Wanna Cry Ransomware: Analysis Infection of MS17-010 After Update, Recovery Prevention and Propagation Mechanisms

Dhruv Pal Singh

Department of Cyber security
Rajiv Gandhi Proudyogiki Vishwavidyalaya
Bhopal, India

***Abstract*– We are observing a WannaCry ransomware is infected system if getting run in a particular system but myself not identify other shared system is infected or not infected after update patch MS17-010 & SMB version 2.0. if infected system is access other pc files & share folder what would be affected or not getting any effect by WannaCry ransomware currently infected system.**

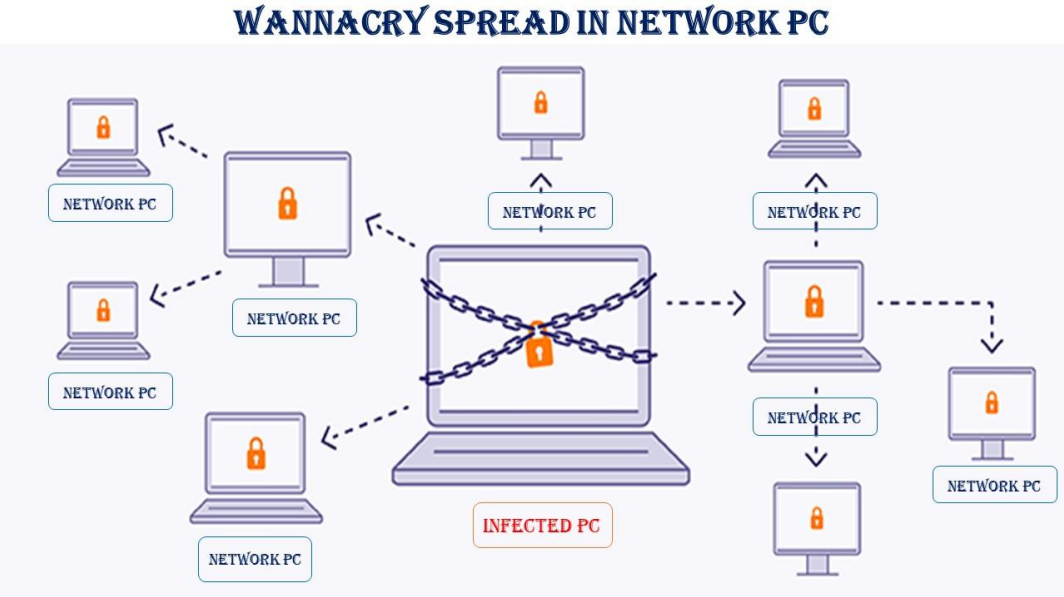
***Keywords*- WannaCry Ransomware, Encryption, Task analysis, Recovery Tools,**

1. INTRODUCTION

Wannacry is the ransomeware worm that rapidly throw across the number of computer in network in may 2017. After infected the systems windows, it encrypts files, folder, other peripherals network drivers. And demanded ransomeware payment as a bitcoin for decrypted all files and folder

A. How to WannaCry works

The Wannacry is executable ransomeware it works straightforward manners. Its arrived in infected computer as a dropper self content program format and execute the program in other computer or infected their files and folders. This is a an application that encrypt or decrypt the data. Files contain encrypted key. This is the copy of tor, used for command-and-control communication with controlling programmer.



B. How does WannaCry Spread

Wannacry is the flow in windows implementation protocol server message block (SMB). SMB protocols is helps for various network PC shared files one node to

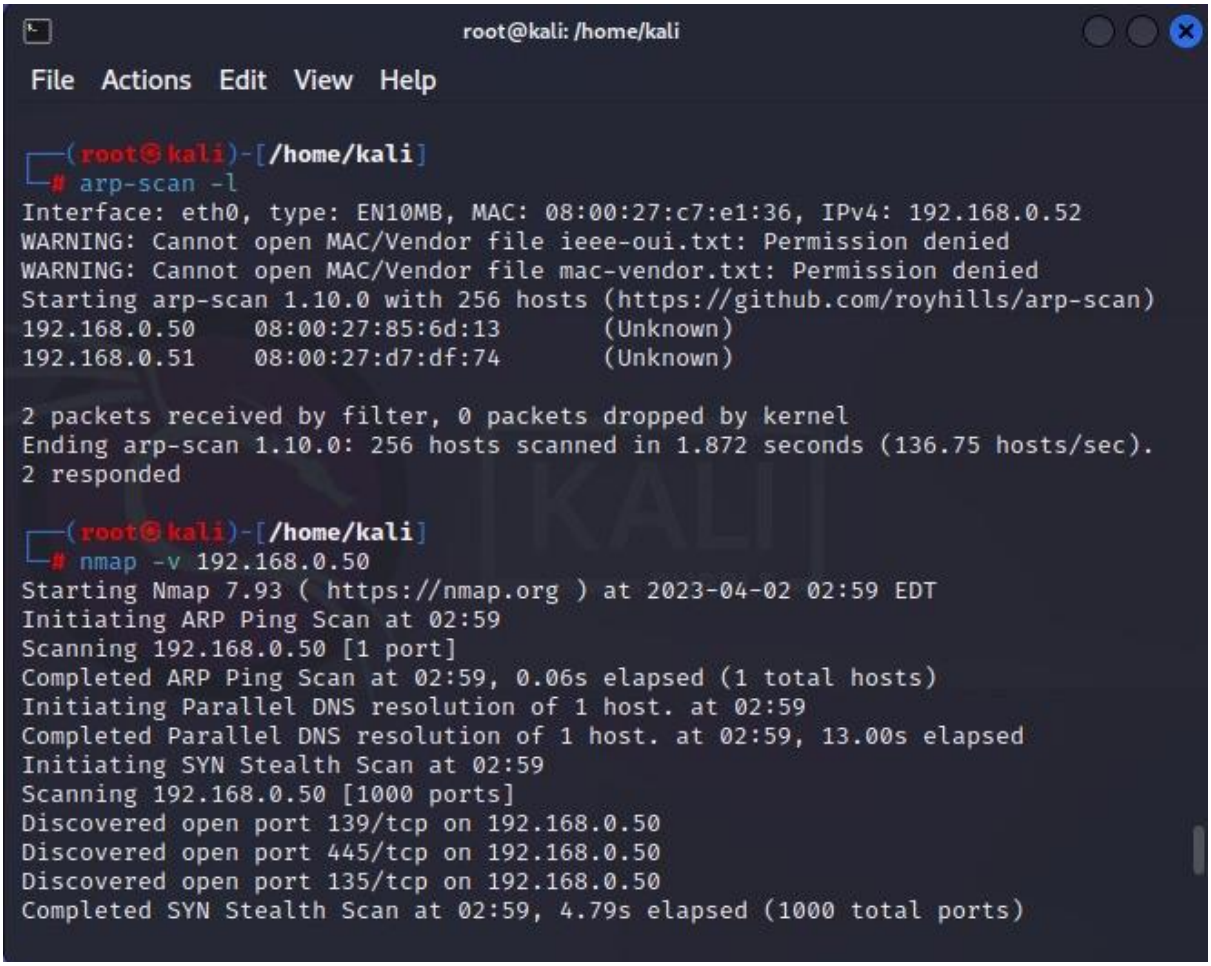
another nodes. Wannacry is infected PC that's are SMB patch is not available. So having EternaBlue vulnerability. That the believe U.S. Nation security was found that vulnerability & reported it to the InfoSec community.

2. TESTBED

A analyze wannacry virtual testbed showing in figure. We have three PC that's installed window 10, 11, Kali Linux for testing purpose and update latest update of windows software and drivers. There IP address of windows 10 PC 192.168.0.50 and windows

11 PC 192.168.0.51 or Kali Linux PC 192.168.0.52 all PC are connected from single 5-Port switch. In window 10, 11 PC create a shared folder that's contained all types of files samples like audio, video, docs, excel, PPTs etc.

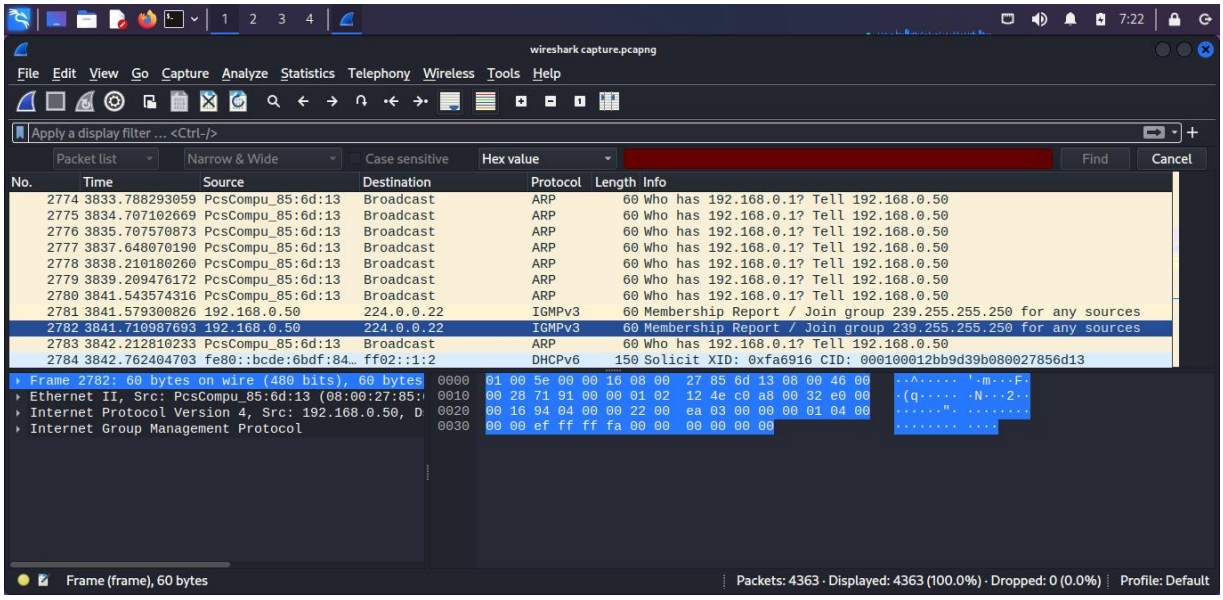
we a done for network scanning in kali linux tools by ARP-SCAN and find network IP 192.168.0.50 and 192.168.0.51 two PC are available in same network. we are tested both PC open port with help of kali Linux tool N-Map command 'nmap –v' and find open port 139/tcp, 445/tcp, 135/tcp. In both PC of windows 10, 11. And launched Wireshark software for network packet capture software in kali linux PC.



2.1 Windows 10 Desktop PC

We are first execute wannacry ransomeware program in windows 10 and find its inbuiled antivirus is quarantines this ransomeware after real-time scanning off in windows 10 we are re-execute this ransomeware and find all are files are infected by this program getting message.

Payment done in bitcoin for getting files back on readable format this message appeared after run the wannacry ransomeware program and find a new IP 239.255.255.250 advise to join this IP by any source of protocol IGMPv3 of destination IP 224.0.0.22 in capturing by wireshark that's have want to connected in third party server. Its find after capturing execute of wannacry ransomeware in windows 10 desktop PC. This encrypted are all types file in contains in shared folder and other drives of windows10 desktop PC.



2.2 Windows 11 Desktop PC

Same condition follow in windows 11 desktop PC and we are find windows 11 having same inbuilt antivirus that's are quarantine wannacry ransomeware and after realtime scanning off we are re-execute this ransomeware and find all files are infected and we are find if we access some other window 10,11 SMB sharing folder they are not infected by this ransomeware and all files are safe. We are find wannacry working directory its modifies folder pattern and find working condition.

```
Created         C:\ProgramData\midtxzggq900\b.wnry
Modifed 15F936  C:\ProgramData\midtxzggq900\b.wnry
Created         C:\ProgramData\midtxzggq900\c.wnry
Modifed 30C     C:\ProgramData\midtxzggq900\c.wnry
Created         C:\ProgramData\midtxzggq900\msg
Created         C:\ProgramData\midtxzggq900\msg\m_bulgarian.wnry
Modifed         C:\ProgramData\midtxzggq900\msg
Modifed BB07    C:\ProgramData\midtxzggq900\msg\m_bulgarian.wnry
Created         C:\ProgramData\midtxzggq900\msg\m_chinese (simplified).wnry
Modifed D457    C:\ProgramData\midtxzggq900\msg\m_chinese (simplified).wnry
Created         C:\ProgramData\midtxzggq900\msg\m_chinese (traditional).wnry
Modifed 135F2   C:\ProgramData\midtxzggq900\msg\m_chinese (traditional).wnry
Created         C:\ProgramData\midtxzggq900\msg\m_croatian.wnry
Modifed 989E    C:\ProgramData\midtxzggq900\msg\m_croatian.wnry
Created         C:\ProgramData\midtxzggq900\msg\m_czech.wnry
Modifed 9E40    C:\ProgramData\midtxzggq900\msg\m_czech.wnry
Created         C:\ProgramData\midtxzggq900\msg\m_danish.wnry
Modifed 90B5    C:\ProgramData\midtxzggq900\msg\m_danish.wnry
Created         C:\ProgramData\midtxzggq900\msg\m_dutch.wnry
Modifed 907B    C:\ProgramData\midtxzggq900\msg\m_dutch.wnry
Created         C:\ProgramData\midtxzggq900\msg\m_english.wnry
Modifed 906D    C:\ProgramData\midtxzggq900\msg\m_english.wnry
Created         C:\ProgramData\midtxzggq900\msg\m_filipino.wnry
Modifed 92CC    C:\ProgramData\midtxzggq900\msg\m_filipino.wnry
Created         C:\ProgramData\midtxzggq900\msg\m_finnish.wnry
Modifed 95E9    C:\ProgramData\midtxzggq900\msg\m_finnish.wnry
```

In summery of dynamic analysis of wannacry ransomare that to archived persistence of infected machines –

- Creates a entry of windows registry to ensure that's execute every restart
- Archive to attempt memory auto start programs
- Uses windows icacls command for granting full access in windows files and machines functions
- Deleted all backups (shadow) copy are find ifopen safe mode. Execute several command in background process
- By using the windows command lines its create VB scripts files for encryption of data and deleted its backup files
- Try to kill ms access and mysql data base by several command line process

3. ENCRYPTION PROCESS

Wannacry ransomeware encryption component is invoked with the task start system thread. During the encryption component checks is one of the following component is available
GlobalnMsWinZonesCacheCounterMutexA, GlobalnMsWinZonesCacheCounterMutexW, MsWinZonesCacheCounterMutexA

If the mutex "MsWinZonesCacheCounterMutexA" is present, then the encryption component is automatically stops without talking any further action. If the mutex is not available in the system, the encryption process is start. In particular task created a new mutex name "MsWin ZonesCache CounterMutexA" and read the content of c.wnry files from the current directory. After the wannacry create three new files as per given below –

WannaCry configuration files

Filename	Description
00000000.res	TOR/C2 info
00000000.pky	Public RSA key
00000000.eky	Encrypted private RSA key

After these three files creation component is ready for encryption files on the system. It is the spawns server threads. First wannacry attempt to load existing two keys in the 00000000.pky and 00000000.dky files present decrypt by RSA key which received after payment verify.

4. RECOVERY

1. First we try to unhide all folder and files for recovery process. So find some shadow /Hide files.
2. Second things reboot the PC in Safe mode this is provide in advance boot option.
3. Enter task manager and terminate all suspicious process
4. Try to 'MSCONFIG' command and terminate all suspicious auto start process
5. After this we select location wich have files lost/deleted and encrypt
6. Using registry key edit and deleted 'CryptLocker' and 'CryptoLocker' folder by manually.
7. And go to MyComputer local dis C: User admin mode and deleted 'cuppidloggus' files

We a recover all deleted files and encrypted by wannacry ransomeware with Wondershare Recovery tool in Kali linux. Its provide facility recover lost or deleted files from wide range of devices, including NAS server, Compute/Laptops, Hard drives, USB drives, and Memory Cards, Its support multiple flies system including NTFS, FAT16/32, exFAT.
Some other software for recover wannacry ransome enfected files likes DiskDrill, Steller Data Recovery Professional , Recoverit(IS), Recuva decryptor software.

5. CONCLUSION

Stay Calm: Ransomeware attack can be stressful its infected more importance files and images. Its more pain full and going to more mistakes and we care full for tacking any decision before paid any types of money
Quarantine Affected System: ransomeware is try to spread attacks in a network to infected more system. So disconnect and quarantine affected device don't connect any networks.
Backups: taking backups of infected system/Hard Disk. Make a other copy for every recovery process
Identify the variant: Many different types variant of ransomeware circulate in a system. Its list change constantly. So are very difficult to identify which types of variant encrypted data.
To Pay or Not: this question is more difficult one. If paid so one thing to data recovered easily and not pays so getting more research for data recovery. Second Condition paid are not guarantee to recover all data.

REFERENCES:

1. Hiran V. Nath and Babu M. Mehtre, "Static Malware Analysis Using Machine Learning Methods", International Conference on Security in Computer Networks and Distributed Systems, 2014.
2. Kharraz A., Robertson W., Balzarotti D., Bilge L., Kirda E., "Cutting the
3. Gordian Knot: A Look under the Hood of Ransomware Attacks"". In: Almgren M., Gulisano V., Maggi F. (eds) Detection of Intrusions and Malware, and Vulnerability Assessment. DIMVA. Lecture Notes in Computer Science, vol 9148. Springer, Cham, 2015.
4. MattiasWeckstén, Jan Frick, Andreas Sjöström, Eric Järpe, "A novel method for recovery from Crypto Ransomware infections", Computer and Communications (ICCC), 2016 2nd IEEE International Conference.
5. Pathak, P B."Malware a Growing Cybercrime Threat: Understanding and Combating Malvertising Attacks",2016,
6. Nolen Scaife, Henry Carter, Patrick Traynor, Kevin R. B. Butler." CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data",2016, IEEE 36th International Conference on Distributed Computing Systems
7. Sanggeun Song, Bongjoon Kim, and Sangjun Lee. "The Effective Ransomware Prevention Technique Using Process Monitoring on Android Platform", Hindawi Publishing Corporation Mobile Information Systems Volume 2016, Article ID 2946735, 9 pages
8. D. O'Brien, "Ransomware 2017", Internet Security Threat Report, Symantec, July 2017 [Online]. Available: https://www.symantec.com/content/dam/symantec/docs/securitycenter/white-papers/istr-ransomware-2017-en.pdf
9. K. Savage, P. Coogan, and H. Lau, "The evolution of ransomware", Security Response, Symantec, June 2015