p-ISSN: 2460-092X, e-ISSN: 2623-1662
Volume 4, Nomor 1, Juni 2018
Hal. 37 - 48

JUSIFO
JURNAL SISTEM INFORMASI

Analisis Aktivitas dan Pola Jaringan Terhadap *Eternal Blue* & *Wannacry Ransomware*

Ferdiansyah
ferdi@binadarma.ac.id

Teknik Informatika, Fakultas Ilmu Komputer, Universitas Bina Darma

Diterima: 5 Maret 2018 | Direvisi: 4 April 2018 | Disetujui: 11 Mei 2018

Abstrak: *Internet memainkan perananan sangat penting saat ini dalam kehidupan dengan pertumbuhan yang cepat harus pula di ikuti dengan meningkatkan kewaspadaan terhadap ancaman siber. Wannacry dan Eternal blue adalah salah satu ancaman kejahatan siber yang sangat besar karena banyak sekali dampak serta kerugian yang ditimbulkan. Penelitian ini diharapkan dapat membantu dalam mengetahui aktivitas dan pola serangan Eternal blue dan Wannacry Ransomware beraksi pada jaringan dan bagaimana Malware mengeksploitasi korban.*
Kata Kunci: *Ransomware, Wannacry, Eternal blue*

Abstract: *The Internet plays a very important role today in life with rapid growth must also be followed by increasing awareness of cyber threats. Wannacry and Eternal blue is one of the greatest threats of cyber crime because of the many impacts and losses. This research is expected to help in knowing the activity and pattern of attacks Eternal blue and WannacryRansomware act on the network and how Malwareexploits the victim.*
Keywords: *Ransomware, Wannacry, Eternal blue*

1 PENDAHULUAN

Internet memainkan peranan sangat penting dalam kehidupan kita saat ini. Dengan pertumbuhan yang cepat dan kemudahan akses ke Internet, jumlah dan kecanggihan serangan di dunia maya juga meningkat. Dampak serangannya pun semakin bervariasi dari pencurian informasi pribadi, mendapatkan akses ke sistem yang dibatasi, kerusakan reputasi organisasi, kerugian finansial, dan sebagainya.

Perangkat lunak berbahaya, dikenal sebagai *Malware*, *Malware* merupakan salah satu cara untuk melakukan serangan siber. Ada beragam jenis *Malware* berdasarkan tingkat ancaman dan cara mereka melakukan aktivitas jahat.

Salah satu kategori Malware tersebut adalah *"Ransomware"*. *Ransomware* adalah perangkat lunak berbahaya yang mengenkripsi data pengguna dan menuntut pembayaran tebusan untuk mendekripsi data dalam jangka waktu tertentu.

Perbedaan utama antara *Malware* dan *ransomware* adalah *Malware* akan mencoba untuk tetap tersembunyi dan tidak terdeteksi ke pengguna, sementara ransomware saat mengenkripsi file meminta secara eksplisit (yaitu terang-terangan) untuk meminta tebusan dengan menampilkan pesan. hal ini pada dasarnya memberi tahu pengguna tentang keberadaannya.

Berdasarkan ciri khas *ransomware* yang meminta tebusan secara terang-terangan tersebut, peneliti berinisiatif untuk melakukan analisis aktivitas *ransomware* tersebut pada aktivitas jaringan sehingga didapatkan pola serangan dan asal muasal serangan tersebut berasal.

2 METODOLOGI PENELITIAN

2.1 Tinjauan Pustaka

2.1.1 Analisis Malware

Secara umum, Malware mempunyai banyak karakteristik. Misalnya, dapat menciptakan atau memodifikasi file, menggunakan pustaka yang dibangun, terhubung ke Internet, mengubah kunci registri, dll. Saat melakukan Malware analisis, dapat dilakukan dengan menganalisa sampel Malware biasanya (.exe atau .dll).

Untuk mengungkapkan sejumlah informasi, alat dan teknik yang berbeda harus digunakan untuk melihat gambaran lengkap dari *Malware*. Ada dua cara untuk melakukan Malware analisis: statis dan dinamis. Analisis statis melibatkan pemeriksaan kode *Malware* tanpa menjalankannya, sementara *Dynamic* Analisis melibatkan menjalankan *Malware* secara langsung (Patel, 2018).

2.1.2 *Static Analysis*

Static Analysis memerlukan pemeriksaan executable tanpa menjalankan file, dengan memeriksa struktur internal dari sebuah file, seseorang dapat mengetahui, apakah sebuah file executable adalah *Malware* atau bukam. Sebagai contoh melihat lebih dekat struktur *headers* dan *sections* dari *Portable Executable (PE)* dapat memberikan wawasan yang baik tentang fungsionalitas dari sebuah file. Teknik lainnya adalah dengan mengamati instruksi program setelah di bongkar untuk mengungkap isi didalamnya, dan dengan demikian akan meningkatkan kemampuan untuk mendeteksi Malware.

2.1.3 *Dynamic Analysis*

Menganalisa file *executable* dengan teknis statis hanya bisa mengungkapkan beberapa informasi tentang Malware, tetapi menjalankan *Malware* dan memeriksa perilakunya saat run-time (sistem sedang berjalan) menyediakan lebih banyak pengetahuan dan meningkatkan kemampuan untuk mengidentifikasi *Malware*, bahkan untuk *Malware* yang disamarkan. *Dynamic analysis* akan menjalankan *Malware* di lingkungan yang aman secara virtual dan memeriksa dengan cermat aktivitasnya sambil memanfaatkan alat atau fitur yang canggih (Sikorski & Honig, 2012).

2.1.4 *Malware*

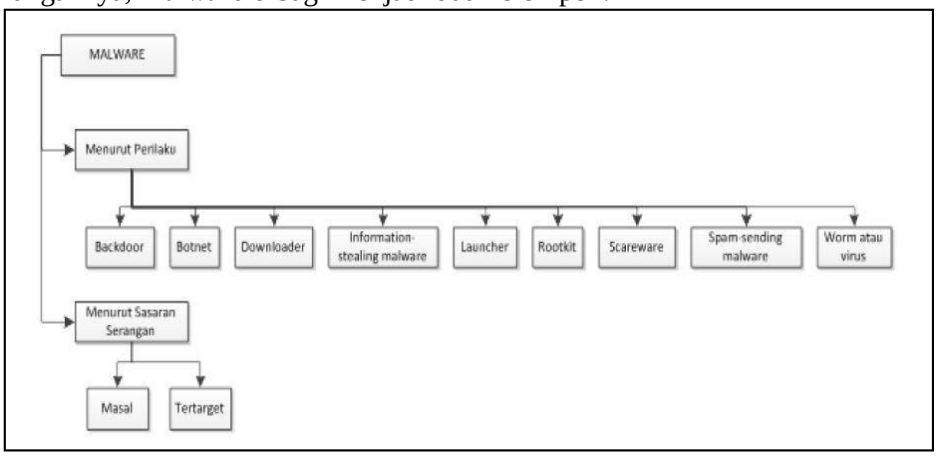
Malware merupakan singkatan dari “Malicious Software”yang berarti perangkat lunak mencurigakan. *Malware* mempunyai beberapa pengerianya ngintinya sama, berikut merupakan beberapa pengertian yang dapat kamitulis berdasarkan jurnal yang telah dibaca (Adenansi & Novarina, 2017):

1. Malware adalah perangka tlunak berbahaya dengan tujuan jahat.
2. Malware adalah programyang diinsta lpada system tanpa pengetahuan pemilik sistem
3. Malware adalah segala bentuk software yang membahayakan baik bagi pengguna, computer atau jaringan.

Jadi dari beberapa pengertian Malware diatas dapat disimpulkan bahwa Malware merupakan suatu *software* yang dibuat untuk tujuan tertentu dengan mencari celah keamanan sistem. *Malware* dapat mengakibatkan dampak buruk bagi *computer* maupun penggunanya karena penyerang dapat mencuri informasi ataupun data pribadi seseorang. Tujuan *Malware* diciptakan oleh penyerang untuk merusak atau membobol suatusi stem operasi melalui *script* rahasia atau dapat dikatakan disisipkan oleh penyerang secara tersembunyi.

a. Taksonomi *Malware*

Malware dapat dibedakan menurut perilaku dan sasaran serangannya. Menurut perilakunya, *Malware* dibagi menjadi 9 kelompok sedangkan menurut sasaran serangannya, *Malware* dibagi menjadi dua kelompok.



Gambar 1. Taksonomi Malware menurut (Sikorski & Honig, 2012)

b. Berikut beberapa jenis Malware menurut perilakunya:

1. *Backdoor*
   Backdoor adalah suatu teknik hacker yang dapat mengakses kesuatu system tanpa melalui autentifikasi normal (login) terlebih dahulu dan berusaha tidak terdeteksi
2. *Botnet*
   Botnet adalah teknik membuka akses suatu system oleh penyerang dengan semua komputer yang terinfeksi botnetakan menerima suatu Intruksi yang sama dari server milik penyerang
3. *Downloader*
   Downloader adalah suatu kode jahat yang bertugas untuk mengunduh kode jahat lainnya. Penyerang menginstal download erketika mendapatkan akses kesebuah sistem. Program download eriniakan menginstal kode jahat tambahan Information-stealing Malware Information-stealing Malwarea dalahsuatu Malware yang mengumpulkan berbagai macam informasi korban dan mengirimkannya kepenyerang. Malware jenis ini biasa digunakan penyerang untuk mendapatkan akeses akun online seperti internet banking.
4. *Launcher*
   Launcher adalah suatu program jahat yang digunakan penyerang untuk menjalankan program jahat lainnya. Launcheini menggunakan teknik non-tradisional untuk menjalankan program jahat lainnya agar tidak terdeteksi dan penyerang bias mendapat akses lebih dalam kesuatu sistem.
5. *Rootkit*
   Rootkit adalah suatu kode yang didesain untuk menyembunyikan keberadaaan kodelainnya. Rootkit dipasang oleh penyerang bersama Malware lainnya untuk dapat mengakses jarak jauh serta membuat kode sulit terdeteksi oleh korban.
6. *Scareware*
   Scareware adalah suatu jenis Malware yang dibuat untuk menakuti korban agar mau membelise suatu. Scareware mempunyai interface yang menyerupai antivirus, biasanya scareware memberi informasi kepengguna bahwa ada kode jahat dalam sistemnya dans atu-satunya cara dengan membeli software tersebut. Namun kenyataannya software tersebut hanya mampu menghapus scareware tersebut
7. *Spam-sending Malware*
   Spam-sending Malware adalah suatu Malware yang menginfeksi mesin pengguna dan kemudian menggunakanya untuk mengirimkan spam. Malware jenis ini dapat menghasilkan uang bagi penyerang dengan cara menjual layanan pengiriman spam.

8. *Worm atau virus*
   Worm atau virus adalah sebuah program yang memiliki kemampuan untuk menggandakan dirinya secara mandiri dan menyebar dengan cepat pada jaringan komputer melalui port keamanan yang terbuka. *Worm* dapat dikatakan evolusi dari virus karena worm memiliki karakteristik yang hampir sama dengan virus, perbedaannya virus bergantung pada program sedangkan worm tidak.

2.1.5 *Ransomware*

Ransomware: Jenis Malware yang yang salah satunya paling merusak Ini awalnya menginfeksi seluruh sistem dengan mengunjungi situs web yang mengandung file berbahaya, menggunakan eksploitasi kerentanan atau melalui email phishing. Selanjutnya, Malware ini akan mengekripsi seluruh data korban dan meminta tebusan dalam bentuk bitcoin dan dalam janga waktu tertentu. Bahkan jika tebusan dibayarkan, tidak dijamin bahwa file akan dipulihkan (Patel, 2018)

2.1.6 *Eternal blue / Double Pulsar*

Bagaimana kita bisa terinfeksi ransoware Wannacry?
Saat ini WCry tersebar melalui Exploit NSA (Network Security Agent) (NSA, 2016) yang bocor yang baru-baru ini dirilis oleh kelompok Shadow Brokers. Peneliti dari Prancis, Kaffine percaya bahwa WCry menyebar melalui exploit ETERNALBLUE.

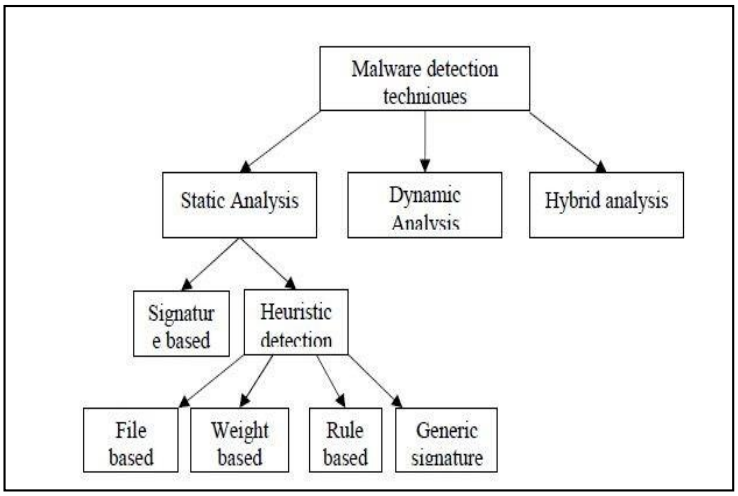
Eternalblue adalah vulnerability pada protocol SMBv1. Exploit ini menyerang sistem yang:

1. Memiliki protocol SMBv1
2. Bisa diakses melalui internet
3. Belum melakukan update patch MS17-010

Saat Malware ini menyerang satu komputer, maka akan dengan cepat menyerang komputer yang lainnya yang berada pada satu jaringan. (ID-SIRTII, 2017).

2.1.7 Teknik Analisis *Malware*

Analisis *Malware* merupakan dasar untuk mendapatkan informasi dalam rangka mengatasi serangan dalam sistem korban. Dari informasi tersebut, dapat dikembangkan signature untuk mendeteksi infeksi *Malware*. Tujuan akhir dari analisis adalah menggambarkan secara tepat cara kerja sebuah *Malware* (Adenansi & Novarina, 2017).



Gambar 2. Representasi Hierarchal Berbagai Teknik Deteksi Malware
(Adenansi & Novarina, 2017)

Teknik yang digunakan untuk analisis ini sebagai berikut : (Adenansi & Novarina, 2017)

1. Analisis Statis

Analisis statis adalah analisis yang dilakukan dengan cara mengamati secara langsung *source code Malware* tanpa mengeksekusi Malware tersebut. Dalam mengamati *source code Malware* dapat menggunakan program seperti program analyze, debugger dan disassembler. Berikut meupakan beberapa teknik analisis statis:

a. Teknik deteksi berbasis signature

Teknik ini menggunakan pencocokan pola atau string atau teknik *finger printing* Penyerang menyisipkan *signature* ke dalam suatu aplikasi dan signature ini digunakan untuk mengidentifikasi jenis Malware tertentu. Untuk dapat mencari kode *Malware*, *detector Malware* akan mencari *signature* yang sudah ada dalam kode.

b. Teknik deteksi *heuristic*

Teknik ini juga dikenal sebagai teknik proaktif .Teknik ini hampir mirip dengan teknik deteksi berbasis signature. Perbedaannya teknik heuristic ini mencari perintah atau intruksi dalam suatu program aplikasi. Hasil akhirnya adalah mudah untuk mendeteksi varian baru dari *Malware* yang semakin banyak jenisnya.

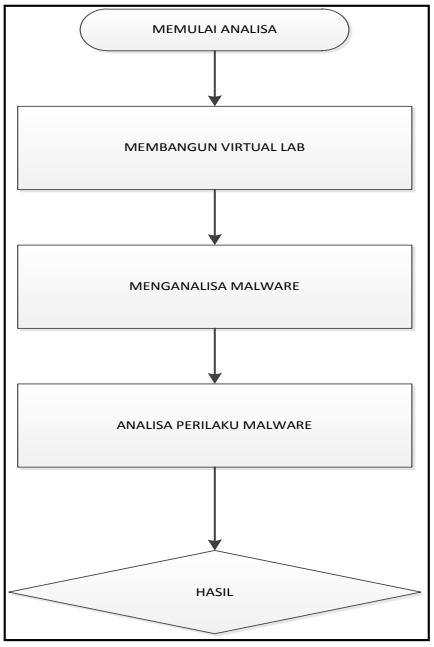
2. Analisis *Dynamic*

Analisis dinamik merupakan metode analisa yang mengamati kerja suatu sistem yang dapat terlihat dari perilaku suatu sistem sebelum Malware dijalankan dengan perilaku setelah Malware tersebut dijalankan atau dieksekusi dalam sistem tersebut. Metode analisis ini biasanya menggunakan software seperti VirtualBox, sehngga apabila Malware yang dieksekusi tersebut merusak sistem maka sistem utama tidak mengalami kerusakan akibat Malware yang dijalankan

3. Analisis *Hybrid*

Teknik analisis ini adalah teknik analisis kombinasi dari analisis statis dan analisis dinamis. Teknik ini menggabungkan keunggulan teknik statis dan dinamis yaitu melakukan pengecekan untuk setiap signature Malware jika ditemukan kode di bawah pemeriksaan dan kemudian memonitor perilaku kode.

2.2 Metode Penelitian



Gambar 3. Metode Penelitian Dinamis *Malware*

Metode yang digunakan dalam penelitian ini adalah metode analisa *Malware* dinamis. Berikut urutan metode penelitian Analisa Dinamis Malware(Cahyanto, Wahanggara, & Ramadana, 2017):

1. Membangun Malware
2. Membangung virtual lab
3. Menganalisa pola aktivitas dan perilaku Malware menggunakan *wireshark* dan *snort* (IDS)
4. Hasil analisa.

2.3 Metode Pengmpulan Data

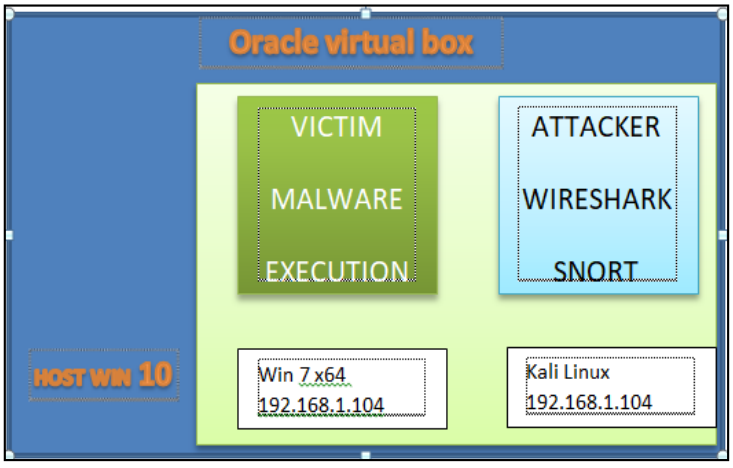
1. Pengamatan (Observasi)

   Yaitu metode pengumpulan data dengan cara mengadakan tinjauan secara langsung ke objek yang diteliti. Untuk mendapatkan data yang bersifat nyata dan meyakinkan maka penulis melakukan pengamatan langsung pada objek yang diteliti yaitu eternal blue Malware dan wannacry ransomware

2. Studi Pustaka

   Untuk mendapatkan data-data yang bersifat teoritis maka penulis melakukan pengumpulan data dengan cara membaca dan mempelajari buku-buku, makalah ataupun referensi lain yang berhubungan dengan masalah yang dibahas.

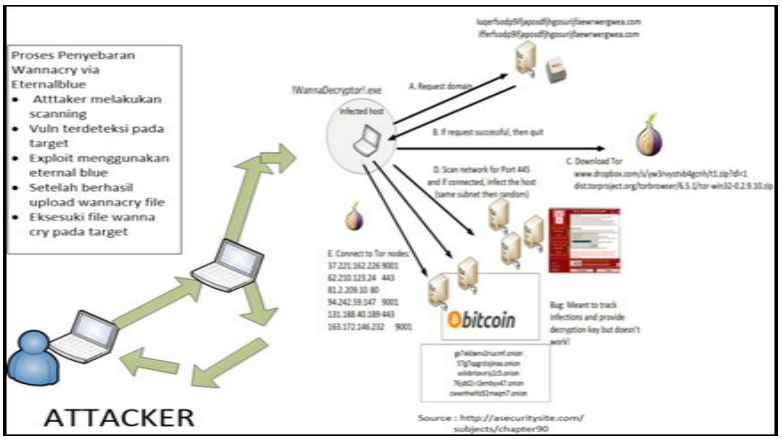
2.4 Perancangan Virtual LAB



Gambar 4. Virtual Lab

3 HASIL DAN PEMBAHASAN

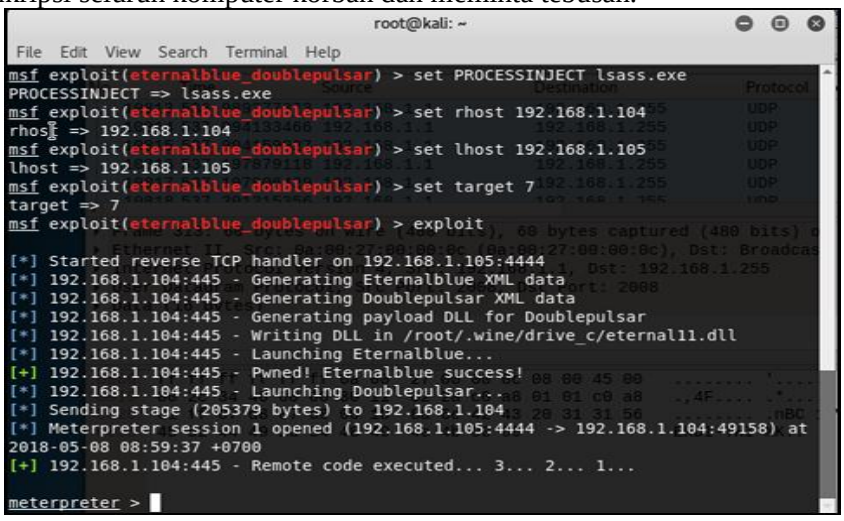
3.1 Hasil



Gambar 5. Proses Penyebaran *Wannacry*

Berdasarkan hasil penelitan ini didapatkan pola penyebaran wannacry melalui eternal blue seperti berikut:

1. *Attacker* melakukan *scanning vuln* (kelemahan) smb_ms017_010.
2. Apabila terbukti vuln maka alur kembali ke attacker untuk melakukan exploitasi penyerangan dengan metode eternal blue.
3. Setelah berhasil masuk ke korban maka attacker mengunggah file wannacry ke korban dan langsung mengeksukinya.
4. Setelah dieksekusi wannacry akan bereaksi di komputer korban dan melakukan aksinya mengenkripsi seluruh komputer korban dan meminta tebusan.



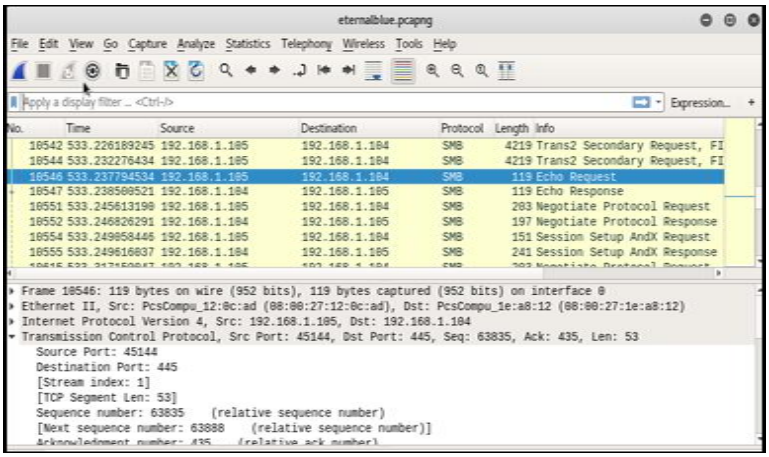
Gambar 6. Proses *Exploit Eternalblue*

```
msf > use exploit/windows/smb/eternalblue_doublepulsar
msf exploit(eternalblue_doublepulsar) > set ETERNALBLUEPATH /root/Eternalblue-Do
ublepulsar-Metasploit/deps/
ETERNALBLUEPATH => /root/Eternalblue-Doublepulsar-Metasploit/deps/
msf exploit(eternalblue_doublepulsar) > set DOUBLEPULSARPATH /root/Eternalblue-D
oublepulsar-Metasploit/deps/
DOUBLEPULSARPATH => /root/Eternalblue-Doublepulsar-Metasploit/deps/
msf exploit(eternalblue_doublepulsar) > set payload windows/x64/meterpreter/reve
rse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf exploit(eternalblue_doublepulsar) > set TARGETARCHITECTURE x64
TARGETARCHITECTURE => x64
msf exploit(eternalblue_doublepulsar) > set PROCESSINJECT lsass.exe
PROCESSINJECT => lsass.exe
msf exploit(eternalblue_doublepulsar) > set rhost 192.168.1.104
rhost => 192.168.1.104
msf exploit(eternalblue_doublepulsar) > set lhost 192.168.1.105
lhost => 192.168.1.105
msf exploit(eternalblue_doublepulsar) > set target 7
target => 7
msf exploit(eternalblue_doublepulsar) > exploit
```

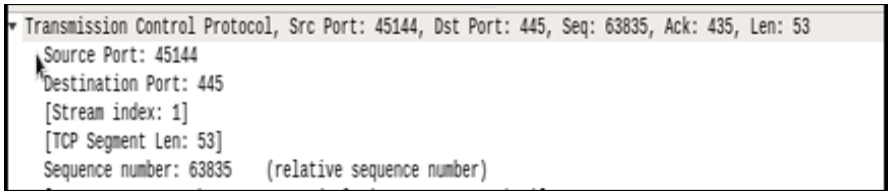
Gambar 7. Hasil Eksekusi *Exploit*

3.2 Pola Aktivitas Pada Jaringan

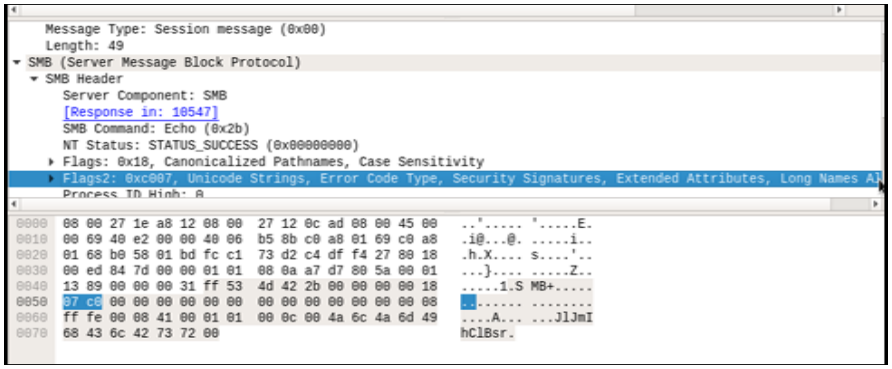
3.2.1 *Wireshark*



Gambar 8. Wireshark smb Status



Gambar 9. *Source Port* dan *Dest. Port*



Gambar 10. *Smb Content*

Berikut adalah hasil analisa yang dapat di gunakan pada pembuatan *rules ids snort*:
content:"|00 00 00 31 ff|
SMB|2b 00 00 00 00 18 07 c0|"|4a 6c 4a 6d 49 68 43 6c 42 73 72 00|"

Bilangan diatas merupakan hexadecimal yang didapat dari *wireshark*:
1. content:"|00 00 00 31 ff| (bilangan ini didapat dari *length*)
2. SMB|2b 00 00 00 00 18 07 c0|"|
3. |4a 6c 4a 6d 49 68 43 6c 42 73 72 00|" (bilangan ini merupakan echo data request).

3.2.2 *Snort*

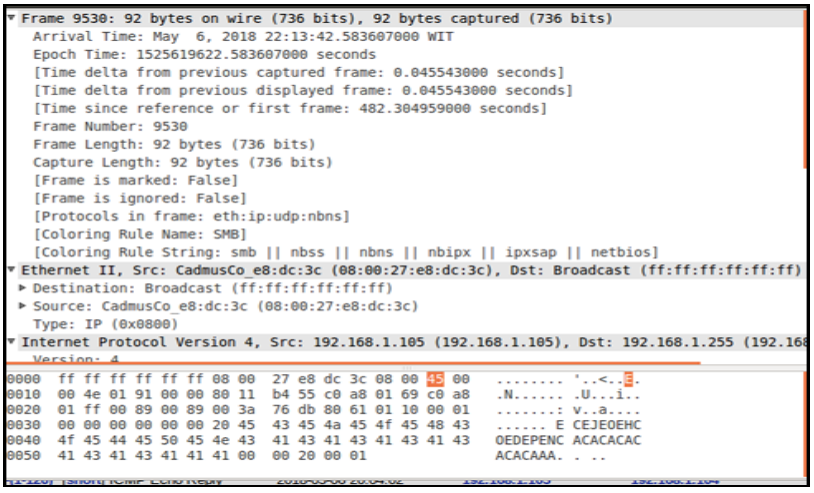
Dari hasil diatas *rules* yang dimasukan ke dalam *snort* adalah sebagai berikut:
alert tcp any any -> any any (msg:"ET EXPLOIT Possible ETERNALBLUE MS17-010 Echo Request (set)"; flow:to_server,established; content:"|00 00 00 31 ff|SMB|2b 00 00 00 00 18 07 c0|"; depth:16; fast_pattern; content:"|4a 6c 4a 6d 49 68 43 6c 42 73 72 00|"; distance:0; flowbits:set,ETPRO.ETERNALBLUE; flowbits:noalert; sid:2024220; rev:1;)

Kemudian hasil alert yang didapat pada snort sebagai berikut:
[**] [1:2024218:1] ET *EXPLOIT* Possible ETERNALBLUE MS17-010 Echo Request [**]
[Priority: 0]
05/18-08:12:21.130265 192.168.1.105:445 -> 192.168.1.104:45144
TCP TTL:128 TOS:0x0 ID:379 IpLen:20 DgmLen:93 DF
AP Seq: 0xD8C0117F Ack: 0x8869C7C6 Win: 0xFB TcpLen: 20

3.3 Analisis *Wannacry*

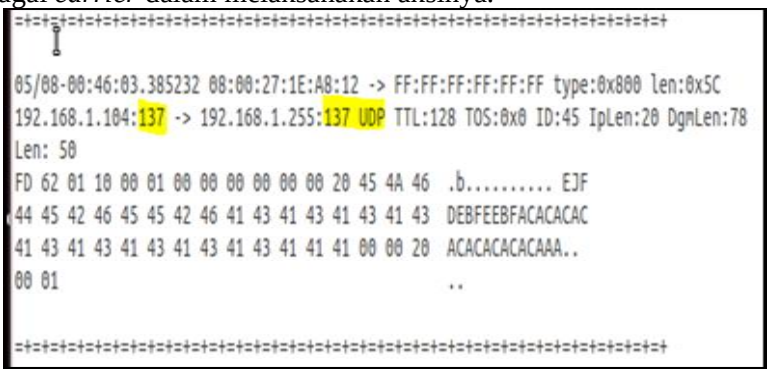
Setelah file *wannacry* di upload melalui *eternal blue* dan di eksekusi secara otomatis *ransomware* langsung mengekripsi seluruh file yang ada di komputer korban.

Gambar 11. *Wannacry Impact*



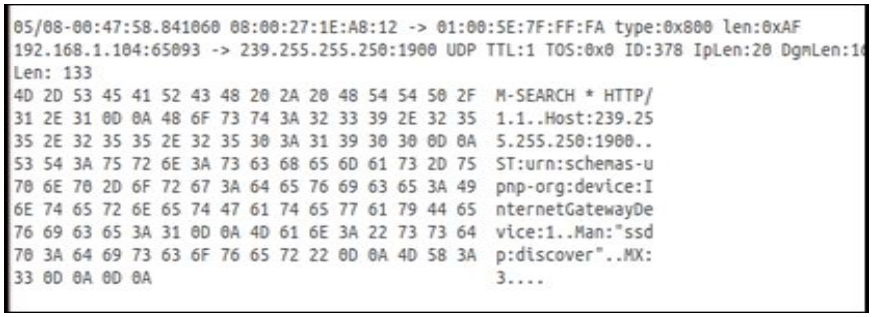
Gambar 12. *Traffic Wannacry* Pada *Wireshark*

Pada Gambar 12 hasil analisa wireshark terlihat ada penggunaan SMB yang digunakan oleh *ransomware wannacry* dengan port 137 yang biasa salah satunya dimanfaatkan oleh *wannacry* sebagai *carrier* dalam melaksanakan aksinya.



Gambar 13. Hasil Analisa *Snortwannacry*

Pada Gambar 13 terlihat hasil yang sama diberikan oleh *snort* sama dengan hasil yang diberikan oleh *wireshark.*



Gambar 14. IP *Attacker Wannacry*

Pada Gambar 14 terlihat hasil yang diberikan oleh *snort* yaitu ada IP yang mencurigakan yang berasal dari 192.168.1.104 menuju IP 239.255.255.250 yang diperkirakan sebagai *IP gateway* dari *attacker wannacry*.

4 KESIMPULAN

Dengan hasil penelitian ini kita dapat mengetahui pola aktifitas dan bagaimana *ransomware wannacry* dapat mengeksploitasi juga mengenkripsi seluruh file pada komputer korban, diharapkan hasil penelitian ini dapat bermanfaat dalam mendeteksi serta mengantisipasi serangan *Ransomware wannacry*.

DAFTAR RUJUKAN

Adenansi, R., & Novarina, L. A. (2017). Malware dynamic. JoEICT (Journal of Education And ICT), 1(1).

Alder, R. (2004). Snort 2.1 intrusion detection. Syngress Publishing, Incorporated.

Cahyanto, T. A., Wahanggara, V., & Ramadana, D. (2017). Analisis dan Deteksi Malware Menggunakan Metode Malware Analisis Dinamis dan Malware Analisis Statis. JUSTINDO, 2(1), 19–30.

ID-SIRTII. (2017). Apa itu WannaCry? Retrieved from https://idsirtii.or.id/berita/baca/423/apa-itu-wannacry-.html[Diakses 10 May 2014].

NSA. (2016). ABOUT US. Retrieved from https://www.nsa.gov/about/

Patel, D. (2018). Mining Ransomware Signatures from Network Traffic.

Septiyanti, D. (2013). Retrieved from http://myrunds.com/sniffing-menggunakan-wireshark-2/[Diakses 10 May 2014].

Sikorski, M., & Honig, A. (2012). Pratical Malware Analysis. No starch press. https://doi.org/10.1017/CBO9781107415324.004

Snort.org. (2017). What is Snort? Retrieved from https://www.snort.org/faq/what-is-snort[Diakses 10 May 2014].

Stiawan, D. (2009). Intrusion Prevention System (IPS) dan Tantangan dalam Pengembangannya. Deris. Unsri. Ac. id.[Diakses 10 May 2014].

Stiawan, D., Abdullah, A. H., & Idris, M. Y. (2011). Characterizing Network Intrusion Prevention System. International Journal of Computer Applications, 14(1), 975–8887. https://doi.org/10.5120/1811-2439

Umar, H. (2000). Metodologi Penelitian. Gramedia Pustaka Umum, Jakarta.