WannaCry Malware Analysis:

An examination of the exploit, its evolution and how it held the world to ransom.

Finlay Reid

CMP320: Ethical Hacking three

BSc Ethical Hacking Year three

2020/21

Note that Information contained in this document is for educational purposes.

.

Abstract

The following white paper was a submission for CMP320's mini project assessment, the research for this assignment was completed over a 2-week period and it was concluded with this document. Overall, the paper aims to examine the WannaCry malware and each of its induvial parts. Furthermore, the techniques the malware employs to detect sandbox environments and methods in which WannaCry attempts to evade anti-virus were discussed also. To achieve this a number of important tools were utilized to thoroughly investigate the exploit in order to discover what makes the malware so effective in exploiting victims' machines. The results show that while WannaCry is an efficient malware it has numerous weaknesses which can be used to mitigate the risk posed by the virus.

.

Contents

.

1 INTRODUCTION

1.1 BACKGROUND

As the threat posed from malware increases, due to society's reliance on technology and the ever-growing complexity of cyberattacks. One form of malware should be made sure to be highlighted – the ransomware attack. This attack is built for the 21st century, an age where the majority of users store sensitive data on their devices, an environment this piece of malware can thrive in. On a very basic level the attack operates by first encrypting a victim's data, essentially holding your data hostage, the digital extortionists will then present an ultimatum demanding some form of ransom or the stolen data will remain locked indefinitely.

In the days before the creation of malware there has been countless infamous hostage situations that has gripped worldwide attention, with the evolution of technology new opportunities have presented themselves to today's criminals. The ransom attack is exactly this, a digitized version of a hostage situation on a much larger scale, valuing the quantity of machines infected in order to cause the most destruction and maximize profit.

The infamous WannaCry crypto worm of summer 2017 was a form of ransomware that cost the global economy an estimated $4 billion dollars and infected computers numbering over 300,000 in 150 different countries (What is WannaCry ransomware?, 2021), a full breakdown of the most popular vulnerabilities can be seen in Figure 2 .The aforementioned piece of malware is reliant on a SMB vulnerability named "EternalBlue", which permits the ransomware to not only comprise the integrity of computer systems but also propagate to other machines available on the network. National Security Agency (NSA) are credited with developing the exploit while the shadow brokers hacker group are responsible for leaking it to the public, just shortly after Microsoft released patches for the vulnerability. All three of these originations share some of the blame for the ensuing cyber-attacks, not equally but each group played an important role (A Technical Analysis of WannaCry Ransomware | LogRhythm, 2021).

In order to mitigate the risks posed by ransomware it is recommend following best practice including installing a component intrusion detection system and regularly updating operating systems to ensure weaknesses are patched. These recommendations are all well and good, however people are unreliable, like all malware machines aren't only ones being exploited. The WannaCry exploit depended on this human error as a number of the businesses and users worst hit ran old versions of windows.

Back in the early hours of May 12th the first initial reports were registered that a suspected attack on Telefónica, a Spain-based telecommunications company had occurred (Staff, 2021), a full breakdown of the timeline can be seen in Figure 1. Over the next few hours, the exploit spread like wildfire around the globe affecting some of most powerful companies and nations in existence. The reaction to this attack was notable, with one cyber security website labeling it "The Largest Cyber Attack Worldwide in History" (Largest Cyber Attack Worldwide In History;

WannaCry Ransomware, 2021), after the first details began to surface the exploit went on to cripple the NHS and brought some organizations to their very knees (The NHS cyber-attack: how and why it happened, and who did it, 2021). Even after first initial wave of attacks the WannaCry malware is still to this day causing non updated machines issues (Three Years After WannaCry, Ransomware Accelerating While Patching Still Problematic, 2021), with the subsequent development of new variants that somehow inadvertently works as an ill-advised, vaccine against infection from the original piece of malware.

As previously mentioned, the impact of the ransomware attack was great, costing the NHS 92 million after 19,000 appointments were canceled as a result of the attack. On the other side of the Atlantic it was reported by Shodan that over 400,000 systems were exposed to exploitation by NSA's lost hacking implement (TechCrunch is now a part of Verizon Media, 2021). Prospects of preventing the malware in the east were also looking grim, with damage caused by the exploit showed no signs of slowing down as two of the four most affected countries were in the east. India was particularly hit bad, worse than the initial reports suggested at 45,000 infected computers with some important government organizations notably the Andhra Pradesh Police being hit the hardest (WannaCry ransomware: Andhra police fall prey to global cyber-attack, 2021). Overall, the consequences of the WannaCry attack cannot be underestimated and the reason why it hit so hard was down to poor cyber hygiene and a lack of education surrounding cyber security.

This paper will discuss the evolution of the WannaCry exploit and its variants including its impact on the field of cyber security, comparisons will also be made with other popular Ransomware exploits. The practical element will consist looking at how the exploit reinvents itself to evade anti-virus software and the detection systems it uses for discovering if it's in a sandbox environment.

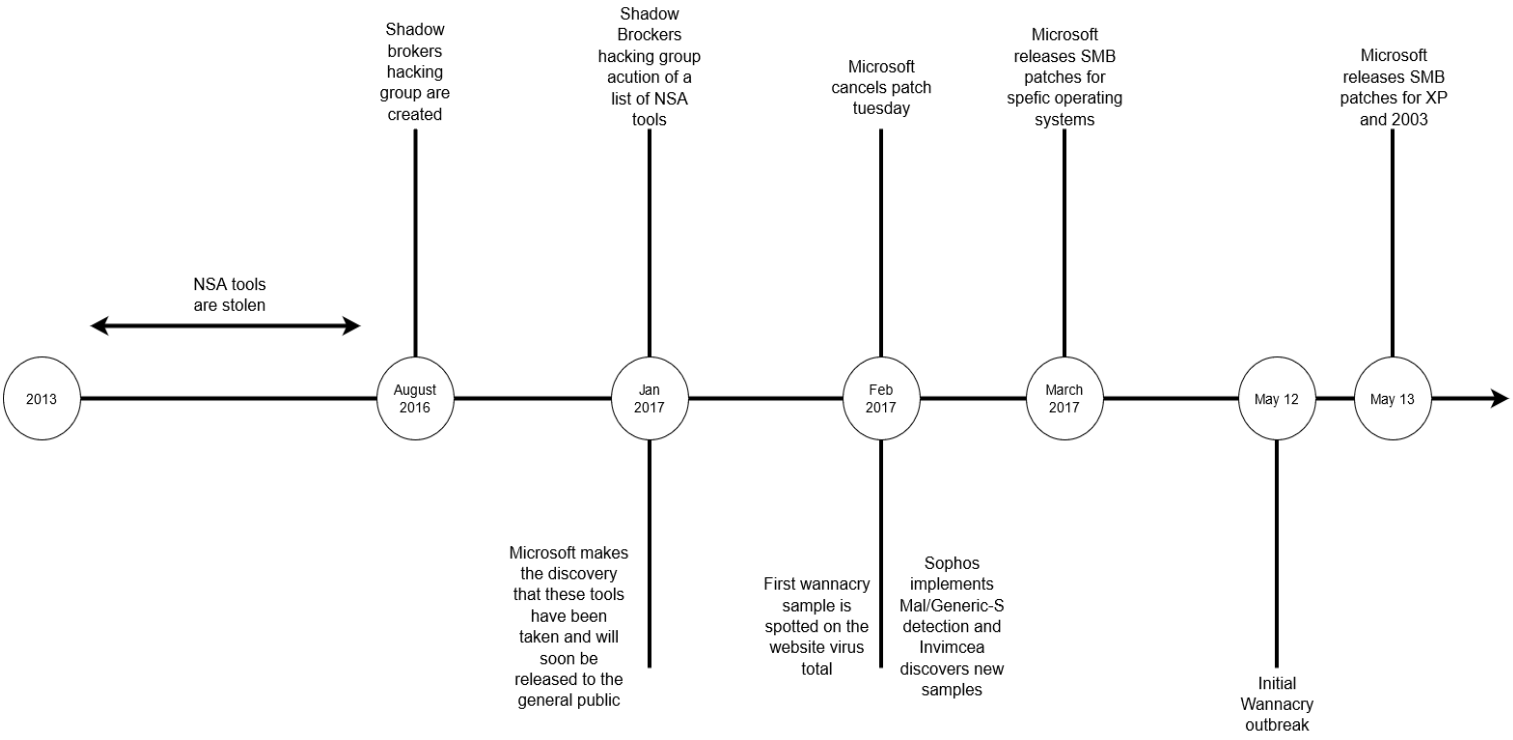

Figure 1 - Timeline of WannaCry

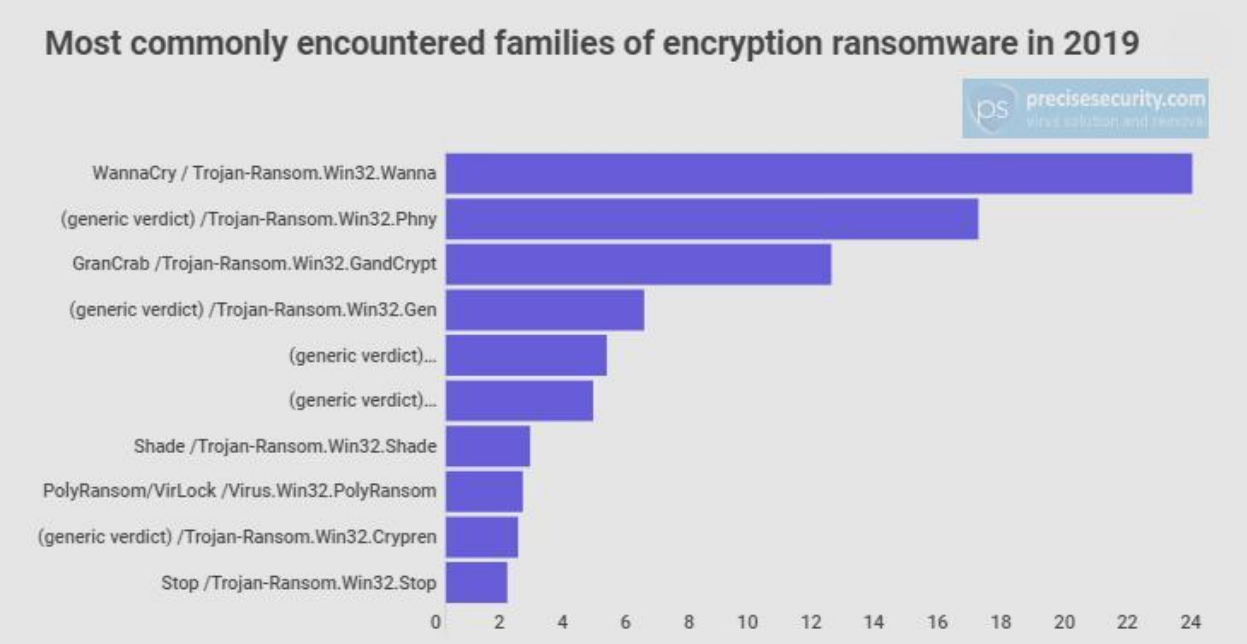

Figure 2 - chart of most common vulns source : https://securelist.com/ransomware-by-the-numbers-reassessing-the-threats-global-impact/101965/

1.2 AIM

The following white paper aims to analyze the evolution of the WannaCry malware, comparing against different generations of the exploitation and the latest variants of ransomware. Both how the exploitation employs techniques to evade anti-virus and its impact on the cyber security field will be examined in the report. To accomplish these aims, the subsequent objectives will be met:

- WannaCry code investigation of the most important features employed by the malware.
- Installation of three prominent anti-virus software
- The way in which these malwares react to each specific anti-virus will be recorded and analyzed
- Investigation and discussion into the resulting security mitigations caused by the WannaCry malware specifically the windows patches implemented by Microsoft.
- An outlining of how the WannaCry program operates and its particular functions i.e the kill switch.
- Deep dive into the evolution of ransomware and WannaCry.

1.3 METHODOLOGY

In order to fully comprehend the WannaCry's impact and evolution as an exploit, other notable ransomware will be compared to grade its efficiency in exploiting. Before this however, an in-depth review of its main features, techniques and plan of attack will be covered to ensure there is an understanding of

the malware prior to the discussion of its evolution. Both PC cyborg and crypto locker ransom wares will be briefly explained also.

Tool used	Purpose
Cuckoo sandbox	A software used to thoroughly analyze WannaCry. It provides a comprehensive report outlining the behavior of the file when ran inside a realistic but secure environment.
Ghidra	An NSA developed reverse engineering tool used to dissect parts of the WannaCry code.
Fire eye VM	An open source security distribution aimed at reverse engineers which includes useful software such as Wireshark and ghidra.
VMware workstation	Hypervisor used to create the virtualized environments including the ubuntu and windows 10 machine.
Ubuntu	Linux distro based on Debian and was used to run cuckoo sandbox
Windows 10	Operating system used to run ghidra and wire shark.

Table 1 - Tools used in procedure

The methodology of this white paper consisted of first analyzing the malware using the various tools shown in Table 1, then testing the WannaCry malware to see its behavior. Finally, an in depth look at how it got to that point was discussed to show its evolution and how ransomware as a whole has progressed. These following steps were taken to thoroughly examine the WannaCry malware:

- Set up of safe test environment ensuring malware is unable to propagate
- Discussion of some prominent features used by the exploit in its quest of infection.
- Analyzation of code using the tool ‘ghidra’.
- Analyzation of network traffic using the tool Wireshark
- Examination of malwares encryption module using ‘ghidra’
- Investigation of payment received and the methods in which the attackers used.
- Analyzation on how these individual components come together to make the malware function.
- Examination of how the malware attempts to evade anti-virus by running the file though three prominent anti-virus software.
- Looking at how the malware attempts to evade analyzation in a virtual environment.
- Discussion of the WannaCry’s evolution and the ransomware as a whole.

2 PROCEDURE & RESULTS

2.1 SET UP OF TESTING ENVIRONMENT

To make an analysis of the WannaCry malware necessary precautions were taken to ensure the exploit did not propagate to the host computer. A safe environment was crafted for this demonstration while following practices recommend when undertaking malware analysis. The virtualization software 'virtual box' was used to create a dummy machine capable of testing and analyzing the chosen exploits. A base windows 10 system in a virtualized machine was chosen, before the creation of the testing environment all software was confirmed to be running the latest patches to ensure malware could not propagate to the host system. Other precautions taken include:

Security Precaution	Reason For
Network configuration is set to host only	To ensure certain malware cannot infect other machines on the host network.
Removal of USB devices from VM	To ensure important hard drives remain non infected from malware
Utilization of compressed and password protected sample malware	To avoid the accidental execution of malware
Continuous VMware snapshots	To avoid having to reinstall if something unexpected occurs.
Important data not stored on the analysis virtual machine	To ensure infected data is not transferred to the host computer and important documents are not lost
Removal of shared folders	To stop malware capable of transferring over the network spreading to other systems.

Table 2 - Security precaution table

The first step in setting up a safe environment for malware analyzation involved downloading a free windows 10 virtual machine from Microsoft. This fresh installation was imported to VMware and the necessary security configurations were implemented, crucially both the network was set to host only, and shared folders were disabled. To remove the possibility of windows interfering during downloading/analyzing malware windows defender was also disabled, this was achieved by utilizing group policy to guarantee the antivirus did not re-enable itself when the virtual machine was reset.

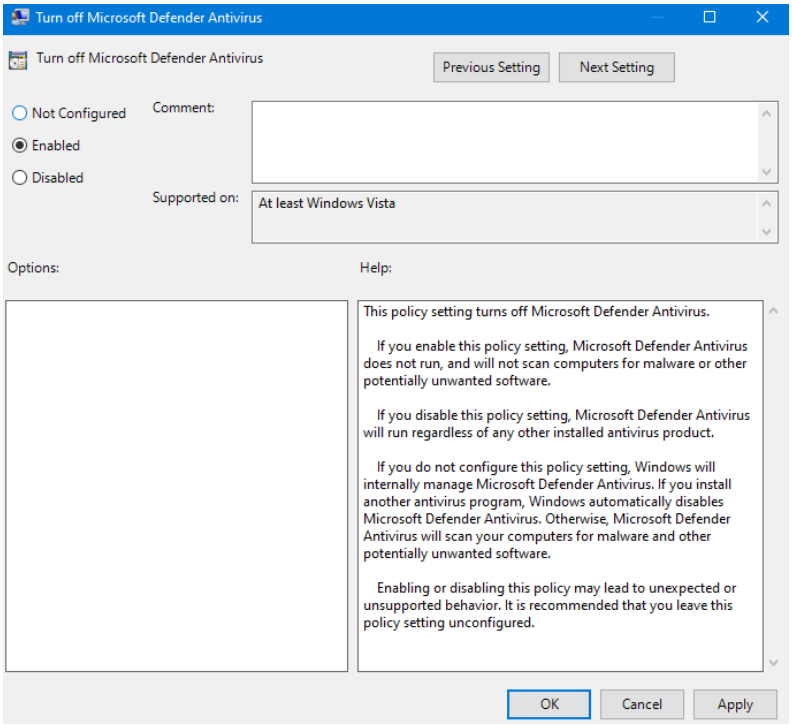

Figure 3 - Disabling Anti-virus

After resetting the virtual machine to implement the changes made, a snapshot of the virtual machine was created to save the current state. Having correctly configured the base windows system and with the security precautions in place, the next step included installing malware analyzation software. For this Fire eyes 'FLARE VM' was utilized as it incorporates all the essential software needed for the analyzation of malware. To install this bundle of software, a zip file from the fire eyes website was downloaded and the tutorial located underneath was followed. Steps included in the tutorial involved:

1. Decompressing the FLARE VM package to a directory.
2. Starting a new session of PowerShell with advanced privileges. FLARE VM attempts to install additional software and modify system settings; therefore, escalated privileges are required for installation.
3. Within PowerShell, changing the directory to the location where the FLARE VM repository had been extracted.
4. Enabling unrestricted execution policy for PowerShell by executing the following command 'Set-ExecutionPolicy unrestricted' and answering "Y" when prompted by PowerShell.
5. Executing the install.ps1 installation script. Entering the current password 'Passw0rd! – the default password when downloading a VM from Microsoft'. FLARE VM needs the current user's password to automatically login after a reboot when installing.

Figure 4 - Flare VM desktop

After successfully installing Flare VM the independent virtual environment had been completed and all that was next was analyzation.

2.2 COMPONENTS OF WANNACRY MALWARE

The WannaCry malware relies on four induvial components to achieve its primary goal, first a dropper containing an encrypter. This particular component is responsible for the other three as the dropper contains a decryption program termed 'Wana Decrypt0r 2.0', a secure copy of TOR – an open source program enabling anonymous communication and a list of files relating to its configuration.

The initial reports disturbed by the media suggesting the malware was spread by a malicious spam campaign was false, however this line of thought was understandable due to the numerous cases propagated this way prior to WannaCry. Roughly around the same time of the WannaCry attack a newly developed ransomware operation was distributing malware through email. The true offender however in the spread of this malware was vulnerable SMB ports being abused by an exploit termed Eternal Blue. The architects of the malware cared very little about preventing analysis of the exploit due to severe lack of obfuscation, anti-debugging, or VM-aware code. This enables a thorough investigation in how this malware was able to exploit over 230,000 computers.

Eternal blue

As previously mentioned in the introduction Eternal blue is an exploit created the NSA, by exploiting a vulnerability located in SMB – a protocol used for sharing access to files, printers, and serial ports between machines on a network, it is able to propagate the malware to all pre patched windows machines that has

the protocol enabled. The exploit essentially allows for remote code execution over smbv1. In the case of WannaCry it employs this exploit to create a tailored SMB session customized for that particular machine. Three packets are sent to a host's machine including two which contain hard-coded IP addresses. Furthermore, the exploit also checks for the presence of double pulsar a component which will be discussed in the next section.

```
[*] Sending SMB Echo request
[*] Good reply from SMB Echo request
[-] Error doing SMB setup 0x%08X
    [+] Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[-] Error sending data for final SMBv2 buffer.
    [+] Sending final SMBv2 buffers.
    [+] Sending large SMBv1 buffer.
[-] Unable to allocate buffer for shellcode
    [+] Ping returned Target architecture: x64 (64-bit)
    [+] Ping returned Target architecture: x86 (32-bit)
        [+] Backdoor returned code: 70 - Error: ExAllocate/Free not found - Backdoor removed
        [+] Backdoor returned code: 60 - Error: Allocation Failed
        [+] Backdoor returned code: 50 - Error: Invalid Params
        [+] Backdoor returned code: 40 - Error: Invalid Transaction Params
        [+] Backdoor returned code: 30 - Error: Bad Transaction
        [+] Backdoor returned code: 20 - Error: Bad Opcode
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: %X - Error: Unknown error
[-] No response received from exploit packet. Not good.
    [+] ETERNALBLUE overwrite completed successfully (0x%08X)!
[*] Fingerprinting SMB non-paged pool quota
[*] Trying again with %d Groom Allocations
    [+] Backdoor installed
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] Triggering free of corrupted buffer.
[*] Sending egg to corrupted connection.

DONE.
[*] Sending all but last fragment of exploit packet
[*] Building exploit buffer
[*] Target OS selected valid for OS indicated by SMB reply
[*] Auto target successful based on SMB reply
[*] Auto targeted based on SMB string
    [+] Backdoor not installed, game on.
    [+] Backdoor is already installed -- nothing to be done.
[*] Pinging backdoor...
```

Figure 5 – review of Eternal blue .exe file

A review of the EternalBlue-2.2.0.exe file provides a substantial idea on the predicted actions of the malware. From Figure 5 it is possible to deduct the exploit will first send the initial SMB request to the target, depending on the subsequent response the exploit will then preform SMB fingerprinting and will attempt the exploit. If the exploit has succeeded in compromising the targeted machine it will ping the double pulsar backdoor to determine if this component has been installed on the host's machine. This is what makes WannaCry so efficient as a malware, its ability to sound out potential targets by propagating the malicious code thereby infecting connected nodes on the network.

Double pulsar

Double pulsar is a component that works hand in hand with eternal blue, as previously mentioned eternal blue queries the hosts machine for the existence of double pulsar. If the exploit is not discovered, eternal blue injects the target with double pulsar. Double pulsar as a standalone exploitation is an extremely complex memory-based kernel package that utilizes weaknesses found in multiple computer architectures. It grants malicious users the ability to execute any raw shellcode, allowing for its purpose in the WannaCry malware to be successful, the purpose of establishing a connection with a target, to then install additional malware (WannaCry).

Kill switch

During the initial infection process of WannaCry, the dropper is executed then it attempts to make a connection to the domain 'http://www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com'. If the connection is successful it will exit, however before this the domain was inactive causing the connection to fail. Due to the quick thinking of one malware researcher the domain was registered essentially becoming a kill switch that slowed the spread rate and effectivity neutered the exploit. While this did stop the spread, systems in which malware connected through proxies remained vulnerable.

To analyze the kill switch component a sample of WannaCry malware was downloaded from the 'ghidra ninja' website, it was unpacked securely onto the virtualized test environment and ran through 'Ghidra' – an open source reverse engineering kit created by the NSA. The initial section of code being examined is the 'entry function' as WannaCry is a windows exploit, it requires 'Winmain'. This is an application entry point used by all window programs and is required at the end of function entry.

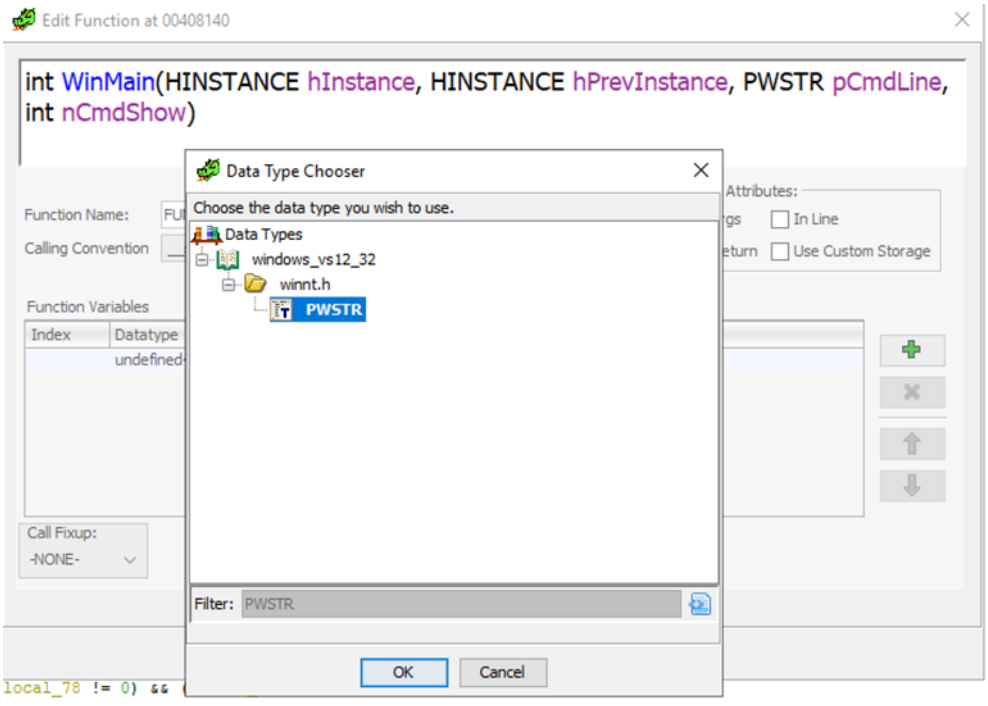

Figure 6 - edit function to Win main

For the sake of simplicity variable names were renamed to help with readability, this was achieved by double clicking on the variable name then inputting the change. At first glance one variable named 'puVar3' stood out with its stored data being a curious URL, which can be seen below in Figure 7.

```
puVar3 = (undefined4 *)s_http://www.iuqerfsodp9ifjaposdfj_004313d0;
```

Figure 7 - Strange URL

The next point of interest that was identified is the 'while loop' displayed below in Figure 8, this segment of code essentially iterates through the loop copying four bytes of the URL into a stack buffer. As long as the integer 'I' is not equal to 0 it will enter the loop, first the variable 'I' is subtracted by one and the code proceeds to copy the URL four bytes at a time.

```
while (iVar2 != 0) {
  iVar2 = iVar2 + -1;
  *puVar3 = *(undefined4 *)URL;
  URL = URL + 4;
  puVar3 = puVar3 + 1;
}
```

Figure 8 - while loop

Moving on to a different segment of code that is important to how the kill switch functions, the if statement shown below in Figure 9. This section required the importation of both windows functions 'InternetOpenA' and 'InternetOpenUrlA', however when trying to implement them an error was received. The problem was solved by creating a new a new data type called 'HINTERNET' and making sure it was a void pointer.

```
uVar1 = InternetOpenA(0,1,0,0,0);
i = InternetOpenUrlA(uVar1,local_50,0,0,0x84000000,0);
if (i == 0) {
  InternetCloseHandle(uVar1);
  InternetCloseHandle(0);
  FUN_00408090();
  return 0;
}
```

Figure 9 - kill switch if statement

Having renamed a number of variables the picture starts to become clearer on how the kill switch operates. At a basic level this piece of code queries the URL defined as the variable 'URL' on line 19, this is done in four-byte sequences and if it returns a null handle this means the request has succeeded. The program will return from win main ending the routine. Figure 10 displays the code that makes the query.

```
hInternet = (HINTERNET)InternetOpenA(0,1,0,0,0);
hInternet_return = InternetOpenUrlA(hInternet,(LPCSTR)URL_BUFFER,(LPCSTR)0x0,0,0x84000000,0);
if (hInternet_return == (HINTERNET)0x0) {
  InternetCloseHandle(hInternet);
  InternetCloseHandle(0);
  FUN_00408090();
  return 0;
}
InternetCloseHandle(hInternet);
InternetCloseHandle(hInternet_return);
```

Figure 10 - code that queries the URL

Network analyzation

Analyzing the network component of WannaCry malware involved loading the 'wannacry.pcap' file into Wireshark. This file was downloaded from the malware traffic website then subsequently extracted and imported to a new project in Wireshark – a free and open-source packet analyzer. The packet capture was taken in a test environment using windows servers and workstations established in a LAN environment.

The kill switch that was reported heavily can be seen below in Figure 11; a DNS query is made to the URL which was discussed previously. Furthermore, when the domain was registered it stopped the virus from spreading as it relied on this to decide if it should execute.

→	1	0.000000	192.168.56.102	8.8.8.8	DNS	109 Standard query 0xe9f4 A www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
←	2	0.647439	8.8.8.8	192.168.56.102	DNS	109 Standard query response 0xe9f4 Server failure A www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
	3	0.809306	192.168.56.102	8.8.8.8	DNS	109 Standard query 0xf6a2 A www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
	4	1.210133	8.8.8.8	192.168.56.102	DNS	109 Standard query response 0xf6a2 Server failure A www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
	5	2.702100	192.168.56.102	105.162.147.224	TCP	66 49243 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1

Figure 11 - DNS query to URL kill switch

According to Microsoft's documentation pertaining to the SMB header the protocol field should include the hex string 'ff 53 4d 42', this translates to SMB in ASCIII. In order to specify these SMB requests a filter was used to focus on the important requests which can be seen below in Figure 12.

ip.addr == 192.168.116.149 && frame contains ff:53:4d:42

Figure 12 - filter used for finding string

Figure 13 displays evidence confirming SMB v1 was being used, as previously mentioned this implementation of the protocol is vulnerable and can be exploited using eternal blue.

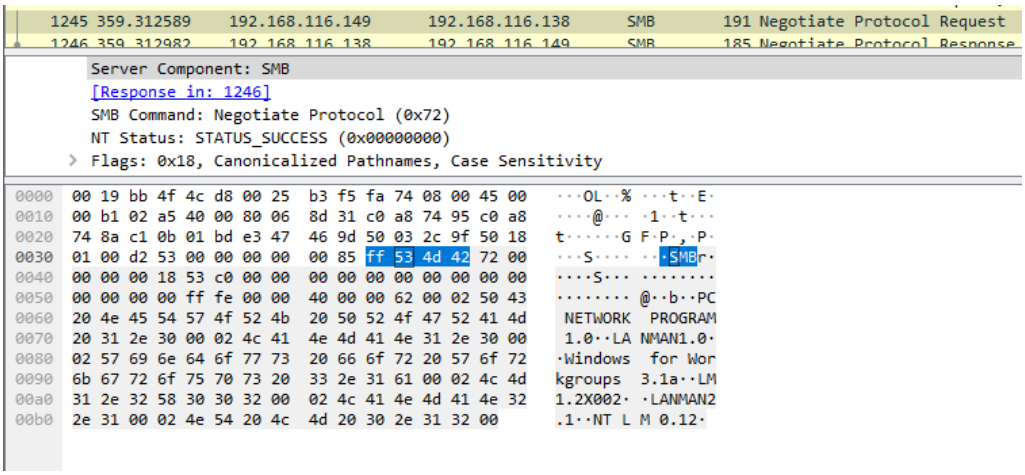

Figure 13 - SMB confirmation

WannaCry dispatches a 'trans 2 Request, SESSION_SETUP' packet to the victims compromised machine, 'trans 2' is a shortened version of 'Transaction 2 Subcommand Extension'. The purpose of this request is to analyze the victims machine discovering if it has been infected or not. With investigating the response codes, it is possible to ascertain whether a machine has been infected or remains clean of malware. Figure 14 displays the requests and responses including the 'trans 2 request'.

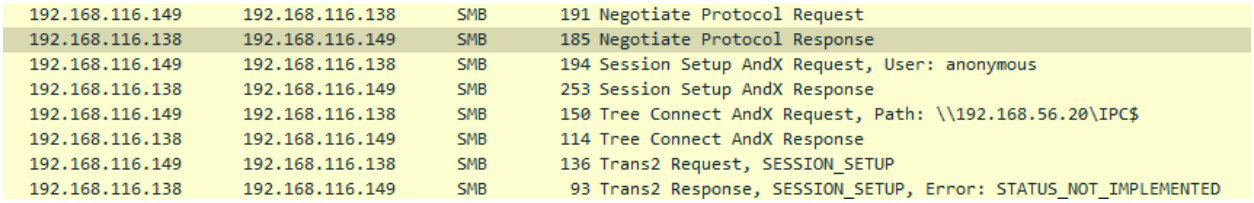

Figure 14 - Request and responses

As previously mentioned, the WannaCry malware essentially uses the eternal blue exploit to propagate to other machines through NetBIOS. WannaCry creates random IP addresses allowing the exploit to spread to websites outside the infected network and the malware will send three NetBIOS session setup packets to it. One has the proper IP of the machine being exploited, and the other two contain two IP addresses hardcoded in the malware body. The presence of two hardcoded IP could be used by the exploit to detect network intrusion prevention systems.

Encryption/ decryption

Before the exploit begins the exploit first enumerates all available drives on the machine including USB, standard hard disks and network drives. The Task Start export receives two variables, a handle to the module and integer value that is required to be 0. The function that scans for new drives can be seen below in Figure 15, this function stores a bitmask of all the connected drives to the machine called 'drives'.

```
uint original_drives;
DWORD drives;
HANDLE hObject;
uint drive_difference;
LPVOID lpParameter;

drives = GetLogicalDrives();
while (original_drives = drives, decryption_successful_glob == 0) {
  Sleep(3000);
  drives = GetLogicalDrives();
  drive_difference = original_drives ^ drives;
  if (drive_difference != 0) {
    lpParameter = (LPVOID)0x3;
    do {
      if (decryption_successful_glob != 0) goto exit;
      if ((((drive_difference >> ((byte)lpParameter & 0x1f) & 1) != 0) &&
          ((original_drives >> ((byte)lpParameter & 0x1f) & 1) == 0)) &&
         (hObject = CreateThread((LPSECURITY_ATTRIBUTES)0x0,0,ransomware_thread,lpParameter,0,
                                 (LPDWORD)0x0), hObject != (HANDLE)0x0)) {
        CloseHandle(hObject);
      }
      lpParameter = (LPVOID)((int)lpParameter + 1);
    } while ((int)lpParameter < 0x1a);
  }
}
it:
```

Figure 15 - enumeration of drives

The while loop located underneath the drives variable first stores the result of the 'getLogicalDrives' function into a variable. After this the while loop will continually iterate until global variable 'description_sucessful_glob' is not equal to 0, this essentially means it will run until the ransom has been paid. In the first if statement this checks if there has been a newly/removed connected drive, if the criteria is met and the exploit enters the statement, it begins encrypting the discovered drives files.

WannaCry also intelligently selects specific file extensions and skips file types it deems unnecessary. The exploit searches for files related to productivity and multimedia i.e. docx. Two while loops shown below in Figure 16 are responsible for checking file types. A full list of file types that WannaCry encrypts can be found in **Appendix A.**

```
document_suffixes = &PTR_u_.doc_1000c098;
current_suffix = (wchar_t *)PTR_u_.doc_1000c098;
while (current_suffix != (wchar_t *)0x0) {
  iVar1 = _wcsicmp((wchar_t *)*document_suffixes,path_end);
  if (iVar1 == 0) {
                    /* Return 2 for file-endings from first l
    return 2;
  }
document_suffixes2 = &PTR_u_.docb_1000c0fc;
current_suffix2 = (wchar_t *)PTR_u_.docb_1000c0fc;
while (current_suffix2 != (wchar_t *)0x0) {
  iVar1 = _wcsicmp((wchar_t *)*document_suffixes2,path_end);
  if (iVar1 == 0) {
                    /* Return 3 for file-endings from second l
    return 3;
```

Figure 16 - file extension check

The WannaCry malware makes use of two encryption algorithms to successfully lock away user files. One is windows Crypto API for RSA encryption and the other is an unofficial version of AES which is included in the malware. It was concluded by encryption specialists that the implementation of algorithms within the malware was sound and decryption is extremely unlikely unless with the possession of the decrypted private key from the ransomware engineers.

After completing the previous segments of code, the malware will then begin to generate an RSA-2048 key, this key is unique to each infected machine and is stored locally. Having created the RSA key, it is then used to encrypt a random AES-128 key generated for each encrypted file. Individual files are then encrypted and written to the malwares directory, following the name format of their original filename with a .WINCRY extension appended on. Files compromised by the malware are not completely overwritten suggesting they could be recovered.

The exploit has the possibility of using either a random number generator or an RSA key, when encrypting the AES key with RSA. Criteria for this includes file ‘f.wnry’ not being present during initialization and the exploit will then generate a random number that is less than 209,715,200 bytes. RSA is used to encrypt AES when the number is a multiple of 100 - which is hardcoded in the malware, however a maximum of 10 files can be encrypted. When an AES key is encrypted with this RSA key, the malware will write to file f.wnry. If the arbitrary number is not a multiple of 100 or the file f.wnry already is present on the machine, the exploit will encrypt the AES key with the randomly generated RSA key. A full table of the encrypted files can be found in **Appendix B.**

Payments

The actual mode of payment was in the form of the crypto currency bitcoin, newer forms of ransom ware are usually paid in crypto currency and WannaCry was no different. Three bitcoin wallets were used to collect payments from the malware's victims, statistics of the wallets can be seen below in the bitcoin tables. From these tables it is possible to determine how much attackers earned as of May 2021, roughly 2.4 million dollars. When the exploit has completed its infection of the victims computer, the executable will display a timer like the one shown in Figure 17. This shows two timers decreasing with one suggesting if the payment is not received the ransom will increase and the other advising that if the ransom is not paid all the files will be lost. WannaCry is also customizable with its ransom as variants have been seen that pressure for bitcoin payments worth between 300 and 600 dollars. A full breakdown of each wallet can be found in **Appendix A.**

Figure 17 - WannaCry home screen

How it comes together

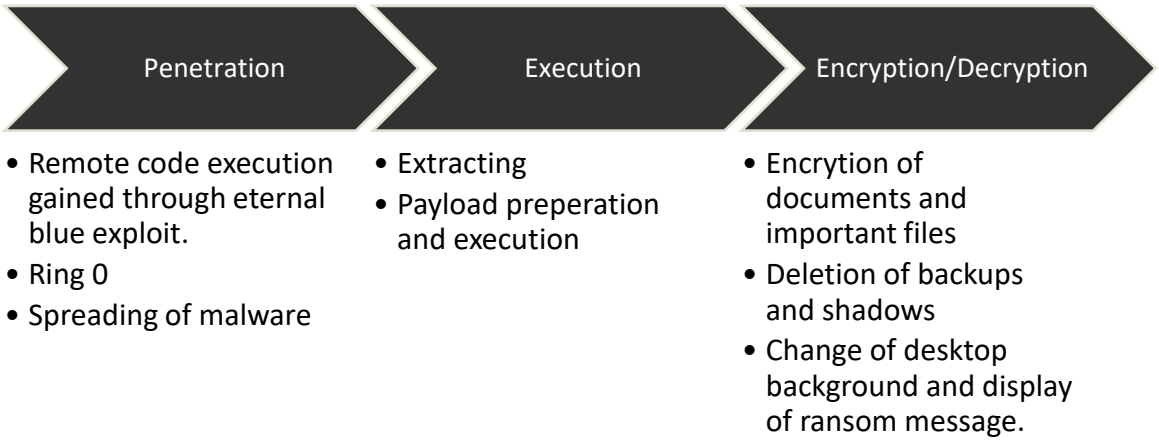

Figure 18 - Breakdown of WannaCry

Start of infection

As previously stated, the WannaCry malware relies on many different components in the process of exploiting a user. Figure 19 sourced from a technical analysis done by elsatacio provides a breakdown on the execution process of the malware. The first stage of the exploit is the initial infection, the kill switch module is the start of the process where the malware attempts to connect to the beacon. If successful the malware will cease, failure to connect and the malware dropper attempts to create a service termed “mssecsvc2.0”. After initiating this service, the malware will then attempt to propagate through eternal blue exploiting the vulnerability found in SMBv1. Eternal blue will first begin the setup of SMB by connecting to the SMB socket and getting the getting SMB tree id, it then begins to inquire for MS17-010. Having discovered if the target machine is vulnerable to the MS17-010 exploit the malware now begins to initiate the Base64 Payload in Memory, before executing the payload it will then probe for the existence of double pulsar and listen for the response, if the returned code equals 51 this informs the malware that the payload is ready. Finally, if the exploit is successful the malware will perform these closing statements:

- Gets the machines name
- Creates random string
- Gets command line arguments and checks for switch “/i”

Malware preparation

The next set of instructions involves the malware preparing for the actual ransom ware scheme. It first has to extract the zip file with its designated password, after this the process of setting up tor – open source software allowing anonymous commination will begin. To achieve this it will search for the ‘c.wnry’ file which includes information relating to the configuration of tor and the chosen bitcoin wallets. Before the setup of encryption keys occurs, the exploit runs a command that grants all users unfettered access to all files, including ones in the current directory and all directories below. A full table of files used by WannaCry can be seen in **Appendix C.**

After completing the previous instructions, the program now gets the go ahead to start preparation for encrypting the keys and decrypting the DLL. It first has to load/setup all the relevant exports including the ones related to the ‘getprocaddress’ and the ‘Cypto function’ exports, a full list of these exports can be seen below in Table 3.

Cypto function exports	Getprocaddress exports
CryptGenKey	CreateFileW
CryptDecrypt	WriteFile
CryptEncrypt	ReadFile
CryptDestroyKey	MoveFileW
CryptImportKey	MoveFileExW
CryptAcquireContextA	DeleteFileW
	CloseHandle

Table 3 - Export table

The exploit then gets the RSA_AES cryptographic Provider – a program used for creating, storing and accessing cryptographic keys and imports the key using the ‘CryptImportKey’ function. WannaCry will then begin to parse ‘t.wnry’ to get the AES key used to decrypt the DLL key, it will then attempt to retrieve information about the victims computer using the windows function ‘GetNativeSystemInfo’ and get a handle to the default heap of the calling process using windows function ‘GetProcessHeap’ – which can be used in calls to heap functions. The encrypted data is then inserted into the heap and wherever the data is located will have its protection changed.

WannaCry now has the ability to create the encryption keys used for locking away the victim’s files. It achieves this by encrypting the user’s private key with the ransomware public key and storing it in the “%08X.eky” file. The encryption tool will then check to see if the mutex “MsWinZonesCacheCounterMutexA0” exists and it will go ahead if this does not exist. Importantly,

WannaCry does not actually create the mutex implying that the exploit also checks for different software on the machine. From this it is possible to deduct that this could be used as a method to mitigate the risk posed by WannaCry, as if this mutex is present, the malware will not start. Finally, the program will create a new thread that puts the preparation into practice by encrypting files.

Encryption module

The encryption routine initiates by creating a brand-new thread to overwrite the files on the victim's machine. It will first generate a unique key and create data buffers for each induvial file, after this it calls the function 'start address' to begin encrypting the file contents. Function start address is also responsible for appending on the '.WNCRYT' extension to the end of files. The program will then look for the location of '@WanaDecryptor@.exe' starting process 'taskse.exe @WanaDecryptor@.exe'. After setting up decryption tool persistence the exploit can now run '@WANADECRYPTOR@.EXE', this means the configuration file of tor will be read then executed.

The exploit will then create the ransomware notes from "r.wnry" which will be named 'Please_Read_Me.txt'. It will then encrypt all the files killing database and email server-related processes if they are running. Finally, the program Deletes the volume shadow copies.

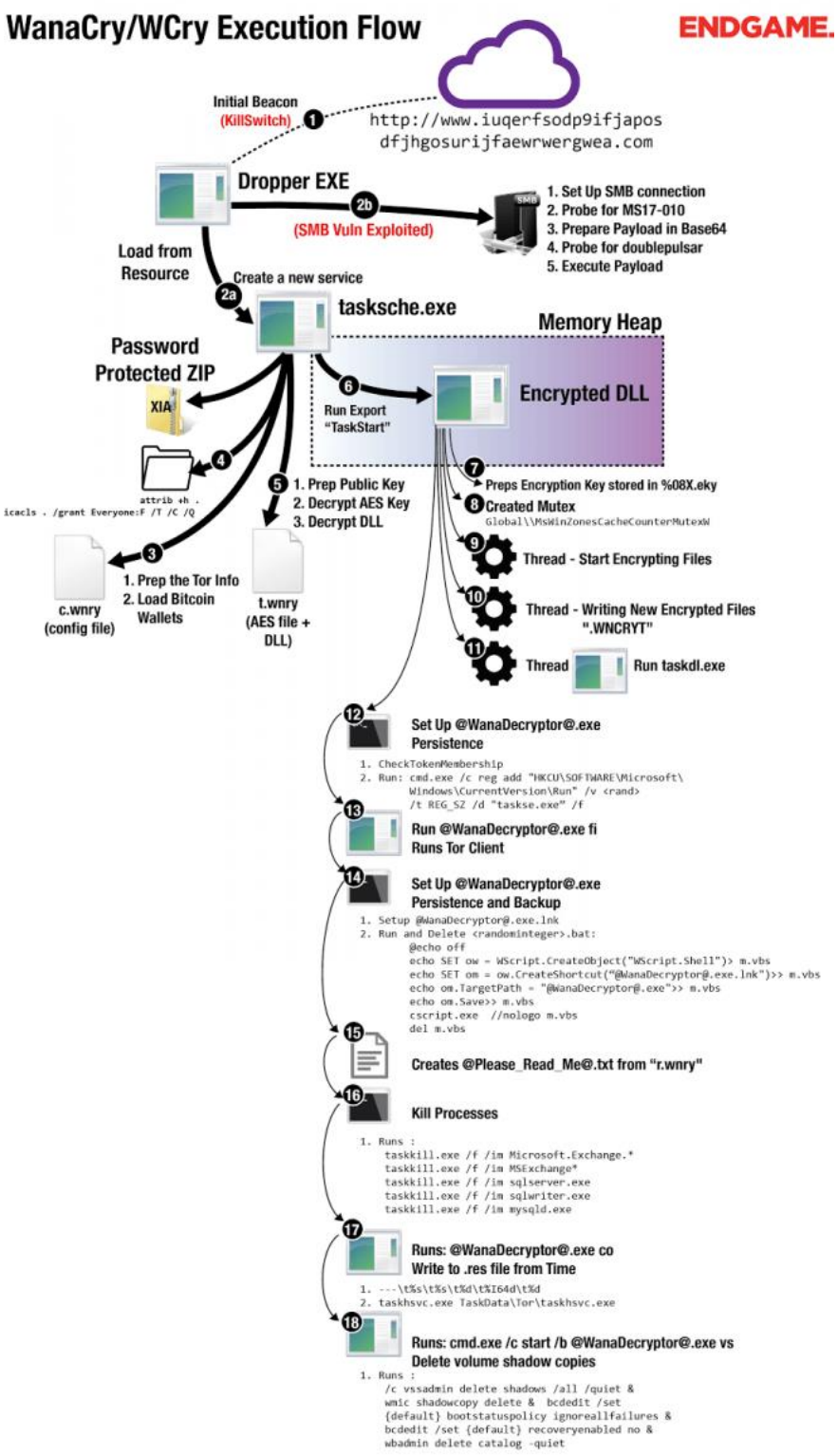

Figure 19 - WannaCry execution flow source: https://www.elastic.co/blog/wcrywanacry-ransomware-technical-analysis

2.3 PROCEDURE PART 2 ANTI-VIRUS & SANDBOX TESTING

How the malware evades anti-virus

This section of the white paper involves looking at how the WannaCry evades anti-virus and what techniques it uses to achieve this. Three prominent anti-virus software has been acquired to test this including Malwarebytes, Bitdefender and Kingsoft. First up for testing is Malwarebytes an extremely popular anti-virus software developed by Malwarebytes Inc, this software comes with the ability of scanning induvial files and this was used to scan WannaCry. Figure 20 displays the result of the scan showing that Malwarebytes correctly identified the file as a form of malware.

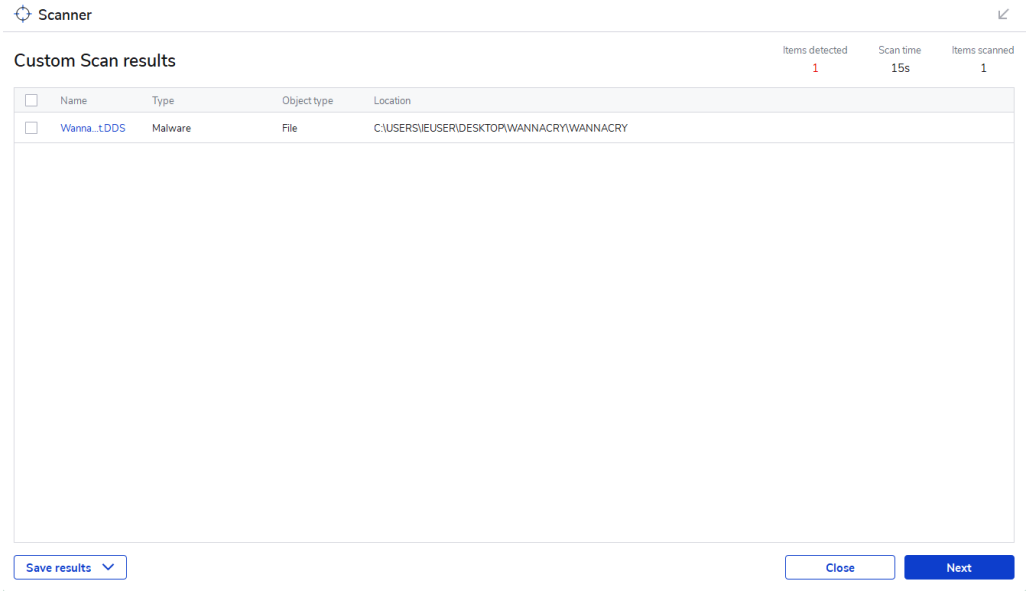

Figure 20 - Malwarebytes result

The next Anti-virus used to scan the WannaCry was Bitdefender – a Romanian developed anti-virus software that has numerous accolades. Figure 21 presents the results of the scan showing that bit defender correctly identified the malware. Furthermore, the antivirus also returned that is was ransomware and the name of it.

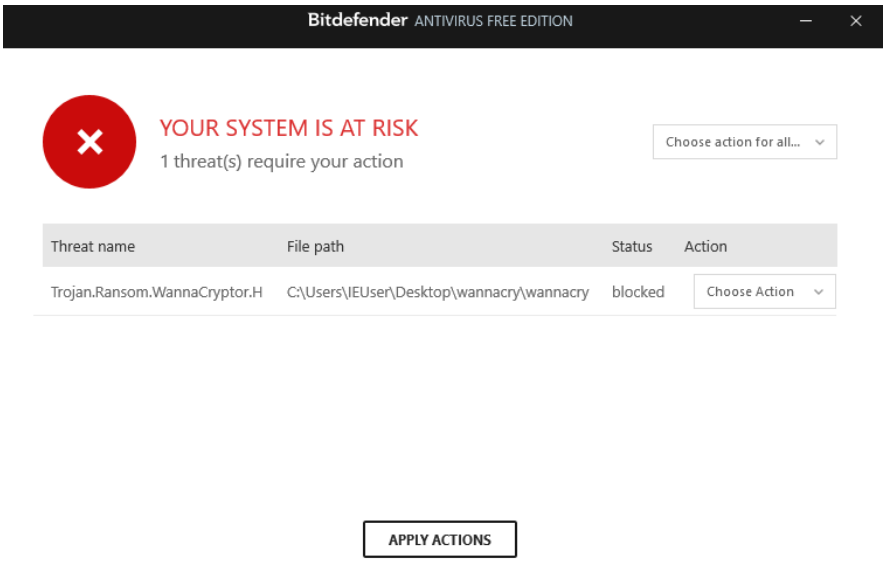

Figure 21 - Bitdefender results

The final anti-virus selected to be tested was CMC Anti-virus, this software is based in Thailand and is used by the government in its home country. Figure 22 presents the results of the scan which shows the software failed to detect the file was malicious.

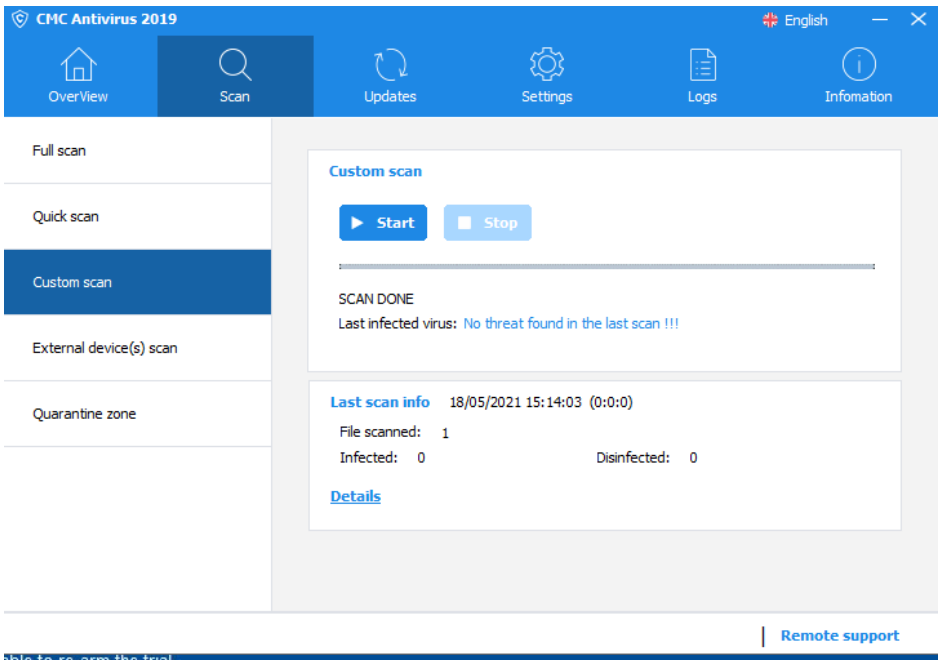

Figure 22 - CMC anti-virus results

How WannaCry attempts to prevent analyzation in a virtualized environment

The exploit WannaCry employs a number of techniques to ensure professionals are unable to analyze the malware in a virtualized environment. One way in which the exploit checks for the existence of a virtual test environment is using the windows function 'IsDebuggerPresent', this function is used to determine if the program is being debugged by a user debugger, so it can alter its functionality and behavior. 'IsDebuggerPresent' is present on all windows machines as it is located in the kernel 32.lib library and it can be bypassed using a number of methods.

Another form of evasive technique WannaCry uses to stunt analyzation is querying the host machine for internet access, if the malware was being analyzed in a virtualized environment it would receive a reply from the server and shutdown. This technique is actually the kill switch which was covered in the previous section. With no way to understand the minds of the WannaCry architects it is possible to presume the attackers wanted the option to stop the attacks at their leisure or the kill switch was indeed an anti-sandbox evasion technique. The exploit will also check for low amounts of memory by using the windows functions 'GlobalMemoryStatusEx' which retrieves information about the system's current usage of both physical and virtual memory. Furthermore, the malware also has checks present for storage devices this is done through the 'GetDiskFreeSpaceExW' windows function which retrieves information about the amount of space that is available on a disk volume.

Other methods employed by WannaCry to determine if it is being analyzed in a virtualized environment include scouring the currently running processes used by the host machine. Furthermore, the malware also attempts to sleep all tasks on the machine, this could be the exploit attempting to time out any important malware analysis programs.

2.4 EVOLUTION OF RANSOMWARE AND WANNACRY

The first use of ransomware can be traced back to PC Cyborg the first glimpse at what modern ransomware would become. This malware was active even before the invention of the internet as it was distributed through physical mail and was cleverly masqueraded as an AIDS education software – this virus is also known as the aid's virus. Real world extortion but digitalized, this came as a shock to the general public and the exploits victims. The program worked by incrementing a counter every time the machine was booted up, when the counter reached 90 it began to hide the victim's directories and encrypt or lock the names of the files on the C drive. For a user to recover access to the files, a ransom would be required in order to regain permissions, this payment was 189$ which would be sent to a PO box located in Panama.

In the following years new types of ransomware would emerge looking to extort payment from unsuspecting victims. These newer forms were based on the template of PC cyborg but handled encryption differently, instead of using symmetric encryption which makes use of only one key to encrypt and decrypt. The exploits used asymmetric encryption algorithms which uses two separates yet connected keys to encrypt and decrypt information. One example of this is GPCoder a ransomware that would encrypt the files with particular extensions and then inform the victim that $100 to $200 must be paid to retrieve the encrypted data.

Rather than encrypting a user's data new variants of ransomware instead relied on completely shutting users out of their account and leveraging this in the ransom. The heart of the strategy was the same, making the users data inaccessible but in a substantially blunter manner. An example of this is Winlock, a ransomware variant discovered in 2010, this exploit would stop access to the computer and demand a fee to unlock the computer. This displays the way in which ransomware progressed from encrypting a victim's data to completely obstructing the user from accessing the machine.

The increasing complexity and quantity of malware can be attributed to the lack of cyber hygiene and the increasing intelligence of cyber criminals looking to strike gold. There has been an emergence of newer forms of ransomware which use encryption through 2048-bit RSA public key algorithms and communications through the anonymous tor network. Some of the malware which use these methods include WannaCry, Crypto Locker and Crypto Wall. The diversification of malware has also occurred with IOT devices suffering attacks, in 2014 a ransomware termed Simp Locker was discovered capable of scouring the device's SD card for data with particular extensions for the same cause: to encrypt and demand a ransom fee for the files to be unlocked.

WannaCry variants

Research undertaken by the security company Sophos, headed by Peter Mackenzie, global malware escalations manager at Sophos, suggests that there was over 5.1 million detections of the exploit WannaCry in the time frame of Oct. 1, 2018 and Dec. 31, 2018. What is most alarming is the sheer number of variants discovered, totaling at over 12,000 distinctive WannaCry variants. Just one of these implementations was responsible for over 66.7% of detections.

The reason for such a high number of variants could be attributed to the fact that only a minuscule change affecting one byte changes the exploits hash file. Some variants also removed the highly publicized kill switch therefore making the worms ability to propagate even more effective. Something interesting that was discussed in the report was the fact the malware intelligently looks to ignore a machine if there is already an instance of WannaCry present on the system. However, these new variants essentially removed the ransomware component of WannaCry turning it into a standard worm. Through the use of hex editing the kill switch, the binary of WannaCry was corrupted, these variants pose little risk apart from occupying network bandwidth and being an inconvenience.

Expanding on the point of the kill switch being removed, around half of the variants tested removed the kill switch or simply changed the URL. Figure 23 displays the original WannaCry sample and Figure 24 presents the updated WannaCry sample.

```
mov     ecx, 0Eh
mov     esi, offset aHttpWwwIuqerfs ; 'http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com'
lea     edi, [esp+58h+szUrl]
```

Figure 23 - Original WannaCry sample

Figure 24 - Updated WannaCry sample

Other methods in which the malware bypassed the kill switch include altering the code to order the exploit to execute no matter what, replacing the kill switch code with a NOP slide essentially instructing the program to do nothing and finally the last method involved using a 2 byte JMP instruction to bypass the statements which check the result of the kill switch connection.

3 DISCUSSION

3.1 GENERAL DISCUSSION

Overall, the malware WannaCry is an extremely efficient exploit combining different components to successfully compromise unsuspecting machines. Its use of eternal blue allows it to propagate to other machines on the network and gives it that beginning foothold in a victim's computer. With the advancement of technology exploit designers and their malware continue to become more intelligent and WannaCry proves this, from the earliest ransomware of PC Cyborg to today's tesla crypt, cyber security specialists have their hands full. WannaCry is not perfect however, it does have its weaknesses and these well known. Any competent anti-virus has the ability to correctly identify the malware as shown in the previous section however it is worrying that a piece of software used by government bodies in Thailand still to this day failed to recognize a notorious piece of malware. Its use of basic sandbox detection techniques is problematic, but these can be easily bypassed through making minor adjustments and configurations, they are really standard techniques employed by most modern malware.

Where the exploit excels is the encryption module which uses both RSA and AES, once the files have been encrypted there is a very slim chance of getting them back. However, it is not all bleak, files cached in any of the following places: Desktop, My Documents, or on any removable disks in the computer at the moment of contamination are overridden with randomly generated information and deleted. This shows users are unable to recover their data with a disk recovery tool. However, due to the many weak points found in exploit it is possible to recover other encrypted files on the system when they were stored outside of these locations, using an undelete of disk recovery tool, as most of the files are moved to a temporary folder and then normally deleted. However, the recovery ratio may on differ on unique machines because the deleted file may be overwritten by other disk methods.

The payment aspect of WannaCry could be improved, using bitcoin is satisfactory as it is effectively anonymous so hackers do not need to provide personal information when starting a bitcoin account and law enforcement can't freeze assets like they would do with a back account. However, there is a growing concern on whether bitcoin is actually anonymous, several big cases recently in which bitcoin has been used as evidence in prosecution have occurred including the founder of silk road. Using a crypto currency such as monero would provide more anonymity as the coin uses ring signatures and stealth addresses.

There is a number of methods in which the WannaCry malware can be mitigated and also completely halted. Due to its unique ability to propagate to other machines on the network the malware has more mitigation techniques than the bog-standard ransomware. Some of these methods include:

Mitigations

Disabling/blocking both incoming and outgoing data from the SMB ports. Both UDP ports 37 and 138 and TCP ports should also be disabled to ensure the worm component of WannaCry is unable to spread to other nodes on the network. If possible, it is recommended that these are blocked through the use of internal network segmentation when sending data to other VLANs, remote WAN connections and IPsec tunnels. This allows the network to remain more secure as the area of attack is smaller. A good network design can significantly help contain the propagation of this infection and reduce its impact.

Another method that successfully mitigates the risk posed by WannaCry involves updating windows to the most recent implementations. The worm component that was responsible for infecting other computers connected to the network was patched even before WannaCry was first seen on the 14 of March 2017. This vulnerability affects both current and older operating systems including Windows XP, Windows 8 and Server 2003.

If the machine has already been compromised it is imperative that the computer is thoroughly cleaned. Apart from encrypting all a user's files the exploit as previously mentioned will install double pulsar, this is why it is so important to wipe the computer and restore data from before infection.

There is also a number of different software's out there that can be used to prevent malware infecting machines, for instance an anti-virus like Malwarebytes easily identifies the exploit and quarantines the piece of malicious code. Using a component intrusion detection system like snort would stop the malware in its first phase. Snort comfortably identifies eternal blue and would alert the user of malicious activity, a few software can be combined to significantly improve the security of a machine.

To counteract the encryption functionality of WannaCry and other ransomware it is important to make regular backups ensuring that if a piece of ransomware does infect a machine with sensitive information a backup is available. This why ransomware is so effective as it targets human weaknesses by locking away important documents and photos.

Paying particular attention to keeping older machines on the network is essential as this exploit takes advantage of an older attack.

3.2 FUTURE WORK

In the future analyzing different types of ransomware and making comparisons between different strands would be beneficial to see contrasting methods. The way in which one form of ransomware attempts to evade anti-virus is different from another. Furthermore, looking into the encryption methods used by WannaCry would help with understanding the exploit as a whole better.

Possibly creating a python script that checks for weaknesses in the host machine could be beneficial to guard against ransomware attacks. Furthermore, recreating some of the most prominent features/components of WannaCry in a different programming language would enable for a better understanding of the minds behind these attacks.

Due to time and resource constraints only a select number of malware analysis software's were used, in the future it would be beneficial to try a variety.

REFERENCES

For URLs, Blogs:

Fruhlinger, J., 2021. *What is WannaCry ransomware, how does it infect, and who was responsible?*. [online] CSO Online. Available at: <https://www.csoonline.com/article/3227906/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html> [Accessed 12 May 2021].

Dsimg.ubm-us.net. 2021. [online] Available at: <https://dsimg.ubm-us.net/envelope/401303/576833/Anomali-WannaCry_One_Year_Later-Whitepaper.pdf> [Accessed 14 May 2021].

Blogs, F., 2021. *SMB Exploited: WannaCry Use of "EternalBlue"*. [online] FireEye. Available at: <https://www.fireeye.com/blog/threat-research/2017/05/smb-exploited-wannacry-use-of-eternalblue.html> [Accessed 20 May 2021].

LogRhythm. 2021. A Technical Analysis of WannaCry Ransomware | LogRhythm. [online] Available at: <https://logrhythm.com/blog/a-technical-analysis-of-wannacry-ransomware/> [Accessed 12 May 2021].

Tahiri, S., 2021. How did Wanna Cry get past Antivirus Programs. [online] Information Security Stack Exchange. Available at: <https://security.stackexchange.com/questions/166744/how-did-wanna-cry-get-past-antivirus-programs> [Accessed 15 May 2021].

Ft.com. 2021. *Timeline: How the WannaCry cyber attack spread*. [online] Available at: <https://www.ft.com/content/82b01aca-38b7-11e7-821a-6027b8a20f23> [Accessed 16 May 2021].

www.kaspersky.co.uk. 2021. *What is WannaCry ransomware?*. [online] Available at: <https://www.kaspersky.co.uk/resource-center/threats/ransomware-wannacry> [Accessed 18 May 2021].

ComputerWeekly.com. 2021. *WannaCry variants accidentally protecting against WannaCry*. [online] Available at: <https://www.computerweekly.com/news/252470868/WannaCry-variants-accidentally-protecting-against-WannaCry> [Accessed 17 May 2021].

News, A., 2021. *A timeline of the WannaCry cyberattack*. [online] ABC News. Available at: <https://abcnews.go.com/US/timeline-wannacry-cyberattack/story?id=47416785> [Accessed 20 May 2021].

Techcrunch.com. 2021. *TechCrunch is now a part of Verizon Media*. [online] Available at: <https://techcrunch.com/2019/05/12/wannacry-two-years-on/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAB9n2TOJXssf75u3pnFRLRbOptVvEcMFIMYwwg_5AQ96RrOCL60kGWF__0w6vGzsSZfaYgRusvhAU8S15w6GTrI59hJWdwSzIZ5ewGyr4Fmpb8M9oqe-UxYLXr_XeQuNs6O7dBLBE34B5y_Iy_pnOYrDqNAMJskXpTkMJ83n2FAR> [Accessed 19 May 2021].

The Indian Express. 2021. *WannaCry ransomware attack: List of Indian states that have been affected*. [online] Available at: <https://indianexpress.com/article/technology/tech-news-technology/wannacry-ransomware-attack-list-of-indian-states-that-have-been-affected-4660449/> [Accessed 9 May 2021].

2021. [online] Available at: <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/wannacry-wcry-ransomware-how-to-defend-against-it> [Accessed 20 May 2021].

Labs, M., 2021. *Further Analysis of WannaCry Ransomware | McAfee Blogs*. [online] McAfee Blogs. Available at: <https://www.mcafee.com/blogs/other-blogs/mcafee-labs/analysis-wannacry-ransomware/> [Accessed 7 May 2021].

Digital-forensics.sans.org. 2021. [online] Available at: <https://digital-forensics.sans.org/community/papers/grem/reverse-engineering-wannacry-worm-anti-exploit-snort-rules_5549> [Accessed 20 May 2021].

Medium. 2021. *Cuckoo Sandbox Installation Guide*. [online] Available at: <https://medium.com/@warunikaamali/cuckoo-sandbox-installation-guide-d7a09bd4ee1f> [Accessed 17 May 2021].

Docs.microsoft.com. 2021. *IsDebuggerPresent function (debugapi.h) - Win32 apps*. [online] Available at: <https://docs.microsoft.com/en-us/windows/win32/api/debugapi/nf-debugapi-isdebuggerpresent> [Accessed 18 May 2021].

Bhat, S., 2021. *DoublePulsar – A Very Sophisticated Payload for Windows - SecPod Blog*. [online] SecPod Blog. Available at: <https://www.secpod.com/blog/doublepulsar-a-very-sophisticated-payload-for-windows/> [Accessed 20 May 2021].

SANS Internet Storm Center. 2021. *Detecting SMB Covert Channel ("Double Pulsar")*. [online] Available at: <https://isc.sans.edu/forums/diary/Detecting+SMB+Covert+Channel+Double+Pulsar/22312/> [Accessed 20 May 2021].

Malware-traffic-analysis.net. 2021. *Malware-Traffic-Analysis.net - 2017-05-18 - Guest blog by David Szili - pcap of WannaCry spreading using EtnernalBlue*. [online] Available at: <https://malware-traffic-analysis.net/2017/05/18/index2.html> [Accessed 18 May 2021].

Blockchain.com. 2021. *Blockchain.com Explorer | BTC | ETH | BCH*. [online] Available at: <https://www.blockchain.com/btc/address/12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw> [Accessed 18 May 2021].

Docs.microsoft.com. 2021. *[MS-SMB2]: SMB2 NEGOTIATE Response*. [online] Available at: <https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-smb2/63abf97c-0d09-47e2-88d6-6bfa552949a5> [Accessed 17 May 2021].

MalwareTech. 2021. *How to Accidentally Stop a Global Cyber Attacks - MalwareTech*. [online] Available at: <https://www.malwaretech.com/2017/05/how-to-accidentally-stop-a-global-cyber-attacks.html> [Accessed 7 May 2021].

To, H., 2021. *Permanently disable Microsoft Defender Antivirus on Windows 10*. [online] Windows Central. Available at: <https://www.windowscentral.com/how-permanently-disable-windows-defender-windows-10#disable-microsoft-defender-with-group-policy> [Accessed 20 May 2021].

Bradford, C. and Bradford, C., 2021. *How to Optimize Your VM for Malware Testing*. [online] StorageCraft Technology, LLC. Available at: <https://blog.storagecraft.com/how-to-optimize-vm-malware-testing/> [Accessed 20 May 2021].

APPENDICES

APPENDIX A

List of file types the malware searches for

```
.der
.pfx
.key
.crt
.csr
.p12
.pem
.odt
.ott
.sxw
.stw
.uot
.3ds
.max
.3dm
.ods
.ots
.sxc
.stc
.dif
.slk
.wb2
.odp
.otp
.sxd
.std
.uop
.odg
.otg
.sxm
.mml
.lay
.lay6
.asc
.sqlite3
.sqlitedb
.sql
.accdb
.mdb
.db
.dbf
.odb
.frm
.myd
```

.myi
.ibd
.mdf
.ldf
.sln
.suo
.cs
.c
.cpp
.pas
.h
.asm
.js
.cmd
.bat
.ps1
.vbs
.vb
.pl
.dip
.dch
.sch
.brd
.jsp
.php
.asp
.rb
.java
.jar
.class
.sh
.mp3
.wav
.swf
.fla
.wmv
.mpg
.vob
.mpeg
.asf
.avi
.mov
.mp4
.3gp
.mkv
.3g2
.flv
.wma
.mid
.m3u
.m4u
.djvu

.svg
.ai
.psd
.nef
.tiff
.tif
.cgm
.raw
.gif
.png
.bmp
.jpg
.jpeg
.vcd
.iso
.backup
.zip
.rar
.7z
.gz
.tgz
.tar
.bak
.tbk
.bz2
.PAQ
.ARC
.aes
.gpg
.vmx
.vmdk
.vdi
.sldm
.sldx
.sti
.sxi
.602
.hwp
.snt
.onetoc2
.dwg
.pdf
.wk1
.wks
.123
.rtf
.csv
.txt
.vsdx
.vsd
.edb
.eml

.msg
.ost
.pst
.potm
.potx
.ppam
.ppsx
.ppsm
.pps
.pot
.pptm
.pptx
.ppt
.xltm
.xltx
.xlc
.xlm
.xlt
.xlw
.xlsb
.xlsm
.xlsx
.xls
.dotx
.dotm
.dot
.docm
.docb
.docx
.doc

Bitcoin Wallet information

Bitcoin information	Data
Address	12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Format	Base58 (P2PKH)
Transactions	233
Total Received	19.68111950 BTC ($883,549.81)
Total Sent	17.77113037 BTC ($797,804.15)
Final Balance	1.90998913 BTC ($85,745.66)

Table 4 - 1st bitcoin wallet

Bitcoin information	Data
Address	13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94
Format	Base58 (P2PKH)
Transactions	142
Total Received	20.06583352 BTC ($900,820.88)
Total Sent	19.74510304 BTC ($886,422.24)
Final Balance	0.32073048 BTC ($14,398.64).

Table 5 - 2nd bitcoin wallet

Bitcoin information	Data
Address	115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
Format	Base58 (P2PKH)
Transactions	124
Total Received	14.87769994 BTC ($667,908.60)
Total Sent	14.41067602 BTC ($646,942.37)
Final Balance	0.46702392 BTC ($20,966.23).

Table 6 - 3rd bitcoin wallet

APPENDIX B

Kill switch domains

Domain	Associated Sample MD5 Hash
iuqssfsodp9ifjaposdfjhgosurijfaewrwergwea.com	c2559b51cfd37bdbd5fdb978061c6c16
ayylmaotjhsstasdfasdfasdfasdfasdfasdfasdf.com	a44964a7be94072cdfe085bc43e7dc95
ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com	80ce983d22c6213f35867053bec1c293
iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com	db349b97c37d22f5ea1d1841e3c89eb4
iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.test	96dff36b5275c67e35097d77a120d0d4

Table 7 - kill switch domain table

Format of encrypted files

Offset	Value
0x0000	WANACRY!
0x0008	Length of RSA encrypted data
0x000C	RSA encrypted AES file encryption key
0x010C	File type internal to WannaCry
0x0110	Original file size
0x0118	Encrypted file contents (AES-128 CBC)

Table 8 - format of files table

APPENDIX C

Files found from WannaCry

Filename	MD5 Hash	Description
r.wnry	3e0020fc529b1c2a061016dd2469ba96	Text ransom note
s.wnry	ad4c9de7c8c40813f200ba1c2fa33083	Zip file containing Tor files
t.wnry	5dcaac857e695a65f5c3ef1441a73a8f	Encrypted encryption tool
taskdl.exe	4fef5e34143e646dbf9907c4374276f5	*.WNCRYT file deletion tool
taskse.exe	8495400f199ac77853c53b5a3f278f3e	Utility used to launch decryption tool
u.wnry	7bf2b57f2a205768755c07f238fb32cc	Decryption tool
b.wnry	c17170262312f3be7027bc2ca825bf0c	Ransom image (BMP)
c.wnry	ae08f79a0d800b82fcbe1b43cdbdbefc	Configuration data

Table 9 - files found table