Jurnal Informatika: Jurnal Pengembangan IT (JPIT), Vol.03, No.03, September 2018 ISSN: 2477-5126
DOI: 10.30591/jpit.v3i3.1019 e-ISSN: 2548-9356

Analysis *Malware Flawed Ammyy RAT* Dengan Metode *Reverse Engineering*

Tesa Pajar Setia[1*)], Nur Widiyasono[2], Aldy Putra Aldya[3]
[1]Jurusan Informatika, Fakultas Teknik, Universitas Siliwangi, Tasikmalaya
[1]Jln. Siliwangi no 24, Kota Tasikmalaya, 46115, Indonesia
email: [1]tesa.paja14@student.unsil.ac.id, [2]nur.widiyasono@unsil.ac.id, [3]aldy@unsil.ac.id

Received: 30 Juli 2018; Revised: 1 Oktober 2018; Accepted: 20 Oktober 2018
Copyright ©2018, Politeknik Harapan Bersama, Tegal

***Abstract* – Malware is currently growing rapidly, diverse and complex. But, human resources that can carry out malware analysis is limited, because special expertise is needed. Reverse engineering is one of many solution that can carry out malware analysis, because reverse engineering techniques can reveal malware code. On March 5, 2018, found spam email containing files, the file contained malware flawed ammyy. This flawed ammyy is a software that comes from Ammyy Admin version 3 and then misused by hackers TA505. This study aims to identify the malware, especially the Flawed Ammyy RAT malware. This research uses descriptive methodology, then to do malware analysis used dynamic analysis and reverse engineering methods. The results of the study show that the Flawed Ammyy RAT malware works by hiding in the Ammyy Admin application then connecting to the attacker with ip address 103.208.86.69. netname ip address 103.208.86.69 is zappie host. There are 50 registry changes that are carried out by malware on infected systems. After the attacker has been connected with the victim, the attacker can easily do the remote control without the victim's knowledge.**

***Abstrak* – *Malware* saat ini berkembang dengan pesat, beragam dan komplek. Namun kurangnya sumber daya manusia yang dapat melakukan analisis *malware* karena diperlukan keahlian khusus. *Reverse engineering* merupakan salah satu solusi untuk melakukan analisis *malware* karena menggunakan teknik *reverse engineering* kode pada *malware* dapat diketahui. 5 Maret 2018 ditemukan *spam email* yang berisi *file, file* tersebut terdapat *malware flawed ammyy*. *Flawed ammyy* ini merupakan *software* yang berasal dari *Ammyy Admin* versi 3 kemudian disalah gunakan oleh *hacker* TA505. Penelitian ini bertujuan untuk melakukan proses identikasi *malware* kususnya *malware Flawed Ammyy RAT*. Penelitian ini menggunakan metodologi deskriptif, kemudian untuk melakukan analisis *malware* digunakan metode analisis dinamis dan *reverse engineering*. Hasil dari penelitian menunjukan bahwa *malware Flawed Ammyy RAT* bekerja dengan bersembunyi pada aplikasi *Ammyy Admin* kemudian melakukan koneksi dengan *attacker* dengan ip *address* 103.208.86.69. *netname ip address* 103.208.86.69 adalah *zappie host*. Perubahan 50 *registry* yang dilakukan *malware* pada system yang terinfeksi. Setelah *attacker* terkonesi dengan korban maka *attacker* dengan mudah melakukan *remote control* tanpa sepengetahuan korban.**

Kata Kunci – Ammyy, Flawed, Engineering, Malware, Reverse

*) **Corresponding author**: (Tesa Pajar Setia)
Email: tesapajarsetia27@gmail.com

I. PENDAHULUAN

Internet telah menjadi bagian penting dari kehidupan sehari-hari bagi orang-orang. *Internet* dapat membantu seseorang memanfaatkan banyak layanan hanya dengan bantuan beberapa klik [1]. Tingginya penggunaan *internet* menciptakan kejahatan tak hanya terjadi dalam dunia nyata, tetapi merambah ke dunia maya yang sering disebut sebagai *cybercrime* [2]. Kejahatan di dunia *cyber* saat ini beragam. Teknik yang digunakan oleh penyerang semakin beragam dan kompleks. Berbagai serangan tersebut diantranya melibatkan *malicious software* atau yang biasa disebut *malware* yang merupakan suatu program jahat [3]. Beragam tujuan yang dimiliki para pelaku ini beberapa diantaranya adalah untuk mencari kesenangan dan mencari keuntungan [4].

Malware diciptakan dengan maksud tertentu yaitu melakukan aktifitas berbahaya yang berdampak sangat merugikan bagi para korbannya, antara lain seperti penyadapan serta pencurian informasi pribadi [5]. *Malware* dapat berisi kode berbahaya seperti *Virus, Worm, Trojan Horse*, juga bisa membuat *Back Door* yang dapat melakukan pencurian informasi pribadi atau mengambil kendali sistem seseorang [6]. Seringkali *malware* masuk ke sistem melalui *file* yang diunduh. Setelah *malware* memasuki sistem, *malware* melakukan aktivitas dan merusak seluruh sistem [7].

Kemampuan untuk melakukan analisa *malware* bagi seorang *investigator* menjadi tuntutan dalam setiap melakukan investigasi. Meningkatnya sejumlah *malware* serta evolusi dan mampu beradaptasinya terhadap perangkat analisis yang selama ini digunakan [8]. Analisa *malware* dengan menggunakan *Reverse engineering* merupakan salah satu solusi yang bisa digunakan saat ini. *Reverse engineering* dalam analisis *malware* berguna untuk ekstraksi data yang memuat informasi yang ada didalam *malware* [9].

Para analis Proofpoint telah menemukan *Trojan* akses jarak jauh yang sebelumnya tidak terdokumentasi yang disebut *Flawed Ammyy RAT* [10]. *Malware Flawed ammyy* dibangun diatas kode *Ammyy admin*versi versi 3 yang disalah gunakan. *Ammyy admin* merupakan perangkat lunak desktop jarak jauh yang digunakan diantara jutaan konsumen dan bisnis untuk menangani *remote control* dan *diagnosis* pada platfom *Windows*, ini bukan pertama kalinya *Ammyy admin*disalahgunakan, serangan Juli 2016 juga menggunakannya untuk menyembunyikan *malware* [11].

Penyerang yang mendistribusikan *Flawed ammyy* remote control trojan melalui kelompok peretas TA505 yang terkenal karena mendistribusikan kampanye spam besar seperti *Trojan Dridex* perbankan, *Locky ransomware*, dan *Jaff ransomware*. [12]

II. PENELITIAN YANG TERKAIT

Penelitian yang telah dilakukan sebagai dasar mengenai penelitian ini diantaranya [13] menjelaskan penggabungan dari dua metode analisis *malware* yaitu analisis statis dan analisis dinamis mampu memberikan gambaran yang lebih lengkap tentang karakteristik dari *malware* TT.exe. *Malware* TT.exe adalah *malware* tipe *trojan*, dibuat pada hari Rabu 30 Juli 2014, menargetkan windows 7 dan windows 8.

Peneltian [1] melakukan analisis statis dan analisis dinamis pada *malware DrakComet*. Hasil dari penelitian ini adalah menguraikan metodologi yang efektif dan efisien yang dapat diterapkan untuk meningkatkan kinerja deteksi dan penghapusan *malware* yang dikumpulkan. Analisis dinamis cara terbaik untuk melakkan analisis sample *malware*.

Penelitian [14] menjelaskan hasil komparasi terhadap metode analisis *malware* statis. Peneliti melakukan ekstraksi 11 vektor kelompok kecil untuk 600 *malware*, dan berhasil mengklasifikasikan lebih dari setengah kode ke dalam kelompok yang sesuai menggunakan vektor. Pemeriksaan yang cermat pada kode biner juga menegaskan bahwa vektor bit telah mengklasifikasikannya dengan cara yang benar. Hasil eksperimen menunjukkan bahwa bit vektor dapat digunakan secara efektif untuk melakukan analisis malware statis, dan bahwa vektor bit grup dapat membantu mengklasifikasikan malwares ke dalam kelompok yang sesuai.

Penelitian [9] melakukan proses *reverse engineering* pada *malware Biscuit*. Hal mendasar dari cara kerja *malware* tersebut adalah adanya auto request untuk koneksi ke ip tertentu yaitu ip pada alamat: 114.101.115.115. Selanjutnya proses *reverse engineering* melalui penulusuran perintah: ***bdkzt, ckzjqk, download, exe, exit*** dan ***lists*** telah dapat memetakan bagaimana cara kerja dari *malware* Biscuit.

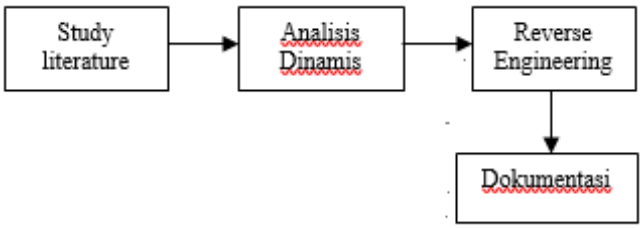
Peneliti [15] melakukan *reverse engineering* untuk membedah *kode ransomware* kemudian analisis lebih lanjut. Hasil menunjukkan bahwa meskipun penggunaan enkripsi tangguh, seperti *ransomware* lain menggunakan serangan yang sama struktur dan primitif kriptografi. Analisis menuntun pada kesimpulan bahwa strain ransomware ini tidak serumit dilaporkan sebelumnya. Analisis praktis terperinci ini mencoba meningkatkan kesadaran kepada komunitas bisnis tentang realitas dan Pentingnya keamanan TI sementara mengisyaratkan pencegahan, pemulihan dan keterbatasannya.

Peneliti [16] melakukan *reverse engineering* pada *malware botnet*. Tujuan utama dari penelitian ini adalah untuk menentukan pendekatan yang paling memadai untuk menciptakan kembali insiden *botnet*. Gangguan jaringan pada proses ini, aktivitas *online* ilegal dan pencurian data organisasi dapat dicegah dan bahkan bot sistem *Intrusion Prevention* spesifik dapat dikembangkan. Ini juga menjamin aliran data yang dikonfirmasi dalam ruang digital oleh komunikasi e-*governance* yang diasuransikan untuk setiap negara dari terorisme *cyber*.

Hasil dari studi literatur yang telah dilakukan, jika dibandingkan dengan penelitian kali ini, analisis terhadap sample malware Flawed ammyy RAT menggunakan analisis dinamis dengan tambahan membuat virtual network pada virtual mesin agar system terlihat melakukan koneksi pada suatu jaringan. *Reverse engineering* yang dilakukan sebelumnya menggunakan teknik *debugger* dan *assembler* sedangkan penelitian kali ini menggunakan *disassembler*.

III. METODE PENELITIAN

Metodologi yang digunakan pada penelitian ini menggunakan metodologi deskriptif dengan alur seperti pada Gbr 1 sebagai berikut:

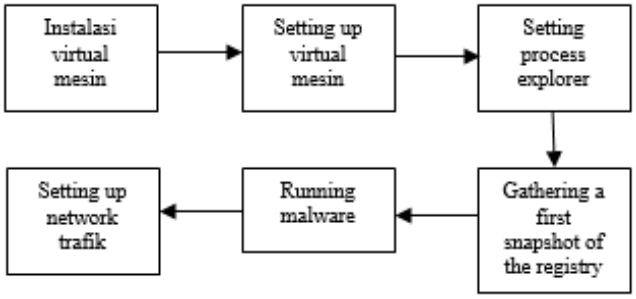


Gbr. 1 Alur penelitian

A. *Studi Literature*

Study literature uraian tentang teori, temuan, dan bahan penelitian lainnya yang diperoleh dari bahan acuan untuk dijadikan landasan kegiatan penelitian untuk menyusun kerangka pemikiran yang jelas dari perumusan masalah yang ingin diteliti. Bahan acuan yang digunakan adalah jurnal-jurnal dan buku mengenai analisis *malware* dan *reverse engineering malware*.

B. *Analisis Dinamis*



Gbr. 2 Alur metode analisis dinamis

1) *Instalasi virtual mesin*

Menentukan ruang lingkup, penelitian ini mengkhususkan pada ruang penelitian yang akan dilakukan pada lingkungan aman dimana menggunakan lingkungan *virtual* untuk pengujian sample virus. Lingkungan mesin *virtual* atau yang dikenal dengan *virtual mechine* (VM). *Spesifikasi* yang akan di gunakan sebagai penelitian adalah sperti pada Tabel I.

TABEL I
SPESIFIKASI KOMPUTER

No	Uraian	Spesifikasi
1	Sistem operasi	*Windows 7 Ultimate 32-bit (6.1, Build 7601) Service Pack 1*
2	Prosesor	*Intel(R) Core(TM) i3-2350M CPU @ 2.30GHz (4 CPUs), ~2.3GHz*
3	Memory	4GB RAM
4	Hardisk Capacity	500

TABEL II
SPESIFIKASI *VIRTUAL*

No.	Uraian	Spesifikasi
1	Aplikasi VM	Virtual Box
2	Sistem operasi	Windows7
3	Memori	30MB / 1GB RAM
4	Processor	*Single core*

Tabel I dan Tabel II merupakan spesifikasi lab yang digunakan untuk membuat vitual mesin yang digunakan untuk melakukan analisis *malware*.

2) Setting up virtual network

Setting up virtual network menggunkana *tools ApateDNS. ApateDNS* untuk melihat apakah permintaan *DNS* dilakukan. *ApateDNS* memalsukan respons *DNS* ke alamat *IP* yang ditentukan pengguna pada komputer lokal, ini menanggapi permintaan *DNS* dengan respons *DNS* diatur ke alamat *IP* yang ditentukan. *ApateDNS* dapat ditampilkan hasil heksadesimal dan *ASCII* dari semua permintaan yang diterimanya.

3) Starting process explorer

Monitoring process menggunakan *process Hacker* 2.39, *Process Hacker* 2.39 menunjukan informasi tentang penanganan dan proses *DLL* yang telah berjalan. Pembahasan lengkap untuk analisis menggunakan *Process Explorer* 2.39 akan dilakukan pada langkah berikutnya.

4) Gathering first snapshot of the registry

Analisis berikutnya adalah memonitor perubahan pada registri. Hasil dari *Regshot* 1.9.0 ini bisa dipilih, berupa *file* teks atau HTML, yang menunjukkan berapa jumlah perubahan registri dan apa serta dimana saja perubahan tersebut. Pembahasan lengkap untuk analisis menggunakan *Regshot* akan dilakukan pada langkah selanjutnya.

5) Running malware

Dalam tahap ini dilakukan pengujian dengan menjalankan sampel *file malware* (*Flawed Ammy RAT*) pada *virtual* lab, sehingga dapat menghasilkan informasi mengenai perilaku apa saja yang dilakukan oleh *malware* terhadap sistem ketika *file* tersebut dijalankan. *Malware Flawed Ammy rat* ini *file exe* maka menjalankannya dengan double clik *malware* tersebut.

6) Setting up network traffic

Monitoring lalu lintas jaringan, *WireShark* karena memiliki tampilan antarmuka (GUI) dan fitur filtrasi sehingga sangat mudah dalam penggunaannya. *WireShark* sudah cukup untuk meneliti paket yang berada pada jaringan yang mungkin dikirim oleh *malware*. Analisis menggunakan *WireShark* untuk pembahasan lengkap akan dilakukan pada langkah selanjutnya.

C. Reverse engineering

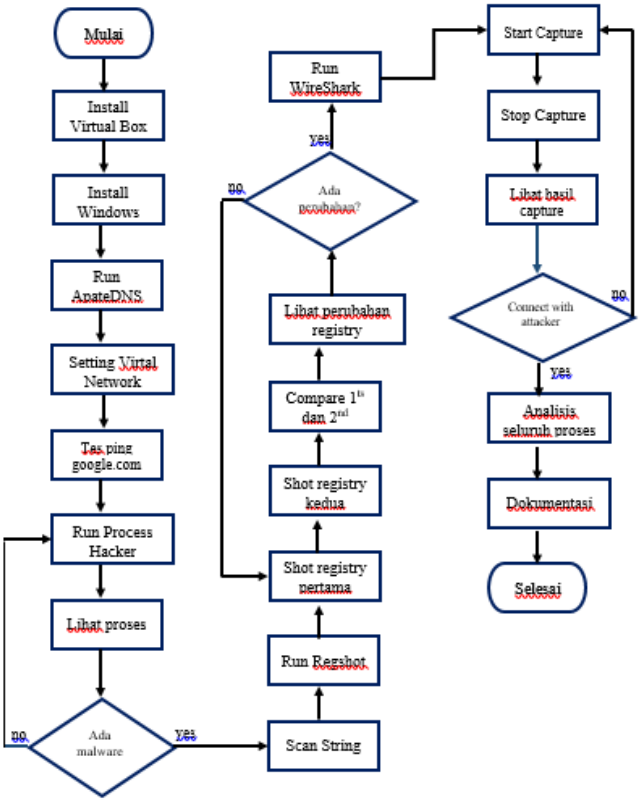
Proses *disassembly* digunakan dalam teknik *Reverse engineering* untuk menerjemahkan dari bahasa mesin ke bahasa yang mudah dimengerti manusia, yaitu bahasa *assembly* [9].

D. Dokumentasi

Dokumentasi menyimpan hasil keluaran data dari pengolahan proses scan dari sample *malware* dari berbagai *software* analisis, untuk kemudian diterapkan pada jurnal penelitian.

IV. HASIL DAN PEMBAHASAN

A. Analisis dinamis



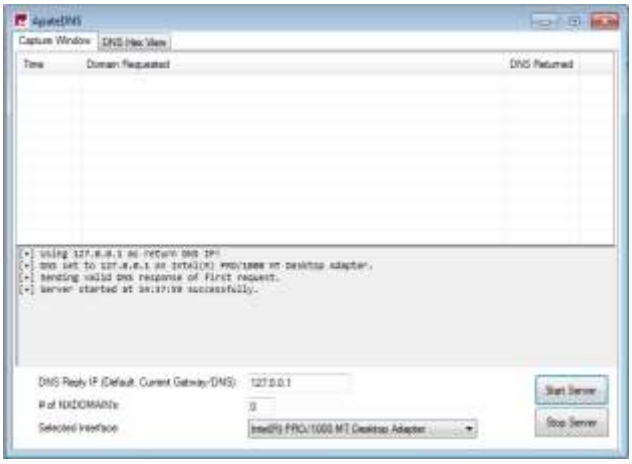
Gbr. 3 flowchart analisis dinamis

Pada Gbr. 3 menunjukan bagaimana cara melakukan analisis dinamis khususnya analisis *malware flawed ammyy RAT*. Sesuai Gbr.3 penjelasan lebih lengkap sebagai berikut:

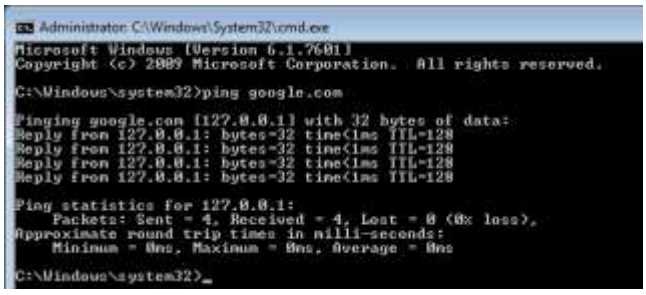
1) Instalasi Virtual Mesin

Penggunaan sistem pada *virtualbox* yaitu *operating system* yang digunakan menggunakan *windows7*, kemudian untuk *memory* yang di berikan yaitu sebesar 512MB dan 1 buah *processor* dengan kapasitas penyimpanan yaitu 30GB, untuk jaringan yang digunakan tidak dianjurkan untuk menggunakan *network Bridge conection* ataupun *Host-only*

conection, dikarenakan pada *bridge connection* jaringan akan secara langsung terhubung dengan jaringan komputer fisik. *Network* yang digunakan pada praktek penelitian ini yaitu NAT pada jaringan merupakan langkah aman untuk melakukan uji coba karena pada prakteknya data tidak akan langsung dikirimkan pada komputer fisik data yang dikirim harus melalui perangkat NAT dan Firewall terlebih dahulu.



Gbr. 4 *ApateDNS*



Gbr .5 Ping google pada cmd *virtual* mesin

2) Setting up virtual network

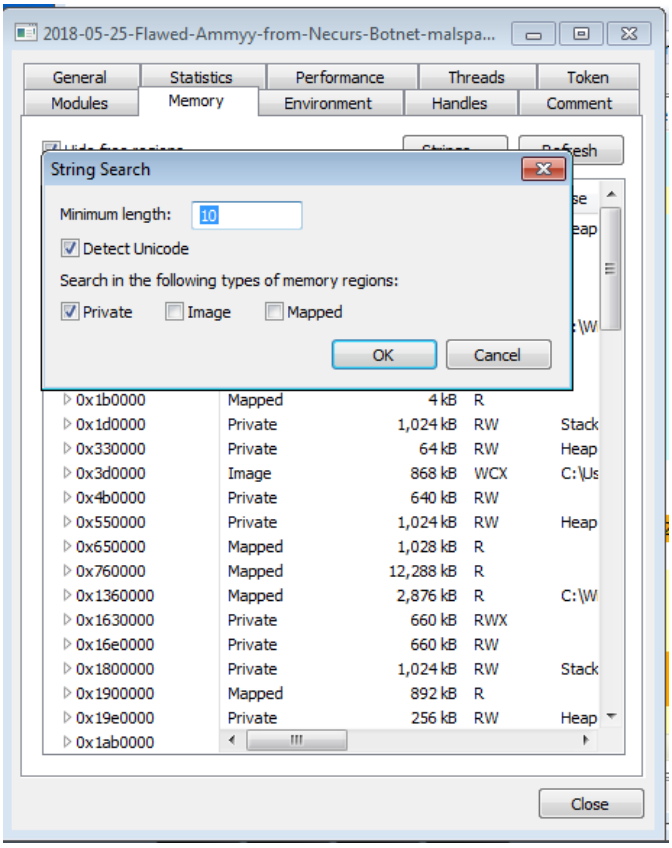
Tools yang digunakan untuk proses setting up *virtual network* menggunakan *ApateDNS*. *ApateDNS* ini telah diinstal pada *virtual* mesin selanjutnya DNS *reply* ip di ubah menjadi ip address *localhost* yakni 127.0.0.1 kemudian tekan tombol *start server* seperti pada Gbr 4. Mengetahui apakah setting up *virtual* mesin ini berhasil atau tidak, buka CMD pada lab *virtual* mesin tersebut kemudian *ping* ke alamat *google.com* seperti pada Gbr 5. Hasil dari Gbr 5 menunjukan bahwa *virtual network* telah berhasil dilakukan setting up, ini terbukti dengan ketika dilakukan *ping google* pada cmd ip address yang dituju menuju ip addres yang telah dilakukan *setting up* pada *ApateDNS*.

3) Starting process explorer

Tahap *staring process* explore ini menggunakan tools *process hacker* versi 2.39. *Process Hacker* merupakan aplikasi untuk menampilkan proses apa saja yang dijalankan, untuk kelebihan aplikasi ini portable yang tidak membutuhkan proses instalasi. Aplikasi ini memiliki fitur yang hampir sama dengan *process explorer* dan memiliki semua fungsionalitas yang diberikan *Process Explorer*, namun memiliki banyak kelebihan, salah satu contohnya mempunyai fitur scan *string* yang lebih, mengijinkan melihat thread apa yang berjalan, dan informasi detai lainnya.

Tahap selanjutnya *malware Flawed Ammyy RAT runnig*. Setalah *malware* tersebut dilakukan *runnig* lihat proces pada *process hacker* seperti pada Gbr 6.

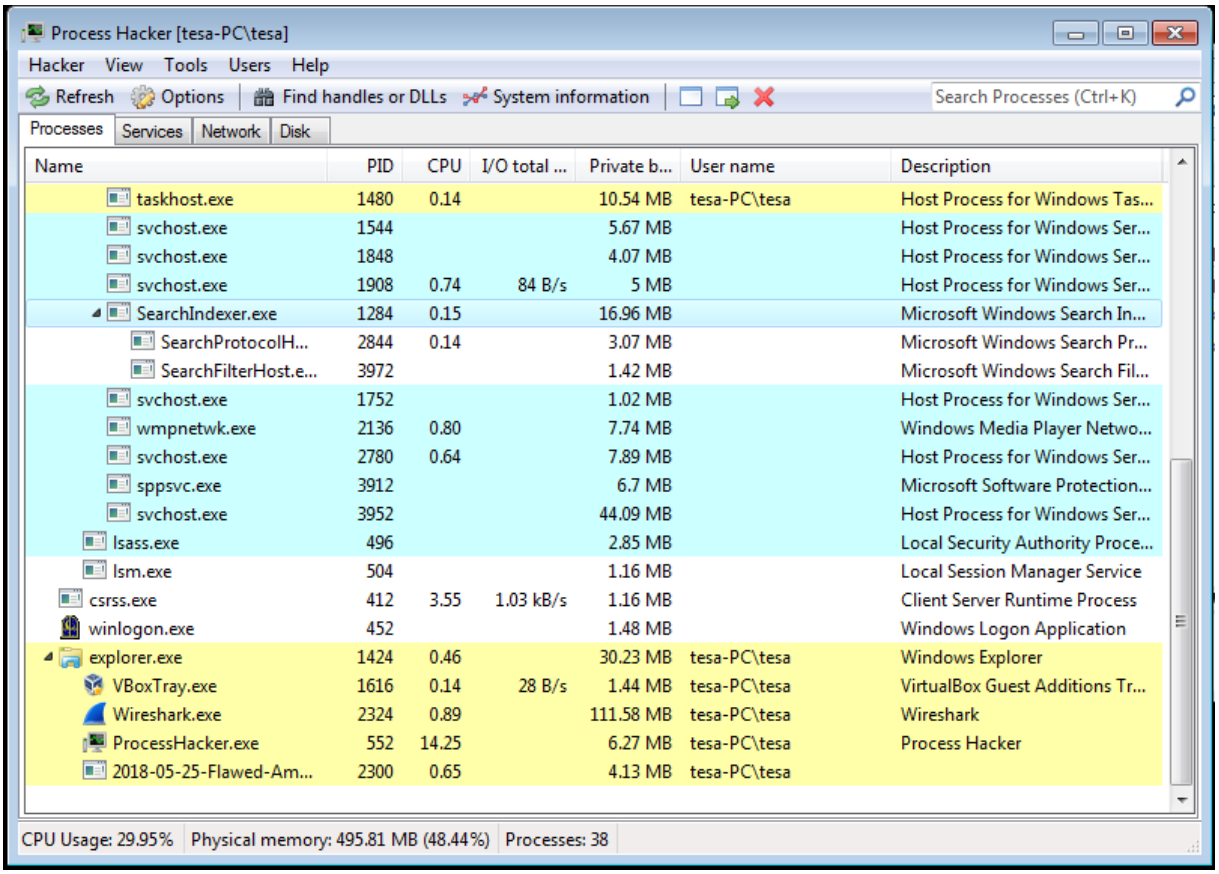
Merujuk pada Gbr 6 *malware* berjalan dengan *no pid* 2300 dengan menggunakan 0.65 proces pada cpu *virtual* dengan besar *file* 4.13MB. Informasi lebih detail dapat menggunakan fitur lain yang ada pada *process hacker* contohnya ialah *scan string*, yang akan ditunjukan pada Gbr 7.



Gbr 7 tampilan *string* search pada fitur *process hacker*

Merujuk Gbr 7 untuk mencari proses yang berupa *string* atau kata yang terdapat pada file Little.dll yang telah berjalan menggunakan *process hacker* dapat ditemukan pada *properties -> memory -> string*.

Hasil data informasi yang didapat dari *malware* teserbut cukup banyak, berikut sebagian informasi aktivitas *malware* yang terdapat pada sampel *malware Flawed Ammyy RAT* yang diteliti diunjukkan pada tabel III sebagai berikut:



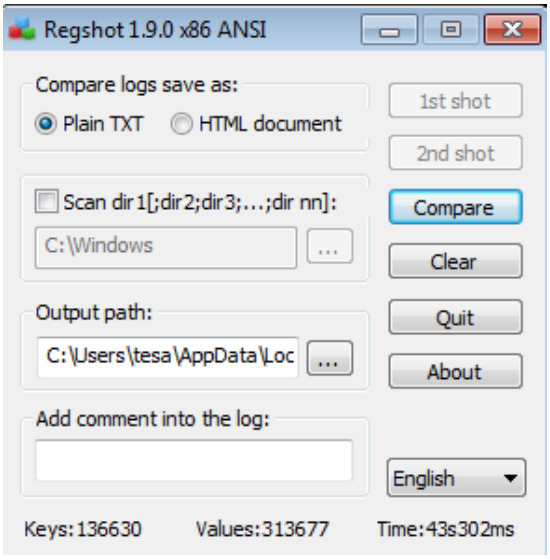
Gbr. 6 Tampilan process hacker setelah runnig malware

Tabel III merupakan hasil string *malware Flawed Ammyy* menggunakan *tool proses hacker. String* tersebut menunjukkan bagaimana *malware flawed ammyy* berjalan pada system.

4) Gathering first snapshot of the registry

Tools yang digunakan untuk melakukan *gathering a first snapshot of the registry* menggunakan *Regshot* versi 1.9.0. *Regshot*, *monitoring* perubahan pada *registry* menggunakan aplikasi *regshot*. Hasil keluaran dari *Regshot* menunjukkan berapa jumlah perubahan registri dan apa serta di mana saja perubahan tersebut ditunjukkan pada Gbr 8.

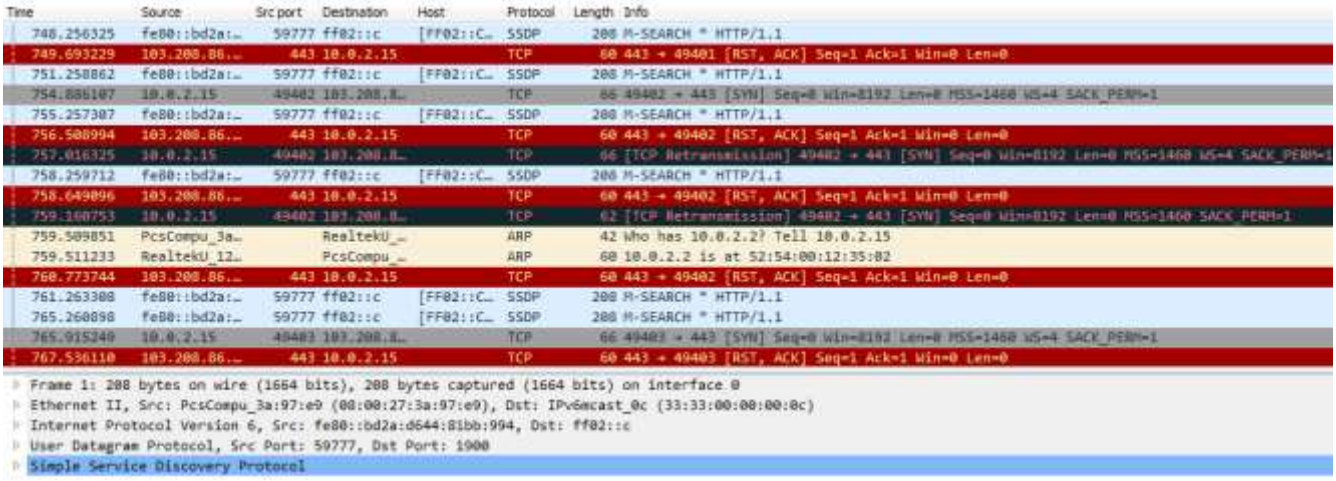
Hasil dari *shot* registry pertama sebelum *malware* dijalankan dengan *shot* registry setelah *malware* dijalanakan terlihat ada beberapa perubahan registry pada sistem operasi setelah *malware* di jalankan, total perubahan adalah 50 perubahan, dimana 2 penghapusan keys, 5 penambahan keys, 4 penghapusan values, 9 penambahan values dan 30 perubahan values pada registry.



Gbr. 8 Tampilan *Regshot*

TABEL III
STRING MALWARE FLAWED AMMYY RAT

No.	Address dan Result	Keterangan
1	*0x2f1b6b !This program cannot be run in DOS mode.*	*Malware* tidak dapat berjalan ketika mode DOS
2	*0x2f2ec2 kernel32.dll*	Windows NT BASE API Client DLL
3	*0x2f2f2b LoadLibraryA*	*Malware* memuat modul yang ditentukan ke dalam ruang alamat dari proses panggilan
4	*0x2f2f38 GetProcAddress*	*Malware* mengambil alamat fungsi atau variabel yang diekspor dari pustaka *dynamic-link* yang ditentukan
5	*0x2f2f47 VirtualAlloc*	*Malware* mengubah keadaan suatu wilayah halaman di ruang alamat *virtual* dari proses panggilan
6	*0x2f2f54 VirtualProtect*	*Malware* mengubah perlindungan akses proses apa pun pada lingkungan *virtual*
7	*0x2f2f98 FreeConsole*	*Malware* melepaskan proses panggilan dari konsolnya
8	*0x3b0f93 ComSpec=C:\Windows\system32\cmd.exe*	*Malware* membaca spesifikasi komputer korban
9	*0x3b0fb7 FP_NO_HOST_CHECK=NO*	*Malware* melakukan cek apakah ada *host* atau tidak
10	*0x3e6660 Security=Impersonation Dynamic True*	*Malware* menjalakan peniruan pada security
11	*0x3e8194 Ammyy Admin*	Menjalakan perintah dasar ammyy admin
12	*0x3edc50 103.208.86.69*	Ip address tujuan
13	*0x3fe1f0 NT Authority\NetworkService*	*Malware* melakukan pengaturan akses keamanan untuk folder bersama pada jaringan
14	*0x3fe7a4 root\SecurityCenter2*	*Malware* masuk ke root kemudian melakukan akses ke security center 2
15	*0x4098d4 Remote Desktop Services*	*Malware* mejalankan service remote desktop
16	*0x40a2f6 windows_tracing_logfile=C:\BVTBin\Tests\installpackage\csilogfile.log*	*Malware* mencoba membaca *log* pada komputer yang terinfeksi
17	*0x40efed id=52399915&os=7 SP1 x86&priv=User+UAC&cred=tesa-PC\tesa&pcname=TESA-PC&avname=&build_time=25-12-*	*Malware* menyimpan data yang ada pada komuter yang terinfeksi, seperti operasi sistem, *user*, dan *pc name*
18	*0x482c94 ERROR: Couldn`t connect to router 103.208.86.69:443*	*Malware* tidak dapat koneksi pada router tujuan karena ketika proses analisis jaringan pada komputer telah dilakukan *virtual network*



Gbr. 9 Hasil *capture WireShark* terhadap paket data *malware*

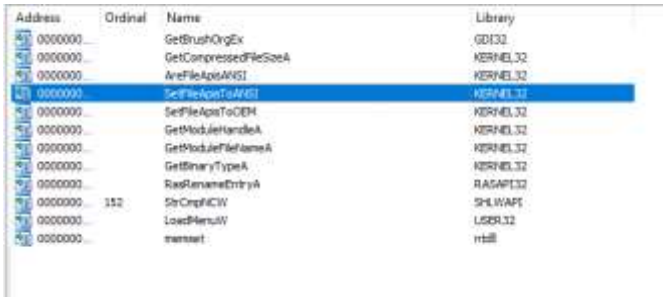
5) Setting up network trafik

WireShark, sebagai alat *software monitoring* dan juga analisis jaringan, menangkap paket secara *real time* dan menampilkannya dalam format yang dapat dibaca. Aplikasi ini digunkan dalam penelitian untuk mengetahui aktivitas *malware* terhadap jaringan.

Merujuk dari gambar 9 hasil capture *WireShark* dapat dilihat bahwa pc atau komputer *virtual* mesin yang terinfeksi *malware Flawed Ammyy RAT* dengan ip address 10.0.2.15 selalu melakukan singkron terhadap ip address 103.208.86.69 yang telah di jelaskan sebelumnya pada tahap *starting process explore* dimana ip address ini merupakan ip address router *attacker*. Dilihat pada gambar 4.10 *virtual* mesin hanya bisa melakukan sinkron terhadap *attacker* ini karena jaringan yang telah dilakukan *virtual network*, *malware* tidak dapat melakukan komunikasi atara *malware* dengan *router attacker*.

B. Reverse engineering

Proses *disassembler* ini menggunakan tools *IDAPro* Setelah *malware* terbuka selanjutnya adalah melakukan analisa *command* yang ada didalam *malware*. Berikut ini adalah gambar hasil disassembler malware menggunakan tools IDAPro ditunjukkan pada Gbr.10.



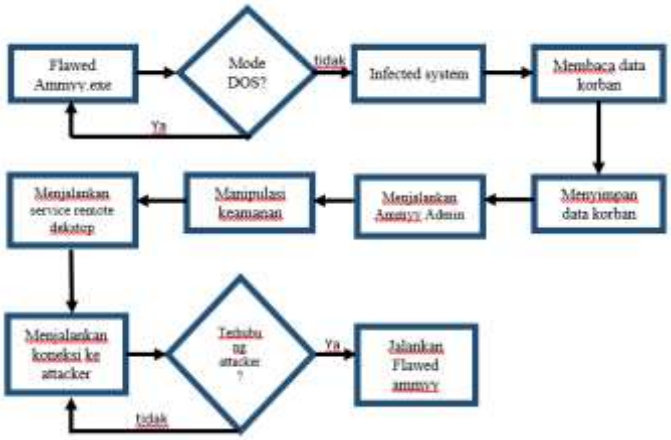
Gbr. 10 Disassembler malware Flawed Ammyy RAT

Pada Gbr.10 menunjukkan malware flawed ammyy RAT menggunakan 12 function untuk melakukan infeksi dan melakukan penyerangan pada system yang telah terinfeksi *malware flawed ammyy rat*. 12 function tersebut dijelaskan pada Tabel IV.

TABEL IV
HASIL DISSEMBLER

Hasil *dissembler*	Keterangan
BOOL_stdcall Get GetBrushOrgEX(HDC hdc, LPPOINT lppt) *extrn GetBrushOrgEX:dword*	*Malware* memamnggil *function* tersebut untuk mengambil alih fungsi pointer agar dapat mempermudah pencurian data.
DWORD_stdcall GetCompressedFileSizeA (LPCSTR lpFileName, LPDWORD lpFileSizeHigh) *extrn GetCompressedFileSizeA:dword*	*Malware* memanggil *function* diatas untuk melakukan proceses *compress file* tertentu kemudian menyimpannya.
BOOL _stdcall AreFileApisAnsi () *extrn AreFileApisAnsi:dword*	Perintah dengan *function* tersebut *malware* dapat menentukan apakah fungsi *file* I / O menggunakan halaman kode karakter ANSI atau OEM.
Void _stdcall SetFileApisToAnsi() *extrn SetFileApisToAnsi:dword*	*Function* tersebut *malware* dapat membuat *file* I / O berfungsi untuk menggunakan halaman kode set karakter ANSI untuk proses saat ini. Fungsi ini berguna untuk operasi input dan output masukan 8-bit.
Void _stdcall SetFileApisToOEM() *extrn SetFileApisToOEM:dword*	*Function* tersebut dapat membuat *file* I / O berfungsi untuk proses untuk menggunakan halaman kode karakter set OEM. Fungsi ini berguna untuk operasi input dan output masukan 8-bit.
HMDULE_stdcall GetModuleHandleA(LPCSTR lpModuleName) *extrn GetModuleHandleA:dword*	*Malware* dengan *function* tersebut memilih *file* yang memenuhi syarat yang mengandung modul tertentu.
DOWRD_stdcall GetModuleFileNameA(HMODULE hModule, LPSTR lpFilename, DOWRD nSize) *extrn GetModuleFileNameA:dword*	*Malware* dengan *function* tersebut dapat meneangani modul yang telah ditentukan
BOOL_stdcall GetBinaryTypeA(LPCSTR lpApplictionName, LPDWORD lpBinaryType) *extrn GetBinaryTypeA:dword*	*Function* tersebut *malware* dapat menentukan apakah *file* dapat di eksekusi, jika ia subsistem mana yang menjalankan *file* yang dapat dieksekusi
DWORD_stdcall RasRenameEntryA(LPCSTR, LPCSTR LPCSTR) *extrn RasRenameEntryA:dword*	*Malware* dengan *function* RasRenameEntry dapat mengubah nama entri di buku telepon.
extrn StrCmpNCW:dword	M*malware* dapat membandingkan nomor spesifik sejumlah karakter dari awal dua string menggunakan C *run-time* (ASCII)
HMENU_stdcall LoadMenuW(HINSTANCE hInstance, LPCWSTR lp MenuName) *extrn RasRenameEntryA:dword*	*Malware* dapat memuat sumber daya menu yang spesifik dari *file* yang dapat *executable* (.exe) yang terkait dengan *instance* aplikasi.
*void _cdecl memset(void *Dst, int Val, size_t Size)* *extrn _imp_memset:dword*	*Malware* melakukan setel *buffer* ke karakter yang ditentukan

C. Malware workflow



Gbr. 11 proses dari *malware* Flawed Ammyy RAT

Merujuk pada Gbr 11 cara kerja *malware Flawed Ammyy RAT* sebagai berikut:

1) *Malware* yang telah dijalankan akan melakukan infected pada sistem. *Malware* akan membaca data yang ada pada komputer korban, seperti operasi sistem yang digunakan, *user*name, dan PC name, kemudian *malware* akan menyimpan data tersebut.

2) *Malware* akan menjalankan perintah dasar ammy admin selain sebagai remote access, menjalakan *ammyy admin*ini bertujuan untuk memanipulasi keamana seolah-olah *ammyy admin* yang berjalan pada sistem.

3) *Malware* selanjutnya akan melakukan koneksi dengan *server attacker*. *Malware* akan melakukan sinkron dengan *server* terlebih dahulu, setelah sinkron *server* akan merespon. *Malware* akan mengirimkan data spesifikasi yang dimiliki komputer korban, seperti operasi *system*, *user* dan *pc name*.

D. Pencegahan malware

1) Proses pencegahan untuk melindungi *mail server* dari serangan *malware* agar *mail server* tidak terinfeksi *malware* dan *malware* tidak akan melakukan *broadcast malware spam* pada sistem, bagi para *administrator server* dapat melakukan hal-hal berikut ini:

- *Admin* lakukan update *firewall versi* terbaru
- *Admin* menggunakan *Antispam* pada mail server, contoh tools antispam seperti *zero bounce, spam titan, barracuda spam firewall*, dan lain-lain
- *Admin* lakukan konfigurasi *mail relay*, hindari *relay* terbuka bagi pengirim *spam* dengan menentukan *domain* atau alamat ip mana yang akan digunakan oleh *mail server*
- *Admin* lakukan *Encryption* pada *encrypt POP3, IMAP authentication*, gunakan *SSL* dan *TLS*
- *Admin* lakukan Koneksi dan *default setting* untuk menghindari serangan *DOS*, batasi jumlah koneksi dan kesalahan otentikasi yang akan diterima oleh system, hapus fungsi *server* tidak dibutuhkan dengan melakukan nonaktif pada pengaturan default yang tidak diperlu.
- System miliki *mail server* khusus dan memindahkan layanan lain seperti FTP ke server lain,
- *Admin* lakukan *control access* untuk melindungi *mail server*, terapkan *authentication* seperti *authentication SMTP* pengguna harus memberi *username* dan *password* untuk dapat melakukan pengiriman melalui *server*
- *Admin* lakukan periksa daftar *DNS-based blacklists (DNSBL)* dan tolak *email* dari *domain* atau IP apapun yang terdaftar didalamnya
- *Admin* lakukan periksa *URL Real-Time blocklists* dan tolak pesan berisi tautan tidak *valid* atau berbahaya
- *Admin* lakukan *maintain blacklists* dan *block IP* yang secara khusus menyerang *mail server* Pemulihan system setelah terinfeksi malware

2) Proses pencegahan untuk melindungi pengguna dari serangan *malware* agar data pengguna aman dari serangan *malware* khususnya malware Flawed Ammyy RAT, bagi para pengguna dapat melakukan hal-hal berikut:

- Pengguna tidak membuka *email* dari pengirim yang tidak dikenal
- Pengguna tidak mudah percaya apabila tiba-tiba menerima *email* dari pengirim yang dikenal
- Pengguna tidak melakukan unduhan *file* yang mencurigakan dan dari sumber yang mencurigakan
- Pengguna tidak melakukan klik *link phising*. Domain yang mirip sering digunakan *hacker* untuk menjebak *user* yang kurang berhati hati, kurang cermat. *Phishing* yang paling sering ditemui biasanya adalah phising pada akun media sosial, situs palsu tersebut tersebar dengan menggunakan foto-foto porno, memancing korban untuk melakukan kilk, tidak jarang foto tersebut menyerupai sebuah video yang siap di klik. maka dari itu sebaiknya cermati lagi alamat tujuannya.
- Pengguna melakukan *install antivirus* dan aktifkan *antivirus*
- Pengguna lakukan pindai komputer secara berkala

E. Ciri-ciri komputer terinfeksi malware Flawed Ammyy RAT

Berikut ini ciri-ciri system terinfeksi *malware Flawed Ammyy RAT*:

- Sistem pada *task manager* ada proses yang tidak dikenal
- Sistem pada *wifi* status atau *local area network* status aktifitas *sent* lebih besar disbanding *download*
- Kursor pada sistem bergerak sendiri

F. Pemulihan system setelah terinfeksi malware

Korban yang telah terinfeksi *malware Flawed Ammyy RAT* dapat melakukan hal-hal berikut ini

- Pengguna melakukan putus koneksi dengan jaringan apapun, baik itu *LAN* maupun *access point*.
- Pengguna yang menggunakan *windows* 10 buka *task manager* kemudian lihat pada bagian details klik *Flawed Ammyy RAT* kemudian *end task*

- Pengguna yang menggunakan *windows* 7 buka *task manager* kemudian lihat pada process klik *Flawed Ammyy RAT* kemudian klik *end process*
- Sistem setelah *malware* tidak berjalan, lakukan *install antivirus* dan pemindaian.
- Pengguna lakukan ganti *user name* komputer
- Sistem yang sebelumnya *user* tidak di *password*, sekarang lakukan *password* pada user
- Sistem yang sebelumnya *user* menggunakan *password*, ganti *password* yang dulu sebelum terinfeksi *malware*
- Pengguna lakukan ganti *user name password social media* yang diakses melalui komputer yang terinfeksi
- Pengguna yang melakukan internet banking, segera ganti *pin* atau *username password* akun *internet banking.*

V. KESIMPULAN

Berdasarkan hasil yang diperoleh dari pembahasan dan hasil penelitian ditarik kesimpulan, proses identifikasi malware dapat dengan dua metode yaknik analisis dinamis dan *reverse engineering* menggunakan proses *disassembler*. Proses analisis dinamis dimulai dari instalasi *virtual* mesin, *setting up virtual network, starting process explorer, gathering a first snapshot of the registry, setting up network trafik.* Hasil dari proses identifikasi *malware Flawed Ammyy RAT* menggunakan metode dinamis dan *reverse engineering* telah dilakukan dokumentasi berupa jurnal ilmiah.

Cara kerja *malware Flawed Ammy RAT* ini tidak dapat berjalan ketika korban sedang keadaan *mode DOS*. Malware melakukan infeksi pada system, membaca dan menyimpan data yang ada pada komputer. Mejalankan *Ammy Admin* dan memanipulasi keamanan, melakukan aktif *remote desktop*. Koneksi dengan *attacker* pada *ip address* 103.208.86.69 dan melakukan pengiriman data yang ada pada komputer, ketika korban dan *attacker* sinkron, *attacker* dapat dengan mudah *remote access* jarak jauh tanpa sepengetahuan korban. *Malware* menggunakan 12 *function* untuk melakukan infeksi dan penyerangan pada system.

Kelebihan dari penelitian ini dapat menjelaskan alur analisis dinamis dengan rinci, kemudian menambakan satu tahapan yakni *virtual network* pada virtual mesin yang digunakan sebagai lab analisis *malware*. *Reverse engineering* dengan teknik *disassembler* dapat mempermudah proses investigasi mendalam mengenai pergerakan *malware*. Kekurangan dari penelitian ini adalah tidak dapat melihat lebih jauh penyerangan yang *malware* lakukan pada system, karena *malware* yang telah melakukan infeksi pada system tegantung pada perintah *attacker* selanjutnya, untuk melakukan tahap tersebut system yang terinfeksi *malware Flawed Ammyy RAT* harus melakukan koneksi dengan attackernya kemudian *attacker* akan menjalakan fitur lain yang ada pada *malware Flawed Ammyy RAT.*

UCAPAN TERIMA KASIH

Penulis mengucapkan bersyukur kepada Allah swt, karena berkat rahmat dan barokahnya penulis dapat menyelesaikan penelitian ini. Penulis mengucapkan terimakasih kepada para pembimbing yang sabar mengajarkan dan mmbimbing penulis, kepada orang tua atas segala dukungan dalam bentuk apapun serta pihak-pihak yang terkait yang telah membantu penulis dalam menyelesaikan penelitian ini.

DAFTAR PUSTAKA

[1] N. Zalavadiya and S. Priyanka, "A Methodology of Malware Analysis, Tools and Technique for Windows Platform - RAT Analysus," 2017.

[2] S. C. Y. Hutauruk, F. A. Yulianto and G. B. Satrya, "Malware Analysis Pada Windows Operating System Untuk Mendeteksi Trojan," *e-Proceding of Enggineering* , vol. III, no. 2, pp. 3590-3595, 2016.

[3] R. Adenansi and L. A. Novarina, "Malware Dynamic," *JOEICT (Jurnal of Education and Information Communication Technology),* vol. 1, no. 1, p. 37, 2017.

[4] D. R. Septani, N. Widiyasono and H. Mubarok, "Investigasi Serangan Malware Njrat Pada PC," *Jurnal Edukasi dan Penelitian Informatika (JEPIN),* vol. II, no. 2, pp. 123-128, 2016.

[5] T. A. Cahyanto, V. Wahanggara and D. Ramadana, "Analisis dan Deteksi Malware Menggunakan Metode Analisis Dinamis," *JUSTINDO, Jurnal Sistem & Teknologi Informasi Indonesia* , vol. II, no. 1, pp. 19-30, 2017.

[6] U. K. Bavishi and B. M. Jain, "Malware Analysis," *International Journals of Advanced Research in Computer Science and Software Engineering,* vol. VII, no. 12, pp. 27-33, 2017.

[7] D. Uppal , V. Mehra and V. Verma, "Basic on Malware Analysis, Tools, and Technique," *International Journal on Computational Sciences & Applications (IJCSA) Vol.4, No.1,* pp. 103-112, 2014.

[8] A. H. Muhammad, B. Sugiantoro and A. Luthfi, "Metode Klasifikasi dan Analisis Karakteristik Malware Menggunakan Konsep Ontologi," *Tenomatika,* vol. IX, no. 2, pp. 16-28, 2017.

[9] H. A. Nugroho and Y. Prayudi, "Penggunaan Teknik Reverse Engineering Pada Malware Analysis Untuk Identifikasi Serangan Malware," *KNSI 2014, 27-28 Februari 2015, STMIK Dipanegara Makasar,* pp. 1-8, 2015.

[10] Proofpoint Staff, "Proofpoint," 7 Maret 2018. [Online]. Available: https://www.proofpoint.com/us/threat-insight/post/leaked-source-code-ammyy-admin-turned-flawedammyy-rat.

[11] K. Sheridan, "Darkreading," 12 Maret 2018. [Online]. Available: https://www.darkreading.com/endpoint/flawedammyy-rat-campaign-puts-new-spin-on-old-threat/d/d-id/1331248.

[12] A. Saraswat, "Hacking, Hacking Tools, Vulnerability," 10 Maret 2018. [Online]. Available: https://professionalhackers.in/beware-of-flawedammyy-rat-that-steals-credentials-and-record-audio-chat/.

[13] S. Y. S, Y. Prayudi and I. Riadi, "Implementation of Malware Analysis using Static and Dynamic Analysis Method," *International Journal of Computer Applications,* vol. CXVII, no. 6, pp. 11-15, 2015.

[14] K. Ki-Su, S. Hyo-Jeong and K. Hyong-Shik, "A Bit Vector Based Binary Code Comparison Method for Static Malware Analysis," *Journal of Computers,* vol. xiii, no. 5, pp. 545-554, 2018.

[15] A. Zimba, L. Simukonda and M. Chishimba, "Demystifying Ransomware Attacks: Reverse Engineering and Dynamic Malware Analysis of WannaCry for Network and Information Security," *ZAMBIA INFORMATION COMMUNICATION TECHNOLOGY (ICT) JOURNAL,* vol. i, no. 1, pp. 35-40, 2017.

[16] B. Thakar and C. Parekh, "Reverse Engineering of Bonet (APT)," *Information and Communication Technology for Intelligent Systems,* vol. ii, no. 1, pp. 252-262, 2017.