**WannaCry tactical report**

Identification

|  |  |
| --- | --- |
| **Vendor** | **Detection** |
| Symantic | Ransom.Wannacry |
| Kaspersky | Trojan-Ransom.Win32.Wanna.m |
| Microsoft | Ransom:Win32/WannaCrypt |

The following table contains list of artifacts that had been analyzed within this document.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| PE timestamp | Md5 | Size in bytes | Filename | Description |
| 2010/11/20 sat 09:03:08 UTC | db349b97c37d22f5ea1d1841e3c89eb4 | 3723264 | Mssecsvc.exe | Installer |
| 2010/11/20 sat 09:05:05 UTC | 84c82835a5d21bbcf75a61706d8ab549 | 3514368 | Tasksche.exe | Loader + connection to attacker ip |
| 2009/07/13 Mon 23:19:35 UTC. | 7bf2b57f2a205768755c07f238fb32cc | 43906 | @WanaDecryptor@.exe | Decryptor |
| 2009-07-14 Tue 01:12:55 UTC | f351e1fcca0c4ea05fc44d15a17f8b36 | 65536 | Unavailable.exe | Encryptor component |

**Prevalence:-**

Ransomware called WannaCry spreads to many countries. It affects telecommunications, manufacturers, hospital and companies. It demands a payment of $300 bitcoins to specific address .it is also composed of multiple components. The First component is dropper that contains encryption, Zip file that contains main functionality of Ransomware, WannaDecryptor and other files. The reason of rapid spread of ransomware is exploiting vulnerability in the protocol called windows server message block (SMBv1).The exploit is known as “Eternal Blue “which developed by the group who called shadow brokers. Microsoft provides a patch for their operating systems that prevents WannaCry.

Figure (2)

As shown in figure (2), the most affected countries were Russia, Ukraine, India and Taiwan.

**Infection vector**

* Exploitation kit

**Exploitation kits**

|  |  |
| --- | --- |
| **CVE** | **Exploit description** |
| CVE-2017-0143 | Remote code execution |
| CVE-2017-0144 | Remote code execution |
| CVE-2017-0145 | Remote code execution |
| CVE-2017-0146 | Remote code execution |
| CVE-2017-0147 | Remote code execution |
| CVE-2017-0148 | Remote code execution |

Wannacry is self-propagation ransomware because it uses exploit called MS17-010 which infected other machine in the network. First it determines the subnet mask of infected machine. It generates random ips belong to the same subnet then tries to connect to these ips using port 445 if it succeed it will use this vulnerability to infected connected machine.

You can know more information about this payload using this link: - <https://arstechnica.com/information-technology/2017/04/nsa-leaking-shadow-brokers-just-dumped-its-most-damaging-release-yet/>

**Auto-Sandboxing:-**

* Initial check
* Reason

**Initial check**

WannaCry starts to connect to this URL [www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com](http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com) if successful connection occurs then ransomware will not affect the machine. Otherwise it affects the machine.

**Reason**

Ranosmaware makes initial check to prevent auto sandboxing technique that most antivirus programs use it.

**Installer**

|  |  |
| --- | --- |
| FileName | mssecsvc |
| PE timestap | 2010/11/20 sat 09:03:08 UTC |
| MD5 | db349b97c37d22f5ea1d1841e3c89eb4 |
| SHA256 | 24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c |
| Size | 3723264 |
| Purpose | Installer+Dropper |

**Initial Infection and propagation:**

1. As shown in figure (3) ransomware starts to connect to this URL <http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com> if successful connection occurs then ransomware will not affect the machine. Otherwise it affects the machine. There are other URLs in other samples that make malware will not affect machine. The reason of making initial check is to prevent auto sandbox from detecting Ransomware.

****

Figure(3)

**Note:-**

There are other URLs that ransomware connect to.

|  |  |
| --- | --- |
| **URL** | **SHA256** |
| www.iuqssfsodp9ifjaposdfjhgosurijfaewrwergwea.com | 7b7aa67a3d47cb39d46ed556b220a7a55e357d2a9759f0c1dcbacc72735aabb1 |
| www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.testing | 7b7aa67a3d47cb39d46ed556b220a7a55e357d2a9759f0c1dcbacc72735aabb1 |

**Http Request:-**



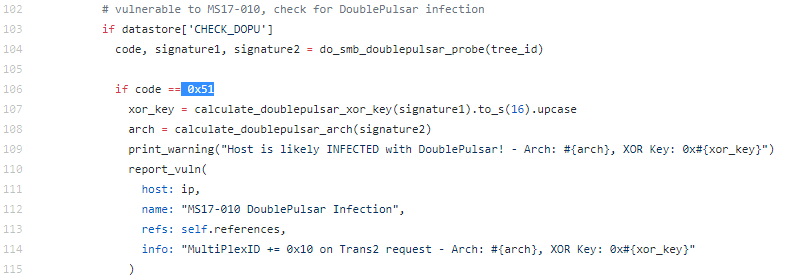
1. It gets module file name which is mssecsvc2.0 then creates service called “mssecsvc2.0 “.and starts the service.

|  |  |  |  |
| --- | --- | --- | --- |
| **Action** | **Registry key** | **Service name** | **Display name** |
| create | HKLM\Software\WanaCrypt0r\wd | mssecsvc2.0 | Microsoft Security Center (2.0) Service |
| create | HKLU\Software\WanaCrypt0r\wd | mssecsvc2.0 | Microsoft Security Center (2.0) Service |



1. It Starts service control Dispatcher which actually executes (SMB Exploit )
2. It gets ips, connects to port 445 (SMB) and execute shell code.

As shown in figure if the value == 0x51 then successful payload.

Figure (4)

As shown in figure (5) the Value in ida pro.

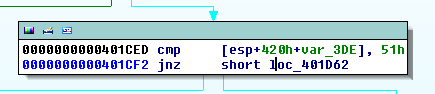


Figure (5)

It checks for value equal to 0x51. This value represents Multiplex ID.

* If Multiplex\_ID = 0x51 then host is vulnerable.
* If Multiplex\_ID = 0x41 then host is not vulnerable.

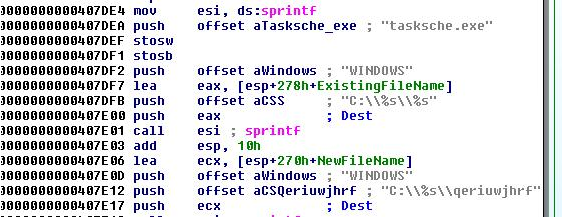
**Payload:**

Wannacry is self-propagation ransomware because it uses exploitation called MS17-010 which infects other machines in the same network.

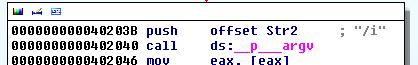
* It determines the subnet mask of infected machine.
* It generates random ips belong to the same subnet then try to connect to these ips using port 445.
* If successful connection occurs, it will use this vulnerability to infect connected machines.  
  Once the malware find NetBIOS opened, it sends 3 packets. One of these packets is the ip address of victim and the others are hardcoded two ip addresses (172.16.99.5 and 192.168.56.20).

You can know more information about this payload using this link <https://arstechnica.com/information-technology/2017/04/nsa-leaking-shadow-brokers-just-dumped-its-most-damaging-release-yet/>

After creating service mssecsvc2 and starting service it unlocks (R) resource in memory and puts it to file tasksch.exe.



**Run with Command:**

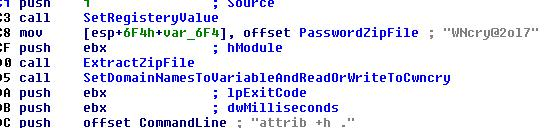
****

* It pushes (/I) argument to copy the tasksche.exe to the [\\ProgramData](file:///\\ProgramData) .
* If it exists it will copy it to [\\Intel](file:///\\Intel) .
* It creates service tasksche and starts it with option autostart.

|  |  |  |  |
| --- | --- | --- | --- |
| **Action** | **Registry key** | **Service name** | **Display name** |
| Create | HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\*Random* | tasksche | Random |
| Create | HKCL\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\*Random* | tasksche | Random |

* It creates mutex called Global\\MsWinZonesCacheCounterMutexA.
* If it failed to create mutex then it executes tasksche.exe without (I) argument.

**Run without command**

****

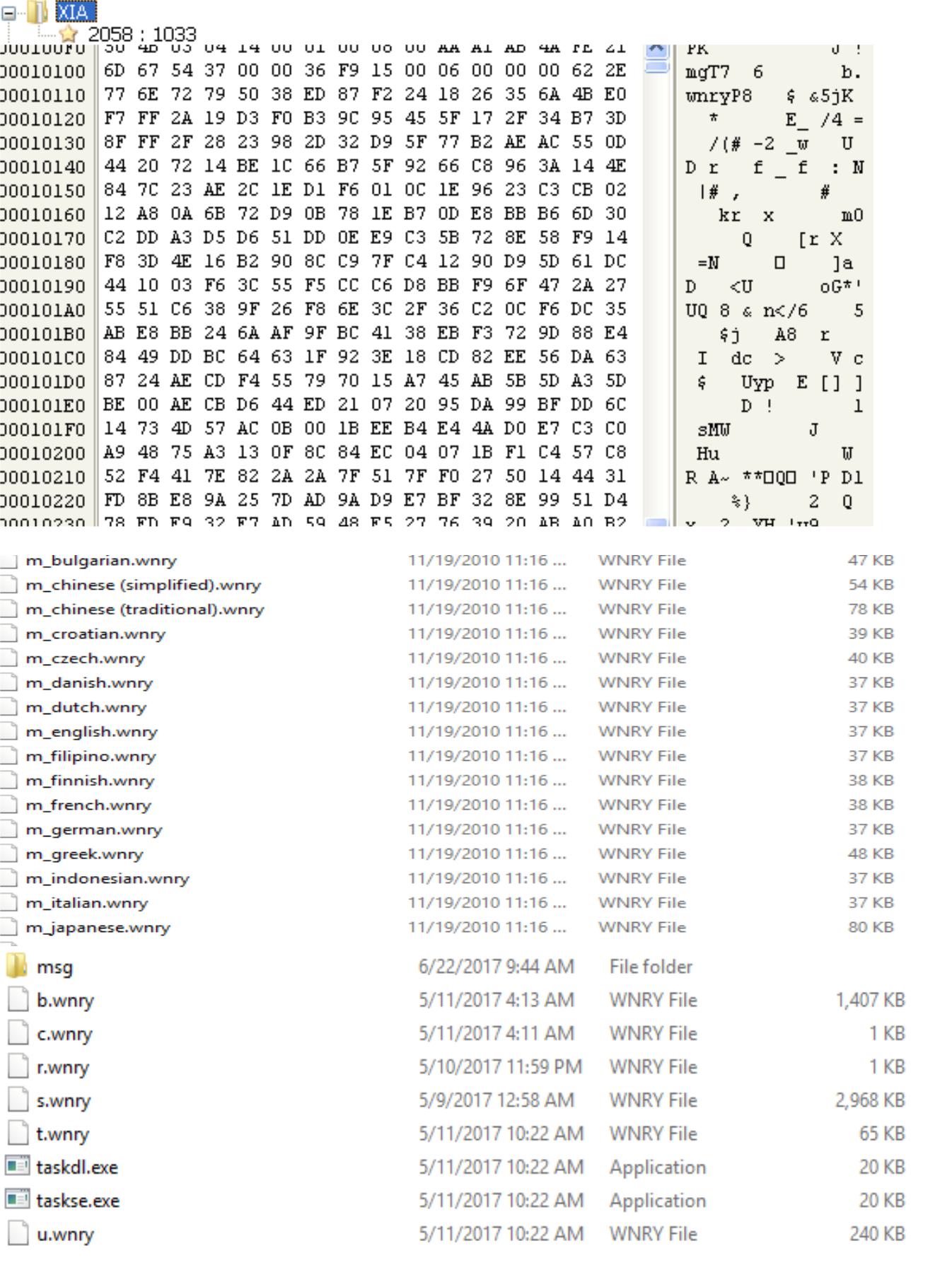
* It unlocks resource “XIA” and extracts zip file with password “WNcry@2ol7”.
* It opens file c.wnry. Then chooses from these 3 strings and writes to c.wncry file.

(1)-13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94.

(2)-12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw.

(3)-115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn.

* It executes command called attrib +h to hide directory of current path.
* It executes command "icacls. /grant everyone /T /C /Q” to give permission to all user for accessing current directory.

**Resource(R):-**

There is a resource called “XIA” you have to convert it to bin using resource hacker tool then extract zip file with password “WNcry@2ol7” and analysis each file.

**Dropped Files in XIA Resource:**

|  |  |  |  |
| --- | --- | --- | --- |
| **File Name** | **Path** | **MD5** | **Description** |
| b.wnry | current path of extraction of zip file | 4B613667DA96605ABC1173EDFB119C42 | Ransomware Image |
| c.wnry | current path of extraction zip file | AE08F79A0D800B82FCBE1B43CDBDBEFC | Configuration File Connection To server And Download Tor browser |
| r.wnry | current path of extraction zip file | 3E0020FC529B1C2A061016DD2469BA96 | words of Ransomware in view |
| s.wnry | current path of extraction zip | AD4C9DE7C8C40813F200BA1C2FA33083 | Zip File Contain Tor Browser |
| t.wnry | current path of extraction zip file | 5DCAAC857E695A65F5C3EF1441A73A8F | Encryption Tool |
| taskdl.exe | current path of extraction zip file | 4FEF5E34143E646DBF9907C4374276F5 | used for delete Temporary Files |
| taskse.exe | current path of extraction zip file | 8495400F199AC77853C53B5A3F278F3E | Support Decryption Tool |
| u.wnry | current path of extraction zip file | 7BF2B57F2A205768755C07F238FB32CC | Decryption Tool |

**Languages Files:**

|  |  |
| --- | --- |
| **File Name** | **MD5** |
| m\_bulgarian.wnry | 95673b0f968c0f55b32204361940d184 |
| m\_chinese (simplified) | 0252d45ca21c8e43c9742285c48e91ad |
| m\_chinese (traditional).wnry | 2efc3690d67cd073a9406a25005f7cea |
| m\_czech.wnry | 537efeecdfa94cc421e58fd82a58ba9e |
| m\_danish.wnry | 2c5a3b81d5c4715b7bea01033367fcb5 |
| m\_dutch.wnry | 7a8d499407c6a647c03c4471a67eaad7 |
| m\_english.wnry | fe68c2dc0d2419b38f44d83f2fcf232e |
| m\_filipino.wnry | 08b9e69b57e4c9b966664f8e1c27ab09 |
| m\_finnish.wnry | 35c2f97eea8819b1caebd23fee732d8f |
| m\_french.wnry | 4e57113a6bf6b88fdd32782a4a381274 |
| m\_german.wnry | 3d59bbb5553fe03a89f817819540f469 |
| m\_greek.wnry | fb4e8718fea95bb7479727fde80cb424 |
| m\_indonesian.wnry | 3788f91c694dfc48e12417ce93356b0f |
| m\_italian.wnry | 30a200f78498990095b36f574b6e8690 |
| m\_japanese.wnry | b77e1221f7ecd0b5d696cb66cda1609e |
| m\_korean.wnry | 6735cb43fe44832b061eeb3f5956b099 |
| m\_latvian.wnry | c33afb4ecc04ee1bcc6975bea49abe40 |
| m\_norwegian.wnry | ff70cc7c00951084175d12128ce02399 |
| m\_polish.wnry | e79d7f2833a9c2e2553c7fe04a1b63f4 |
| m\_portuguese.wnry | fa948f7d8dfb21ceddd6794f2d56b44f |
| m\_romanian.wnry | 313e0ececd24f4fa1504118a11bc7986 |
| m\_russian.wnry | 452615db2336d60af7e2057481e4cab5 |
| m\_slovak.wnry | c911aba4ab1da6c28cf86338ab2ab6cc |
| m\_spanish.wnry | 8d61648d34cba8ae9d1e2a219019add1 |
| m\_turkish.wnry | 531ba6b1a5460fc9446946f91cc8c94b |
| m\_vietnamese.wnry | 8419be28a0dcec3f55823620922b00fa |

It searches for specific type of file to encrypt as shown in table.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| doc | .docx | .docb | .docm | .dot | .dotm | .dotx | .xls | .xlsx | .xlsm |
| .xlsb | .xlw | .xlt | .xlm | .xlc | .xltx | .xltm | .ppt | .pptx | .pptm |
| .pot | .pps | .ppsm | .ppsx | .ppam | .potx | .potm | .pst | .ost | .msg |
| .eml | .edb | .vsd | .vsdx | .txt | .csv | .rtf | .123 | .wks | .wk1 |
| .pdf | .dwg | .onetoc | .snt | .hwp | .602 | .sxi | .sti | .sldx | .sldm |
| .vdi | .vmdk | .vmx | .gpg | .aes | .ARC | .PAQ | .bz2 | .tbk | .bak |
| .tgz | .gz | .7z | .rar | .zip | .backup | .iso | .vcd | .jpeg | .jpg |
| .bmp | .png | .gif | .raw | .cgm | .tif | .tiff | .nef | .psd | .ai |
| .svg | .djvu | .m4u | .m3u | .mid | .wma | .flv | .3g2 | .mkv | .3gp |
| .mp4 | .mov | .avi | .asf | .mpeg | .vob | .mpg | .wmv | .fla | .swf |
| .wav | .mp3 | .sh | .class | .jar | .java | .rb | .asp | .php | .jsp |
| .brd | .sch | .dch | .dip | .pl | .vb | .vbs | .ps1 | .bat | .cmd |
| .js | .asm | .h | .pas | .cpp | .c | .cs | .suo | .sln | .ldf |
| .mdf | .ibd | .myi | .myd | .frm | .odb | .dbf | .db | .mdb | .accdb |
| .sql | .sqlitedb | .sqlite3 | .asc | .lay6 | .lay | .mml | .sxm | .otg | .odg |
| .uop | .std | .sxd | .otp | .odp | .wb2 | .slk | .dif | .stc | .sxc |
| .ots | .ods | .3dm | .max | .3ds | .uot | .stw | .sxw | .ott | .odt |
| .pem | .p12 | .csr | .crt | .key | .pfx | .der |

It skips some types of files:-

* exe
* dll
* wncry

It also neglects the folders with the following names:-

* Intel
* Program Data
* WINDOWS
* Program Files
* Program Files (x86)
* AppData\\Local\\Temp
* Local Settings\\Temp
* This folder protects against ransomware. Modifying it w reduce protection
* Temporary Internet Files
* Content.IE5

**Encryption:-**

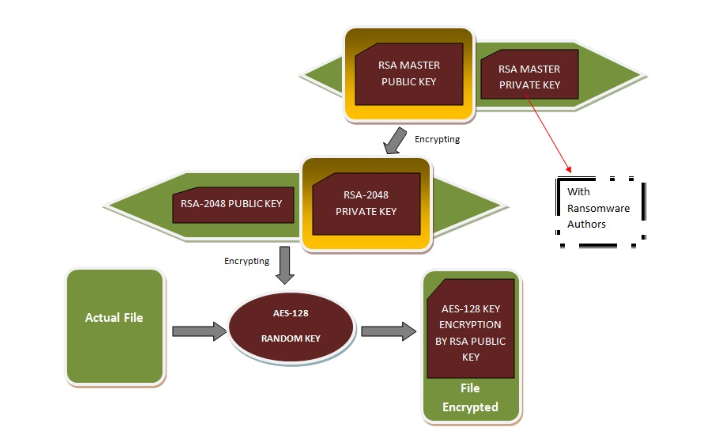
Wannacry has a combination of RSA and AES. It generates random key, then encrypts target files and any drive that could attach to victim machine. We cannot identify the flow of cryptographic implementation so file recovery decryption may not be possible. Every target file encrypts with wannacry added to file extension so if the name of file is example.txt so the new name will be example.txt.wncry then delete the original file and save the modified file to its current directory.

* **Encryption Files**
* **Graphical representation**
* **Overview of encryption**
* **Technical analysis of encryption**

**Encryption Files**:-

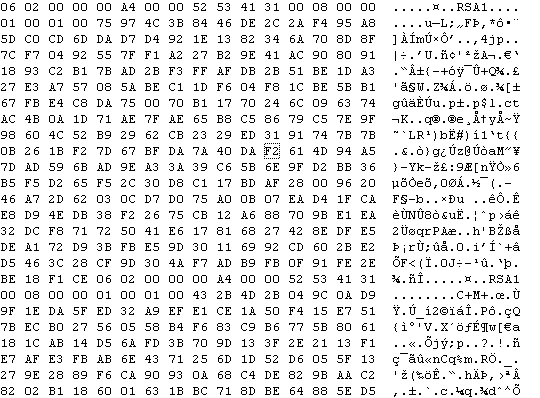
|  |  |  |
| --- | --- | --- |
| **File Name** | **MD5** | **Description** |
| 00000000.res | 58F33FCB1B73E2800EC614B9F1F76569 | C&C |
| 00000000.pky | 53DDD4291EE50BC74AD9D64312E1D0CC | Public key |
| 00000000.eky | 53DDD4291EE50BC74AD9D64312E1D0CC | private key |

**Graphical representation**:-

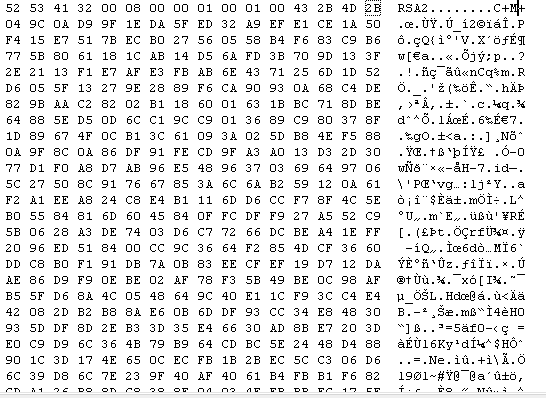


**Overview of encryption**: - .

* Ransomware has two hardcoded public keys existed in malware.
* The First key is used for encryption all files.
* The Second key is used for encryption small number of specific files which are used for demo decryption.
* Once ransomware infects machine then it generates new RSA key this means that each machine needs unique key for decryption.
* It generates key using CryptGenRandom API.
* Once generates new public key then exports to local file 00000000.pky using CryptExportKey API. ( public key )
* Then encrypts generated RSA public key with attacker public key and saves it to file 00000000.eky so this is (private key).
* It uses CryptoDestroyKey API to destroy the private key in memory so you couldn't get private key well.
* If the original file size is less than 209,715,200 bytes then it uses demo RSA Public key.



(Public Key)



(Private Key)

**Technical analysis of Encryption**:-

* It searches for file c.wncry which includes tor browser and bitcoin addresses.
* These following addresses are used for payment :-

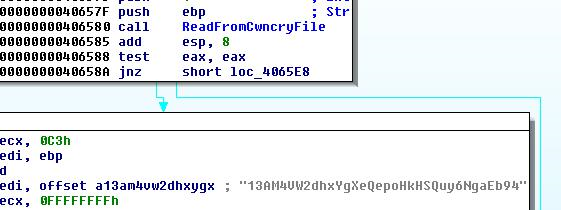
|  |
| --- |
| 13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94 |
| 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw |
| 115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn |

As shown in figure (5) to make decryption of files you need to send $300 to this address.

|  |
| --- |
| 115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn |



Figure (5)



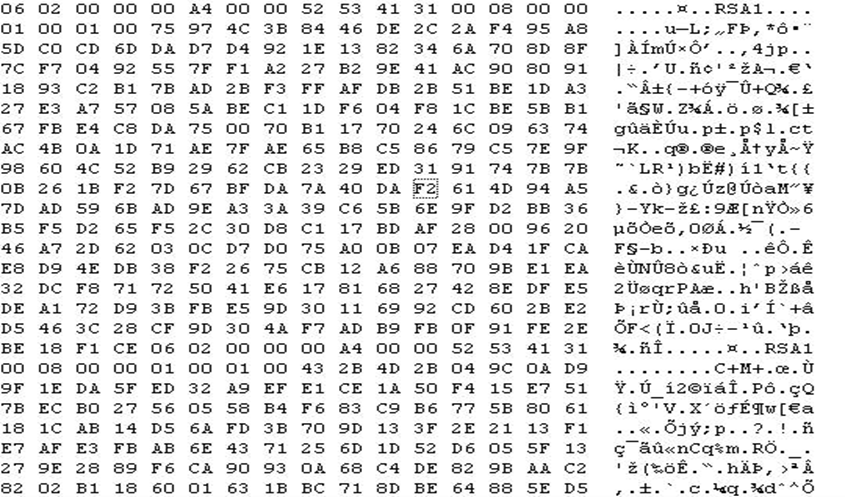
(Assembly code in Ida Pro)

* Then extract tor browser and onion sites which is used for communication.

**Onion sites**

|  |
| --- |
| gx7ekbenv2ri ucmf .onion |
| 57g7s pgrzlojinas.onion |
| xxlvbrloxvriy2 c5.onion |
| 76jdd2i r2embyv47.onion |
| cwwnhwhlz52maqm7 .onion |

* It opens the file c.wncry.
* It Reads 780 bytes from c.wncry File and closes it.
* It creates names of these files res, eky, and pky.
* It creates mutex called MsWinZonesCacheCounterMutexW.



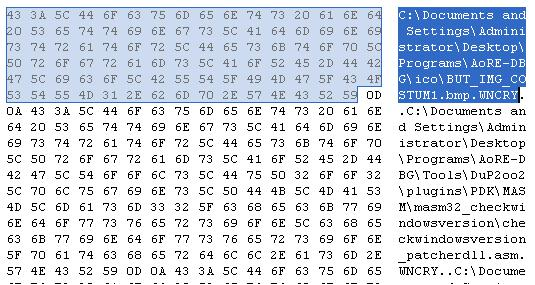
(Public key)

* The key above is used to encrypt the target files.
* It adds the extension .wncry or wncryt to the end of each encrypted file.
* Every encrypted file starts with string WANACRY! To define this file is encrypted or not.
* It executes a thread that writes every 25 seconds current time of system to file res.
* It also creates a thread that scan every 3 second for new driver can attach to system if successful it starts to encrypt new drive.
* It executes this command “attrib +h + s +” Drive Name +$RECYCLE to create new directory.

**Update f.wncy**

|  |  |  |
| --- | --- | --- |
| **File name** | **MD5** | **Description** |
| F.wncry | 8A503D10E60D40702C34541E5885296D | Save path of randomly encrypted file. |

* It encrypts small number of files with key stored in malware and these files used for demo decryption.



Ransomware creates registry key using this command:-

'cmd.exe /c reg add %s /v "%s" /t REG\_SZ /d "\"%s\"" /f’.

* It executes file WannaDecryptor.exe with argument Fi as shown in figure (6).
* Updates file c.wncry with current time.
* Copies file u.wncry to location of WannaDecryptor file.

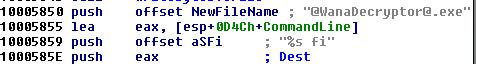


Figure (6)

It copies WannaDecrupto.exe file and executes script file to create @WanaDecryptor@.exe.lnk as shown in script (2).

**Script File:**

@echo off  
echo SET ow = WScript.CreateObject ("WScript.Shell")> m.vbs echo SET om = ow.CreateShortcut ("%s%s")>> m.vbs echo om.TargetPath = "%s%s">> m.vbs  
echo om.Save>> m.vbs  
cscript.exe //nologo m.vbs  
del m.vbs

The script above is used for copying files, deleting and creating shortcut by pushing File name.

**Script (2)**

@echo off

echo SET ow = WScript.CreateObject ("WScript.Shell")> m.vbs echo SET om = ow.CreateShortcut ("Path \@WanaDecryptor@.exe.lnk ")>> m.vbs echo om.TargetPath = " Path \@WanaDecryptor@.exe.lnk ">> m.vbs

echo om.Save>> m.vbs

cscript.exe //nologo m.vbs  
del m.vbs.

* When ransomware completes encryption of desktop it executes following command to terminate some services because the data stored in these services will be encrypted.

|  |
| --- |
| **taskkill.exe /f /im mysqld.exe** |
| **taskkill.exe /f /im sqlwriter.exe** |
| **taskkill.exe /f /im sqlserver.exe** |
| **taskkill.exe /f /im MSExchange** |
| **taskkill.exe /f /im Microsoft.Exchange** |

* It copies file r.wncry and WanaDecryptor to every directory that ransomware makes encryption.
* The file will be the instruction of what happened and how to pay.
* It always shows this view as shown in figure (7).
* It copies b.wncry image and put it as desktop image.

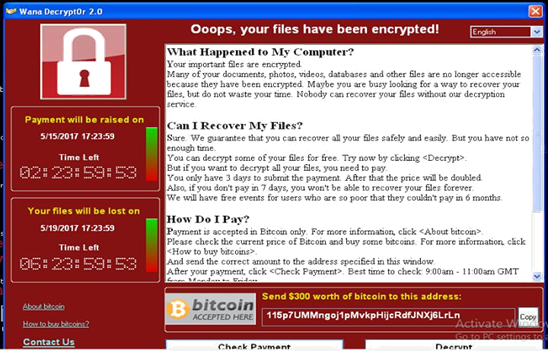
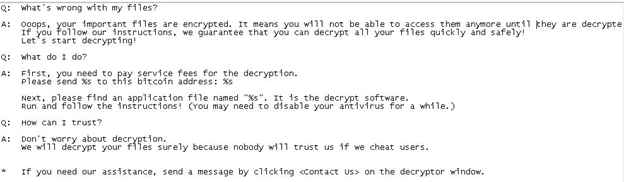


Figure (7)



b.wncry

**Additional URLs:-**

* https://www.google.com/search?q=how+to+buy+bitcoin
* http://www.btcfrog.com/qr/bitcoinpng.php?address
* https://en.wikipedia.org/wiki/Bitcoin

These links above are embedded into ransomware file and explain what bitcion is and how to buy bitcoin.

**Decryption:**-

* **Decryption possible?**
* **Overview of decryption**

**Decryption possible?**

Can we decrypt files of wannacry?   
It’s impossible to decrypt files of wannacry.

**Reason:**

This ransoware uses public and private key for encryption and decryption.

* It generates new key in your pc.
* It encrypts new private key with the original public key then move it to hacker server.
* It uses new public key to encrypt documents and pictures.
* It uses unique key for each pc to prevent sharing decryption key.

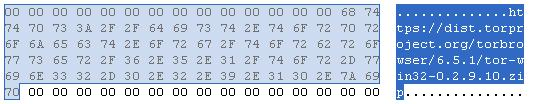
**So if you have public key you can decrypt file?**

* Answer no because having the public key is not enough. You need the matching private key that the hacker is holding.

**Overview of decryption:**-

|  |  |  |
| --- | --- | --- |
| **File Name** | **MD5** | **Description** |
| c.wncry | AE08F79A0D800B82FCBE1B43CDBDBEFC | Zip File that contains Configuration File Connection To server And Download Tor browser. |
| @WanaDecryptor@.exe | 7bf2b57f2a205768755c07f238fb32cc | Decryptor |

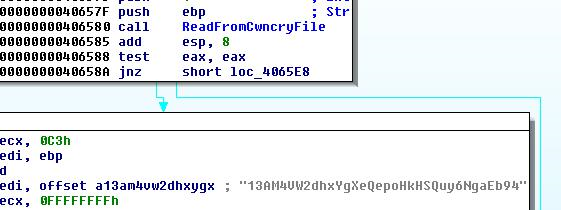
It extracts content of c.wncry zip file especially tor browser then connect to 127.0.0.1 using port 9050.



(Content of c.wncry)

* Ransomware registers machine with onion server.
* It transfers private key of the victim.
* If the victim pays ransom then he could obtain decryption key from onion server and decrypt files.
* It opens c.wncry and reads 780 bytes from it.
* If file doesn’t exist it will create file c.wncry then get actual time of system and write time and this string to file.

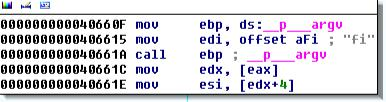
|  |
| --- |
| 13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94 |



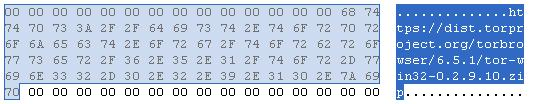
**Important commands:**-

|  |  |
| --- | --- |
| **Command** | **Description** |
| **Fi** | Connect to onion server |
| **Co** | initial check with ransomware server |
| **Vs** | Delete volume shadow copy |
| **No command** | Display Decryption Window |

Fi Command:

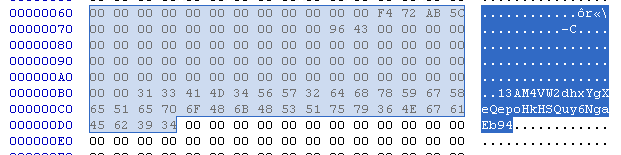


* It checks for command fi if true then it reads 136 bytes from 00000000.res file.
* It reads the content of file c.wncry especially tor browser then connects to 127.0.0.1 using port 9050.

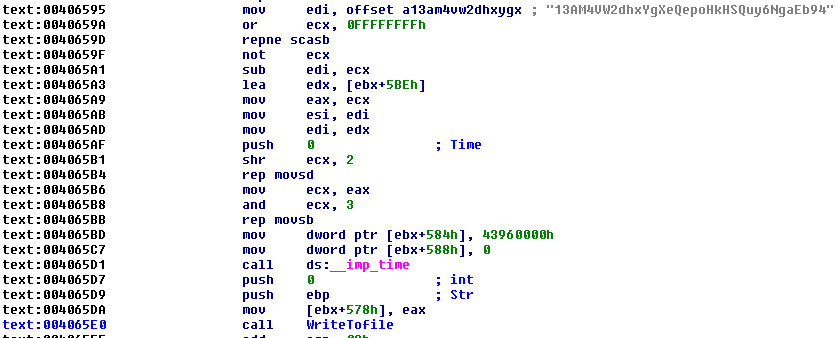


(Content of c.wncry if it exists)

* If c.wncry doesn’t exist it will create content shown in figure.



(Content of c.wncry if it’s not exists)

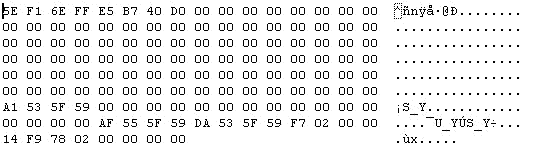


(Assembly code)

* The value at offset (0x5CAB72F4) in the figure below refers to timestamp of creation file.
* The string 13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94 below is used for connection to onion server.
* It searches for directory TaskData\Tor\tor.exe
* It executes tor.exe and connects to one of onion servers.
* **Onion sites**

|  |
| --- |
| gx7ekbenv2ri ucmf .onion |
| 57g7s pgrzlojinas.onion |
| xxlvbrloxvriy2 c5.onion |
| 76jdd2i r2embyv47.onion |
| cwwnhwhlz52maqm7 .onion |

* it opens file 00000000.res to read 8 bytes from file 00000000.res



(00000000.res content)

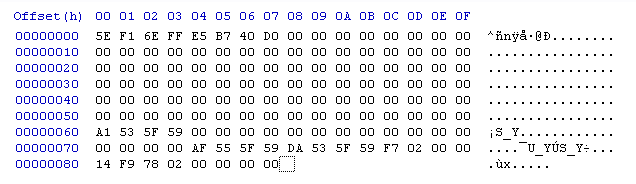
* It pushes string ‘+++’ and gets username then sends this information to server.

**C&C message**

|  |
| --- |
| < 8 bytes res file > < hostname > < username > <string +++ > |

Co command:-

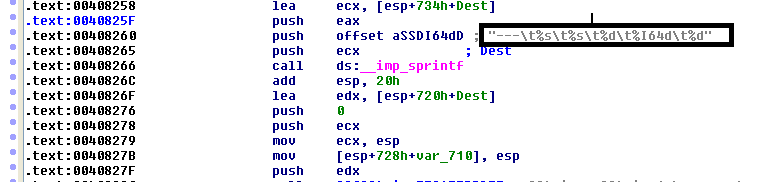
* First It checks for command Co
* It searches for file 00000000.res and read data of it.
* It sends a massage to onion server.



(Content of res file)

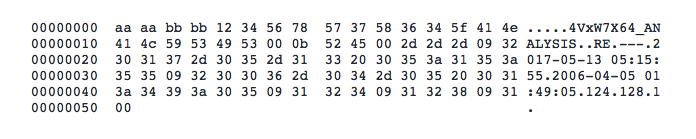
Format of massage

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| --- | Time\_0 | Time\_1 | Unknown integer | Unknown long | Index |



(Format of massage in ida pro)

|  |  |
| --- | --- |
| Value | Description |
| --- | String to identify command |
| Time\_0 | Time obtained from offset 0x60 |
| Time\_1 | Time obtained from offset 0x78 |
| Unknown integer | Integer obtained from offset 0x7c |
| Unknown long | Integer obtained from offset 0x80 |
| Index | Count of the current file when scanning for files in the format <8\_Uppercase\_Hex>.res |



Message

Vs command:-

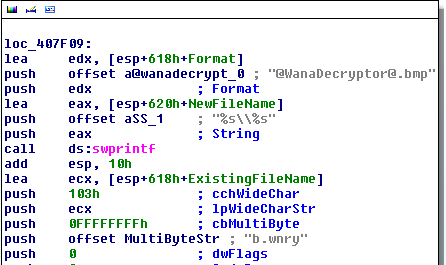


* Ransomware checks for arguments vs if true it deletes volume shadow copy using this command and sleeps for 10 seconds.

|  |
| --- |
| /c vssadmin delete shadows /all /quiet & wmic shadowcopy delete &bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcde dit /set {default} recoveryenabled no & wbadmin delete catalog –q uiet vs |

The reason for this command is to disable data recovery.

No command:-

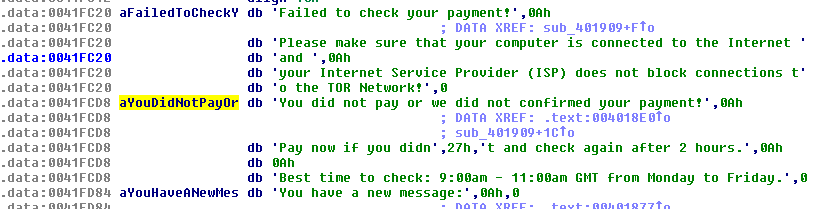


If there is no argument then it copies b.wncry and @WanaDecryptor@.bmp to desktop and executes them.



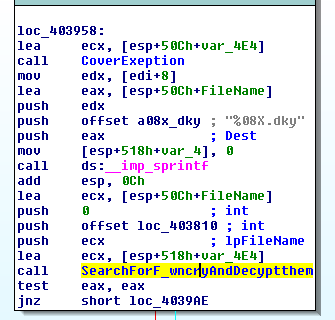
You will receive one of these messages box from server if you pay or try to contact them.

|  |
| --- |
| Congratulations! Your payment has been checked! |
| Start decrypting now |
| Failed to check your payment! |
| Please make sure that your computer is connected to the Internet |
| your Internet Service Provider (ISP) does not block connections to the TOR Network! |
| You did not pay or we did not confirmed your payment! |
| Pay now if you didn',27h,'t and check again after 2 hours |
| Best time to check: 9:00am - 11:00am GMT from Monday to Friday |
| You have a new message : |
| Please select a host to decrypt |
| All your files have been decrypted! |
| Pay now, if you want to decrypt ALL your files! |
| Failed to send your message! |
| Please make sure that your computer is connected to the Internet |
| Your message has been sent successfully! |
| You are sending too many mails! Please try again %d minutes later |
| Too short message! |



(Ida pro assembly code)

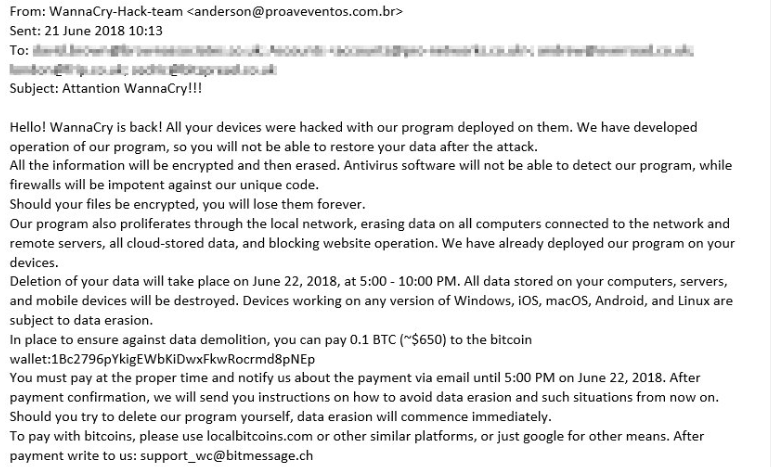
When clicking decrypt button without pay ransom it will decrypt paths stored in file f.wncry with embedded key.



**Spam Email**

* Scam message
* Spam email address

Scam message:-



This is an email that needs you to pay around $650, when you pay then ransomware will be deleted from your machine otherwise the files will be encrypted.

Spam email address:-

This is the list of sender email addresses that sends word document infected with ransomware wannacry.

|  |
| --- |
| alertair@serviciobancomer.com |
| notificacionbcom@serviciobancomer.com |
| alertatdu@serviciobancomer.com |
| notificacionnetcash@serviciobancomer.com |

**Conclusion**:-

WannaCry is type of ransomware family that spread quickly using exploits of SMBv1.

CTU Researchers recommend some rules to mitigate the thread.

* Apply the Microsoft security updates for MS17-010, including the updates for the Windows XP and Windows Server 2003 legacy operating systems.
* Disable SMBv1 on systems where it is not necessary (e.g., hosts that do not need to communicate with Windows XP and Windows 2000 systems). Carefully evaluate the need for allowing SMBv1-capable systems on interconnected networks compared to the associated risks.
* Segment networks to isolate hosts that cannot be patched, and block SMBv1 from traversing those networks.
* Scan networks for the presence of the DoublePulsar backdoor using plugins for tools such as Nmap.
* Use network auditing tools to scan networks for hosts that are vulnerable to the vulnerabilities described in MS17-010.
* Filter emails containing potentially dangerous file types such as executable, scripts, or macro-enabled documents.
* Implement a backup strategy that includes storing data using offline backup media. Backups to locally connected, network-attached, or cloud-based storage are often insufficient because ransomware frequently accesses and encrypts files stored on these systems.

**Yara Rules:**

/\*

Yara Rule Set

Author: Mahmoud Elmenshawy

Date:2019-05-1

Identifier: WannaCry

\*/

private rule IsPE

{

condition:

// MZ signature at offset 0 and ...

uint16(0) == 0x5A4D and

// ... PE signature at offset stored in MZ header at 0x3C

uint32(uint32(0x3C)) == 0x00004550

}

rule WannaCry\_Ransomware {

meta:

Author = "Mahmoud Elmenshawy"

Description = " WannaCry Rule "

Hash="ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa"

strings:

$x2 = "115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn"

$x3 = "12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw"

$x4 = "13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94"

$x5 = "Global\\MsWinZonesCacheCounterMutexA"

$x6 = "tasksche.exe"

$x7 = "icacls . /grant Everyone:F /T /C /Q"

$x8 = "WNcry@2ol7"

$x9 = "msg/m\_english.wnryF"

$x10 = "Microsoft Enhanced RSA and AES Cryptographic Provider"

$x11 = "Global\\MsWinZonesCacheCounterMutex"

$x12 = "XIA"

$x13 = "unzip 0.15 Copyright 1998 Gilles"

condition:

3 of them and IsPE

}

/\*

Yara Rule Set

Author: Mahmoud Elmenshawy

Date:2019-05-1

Identifier: WannaCry

This rule to detect file mssecsvc.exe

\*/

private rule IsPE

{

condition:

// MZ signature at offset 0 and ...

uint16(0) == 0x5A4D and

// ... PE signature at offset stored in MZ header at 0x3C

uint32(uint32(0x3C)) == 0x00004550

}

rule WannaCry\_Ransomware {

meta:

Author = "Mahmoud Elmenshawy"

Description = " WannaCry Rule "

hash ="24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c"

strings:

$x1 = "PlayGame"

$x2 = "mssecsvc.exe"

$x3 = "SMBr"

$x4 = "PC NETWORK PROGRAM 1.0"

$x5 = "LANMAN1.0"

$x6 = "\_\_USERID\_\_PLACEHOLDER\_\_@"

$x7 = "\_\_USERID\_\_PLACEHOLDER\_\_@"

$x8 = "SMB3"

$x9 = "\_\_TREEPATH\_REPLACE\_\_"

$x10 = "\\%s\\IPC$"

$x11 = "mssecsvc2.0"

$x12 = "%s -m security"

$x13 = "tasksche.exe"

$x14 =” <http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com>”

condition:

3 of them and IsPE

}

/\*

This rule to detect file UnAvialbe.exe

this file used for encryption commponent

\*/

private rule IsPE

{condition:

// MZ signature at offset 0 and ...

uint16(0) == 0x5A4D and

// ... PE signature at offset stored in MZ header at 0x3C

uint32(uint32(0x3C)) == 0x00004550}

rule WannaCry\_Ransomware {

meta:

Author = "Mahmoud Elmenshawy"

Description = " WannaCry Rule for detecting Encryption File and script file "

hash = "f351e1fcca0c4ea05fc44d15a17f8b36"

strings:

$x1 = "kgptbeilcq"

$x2 = "TaskStart"

$x3 = "c.wnry"

$x4 = "ConvertSidToStringSidW"

$x5 = "WANACRY!"

$x6 = "RSA1"

$x7 = "Microsoft Enhanced RSA and AES Cryptographic Provider"

$x8 = "MsWinZonesCacheCounterMutexA"

$x9 = "Global\\MsWinZonesCacheCounterMutexW"

$x10 = "taskse.exe"

$x11 = "@WanaDecryptor@.exe"

$x12 = "tasksche.exe"

$x13 = "@WanaDecryptor@.exe.lnk"

$x15 = "cscript.exe //nologo m.vbs"

$x16 = "echo om.Save>> m.vbs"

$x17 = "$%d worth of bitcoin"

$x18 = "attrib +h +s %C:\\%s"

$x19 = "cmd.exe /c start /b %s vs"

$x20 = "%s co"

$x21 = "%08X.eky"

$x22 = "%08X.pky"

$x23 = "%08X.res"

Condition :

3 of them and IsPE

}

/\*

Yara Rule Set

Author: Mahmoud Elmenshawy

Date:2019-05-1

Identifier: WannaCry

This rule to detect file @WanaDecryptor@

\*/

private rule IsPE

{

condition:

// MZ signature at offset 0 and ...

uint16(0) == 0x5A4D and

// ... PE signature at offset stored in MZ header at 0x3C

uint32(uint32(0x3C)) == 0x00004550

}

rule WannaCry\_Ransomware {

meta:

Author = "Mahmoud Elmenshawy"

Description = " WannaCry Rule for detecting Decryption "

hash = "7bf2b57f2a205768755c07f238fb32cc"

strings:

$x1 = "Connecting to server..."

$x2 = "Connected"

$x3 = "Sent request"

$x4 = "Succeed"

$x5 = "You have a new message:"

$x6 = "%04d-%02d-%02d %02d:%02d:%02d"

$x7 = "'Please select a host to decrypt."

$x8 = "Your message has been sent successfully!"

$x9 = "tor.exe"

condition:

3 of them and IsPE

}

**References:**

* https://www.symantec.com/connect/blogs/what-you-need-know-about-wannacry-ransomware
* http://news.softpedia.com/news/wannacry-ransomware-spread-halted-by-hero-researcher-515690.shtml
* https://securingtomorrow.mcafee.com/executive-perspectives/analysis-wannacry-ransomware-outbreak/