ANALISIS AKTIVITAS DAN POLA SERANGAN *ETERNALBLUE* DAN *WANNACRY RANSOMWARE* YANG BERAKSI PADA JARINGAN PRODI D3 TEKNOLOGI TELEKOMUNIKASI UNIVERSITAS TELKOM

ANALYSIS OF ACTIVITIES AND ATTACK PATTERNS ON ETERNALBLUE AND WANNACRY RANSOMWARE IN ACT ON THE NETWORK D3 TELECOMMUNICATION TECHNOLOGY PROGRAM TELKOM UNIVERSITY

Hafidudin[1], Muhammad Iqbal[2], Annisaul Khaera Arifin[3]

[1,2,3]Prodi D3 Teknologi Telekomunikasi, Fakultas Ilmu Terapan, Universitas Telkom

hafid@tass.telkomuniversity.ac.id[1] iqbal@tass.telkomuniversity.ac.id[2] annisaulkhaerah@gmail.com[3]

Abstrak

WannaCry adalah sebuah Malware bertipe Ransomware yang mengancam komputer data untuk dienkripsi dan dihapus sampai ransom bisa terbayarkan. WannaCry menargetkan kepada korban yang menjalankan operasi sistem Windows, dengan meminta tebusan pembayaran menggunakan mata uang digital Bitcoin. WannaCry juga menggunakan EternalBlue sebuah eksploitasi yang dibuat oleh NSA dan disebarkan oleh The Shadow Broker beberapa bulan sebelum terjadinya serangan global oleh WannaCry. NSA menggunakan *Eternalblue* untuk meretas dan mengambil alih jarak jauh komputer untuk menjalankan windows. *Eternalblue* adalah exploit kit (EK) yang mengeksploitasi kerentanan dalam implementasi Microsoft dari protokol *Server Message Block* (SMB) yang digunakan untuk berbagi file antar komputer. Kerentanan Server Microsoft Windows yang menjalankan SMB versi 1. *Malware WannaCry* menggunakan ekploit bernama *EternalBlue-Doublepulsar* untuk menginfeksi komputer yang menjalankan versi sistem operasi windows. *Malware* ini menggunakan *Eternalblue* untuk eksploitasi kerentanan SMB, jika berhasil akan menanamkan *Doublepulsar backdoor* dan menggunakannya untuk menginstal malware. WannaCry menggunakan *DoublePulsar* sebagai *backdoor* untuk melakukan pemindahan *resource WannaCry* dan menghapus *backdoor* tersebut setelah melakukan pemindahan. Dengan melakukan teknik *hybrid-analysis* yang merupakan kombinasi dari analisis statis dan dinamis. Teknik ini dilakukan dengan mengecek *signature malware* jika ditemukan kode dan memonitoring perilaku kode sehingga menghasilkan analisis lengkap. Dari hasil penelitian ini akan didapatkan aktivitas dan pola serangan *EternalBlue* dan *WannaCry Ransomware* yang beraksi pada jaringan dengan menggunakan *Hybrid-Analysis* yang menjalankan sampel *malware* ke dalam sebuah *environment.*

Kata kunci : *Ransomware, Wannacry, Eternalblue, Malware, Windows Smb, DoublePulsar.*

Abstract

WannaCry is a Ransomware type malware that threatens computer data to be encrypted and deleted until ransom can be paid for. WannaCry targets victims who operate Windows systems, by requesting ransom payments using the digital currency Bitcoin. WannaCry also uses EternalBlue, an exploitation made by the NSA and spread by The Shadow Broker several months before the global attack by WannaCry. NSA uses Eternalblue to hack and remotely take over computers to run Windows. Eternalblue is an exploit kit (EK) that exploits vulnerabilities in Microsoft's implementation of the Server Message Block (SMB) protocol that is used to share files between computers. Vulnerability of a Microsoft Windows Server running SMB version 1. The WannaCry malware uses an exploit called EternalBlue-Doublepulsar to infect computers running versions of the Windows operating system. This malware uses Eternalblue to exploit SMB vulnerabilities, if successful it will embed Doublepulsar backdoor and use it to install malware. WannaCry uses DoublePulsar as a backdoor to move WannaCry resources and delete the backdoor after removal. By doing hybrid-analysis techniques which are a combination of static and dynamic analysis. This technique is done by checking the malware signature if found code and monitoring code behavior so as to produce a complete analysis. From the results of this study will get the activity and attack patterns of EternalBlue and WannaCry Ransomware that act on the network using Hybrid-Analysis which runs malware samples into an environment.

Keyword : *Ransomware, Wannacry, Eternalblue, Malware, Windows Smb, DoublePulsar.*

1. PENDAHULUAN

Internet berperan penting dalam kegiatan sehari-hari. Layanan akses internet yang cepat sehingga serangan di dunia maya juga meningkat. Dampak serangan bervariasi dari pencurian informasi pribadi, mendapatkan akses ke sistem terbatas, kehilangan produktivitas, kerusakan reputasi organisasi, kerugian finansial dan sebagainya.

Wannacry dan *Eternalblue* merupakan salah satu ancaman dan serangan siber dengan cara melakukan kegiatan yang berbahaya. *WannaCry Ransomware* adalah serangan *Cyber* yang ada di seluruh dunia, yang telah ditargetkan pada sistem yang berjalan pada sistem operasi *Microsoft* dengan enkripsi data dan mengklaim pembayaran uang tebusan di *Bitcoin Cryptocurrency*.

Serangan *WannaCry ransomware* merupakan serangan tiba-tiba yang muncul dan berhasil menyebarkan dirinya dalam waktu yang singkat. Hanya dalam hitungan jam, ribuan komputer di seluruh dunia terinfeksi. Kemampuannya untuk menyebarkan dirinya melalui jaringan organisasi dan organisai lain menggunakan internet. Serangan tersebut diperbanyak dan memanfaatkan kerentanan dalam beberapa sistem operasi *Microsoft Windows.*

Pada penelitian[1] Hasil yang diperoleh yaitu dengan menggunakan teknik Analisa malware dengan menjalankan sampel malware ke dalam sebuah *environment* dan memantau aktivitas yang ditimbulkan oleh sampel malware. Dengan mengambil informasi API *call network* dan aktivitas trafik jaringannya. Pada penelitian[2] Hasil yang didapatkan dari deteksi dengan menggunakan *packet capture analyzer* adalah perilaku dan aktivitas malware ketika berada pada jaringan seperti *port* yang digunakan dan layanan yang menjadi sasaran oleh malware. Kemudian di dapatkan kriteria serangan yang dilakukan oleh malware, kategorisasi berdasarkan dampak dan resiko yang dihasilkan oleh malware yang mengacu pada aspek *acess control system*, pada trafik jaringan maupun host yang berada di jaringan. Sehingga dapat dilakukan *controlling* terhadap dampak yang dihasilkan berdasarkan data yang didapat dari hasil Analisa paket data pada jaringan. Pada Penelitian[3] Analisis Statis dan Dinamis *WannCry Ransomware* meneliti perilaku *WannaCry* selama eksekusi di *virtual lab environment*. Kemudian, mengembangkan mekanisme deteksi dan mitigasi untuk *WannaCry* atau family *Ransomware* yang menunjukkan perilaku serupa. Pada Penelitian[4] Mempelajari family *Ransomware* yang berbeda dan mengidentifikasi beberapa karakteristik yang berbeda dan dapat digunakan dalam deteksi awal *Ransomware* berdasarkan network *traffic analysis.* Pada penelitian[5] Hasil yang diperoleh yaitu mengetahui cara kerja program tersebut pada sistem komputer, kombinasi metode untuk menganalisa cara kerja malware (*poison ivy*) dengan beberapa *signature, filename* dan *string* sehingga dapat melakukan proses *login* secara *remote* tanpa diketahui oleh pemilik komputer. Pada penelitian[6] Setiap *malware* di analisis satu persatu dengan tujuan untuk mengetahui jenis *malware* apa, seberapa besar ancamannya dan bagaimana cara penanganannya. Untuk mendapatkan informasi lengkap mengenai satu sampel *malware* dibutuhkan analisis *static* dikarenakan analisis ini dilakukan dengan meneliti *malware source code* tersebut. Pada penelitian[7] *Dynamic Analysis* untuk menganalisis informasi *behavioral* seperti aktivitas jaringan, API *call, file operation* dan catatan modifikasi registri dengan mengeksekusi sampel dalam *environment* virtual. Namun, kekurangan dari *Dynamic Analysis* memerlukan waktu dan sumber daya yang besar untuk mengeksekusi *malware*.

Dengan mengembangkan, mengimplementasikan dan menguji seperangkat aturan baru untuk deteksi ransomware menggunakan mesin VirtualBox dan Yara. Untuk menggabungkan aturan ini dalam model generasi aturan evolusi yang akan memungkinkan mendeteksi keluarga *Ransomware* baru secara efektif dan efisien.

Tujuan dari malware analysis yang dilakukan pada malware jenis *WannaCry Ransomware* ini adalah untuk menganalisa *Raw-Packet SMB,* mempelajari teknik *Reverse-Engineering,* memahami taksonomi *Ransomware* dan memahami *Behaviour* sebuah *Ransomware*.

Oleh karena itu dibutuhkan penelitian analisis aktivitas dan pola serangan *Eternalblue* dan *Wannacry Ransomware* yang beraksi pada jaringan dengan menggunakan metode *Hybrid Analysis* yang menjalankan sampel malware ke dalam sebuah *environment*

2. MATERIAL DAN METODOLOGI/PERANCANGAN

2.1 Pengertian Malware

Malware adalah suatu *software* yang dibuat untuk mencari celah keamanan sistem yang mengakibatkan dampak buruk bagi komputer maupun penggunanya. Malware dapat merusak atau membobol suatu sistem operasi melalui *script* yang disisipkan secara tersembunyi dan dapat mencuri informasi-informasi penting yang melibatkan *confidentiality, integrity* dan *availability* data suatu sistem ataupun aplikasi.

2.2 Jenis Malware

Beberapa jenis malware menurut perilakunya[8] :

1. *Backdoor* untuk melakukan pemindahan *resource* dan menghapus *backdoor* tersebut setelah melakukan pemindahan.
2. *Botnet* adalah teknik yang membuka akses pada sistem untuk semua komputer yang terinfeksi *botnet* dan akan menerima instruksi sama dari *broadcast server* dari penyerang.
3. *Downloader* adalah kode jahat untuk mendapatkan akses ke sistem. Dengan mengunduh kode jahat lainnya.
4. *Information-stealing malware* adalah malware yang mengumpulkan berbagai informasi dari korban kemudian mengirimkannya ke penyerang. Biasanya digunakan agar mendapatkan akses akun online seperti *internet banking.*
5. *Scareware* adalah malware dengan menyuruh korban untuk membeli *software*, dan menyampaikan bahwa terdapat kode jahat pada sistemnya.
6. *Rootkit* adalah kode yang menyembunyikan kode lainnya yang sulit terdeteksi oleh korban sehingga dapat mengakses dari jarak jauh .
7. *Spam-sending malware* adalah malware yang digunakan untuk mengirimkan spam. Jenis malware ini dapat menghasilkan uang dengan menjual layanan pengiriman spam.
8. *Worm* atau *virus* adalah malware yang menggadakan dirinya pada program yang sedang berjalan. Jenis malware tersebut dia dapat tersebar dari komputer ke komputer lain melalui data atau jaringan seperti USB.

Malware dapat diklasifikasikan berdasarkan tujuan penyerang, yaitu:

1. Malware Masal, untuk menyerang komputer korban. Malware Masal banyak dijumpai dan lebih mudah dideteksi karena banyak software keamanan yang sudah mengantisipasi jenis malware masal.
2. Malware tertarget, tidak disebarluaskan dan keamanan yang dipakai korban tidak terlindung dari malware tertarget ini.

2.3 Teknik Analisis Malware

Teknik yang digunakan untuk analisis ini sebagai berikut[9] :

2.3.1 Analisis *Static*

Analisis *static* digunakan dengan cara mengamati secara langsung *source code / Binary Malware* tanpa mengeksekusi Malware tersebut. Pada *Binary Malware* dapat menggunakan program misalnya program *analyze, disassembler.*

2.3.2 Analisis *Dynamic*

Analisis *dynamic*[8] metode deteksi malware dengan menjalankan malware tersebut dalam suatu *environment* virtual yang dapat terlihat dari perilaku malware. Metode analisis ini biasanya menggunakan software seperti VirtualBox, dan beberapa program *sandbox* virtual lainnya, sehingga apabila Malware yang dieksekusi tersebut merusak sistem maka sistem utama tidak terkena efek karena menjalankan malware secara langsung pada *virtualbox.*

2.3.3 Analisis *Hybrid*

Analisis hybrid[8] adalah Analisis hybrid adalah kombinasi dari analisis statis dan analisis dinamis. Teknik ini melakukan pengecekan untuk setiap *signature* Malware, jika ditemukannya kode di bawah pemeriksaan dan kemudian memonitor perilaku kode sehingga menghasilkan analisis lengkap.

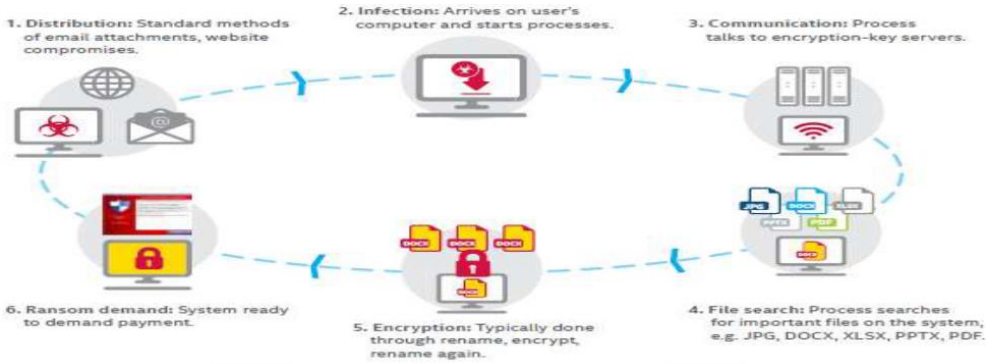
2.4 Ransomware

Ransomware merupakan jenis *malware* yang paling merusak, awalnya menginfeksi seluruh sistem dengan mengunjungi situs web dan mengunduh file berbahaya, menggunakan eksploitasi kerentanan atau melalui *email phishing.* Selanjutnya, *malware* ini akan mengenkripsi seluruh data korban dan meminta

tebusan dalam bentuk *bitcoin* dan dalam jangka waktu tertentu. Bahkan jika tebusan dibayarkan, tidak dijamin bahwa file akan dipulihkan.

.

2.4.1 Cara Kerja *Ransomware*



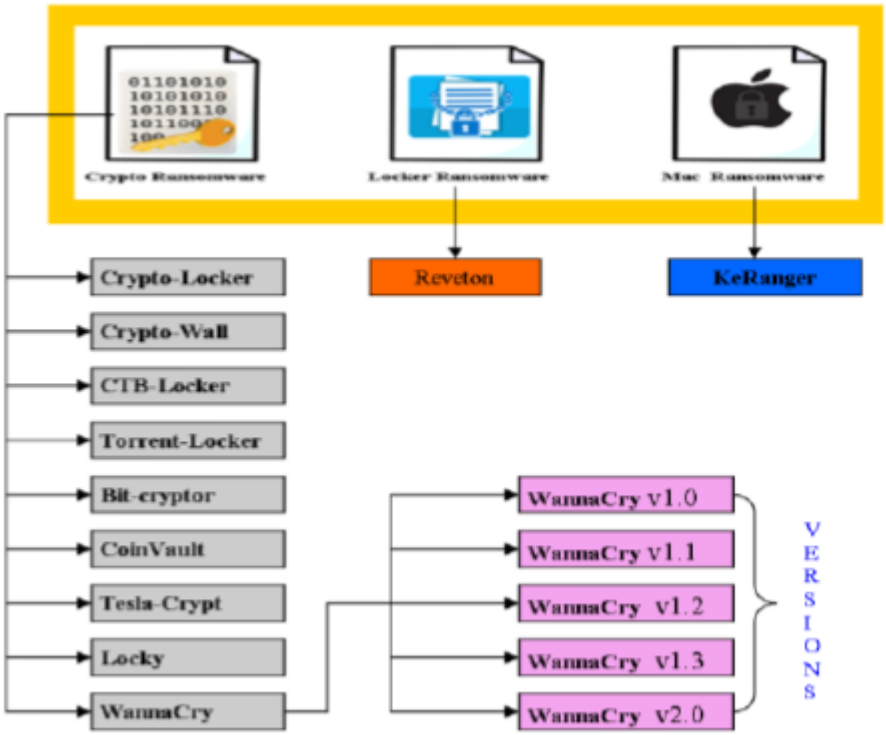
Gambar 2.1 Cara Kerja Ransomware[10]

Ransomware umumnya menggunakan enam langkah untuk menyelesaikan tugasnya, diantaranya[9]:

1. *Distribution ransomware* menggunakan metode distribusi standar. Umumnya itu disebarkan melalui skema *phising* yang melibatkan lampiran atau unduhan *email* dan menginstal pada titik akhir melalui kompromi situs web.
2. *Infection,* melakukan celah eksploitasi dan melakukan proses *Malicious Code*.
3. *Communication,* proses akan berkomunikasi ke server kunci enkripsi untuk mengambil kunci public yang diperlukan untuk mengenkripsi data.
4. *File search,* proses *ransomware* mencari file pada sistem secara sistematis. Biasanya mencari file yang penting bagi pengguna dan tidak dapat dengan mudah direplikasi, seperti file dengan ekstensi jpg, docx, xlsx, pptx dan pdf.
5. *Encryption,* membuat temporary file untuk mengenkripsi file serta mengganti ke nama yang asli dengan ekstensi tambahan dan menghapus file asli.
6. *Ransom demand,* dengan mengambil alih layar titik akhir yang terinfeksi dan menuntut pembayaran.

2.4.2 Jenis Umum *Ransomware*

1. *Locker Ransomware:* Ini juga dikenal sebagai *locker* komputer. *Ransomware* ini tidak mengenkripsi file korban tetapi sebaliknya, menolak akses ke perangkat. Ini mengunci antarmuka pengguna perangkat dan kemudian menuntut korban untuk tebusan[11]. "Reveton" [12]adalah contoh dari tipe ini.



Gambar 2.2 Jenis Ransomware

2. *Crypto Ransomware*: *Crypto Ransomware* adalah semudah persenjataan enkripsi yang kuat terhadap korban untuk menolak akses file mereka. Setelah itu, *ransomware* menyusup ke perangkat korban, malware secara diam-diam mengidentifikasi dan mengenkripsi file yang berharga. Hanya setelah berhasil mengakses file target telah dibatasi *ransomware* meminta pengguna dengan biaya untuk mengakses file mereka. Jenis-jenis *crypto ransomware* ini adalah *crypto-locker, crypto-wall, CTBLocker, Wanna-Cry* dan lain-lain[12] [11].

Menurut *Cisco, WannaCry* telah menggunakan *ETERNALBLUE-DOUBLEPULSAR.* Ini diguanakan untuk mengakses dan mengeksekusi kode pada sistem yang sebelumnya dikompromikan. Lebih lanjut memungkinkan aktivitas dan instalasi perangkat lunak lain seperti malware.

Wanna-Cry menggunakan eksploitasi *Microsoft Windows Smb* yang dipublikasikan setelah sekelompok peretas bernama *Shadow Brokers* merilis file dan alat peretasan milik NSA, AS sinyal utama badan intelijen.

Wanna-Cry bekerja dengan mengenkripsi semua data pada sistem komputer dengan mengubah nama ekstensi file menjadi “WNCRY”. Malware kemudian menampilkan jendela yang memberi tahu pengguna bahwa file mereka telah di enkripsi dan dipulihkan sebagai pengganti pembayaran yang dilakukan dalam *bit-coin* disertai dengan dua *timer*- satu menghitung mundur ke waktu tertentu setelah jumlah tebusan akan dinaikkan sementara yang lain memperingatkan dari waktu sesudahnya file pengguna mana yang akan hilang untuk selamanya.

2.4.3 WannaCry Ransomware

WannaCry Ransomware adalah ransomware yang mengenkripsi file korban dengan dimintai tebusan bayaran untuk mendapatkan file kembali dengan cara mengdecrypt file korban. Cara penyebaran (infeksi) WannaCry menggunakan eksploitasi Windows SMB untuk menyebarkannya terhadap koneksi disekitar.

Eternalblue adalah exploit kit (EK) yang dikembangkan oleh US National Security Agency (NSA) yang mengeksploitasi kerentanan dalam implementasi Microsoft dari protokol Server Message Block (SMB). SMB digunakan untuk berbagi file antar komputer yang terhubung melalui jaringan. Kerentanan ada di server Microsoft windows yang menjalankan SMB versi 1, yang menghasilkan paket yang dibuat secara khusus dari jarak jauh, memungkinkan mereka untuk mengeksekusi *arbitrary code* pada komputer target.

DoublePulsar adalah *backdoor implant tool* yang juga dikembangkan oleh NSA. Untuk melakukan *post-exploitation* setelah diluncurkannya (dijalankan) EternalBlue. WannaCry menggunakan DoublePulsar

sebagai *backdoor* untuk melakukan pemindahan *resources* WannaCry, dan menghapus backdoor tersebut setelah melakukan pemindahan.

2.4.4 EternalBlue

Saat ini WannaCry tersebar melalui Exploit NSA (Network Security Agent) [13] yang bocor yang baru-baru ini dirilis oleh kelompok Shadow Brokers. Peneliti dari Prancis, Kaffine percaya bahwa WannaCry 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

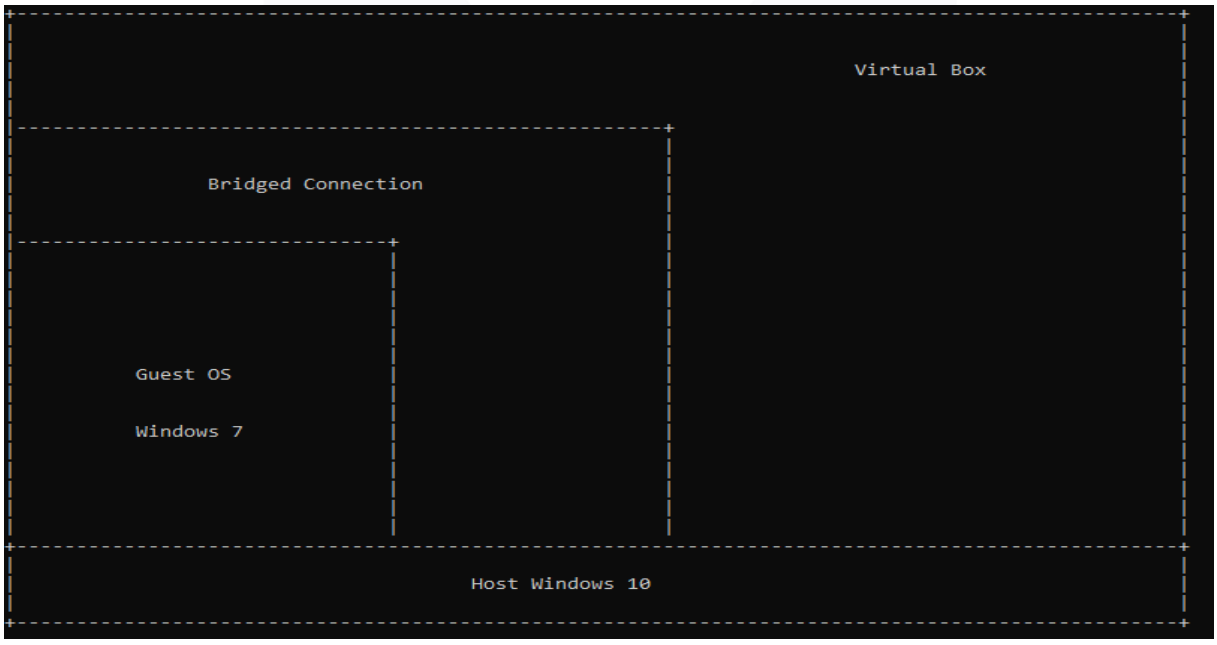
Saat ini WannaCry menyerang satu komputer, maka akan dengan cepat menyerang komputer yang lainnya yang berada pada satu jaringan[14].

Malware, WannaCry, menggunakan eksploit bernama *Eternalblue-DOUBLEPULSAR* untuk menginfeksi komputer yang menjalankan versi sistem operasi Windows. *Eternalblue* pertama kali di publikasikan setelah *Shadow Brokers* merilis banyak alat eksploitasi dan peretasan yang dikembangkan oleh US NSA. Menurut situs web teknologi Ars Techina, NSA menggunakan *Eternalblue* untuk meretas dan mengambil alih jarak jauh komputer untuk menjalankan windows.

Malware ini juga menggunakan modul *ETERNALBLUE* untuk eksploitasi kerentanan SMB. Jika berhasil, akan menanamkan *DOUBLEPULSAR backdoor* dan menggunakannya untuk menginstal malware.

2.5 Model Sistem

Model Sistem dilakukan dengan menggunakan Virtualbox dan menggunakan operasi Windows 7 pada *guests os*. Setelah Windows 7 diinstall di *guests os,* menggunakan Yara untuk melakukan identifikasi bahwa *Binaries* tersebut adalah WannaCry, dan analisa langsung diproses dengan *hybrid-analysis* dan menggunakan Ghidra dan x64dbg untuk di *patching* me-*generate Services* mssecsvc2.0. Dan menganalisa *Services Thread* WannaCry yang melakukan eksploitasi MS17-010 EternalBlue-DoublePulsar.



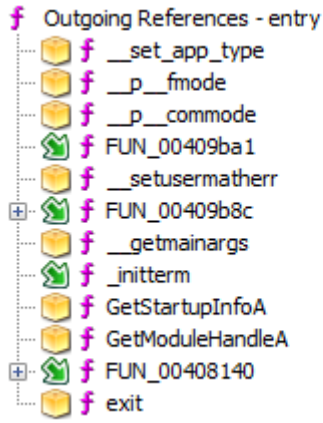
Gambar 2.3 Model Sistem

Tabel 3. 2 Blok Diagram Sistem

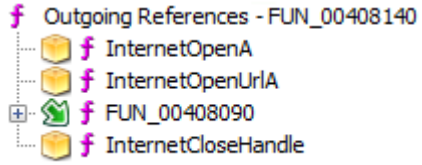
3. HASIL PENELITIAN/HASIL PENGUKURAN, ANALISIS, DAN PEMBAHASAN

3.1 Analisa Awal Simulasi

Langkah awal untuk melakukan analisa adalah dengan mencari *entry function* pada program yang ingin dianalisa. *Entry function* adalah fungsi yang dibuat oleh *compilers* secara otomatis sehingga alokasi memory terhadap *runtime* lebih *compatible*. *entry function* biasanya melakukan *pointers* (menunjuk) terhadap *main function*.



Pada gambar diatas *references main function* biasanya ada dibagian terakhir sebelum *exit function*. Sehingga tidak mungkin untuk diubah oleh user karena berada di *sections* (*.fini*) yang berbeda.



FUN_00408140 adalah *main functions* atau awal masuknya fungsi yang dibuat oleh *user*. **FUN_00408140** memanggil fungsi InternetOpenA, InternetOpenUrlA, fungsi sintaks tersebut berasal dari <wininet.h>.

Windows Internet atau <wininet.h> adalah modules yang melakukan interaksi terhadap *Hypertext Transfer Protocol* (HTTP) dan *File Transfer Protocol* (FTP) untuk melakukan akses Internet & Protocol.

FUN_00408140 menjalankan InternetOpenA dan InternetOpenUrlA untuk melakukan *test-connection* yang digunakan oleh InternetOpenUrlA terhadap www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com, apabila alamat tersebut gagal melakukan *request*, *Control-Flow* akan memanggil fungsi **FUN_00408090** selain itu *return* atau keluar dari fungsi. Dikarenakan alamat *url* tersebut sudah di *sink-holed* atau fungsi InternetOpenUrlA sukses sehingga *control-flow* tersebut tidak memanggil **FUN_00408090**. Untuk bisa melakukan analisa lebih lanjut adalah dengan melakukan *patching* pada program yang dianalisa atau melakukan konfigurasi *block hosts* pada *labs guest operations system windows 7* yang berada di C:\Windows\System32\drivers\etc\hosts terhadap alamat *url* tersebut.

```
109 Standard query 0x6e53 A www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
141 Standard query response 0x6e53 A www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com A 104.17.244.81 A 104.16.173.80
109 Standard query 0xbab9 A www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
141 Standard query response 0xbab9 A www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com A 104.17.244.81 A 104.16.173.80
109 Standard query 0x5ff9 A www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
141 Standard query response 0x5ff9 A www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com A 104.16.173.80 A 104.17.244.81
109 Standard query 0x6399 A www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
141 Standard query response 0x6399 A www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com A 104.16.173.80 A 104.17.244.81
109 Standard query 0xd278 A www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
141 Standard query response 0xd278 A www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com A 104.16.173.80 A 104.17.244.81
109 Standard query 0x2105 A www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
109 Standard query 0x2105 A www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
141 Standard query response 0x2105 A www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com A 104.17.244.81 A 104.16.173.80
141 Standard query response 0x2105 A www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com A 104.17.244.81 A 104.16.173.80
```

Gambar 3.1 Sinkholed Url/Kill-switch domain query

Equivalent C Code:

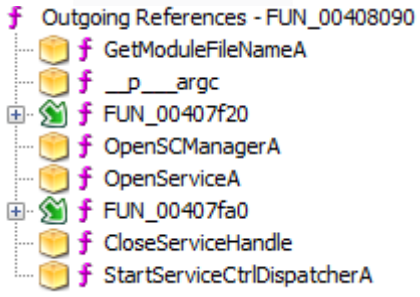
```
#include <wininet.h>

int main(int argc, char * argv[]) {
  HANDLE ih;
  HANDLE ir;

  ih = InternetOpenA(0, 0, 0, 0, 0);
  ir = InternetOpenUrlA(
          ih,
          "www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com",
          0,
          0,
          0x84000000,
          0);

  if (ir == 0) {
    InternetCloseHandle(ih);
    InternetCloseHandle(ir);
    FUN_00408090();
    return 0;
  }

  InternetCloseHandle(ih);
  InternetCloseHandle(ir);
  return 0;
}
```

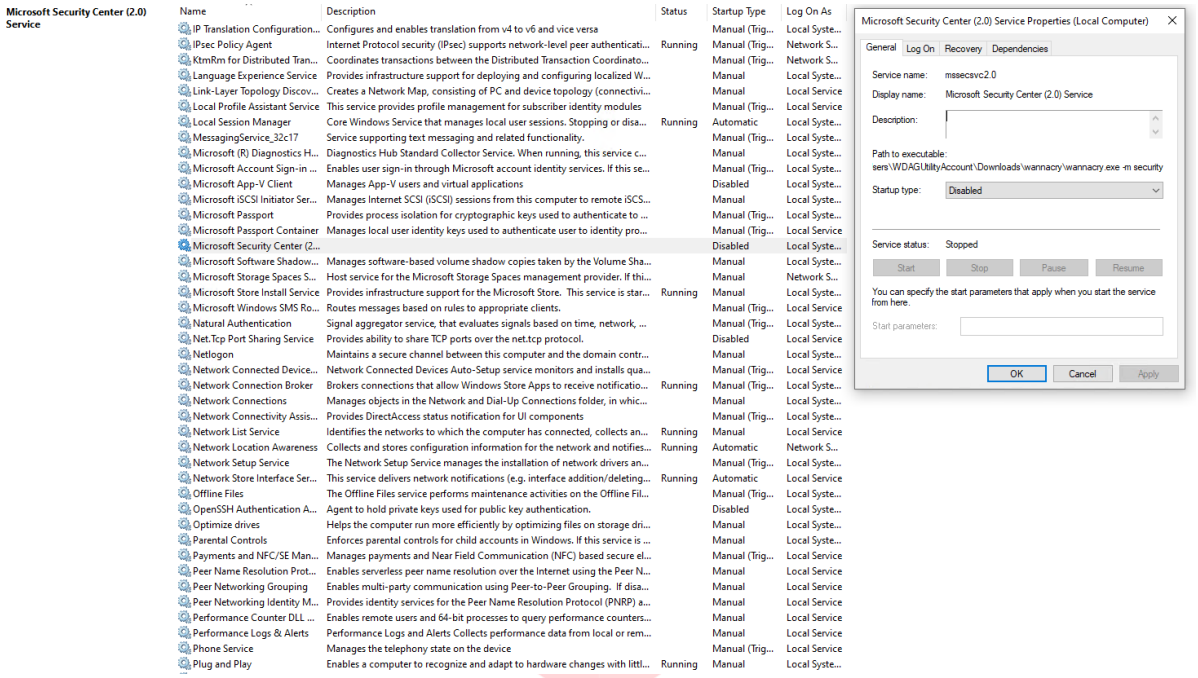


FUN_00408090 adalah fungsi yang membuat Services, **FUN_00408090** memiliki 2 *Control-Flow*, __p___argc memeriksa parameter (*arguments*) apabila program tersebut dipanggil memiliki kurang dari 2 parameter, akan memanggil **FUN_00407f20** setelah itu keluar. Bila program tersebut dipanggil dengan lebih dari 2 parameter, akan melakukan *skip* terhadap fungsi **FUN_00407f20** dan melanjutkan instruksi program dengan memanggil OpenSCManagerA dan mengecek apakah services tersebut sukses melakukan koneksi, bila sukses memanggil **FUN_00407fa0** untuk mengubah konfigurasi *services*, dan menjalankannya.

Bila program tersebut dipanggil kurang dari 2 parameter yang berakhir memanggil fungsi **FUN_00407f20**. Fungsi tersebut memiliki 2 fungsi yang akan dipanggil secara bergantian.

1. **FUN_00407c40**

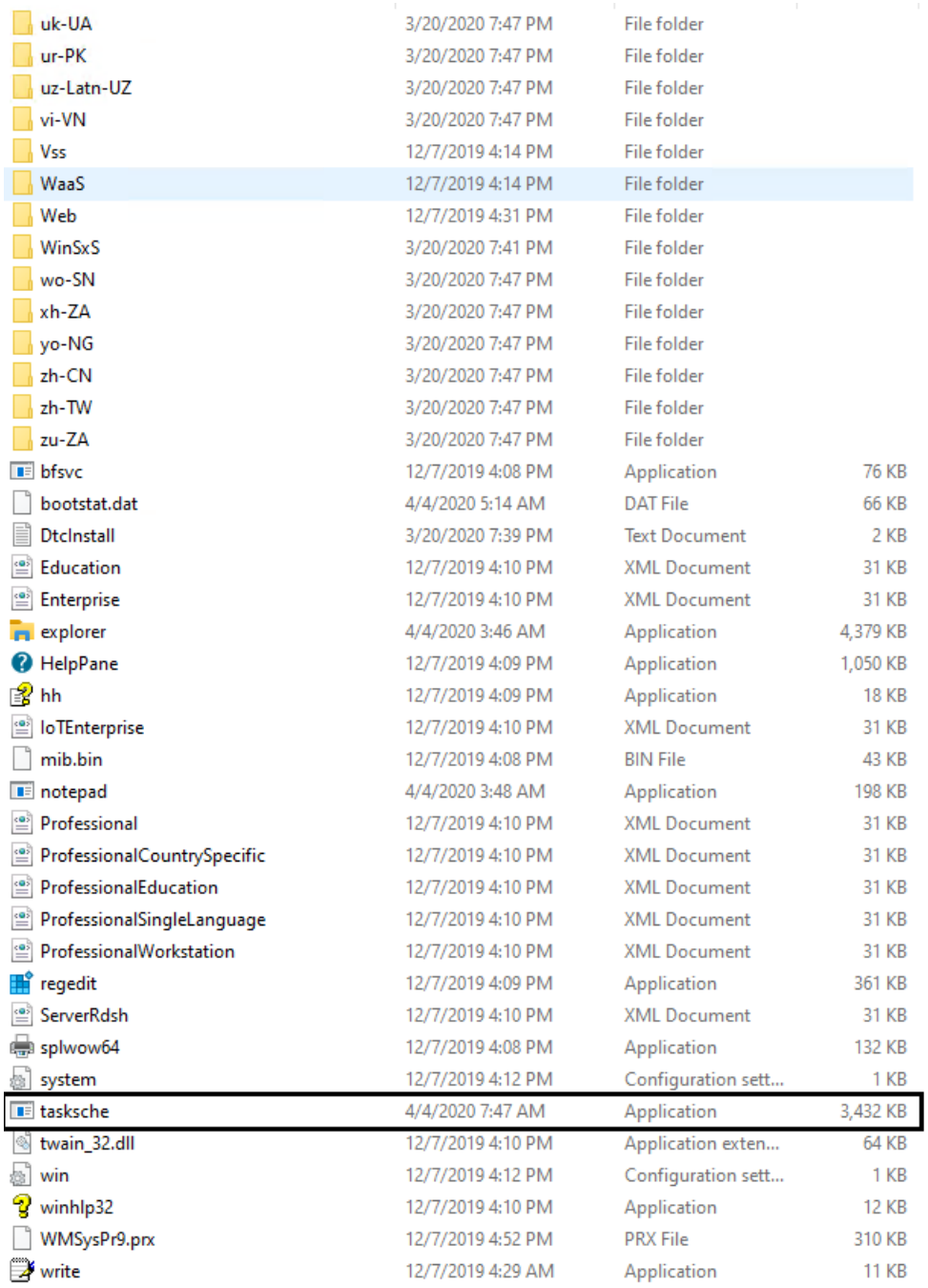
   FUN_00407c40 akan membuat *services* dengan nama “mssecsvc2.0” dan *descriptions* berupa “Microsoft Security Center (2.0) Service” yang menunjuk ke *original path file* wannacry dengan tambahan parameter “-m security”. Bukti fungsi analisa tersebut bisa dicek menggunakan services.msc pada *screenshot* berikut.



Gambar 3.2 Services yang dibuat oleh WannaCry.exe

2. **FUN_00407ce0**

FUN_00407ce0 membuat proses baru melalui <kernel32.dll> dengan menggunakan *imports function* terhadap CreateProcessA, CreateFileA, WriteFileA, CloseHandle. Keempat fungsi tersebut akan membuat *binaries* bernama "tasksche.exe" kedalam *path* "C:\\Windows\\tasksche.exe" dan memanggil file tersebut dengan parameter "/i" lalu mencoba memindahkan dengan MoveFileExA (mengganti nama) kedalam C:\\Windows\\qeriuwjhrf.dll. Setelah itu memulai proses injeksi ransomware dan melakukan CloseHandle pada terakhir fungsi WriteFileA selesai.



uk-UA	3/20/2020 7:47 PM	File folder	
ur-PK	3/20/2020 7:47 PM	File folder	
uz-Latn-UZ	3/20/2020 7:47 PM	File folder	
vi-VN	3/20/2020 7:47 PM	File folder	
Vss	12/7/2019 4:14 PM	File folder	
WaaS	12/7/2019 4:14 PM	File folder	
Web	12/7/2019 4:31 PM	File folder	
WinSxS	3/20/2020 7:41 PM	File folder	
wo-SN	3/20/2020 7:47 PM	File folder	
xh-ZA	3/20/2020 7:47 PM	File folder	
yo-NG	3/20/2020 7:47 PM	File folder	
zh-CN	3/20/2020 7:47 PM	File folder	
zh-TW	3/20/2020 7:47 PM	File folder	
zu-ZA	3/20/2020 7:47 PM	File folder	
bfsvc	12/7/2019 4:08 PM	Application	76 KB
bootstat.dat	4/4/2020 5:14 AM	DAT File	66 KB
DtcInstall	3/20/2020 7:39 PM	Text Document	2 KB
Education	12/7/2019 4:10 PM	XML Document	31 KB
Enterprise	12/7/2019 4:10 PM	XML Document	31 KB
explorer	4/4/2020 3:46 AM	Application	4,379 KB
HelpPane	12/7/2019 4:09 PM	Application	1,050 KB
hh	12/7/2019 4:09 PM	Application	18 KB
IoTEnterprise	12/7/2019 4:10 PM	XML Document	31 KB
mib.bin	12/7/2019 4:08 PM	BIN File	43 KB
notepad	4/4/2020 3:48 AM	Application	198 KB
Professional	12/7/2019 4:10 PM	XML Document	31 KB
ProfessionalCountrySpecific	12/7/2019 4:10 PM	XML Document	31 KB
ProfessionalEducation	12/7/2019 4:10 PM	XML Document	31 KB
ProfessionalSingleLanguage	12/7/2019 4:10 PM	XML Document	31 KB
ProfessionalWorkstation	12/7/2019 4:10 PM	XML Document	31 KB
regedit	12/7/2019 4:09 PM	Application	361 KB
ServerRdsh	12/7/2019 4:10 PM	XML Document	31 KB
splwow64	12/7/2019 4:08 PM	Application	132 KB
system	12/7/2019 4:12 PM	Configuration sett...	1 KB
tasksche	4/4/2020 7:47 AM	Application	3,432 KB
twain_32.dll	12/7/2019 4:10 PM	Application exten...	64 KB
win	12/7/2019 4:12 PM	Configuration sett...	1 KB
winhlp32	12/7/2019 4:10 PM	Application	12 KB
WMSysPr9.prx	12/7/2019 4:52 PM	PRX File	310 KB
write	12/7/2019 4:29 AM	Application	11 KB

Gambar 3.3 Binaries yang dibuat oleh WannaCry.exe

3.2 Menganalisa Raw-Packet SMB

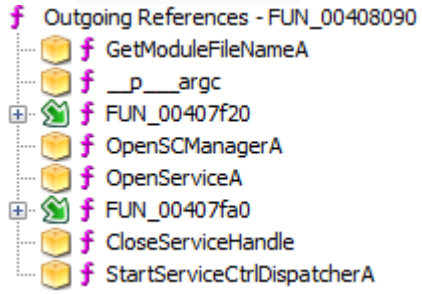
SMB Packet adalah sebuah protokol yang digunakan untuk *file sharing*, SMB Packet memiliki Data Structure protokol seperti ini:

```
SMB_Header
  {
  UCHAR  Protocol[4];
  UCHAR  Command;
  SMB_ERROR Status;
  UCHAR  Flags;
  USHORT Flags2;
  USHORT PIDHigh;
  UCHAR  SecurityFeatures[8];
  USHORT Reserved;
  USHORT TID;
  USHORT PIDLow;
  USHORT UID;
  USHORT MID;
  }
```

1. Protocol yang dikirim harus memiliki Signature String '\xFF', 'S', 'M', 'B' agar bisa mengirim packet smb
2. Command memiliki setidaknya 255 (1 byte)
3. Status digunakan untuk mengirim pesan status dari server ke client
4. Flags/Flags2 untuk mendeskripsikan fitur terhadap pesan
5. PIDHigh digunakan untuk mengidentifikasi proses id
6. SecurityFeatures digunakan untuk interpretasi SecuritySignatures
7. SecuritySignature sebuah data yang mengenkripsi pesan.
8. Reserved data yang tidak bisa diubah
9. TID tree identifier
10. PIDLOW process id lower
11. UID User identifier
12. MID multiplexer id

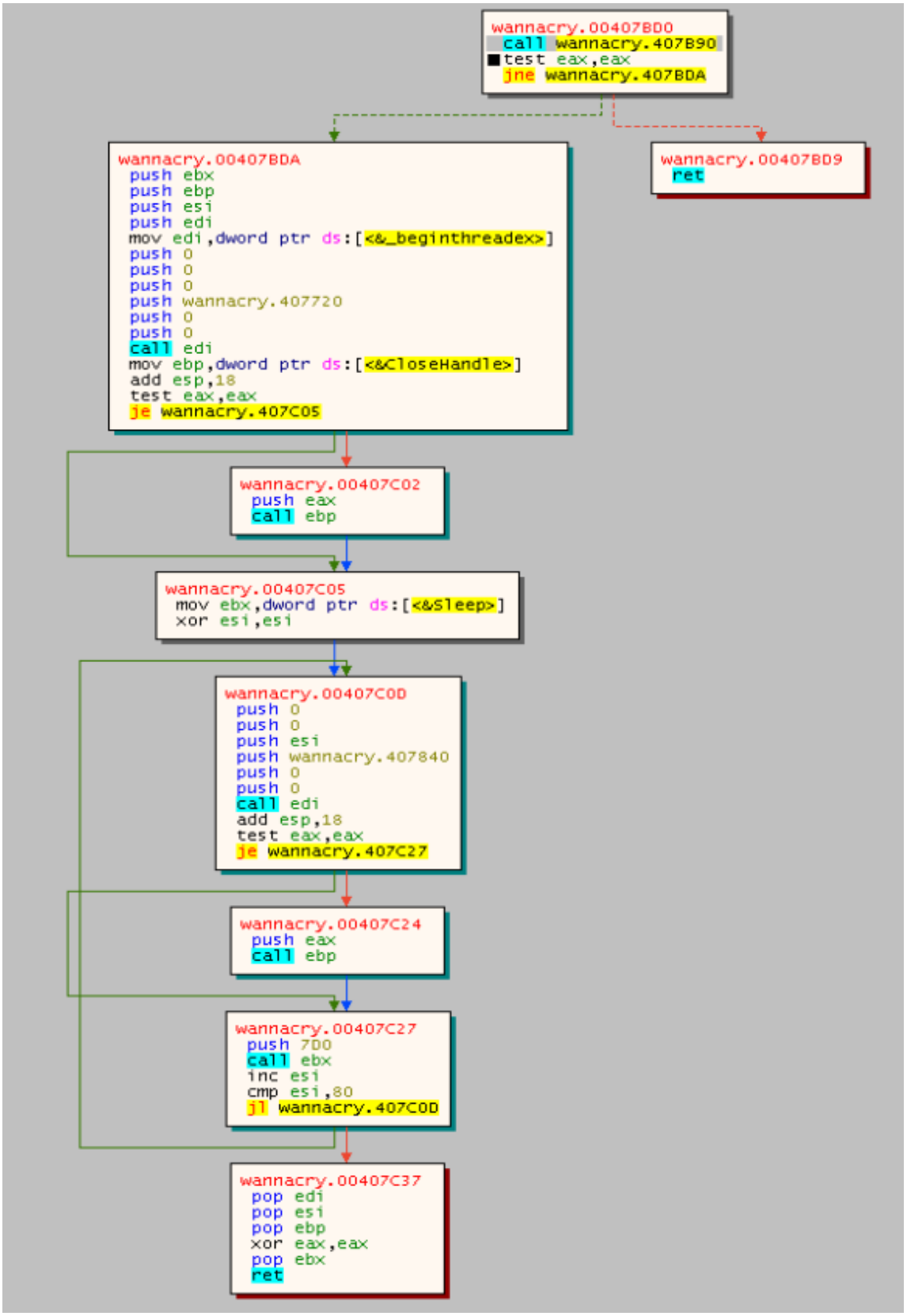
3.3 Analisa Lanjut

Langkah selanjutnya adalah dengan menganalisa file “wannacry.exe” dengan parameter “-m securitry” untuk mengetahui *General Behaviour Exploit* yang dilakukan oleh file tersebut.



Service Mode akan memanggil wannacry.exe (mssecsvc.exe) dengan menambahkan paramaters “-m security”, setelah dipanggil __p__argc akan melakukan skip terhadap fungsi **FUN_00407f20** dan membuka **OpenSCManagerA** dan **OpenServiceA** untuk mengubah *Config Services* dan memanggil *Main Services Handler* pada alamat 0x00408000 lewat **StartServiceCtrlDispatcherA**.

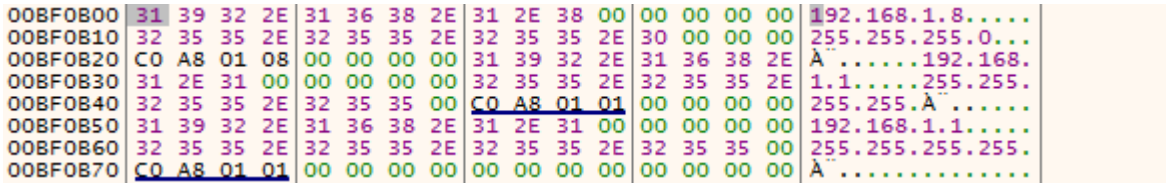
Bila *Main Services Handler* sukses melakukan interaksi (terhubung) dengan mssecsvc2.0, mengubah *status services* menjadi proses berjalan (SetServiceStatus), dan memanggil fungsi 0x407BD0 (wannacry.407BD0).


wannacry.00407BD0
call wannacry.407B90
test eax,eax
jne wannacry.407BDA
wannacry.00407BDA
push ebx
push ebp
push esi
push edi
mov edi,dword ptr ds:[<&_beginthreadex>]
push 0
push 0
push 0
push wannacry.407720
push 0
push 0
call edi
mov ebp,dword ptr ds:[<&CloseHandle>]
add esp,18
test eax,eax
je wannacry.407C05
wannacry.00407BD9
ret
wannacry.00407C02
push eax
call ebp
wannacry.00407C05
mov ebx,dword ptr ds:[<&Sleep>]
xor esi,esi
wannacry.00407C0D
push 0
push 0
push esi
push wannacry.407840
push 0
push 0
call edi
add esp,18
test eax,eax
je wannacry.407C27
wannacry.00407C24
push eax
call ebp
wannacry.00407C27
push 7D0
call ebx
inc esi
cmp esi,80
jl wannacry.407C0D
wannacry.00407C37
pop edi
pop esi
pop ebp
xor eax,eax
pop ebx
ret

Pada fungsi wannacry.407B90, memiliki 2 *threads* terpisah yang akan dijalankan secara *looping* sampai 128 kali dengan *pause* (sleep) 2 detik.

3.4 Memahami SMB Packet

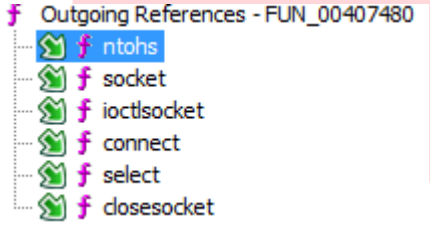
1. Thread Pertama



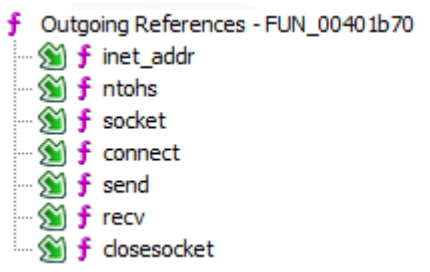
Gambar 3.4 Raw-packet

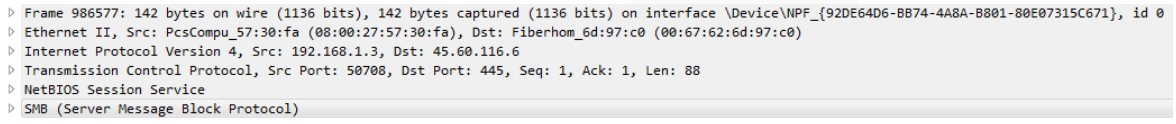
Mencari informasi socket ip address yang dipakai dengan menggunakan GetAdaptersInfo.

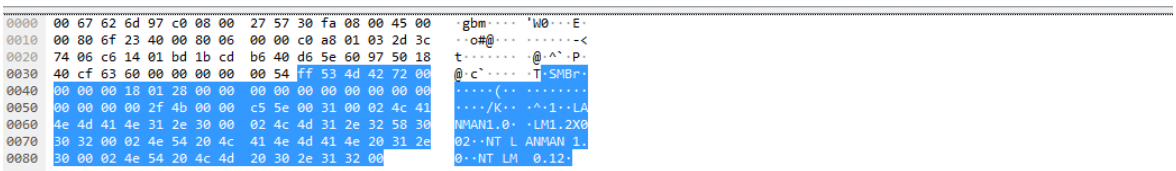
2. Thread Kedua



Melakukan tes koneksi socket

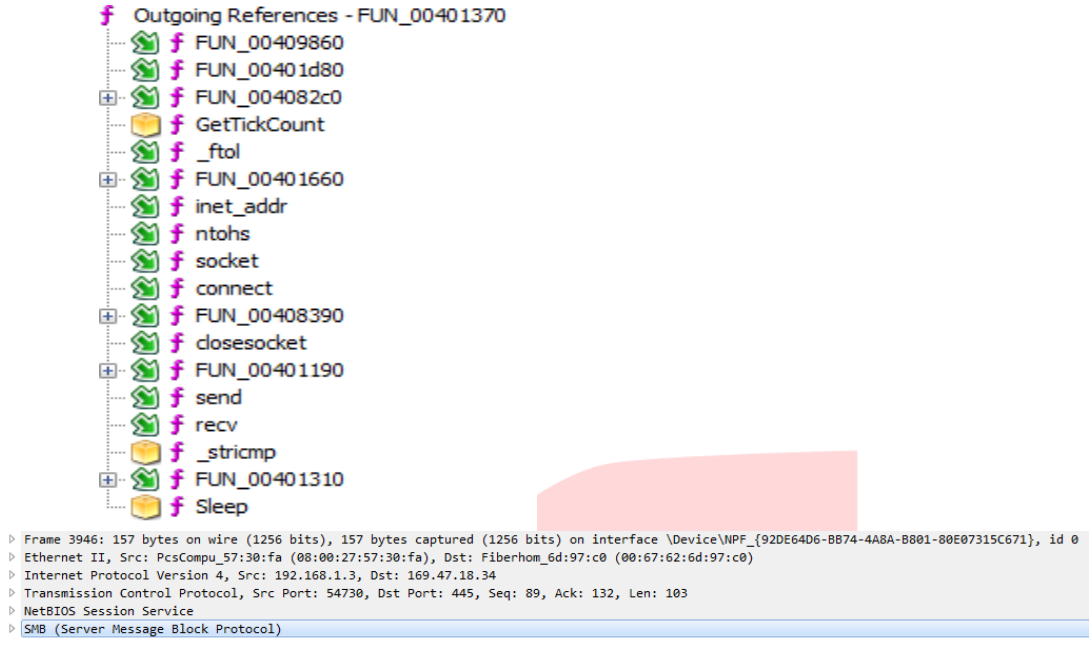






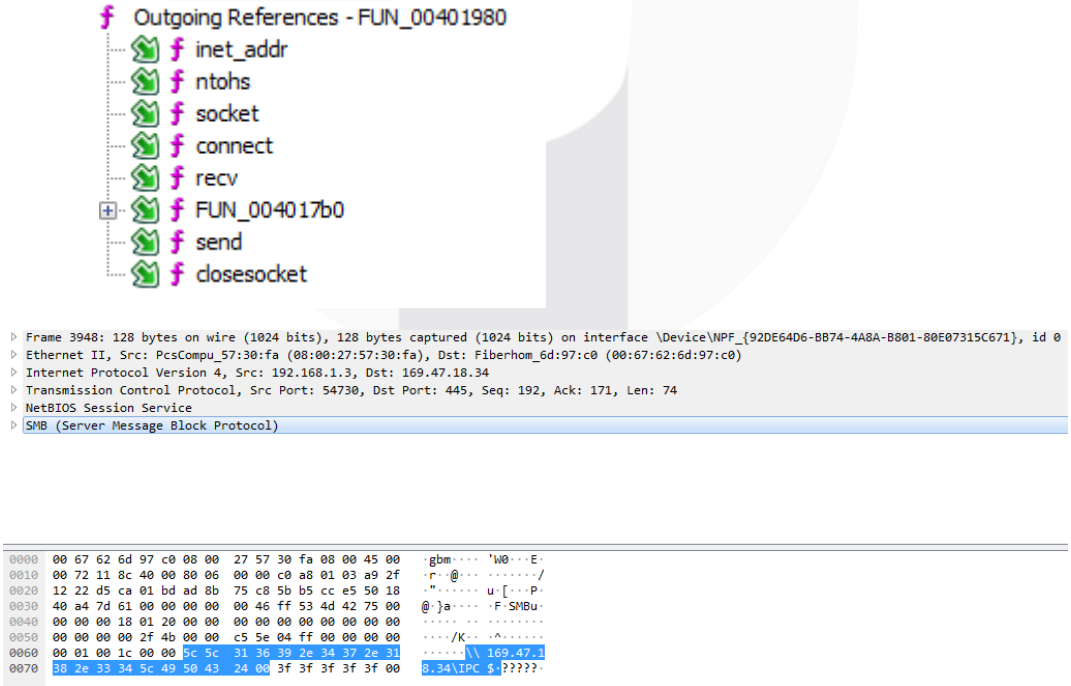
Gambar 3.5 Raw-packet SMB

Mengirim payload pertama *Negotiate Request Protocol SMB*. Tujuan ini untuk melakukan interaksi *discovery* & *file sharing*.



Gambar 3.6 Raw-packet SMB

Mengirim payload kedua *Session Setup AndX Request*. Setelah *discovery* diterima oleh pengirim (pelaku) & penerima (korban) akan melakukan *Request Session* untuk melakukan interaksi *file sharing*.



Gambar 3.7 Eksploitasi Nested SMB AndX Request dan SMB Pipe

Melakukan eksploitasi SMB AndX Request dengan campuran SMB Pipe, sehingga dapat membuka *Command Line Windows* dan mengeksploitasi korban.

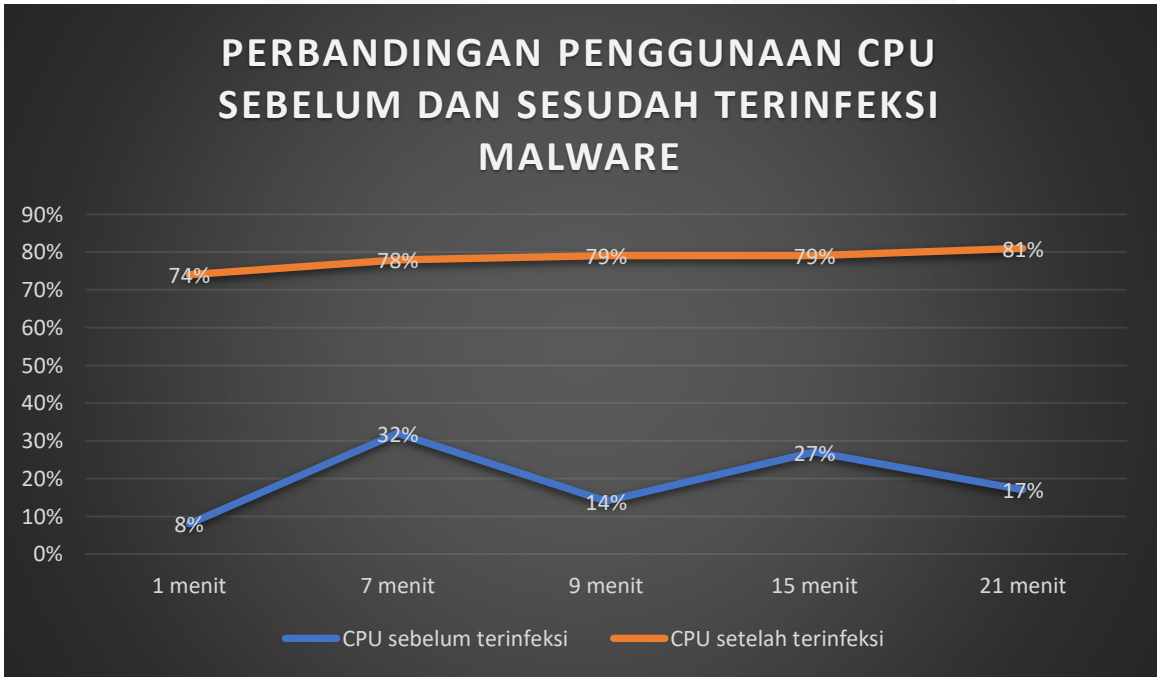
Performa pada *System computer*

Pada saat menjalankan aplikasi apapun, kinerja komputer akan semakin meningkat setelah terinfeksi malware. Dengan melihat performa komputer penggunaan CPU sebelum dan sesudah terinfeksi Malware di tiap waktu tertentu secara berkelanjutan semakin meningkat. Sehingga saat menggunakan komputer terasa berat atau tiba-tiba melambat secara signifikan atau mengalami crash secara teratur. Seperti yang terlihat pada tabel 4.1 dan gambar 4.12.

NO	WAKTU	CPU SEBELUM TERINFEKSI	CPU SETELAH TERINFEKSI
1.	1 MENIT	8%	74%
2.	7 MENIT	32%	78%
3.	9 MENIT	14%	79%
4.	15 MENIT	27%	79%
5.	21 MENIT	17%	81%

Tabel 4. 1 Penggunaan CPU sebelum dan sesudah terinfeksi malware

Berdasarkan data pengguna CPU sebelum dan sesudah terinfeksi malware, maka dapat dilihat grafik perbandingannya pada gambar 4.12



Gambar 4. 1 Perbandingan penggunaan memory sebelum dan sesudah terinfeksi malware

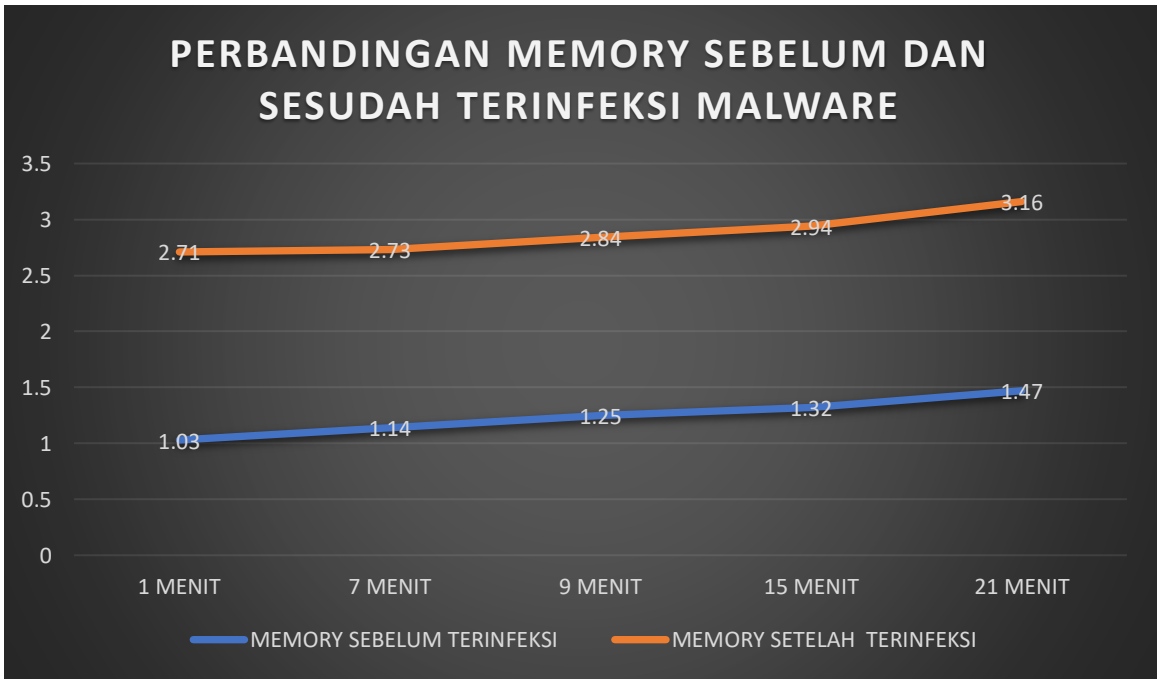
Sedangkan pada saat menjalankan aplikasi apapun, kinerja komputer berjalan dengan normal sebelum terinfeksi malware. Dengan melihat performa komputer penggunaan Memory sebelum dan sesudah terinfeksi Malware di tiap waktu tertentu secara berkelanjutan mengalami peningkatan. Sehingga saat

menggunakan komputer terasa cepat berbeda dengan setelah terinfeksi mengalami *loading* yang cukup lama. Seperti yang terlihat pada tabel 4.2 dan gambar 4.13.

NO	WAKTU	MEMORY SEBELUM TERINFEKSI	MEMORY SETELAH TERINFEKSI
1.	1 MENIT	1.03 GB	2.71 GB
2.	7 MENIT	1.14 GB	2.71 GB
3.	9 MENIT	1.25 GB	2.84 GB
4.	15 MENIT	1.32 GB	2.94 GB
5.	21 MENIT	1.47 GB	3.16 GB

Tabel 4. 2 Penggunaan Memory sebelum dan sesudah terinfeksi malware

Berdasarkan data pengguna Memory sebelum dan sesudah terinfeksi malware, maka dapat dilihat grafik perbandingannya pada gambar 4.13



Gambar 4. 2 Perbandingan penggunaan cpu sebelum dan sesudah terinfeksi malware

3.5 Kesimpulan Analisa

Dari hasil analisis dapat disimpulkan beberapa tahap analisis *WannaCry :*

1. Memulai Malware dengan menghubungkan domain InternetOpenUrl: www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com. Jika berhasil, malware segera keluar.
2. Selanjutnya, membuat service baru bernama mssecsvc2.0 dengan menunjukkn biner path ke module yang sedang berjalan dengan parameter "-m security". Setelah dibuat, malware kemudian menjalankan service dan mengeksploitasi MS17-010 terhadap service SMB EternalBlue-Double Pulsar yang dapat mengambil alih jarak jauh komputer untuk menjalankan windows.

3. Pada fungsi WannaCry memiliki 2 threads, menghubungkan komputer ke jaringan bisa berupa port dan menentukan subnet mana yang menjalankan sistem. Masing-masing threads mencoba menyambungkan ke IP pada port 445 dan jika berhasil, akan mengeksploitasi service. Dan melakukan serangan SMB (*Server Message Block*) pada sistem
4. .Malware menempatkan resource R-nya dan memuatnya ke dalam memori. Malware menulis data resource ke file C:\WINDOWS\tasksche.exe /i dengan CreateProcessAPI. Malware kemudian mencoba memindahkan C:\WINDOWS\tasksche.exe ke C:\WINDOWS\qeriuwjhrf, dengan menggantikan file aslinya jika ada.

4. KESIMPULAN

Berdasarkan hasil perancangan, pengujian dan analisa yang telah dilakukan maka dapat diambil beberapa kesimpulan sebagai berikut:

1. Analisis aktivitas dan pola serangan eternalblue dan wannacry ransomware yang beraksi pada jaringan menggunakan teknik deteksi hybrid-analysis dapat dilakukan dengan pengecekan untuk setiap signature malware, dan memonitoring perilaku kode ransomware.
2. Dengan menggunakan teknik hybrid-analysis dapat mengetahui karakteristik ransomware serta serangan target dari serangan ransomware dengan mencari fungsi internal dari sebuah library bawaan.
3. Dengan melakukan teknik reverse engineering dapat memahami binary code atau biasa disebut bahasa assembly.
4. Simulasi hybrid-analysis dilakukan dengan menggunakan software ghidra. Pada static analysis dapat dilihat source code yang dituliskan pada program tersebut. Dan memberikan informasi cukup lengkap tentang mekanisme kerja ransomware.
5. Dapat mengetahui pola aktivitas dan bagaimana ransomware wanncry dapat mengeksploitasi dan mengenkripsi seluruh file pada komputer korban. Terutama dalam hal ini sistem operasi windows sebagai subjek percobaan.
6. Perubahan trafik *performance* yang terjadi pada PC yang disisipkan *malware* semakin lama semakin cepat tetapi pada *performance* di *network* semakin melemah *(loading).*
7. WannaCry tidak bekerja karena adanya sinkholed sehingga malicious code tidak tereksekusi
8. Program WannaCry bisa dijadikan services dan melakukan eksploitasi SMB

DAFTAR PUSTAKA

[1] Adib, Avon & Ahmad. Analisis Dampak *Malware* Terhadap Trafik Jaringan dengan Teknik *Deteksi Behavior-based.* Jurnal *Telkom University*

[2] Waskito, Avon & Adityas. Analisa Malware Pada Traffic Jaringan Data Menggunakan Wireshark. Jurnal Telkom University

[3] Maxat, Vassilions, Ioannis & Michael *Static and Dynamic Analysis of WannaCry Ransomware*

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

[5] Triawan, Victor & Darmawan (2017). Analisis dan Deteksi Malware Menggunakan Metode Malware Analisis Dinamis dan Malware Analisis Statis. JUSTINDO, Jurnal Sistem & Teknologi Informasi Indonesia, Vol. 2, No. 1, Februari 2017

[6] J. Ismail, “Analisa Malware Metode Statik | Jul Ismail,” 2016.

[7] Y. S. Kim, E. Wang, and H. M. Rho, “Geometry-based machining precedence reasoning for feature-based process planning,” *Int. J. Prod. Res.*, vol. 39, no. 10, pp. 2077–2103,2001.

[8] M. Sikorski and A. Honig, "Practical Malware Analysis", The Hands-On Guide to Dissecting Malicious Software.

[9] (Adenansi & Novarina, 2017). Malware dynamic. JoEICT (Journal of Education And ICT), 1(1).

[10] Anjana TK (2017). *Discussion On Ransomware, Wannacry Ransomware and Cloud Storage Services Against Ransom Malware Attacks.* IJRTI, *International Journal for Research Trends and Innovation (*www.ijrti.org*)*, Vol 2, Issue 6, ISSN:2456-3315

[11] https://www.esecurityplanet.com/malw-are/types-ofransomware.html

[12] Gandhi Krunal A., Patel Viral Kumar D. “Survey on Ransomware: A New Era of Cyber Attack”

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

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