintext” or any key. For this Perfect Security to be accomplished it requires that the key contain as many characters as the “plaintext” which causes analysis and brute force to be ineffective. Deniable Authentication is a way that users during an exchange of messages can be confident of the authenticity of the messages. Cryptography is associated with mathematical algorithms that are used to encrypt and decrypt messages, while “cryptanalysis” is the science of analyzing and cracking encryption schemes. Cryptology is the term for the broad study of secret writing which encompasses both cryptography and cryptanalysis (Kessler, 2022).

History of Cryptographic Defenses

Ancient Cryptography

As stated before, the earliest known cryptography was in 1900 B.C. written by Egyptian scribes who made use of hieroglyphs differently from normal to keep the meaning hidden (Naser, 2021). The Greeks had a version where they would take the tape and wrap it around a stick and write a message along the tape. When someone would unravel the tape, the words

would make no sense unless you had the other stick of the same diameter that would be able to decipher the message. This method was called the "Scytale" of Sparta, which is thought to have been employed by the Spartan military (Naser, 2021). The Romans had a method that was called the "Caesar Shift Cipher" that would take the idea of moving letters around by a certain number to write out the message. Then the receiver would reverse the operation to decrypt the message (Damico, 2009). The earliest known cipher within the Hebrew language was called the "Atbash" (Naser, 2021). In India, they employed two different kinds of ciphers known as the "Kautiliyam" cipher and the "Mulavediya" cipher. The "Kautiliyam" was constructed on phonetic relations, while the "Mulavediya" was constructed using pairs of letters and using reciprocal ones.

Middle Age-20th Century Cryptography

Cryptography did not see any major evolutions or advancements until around the time of the Middle Ages. Most of the western European countries were employing some type of cryptography. Leon Battista Alberti also known as "The Father of Western Cryptology," created the polyalphabetic substitution method of using two copper disks that would join, and the alphabet engraved upon them (Damico, 2009). This worked by every few words the disks would be rotated to alter the encryption logic, thus making using frequency analysis to crack the cipher all but useless. Employment of this style of cryptography was being used even during the Civil War, where the South would utilize brass disks to encrypt but the North would often crack the messages.

Naser (2021) tells us that Leon Battista Alberti was the first to invent an automated cipher device that was employed using the wheel. The "Vigenere" cipher was a polyalphabetic cipher created by Blaise de Vigenere. A man named Gilbert Vernam worked to evolve the cipher to make it more effective and created the Vernam-Vigenere cipher in 1918. Another type of

cryptography was employed by a group called the “wind talkers.” These were Navajo people who utilized their language as a method for cryptography (Damico, 2009). The method and code they used were never cracked and were an important instrument for victory in the Pacific Theater during World War II. Also, during World War II, the “Enigma” machine was employed by German soldiers to communicate confidential data between Nazi soldiers. The “Enigma” machine was created by Arthur Scherbius near the end of World War I (Naser, 2021).

Modern Cryptography

Cryptography today employs a public key method that makes use of a common public key and a private key that only the sender has to create a type of asymmetric encryption (Damico, 2009). This works by a sender of a message employing a private key to encrypt their message, and then whoever is to receive the message employs a public key to be able to decipher it. With this, the receiver will be able to determine whom the message came from. This form of cryptography is what makes up most of Digi Signatures. The idea of the digital signature was first introduced by Diffie-Hellman in a paper titled “New Directions in Cryptography” (Naser, 2021). Damico (2022) tells us that there can be issues with this when multiple organizations sending communications require multiple different public keys and need to know which one is needed.

Types of Methods

Symmetric and asymmetric are largely accepted versions of cryptography (Maqsood et al., 2017). Symmetric focuses on making sure there is secure communications between users by employing the same secret key. Asymmetric cryptography secures communication by employing both public and private keys. Private keys are known to certain individuals, while public keys are known by all. Key size is important in symmetric and asymmetric cryptography, with the key

size of symmetric being less than asymmetric. This also means that symmetric cryptography is less secure. The time it takes to compute asymmetric cryptography is greater than that of symmetric cryptography, which causes the encryption and decryption to become more complex for huge amounts of data. This computational time is broken down into classifications of encryption/decryption time, key generations, and key exchange time (Maqsood et al., 2017).

Encryption/decryption time is determined by how long it takes to convert "plaintext" into "ciphertext" and vice versa. Key generation time is determined by using the length of the key, which as discussed is different between symmetric and asymmetric cryptography. The key exchange time is determined by the time it takes to send the communications between the sender and receiver. There are multiple different ways to classify cryptographic algorithms. They are mostly categorized by the number of keys that are needed for encryption and decryption, and then they are subcategorized by their use and application. Three different types of algorithms are Secret Key Cryptography, Public Key Cryptography, and Hash Functions (Kessler, 2022).

Secret Key Cryptography

Secret key cryptography is the method of employing one key for encryption and decryption (Kessler, 2022). With this, the sender uses a key that will encrypt the plaintext and then sends the new ciphertext over to the receiver. Then the receiver uses the same key to be able to decrypt the message back over to plaintext. With this method only employing one key, it is also known as symmetric encryption. With secret key cryptography, the key needs to be known by the sender and the receiver, but the issue is how to distribute the key. The schemes of secret key cryptography are normally categorized as stream ciphers or block ciphers (Kessler, 2022).

Stream Ciphers. Stream ciphers work with a single bit at a time and also employ a feedback mechanism to be able to keep the key always changing. There are multiple types of

stream ciphers, but two important ones according to Kessler (2022) are self-synchronizing stream ciphers and synchronous stream ciphers.

Self-synchronizing Stream Ciphers. Self-synchronizing stream ciphers calculate every bit within a keystream as a function of an *n-bit* that came before in the keystream. The reason it is known as "self-synchronizing" has to do with the fact that the decryption process can maintain synchronization with the encryption process because it knows where it is in the n-bit keystream. Kessler (2022) tells us that a problem with this is error propagation, which is where a garbled bit in the transmission will cause *n-bits* to be garbled on the receiving end.

Synchronous Stream Ciphers. Synchronous stream ciphers work by generating a keystream that is independent of the message stream but employs the same keystream generation function at both the sender and receiver. Stream ciphers do not propagate transmission errors, but they are periodic, so the keystream will eventually repeat (Kessler, 2022).

Block Ciphers. Block ciphers are a method where one block of data of a certain size is encrypted one at a time. Kessler (2022) tells us how in a block cipher a plaintext block will always encrypt to the same ciphertext when employing the same key, unlike stream ciphers that would encrypt into a different ciphertext. The most used construct employed to block encryption algorithms is the Feistel cipher, which is named after the cryptographer Horst Feistel (Kessler, 2022). Feistel ciphers blend substitution, permutation, and key expansion to build confusion and diffusion within the cipher. One perk from the Feistel cipher construct is that the encryption and decryption are almost identical and thus only require the key operation to be reversed, which greatly lowers the size of the code or circuitry that is required to employ the cipher for either software or hardware. Block ciphers run in different modes such as Electronic Codebook Mode,

Cipher Block Chaining Mode, Cipher Feedback Mode, Output Feedback Mode, and Counter Mode.

Electronic Codebook Mode. Electronic Codebook Mode is considered the easiest of applications. The secret key is employed to encrypt the plaintext block into a ciphertext block and identical plaintext blocks will create identical ciphertext blocks. Kessler (2022) explains how this mode is vulnerable to brute-force attacks, deletion attacks, and insertion attacks, and is also vulnerable to the possibility that a single-bit error during the transmission of ciphertext will cause an entire block of decrypted plaintext to be in error.

Cipher Block Chaining Mode. Cipher block chaining includes a feature of a feedback mechanism to the encryption design. With this mode, a plaintext is exclusively ORed to the ciphertext block from before. This is done before the encryption to allow identical plaintext blocks to encrypt, in different ways from each other. According to Kessler (2022), this mode does well in protecting against brute-force, deletion, and insertion attacks but a single bit error within the ciphertext will create an entire block error within the decrypted plaintext block and create a bit error in the next one as well.

Cipher Feedback Mode. Cipher feedback is a block cipher implementation as a self-synchronizing stream cipher (Kessler, 2022). This mode encrypts data into smaller units compared to block size, which can be advantageous to some applications. Cipher feedback mode creates a keystream molded after the previous ciphertext. A single-bit error can cause the ciphertext block and the one after to have an error.

Output Feedback Mode. Output feedback is a block cipher implementation that is similar to the synchronous stream cipher (Kessler, 2022). This mode keeps the same plaintext block from creating the same ciphertext block by employing the internal feedback mechanism that

creates the keystream by itself. A single-bit error within a ciphertext in output feedback mode will cause the decrypted plaintext to have a single-bit error as well.

Counter Mode. Counter Mode is a newer type of block cipher. This mode works on blocks within a stream cipher like cipher feedback and output feedback, but it also works on the blocks independently, like an electronic codebook (Kessler, 2022). Counter mode is different from the electronic codebook because it employs different key inputs to different blocks to ensure that two identical plaintext blocks will not turn into identical ciphertext blocks. Kessler (2022) also tells us that this mode allows blocks to be processed in parallel, which provides performance advantages when parallel processing and multiple processors are available. Also, this mode is not vulnerable to brute-force, deletion, or insertion attacks like electronic codebooks.

Public Key Cryptography

Public key cryptography has been said to be the most significant new development in cryptography within the last 300-400 years (Kessler, 2022). This type of cryptography relies on the existence of what is called one-way functions. Public key cryptography employs using two keys that are related to each other through mathematics. Knowing about one of the keys does not make figuring out the other easy. One of the keys is employed to encrypt the plaintext, while the other is employed to decrypt the ciphertext. The process does not care which key is applied at the beginning as long as both keys are employed. Since this process requires two keys, it is also called asymmetric cryptography (Kessler, 2022).

Hash Functions

Hash functions, also known as message digests or one-way encryption, are algorithms that do not use a key but instead employ a fixed-length hash value that is computer-based upon

the plaintext (Kessler, 2022). This makes it impossible for anyone to discover the contents or length of the plaintext. Kessler (2022) explains that hash algorithms are normally used to provide a digital fingerprint of a file's contents to ensure the file has not been changed in any way by a cybercriminal or virus. This type of cryptography is also employed by operating systems to be able to encrypt passwords.

Firewalls

Definition of Firewalls

A firewall is defined as a cybersecurity tool that monitors incoming and outgoing network traffic and permits or blocks data packets based on a set of cybersecurity rules (Kanade, 2022). Firewalls are employed to protect network nodes from data traffic coming in and out or even certain applications. They are employed utilizing software, hardware, or cloud-based methods to defend a network against malicious attacks. Kanade (2022) explains that firewalls examine inbound traffic based on predefined security rules, and they also filter traffic coming in from unsecured or untrustworthy sources to defend and prevent attacks. The traffic is filtered at the computer's entry points called ports. This is where the data is exchanged with other devices.

The operation of firewalls can be understood by using the analogy of IP addresses being houses and port numbers as rooms within the house. The only people allowed inside the house are those that are trusted. Within the house, trusted people are filtered and restricted further from moving around the rooms. Visitors are allowed to enter certain rooms depending on their access.

The owner can go into all of the rooms. This is how a firewall works once installed onto a network.

Key Components of a Firewall

The architecture of firewalls is constructed using four primary components. Those components are Network Policy, Advanced Authentication, Packet Filtering, and Application Gateways (Kanade, 2022).

Network Policy. Network policy impacts the installation, design, and use of firewalls within a network and it is broken into two levels: higher-level policy and lower-level policy. The higher-level policy outlines the services that are permitted or denied from a controlled network, how they would be employed, and any exceptions to the policy. The lower-level policy reveals exactly how the firewall will control access restrictions and service filtration specified within the higher-level policy (Kanade, 2022).

Service Access Policy. The service access policy concentrates on internet-specific usage issues and any outside network admissions. For the firewall to function properly and be successful, service access policy requires realism and soundness before employing the firewall itself. A realistic policy maintains a balance between allowing users access to the network and defending the network from risks. Kanade (2022) tells us that firewalls can employ many service access policies. Firewalls employ service access policies to permit user access from the internet to an internal host, but only if this access was required and if it could be joined with advanced authentication.

Firewall Design Policy. The firewall design policy is explicit to the firewall and outlines the rules employed to execute the service access policy. The policy cannot be designed within a void secluded from comprehending firewall capabilities and restrictions and any threats and

susceptibilities associated with TCP/IP (Kanade, 2022). Firewalls employ one of two types of design policies: permit and deny. The permit allows a service unless it has been restricted. Deny blocks a service unless it has been given permission.

Advanced Authentication. Advanced authentication is employed by using smart cards, biometrics, authentication tokens, and software-based mechanisms and is utilized against easily broken traditional passwords. These techniques are similar to each other because any password that is generated by the advanced authentication devices is unable to be used again by a cybercriminal who may have been watching the connection. Kanade (2022) tells us how the more popular advanced authentication devices employed today are called one-time password systems.

IP Packet Filtering. IP packet filtering is the process of employing a packet-filtering router to filter packets when they cross between a router's interface. Packet-filtering routers can filter IP packets centered on the source IP address, destination port, TCP/UDP source port, or destination IP address (Chopra, 2016). According to Kanade (2022), not all packet-filtering routers currently filter the source TCP/UDP port. Some routers are capable of analyzing which of the router's network interfaces a packet arrived at and then employing that as another filtering criterion.

Application Gateways. To fight the vulnerabilities associated with packet filtering routers, firewalls require employing software applications to filter and forward connections for

services such as FTP and TELNET. These applications are known as proxy services, while the host that is employing the proxy service is known as an application gateway (Kanade, 2022).

History of Firewalls

Firewalls in the past were not difficult to maintain and support because they dealt with fewer internet services at the time. Chopra (2016) explains how today firewalls don't only need to secure Telnet, FTP, SMTP, and USENET but now need to secure WWW, file sharing, news, music, audio, videoconferencing, database access, and whatever else people are trying to connect to. The first firewalls appeared in the 1980s and those were mostly routers employed to separate networks into smaller LANs. The first security type of firewall was employed in the 1990s and those were IP routers that contained filtering rules. Later, security firewalls were constructed on the concept of the Bastion Host, which is a special-purpose computer on a network that is specifically designed and configured to withstand attacks (Chopra, 2016). They were more updated and skilled and were some of the first commercially available firewalls. In 1992, Bell Labs was testing out circuit-relay-based firewalls that could provide a secure network connection between internal and external devices. In 1993, the Trusted Information System Firewall Toolkit was created and released as a source code for everyone on the internet to use. In 1994, Firewall-1 was created and brought user-friendliness by having icons, colors, and mouse drivers. Firewalls before required editing of the files that created them.

Types of Firewalls

Host-based Firewalls

A host-based firewall controls incoming and outgoing packets by being installed on the network nodes. This type of firewall is a software application or suite that was included in the

installation of an operating system. These firewalls defend every host from malicious attacks and unauthorized access (Kanade, 2022).

Network-based Firewalls

Network firewalls as their name suggests work at the network level, employing multiple network interface cards. They filter incoming and outgoing traffic on the network by employing firewall rules. According to Kanade (2022), these network-based firewalls are typically dedicated systems with proprietary software installed. Five specific types of firewalls play important roles within network security and they are Packet Filtering Firewalls, Circuit-Level Gateway, Stateful Inspection Firewalls, Application-Level Gateway, and Next-Generation Firewalls.

Packet Filtering Firewall. Packet filtering firewalls works within junction points where other network devices work as well. These firewalls do not direct packets, instead comparing them to establish a criterion such as: allowed IP addresses, packet types, port numbers, and other packet protocol headers (Kanade, 2022). Packets seen as being an issue are dropped. Chopra (2016) also tells us that they only work on the network level of the OSI model and thus do not support intelligent rule-based models.

Circuit-Level Gateway. Circuit-level gateways supervise TCP handshakes and other network protocol session initiation messages along the network whenever they establish between local and remote hosts to figure out if the session is legitimate and whether the remote system is known to be trusted (Kanade, 2022). They do not examine packets, but they do provide a fast way to detect malicious content. According to Chopra (2016), they operated in the session layer of the OSI model.

Stateful Inspection Firewall. State-aware devices inspect every packet to be able to maintain track of whether that packet is with a known TCP or a different network session. This provides more security than just packet filtering or circuit monitoring, but it does require more resources from network performance (Kanade, 2022). Chopra (2016) also states that they have a momentous impingement on network performance. A different type of stateful inspection is a multilayer inspection firewall that watches the flow of transactions being conducted along many protocol layers of the seven-layer open systems interconnection model.

Application-Level Gateway. Application-level gateways are also called proxy firewalls and they blend a few features of packet-filtering firewalls with circuit-level gateway features. They filter packets based on the service they are meant for and specific characteristics (Kanade, 2022). They are also expensive and due to their complexity and less secure than simpler firewalls (Chopra, 2016).

Next-Generation Firewall. Next-generation firewalls blend packet inspection with stateful inspection along with some deep packet inspection and network security systems. Kanade (2022) tells us that packet inspection in conventional firewalls mostly looks at the protocol headers of packets. Deep packet inspection, on the other hand, looks at data that is being transported by the packet. Deep packet inspection firewalls monitor web browsing sessions and see if a packet payload establishes an authentic HTML format response.

Conclusion

There isn't any question that the number of malware and cybercriminals is rising. With more technology being created and almost all devices now having connections to the unsecure internet, the possibility of being attacked by some form of malware is great. There are no questions as to whether a person or company may be targeted by malware, but it's a matter of when that will happen. With that in mind, people and organizations need to be proactive and put malware defenses in place well before they are ever targeted. Many people, however, do not know the workings of malware or how to best detect and prevent it. Most organizations have some form of IT personnel who do know the importance and hopefully they are putting security in place to prevent a crippling business attack from occurring. Not only do people and organizations need to have firewalls, antivirus software, and cryptographic defenses, but they should also have a form of cybersecurity culture where everyone is practicing safe and secure methods. This is why it is important for people and staff to be educated on malware and how to best defend against it. There are plenty of training and educational videos on this subject because it is such a widespread issue. With this knowledge, people would be able to be more aware and see warning signs of any malicious activity, whether it be phishing or adware. Being knowledgeable and preemptively putting into place security defenses will help people and businesses keep their personal and confidential information private.

References

Arce, D. G. (2018). Malware and market share. *Journal of Cybersecurity*, *4*(1). https://doi.org/10.1093/cybsec/tyy010

Chopra, A. (2016). Security issues of firewall. *International Journal of P2P Network Trends and Technology*, *22*(1), 4–9. https://doi.org/10.14445/22492615/ijptt-v22p402

Dadkhah, M., Jazi, M., Ciobotaru, A.-M., & Barati, E. (2014). *An introduction to undetectable keyloggers with experimental testing*. ResearchGate. Retrieved September 28, 2022, from https://www.researchgate.net/publication/266743342_An_Introduction_to_Undetectable_Keyloggers_with_Experimental_Testing

Damico, T. M. (2009). A Brief History of Cryptography. *Inquiries Journal*, *1*(11), 1. https://doi.org/http://www.inquiriesjournal.com/articles/1698/a-brief-history-of-cryptography

Kanade, V. (2022, March 24). *What is a Firewall? definition, key components, and best practices*. Spiceworks. Retrieved October 21, 2022, from https://www.spiceworks.com/it-security/network-security/articles/what-is-firewall-definition-key-components-best-practices/

Kessler, G. C. (2022, October 1). *An Overview of Cryptography*. Gary Kessler. Retrieved October 19, 2022, from https://www.garykessler.net/library/crypto.html

Laka, D. (2022). Malware: Types, analysis and classification. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4036836

Langendorf, S. (2013, September 24). *Windows registry persistence, part 2: The run keys and search-order*. BlackBerry Blog. Retrieved October 3, 2022, from

https://blogs.blackberry.com/en/2013/09/windows-registry-persistence-part-2-the-run-keys-and-search-order

Namanya, A. P., Cullen, A., Awan, I. U., & Disso, J. P. (2018). The World of Malware: An Overview. *2018 IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud)*. https://doi.org/10.1109/ficloud.2018.00067

Naser, S. M. (2021). Cryptography: From the Ancient History to Now, It's Applications and A New Complete Numerical Model. *International Journal of Mathematics and Statistics Studies*, *9*(3), 11–30. https://doi.org/10.13140/RG.2.2.13438.51524

Newman, A. (2022, March 10). Council Post: How has antivirus software evolved, and where might the industry be heading*? Forbes*. Retrieved October 4, 2022, from https://www.forbes.com/sites/forbestechcouncil/2022/03/09/how-has-antivirus-software-evolved-and-where-might-the-industry-be-heading/?sh=4221afcb5e0f

Maqsood, F., Ahmed, M., Mumtaz, M., & Ali, M. (2017). Cryptography: A comparative analysis for modern techniques. *International Journal of Advanced Computer Science and Applications*, *8*(6). https://doi.org/10.14569/ijacsa.2017.080659

Milosevic, N. (2013). *History of Malware*. ResearchGate. Retrieved September 27, 2022, from https://www.researchgate.net/publication/235666537_History_of_malware

Patil, B., & Joshi, M. (2014). Usages of Selected Antivirus Software in Different Categories of Users in selected Districts. *Journal of Environmental Science, Computer Science and Engineering & Technology*, *33*(22), 801–807. https://doi.org/https://www.researchgate.net/publication/288725296_Usages_of_Selected_Antivirus_Software_in_Different_Categories_of_Users_in_selected_Districts

Rothman, A. (2017, April 20). *Windows registry malware attacks: Knowledge is the best defense*. Red Canary. Retrieved October 3, 2022, from https://redcanary.com/blog/windows-registry-attacks-threat-detection/

Saengphaibul, V. (2022, March 15). *A brief history of the evolution of malware: FortiGuard Labs*. Fortinet Blog. Retrieved September 12, 2022, from https://www.fortinet.com/blog/threat-research/evolution-of-malware

Terekhov, A. (2019, April 16). *History of the Antivirus*. Hotspot Shield VPN. Retrieved October 6, 2022, from https://www.hotspotshield.com/blog/history-of-the-antivirus/#:~:text=The%20beginnings%20of%20antivirus%20software,Ray%20Tomlinson%20developed%20the%20Reaper.

Thomas, R., & Nachamai, M. (2017). Performance investigation of antivirus - A comparative analysis. *Oriental Journal of Computer Science and Technology*, *10*(1), 201–206. https://doi.org/10.13005/ojcst/10.01.27

UK Essays. (2022, July 29). *History of antivirus software*. UK Essays. Retrieved October 4, 2022, from https://www.ukessays.com/essays/information-technology/history-of-antivirus-software.php

Uroz, D., & Rodríguez, R. J. (2019). Characteristics and detectability of windows auto-start extensibility points in memory forensics. *Digital Investigation*, *28*. https://doi.org/10.1016/j.diin.2019.01.026

Wu, F., Narang, H., & Clarke, D. (2014). An overview of mobile malware and solutions. *Journal of Computer and Communications*, *02*(12), 8–17. https://doi.org/10.4236/jcc.2014.212002