Cowen M. Hames

MIS 545 | Dr. Helmer

Term Research Paper

April 9, 2021

Past, Present, and Future of Malware

An overview of the origins, types, and consequences of one of the most well-known cyber-attack weapons

Contents

[Abstract 1](#_Toc67301294)

[I: Origins of Malware (1971 – 1999) 2](#_Toc67301295)

[II: Modern Malware (2000 – present) 6](#_Toc67301296)

[III: Case Study: WannaCry Ransomware (2017) 13](#_Toc67301297)

[IV: Futuristic Malware 14](#_Toc67301298)

[Coda 16](#_Toc67301299)

[References 17](#_Toc67301300)

# Abstract

I have been waiting a long time to be able to write a personal research paper about one of my favorite subjects in cybersecurity and IT in general. Malware has fascinated me since I was in middle school after I fell victim to a malware attack via email. I remember clicking on a link in an email, completely oblivious at the time (2007) to malware and viruses, and before I knew it my entire computer was locked out because of a malicious program being downloaded and executed. The message on the computer stated I had to send a payment to unlock the computer. My dad had knowledge of computers and software and quickly realized it was ransomware (a version of malware that usually results in the device being taken over and wanting payment before unlocking it) and ended up swiping (deleting) the entire OS and rebooting the initial setup to get around it.

In the aftermath, I had been scolded and warned about the dangers of viruses and malware. I quickly became more vigilant throughout high school, but that curiosity about how malware works and the deeper exploration of it was always lingering. Finally, during my last semester of undergraduate, I was able to take a cybersecurity course and learn more about these attacks, but it was not until this graduate class I was assigned to research and write about a topic. I am taking full advantage of the opportunity to do so with this paper.

This research paper will be divided into four components: first I will discuss the origins of malware with early attacks and examples, then I will go over the modern era of attacks and the evolution of malware. There will be a subsection completely dedicated to the 2017 WannaCry ransomware attack which I consider one of the most interesting cyber-attacks in history. Finally, I will close the paper with hypothetical future scenarios and consequences of futuristic malware attacks. Throughout the paper, I will include an image depicting the virus from each decade, usually of significant importance in the evolution of malware. I will also briefly discuss different types of malware and the AV-Test in this paper.

There are numerous sources used for this paper, as needed for a topic with such a deep history, however, the chief source used throughout this research paper is John Love’s article: *A Brief History of Malware- Its Evolution and Impact.*

# I: Origins of Malware (1971 – 1999)

Defined in 1986 by Fred Cohen as “A program that can infect other programs by modifying them to include, a possibly evolved, version of itself”(1). Short for malicious software, malware has been around for about 40 years now and has evolved to become sophisticated and tricky to navigate compared to its original roots. Malware consists of numerous different types, including ransomware, trojans, worms, spyware, adware, wiper, and scareware. Even though there are numerous different types of malware, the purpose has never changed- to compromise a system and perform malicious acts (illicit funds, steal information, or cause havoc). Malware usually works in a process: A user will unknowingly download or install malicious software, oftentimes hidden behind something that looks real. After installation, the malicious code usually executes and performs various actions, such as keylogging, information capturing, internal system corruption, or in more modern cases system takeover (lockout). While malware is sophisticated nowadays with all these different types, it did not start that way, but rather through much simpler methods such as being installed via floppy disks. Eventually, the primary delivery method of malicious code was through the download of malicious executable files.

According to John Love’s 2018 article “A Brief History of Malware- Its Evolution and Impact”, malware, as we know it today, was born with the 1971 virus named “Creeper”. Creeper reportedly did very little but was able to move between computers with a message: “I’m the creeper, catch me if you can!”(1). The message and purpose may seem childish, but a closer look will realize that this program had successfully created a new and exponentially dangerous threat: A program invading a device and having the ability to infiltrate and compromise the structural security of it. A very old picture of the creeper message is depicted below (2):

Text

Description automatically generated

Then in 1974, the world was introduced to Wabbit, “a self-replicating program that essentially multiplied itself to the point of corrupting system memory and crashing the computer” (1). At the time, it was likely an extraordinary feeling. This was not just someone cracking a password and causing damage, this was a program manifesting and replicating itself inside a device and conducting damage out of the owner’s control *all on its own.*

Throughout the 1980s, malware attacks would continue, albeit at a slow pace compared to today’s attacks. Also, from John Love’s article, “in 1982, the Elk Cloner virus was one of the first widespread viruses to attack multiple computers” (via floppy disk). The message displayed if infected with the virus was “It will get on all your disks, it will infiltrate your chips, yes it’s Cloner!”. (1) In this attack, there was one significant difference from the Wabbit malware eight years prior- it infected multiple, widespread computers. Part of the reason Elk Cloner was able to infect multiple computers was the lack of anti-virus software and the fact that this was the beginning of the malware saga in computers. The 1980s would continue to see new viruses emerge, namely the Brain Boot Sector Virus, the PC-Write Trojan, and the Morris Worm. The Brain Boot Sector Virus is accepted to be the first malicious software to infect MS-DOS operating systems (The Elk Cloner infected Apple II computers) (1), while the PC-Write Trojan, in addition to being one of the first trojans, could erase everything on the computer (1). The PC-Write Trojan was also delivered via the PC-Write shareware program (a look-alike version that tricked users into installing the malicious files) (1). In 1988, the Morris Worm caused havoc on computers connected to the ARPANET (The predecessor to the internet today). It crashed the ARPANET within a day (1), showing the true damage and widespread problems malware truly is capable of. Things would only escalate from here into the 1990s. The Morris Worm is shown below (3):

Text

Description automatically generated

To wrap up the origins of malware, there were two big viruses before the 2000’s internet boom that would pave the way for new and modern attacks to take place. In 1991, the world would give significantly more attention to the seriousness of viruses when the Michelangelo Virus made headline news. News outlet reporters stated the virus would impact millions of computers and “erase their hard drives on March 6 (Michelangelo’s birthday)” (1). However, the day came and went and only a handful (~10,000) were impacted (1). Regardless, this story heightened public awareness of viruses and what they can truly do. By this time, the internet became a public tool, and what would follow would be the endless waves of cyber-attacks and countermeasures to defend them. In 1999 the Melissa Virus took advantage of public access to the internet by becoming the first, and most certainly not the last, virus to be mass-emailed to potential cyber-attack victims (1). The virus did not stop there, as it would then duplicate and send itself to “up to 50 people at a time” (1), as shown below (4).

Graphical user interface, text, application, table, email

Description automatically generated

By the end of 1999, technology had advanced to the point of many people having personal computers and internet access, and so began the modern era of the dark side of technology- the modernization of malware.

# II: Modern Malware (2000 – present)

The purpose of infecting someone’s device with malware was typically for one or more of the three following reasons:

1. To steal sensitive information
2. To bribe or coerce one into giving the attacker money
3. To intentionally disrupt or otherwise cause damage

Before 2000, most attacks tended to focus on the third reason. However, with the invention of the internet and widespread public access to it, the modern era of malware has seen a massive increase of the first and second reasons, particularly with the creation of ransomware and more sophisticated worms which will be discussed later in this subsection. Two new additional reasons to use malware: cyberterrorism and cyberwarfare, will also be discussed. While the internet was one of humanity’s greatest inventions to date, the ability to connect with other devices remotely also brought along the ability to infect other devices remotely. The following cases will go over some of these attacks.

In 2000, the ILOVEYOU worm infected about “50 million computers by infecting them with a worm attached to an email with the before-stated subject line” (1). According to John Love’s article, the damage exceeded $5.5 Billion and even resulted in “the Pentagon and British Parliament shutting down their email servers” (1). Further research on this unveiled the attacker’s motive was to “steal victims’ passwords and log in to their accounts without having to pay for them, since he was poor” (5). While this is just one example, it is interesting to note the change in reasoning for the attack compared to older malware from the past decades. Instead of a programmer trying to break a system or someone messing around, these individuals infected millions of computers to extract data for their gain. It is important to note this for future attacks in this subsection. Below is an image from 2000 depicting the virus at work (6):Graphical user interface, text, email

Description automatically generated

The early and mid-2000s saw numerous new worms and viruses as the internet continued to expand into more homes. Notable examples include the 2001 Anna Kournikova Virus (again spread through email), the Slammer Worm in 2003, and the Koobface Virus in 2005 (1). The Slammer Worm was a global issue as its “DoS (Denial of Service) attack crippled the internet for much of the world and was also extremely quick at reproducing” (1). The Koobface Virus is known because of its significance being “one of the first social media viruses (1) to emerge”, which was another avenue of accessibility now unlocked for attackers. The early 2000s would continue to see similar viruses and worms until about 2010.

Up until this point, the malware had undergone an incredible transformation, at first becoming possible by curious programmers seeing if computers could be modified with software outside of normal intentional use, and then progressing to a more modern and much more accessible means of attacking one’s device to steal information. The early 2000s saw the rise of using email and social media to spread malicious software and saw the use of malware become a widespread phenomenon by attackers, along with public knowledge of these threats rapidly increasing. Due to the increase in attacks and widespread availability of the internet, anti-virus software began taking off and becoming a staple in all personal computers and businesses. This software would be an additional level of protection along with training in the workplace and public knowledge at home about not clicking on unfamiliar attachments or links, and for people to be cautious when browsing unknown websites. As a response to the improved measures of security and protection, the malware began to transform again, this time with the creation of new forms of malware, namely ransomware. It was also when we began to see governments and criminal organizations use it to create two additional reasons to use malware in a cyber-attack: cyberterrorism and cyberwarfare.

In 2010, the Stuxnet Worm was unleashed and is believed to have been created to target Iran’s nuclear power plants. Debates about who the authors of the worm still stand, although the sophistication, intelligent, and extremely complex design makes some believe it was another government entity who created and released the worm (7). According to the Symantec W32.Stuxnet Dossier, the worm was a “milestone for many reasons, particularly being the first one to successfully exploit the four 0-day vulnerabilities, compromise two digital certificates, and infect industrial control systems with malicious code while being off the radar to employees” (7). The process Stuxnet undertook was extremely complex compared to other malware, as stated in the dossier:

*“The creators amassed a vast array of components to increase their success. They used Windows rootkit, a PLC rootkit, zero-day exploits, anti-malware evasion, complex process injection and hooking code, network infection routines, peer-to-peer updates, and command and control interfaces.”- Symantec W32.Stuxnet Dossier (Nicolas Falliere, Liam O Murchu, and Eric Chien)*

The complexity and deepness that Stuxnet Worm’s contained are worthy of a research paper on its own. However, in this research paper, not all the details will be covered. The Symantec Dossier offers a rich dive into the technical aspects of the worm but is it worth noting the legacy this worm has as being one of the first major instances of malware being used for cyberwarfare purposes. A relevant picture of Stuxnet code is included below, note the technological advancement compared to the previous picture of the ILOVEYOU worm 10 years prior. (8):

Text

Description automatically generated

For the next few years, there would be countless malware attacks with the technological era in full force, although the Stuxnet Worm continued to overshadow them in terms of complexity and power. Numerous applications would be released, with numerous vulnerabilities, both old and new discovered. For each of these vulnerabilities, there could be potential new malware deployed to infect the system. By this point, virtually anything with a processor could now be potentially infected with malware, ranging from computers, mobile devices, gaming systems, and government-owned systems. Notable attacks include the Zeus Trojan, which was known as an efficient botnet software, along with the “source code being released to the world in 2011” (1). The Zeus Trojan used keylogging to steal banking information from various victims infected with the trojan (1).

In 2013, two primary attacks are worth noting. First, as John Love noted in his article (1), the Cryptolocker caused grief globally as one of the “first ransomware programs”. Ransomware is one of the most complex and difficult to remove forms of malware as it usually completely locks a user out of using their device, pending some form of payment which does not guarantee the removal of the malware. Cryptolocker, along with many forms of ransomware use asymmetric encryption to encrypt (and sometimes) decrypt them. Asymmetric encryption requires the use of two keys, one public and one private. Usually, the files to be encrypted are done so with the public key, but then to unlock or decrypt the files you need the private key, which is held by the attacker. After paying the ransom, the attacker may give you the private key, but in some cases (particularly, one attack in 2017 that will be discussed intensively in this article), the attackers never give the private key to decrypt the files, even after payment is sent. According to an article from Kaspersky, “Cryptolocker was usually delivered by email attachments, again appearing to be a real attachment (such as .doc) but are double extended with a malicious .exe file” (9). The article also notes that “anti-malware would remove the trojan, but the files would remain encrypted even after removal (9).”

The second major attack in 2013 is well-known around the world as it made headline news due to the extent of compromised data. According to the Kill Chain Analysis 2013 Target Breach report to the US Senate Committee on Commerce, Science, and Transportation (10), “the 2013 Target breach was the result of an attack group compromising a third-party vendor to Target and then gaining access into Target’s network once inside. From there, the attackers released malware into the system and onto the POS (Point of Sale) terminals, which was able to strip the card data that was inserted into the server and send that sensitive information back to the attacker’s server.” The report goes on to discuss in more detail the attack and consequences, but ultimately millions of customer’s credit card data were stolen and sold on the internet black market. As an extreme case of a malware attack, this case could be considered cyberterrorism due to the extensive damage it caused. Not only did customers have sensitive information stolen, but Target’s reputation suffered as a result, shown easily in its stock performance months after the attack.

The 2013 Target Breach would be one of the largest and most destructive malware attacks over the next few years. A few, smaller cases are worth noting before 2017: In 2014 a new malware called Backoff was released into the wild, targeting POS systems like the malware used in Target’s attack, although not as too much of an extent. (1). According to an alert posted by the U.S. Cybersecurity & Infrastructure Security Agency in 2014, “Backoff is primarily being used to compromise businesses with remote desktop apps, use brute force to log into the desktop and then use POS malware to exfiltrate credit card information with an encrypted POST Request” (11). The alert also mentions that the Secret Service itself was investigating these attacks. Primary methods Backoff used were “memory scraping, keystroke logging, command & control communication, and malicious stub injection into explorer.exe” (11).

Finally, in 2016 (1) the Cerber ransomware was released although this ransomware was unique compared to other recent forms of ransomware. According to an article from Malwarebytes, “Cerber was an application that used ransomware-as-a-service, in which attackers would purchase and then use the malware. Developers even received a commission for the purchase and use of the malware” (12). This ushered in a new era of malware, purchasing already-written software that is readily available for use. Likely, the malware had previously been sold before, but the conception of ransomware-as-a-service is modern and unforeseen before the ransomware era. A picture of an infected computer is included below (13):

Text, timeline

Description automatically generated

To conclude this subsection, it is important to take away a few key points and facts from the intensive evolution of malware. First, the evolution of malware software during modern times should be summarized. Initially beginning as early 2000 email attachments, malware grew to include using social media and becoming harder to detect. It became more widespread and saw the creation of new forms such as advanced trojan horses, adware, spyware, and ransomware. Larger organizations began using it as a form of cyberterrorism and even government bodies are said to have used it for cyberwarfare purposes. The data stolen using POS malware has been sold on the black market of the internet, and ransomware began seeing cases of attackers being paid to unlock the device and choosing to keep the money. Indeed, the use of malware has truly become a weapon against society.

Before investigating one of the most widespread and dangerous malware attacks in history that occurred in 2017, and the final example of malware in this paper, it is important to quickly note the AV-Test and vital statistics collected over the years. According to their official website, AV-Test.org, “The AV-Test is an independent IT-Security Institute located in Germany that conducts research, comparison and individual tests on IT security products” (14). One final note- according to their website, “The institute registers over 350,000 new malicious programs a day” (14). This statistic echoes the earlier words of this paper, as malware has grown exponentially since its conception. The AV-Test has collected data on total malware applications over the years, and their graph is depicted below (15).

Chart, bar chart

Description automatically generated

# III: Case Study: WannaCry Ransomware (2017)

Graphical user interface, text

Description automatically generated

In 2017, the world saw how dangerous malicious code can become a global problem. WannaCry emerged from the depths of the dark internet and infected hundreds of thousands of computers all around the globe. The picture above (16) is the infamous screen a user would be looking at after infection and file encryption was complete. While this was not the first instance of widespread ransomware, WannaCry was an instance of cyberterrorism, global impacting, and contained complex bit of malicious code that resulted in millions to billions of dollars in estimated damages. According to an article from the U.S. National Cybersecurity and Communications Integration Center (17), WannaCry “exploited vulnerabilities in the Windows SMBv1 server to remotely compromise systems, encrypt files, and spread to other hosts”. The article even states that the U.S. Government discouraged paying the ransom, as there was no evidence the attackers would provide the decryption key.

Similarly, to the older ransomware Cryptolocker, WannaCry used an asymmetric key encryption system that uses a public and private key to encrypt and decrypt files, usually respectively. Again, even those who paid the ransom were not guaranteed to get the decryption key, and many did not ever get their files back. There was no easy fix to this malware infection short of wiping the entire computer and restarting, thus losing everything. Even those who downloaded their encrypted files would still come back to them being encrypted on the fresh Windows OS. The only viable solution besides a complete wipe was restoring the system from backup versions.

According to an article from Computerworld, Microsoft did release a patch once the vulnerability was found, a few months before WannaCry being deployed. (18). The article does mention an important piece of information however, not every victim of the WannaCry could install this patch. For example, one of the “major victims of the infection were hospitals”, and in some of these hospitals, they could not update the systems with a patch because of “vendor-relations” regarding the medical devices infected (18). In some cases, “the patch would render the device unusable” (18) which of course is not suitable for a hospital or medical environment. On the other hand, choosing not to install the patch and being infected with the malware would result in the same scenario as WannaCry essentially renders the infected device useless, again short of rebooting from backup files or wiping the OS.

Another article from Kaspersky discusses the WannaCry attack in further detail. Once the device was infected, the attackers demanded payment via bitcoin, initially at around $300 (19). This can be seen in the picture provided at the beginning of this subsection. To increase the level of concern and fear in the victim, another message stated that if they did not pay in three days the price would double, and if it was not paid within a week, the files will never be recoverable. A very interesting note is made from Kaspersky’s article: “reportedly, the coding in the malware execution was bad as it did not have an association to link the infected device and the payment” (19). Of course, the public would not have known this at the launch of the malware attack, but it is extremely interesting because bad code such as this, further leverages the reason not to pay ransoms in ransomware attacks. It does, however, raise an interesting question. Was the code actually “bad”, or was it intentionally made that way by the attackers?

It is unknown how many people paid the ransom and the exact figure the attackers made from the illegal cyber-attack, but the attack lasted globally for a few days before news headlines and public awareness, along with increased precautionary measures slowed the rate of the infection. Numerous computers were damaged throughout the attack, and because of WannaCry, the world became even more security-conscious than before.

# IV: Futuristic Malware

The future of technology and computers is exciting. As it continues to advance there are new avenues that may be available that were previously inaccessible. Consider scenarios such as planet terraforming, and a second, more powerful version of the International Space Station that is further out in space than the current ISS. However, it is important to remember that with technological advances there will also be cyber-crime advances to counter. Looking at the previous sections in this research paper, consider the advancement from infected floppy disks to infected emails, and later into websites that automatically download infected executable files. Similar advancements in the future are inevitable and could prove to have high consequences. Consider two hypothetical scenarios of future malware:

Currently, the internet is mainly restricted to being just inside the planet. Astronauts’ aboard spacecraft and the International Space Station primarily use radio waves to communicate with Earth. However, in recent years NASA and engineers have been working on a project called the Laser Communications Relay Demonstration to expand and stabilize internet access in outer space (20). Imagine in the future if a new ISS (International Space Station) or manned spacecraft was built in the outer reaches of our inner solar system, such as around Saturn or Uranus. If these stations and spacecraft retired radio frequencies and relied on internet access for communications, there could be a potential malware attack payload transmitted to the station. Consider a situation where a cyber-terrorist organization was able to successfully deliver a malicious software executable to the space station and take over the system. The consequences could be catastrophic- they could potentially override the station controls (or spacecraft controls) and change coordinates, modify oxygen output, and so forth. What if contact with extraterrestrial life was made, and the spacecraft had futuristic space weapons? It may sound like something out of a science fiction movie, but this could hypothetically happen with futuristic malware, and enforces the importance of cybersecurity countermeasures to these potential attacks.

In a second hypothetical scenario, and more likely to happen in the future, consider a countries nuclear payload system being compromised by advanced, sophisticated malicious code. Perhaps a country is at war with another and has its military cyber team send a payload to compromise its defense systems and take over a nuclear warhead launch site. Or an intelligent, resourceful terrorist organization has the resources and technology to send an advanced malware payload through a strong defense network of firewalls and anti-malware. Theoretically, if the malware were able to successfully infiltrate the receiving countries defense grid, the attacking country could gain access to its nuclear missiles. This alone is a terrifying scenario, as the attack group could be in control of a country’s nuclear arsenal. Should this scenario occur and not stopped quickly, the threat actor could launch nuclear warheads at another target, resulting in catastrophic cyberwarfare.

These are just two hypothetical scenarios that could be the result of futuristic and advanced malware attacks. With the history of cybercrimes, technological advancements, and the evolution of malware, it is important to remember to keep up with technology and anti-malware software. It is almost ironic- the original Creeper virus printed a message: “Catch me if you can!”, and ever since the IT world has been in a constant race to keep up with a defense against malware and cyber-attacks. While these hypothetical scenarios are unlikely to happen due to excellent cybersecurity knowledge, education, and defense systems in place, one thing is for sure: technology and malware will continue to advance in the coming years.

# Coda

Malware has significantly changed, been enhanced, or upgraded numerous times since its conception in 1971. Once originally designed as a joke, prank, or simply a way of showing someone their system had a vulnerability, it has evolved to become a devastating weapon in cybercrimes. In essence, malware went from a printed message stating “I’m the creeper, catch me if you can!”, to millions of credit card data being seized and sold for illegal funds. Today, there are now five reasons an attacker will use malware:

1. To steal sensitive information
2. To bribe or coerce one into giving the attacker money
3. To intentionally disrupt or otherwise cause damage
4. Cyberterrorism
5. Cyberwarfare

Malware’s evolution and immerse changes are nothing short of shocking. Originally a result of a test, then becoming used for pranks and inconveniences, to later being a weapon of cyber terrorism and cyberwarfare is jaw-dropping. Its history is short but intense, and there have been countless cases of attacks over the years. As is forever true in the world of cybersecurity, the key is to keep upgrading systems, checking for vulnerabilities, internal penetration testing, education, and acting quickly on an attack. Businesses should maintain a high level of internal and external security such as using VPNs, having strong firewalls, maintaining multiple defense systems, and keeping sensitive data deep inside the defense perimeter so it is harder to access from attackers. The public should be cautious when receiving suspicious emails, maintaining strong passwords, keeping anti-malware updated, and using VPNs over public networks.

For every upgrade there is on a system, server, or network, there is most certainly an attacker out there writing new malicious code. For every new application or system created, there will be malicious software waiting to be deployed. Being vigilant with technology and understanding the risks of malware cannot be overstated.

# References

1. Love, P., & Love, J. (2019, September 19). A brief history of malware-its evolution and impact. Retrieved March 21, 2021, from <https://www.lastline.com/blog/history-of-malware-its-evolution-and-impact/>
2. <https://s3.amazonaws.com/s3.timetoast.com/public/uploads/photos/11044129/download-20.jpg>
3. <https://2.bp.blogspot.com/-U83lRnHlBmM/WI6_ikuVtmI/AAAAAAAAAMU/7bthvPeIySsqaoomHw-jojTUSkunJMdrACEw/s1600/morrisworm.jpg>
4. <https://zdnet4.cbsistatic.com/hub/i/2014/08/28/2849efd0-2e55-11e4-9e6a-00505685119a/f80db6db92ddb6ad10316a6d70da026b/viruses-melissa-jr-whipple.jpg>
5. White, G. (n.d.). The 20-year hunt for the man behind the Love Bug Virus. Retrieved March 21, 2021, from <https://www.wired.com/story/the-20-year-hunt-for-the-man-behind-the-love-bug-virus/>
6. <https://www.pinoyhacknews.com/wp-content/uploads/2014/05/payload_I_love_you-641x330.gif>
7. <https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf>
8. <https://cdni.rt.com/files/oldfiles/news/flame-stuxnet-kaspersky-iran-607/photo-wordyouru.n.jpg>
9. Kaspersky. (2018, August 06). Cryptolocker virus definition. Retrieved March 21, 2021, from <https://usa.kaspersky.com/resource-center/definitions/cryptolocker>
10. U.S. Senate Committee on Commerce, Science, and Transportation, March 26, 2014, “A Kill Chain Analysis of the 2013 Target Data Breach”
11. Alert (TA14-212A). (July 31, 2014). Retrieved March 21, 2021, from <https://us-cert.cisa.gov/ncas/alerts/TA14-212A>
12. Ransom.cerber. (2020, October 20). Retrieved March 22, 2021, from <https://blog.malwarebytes.com/detections/ransom-cerber/>
13. <https://www.varonis.com/blog/wp-content/uploads/2018/09/cerber-ransomware-1-787x464.png>
14. About AV-TEST: Antivirus & malware DETECTION RESEARCH. (n.d.). Retrieved March 22, 2021, from <https://www.av-test.org/en/about-the-institute/>
15. Malware statistics & Trends REPORT: AV-TEST. (n.d.). Retrieved March 22, 2021, from <https://www.av-test.org/en/statistics/malware/>
16. <https://images.techhive.com/images/article/2017/05/wannacry_ransom_screenshot-100722810-large.jpg>
17. <https://us-cert.cisa.gov/sites/default/files/FactSheets/NCCIC%20ICS_FactSheet_WannaCry_Ransomware_S508C.pdf>
18. Winkler, I. (2017, May 16). Wannacry: Sometimes you can blame the victims. Retrieved March 22, 2021, from <https://www.computerworld.com/article/3197048/wannacry-sometimes-you-can-blame-the-victims.html>
19. Kaspersky. (2021, January 13). What is WANNACRY RANSOMWARE? Retrieved March 22, 2021, from <https://usa.kaspersky.com/resource-center/threats/ransomware-wannacry>
20. Garner, R. (2017, March 21). First steps toward high-speed space 'internet'. Retrieved March 22, 2021, from <https://www.nasa.gov/feature/goddard/2017/nasa-taking-first-steps-toward-high-speed-space-internet>