Evolution of Malware Threats and Techniques: A Review

Mohammed N. Alenezi [1], Haneen Alabdulrazzaq[1], Abdullah A. Alshaher[1] and Mubarak M. Alkharang[1]

[1]Computer Science Department, Public Authority for Applied Education & Training, Kuwait

Abstract: The rapid development of technology, and its usage, in our everyday lives caused us to depend on many of the aspects it offers. The evolution of the Internet in recent decades has changed human life drastically as accessing knowledge, communication, and social interaction, became readily available. Nowadays, we have become dependent on our PCs and smart devices in accomplishing everyday tasks. People are using these devices to store valuable information. This information became the target of cybercriminals who are constantly creating new ways to gain unauthorized access to it. In the past few decades, cybercrime and the construction of malicious software (malware), have seen a significant rise. In this research, we present a literature review of the historical evolution of malware. We describe the common characteristics and propagation methods for the types of malware in each phase of its evolution. Furthermore, we illustrate the purpose of its creation and the damages it has caused. The purpose of this study is to provide researchers with background about malware and its evolution leading up to present day threats.

Keywords: Malware, Cyber security, Ransomware, Rootkits, Worms, Trojans, Advanced Persistent Threat.

1. Introduction

In today's modern world, computers and their applications play a vital role in our everyday life. Computers help us store large amounts of data, accomplish our tasks quickly and accurately, and connect us with the rest of the world through the Internet. The evolution of the Internet in recent decades, changed human life drastically as accessing knowledge, communication, and social interaction, became readily available.

With the development of technology, computer usage and data storage have seen a significant rise. People, nowadays, are storing valuable information in their personal devices like PCs and smartphones. This information has to be secured against breaches and unauthorized access, especially when these devices are connected to the Internet.

A security breach or violation occurs when an individual or entity, succeeds in gaining unauthorized access to data and information that was protected. Nowadays, cyber threats are prevalent and cybercriminals are targeting both corporations and individuals. As a result, cybersecurity has become a priority for companies in order to guard their data and assets. Cybersecurity focuses on providing the necessary measures required to protect devices and networks from unauthorized access and attacks.

Cybersecurity is built on 3 principles; Confidentiality, Integrity, and Availability (CIA). Confidentiality guarantees that only authorized persons can access valuable information. It is implemented by utilizing mechanisms such as usernames, passwords, and access control lists. Integrity ensures that the information remains true to its origins and is only modified by authorized persons. This means that the information sent is the same as the information received and it is not tampered with during transfer or after reception. Integrity is mainly achieved through mechanisms such as encryption/decryption and hashing. Availability means that systems, data, and functions are available on demand. It is achieved by performing periodical hardware maintenance, software updates, and network optimization [1]. Today, cybersecurity has become an integral part in a company's organizational structure. Companies are constantly facing the threat of cybercrimes targeting their data with the intention of theft or sabotage [2]. In 2017, companies have spent around 34 billion dollars on cybersecurity solutions with a projected increase to 42 billion dollars by 2020 [3].

Malicious software, malware for short, is the collective name of a variety of hostile or intrusive software. Cybercriminals develop malware to steal data, bypass access controls, and gain access to a personal computer or to harm the target computer, its data, or applications. Nowadays the malware industry has become very profitable which attracted more efforts by cyber criminals and caused an exponential growth in the numbers, types, and complexity of malware created [4]. Moreover, generic anti-virus software alone is unable to detect malware mutations and its variants which makes the user and system vulnerable at any given time [5].

Malware is mainly divided into two categories: first-generation malware or static malware and second-generation malware or dynamic malware Malware is mainly divided into two categories: first-generation malware or static malware and second-generation malware or dynamic malware [6]. The different types of malware are shown in figure 1.

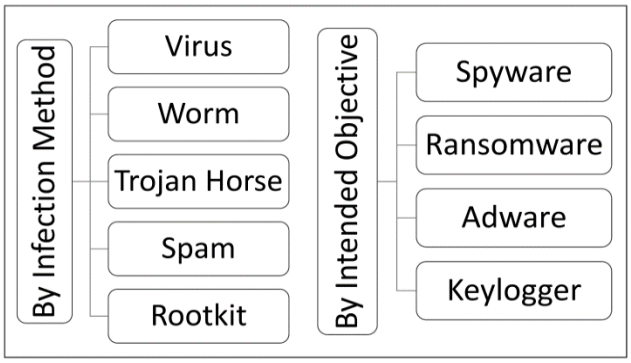

Figure. 1: Classification of Malware

The first generation malware is classified based on the infection strategy; the behavior or structure of the malware remains unchanged after it infects the target system. However, the second-generation malware changes its structure after each infection and forms a new variant. Generally, there are different types of dynamic malware; Metamorphic, Encrypted, Polymorphic, and Oligomorphic malware [6]. Furthermore, malware can also be categorized according to the goal or objective it achieves. For example, the goal of ransomware is to acquire financial data, whereas spyware is used to steal confidential information or data, and key logger is used to capture usernames and passwords.

In this paper, we present the state of malware evolution from the early phases into current day threats. The aim of this paper is to provide a broad overview of the current state of malware. This paper is organized as follows: in Section II, we describe the phases of malware evolution listing common characteristics and objectives found in each phase. Next, our findings are presented and discussed in Section III. Finally, the conclusion is presented in Section IV, where we summarize our findings.

2. Evolution of Malware

The evolution of malware is mainly split across five phases based on the time frame it emerged. The first phase is the early phase of malware, in which it came to life. The first windows and mail worms were introduced in the second phase of malware evolution. The third phase came to happen after the development of the Internet. In this phase, network worms were the prevalent threats that were widespread with the advancements of the Internet. Rootkits and ransomware were introduced in the fourth phase of evolution, and they are the most dangerous. The last phase in the evolution is the type of malware being faced currently and it includes the creation of malware by the secret services of some countries for the purpose of espionage [7]. Figure 2 illustrates the timeline of the 5 phases.

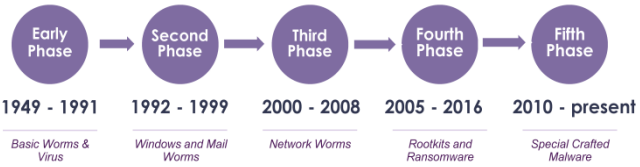

Figure 2: Malware evolution: timeline of the 5 stages

2.1. Early Phases of Malware Evolution (1949 - 1991)

Nowadays, malware is the most significant threat faced by the modern digital world. Initially, the intention of malware was not to harm, steal, or manipulate, but it evolved into becoming dangerous threats to our society. Here we are going to discuss some of the malware designed in the early phases of its evolution. John Von Neumann introduced the first virus as an idea of "self-replicating string of code" in 1949. He designed a "self-reproducing automata", which was able to transform a new version by itself [8].

Most of the malware in the early phases was not developed to harm the system or steal data. It was mainly used to point out the loopholes in MS-DOS systems. The payload caused by malware in this phase was a temporary crash in the system due to the consumption of the system resources. Viruses and worms in this phase have propagated through infected floppy drives or the ARPANET. An accepted definition of a computer virus was crafted by Fred Cohen to be "a program that can infect other programs by modifying them to include a possibly evolved copy of itself" [9]. Viruses can spread throughout a computer system or network. The difference between viruses and worms is that a virus usually requires human interference such as opening an infected file to start replicating, whereas worms can replicate without an intervention [10]. A common characteristic for malware in this phase is that they do not try to remain hidden from the user. Most would display a message or image on the computer's screen.

The first instance of a worm was developed by Robert H Thomas in 1971 and was called Creeper worm. It could move from one system to another and display a message that read "I'm the creeper: catch me if you can" [11]. Wabbit is a self-replicating program developed in 1974 to reduce sys- tem performance and ultimately crash the system. The name Wabbit (rabbit) came from the speed at which it replicates [12]. Wabbit was only capable of infecting the system it was installed on [13].

Elk Cloner is one of the first epidemic self-replicating viruses developed by a 15-year old named Richard Skrenta to infect PCs. On each infected system, it displayed a loving poem, "It will get on all your disks; It will infiltrate your chips; Yes, it's Cloner!" [14]. Basit and Amjad, two Pakistani brothers, developed Brain Boot Sector Virus in 1986 to infect MS-DOS computers, which was the first virus to infect the MS-DOS system [15]. They designed this virus to test their company's software and to prove that it was not a secure platform. This virus was replicating with the help of a floppy disk. Authors designed this virus to point out loopholes in their system rather than cause damage or harm to the system. PCwrite Trojan was one of the earliest Trojans designed in 1986 to erase all the user files once affected [16]. It was spreading through a shareware program called PC-Writer [17]. In 1988, Robert Tappan Morris, a graduate student at Cornell, drafted a program that would check a computer system's configuration to jump from one computer to another utilizing UNIX's sendmail program and the Internet's SMTP protocol [18]. It caused an increase in network traffic and eventually caused the Internet to crash at that time. Morris was arrested for creating this worm and convicted by the Computer Fraud and Abuse Act from 1986 [19].

Stoned is a boot sector virus that appeared in 1987 and infected floppy disks. It would sometimes display a message on the infected machine upon startup that would read: "Your computer is now stoned" [20]. Stoned virus has spawned many variants, one of these appeared in 1991, and was called Monkey. Monkey infects the master boot record of hard drives and floppies. It would embed its code into the first block of the master boot record and place the master boot record in the third block. The affected system would usually boot except in the case of booting from a floppy disk [21].

AIDS Trojan, also called PC Cyborg, was the first ransomware

released in 1989 [22]. Joseph L. Popp designed it, and it was comparatively easy to break. He made this attack by distributing infected floppy disks to AIDS researchers at the World Health Organization's conference for AIDS research. Simple symmetric cryptography was used in this malware [23].

One of the fascinating viruses created after Brain Boot Sector Virus was the Omega virus, which affected the boot sector of the system. An infected system could not boot on Friday the 13th, however, on all the other days, the system would function normally. Michelangelo designed a virus in 1991 as his name to affect DOS systems. Since it redrafts the first 100 sectors of hard disk, the file allocation table would be destroyed, and the PC will not boot. The system would get infected with the virus, on March 6th, which is the author's birthday [7].

Casino virus was a fascinating virus that originated at the start of 1991. It would infect command.com in C drive root directory. When a system is affected by this virus, the user will get the following message: "I have just DESTROYED the FAT on your Disk!! However, I have a copy in RAM, and I'm giving you a last chance to restore your precious data. WARNING: IF YOU RESET NOW, ALL YOUR DATA WILL BE LOST - FOREVER!! Your Data depends on a game of JACKPOT". If the user loses the game, the FAT table would be destroyed [24]. The mutation engine or Dark Avenger Mutation Engine (DAME), a toolkit from Virus Creation Laboratory, was the next innovative step in malware evolution [25]. It introduced mutation functionality to existing viruses to make it difficult to detect by anti-virus software. Table 1 summarizes the malware in this phase.

2.2. The Second Phase of Malware Evolution (1992-1999)

Hackers and attackers became interested in the Windows Operating System since it attracted many users for its simplicity and powerful user interface. Most of the malware in this phase was targeting the Windows Operating systems. This phase describes the development of Windows malware, early mail worms, and macro worms. This phase also saw the development of antivirus software.

The first windows malware introduced in 1992 was WinVir [26]. It was a replicating malware with minimal effect on infected files [27]. Also, in 1992, a virus called V-sign also infected the boot sector and displayed a V-sign on the screen with the intent of halting the system [7]. One-half or Slovak bomber is an utterly pernicious virus that infects master boot record, com, and exe files. It is a fascinating virus that will not harm the files whose name consists of words like [SCAN, CLEAN, FINDVIRU, GUARD, NOD, VSAFE, MSAV or CHKDSK] since these might be anti-virus software [7]. It would encrypt parts of the hard disk with some known private key. These encrypted files were decrypted temporarily when the user tries to access them. This was done so that the user was not aware of this infection. It would display a message, which is "Dis is one half. Press any key to continue. . . ", on the 4^{th}, 8^{th}, 10^{th}, 14^{th}, 18^{th}, 20^{th}, 24^{th}, 28^{th}, and 30^{th} of every month [28].

The first macro virus discovered in 1995 was WM Concept, which was drafted in Microsoft Word macro language. It affected the systems which contained MS word and was spreading through document sharing. This virus would only replicate itself and did not create any damage [29]. The first MS Excel macro virus drafted in VBA (Visual Basic for Application) was X97M/Laroux. Just like WM Concept, it was a replicating malware that would infect Excel versions 5.x, 7.x and Windows 3.x, 95, NT [29]. Boza is a virus drafted particularly for Windows 95. It would infect portable exe files. Slowly spreading Boza has no harmful routines, but the virus had an activation routine and did display a message on the 31st of every month which read: "The taste of fame just got tastier!" and "From the old school to the new" [7]. The first email virus, Happy 99, was spotted in 1998, and it was spreading as an executable email attachment. Once the user executes this attachment, it displays fireworks on the screen and would then spam the user's contacts with copies of itself [30]. Melissa, discovered in 1999, mingled both the techniques of macro viruses and mail worms. It transmitted through an attached malicious MS word file [31]. If the user opened the mail containing the malicious word file, Melissa would replicate by querying the user's address book contacts and send out an infected file attachment [29]. Table 2 summarizes the prominent viruses that appeared during the second phase.

2.3. The Third Phase of Malware Evolution (2000-2008)

The third phase of malware evolution began with the widespread use of the Internet. This phase is the evolution of network worms and viruses. Malware in this phase was mainly transmitted through email attachments, free downloads from compromised websites, or open network shares.

During the initial phases of the Internet, security was not a consideration and this helped the Morris worm to spread. All Internet worms scan the network using its scanning algorithm and infect the system connected to the network which had no protection mechanisms in place. It harms the system and then tries to propagate from there [32]. ILoveYou was one of the more damaging viruses to hit Micorosoft Outlook users. The virus would lure users to open an attachment on the premises of love. The virus spread among users of Outlook and networks running Microsoft's Exchange mail servers. Once a machine is infected, copies of the virus would be sent out to all Outlook contacts in the victim's machine [33]. Anna Kurnikova virus, analogous to Love virus, was also mailing an executable file which attracted the victims by employing photos of alluring tennis player Anna Kurnikova [34].

The first deliberately drafted Internet worm discovered after Morris worm was Code Red. It was discovered in 2001 and was able to infect more than 359000 computers in less than 14 hours. Code Red propagated over the Internet through buffer overflow vulnerability in Microsoft's Internet Information Server (IIS) web servers. After that, it initiated a DDoS attack on a set of websites including the Whitehouse [35]. Another Internet worm similar to Code Red was Nimda, which got the name from interchanging the letter positions of the word admin [36]. The propagation of Nimda

was faster and more dangerous than Code Red because it used multiple methods to spread, including email attachment of a readme.exe file, open network shares in .dll files, and by adding malicious javascript code at the end of web pages [37]. A mail worm introduced in 2003 was called Fizzer, and it was the first malware to gain profit. The machines were infected from mail attachments. Slammer was one of the first malware to attack Linux machines and Apache servers utilizing a vulnerability in OpenSSL. Because of the massive network traffic generated by Slammer, a large number of network packets were lost [29]. It caused several damages including flight delays for a US airline company, and stalling the ATM network of Bank of America, as well as the 911 service in Bellevue Washington, and gaining access into an Ohio nuclear power plant [29][38] [39].

A worm introduced in July 2003, utilizing a buffer overflow in Windows Remote Procedure Call, was called Blaster. It infected around 100,000 Windows systems [40]. A variant of Blaster called SoBig.F has caused the network traffic to slow down in D.C., and disabled several services like Air Canada planes, and US train company CSX [41][42]. MyDoom, also known as Norvag, is worm that appeared in early 2004, spreading through email attachments and peer to peer networks. It was estimated that 25% of emails at that time were infected with MyDoom [43]. Sasser was another worm discovered in 2004. It did significant damages to Railcop trains in Australia, Delta Airlines, British Airways flights, two of Hong Kong's government departments, Heathrow airport, UK Coastguard, and several Banks [7]. Sasser took advantage of a vulnerability in Window's Local Security Authority Subsystem Service (LSASS) [44].

Koobface virus emerged in 2008 and it spread to social networking sites, mainly targeting Facebook and MySpace. It would use the private messaging services of these social networking sites to send out a video link from an infected friend's PC. It would then prompt the victim to download an update for flash player, when in actuality what they are downloading is the virus file [45]. In 2008, Conficker worm and variants of it have appeared in the wild and infected around 9 million computers turning off anti-virus software, spreading through intranet, and infecting USB drives [46]. Conficker utilized a vulnerability in Windows, but its author's intentions were not identified. It spread by cracking weak passwords, but it never used its very complex botnet network for any of its attacks [47]. Table 3 summarizes malware that appeared during the third phase.

2.4. The Fourth Phase of Malware Evolution (2005-2016)

The fourth phase consists of the introduction of Rootkits and Ransomware. The most common ways for fourth phase malware to infect the victims are phishing emails, remote desktop protocols, downloads from compromised websites, and USB or other removable media. Malware in this phase was mainly focused on financial gain or illegal control of the infected machines.

Rootkits have been described as a set of programs that illegitimately take over control of an operating system and aim to gather information from the infected machine. While viruses and worms are characterized by replication; rootkits are characterized by stealth. Rootkits aims to hide an attacker's presence on an infected system [48]. In [49], a rootkit is defined as "any software that gives continued privileged access to a computer while actively hiding its presence and other information from administrators by subverting standard operating system functionality or other applications". There are 5 main types of rootkits; hardware (firmware) rootkit, bootloader rootkit, memory rootkit, application rootkit, and kernel-mode rootkit [50]. The first Rootkit, SONY BMG RootKit, was developed by Sony Entertainment in 2005, and it harmed their reputation. They developed this Rootkit to identify and prevent the copying of publications that were made by Sony. Due to the adverse impact of this Rootkit, Sony issued a recall of unsold music CDs with BMG RootKit. It also accepted mail in exchange from customers who already bought the CDs. Sony faced several class actions due to this incident [51].

A worm similar to ILoveYou, named StormWorm, using fear and horror instead of love, came seven years after ILoveYou. It was also installing a rootkit to hide malware. It used phrases such as "230 dead as storm batters Europe" in the mail subject to propagate through email [7]. Mebroot was a Master Boot Record (MBR) rootkit that was detected in late 2007. It infected a machine through visiting compromised websites. It gained access to the victim's machine and installed a rootkit even before the operating system loads. Mebroot would steal data from the victim's machine for financial gain [20].

Ransomware is a type of malicious software specially designed to acquire revenue. Nowadays, malware became the most profitable industry. Once a system executed ransomware, the malicious code would gain access to that system. It would block the users from accessing their data until they pay a sum of money, called a ransom. Mainly there are two types of ransomware: locker and crypto [52–54]. The locker ransomware prevents the user from accessing the system [55], whereas crypto ransomware would transform the user data making it unusable through the application of encryption algorithms. From these two, crypto-ransomware is the most destructive [56].

GPCode is a ransomware Trojan developed in 2005 and is the first reported to use the RSA algorithm for encryption. It encrypted the victim's file using a 660 bit RSA public key. It appeared as a job application mail attachment. There are many versions of GPCode malware [57]. Cryzip is ransomware that appeared in early 2006. It copied a user's data files into password protected files and then deleted the original files. It is thought to have spread via email spam and compromised websites [58]. Archiveus Trojan, introduced in 2006, also used the RSA algorithm for encryption. It was more challenging to break than its predecessor. It encrypted the victim's MyDocuments directory and asked them to shop items from an online pharmacy to get the decryption key [23].

In the mid of 2011, there was a hike in the number of ransomware attacks due to the use of anonymous payment

service, which made it easier for the attackers to collect the ransom. The number of new ransomware increased to 30,000 in the first two quarters of 2011; then it doubled in the third quarter [23].

In the beginning of 2012, Citadel, a toolkit for distributing malware and managing botnets, was introduced. Due to the introduction of this toolkit, the number of new malware increased [23]. Botnets are remotely controlled networks of hijacked computers by bot-masters with malicious intentions such as coordinating DDoS attacks and delivering spam email [59]. In July 2013, Kaspersky detected a new mobile Trojan, Svpeng, which spreads by SMS spam. It was mainly targeting information of Russian Bank customers.

New ransomware, Cryptolocker introduced in 2013, was the first cryptographic malware that spread through mail attachments and downloads from compromised websites. 2048-bit RSA encryption was used to encrypt the user files. The attackers compelled the victim to pay the ransom within three days. If the user failed to pay, they would give them one more chance with a higher ransom for getting the Private Key.

Cybercriminals introduced another ransomware CryptoDefence and its improved version, CryptoWall, in 2014. CryptoDefence utilized the built-in encryption API of Windows and saved the private key in the infected system itself, whereas CryptoWall did not store the private key. For infecting a machine, the former was spread through an email attachment, whereas the latter spread via a vulnerability in Java. There were several versions of CryptoWall created [54]. Cerber was ransomware that affected a large number of enterprise PCs. It was a crypto-ransomware, introduced in 2016. Table 4 summarizes the malware in fourth phase.

2.2. The Fifth Phase of Malware Evolution (2010-present)

The fifth phase is the current phase of malware evolution. The malware designed in this phase is mainly for the purpose of virtual espionage and sabotage. Previous malware types were created by cybercriminals to target businesses or personal PCs. However, current malware types are created by the military, police forces, and secret agencies of many countries. Nowadays, malware became a powerful weapon because it causes severe damage without affecting human lives. Malware in this phase is labeled as advanced persistent threat (APT). An advanced persistent threat is a carefully planned cyber-attack with a specific target or entity in mind. One of the most known malware of this type was Stuxnet, introduced in 2010 [7].

Stuxnet was a super malware detected after it finished its task. It was designed to demolish or slow down the Iranian Nuclear Program. Stuxnet infected the machines over a USB stick, and it would hide from the anti-malware software by installing Rootkit. The author of this malware was not identified, but it is believed to be the US and Israeli secret services. All instances of this malware were wiped out by itself on its death date, which was set to be the 24th of June 2012 [7, 60].

DuQu is another malware designed to spy on the victim with a similar code base of Stuxnet. DuQu was drafted in object-oriented C, and was compiled in Microsoft Visual Studio 2008. It is also believed that the US and Israeli secret services are behind it [7, 60].

Another malware of this category was Flame which was identified in 2012. Like DuQu and Stuxnet, it is suspected that Israel and US secret services and military have created it. It affected mainly computers in the Middle East. It was a very complicated malware; with the ability to control and add new modules, remotely. It was spreading over both USB and networks. It also installed Rootkit to be undetectable by the victim. It had a variety of capabilities such as recording audio and video, calling through Skype, stealing files from the hard disk, and sending it to the hacker. The attacker demolished this malware by sending a kill command when the anti-virus companies started to study a sample of it [61].

Shamoon was malware designed to attack Saudi Aramco which is the largest refinery in the world. Shamoon targeted Aramco on 15th August 2012 with a rupturing cyber-attack. It affected almost 30000 Aramco workstations and destroyed computer hard drives [62]. Shamoon overwrote the infected machines' MBR (Master Boot Records) and deemed the machines unusable. The creators were able to select and delete files on Aramco computers [63]. RasGas, the second largest producer of Liquid Natural Gas in Qatar, is also attacked Shamoon on 16 August 2012[60].

WannaCry was the first ransomware to propagate by exploiting a vulnerability developed by the National Security Agency [54]. It gained access to significant computer systems in about 150 countries such as Russia, China, and the US. It infected many hospitals, banks, telecommunication companies, warehouses, and industries. The US government believes that North Korea is behind the WannaCry attack. Table 5 summarizes the main malware in this current phase of malware evolution.

3. Discussion and Future Research Directions

Malware has evolved into sophisticated, extremely malicious software reaping billions of dollars in profits. Predominantly, malware in its earliest phase was not intended to cause damage or gain profit. Many examples of malware that appeared in the early phase, such as Creeper and Brain Boot Sector, were a result of experimentation gone wrong. The viruses that appeared in malware's early phase shared some common characteristics. One such characteristic is that they would replicate and not mutate making it easier for antivirus software to mitigate their threat. Another characteristic is that they lacked stealth. Unlike rootkits which came at a later phase, early malware was not trying to hide from antivirus programs. The damages caused by malware in its early stages were restricted to infected machines and for the most part would cause a slight aggravation for users. Propagation of malware in its early phase was usually through the use of infected floppy disks.

The second phase of malware evolution was focused on the Windows operating system. The Windows operating system was the most common system on personal computers at the time. This has made it an obvious target for malware creators. Moreover, the

increased usage of the Internet also played a large role, and continues to do so, in the spread of malware. The Internet has brought on many benefits to users such as ease of connectivity and exchange of information. As is the case with any new technology, it saw some abuse from users with malicious intentions. Malware authors took advantage of Microsoft's macro language to craft malware. Also, malware in the second phase has become more varied in infection methods. The methods of propagation were sharing infected Microsoft office files as well as through email attachments.

The third phase of malware witnessed the increased creation of network worms. At the time, the Internet was thriving with the dot-coms of the late 90s and early 2000s. The most common form of propagation for malware in this phase was email attachments and visits to compromised websites. The malware in this phase is characterized by its exploitation of existing vulnerabilities in operating systems. Network worms, like Code Red, were memory-resident which meant they would execute when the OS loads. Malware in the previous stages would require a file to be executed in order to infect the system. Malware in the third phase was causing damages estimated in billions of dollars. This had caught the media's attention and reports of malware such as SoBig.F and Conficker were making headline news.

Rootkits were introduced in the fourth phase of malware. The main characteristic for rootkits is stealth. The fourth phase of malware evolution also witnessed the birth of ransomware. In this phase, malware had incorporated more sophisticated techniques such as encryption to take over valuable data in the host machine. Furthermore, the use of anonymous payment services spiked the creation of ransomware as it became easier for the attacker to get paid using these services. It is in this phase that cybersecurity gained more attention. Companies are investing large amounts of money and resources to protect their assets from ransomware attacks.

The fifth phase of malware evolution is focused on creating malware for the purpose of virtual espionage. The creation of these types of malware is believed to be foreseen by government entities. In this phase, malware is mostly categorized as Advanced Persistent Threats (APTs). There are different objectives for APTs. For instance, an APT can be carried out with the purpose of sabotaging an adversary's project such as in the case of Stuxnet. An APT can also aim to steal an adversary's classified information or erase it as was the case in Flame. Ransomware and APTs are the current malware threatening individuals, organizations, and even nations. Table 6 summarizes all five phases of malware evolution in terms of common characteristics and propagation methods used.

Future research on malware should be focused on early detection of platform specific types. The rise in usage of smart devices and mobile phones has cybercriminals turning their attention more towards this platform. Machine learning and AI must be employed to come up with new and fast malware detection methods. Furthermore, while IoT malware is still in its infancy, the potential for it to grow exponentially is alarming. IoT devices are creating new endpoints that are directly connected to a network and can be targeted by cybercriminals at any time. Increased usage of IoT devices will introduce a variety of new attack vectors that will emerge and therefore must be addressed in research. Malware can target any device from wearable devices to driver-less cars. Therefore, it becomes essential for researchers to address security issues and prevention techniques for IoT malware attacks.

4. Conclusion

In its beginnings, malware was harmless and easily detectable, causing some aggravation to a victim with an infected machine. Many early forms of malware would publicize their presence by displaying messages on a victim's machine. Nowadays, malware has evolved into sophisticated types that are extremely malicious with the intention of extorting a victim for financial gain. These types are referred to as ransomware and are considered the prominent threat being faced by companies and individuals today. Moreover, governments around the world have begun creating malware for espionage purposes in order to sabotage or spy on other countries' systems. This type of malware is referred to as an Advanced Persistent Threat. In recent years, malware became a profitable industry attracting many cyber criminals to create more intricate forms of malware. Many large corporations around the world are investing billions of dollars in building up cyber security systems for their organizations in order to counter any possible threats. This study has presented a historical evolution of malware, in chronological order; leading up to the conception of ransomware and APTs. Ransomware can target several entities at a time whereas an APT would aim for a specific target. The study also highlighted the common propagation methods used and the damages that were caused by malware over the past 70 years. The purpose of this study was to provide researchers with the history and evolution of malware from its early stages to current day threats.

References

[1] L. Sheldon, "Implementing information security architecture and governance: A big framework for small business," 05 2016. [Online]. Available: Link

[2] B. Violino, "Cybercrime is increasing and more costly for organizations," Link, March 2019, [Online; accessed 16 July 2020]. [Online]. Available: Link

[3] M. Bayern, "Nearly 70 % of major companies will increase cybersecurity spending post-coronavirus," Link, May 2020, [Online; accessed 16 July 2020]. [Online]. Available: Link

[4] M. Chikapa and A. P. Namanya, "Towards a fast offline static malware analysis framework," in 2018 6th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW). IEEE, Barcelona, Spain, pp. 182–187, 2018.

[5] J. El Abdelkhalki, M. B. Ahmed, and B. A. Abdelhakim, "Image malware detection using deep learning," International Journal of Communication Networks and Information Security, vol. 12, no. 2, pp. 180–189, 2020.

[6] S. K. Sahay, A. Sharma, and H. Rathore, "Evolution of malware

and its detection techniques," in Information and Communication Technology for Sustainable Development. Springer, vol. 933, pp. 139–150, 2020.

[7] N. Milosevi˘ c, "History of malware," 2014. [Online].´ Available: Link

[8] M. Gaudesi, A. Marcelli, E. Sanchez, G. Squillero, and A. Tonda, "Challenging anti-virus through evolutionary malware obfuscation," in Lecture Notes in Computer Science. Springer, vol. 9598, pp. 149–162, 2016.

[9] F. Cohen, "Computer viruses: theory and experiments," Computers & security, vol. 6, no. 1, pp. 22–35, 1987.

[10] M. Draief, A. Ganesh, and L. Massoulie, "Thresholds´ for virus spread on networks," in Proceedings of the 1st international Conference on Performance evaluation methodolgies and tools, Pisa, Italy, pp. 51–es, 2006.

[11] D. Gibert, C. Mateu, and J. Planes, "The rise of machine learning for detection and classification of malware: Research developments, trends and challenges," Journal of Network and Computer Applications, p. 102526, 2020.

[12] C. Chen, Z. Duan, C. Tian, and H. Du, "Cloning automata: Simulation and analysis of computer bacteria," in International Conference on Combinatorial Optimization and Applications. Shanghai, China, pp. 401–416, 2017.

[13] InfoSecInstitute, "Malware spotlight: Wabbit," Link, January 2020, [Online; Accessed 16 July 2020]. [Online]. Available: Link

[14] V. Tasril, M. Ginting, M. Mardiana, and A. P. U. Siahaan, "Threats of computer system and its prevention," International Journal of Scientific Research in Science and Technology, vol. 3, pp. 448–451, 08 2017.

[15] R. Husain and S. U. Suru, "2321-0869," International Journal of Engineering and Technical Research (IJETR), vol. 2, 11, 2014.

[16] L. Fu, "Design of hidden communication remote monitoring based on c/c mfc," in 2019 4th International Conference on Mechanical, Control and Computer Engineering (ICMCCE). IEEE, Honhot, China, pp. 589–5892, 2019.

[17] J. Love, "A brief history of malware - its evolution and impact," Link, April 2018, [Online; accessed 16 July 2020]. [Online]. Available: Link

[18] H. Orman, "The morris worm: A fifteen-year perspective," IEEE Security & Privacy, vol. 1, no. 5, pp. 35–43, 2003.

[19] C. Kelty, "The morris worm," Limn, vol. 1, no. 1, 2011. [Online; accessed 28-April-2020]. [Online]. Available: Link

[20] Kasslin and Florio, "Virus bulletin 2008, your computer is now stoned ... again," Link, 2008, [Online; accessed 1-May-2020]. [Online]. Available: Link

[21] F-Secure, "Boot/stoned.monkey," Link, [Online; accessed 1-May-2020]. [Online]. Available: Link

[22] A. Kumari, M. Z. A. Bhuiyan, J. Namdeo, S. Kanaujia, R. Amin, and S. Vollala, "Ransomware attack protection: A cryptographic approach," in International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage. Atlanta, USA, pp. 15–25, 2019.

[23] R. Richardson and M. M. North, "Ransomware: Evolution, mitigation and prevention," International Management Review, vol. 13, no. 1, p. 10, 2017.

[24] McAfee, "Casino.2330," Link, [Online; accessed 30April-2020]. [Online]. Available: Link

[25] S. Spencer, "Timeline of computer viruses," Link, January 2012, [Online; accessed 30-April-2020]. [Online]. Available: Link

[26] C. Researcher, Issues in Terrorism and Homeland Security: Selections From CQ Researcher. SAGE Publications, 2009. [Online]. Available: Link

[27] F-Secure, "Winvir," Link, [Online; accessed 01-May-2020]. [Online]. Available: Link

[28] G. Torres, "What is a computer virus," Link, December 2017, [Online; accessed 1-May-2020]. [Online]. Available: Link

[29] P. Szor, The Art of Computer Virus Research and Defense. Addison-Wesley Professional, 2005.

[30] B. Sullivan, "Happy99.exe worm spreads on net," Link, January 1999, [Online; accessed 1-May-2020]. [Online]. Available: Link

[31] M. Rouse, "Macro virus," Link, January 2018, [Online; accessed 1-May-2020]. [Online]. Available: Link

[32] F. Touchette, "The evolution of malware," Network Security, vol. 2016, no. 1, pp. 11 – 14, 2016. [Online]. Available: Link

[33] CNNMoney, "U.S. catches love virus," Link, May 2000, [Online; accessed 30-April-2020]. [Online]. Available: Link

[34] T. M. Chen and J.-M. Robert, "The evolution of viruses and worms," Statistical methods in computer security, vol. 1, pp. 1–16, 2004.

[35] D. Moore, C. Shannon, and K. Claffy, "Code-red: a case study on the spread and victims of an internet worm," in Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurement, Marseille, France, pp. 273–284, 2002.

[36] M. Joshi and D. B. Patil, "Computer virus: Their problems & major atttacks in real life," Journal of Advanced Computer Science & Technology, vol. 1, 08 2012.

[37] A. Machie, J. Roculan, R. Russell, and M. Velzen, "Nimda worm analysis," Tech. Rep., Incident Analysis, SecurityFocus, Tech. Rep., 2001.

[38] K. Poulson, "Slammer worm crashed ohio nuke plant network," Link, August 2003, [Online; accessed 2-May2020]. [Online]. Available: Link

[39] B. Schneier, "Blaster and the great blackout," Link, December 2003, [Online; accessed 3-May-2020]. [Online]. Available: Link

[40] M. Bailey, E. Cooke, F. Jahanian, and D. Watson, "The blaster worm: Then and now," IEEE Security & privacy, vol. 3, no. 4, pp. 26–31, 2005.

[41] CNNTech, "Sobig.f breaks virus speed records," Link, August 2003, [Online; accessed 3-May-2020]. [Online]. Available: Link

[42] CBSNews, "Virus disrupts train signals," Link, August 2003, [Online; accessed 3-May-2020]. [Online]. Available: Link

[43] D. Balaban, "A short history of computer viruses," Link, March 2019, [Online; accessed 3-May-2020]. [Online]. Available: Link

[44] CNNTech, "Sasser worm spreading quickly," Link, May 2004, [Online; accessed 3-May-2020]. [Online]. Available: Link

[45] S. Gilbertson, "'koobface' virus attacks facebook," Link, December 2008, [Online; accessed 2-May-2020]. [Online]. Available: Link

[46] R. Mohan, "Two years after the conficker worm, are we still at risk?" Link, April 2011, [Online; accessed 3-May-2020]. [Online]. Available: Link

[47] S. Ranger, "Opening up a can of worms: Why won't conficker just die, die, die?" Link, June 2015, [Online; accessed 4-May-2020]. [Online]. Available: Link

[48] S. Embleton, S. Sparks, and C. C. Zou, "Smm rootkit: a new breed of os independent malware," Security and Communication

Networks, vol. 6, no. 12, pp. 1590–1605, 2013.

[49] P. Bravo and D. F. Garcia, "Proactive detection of kernelmode rootkits," in 2011 Sixth International Conference on Availability, Reliability and Security. IEEE, Washington DC, USA, pp. 515–520, 2011.

[50] D. Rafter, "What is a rootkit? and how to stop them," Link, [Online; accessed 3-May-2020]. [Online]. Available: Link

[51] D. K. Mulligan and A. K. Perzanowski, "The magnificence of the disaster: Reconstructing the sony bmg rootkit incident," Berkeley Tech. LJ, vol. 22, p. 1157, 2007.

[52] K. Cabaj, M. Gregorczyk, and W. Mazurczyk, "Software-defined networking-based crypto ransomware detection using http traffic characteristics," Computers & Electrical Engineering, vol. 66, pp. 353-368, 2018.

[53] M. U. Kiru and A. B. Jantan, "The age of ransomware: Understanding ransomware and its countermeasures." Artificial Intelligence and Security Challenges in Emerging Networks. Chapter 1, pp. 1–37, 2019.

[54] B. Celiktas, N. Unlu, and E. Karacuha, "Ransomware, detection and prevention techniques, cyber security, malware analysis," Ph.D. dissertation, Department of Applied Informatics, 05 2018.

[55] N. Shah and M. Farik, "Ransomware-threats, vulnerabilities and recommendations," International Journal of Scientific & Technology Research, vol. 6, pp. 307–309, 06 2017.

[56] D. Nieuwenhuizen, "A behavioural-based approach to ransomware detection," Whitepaper. MWR Labs Whitepaper, 2017.

[57] H. Sultan, A. Khalique, S. I. Alam, and S. Tanweer, "A survey on ransomeware: Evolution, growth, and impact." International Journal of Advanced Research in Computer Science, vol. 9, no. 2, 2018.

[58] J. Stewart, "Cryzip ransomware trojan analysis," Link, March 2006, [Online; accessed 17 July 2020]. [Online]. Available: Link

[59] W. W. A. Ramzi, M. Faizal, R. M. Fadhlee, and N. M. Hidayah, "Revealing influenced selected feature for p2p botnet detection," International Journal of Communication Networks and Information Security, vol. 9, no. 3, pp. 500–506, 2017.

[60] S. Alelyani and H. Kumar, "Overview of cyberattack on saudi organizations," Journal of Information Security and Cybercrimes Research, vol. 1, no. 1, 2018.

[61] E. Mills, "Behind the flame malware spying on mideast computers (faq)," Link, June 2012, [Online; accessed 30 June 2020]. [Online]. Available: Link

[62] S. Alshathry, "Cyber attack on saudi aramco," International Journal of Management and Information Technology, vol. 11, pp. 3037–3039, 12 2016.

[63] C. Bronk and E. Tikk, "The cyber attack on saudi aramco," Survival, vol. 55, no. 2, pp. 81-96, 2013.

Table 1. Summary of Malware in the Early Phase of Evolution

Name	Creator	Propagation	Year	Target/Damages
Self-replicating string of code	John Von Neumann	Self-reproducing	1949	Introduce the idea of replication.
Creeper worm	Unknown	ARPANET	1971	Tested the theory of self-replicating programs
Wabbit	Unknown	Local system	1974	Reduce performance and crash the system.
Elk Cloner	Richard Skrenta	Floppy disks	1981	Apple II systems.
Brain Boot Sector virus	Basit and Amjad	Floppy disks	1986	MS DOS computers. Developed to point out loop holes in the system.
PCwrite trojan	Unknown	Shareware programs	1986	Erase all users' files upon infection.
Morris worm	Robert Tappan Morris	Sendmail/SMTP	1988	Increased network traffic and crashed the Internet
AIDS trojan	Joseph L. Popp	Floppy disks	1989	Attendees of WHO AIDS conference for ransom
Omega virus	Unknown	Unknown	1991	Infected systems. Would not boot on Friday 13th.
Michelangelo virus	Michelangelo	Floppy disks	1991	Destroy FAT and prohibit PCs from booting.
Monkey	Unknown	Floppy disks	1991	Variant of boot sector virus. Infects master boot record of hard drives and floppies.
Casino virus	Unknown	Unknown	1991	Destroy FAT when victim loses game

Table 2. Summary of Malware in the Second phase of Evolution

Name	Creator	Propagation	Year	Target / Damages
WinVir	Masud Khafir	Network or removable media	1992	MS Windows 3.0. Infected files will not start in the first try, but the second.
V-sign virus	Unknown	Floppy disks	1992	Halt the system.
One-half or Slovak bomber	Vyvojar	floppy disks	1994	MS-DOS. Infected master boot record, com, and exe files.
WM Concept	Unknown	Sharing infected MS-word documents	1995	MS-Word. Replicates itself without damages.
X97M/Laroux	Unknown	Sharing infected MS-word documents	1996	MS-Excel. Overwrites target file with infected file.
Boza	Quantum/VLAD	Floppy disks	1996	Windows 95. No reported harmful routines.
Happy 99	Spanska	Executable email attachment	1998	Spammed the user's contacts with copies of itself
Melissa	David L. Smith	Email attached malicious MS word file	1999	Caused $1.1 billion in damages worldwide.

Table 3. Summary of Malware in the Third Phase of Evolution

Name	Creator	Propagation	Year	Target/Damages
Anna Kurnikova virus	Jan de Wit	Email attachment	2001	Infected millions of machines and crashed email servers.
Code Red	Unknown	Internet	2001	Infected more than 3.59K computers in less than 14 hours costing billions in damages.
Nimda	Unknown	Email attachment, open network shares	2001	Damages estimated at $2.6 billion.
Fizzer	Unknown	Mail attachment	2003	First malware to gain profit.
Slammer	Unknown	Internet, Exploits the vulnerability of SQL server 2000	2003	Caused almost $1.2 billion in damages.
Blaster	Jeffrey Lee Parson	Internet, Exploits buffer overflow	2003	Infected around 100,000 Windows systems.
SoBig.F	Unknown	Email attachment	2003	Caused damages estimated at $37.1 billion.
MyDoom	Unknown	Email attachment and peer to peer networks	2004	Caused damages estimated at almost $38.5 billion.
Sasser	Sven Jaschan	Internet, Exploit the Local Security Authority Subsystem Service vulnerability of windows machines.	2004	Caused damages to airline systems, governments and several banks.
Koobface virus	Unknown	Through private messaging services of social networking sites.	2008	Targeted users of social networking sites and mail servers.
Conficker worm	Unknown	Intranet and USB drives.	2008	Infected around 9 million computers turning off antivirus software.

Table 4. Summary of Malware in the Fourth Phase of Evolution

Name	Creator	Propagation	Year	Target/Damages
Sony BMG Rootkit	Sony Entertainment	CD	2005	It harmed their reputation.
GP Code	Unknown	Spam email claiming job application.	2005	Windows OS. Encrypts files and demands a ransom for decryption.
Cryzip	Unknown	Spam email and compromised websites.	2006	Deletes files and creates password protected archived file.
Archives Trojan	Unknown	Email attachments and downloads from compromised websites	2006	Required the purchase of drugs from a particular pharmacy to get decryption password.
Storm worm	Unknown	Email spam	2007	Infected more than 20 million computers and built a zombie army.
Mebroot	Unknown	Visiting compromised websites.	2007	Captures data from the victim's machine for financial gain.
Svpeng	Unknown	SMS spam.	2013	Mobile trojan. Targets

				customers of Russian Bank.
Cryptolocker	Unknown	Email attachments and downloads from compromised websites	2013	Encrypts users' hard drives and demands ransom. Almost 3% of the victims paid ransom.
CryptoDefence	Unknown	Email attachment.	2014	Encrypts text, picture, video, PDF and MS Office files with a strong RSA-2048 key that is hard to undo.
CryptoWall	Unknown	Vulnerability in Java.	2014	Caused over 325 million dollars damage.
Cerber	Unknown	botnets, spam emails and drive-by downloads.	2016	Affected a large number of enterprise PCs.

Table 5. Summary of Malware in the Fifth Phase of Evolution

Name	Creator	Propagation	Year	Target / Damages
Stuxnet	Unknown	USB Stick	201	Demolishes or slows down the Iranian Nuclear Program.
DuQu	Unknown	Exploits the CVE-2011-3402 vulnerability or zero day vulnerability	2011	Spies on the victim machine.
Flame	Unknown	Both USB and networks	20	Affected computers in the Middle East.
Shamoon	Unknown	Network	2012	Saudi Aramco and RasGas.
WannaCry	Unknown	Exploiting a vulnerability developed by the National Security Agency	201	Infected computer systems in 150 countries worldwide.

Table 6. Summary of Malware in the Five Phases of Evolution

Time	Characteristics	Propagation
Phase 1	– Self-replicating in nature. Discover loop-holes in system without serious harm or information stealing. Not for financial gain	• ARPANET • Removable media such as floppy disk, USB, CD, etc.
Phase 2	– Malware targets Windows due to its simplicity and ease of use. – Malware applies the art of escape, which helps antivirus business to grow.	• Removable media • File sharing • Email
Phase 3	– Malware characteristics changed into a most dangerous form and a large number of machines are affected. – Some of the cybercriminals got arrested in this phase. – Viruses in this stage are most destructive and its aim changed to money oriented.	• Email attachments • Removable media • Internet

Phase 4	– Malware in this phase is mainly focused on gaining income or taking the illegal control of the infected machines. – Malware encrypt the crucial information and ask ransom for the decryption key. If the victim is unable to pay the ransom the data is destroyed.	• Email attachments • Compromised websites
Phase 5	– Malware is developed by the secret services of some countries for the purpose of espionage. – Malware in this phase are considered as best blood free weapon. Most of the malware in this phase are used to destroy some important areas of some countries. These are the most dangerous weapon which affects countries economic, social, and political strengths. These all are state sponsored attacks.	• Removable media • Internet