A Comprehensive Analysis of WannaCry: Technical Analysis, Reverse Engineering, and Motivation

Waleed Alraddadi, *and* Harshini Sarvotham

***Abstract*— WannaCry is a self-propagated malware, classified as crypto-ransomware, that spread around the internet affecting more than 200,000 computers. A malware is a malicious software that intentionally design to do harmful actions to a computer system. A crypto-ransomware is a harmful computer program that encrypts user's files for money extortion purposes. WannaCry also has a computer worm component. A computer worm is a harmful program that can propagate to other computers through computer networks. WannaCry utilizes Bitcoin for receiving victim's payment in order to evade law enforcements tracking. Bitcoin is an electronic currency that allows anonymous transactions. Additionally, WannaCry uses Tor network for it's Command & Control communications. Command and control refer to the communications between an operator of malware and the malware itself. Tor network is a number of connected computers (routers) that allows anonymous internet communications. In this paper we investigate the workings of the two different components of WannaCry namely the ransomware component and the worm component. Moreover, we discuss the motivation behind WannaCry.**

***Index Terms*— WannaCry, analysis, ransomware, encryption, files, propagation, network, SMB, vulnerability, motivation.**

I. Introduction

WannaCry is a malware that is classified as a crypto-ransomware which is defined as a software that encrypts users' files and demands them to pay some amount of money in exchange to decrypt their files. The purpose of this kind of malwares is money extortion. Crypto-ransomwares use shock and fear tactics to push users to pay the required ransom for instance in WannaCry, such tactic is being implemented by showing a three-day countdown and threatening the user that the decryption key will be deleted if he didn't pay on time. WannaCry also has been considered a network worm because of its self-propagation capability via computer networks. WannaCry first time seen in the wild on May 12, 2017[1]. WannaCry is considered the biggest ransomware outbreak in the history. It had infected more than 200,000 computers in over 150 countries [1]. WannaCry consists of two components: a worm module for self-propagation and ransomware for files encryption. WannaCry uses Tor hidden services for its C & C (command and control) communications. The main purpose of the C & C in WannaCry is to check if the victim has paid the ransom and delivering the decryption key.

II. Worm Module

WannaCry is referred to as a self-propagating malware due to the presence of the worm module. This module is used just for the purpose of propagation and thus spreading itself to all the computers connected to the internal and external network. In this section we will discuss the vulnerability that the malware exploited along with the propagation procedure.

A. SMB Vulnerability

The WannaCry malware exploits the vulnerability that is in the Server Message Block (SMB) protocol of the Windows implementation. SMB is a Transport protocol used for file sharing, printer sharing and access to remote services in Windows. SMB protocol operates over TCP ports 139 and 445. The malware makes use of the Vulnerability in SMB Version 1 (SMB v1) and TCP port 445 to propagate. This vulnerability allows malformed packets from the remote attackers to execute arbitrary code on the victim's computer.

B. Experiment Information

In order to learn about the propagation characteristics of the malware we executed the WannaCry sample in a controlled environment and monitored its network traffic flow. We used the following tools to perform our analysis.

Tools	Description
Kali Linux	Linux based Operating System used for forensics and penetration testing
Wireshark	Packet analyzer used for network analysis
ApateDNS	Tool used for retrieving the IP address or hostnames from the malware
IDA Pro	A dissembler that generates assembly language source code from machine executable code

A Local Area Network (LAN) was created using three Virtual Machines (VMs):

A kali Linux machine to capture the packets in Wireshark – 172.16.182.156

A Windows 7 Professional x64 Service Pack 1 where the malware was executed (Main victim's machine) – 172.16.182.128

A Windows 7 x64 VMware machine connected in the same LAN – 172.16.182.158

A few prerequisites to carry out the network analysis is to enable the SMB v1 protocol in all the machines connected in the LAN and disable the Windows Firewall so that all the machines are connected to each other. Now upon successful establishment of connection between all the machines we execute the malware in the victim's machine (Windows 7 Professional).

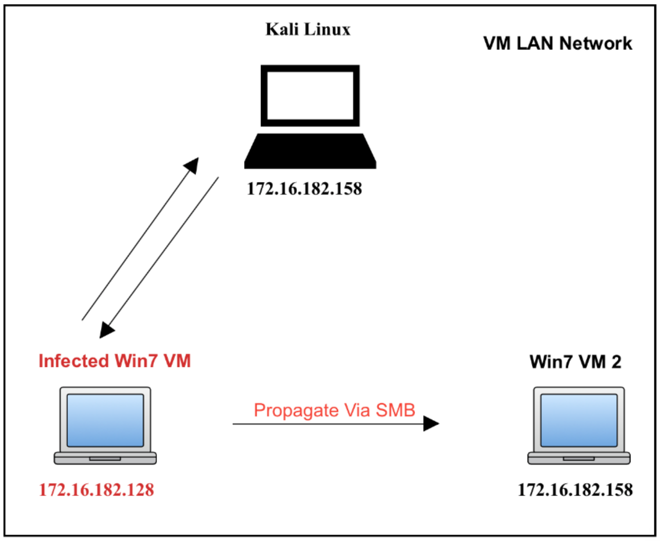
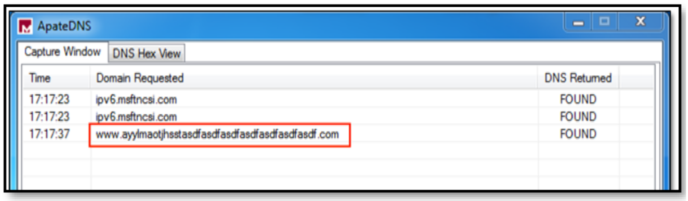


Figure 1: Experiment Architecture

C. *Network Analysis*

The malware executable sends a request to a domain - http://www.ayylmaoTJHSSTasdfasdfasdfasdfasdfasdfasdf.com for connection. If the domain is connected or reachable then the dropper will exit immediately which means that the malware will not be executed. The malware will be executed only if it fails to connect to the domain. Therefore, one of the ways to stop the attack is to sinkhole the domains. Thus, this was called the kill switch to the malware. Therefore, before the launch of the malware this domain was inactive or not registered. The malware contacting the domain can be seen in the ApateDNS tool as below:

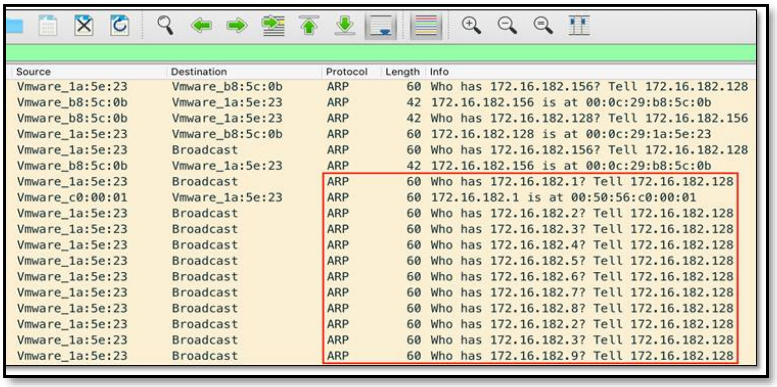


```
Time      Domain Requested                                          DNS Returned
17:17:23  ipv6.msftncsi.com                                         FOUND
17:17:23  ipv6.msftncsi.com                                         FOUND
17:17:37  www.ayylmaotjhsstasdfasdfasdfasdfasdfasdfasdf.com         FOUND
```

Figure 3: ApateDNS results

- The victim's machine will scan the local network for other machines that are accessible and have an exposed SMB port (445). Therefore, we can see that it sends TCP (Transmission Control Protocol) requests SYN (synchronize) in port 445.

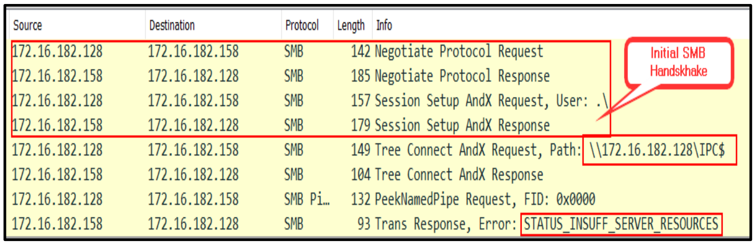
- It then sends ARP request as a broadcast to all the IP addresses available in the network. It increments the IP address by 1 and checks for a response from any one of them.



```
Source            Destination       Protocol  Length  Info
Vmware_1a:5e:23   Vmware_b8:5c:0b   ARP           60  Who has 172.16.182.156? Tell 172.16.182.128
Vmware_b8:5c:0b   Vmware_1a:5e:23   ARP           42  172.16.182.156 is at 00:0c:29:b8:5c:0b
Vmware_b8:5c:0b   Vmware_1a:5e:23   ARP           42  Who has 172.16.182.128? Tell 172.16.182.156
Vmware_1a:5e:23   Vmware_b8:5c:0b   ARP           60  172.16.182.128 is at 00:0c:29:1a:5e:23
Vmware_1a:5e:23   Broadcast         ARP           60  Who has 172.16.182.156? Tell 172.16.182.128
Vmware_b8:5c:0b   Vmware_1a:5e:23   ARP           42  172.16.182.156 is at 00:0c:29:b8:5c:0b
Vmware_1a:5e:23   Broadcast         ARP           60  Who has 172.16.182.1? Tell 172.16.182.128
Vmware_c0:00:01   Vmware_1a:5e:23   ARP           60  172.16.182.1 is at 00:50:56:c0:00:01
Vmware_1a:5e:23   Broadcast         ARP           60  Who has 172.16.182.2? Tell 172.16.182.128
Vmware_1a:5e:23   Broadcast         ARP           60  Who has 172.16.182.3? Tell 172.16.182.128
Vmware_1a:5e:23   Broadcast         ARP           60  Who has 172.16.182.4? Tell 172.16.182.128
Vmware_1a:5e:23   Broadcast         ARP           60  Who has 172.16.182.5? Tell 172.16.182.128
Vmware_1a:5e:23   Broadcast         ARP           60  Who has 172.16.182.6? Tell 172.16.182.128
Vmware_1a:5e:23   Broadcast         ARP           60  Who has 172.16.182.7? Tell 172.16.182.128
Vmware_1a:5e:23   Broadcast         ARP           60  Who has 172.16.182.8? Tell 172.16.182.128
Vmware_1a:5e:23   Broadcast         ARP           60  Who has 172.16.182.2? Tell 172.16.182.128
Vmware_1a:5e:23   Broadcast         ARP           60  Who has 172.16.182.3? Tell 172.16.182.128
Vmware_1a:5e:23   Broadcast         ARP           60  Who has 172.16.182.9? Tell 172.16.182.128
```

Figure 2: Scanning internal network

- In our experiment the other machine that is connected to the network is 172.16.182.158. Once the response from the other machine in the same LAN is received it checks for the exposed SMB ports (445)
- Once it establishes a connection with the other machine it checks whether the machine has the SMB v1 protocol and thus checking for the vulnerability.
    - There occurs an initial SMB Handshake (Negotiation Req/Response and Session Setup Req/. Response).
    - Once this completed it connects to the IPC$ share - This is a session in Windows that allows anonymous user to perform certain activities.
    - The malware then connects to the IP address of the main victim's machine (172.16.182.128)
    - It then receives a trans response from the other machine in the LAN to the main victim's machine Status as STATUS_INSUFF_SERVER_RESOURCES which confirms that the machine does have the vulnerability in SMB v1.

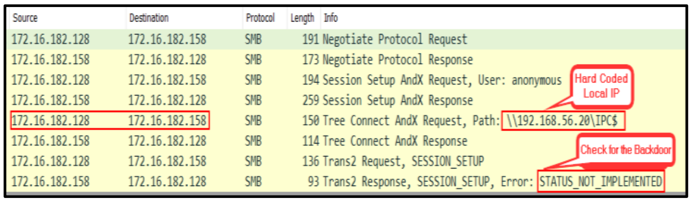


```
Source          Destination     Protocol  Length Info
172.16.182.128  172.16.182.158  SMB       142 Negotiate Protocol Request
172.16.182.158  172.16.182.128  SMB       185 Negotiate Protocol Response
172.16.182.128  172.16.182.158  SMB       157 Session Setup AndX Request, User: .\
172.16.182.158  172.16.182.128  SMB       179 Session Setup AndX Response
172.16.182.128  172.16.182.158  SMB       149 Tree Connect AndX Request, Path: \\172.16.182.128\IPC$
172.16.182.158  172.16.182.128  SMB       104 Tree Connect AndX Response
172.16.182.128  172.16.182.158  SMB Pi…   132 PeekNamedPipe Request, FID: 0x0000
172.16.182.158  172.16.182.128  SMB        93 Trans Response, Error: STATUS_INSUFF_SERVER_RESOURCES
```

Figure 4: Vulnerability check

- The next check is to determine whether the DoublePulsar backdoor exist.

- DoublePulsar injects a backdoor into the affected hosts for easier access and can be removed upon system reboot. This is an implant tool that has been developed by NSA to get access to Microsoft Windows systems. This tool had been stolen along with several other tools by Shadow Brokers group. WannaCry authors had utilized this stolen tool to make it more effective in propagation.
- After that, the malware connects to the IP address that is a hardcoded Local IP.
- It then checks for the status -STATUS_NOT_IMPLEMENTED to determine whether the machine is compromised with the backdoor or not.

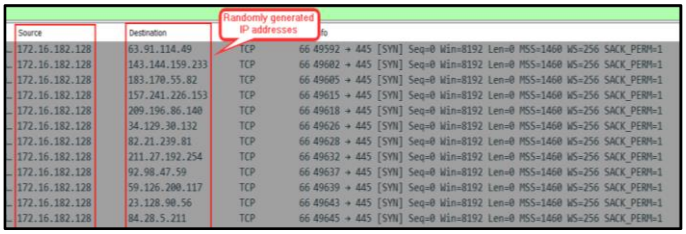


```
Source          Destination     Protocol Length Info
172.16.182.128  172.16.182.158  SMB       191 Negotiate Protocol Request
172.16.182.158  172.16.182.128  SMB       173 Negotiate Protocol Response
172.16.182.128  172.16.182.158  SMB       194 Session Setup AndX Request, User: anonymous
172.16.182.158  172.16.182.128  SMB       259 Session Setup AndX Response
172.16.182.128  172.16.182.158  SMB       150 Tree Connect AndX Request, Path: \\192.168.56.20\IPC$
172.16.182.158  172.16.182.128  SMB       114 Tree Connect AndX Response
172.16.182.128  172.16.182.158  SMB       136 Trans2 Request, SESSION_SETUP
172.16.182.158  172.16.182.128  SMB        93 Trans2 Response, SESSION_SETUP, Error: STATUS_NOT_IMPLEMENTED
```

Figure 5: DoublePulsar check

- The next step is to exploit the vulnerability.
  - We can see from our analysis that it sends a sequence of NOPs (No-operation instructions) to overflow the NT trans request which leads to multiple Trans 2 secondary response.
  - This Trans 2 secondary response will contain the shellcode (arbitrary code) that executes the payload to exploit the vulnerability.
  - Therefore, the attackers exploited this buffer-overflow vulnerability that occurs in the SMB protocol implementation.

It then generates random IP addresses and sends TCP requests via 445 port to scan the external network and carry out the same instructions to check for the vulnerability and proceed with the execution.



```
Source          Destination                  fo
172.16.182.128  63.91.114.49     TCP   66 49592 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
172.16.182.128  143.144.159.233  TCP   66 49602 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
172.16.182.128  183.170.55.82    TCP   66 49605 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
172.16.182.128  157.241.226.153  TCP   66 49615 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
172.16.182.128  209.196.86.140   TCP   66 49618 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
172.16.182.128  34.129.30.132    TCP   66 49626 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
172.16.182.128  82.21.239.81     TCP   66 49628 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
172.16.182.128  211.27.192.254   TCP   66 49632 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
172.16.182.128  92.98.47.59      TCP   66 49637 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
172.16.182.128  59.126.200.117   TCP   66 49639 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
172.16.182.128  23.128.90.56     TCP   66 49643 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
172.16.182.128  84.28.5.211      TCP   66 49645 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
```

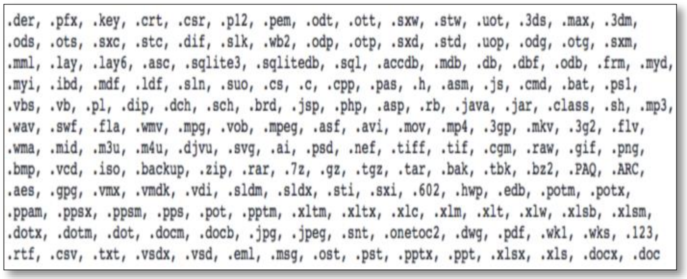
Figure 6: Scanning external network

III. Ransomware Module

Upon execution the ransomware establishes persistence by creating a Windows registry key that allows the ransomware to run upon system start. The registry key is HKCU\Software\Microsoft\Windows\CurrentVersion\Run\vyzrjjjywpoefn971 the last part of the registry key is the folder that the ransomware creates to itself. The folder name shows that the ransomware creates a unique identifier for each computer. We can see that the name it generates is a random lowercase characters appended with three random numbers.

A. Observations

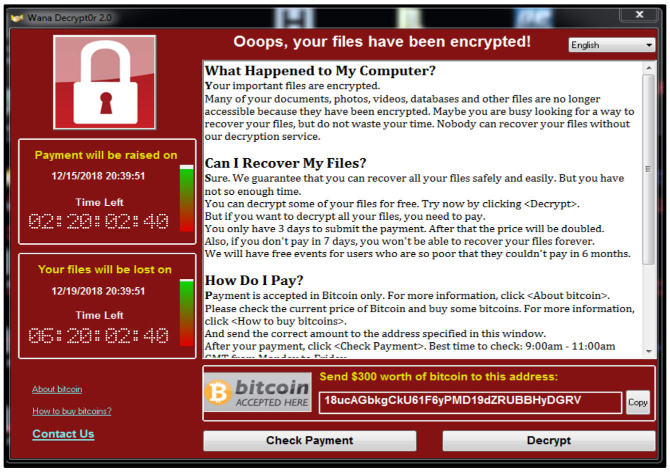
Once the malware runs it will start searching for specific Windows file extensions, file extension is the end of a file name that defines the file types e.g. File1.txt. Next, it encrypts these targeted files using and save the encrypted files. Once it is done it deletes the original files from the system to prevent the victim's from accessing them.



```
.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, .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, .edb, .potm, .potx,
.ppam, .ppsx, .ppsm, .pps, .pot, .pptm, .xltm, .xltx, .xlc, .xlm, .xlt, .xlw, .xlsb, .xlsm,
.dotx, .dotm, .dot, .docm, .docb, .jpg, .jpeg, .snt, .onetoc2, .dwg, .pdf, .wk1, .wks, .123,
.rtf, .csv, .txt, .vsdx, .vsd, .eml, .msg, .ost, .pst, .pptx, .ppt, .xlsx, .xls, .docx, .doc
```

Figure 7: List of all file extensions targeted by WannaCry (Source: A. Berry, "WannaCry Malware Profile" *FireEye*, 2017. [Online].)

We can observe that the ransomware doesn't target any executable files (.exe and .dll) to avoid system interruption. Once the encryption procedure is done the ransomware will show a window (Wana Decrypt0r program) that has decryption instructions.



Ooops, your files have been encrypted!

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on
12/15/2018 20:39:51
Time Left
02:20:02:40

Your files will be lost on
12/19/2018 20:39:51
Time Left
06:20:02:40

Send $300 worth of bitcoin to this address:
18ucAGbkgCkU61F6yPMD19dZRUBBHyDGRV

Figure 8: WannaCry main Windows

In this Wana Decrypt0r program the ransomware demands the victim to pay $300 in Bitcoin to that specific address in order to be able to decrypt the files

B. Cryptographic Model

This ransomware utilizes a hybrid cryptographic model in which it combines an asymmetric cryptography with a symmetric cryptography. To explain this model, we created the following diagram:

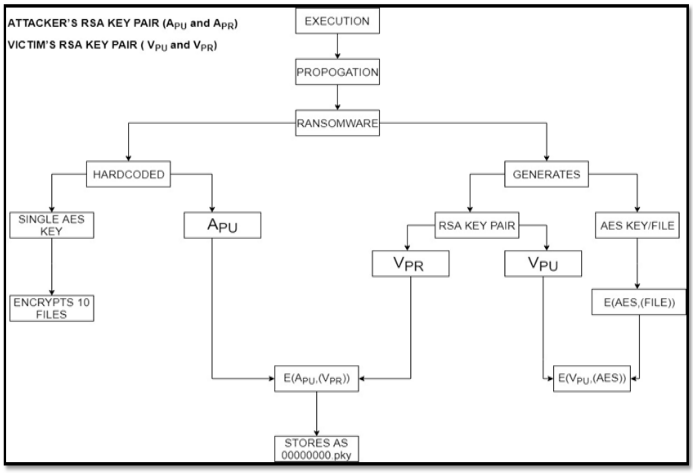


Figure 9: Cryptographic Model

- There are two hardcoded keys in the malware file:
  - An AES key that is being used for encrypting 10 random files located at the victim's Desktop. The purpose of this is to show that the @WanaDecryptor@.exe program is capable of decrypting victim's file. This is done once the victim clicks on the "Decrypt" button. The goal of this step is to convince the victim to pay the ransom.
  - RSA public key which we refer to as Attacker's public key (A_{PU}).
- It then generates a 2048-bit RSA key pair which we refer to as Victim's key pair (V_{PU} V_{PR})
- The victim's private key (V_{PR}) itself will get encrypted using the attacker public key (A_{PU}) and then will be stored at 00000000.pky.
- The original victim's private key (V_{PR}) will be destroyed.
- After that it generates unique AES keys for each file. These keys will be used to encrypt the victim's files.
- After the encryption process is done the ransomware will encrypt all the AES keys using the V_{PU} . Then it will add the encrypted key to each file it encrypts.
- Once the files are encrypted it appends. WNCRYT extension to each file and then it wipes the original files by overwriting their memory space.

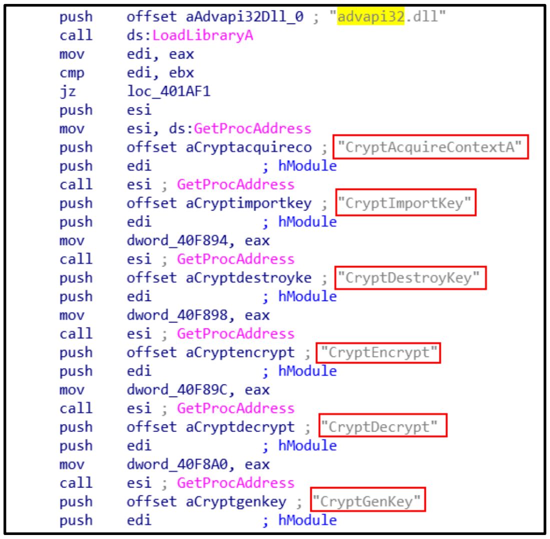
The only way to decrypt the victim's files is to:

1. Use attacker's private key (A_{PR}) to decrypt the victim's private key (V_{PR})
2. Use victim's private key (V_{PR}) to decrypt all AES keys
3. Use AES to decrypt the files

The problem is the attacker private key is unknown therefore the only way to decrypt the files is to ask the attackers to decrypt the victim's private key.

The ransomware performs all these operation using Windows API functions:

- CryptGenKey is used to generate RSA key pair.
- CryptEncrypt is used for encrypting the files using the symmetric key - AES in this case
- CryptImportKey is for importing the Attacker's public key (A_{PU})
- CryptExportKey is used for exporting the AES keys that are encrypted using the V_{PU}
- CryptDestroyKey is to destroy the memory area where the key was held in such a way that the key can never be recovered



```
push    offset aAdvapi32Dll_0 ; "advapi32.dll"
call    ds:LoadLibraryA
mov     edi, eax
cmp     edi, ebx
jz      loc_401AF1
push    esi
mov     esi, ds:GetProcAddress
push    offset aCryptacquireco ; "CryptAcquireContextA"
push    edi             ; hModule
call    esi ; GetProcAddress
push    offset aCryptimportkey ; "CryptImportKey"
push    edi             ; hModule
mov     dword_40F894, eax
call    esi ; GetProcAddress
push    offset aCryptdestroyke ; "CryptDestroyKey"
push    edi             ; hModule
mov     dword_40F898, eax
call    esi ; GetProcAddress
push    offset aCryptencrypt ; "CryptEncrypt"
push    edi             ; hModule
mov     dword_40F89C, eax
call    esi ; GetProcAddress
push    offset aCryptdecrypt ; "CryptDecrypt"
push    edi             ; hModule
mov     dword_40F8A0, eax
call    esi ; GetProcAddress
push    offset aCryptgenkey ; "CryptGenKey"
push    edi             ; hModule
```

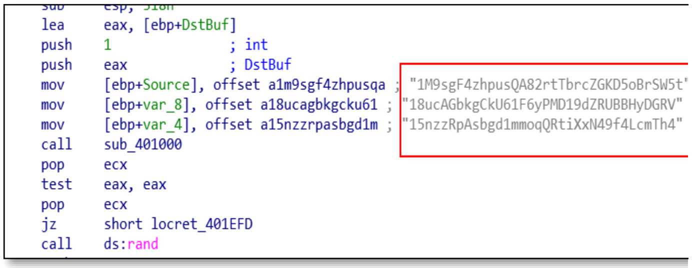
Figure 10: Cryptographic Functions

C. Advantages of This Cryptographic Model

- Encrypting the files very fast by using the symmetric AES encryption
- The C & C communications is minimal because all of the required encryption keys are either generated in the victim's computer or hard coded in the malware file
- Using a unique AES key for each file minimize the risk of key leaking, for instance if the encryption process got disrupted and the victim was able to obtain an AES key from memory, he can only use that key to decrypt a single file
- The attacker's private key A_{PR} that to be used for decrypting the victim's private key V_{PR} is safely kept secret and never transmitted
- The use of secure cryptographic encryption tools (RSA, AES) and key sizes makes it difficult to break.

D. Bitcoin

In order to evade prosecution, the attackers used Bitcoin in the payment method. In Our analysis we found that WannaCry uses three different hardcoded bitcoin addresses



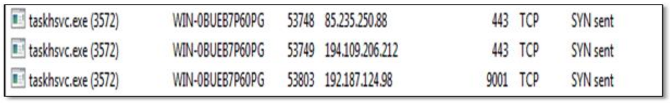
```
sub     esp, 318h
lea     eax, [ebp+DstBuf]
push    1               ; int
push    eax             ; DstBuf
mov     [ebp+Source], offset a1m9sgf4zhpusqa ; "1M9sgF4zhpusQA82rtTbrcZGKD5oBrSW5t"
mov     [ebp+var_8], offset a18ucagbkgcku61 ; "18ucAGbkgCkU61F6yPMD19dZRUBBHyDGRV"
mov     [ebp+var_4], offset a15nzzrpasbgd1m ; "15nzzRpAsbgd1mmoqQRtiXxN49f4LcmTh4"
call    sub_401000
pop     ecx
test    eax, eax
pop     ecx
jz      short locret_401EFD
call    ds:rand
```

Figure 11: Bitcoin Addresses

Using the same Bitcoin addresses for all victims make it impossible for the attacker to know who has paid and who hasn't. This means there is no point of paying the ransom and there is very small chance of getting the decryption key back. The best way to retrieve the files is to restore a system back. However, we have observed that the ransomware also deletes Windows backup files. Which means again to restore system the backup files have to be stored on an external medium.

E. *Command and Control:*

WannaCry make use of Tor network for its C&C communications. In our experiment we have observed that it tries to connect to some hardcoded IP addresses which belong to Tor Hidden Services. A Tor hidden service is website that is only accessible via Tor network and the website operator is an unknown individual. It is known that Tor communications performs over port numbers 443 and 9001.



```
taskhsvc.exe (3572)    WIN-0BUEB7P60PG   53748  85.235.250.88      443  TCP   SYN sent
taskhsvc.exe (3572)    WIN-0BUEB7P60PG   53749  194.109.206.212    443  TCP   SYN sent
taskhsvc.exe (3572)    WIN-0BUEB7P60PG   53803  192.187.124.98    9001  TCP   SYN sent
```

Figure 12: TOR Communications

The purpose of the C&C here is to allow attackers to retrieve some basic information about the victims, e.g. number of infected computers, and ip addresses, in order to measure the impact of the attack.

IV. Motivation

In order to figure out the motivation behind WannaCry let us discuss how the events unfold starting from the beginning of the discovery of the exploit.

A. *Timeline of Events:*

- NSA discovered the vulnerability in SMB protocol and created the EternalBlue exploit
- Shadow Brokers steals NSA tools which includes the EternalBlue code on January 2017 [16]
- Microsoft cancels the February 2017 patch cycle for the first time! [17]
- Microsoft releases the patch for the SMB protocol vulnerability on March 14, 2017 [16]
- Shadow Brokers release the vulnerability on April 14 ,2017 (Exactly after one month of the patch, this suggests that there were some communications between Microsoft and Shadow Brokers) [15]
- WannaCry spread all over the internet on May 12 ,2017. [15]
- The kill switch had been discovered and sink hold (register the domain name to stop the malware) on the same day [15]
- The ransom money in the three bitcoin accounts were withdrawn on August 2 ,2017 (possibly to Bitcoin mixer, money laundering service)
- The US government publicly accused the North Korean government of mounting WannaCry attack on December 19 ,2017 [4]
- The US Justice Department charges Park Jin Hyok, believed to be a high-profile member of the Lazarus group, of launching WannaCry attack on September 6 ,2018 [15]

Based on this timeline of events there are two possibilities behind the WannaCry attack.

B. *MONEY MOTIVE:*

The attackers extorted only $140,000 worth of Bitcoin after infecting more than 200,000 computers by August 2017. This amount of money had been collected via only three bitcoin addresses. Money gained by this attack is considered a failure in terms of ransomwares, and in comparison, with number of computers that had been infected by the malware.

C. *POLITICAL MOTIVE:*

WannaCry attack have been linked to Lazarus group. Lazarus group is a North Korean cybercrime group which believed to be sponsored by the North Korean Government. This group have been accused of mounting several major cyber-attacks including the famous Sony Pictures hacking in 2014, and the $81 million Bangladesh central bank heist in 2016. Semantic and Kaspersky (major information security firms) have found similar pieces of code that had been used in previous attacks. For instance, the wiping tool of WannaCry is the same tool that had been used in the Sony Attack. Additionally, the "FakeTLS" data table which used a custom networking protocol that was designed by the lazarus Group to fake the TLS connection.

On December 2017, the White House has publicly attributed WannaCry attack to North Korea [5]. According to the Department of Justice indictment the officials charges Park Jin Hyok, a North Korean citizen, for the WannaCry attack [15]. He is believed to be a member of the Lazarus group. Park works in Chosun Expo Joint venture which is a government-owned company. The officials used the IP addresses that were used to access the malware command and control servers and hacked the servers that hosted the malware [15]. From there they were able to identify a fake name - Kim Hyon Woo which was linked to the Lazarus group. They eventually tied the connections of this fake person to Park Jun Hyok because of the online accounts that were associated with him [15]. At the end, we have reached to a surprising conclusion that WannaCry is actually a cyberweapon and not just ransomware which means the main goal behind the attack is destruction and not money gain. This is also one of the reasons that makes WannaCry stands out from other malwares.

V. Conclusion

WannaCry is a powerful malware because it combines a worm capability with a ransomware functionality. The worm module of WannaCry had facilitated it's enormous spreading. It can propagate in both the local and the external network of an infected system. In this paper we have investigated the propagation mechanism by experimenting the malware in a controlled environment. Moreover, the ransomware module of WannaCry encrypts victim's data and demands a ransom to decrypt them. In our analysis we have studied the cryptographic model that the ransomware utilized which we found well designed and makes it impossible to recover the decryption key. This due to the fact that it utilizes the speed of the symmetric key cryptography and the convenience of the asymmetric key cryptography. Furthermore, we have studied the motivation behind WannaCry attack which surprisingly was not only money extortion as it has been believed before but actually a nation-sponsored cyber-attack. A few lessons learnt from this attack: updating the system regularly and keeping backup files on an external medium are essential to mitigate the effects of such attacks.

References

[1] "WannaCry ransomware attack," *Wikipedia*. Accessed September 17, 2018. [Online].

[2] "Ransomware," *Wikipedia*. Accessed September 17, 2018. [Online].

[3] A. Hern, S. Gibbs, "What is WannaCry ransomware and why is it attacking global computers?" *The Guardian*, May 12, 2016. [Online].

[4] K. Bossert, "Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea," Whitehouse, December 19, 2017. [Online].

[5] E. Nakashima, "U.S. declares North Korea carried out massive WannaCry cyberattack," *The Washington Post*, Dec 19, 2017. [Online].

[6] K. Savage, P. Coogan, H. Lau, "The evolution of ransomware" 2015.

[7] A. Zimba, L. Simukonda, M. Chishimba "Demystifying Ransomware Attacks: Reverse Engineering and Dynamic Malware Analysis of WannaCry for Network and Information Security" 2017.

[8] P. Bajpai, A. K. Sood, R. Enbody "A Key-Management-Based Taxonomy for Ransomware" 2018.

[9] K. Tapsoba "Ransomware: Offensive Warfare using Cryptography," 2018.

[10] LogRhythm Labs, "A Technical Analysis of WannaCry Ransomware" 2017. [Online].

[11] A.Berry,J.Homan,R.Eitzman. "WannaCry Malware Profile," FireEye, 2017. [Online].

[12] Counter Threat Research Team, "WCry Ransomware Analysis," *Secureworks*, 2017. [Online].

[13] A. Rousseau, "WCry/WanaCry Ransomware Technical Analysis" *Endgame*, 2017. [Online].

[14] D. Brien, "Internet Security Threat Report Ransomware," *Symantec*, 2017. [Online].

[15] C. Cimpanu, "How US authorities tracked down the North Korean hacker behind WannaCry," *ZDNet*, 2018. [Online].

[16] Symantec Security Response, "Ransom. WannaCry," *Symantec*, 2017. [Online].

[17] P. Bright, "Microsoft cancels February Patch Tuesday despite 0-day in wild," Ars Technica, 2017. [Online].