**Determining the Best Defense Against Malware and Ransomware**

**Cowen M. Hames**

The Iowa State University of Science and Technology

Graduate College | Ivy College of Business

Department of Information Systems and Business Analytics

MIS 599: Creative Component

Dr. Anthony Townsend

January 24, 2022

**ABSTRACT**

In 2017, the world experienced one of the most damaging cyberattacks in the modern era of cybersecurity, the WannaCry ransomware attack. With the world becoming ever-more dependent on technology and cyber criminals likewise becoming more strategic, the case of WannaCry is a critical pillar of understanding future cybersecurity needs. This literature review will examine numerous research articles to explore and understand malware, ransomware, and WannaCry, thereby helping to determine which prevention techniques are best at preventing future ransomware attacks like WannaCry. It will examine semi-depth to in-depth technical aspects of malware, their components, deployment process, objectives, target victims, and ultimately pinpoint using a combination of mitigation strategies as the best defense strategy against fighting malware and ransomware.

*Keywords: WannaCry, Cybersecurity, Malware, Ransomware, Mitigation, Prevention, Anti-Malware, Detection, Encryption, Decryption, Cerber, Cryptolocker*

**Determining the Best Defense Against Malware and Ransomware**

Ransomware is a child of malware, which is short for malicious software. Malware exploits vulnerabilities to steal information or to cause the disorder. Malware and computer viruses were born in the 1970s, originally intended as humor or soft gain. However, as the years went on, malware became extremely dangerous software, damaging countless computers and becoming a staple in the cybercriminal underworld. Ransomware takes even further advantage of users and usually receives payment in exchange for having access to the computer again.

Most ransomware files are downloaded to a computer in numerous ways, such as after a user unknowingly clicks on a malicious email attachment or downloads a file impersonating a legitimate purpose. Once the file is downloaded, malicious code is executed on the device, resulting in usually one of two scenarios. "Locker" ransomware will lock the computer from use, displaying only a single page demanding payment be sent to a location or never be able to use the computer again. The second and more modern version is a bitcoin variant, where important files are encrypted (the encryption process is additional code in the executable file). In this situation, a message is displayed to the user saying their files will be locked until payment in bitcoin is received. Usually, there is a timer to encourage the user to act quickly and a threat saying if payment is not received, the attacker will delete the files.

WannaCry was a 2017 global attack that was extremely large and widespread. It affected over 150 countries and 200,000 computers. The attack saw illegal funds of around $100,000 and affected multiple businesses- including train companies, hospitals, and FedEx (Berr, 2017). At the time, its spreading capability and results were unprecedented. WannaCry has changed the cybersecurity landscape- for consumers, businesses, threat actors, and cybercriminal organizations. This literature review will study malware and ransomware. This review will also study WannaCry itself to help determine the best mitigation strategy for future malware and ransomware attacks.

**LITERATURE REVIEW PART I: MALWARE AND RANSOMWARE ANALYSIS**

**Malware**

WannaCry is four levels below the basic understanding of cybersecurity. To fully understand the in-depth components, process, and ultimately mitigation strategies- we must first understand the core foundation from which it stems. Malware is a form of malicious intent in software that contains malicious code to attack, extract, or otherwise infiltrate a device using vulnerability exploitation. Originally isolated in computers, malware has since evolved rapidly- becoming a universal weapon in the cyber world. Malware can be found on almost any device- phones, tablets, external storage, and computers.

The malware was originally used on floppy disks- one of the first being the Brain. A. This malware was used as a symbol of the practice, in the sense that it did not conduct malicious intent- rather showed the event occurring (Patten, 2017). Malware would mutate into different forms, from primitive floppy disks to operating system infections. Generally, malware could infect Microsoft Word documents or update patch files, but in these early stages, minimal damage was caused (Patten, 2017). Eventually, malware would mutate again in the 1990s and 2000s by taking advantage of the internet. This critical milestone was monumental to the cybersecurity landscape, as malware could rapidly traverse multiple devices. Numerous forms of malware were seen during this time, namely the Melissa Virus, ILOVEYOU, and Happy99- all three of these being email attachment forms of malware (Patten, 2017).

Pre-Ransomware era malware all work similarly. The core of malware is the malicious executable file, code that executes a certain command- resulting in various activities. The malicious code is usually obliviously downloaded by a user through email attachments, file downloads, or program installations. Different types of malware behave differently; however, malware analysis tools can study their behavior. Using a malware analysis platform named Anubis was able to monitor the behavior of malicious program samples. Researchers discovered numerous behaviors, but a handful had a large sample pool. These include file creation, file deletion, showing a GUI window, utilizing network traffic, and modifying a registry key. All these behaviors had a greater than 30% of the sample pool (Bayer et al., 2009).

Additional components of malware include the Obfuscator (packer or protector for encryption and compressing), components to help keep the malware in the device, components to help conceal it from detection, "armoring" to help stay hidden from researchers, and command & control (the command center for the package) (Mohanta et al., 2018). Of these- the anti-detection and armor components are the most interesting as they contribute heavily to the problem of late detections. Note that these components are not always used or always the same and can see numerous modifications between different malware agents. In Mahanta's excellent book, readers can find additional valuable information about a deeper understanding of malware technical operation (by discussing windows operating systems functions), but that is outside the scope of this research paper.

Malware has since spawned several children variants, namely spyware (designed to watch user activity), adware (malware hidden in ads running on website scripts), and ransomware (discussed in the next chapter)- each coming with additional challenges and security concerns. Before the rise of ransomware, malware could modify computer files, steal information from computers, delete important files, and even render devices unusable. While these behaviors are undoubtedly malicious and cause loss to the device and users, they were essentially limited in the sense that no other monetary commitment would be made other than device resolution. In many cases, malware could be discovered using anti-malware software and subsequently removed (the primary solution post-infection). In more severe cases, the device may have been unusable post-boot up, but the device could be restored using BIOS commands at startup (whether from a past update or a complete wipe of the drive). Despite this, it can still be costly to remove malware, particularly on enterprise devices that may cause service interruptions during malware removal.

In a more recent case, a study performed by those at the University of Maryland used CRIU-MR, a process that reverts a server system before malware infection using Checkpoint/Restore in User-space (CRIU) (Webster et al. 2018). Essentially, the source code in CRIU is modified to work with essential malware detection tools and removes malware (within Linux) while a checkpoint/restore event is active (Webster et al., 2018). This process is time-efficient and therefore results in low service interruption impact.

Prevention techniques are critical to the security and integrity of both personal and business enterprise cyber security. Specifically, preventing malware is the best-case scenario, but it may not always be preventable. When an attack is not prevented, malware detection is critical to preventing further damage. The four primary methods of malware detection are anti-malware software (including detection software), update patches, host firewalls, and cybersecurity education. While three of the four are strictly IT-related, education can be practiced by any device user, and extensive IT knowledge is not required. Simply being aware of what malware can do, being cautious when downloading files or opening email attachments, and avoiding suspicious websites can help avoid malware attacks.

The other three methods are IT-focused. Anti-malware software is a critical tool that can monitor for and help detect malware on a device and be up to 98% effective in detecting malware (Garuba et al., 2008). Anti-malware software does have downsides, such as it being complicated to manage on separate user devices, multiple anti-malware programs working together, and the ability for users to disable the software (Garuba et al., 2008).

Patch updates are another critical tool in preventing malware, like operating systems programs, and any tool that uses code can contain vulnerabilities that patches can resolve. The time between vulnerability discovery and patch deployment is critical to the number of event preventions. Some downsides include the time between deployments, managing devices that may be offline, patches that cause misbehaving applications, and the non-stop race to keep up with new forms of malware (Garuba et al., 2008). Some researchers, however, argue that (especially against fileless malware) patch management (along with a combination of good detection software and response) is critical to having a strong defense foundation (Baldin, 2019).

Finally, firewalls provide excellent protection from malicious websites, although this is largely restricted to web-based malware, as it is not highly successful in preventing application/software-based malware (Garuba et al., 2008).

Additional forms of malware include the following (Mohanta et al., 2018):

* Backdoor (use of a port to gain unknown access to a device)
* Download (software that installs malware afterward)
* File Infector (malware code added on to legitimate code in software)
* Worm
* Botnet
* RAT
* Hacktool
* Keylogger (one of the most known forms of malware, this form is notorious for its ability to capture keystrokes then send that data back to the attacker, resulting in password theft)
* Banking (malware specifically designed to attack banking systems)
* POS (malware that attacks POS systems in businesses. The 2013 Target Breach is a notable example)
* Exploits
* Ransomware (Discussed in the next chapter)

Analysis of malware itself is worthy of a research paper or literature review, and many articles are available for more in-depth research of malware in its entirety. For this research paper, we want to cover essential information of the family that WannaCry belongs to before discussing its parent- ransomware. The key points of malware and mitigation strategies against it are:

* Malware is a malicious software program intended to damage or infiltrate a device.
* It has been around for at least 40 years, seeing prominent use in the early 2000s
* Its core component is typically an executable file or program that executes malicious code.
* Its principal delivery methods include file downloads, email attachments, web browse scripts, and legitimate infected software.
* Prevention and mitigation strategies include cybersecurity education, update patches, anti-malware software (including signature-based, anomaly-based, and specification-based) (Idika, Mathur, 2007), and network firewalls.
* The two solutions for handling malware for post-infection actions are malware removal programs and device restoration/reset.

**Ransomware**

As the internet grew, more data and processes became integrated over the modern era. Such functionality contains extremely sensitive data- online banking statements, online tax preparation documents, employee records, PII storage, sales and loss reports, manuscripts, and many others. The rapid digitalization of information has also had a rapid increase in interest from cybercriminals. While malware still serves its purpose to cybercriminals, many began taking an interest in the possibility of financial gain from an attack- with the FBI projecting over $1 billion in losses from ransomware attacks in 2016 (Brewer, 2016). The core process of ransomware is significantly different than general malware attacks, as ransomware intentionally encrypts files on the device, with the decryption key being held by the attacker(s) (Aldaraani, 2018). The attackers then demand a ransom in exchange for the decryption key, although it is never guaranteed to provide the key (O'Gorman, 2012). In many cases, the files are lost forever, mainly when the data is not backed up on an external device or database.

The first ransomware was created by Joseph L. Smith, who created the AIDS Cyborg trojan, which was on a floppy disk and demanded $189 (ComputerForensicsWorld, 2021). Since then, numerous ransomware variants have been developed, but the two primary ransomware families are lockers and bitcoin variants. Locker variants (like the FBI locker) completely lock the user out of their device, rendering it useless without the decryption key (O’Gorman, 2012). The bitcoin variant is a newer version where some functionality remains on the device, primarily to have the user use the tor browser to pay the attackers in bitcoin (which is generally untraceable) in exchange for the decryption key. As a result, from the device losing functionality, the ability to utilize an “anti-ransomware” program is not generally usable (if the executable runs) as such programs are with general malware attacks. More specifically, the ability to run other programs is lost when the ransomware code is executed because that code disables the ability to execute other programs (O’Gorman, 2012). Additionally, ransomware variants are quickly deployed, with newer forms frequently deployed. These new forms make having a known ransomware "watch list" difficult to update and detect by malware detection software.

Ransomware deployment varies greatly. Typical deployment strategies are already mentioned before- file downloads, email attachments, and malicious code is hidden inside a legitimate program. However, one of the most popular methods is using websites. Research done by Abhijit Mohanta provides an excellent example of how "drive-by downloads" work. Web sites are subject to vulnerabilities, and if a site is vulnerable, it is subject to injection attacks. In this case (Mohanta et al., pg. 78-79), a website was compromised, and its iframe code (related to the JavaScript function, which is outside the scope of this paper) was replaced with an injected (malicious) iframe. As a result, when a user went to the legitimate website, they were automatically redirected to a malicious website, resulting in a "flash exploit" to download ransomware, in this case, the Cerber variant. Adware works similarly, with online advertisements on websites being compromised and malicious code injected inside them, resulting in an executable file being downloaded or (like website redirects) being redirected to a malicious website and having automatic file downloads.

In summary, ransomware works like its parent in many ways, but with a few key differences. First, the objective of attackers using ransomware is almost always to obtain revenue. Ransomware can extract data from an infected device but does not appear to be as much of a focus as other malware variants. Second, ransomware can generally be resolved without some loss (Crypto- ransom money or data, and Locker- ransom money or everything on the device). While it is possible to boot the device in safe mode and access anti-malware software, the encrypted files will remain encrypted even if ransomware is removed- if the anti-virus software can find the malicious files (Belcic, 2020). Awareness and education about ransomware are almost always the best way to prevent it, and in this case, prevention is always better than being infected). Below are critical concepts of ransomware:

* Ransomware is a child of malware created in 1989 and saw prominent use around 2005. Instead of focusing on damaging the device, it uses encryption to encrypt users’ files (or lock the entire computer), not allowing the user to access the device until paying the ransom and obtaining the decryption key. Additionally, the files are subject to theft from the attacker even if the ransom is paid (Mos, Chowdhury, 2020)
* Contains two major variants (Locker and Crypto). A locker is a screen/program locker that locks the entire computer, demanding ransom for the decryption key. Crypto also locks program executions but allows the user to access a tor browser to send cryptocurrency in exchange for the decryption key.
* Lacks a “cure” like older variants of its parent malware. While there are detection programs available to detect and stop ransomware from executing (Kurniawan, Riadi, 2018), it is virtually impossible to bypass the encryption without the key- short of factory restoring the device and losing everything on it (unless a decryption program has been able to decrypt them, however, many professional ransomware variants are extremely complex, and their algorithms are very difficult to decrypt). (Filiz et al., 2021). Additionally, research conducted to determine ransomware decryption effectiveness yielded troubling results- out of 78 decryption tools against 61 ransomware samples, roughly 50% of the decryption programs did not successfully decrypt the files. (Filiz et al., 2021).
* The key difference between ransomware and malware detection is that if the detection software does not work on the ransomware variant, the device is locked out, resulting in either device restoration or boot up in a safe mode and attempting to run anti-virus software to remove the virus.
* Despite its primary focus of extorting money, ransomware can perform older malware functions, including extracting files and sending them back to the attacker using the command center in the malicious executable file. C&C is also capable of receiving instructions from the attacker- allowing the virus to perform additional actions post-infection
* Mitigation strategies include cybersecurity awareness and education, app control, patch management, strong network security (including appropriate firewall usage), and backup of important files and data.

**Malware and Ransomware Variants- Expanded**

At this point in the research, we have reviewed an overview of malware, ransomware, its components, functionality, and mitigation strategies. We will research specific variants to better understand these mitigation strategies (a brief description, principal delivery method, data on damage if available, and mitigations). Following this section, we will deeply research Wannacry and answer the question, "what is the best defense against malware and ransomware attacks?”.

**ILOVEYOU (Malware)**

The ILOVEYOU virus (aka Love Bug) appeared in numerous emails to users worldwide and was one of the original mass distributed variants of malware. With a simple email with a text attachment, the virus would end up infecting 45 million computers, including the World Health Organization and the Pentagon (Hajioff, Mckee 2000). The attacker compromised the address book from Microsoft Outlook, emailed 50 addresses, and then spread like wildfire across the world. Symantec and F-Secure's anti-virus companies launched anti-virus updates specifically for ILOVEYOU, which detected and removed it (Hopper, 2000). The attack was alarming that the US Senate even shut down their email servers (Hopper, 2000). Ultimately, the virus would rename and transplant media files and then direct the browser to a malicious website that downloaded additional malware, sending stored passwords on the device to the attacker's website (Knight, 2000). In this case, we can make a few key points:

* Cybersecurity Education and Awareness could have significantly reduced the number of infections. Being suspicious of emails and their attachments is vital to preventing malware.
* Detection software developed from anti-malware software stopped the infection.
* The speed of this virus was unprecedented and cemented the importance of time between discovery and mitigation. ILOVEYOU would be the beginning but far from the last of malware utilizing the internet to spread- acknowledging the importance of network security.

**Zeus (Malware)**

Zeus, originally appearing in 2007, is a toolkit that makes information-stealing trojans, which typically attack banking and financial data (Wyke, 2011). The trojans use stealth to steal login information sent back to the attackers, although numerous data types are stolen (Wyke, 2011). Available on the dark web in both free and high-costing versions, the Zeus toolkit has an easy learning curve, and as a result, numerous instances of Zeus exist (Wyke, 2011). While the components of Zeus are available in Wyke's research article, we will not discuss them here as we are more focused on its operational model, impact, and mitigation strategies. Wyke discusses Zeus's functionality in detail, which is essential to understanding the overarching purpose of mitigation and operation. Key functionalities include decreasing the users’ browsers security settings, using API hooks for data theft, extracting stolen data and sending it back to the attackers using the command-and-control center (a constant process of many malware variants), and self-copying/self-destruction of the original executable file that is downloaded (Wyke, 2011).

Interestingly, attacker bot-commands were discovered and are mentioned in Wykes's article, some with particular interest. The commands "user\_cookies\_get" allow the attacker to harvest data from cookies, and "user\_cookies\_remove" allows the attacker to remotely delete the users’ cookies, requiring them to re-enter login information (and thus allowing the attacker to harvest that newly entered data). Additional commands include "user\_certs\_remove," which deletes digital certificates, and "user\_ftpclients\_get," which allows the attacker to steal FTP credentials saved by FTP clients (Wyke, 2011).

Additionally, another technical aspect of Zeus is in its most recent version, and the executable will clone itself to the user’s application data folder, using a random filename and directory name (Wyke, 2011). This process (in addition to more technical details outside this scope) essentially allows multiple Zeus trojans to compromise the entire device, and different user profiles can become compromised (Wyke, 2011). This attack can be catastrophic in a business setting, particularly where multiple people share devices. There is a lot more in-depth research done on Zeus, but to wrap up our focus on it:

* Zeus was one of the most popular malware attacks in the late 2000s
* It primarily focused on stealing financial data (banking malware)
* It was readily available on the dark web, featuring different versions
* Took advantage of cloning and self-destruction of its original file
* Also took advantage of the Application Data folder, giving it the capability to infect the entire device and compromise multiple user accounts on a single device
* Deployment strategy was through API injections on websites
* Mitigation strategies are cybersecurity education, awareness, network security measures, backup of files, and malware detection software.

**Cerber (Ransomware)**

Another dangerous variant of ransomware is the Cerber variant, appearing in 2016. This ransomware was similar in terms of functionality, following the ransomware standard. Malicious executable files are usually installed through compromised websites, malicious ads, and the "drive-by download" we discussed earlier in this research paper (Kurniawan, Riadi, 2018). One notable piece of research by Kurniawan and Riadi is noted that the Cerber variant will check the devices IP geolocation and if the device is in Armenia, Azerbaijan, Belarus, Georgia, Kyrgyzstan, Kazakhstan, Moldova, Russia, Turkmenistan, Tajikistan, Ukraine, or Uzbekistan, it will stop code execution and not encrypt the files on the device. This conditional is without a doubt intentional as Cerber originated in Russia (Kurniawan, Riadi, 2018). Once Cerber initializes and executes, there is little to decrypt the files other than removing the virus and having data backups (Belcic, 2020). To stay inside the scope of this paper, we will not discuss the in-depth details of the Cerberus process, but its overall operation is typical of other ransomware variants. Key facts of Cerber are:

* Appearing in 2016, Cerber was one of the most prominent ransomware variants in the 2010s
* It had typical process features like other ransomware and had similar deployment strategies.
* Prevention is the best defense against Cerber since decryption of files is usually near impossible.
* Other mitigation strategies include strong network security and offline data backups.
* Post-infection solutions include device restore or booting in Windows Safe Mode and running anti-virus software to remove Cerber (if the software can detect it)

Before diving into WannaCry, we will briefly discuss different ransomware strains in recent years to help emphasize the seriousness of ransomware. The following attacks are short explanations from Julian Dossett’s article (Dossett, 2021) to cover recent attacks for our research.

**CryptoLocker (Ransomware)**

Appearing in 2013, CryptoLocker would be one of the first modern prominent ransomware variants, infecting over 250,000 devices and resulting in over $3 million in revenue for the attackers. (Dossett, 2021).

**CryptoWall (Ransomware)**

Another variant of ransomware following CryptoLocker in 2014, this strain resulted in $18 million in losses and was known for multiple variants resulting in difficulty detecting it with detection software. (Dossett, 2021).

**Locky (Ransomware)**

Locky was a notorious strain of ransomware in 2016 that caused a massive amount of device infections. Deployment was primarily via an email attachment, which affected upwards of 50,000 devices in one day (Dossett, 2021).

**Travelex (Ransomware)**

A strain from 2019, this ransomware extracted customer PII from Travelex. The attackers ended up obtaining a $2.3 million ransom from Travelex in exchange for the decryption key (Dossett, 2021). This case highlights the damage that an attack on a business can have.

**CNA Financial (Ransomware)**

In an attack just last year in 2021, a cybercriminal group called Phoenix used locking ransomware to extort $40 million from CNA Financial (Dossett, 2021).

**Colonial Pipeline (Ransomware)**

The Colonial Pipelines network was compromised by attackers last year in 2021, resulting in $4.4 million from the ransom and major gas issues on the east coast in the United States. The attack was widely reported on major news networks (Dossett, 2021).

**Literature Review Part I Closing**

We have reviewed research and provided our insights on an overview of malware and ransomware until this point. We have also investigated several strains of malware and ransomware and have come to the following conclusions:

* Malware and ransomware have become highly sophisticated in recent years, with attackers utilizing knowledge, resources, and the dark web to successfully attack countless devices
* While attackers have become more diligent, so have mitigation techniques. We have seen in research articles the use of malware detection software, ransomware detection software, network security protocols, education and awareness, the use of offline data backup, device restoration, the use of Windows safe mode, and patch update management. Specifically, anti-malware software, backing up of files, and update patching are notable important in the “ABC of ransomware protection” research journal (Furnell, Emm, 2017).
* While most of these mitigation techniques help somehow, there are criticisms. Patch management requires timely deployment. Offline data backup faces security issues and requires diligence on the user’s part. Device restoration is not a viable solution, particularly for businesses. Booting in Windows safe mode and using anti-virus software depends on getting to the software to detect the malware (which is also a critique on detection software). Network security is not always managed appropriately and may have loopholes and devices outside the network connecting to it later.
* Education and awareness to help prevent the attack from occurring in the first place is an important strategy for multiple reasons. First, being aware of suspicious emails, attachments, file downloads, and ransomware and malware is paramount to infection prevention. Additionally, awareness and education significantly assist detection- a critical prevention measure used in the defense against attacks. (Bansal, 2021). Second, education is not a manufactured solution- in the sense that education cannot have workarounds or fail to respond to an attack. The best defense strategy combines cybersecurity education and access to the tools needed to prevent attacks and help solve a successful one promptly to reduce the loss.

**LITERATURE REVIEW PART II: WANNACRY ANALYSIS**

**Overview**

WannaCry is a ransomware variant that appeared in 2017 and is notorious for being one of the most destructive ransomware attacks in history (Algarni, 2020). Essentially, the ransomware encrypted important files on the user’s device, demanding a ransom be paid in bitcoin. A timer would be displayed along with a warning message, saying that the attacker would double the ransom if the time expired. If the user still didn't pay after so long, the message said that the user would lose the files forever.

WannaCry quickly infected over 250,000 computers in 150 countries (Trautman, Ormerod, 2018). As Trautman and Ormerod explain, the Shadow Brokers group sold cyber weapons owned by the NSA in 2016. This same group would provide tools that exploited network security for Cisco and Huawei. Then in April 2017, Shadow Brokers released tools related to ETERNALBLUE- a zero-day vulnerability on Windows. (Trautman, Ormerod, 2018). WannaCry is considered a Ransomware-as-a-Service (RAAS) because even the code and process are complex, it (along with many other ransomware codes) is released on open-source locations, allowing virtually anyone to launch an attack (Hsiao, Kao, 2018).

The next chapter (Process) will be the most technical of the review as we analyze WannaCry by reviewing Hsiao and Kao’s excellent research on the insides of WannaCry.

**Process A- Deployment**

Technically, the first phase of a ransomware lifecycle (including WannaCry) is creating the malicious software by its author(s). After the ransomware is created, it is either sent to an attacker or group for deployment prep or uploaded on the internet in open forums to allow free access to unlimited people.

Following pre-deployment is deployment. WannaCry utilized the exploitation strategy for its deployment. It exploited the “MS17-010” vulnerability, thereby allowing it to run a “launcher.dll” with the Eternal Blue exploit and Doublepulsar backdoor (Hsiao, Kao, 2018). MS17-010 was a security update from Microsoft that patched vulnerability of the SMBv1 server- a vulnerability that allowed code execution from a remote attacker by sending messages to the Microsoft Server Message Block (SMB) (BetaFred, n.d.).

Following this, WannaCry abuses the SMB driver “srv2.sys” in the kernel module, thus allowing it to gain access to the device. (Hsiao, Kao, 2018). At this point, the device is fully compromised launcher.dll is inserted into lsass.exe system processing, becoming the loader for mssecsvc.exe (Hsiao, Kao, 2018). Following the execution of launcher.dll, “PlayGame” initializes WannaCry. Subfunctions “ExtractResource” and “CreateProcessMSSECSV” are called (Hsiao, Kao, 2018).

When the functions are called, each one has a specific task. Extract Resource extracts a writable file named "W/101," making an active process file (mssecsv.exe) in the C directory. Resources are loaded, and finally, the "CreateProcessMSSECSV" function calls the “CreateProcessA” method- resulting in “mssecsv.exe" running (Hsiao, Kao, 2018). WannaCry then begins to install. Throughout this first process, we can see that WannaCry works like other malware, in the sense that upon finding a vulnerability, the code is specifically designed to take advantage of that exploit. This situation is where patch management and cybersecurity education are critical to help defend against these attacks.

**Process B- Installation**

After "mssecsvc.exe" executes, the program checks whether the computer is real or virtual. Following this, two Windows API functions are called: “InternetOpenA” and “InternetOpenUrlA” (Hsiao, Kao, 2018). These functions check a domain name to see an active connection. If the domain exists and there is a connection, then "mssecsvc.exe” will quit- and no Wannacry infection will occur (Hsiao, Kao, 2018). Without connection, the process will continue, and "tasksche.exe" (the main executable of WannaCry" will run. Note that during the WannaCry outbreak, a malware analysis found the piece of code containing the URL checked and registered the domain- thereby slowing down the spread of new infections (Newman, 2017).

Other researchers debate the reason for the kill switch, but the most common theory is the attackers developed it as a form of anti-malware analysis. (Newman, 2017). As Newman explains, many attackers build these switches on purpose to stop malware analysis- in this with being tested by Virtual Machines (which can confuse the malware into thinking a connection to a domain is real even if it isn’t) (Newman, 2017). This situation shows that malware analysis and reverse engineering are also critical tools in defending against these attacks. Additionally, the kill switch's amateur code shows us that cybersecurity and technical education go both ways. In this case, an error on the attacker’s side ended up working against them.

Continuing in the malware analysis by Hsiao and Kao, “tasksche.exe” controls the loading of package resources and the environment for the imminent encryption. Infection occurs when “mssecsvc.exe” begins processing the MS17-100 and Doublepulsar backdoor exploits. On the attacker side, the “msseccsvc 2.0 service” checks the SMB protocol and port 445, looking for a successful connection (Hsiao, Kao, 2018). If there is a successful connection, the attacker messages (discussed earlier with Microsoft’s bulletin reference) will look at the Doublepulsar backdoor status. If Doublepulsar is not initialized, then the Eternal Blue attack will commence. At this point in the infection, the malicious package includes kernel shellcode, userland shellcode, and launcher.dll (including binary code from mssecsvc). (Hsiao, Kao, 2018). Finally, "tasksche.exe" is run by "mssecsvc.exe," and a zip file named “XIA” is retrieved from the resources in "tasksche.exe ."After the resource loading is complete, "XIA" is unzipped, and WannaCry begins the encryption process (Hsiao, Kao, 2018).

At this point, we are about 50% through the technical analysis of WannaCry. So far, through our literature review of Hsiao and Kao's impressive RE (Reverse Engineer) malware analysis, we have learned important processes of WannaCry, including deployment and infection. We can make the following key points at this point from this literature review:

* WannaCry utilized a software vulnerability from Microsoft that allowed messages to be sent through the SMB, allowing the attack to gain access to the device (Eternal Blue vulnerability)
* WannaCry is highly sophisticated and has a few key components, including "launcher.dll" (primary deployment package), “mssecsvc.exe” (process package), “tasksche.exe” (resource package), and “XIA” (WannaCry files)
* WannaCry contained a self-destruction key located in code written during the deployment of the virus. It checked to see if a random URL domain existed, and while likely intended to be a failsafe for anti-malware analysis, it ended up slowing the spread after being discovered by a malware analyst.
* At this point, we can determine that patch management, malware analysis, and education are all important in defending against WannaCry.

**Process C- Encryption**

Files become encrypted in the malware analysis (Hsiao, Kao, 2018). Specifically, the “tasksche.exe” program will execute a zip file, including the crown jewel of WannaCry: “t. wnry” (Hsiao, Kao, 2018). “tasksche.exe” will decrypt “t. wnry” into a “dll” file, becoming a TaskStart which initializes the encryption process. The encryption process begins, and WannaCry will use multiple pairs of keys during the process, such as RSA (Ron Rivest, Adi Shamir, and Leonard Adleman) and AES (Advanced Encryption Standard) algorithms (Hsiao, Kao, 2018). While on the same level of technicality as this literature review, RSA and AES are outside of the scope of our purpose and will not be discussed in detail here. Essentially, they are encryption algorithms that process file encryption.

At this stage, WannaCry will begin encrypting targeted files using an RSA root public key (Hsiao, Kao, 2018), while the attacker holds the private key (to reiterate the basic encryption process, after a file is encrypted, you need the private key to match with the public key to decrypt, hence the difficulty in decrypting files post-infection from WannaCry). WannaCry will continue encrypting files while also deleting original files. WannaCry will use wiping to prevent the victim from recovering files on the user desktop, user documents, all user’s desktop, and all user documents for which “taskdl" is responsible (Hsiao, Kao, 2018). If the file is not deleted, it is moved to the hidden recycle bin, in addition to being overwritten by “CryptGenRandom()”- a function in WannaCry that replaces original file contents with random numbers (Hsiao, Kao, 2018). After file encryption, the infamous WannaCry GUI window will appear, displaying the countdown to file deletion, bitcoin ransom amount, instructions, and the “decryption tester” button. The example button will allow up to 10 files in the C drive under the Program Data directory to be decrypted (Hsiao, Kao, 2018). The time between infection and the WannaCry GUI window is very quick, and the user cannot stop the process (without detection software).

**Process D- Command and Control**

From this section of the attack to eradication, the user will be looking at the WannaCry GUI window. While the GUI is active, “wanadecrypter.exe” is running- establishing and maintaining a connection between the infected device and the attacker’s server. This connection involves a TOR service and an onion server (Hsiao, Kao, 2018). During this connection, information from the infected device is sent to the attacker, and this is also the connection needed for the transfer of the bitcoin ransom payment. We now conclude the literature review of Hsiao and Kao’s research.

Before discussing the impact of WannaCry worldwide and ultimately our conclusion from this analysis, there is interesting research conducted on “splash screens” (the GUI window displayed to the user post-infection with ransomware). A controlled study was conducted in the Journal of Information Security and Applications that had 538 users interacting with one of three ransomware splash screens. The study concluded that the ransomware splash screen elements did not significantly impact the chance of the user paying the ransom or reporting the incident. 60% of the users said they would like to report an attack but did not know-how. Lack of trust was the main reason for the users not wanting to interact with links depicting cybersecurity advice after interacting with the splash screen. As this controlled study concludes, there is a lack of public awareness about reporting cybercrime, and more effective methods are needed to encourage cybersecurity behavior (Yilmaz et al., 2021).

**Impacts**

WannaCry infected over 250,000 computers worldwide, affecting over 150 countries (Vishnu, Sridharan, 2017). In one case in the UK, 60 NHS trusts, 595 general practices, and over 1000 patients were impacted by WannaCry (Martin et al., 2018). Interestingly, all 200 hospitals inspected by the Care Quality Commission did not meet the United Kingdom’s Essentials Plus certification (Minimum Organizational Security Standards) (Martin et al., 2018). On the other side of the spectrum, some impacts of WannaCry were positive. For example, equity returns on some cybersecurity companies and cybersecurity investment vehicles increased following WannaCry (Castillo, Falzon, 2018). The global impacts of WannaCry cannot be overstated: financial loss, business disruption, data loss and theft, and advancements for defense and attack strategies for future incidents. Indeed, WannaCry could be said to be the "rebirth of ransomware."

**Analysis Conclusion**

While the most in-depth literature review, this analysis has helped us understand the process and components of one of the most dangerous and destructive variants of ransomware in the modern digital era. We reviewed literature discussing the details of WannaCry, its impact on the world, and defense strategies that were used to ultimately overcome it. Key points of this WannaCry analysis include:

* WannaCry was highly sophisticated in the technical aspect
* It’s used Windows SMB exploitation to infiltrate computers (Eternal Blue Vulnerability)
* It was one of the most damaging and widespread pieces of ransomware in history
* Defense strategies include malware analysis (via reverse engineering the virus), cybersecurity education and awareness, malware detection software, and backing up of important files
* Ironically, the attackers used poorly designed self-destruction code to stop the spread. However, its kill-switch is an important reminder of the attacker's skill set and their ability to use anti-malware analysis techniques
* WannaCry helped cement the existence of RaaS (Ransomware-as-a-Service)

This analysis and literature review of WannaCry has shown us the tremendous effect on the world, along with the best defense strategies to fight it.

**SUMMARY**

We have covered a lot of information throughout this literature review. From understanding the basics of malware, its child ransomware, and conducting a deep analysis of WannaCry, we have been able to understand the purpose and process of malware, its impact, and a list of mitigation and resolution strategies:

* Cybersecurity Awareness and Education
* Anti-Malware Software & Detection Techniques
* Firewalls/VPN/Network Security Measures
* Windows Defender and other Virus Scanners
* Data Backup/Offline External Backup/Cloud Storage
* Encrypting sensitive data (such as PII and financials)
* Timely Patch Updates

This list is not exhaustive but contains the most common mitigation strategies; however, all have flaws. Anti-Malware software cannot detect all forms of malware, specifically new/unknown forms. Network security can be compromised, or a device may become infected on another network. Virus scanners, like anti-malware, may not always detect an infection. Cloud storage can be expensive (or an enterprise may not feel comfortable having their data in the cloud), while external storage is concerned with security. Education may be one of the most important pillars, but an attack may cause more damage than if the tools were available without the right tools. Additionally, even basic cybersecurity knowledge can make a tremendous difference in the outcome (or prevention of) an attack.

While it may be impossible to avoid all threats, being educated on safe web browsing, smart data-handling techniques, appropriate use of all other mitigation strategies, and understanding what to do following the discovery of infection is critical in the battle against cyberattacks. One thing remains the same regardless of mitigation strategy is chosen: one is not enough, and it is best to use all available resources to help defend against malware and ransomware attacks.

This literature review has helped us conclude that a combination of all resources (cybersecurity education, backing up of data, patch management, network security, detection software, and anti-malware software) is the best defense against malware and ransomware attacks. To summarize:

* Education allows users to be informed, knowing what to look for and how to handle a potential security incident appropriately
* Awareness allows the public to stay alert and understand the importance of cybersecurity
* Data backup- Provides safe storage of sensitive data away from the computer in case of a ransomware attack resulting in encryption. Data backup prevents loss of data.
* Network security- use of strong firewalls, VPNs, encryption, and strong password management helps keep a secure bubble around the device-significantly important for "drive-by download," malicious ads, compromised websites, and email security.
* Detection software- provides the computer a tool to detect an infection.
* Malware removal software- provides the device a solution for malware removal.
* Patch management- Timely updates to resolve software/operating system vulnerabilities are critical to preventing and stopping a cyberattack. Most malware and ransomware attacks look for vulnerabilities inside the system to gain access.

We have researched malware, ransomware, the WannaCry virus, and defense against these malicious attacks throughout this literature review. By reviewing this research, we have determined that a combination of all the defense strategies listed above is necessary to prevent and mitigate cyber-attacks due to the sophisticated nature of these cyber-attacks.

**REFERENCES**

Aldaraani, N., & Begum, Z. (2018, April). Understanding the impact of ransomware: A survey on its evolution, mitigation, and prevention techniques. In *2018 21st Saudi Computer Society National Computer Conference (NCC)* (pp. 1-5). IEEE.

Algarni, S. (2021). Cybersecurity Attacks: Analysis of “WannaCry” Attack and Proposing Methods for Reducing or Preventing Such Attacks in Future. In ICT Systems and Sustainability (pp. 763-770). Springer, Singapore.

Baldin, A. (2019). Best practices for fighting the fileless threat. *Network Security*, *2019*(9), 13-15.

Bansal, U. (2021, May). A Review on Ransomware Attack. In 2021 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC) (pp. 221-226). IEEE.

Bayer, U., Habibi, I., Balzarotti, D., Kirda, E., & Kruegel, C. (2009, April). A View on Current Malware Behaviors. In *LEET*.

Belcic, I. (2021, September 7). Cerber ransomware: Everything you need to know. Retrieved January 18, 2022, from https://www.avast.com/c-cerber#gref

Berr, J. (2017, May 16). "WannaCry" ransomware attack losses could reach $4 billion. CBS News. Retrieved January 28, 2022, from https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/

Betfred. (n.d.). Microsoft Security bulletin MS17-010 - critical. Microsoft Docs. Retrieved January 19, 2022, from https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010

Bilge, L., & Dumitraş, T. (2012, October). Before we knew it: an empirical study of zero-day attacks in the real world. In Proceedings of the 2012 ACM conference on Computer and communications security (pp. 833-844).

Brewer, R. (2016). Ransomware attacks: detection, prevention, and cure. Network Security, 2016(9), 5-9.

Castillo, D., & Falzon, J. (2018). An analysis of the impact of Wannacry cyberattack on cybersecurity stock returns. Review of Economics & Finance, 13, 93-100.

Dossett, J. (n.d.). *A timeline of the biggest ransomware attacks*. CNET. Retrieved January 18, 2022, from https://www.cnet.com/personal-finance/crypto/a-timeline-of-the-biggest-ransomware-attacks/

Filiz, B., Arief, B., Cetin, O., & Hernandez-Castro, J. (2021). On the Effectiveness of Ransomware Decryption Tools. *Computers & Security*, *111*, 102469.

Furnell, S., & Emm, D. (2017). The ABC of ransomware protection. Computer Fraud & Security, 2017(10), 5-11.

Garuba, M., Liu, C., & Washington, N. (2008, April). A comparative analysis of anti-malware software, patch management, and host-based firewalls prevents malware infections on client computers. In *Fifth International Conference on Information Technology: New Generations (itng 2008)* (pp. 628-632). IEEE.

Hajioff, S., & Mckee, M. (2000). The 'I Love You'virus and its implications for geodiversity. *Journal of the Royal Society of Medicine*, *93*(8), 398-399.

Hsiao, S. C., & Kao, D. Y. (2018, February). The static analysis of WannaCry ransomware. In *2018 20th International Conference on Advanced Communication Technology (ICACT)* (pp. 153-158). IEEE.

Idika, N., & Mathur, A. P. (2007). A survey of malware detection techniques. *Purdue University*, *48*(2).

Knight, P. (2000). ILOVEYOU: Viruses, paranoia, and the environment of risk. *The Sociological Review*, *48*(2\_suppl), 17-30.

Kurniawan, A., & Riadi, I. (2018). Detection and analysis of Cerber ransomware based on network forensics behavior. *International Journal of Network Security*, *20*(5), 836-843.

Martin, G., Ghafur, S., Kinross, J., Hankin, C., & Darzi, A. (2018). WannaCry—a year on. BMJ, 361.

Mohanta, A., Velmurugan, K., & Hahad, M. (2018). *Preventing Ransomware: Understand, prevent, and remediate ransomware attacks*. Packt Publishing Ltd.

Mos, M. A., & Chowdhury, M. M. (2020, July). The Growing Influence of Ransomware. In 2020 IEEE International Conference on Electro Information Technology (EIT) (pp. 643-647). IEEE.

Newman, L. H. (2017, May 13). How an accidental 'kill switch' slowed Friday's massive ransomware attack. Wired. Retrieved January 19, 2022, from https://www.wired.com/2017/05/accidental-kill-switch-slowed-fridays-massive-ransomware-attack/

O'Gorman, G., & McDonald, G. (2012). *Ransomware: A growing menace*. Arizona, AZ, USA: Symantec Corporation.

Patten, D. (2017). The evolution of fileless malware. Retrieved January 19, 2022, from

http://www.infosecwriters.com/Papers/DPatten\_Fileless.pdf

Trautman, L. J., & Ormerod, P. C. (2018). Wannacry, ransomware, and the emerging threat to corporations. *Tenn. L. Rev.*, *86*, 503.

Vishnu, C. R., & Sridharan, R. (2017). SUPPLY CHAIN RISK MANAGEMENT IN THE EVOLVING INDIAN SCENARIO: A CASE STUDY ON THE IMPACT OF DEMONETISATION, WANNACRY ATTACK AND GST IMPLEMENTATION. INDUSTRIAL ENGINEERING JOURNAL.

Webster, A., Eckenrod, R., & Purtilo, J. (2018). Fast and Service-preserving Recovery from Malware Infections Using {CRIU}. In *27th {USENIX} Security Symposium ({USENIX} Security 18)* (pp. 1199-1211).

Wyke, J. (2011). What is Zeus? *Sophos, May*.

Yilmaz, Y., Cetin, O., Arief, B., & Hernandez-Castro, J. (2021). Investigating the impact of ransomware splash screens. Journal of Information Security and Applications, 61, 102934.