



**ANALISIS *MALWARE BACKDOOR* MENGGUNAKAN
METODE ANALISIS STATIS DAN DINAMIS PADA
MALWARE ANALYSIS LAB SERTA RANCANG
BANGUN APLIKASI UNTUK MENGHAPUS
*MALWARE***

LAPORAN SKRIPSI

TRISYA TALIA DAVID

**KONSENTRASI KEAMANAN SISTEM INFORMASI
PROGRAM STUDI TEKNIK MULTIMEDIA
DAN JARINGAN JURUSAN TEKNIK INFORMATIKA
DAN KOMPUTER POLITEKNIK NEGERI JAKARTA**



**ANALISIS *MALWARE BACKDOOR* MENGGUNAKAN
METODE ANALISIS STATIS DAN DINAMIS PADA
MALWARE ANALYSIS LAB SERTA RANCANG
BANGUN APLIKASI UNTUK MENGHAPUS
*MALWARE***

LAPORAN SKRIPSI

**Dibuat untuk Melengkapi Syarat-syarat yang Diperlukan untuk
Memperoleh Gelar Sarjana Terapan**

TRISYA TALIA DAVID

4817050437

**KONSENTRASI KEAMANAN SISTEM INFORMASI
PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN
JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER
POLITEKNIK NEGERI JAKARTA**

2021



HALAMAN PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya saya sendiri, dan semua sumber baik yang dikutip maupun rujukan telah saya nyatakan dengan benar

Nama : Trisya Talia David

NIM : 4817050437

Tanggal : 13 Juni 2021

Tanda Tangan :

**POLITEKNIK
NEGERI
JAKARTA**

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumpulkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta



© Hak Cipta milik Jursusan TIK Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumpulkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

HALAMAN PENGESAHAN

Skripsi diajukan oleh :

Nama : Trisya Talia David
NIM : 4817050437
Program Studi : Teknik Multimedia dan Jaringan
Judul Skripsi : Analisis *Malware Backdoor* Menggunakan Metode
Analisis Statis dan Dinamis pada *Malware* Analisis Lab Serta
Rancang Bangun Aplikasi untuk Menghapus *Malware*
Telah diuji oleh tim penguji dan pembimbing dalam Sidang Skripsi pada hari
Kamis, tanggal 01 bulan Juli tahun 2021 , dan dinyatakan LULUS

Disahkan Oleh

Pembimbing : Ariawan Andi Suhandana, S.Kom., M.T.I. ()
Penguji I : Maria Agustin, S.Kom., M.Kom. ()
Penguji II : Asep Kurniawan, S.Pd., M.Kom. ()
Penguji III : Fachroni Arbi Murad, S.Kom., M.Kom. ()

Mengetahui :

Jurusan Teknik Informatika dan Komputer



Mauldy Laya, S.Kom., M.Kom.

NIP 19780211 200912 1 003



KATA PENGANTAR

Alhamdulillah, uji syukur selalu dipanjatkan kepada Tuhan Yang Maha Esa, atas berkat, terutama kesehatan di masa pandemi ini, serta rahmat yang senantiasa diberikan-Nya, penulis dapat menyelesaikan laporan skripsi berjudul *Analisis Malware Backdoor Menggunakan Metode Analisis Statis dan Dinamis pada Malware Analisis Lab Serta Rancang Bangun Aplikasi untuk Menghapus Malware* ini. Selama menjalani masa perkuliahan dan pelaksanaan penelitian skripsi, tentu banyak dukungan, bantuan, bimbingan dan saran dari berbagai pihak, oleh karena itu penulis mengucapkan terimakasih kepada semua pihak yang telah mendukung, terutama kepada:

1. Bapak Ariawan Andi Suhandana, selaku pembimbing skripsi yang telah membimbing penulis dan memberi masukan yang sangat membantu selama pengerjaan skripsi ini.
2. Bapak Defiana Arnaldy, S.TP, M.Si. selaku dosen dan KPS penulis di Politeknik Negeri Jakarta yang telah memberikan pengetahuan dan bimbingan dalam pengerjaan skripsi ini.
3. Orang tua, adik serta seluruh keluarga penulis yang telah memberikan dukungan yang tidak mengenal kondisi dan tidak terhingga kepada Penulis.
4. Dita Nurhayati, Laily Rachmi Tsani, Sabrina Annisa dan Suci Rahmadhani selaku teman seperjuangan yang selalu mendukung dan menemani pengerjaan skripsi ini hingga larut malam.
5. Cahya Mulyadi, dan teman-teman pada Grup Bismillah yang telah membantu dan mendukung Penulis dalam pengerjaan skripsi.
6. Chelsy Lidesia selaku sahabat yang selalu mendengarkan keluh kesah, memberi saran, dan dukungan kepada Penulis selama penulisan skripsi berlangsung

Semoga Tuhan membalas segala kebaikan dari pihak-pihak yang telah membantu. Penulis juga ingin memohon maaf atas kesalahan yang tidak sengaja dilakukan

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumpulkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jursuan TIK Politeknik Negeri Jakarta



© Hak Cipta Milik Jurusan Teknik Negeri Jakarta

penulis selama sibuknya penulisan skripsi ini. Semoga tulisan ini bermanfaat bagi pembaca dan dunia pengetahuan. Sekian dan terimakasih.

Jakarta, 4 Juni 2021

Prisyta Talia David.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumpulkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta



© Hak Cipta milik Urusan TIK Politeknik Negeri Jakarta

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Politeknik Negeri Jakarta, saya yang bertanda tangan di bawah ini :

Nama	: Trisya Talia David
NIM	: 4817050437
Program Studi	: Teknik Multimedia dan Jaringan
Jurusan	: Teknik Informatika dan Komputer
Jenis Karya	: Skripsi

Sebelum pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Politeknik Negeri Jakarta **Hak Bebas Royalti Noneksklusif (Non-exclusive Royalty-Free Right)** atas karya ilmiah saya yang berjudul :

Analisis Malware Backdoor Menggunakan Metode Analisis Statis dan Dinamis pada Malware Analysis Lab serta Rancang Bangun Aplikasi untuk Menghapus Malware

Dengan Hak Bebas Royalti Noneksklusif ini Politeknik Negeri Jakarta berhak menyimpan, mengalih media/form-kan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan skripsi saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta

Demikian pernyataan ini saya buat dengan sebenarnya

Dibuat di :

Pada tanggal :

Yang menyatakan

Trisya Talia David

**POLITEKNIK
NEGERI
JAKARTA**

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumpulkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta



ANALISIS *MALWARE* BACKDOOR MENGGUNAKAN METODE ANALISIS STATIS DAN DINAMIS PADA *MALWARE ANALYSIS LAB* SERTA RANCANG BANGUN APLIKASI UNTUK MENGHAPUS *MALWARE*

ABSTRAK

Malware merupakan perangkat lunak (software) yang diciptakan dengan niat jahat untuk menyusup atau merusak sistem komputer. Dewasa ini penyebaran malware semakin merkelirakan, baik melalui USB flashdisk, iklan pada website, email dan banyak media lainnya. Tujuan dari penyebaran malware ini adalah untuk mencuri data penting seperti identitas, kartu kredit, internet banking, file, dsb. yang kemudian akan digunakan untuk hal yang merugikan korban. Salah satu upaya dalam melawan malware adalah melakukan analisis terhadap malware, hal ini dilakukan untuk menganalisis bukti digital, menentukan apakah sebuah software adalah malware, mencari tahu identitas malware, mengetahui cara kerja malware tersebut, dan mencari tahu bagaimana cara membersihkan malware dari komputer. Untuk mencapai tujuan-tujuan ini dibangun Malware Analysis Lab sebagai ruang isolasi untuk melakukan Malware Analysis dengan metode yang sesuai untuk digunakan adalah metode Analisis Statis dan Dinamis. Berdasarkan analisa tentang cara kerja malware jenis backdoor (beast dan slackbot), dapat disimpulkan bahwa terdapat signature, string, filename dan windows registry yang menunjukkan bahwa kedua software tersebut adalah malware yang mencoba untuk terus tersambung dengan komputer tanpa sepengetahuan dan persetujuan pemilik komputer, malware beast mencoba untuk login secara remote sedangkan malware slackbot mencoba untuk mengirimkan data internet tanpa sepengetahuan pemilik komputer, juga ditemukan cara untuk menghapus kedua malware ini saat analisis dan program yang dibuat berhasil menghapus kedua malware dari komputer.

Kata kunci: *Malware, Backdoor, Malware Analysis, Malware Analysis Lab, Analisis Static, Analisis Dynamic*

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumpulkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta



BACKDOOR MALWARE ANALYSIS USING STATIC AND DYNAMIC ANALYSIS METHODS IN MALWARE ANALYSIS LAB AND APPLICATION DESIGN TO REMOVE MALWARE

ABSTRACT

Malware is software that was created with malicious intent to infiltrate or damage computer systems. Today the spread of malware has increased significantly, either through USB flash drives, advertisements on websites, email and many other media. The purpose of this malware deployment is to steal important data such as identity, credit cards, internet banking, files, etc. which will then be used for things that harm the victim. One of the efforts to fight malware is to conduct an analysis of malware, this is done to analyze digital evidence, determine that a software is malware, find out the identity of malware, find out how the malware works, and find out how to clean malware from computers. To achieve these goals, the Malware Analysis Lab was built as an isolation room to perform Malware Analysis with the appropriate method to use is the Static and Dynamic Analysis method. Based on an analysis of how backdoor malware (beast and slackbot) works, it can be concluded that there are signatures, strings, filenames and windows registry which indicate that the two software are malware that tries to continue to connect to the computer without the knowledge and approval of the computer owner, malware beast tries to log in remotely while the slackbot malware tries to transmit internet data without the knowledge of the computer owner, also found a way to remove these two malware when the analysis and program created succeeded in removing both malware from the computer.

Keywords: *Malware, Backdoor, Malware Analysis, Malware Analysis Lab, Analysis Static, Analysis Dynamic*

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumpulkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta



DAFTAR ISI

HALAMAN PERNYATAAN ORISINALITAS	i
HALAMAN PENGESAHAN	ii
KATA PENGANTAR	iii
HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS	v
ABSTRAK	vi
ABSTRACT	vii
DAFTAR ISI	viii
DAFTAR GAMBAR	x
DAFTAR TABEL	xii
BAB I	1
PENDAHULUAN	1
1.1 Latar Belakang Masalah	1
1.2 Perumusan Masalah	2
1.3 Batasan Masalah	3
1.4 Tujuan dan Manfaat	3
1.5 Metode Penyelesaian Masalah	4
BAB II	5
TINJAUAN PUSTAKA	5
1. Tinjauan Pustaka	5
2.1 Keamanan Sistem Komputer	5
2.2 <i>Backdoor</i>	5
2.3 <i>VirtualBox</i>	6
2.4 <i>Malware Analysis Lab</i>	6
2.5 Analisa Statis	7
2.6 <i>Packer dan Unpacking File</i>	7
2.7 ExeInfoPE	7
2.8 <i>UPX Packer</i>	8
2.9 PEStudio	8
2.10 VirusTotal	8
2.11 Ghidra	8

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumpulkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta



© Hak Cipta milik Jurusan TIK Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumpulkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

2.12	Analisa Dinamis.....	9
2.13	Process Monitor	9
2.14	Process Hacker	9
2.15	ProcDOT	10
2.16	FlareVM.....	10
2.	Penelitian Sejenis	10
BAB III.....		12
PERENCANAAN DAN REALISASI.....		12
3.1	Perancangan Sistem.....	12
3.2	Realisasi Sistem	17
BAB IV.....		26
PEMBAHASAN		26
4.1	Pengujian	26
4.2	Deskripsi Pengujian.....	26
4.3	Prosedur Pengujian	26
4.4	Data Hasil Pengujian	29
4.5	Analisis Data/Evaluasi.....	47
PENUTUP.....		50
5.1	Simpulan	50
5.2	Saran	51
DAFTAR PUSTAKA		51
LAMPIRAN.....		53
DAFTAR RIWAYAT HIDUP		53



DAFTAR GAMBAR

- Hak Cipta :**
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritis atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
 2. Dilarang mengumpulkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

Gambar 3. 1 workflow dari penelitian	13
Gambar 3. 2 Flowchart analisa keseluruhan	14
Gambar 3. 3 flowchart aplikasi untuk membersihkan malware.....	17
Gambar 3. 4 Jaringan Virtual yang Digunakan.....	18
Gambar 3. 5 installasi FlareVM menggunakan PowerShell	19
Gambar 3. 6 installasi FlareVM berhasil	19
Gambar 3. 7 flowchart analisa statis	20
Gambar 3. 8 tampilan tools exeinfope	21
Gambar 3. 9 tools 'pestudio'	21
Gambar 3. 10 tools virustotal	22
Gambar 3. 11 malware sudah diimport ke ghidra	22
Gambar 3. 12 symbol references.....	22
Gambar 3. 13 flowchart analisis dinamis.....	23
Gambar 3. 14 GUI aplikasi pembersih malware.....	24
Gambar 3. 15 kode fungsi 'changeVariable()' variable pada malware	25
Gambar 3. 16 kode fungsi 'compareProcess()'	26
Gambar 3. 17 teks file yang digunakan dalam fungsi 'comapreFiles()'	26
Gambar 3. 18 teks file yang digunakan untuk fungsi 'compareRegs()'.....	26
Gambar 3. 19 kode fungsi 'tulisKeTxt()'.....	27
Gambar 3. 20 kode fungsi 'tulisKeTable'.....	27
Gambar 4. 1 cek file sampel 1 masih packed sehingga tools menyarankan untuk melakukan proses unpack	27
Gambar 4. 2 command unpacking pada sampel 1.....	30
Gambar 4. 3 cek file sampel 1 menunjukkan sudah tidak lagi packed sehingga ukuran file bertambah	30
Gambar 4. 4 cek file sampel 2 masih packed sehingga tools menyarankan untuk melakukan proses unpack	31
Gambar 4. 5 command unpacking pada sampel 2.....	31
Gambar 4. 6 cek file sampel 1 menunjukkan sudah tidak lagi packed sehingga ukuran file bertambah	31
Gambar 4. 7 hasil dari identifikasi malware sampel 1 pada 'Virusotal'	33
Gambar 4. 8 hasil dari identifikasi malware sampel 2 pada 'Virusotal'	34
Gambar 4. 9 process malware 1 terekam pada tools Process Hacker	38
Gambar 4. 10 diagram kegiatan yang dilakukan malware Beast secara keseluruhan	39
Gambar 4. 11 malware membuat registry persistence berserta value	39
Gambar 4. 12 registry persistence dilihat dari 'registry editor' dan 'task namager'	40
Gambar 4. 13 file persistence yang ditanam oleh malware tercatat oleh 'ProcDOT' dan dilihat di 'windows file explorer'	40
Gambar 4. 14 netstat menunjukkan sambungan pada komputer target	41
Gambar 4. 15 proses malware berjalan pada mesin tercatat oleh 'process hacker'.....	41



- Hak Cipta :**
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
 2. Dilarang mengumpulkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

Gambar 4. 16 gambar keseluruhan grafik aktifitas malware di mesin target.....	42
Gambar 4. 17 membuat registry dengan untuk mempertahankan koneksi	42
Gambar 4. 18 hasil konfigurasi registry dapat dilihat pada menu startup di task manager	42
Gambar 4. 19 registry-registry internet yang diakses oleh sang malware	43
Gambar 4. 20 penampilan aplikasi menemukan malware Beast	43
Gambar 4. 21 hasil komparasi sebelum dan sesudah aplikasi pembersih malware Beast dieksekusi oleh 'regshot'	44
Gambar 4. 22 detail catatan regshot, salah satu value registry dan file yang terhapus adalah value yang ditanam oleh malware Beast.....	44
Gambar 4. 23 aplikasi sudah tidak lagi muncul pada tab Startup di 'windows task manager'	45
Gambar 4. 24 netstat pada cmd menunjukkan mesin tidak terhubung lagi dengan penyerang	45
Gambar 4. 25 penampilan aplikasi menemukan malware Slackbot	45
Gambar 4. 26 hasil komparasi sebelum dan sesudah aplikasi pembersih malware slackbot dieksekusi oleh 'regshot'	46
Gambar 4. 27 detail catatan regshot, salah satu value registry dan file yang terhapus adalah value yang ditanam oleh malware Slackbot.....	47
Gambar 4. 28 aplikasi sudah tidak lagi muncul pada tab Startup di 'windows task manager'	47



DAFTAR TABEL

Table 1 Table Penelitian Sejenis	10
Table 2 tabel fungsi pada aplikasi serta penjelasan tentang fungsi tersebut	24
Table 3 Informasi file 'server.exe' didapatkan dari 'pestudio'	32
Table 4 Informasi file 'tnnbtib.exe' didapatkan dari 'pestudio'	33
Table 5 Penemuan Analisis String malware Beast	34
Table 6 Penemuan Analisis String malware Slackbot	37
Table 7 table kumpulan penemuan analisis statis dan dinamis pada malware 1 Beast	48
Table 8 table kumpulan penemuan analisis statis dan dinamis pada malware 2 Slackbot	48
Table 9 hasil pengujian aplikasi penghapus backdoor	49



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumpulkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta



BAB I PENDAHULUAN

1.1 Latar Belakang Masalah

Dengan pesatnya perkembangan teknologi, internet saat ini memiliki pengaruh yang besar pada kehidupan manusia. Ribuan situs muncul setiap hari membuka jalan yang lebih besar untuk *malware* ikut berkembang dan berkeliaran di internet. Dengan jumlah sumber daya yang terbatas, keamanan berselancar di dunia maya menjadi tantangan besar dan ancaman bagi keamanan data dikarenakan eksploitasi perangkat lunak. Ancaman keamanan ini sangat berbahaya, melihat dari perkembangan *malware* dewasa ini yang semakin canggih, mulai dari pencurian *password* dan ID akun sosial media, pencurian nomor kartu kredit, internet *banking* sampai pencurian identitas dapat terjadi karena satu kesalahan menjalankan *malware* yang berkeliaran di internet (Choudharya & Khuranaa, 2017). Banyak cara dan upaya yang telah dikembangkan oleh para ahli untuk melawan berbagai jenis serangan yang ada. Para ahli bahkan melakukan pengujian kemampuan anti-virus contohnya pada karya tulisan berjudul “*Extending the Metasploit Framework to Implement an Evasive Attack Infrastructure: An exercise for SPICE to test the ability of mainstream antivirus software to prevent intrusion through drive-by downloads*” milik Aubrey Alston pada tahun 2017 yang menganalisis *anti-virus* bertujuan mengembangkan senjata-senjata yang lebih baik untuk melawan *malware*, namun penyerang selalu saja berada satu langkah didepan *defender*. Dengan berkembangnya kemampuan *malware* berserta kemudahan penggunaan *malware* tersebut, penyerangan lebih mudah untuk direncanakan dan direalisasikan. Salah satu jenis *malware* dengan efektifitas tinggi yang logika kondisional penyerangannya dapat dikostumasi oleh sang penyerang sesuai kebutuhan, memiliki tingkat kesuksesan tinggi yaitu 93.5%. Jenis *malware* ini adalah jenis *Backdoor* (Li, et al., 2018). *Malware Backdoor* merupakan *trojan* yang jenis penyerangannya diselipkan ke dalam aplikasi lain menggunakan *tools binder* yang mudah digunakan, sehingga penyerang dapat secara mudah membuat *Backdoor* dengan ekstensi *file* yang paling sering digunakan oleh pengguna komputer yaitu

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumpulkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta



© Hak Cipta milik Jurusan TIK Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang menggunakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

File dengan ekstensi *exe* yang merupakan ekstension nomor 3 terbanyak digunakan di dunia (Cui, et al., 2020) (Sauder, 2015). Dengan analisis *anti-virus* milik Aubrey Alston yang telah ada, penulis memutuskan untuk menghampiri topik *malware* ini menggunakan satu metode yang sedikit berbeda yaitu dengan menggunakan *Malware Analysis Lab* untuk menganalisis *malware*, sehingga dapat menyediakan pemahaman yang menyeluruh dari kedua perspektif teoritikal dan praktikal perangkat lunak yang bersifat jahat (*malicious*) (All Answers Ltd., November 2018). Dengan mengembangkan *malware analysis lab* memungkinkan untuk menganalisa *malware* yang ada. Analisis *malware* pada penelitian ini dilakukan menggunakan metode analisis statis dan dinamis dengan harapan mendapatkan hasil identifikasi *malware*, mengetahui dan mengerti kemampuan maupun cara kerja *malware*, serta pembersihan yang tepat pada mesin yang terinfeksi (Sari, et al., 2020).

Penelitian ini terinspirasi dari kedua ide pokok diatas, yaitu membangun *malware analysis lab* dengan *malware* yang digunakan pada penelitian ini adalah *Backdoor*. Alasan digunakannya *malware* jenis *Backdoor* karena merupakan salah satu jenis program jahat (*malicious*) yang digunakan penyerang untuk mengambil informasi dan kendali sebuah sistem dengan cara membuka pintu belakang dari sebuah sistem itu tanpa sepengetahuan pemilik sistem (Hafiz, et al., 2020). Jenis *malware* ini terus berkembang menggunakan metode-metode baru yang memungkinkan penyerang untuk mengambil kendali sistem secara menyeluruh dan tersambung ke sistem targetnya secara lebih mudah dan praktis (Kara & Aydos, 2019). Pada penelitian ini juga membahas tentang pertolongan pertama yang dilakukan saat sebuah komputer sudah terinfeksi aplikasi jahat. Penulis akan mengembangkan sebuah program yang dapat digunakan untuk memudahkan korban menghapus *Backdoor* dari komputer yang terinfeksi.

1.2 Perumusan Masalah

Dari latar belakang yang sudah dijelaskan, perumusan masalah dari tulisan ini adalah:

- a. Bagaimana sebuah *Malware Backdoor* dapat menginfeksi komputer?
- b. Bagaimana cara melakukan Analisis pada *malware* tersebut?



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang menggunakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

Bagaimana *malware* tersebut berpengaruh pada komputer?

Aplikasi seperti apa yang dapat dibuat untuk digunakan sebagai solusi mengatasi *malware* ini?

1.3 Batasan Masalah

Dalam tulisan ini untuk mengatasi permasalahan yang ada maka disusun beberapa batasan masalah sebagai berikut:

- *Backdoor Malware* akan menginfeksi komputer korban menggunakan metode pengekseskuan *social engineering*
- *Malware* yang digunakan adalah *malware* Trojan dengan spesifikasi *Backdoor*
- Menganalisa informasi-informasi dasar *malware* menggunakan metode analisis statis
- Menganalisis perubahan-perubahan yang dilakukan oleh *malware* di komputer korban menggunakan metode analisis dinamis
- Membuat aplikasi untuk membersihkan *backdoor* agar komputer tidak lagi tersambung dengan penyerang

1.4 Tujuan dan Manfaat

Adapun tujuan dari tulisan ini adalah untuk mengetahui identitas, cara kerja dan efek apa saja yang disebabkan suatu *malware* terhadap mesin yang diinfeksi menggunakan metode analisis statis dan dinamis pada sebuah *malware analysis*, sehingga dapat dibangun aplikasi untuk memulihkan komputer yang telah terjangkit *malware* tersebut.

Manfaat yang dapat diambil dari penulisan ini adalah:

- a. Mengetahui alur metode analisis statis dan dinamis pada sebuah *malware analysis*
- b. Mengetahui identitas, memahami cara kerja dan efek yang disebabkan suatu *malware* terhadap mesin yang diinfeksi
- c. Mengetahui bagaimana cara untuk menghapus sebuah *malware* dari sebuah sistem yang telah terjangkit *malware* yang telah dianalisis
- d. Dapat tercipta aplikasi yang mampu menghapus *malware* yang telah dianalisis.



© Hak Cipta milik Jurusan TIK Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumpulkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

- e. Meningkatkan keamanan pada sistem komputer.

5.5 Metode Penyelesaian Masalah

Penelitian ini dilakukan dengan metode sebagai berikut:

Pengumpulan data

Pengumpulan data dilakukan dengan mencari data atau informasi terkait masalah yang dijadikan topik penelitian melalui studi literatur dari buku-buku dan jurnal penelitian yang berhubungan dengan topik penelitian.

Pengerjaan Konfigurasi

Pengerjaan konfigurasi dilakukan untuk menyesuaikan *backdoor* dengan target yang akan dituju.

Pengujian & Analisis Hasil Pengujian

Melakukan pengujian terhadap kondisi yang telah dikonfigurasi dan melakukan analisis terhadap hasil uji coba

Penyusunan Laporan Penelitian

Melakukan penyusunan laporan sesuai dengan pedoman yang telah ditetapkan oleh panitia skripsi Jurusan Teknik Informatika dan Komputer Politeknik Negeri Jakarta beserta melakukan bimbingan kepada dosen pembimbing sekaligus pakar dan mendokumentasikan pengerjaan dalam bentuk foto, video, ataupun media lain yang dapat dijadikan dokumentasi.

POLITEKNIK
NEGERI
JAKARTA



BAB V PENUTUP

5.1 Simpulan

Setelah melewati analisis *malware* pada mesin *malware analysis lab* menggunakan metode analisis statis dan dinamis, peneliti dapat mengetahui identitas *malware* dan pengaruh dari *malware* berjenis *backdoor* dengan famili *Beast* dan *Slackbot* ini pada sebuah komputer, sehingga dapat dikembangkan aplikasi yang mampu memulihkan komputer dari kedua *backdoor* ini. Peneliti mengambil kesimpulan sebagai berikut:

1. *Malware Backdoor* dapat menginfeksi komputer korban karena kelalaian korban mengeksekusi/menjalankan *file backdoor* tersebut. Dengan mengeksekusi *malware*, sistem operasi (pada penelitian ini: *windows OS*) memberikan izin kepada *malware* untuk berjalan seperti perangkat lunak lainnya yang tidak memiliki niat jahat (*malicious*) terhadap komputer. Sehingga pengguna komputer harus berhati-hati dalam menjalankan aplikasi yang dimiliki.
2. Hasil penelitian menggunakan metode analisis statis yang memiliki 3 proses yaitu proses *unpacking*, identifikasi *malware*, *analysis string* menunjukkan identitas *backdoor/malware*, serta kemampuannya untuk memantau bahkan mengambil alih sebuah komputer. Hasil penelitian menggunakan metode analisis dinamis yang memiliki 1 proses yaitu pemantauan eksekusi menunjukkan perubahan yang disebabkan oleh *backdoor*, perubahan yang dimaksud adalah penanaman *process*, *windows registry*, dan *file* baru pada komputer yang terjangkit.
3. Dari hasil kedua metode analisis di atas peneliti dapat mengembangkan aplikasi yang mampu memulihkan komputer dari *backdoor*, aplikasi ini bekerja dengan cara mencari dan menghapus *process malware*, *windows registry* dan *file* yang ditinggalkan oleh *backdoor* untuk mempertahankan koneksi antara penyerang dan korbannya.

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumpulkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jursuan TIK Politeknik Negeri Jakarta



5.2 Saran

Berdasarkan penelitian yang telah dilakukan, terdapat saran yang dapat diterapkan untuk pengembangan dalam penelitian selanjutnya:

1. Menggunakan lebih banyak jenis *malware*
2. Aplikasi yang dibuat mampu membersihkan lebih banyak jenis *malware*
3. Aplikasi bukan hanya mampu menghapus *malware* tapi juga mampu menentukan apakah sebuah *file* merupakan *malware* atau bukan untuk mencegah *malware* menginfeksi mesin komputer.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang menggunakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta



DAFTAR PUSTAKA

- All Answers Ltd., November 2018. *Creating a Malware Lab with Metasploit*, s.l.: n.
- A., M. K., 2018. *Learning Malware Analysis*. 1 penyunt. Birmingham: Packt Publishing Ltd..
- Anam, M. K. et al., 2020. Optimalisasi Penggunaan VirtualBox Sebagai Virtual Computer Laboratory untuk Simulasi Jaringan dan Praktikum pada SMK Taruna Mandiri Pekanbaru. *J-PEMAS STMIK*, 1(1), pp. 38-44.
- Anon., 2020. Yansong Gao; Bao Gia Doan; Zhi Zhang; Siqi Ma; Jiliang Zhang; Anmin Fu; Surya Nepal; Hyoungshick Kim. *Backdoor Attacks and Countermeasures on Deep Learning: A Comprehensive Review*, 1(1), pp. 1-30.
- Cahyanto, T. A., Wahanggara, V. & Ramadana, D., 2017. Analisis dan Deteksi Malware Menggunakan Metode Malware Analisis Dinamis dan Analisis Statis. *Jurnal Sistem & Teknologi Informasi Indonesia*, pp. 19-30.
- Choudharya, R. & Khurana, M., 2017. Exploitation of PDF Reader Vulnerabilities using Metasploit Tool. *MECS Education and Management Engineering*, 1(1), pp. 23-24.
- Cui, Y. et al., 2020. MMDP: A Novel Malicious PDF File Detector for Mobile Robots. *IEEE Sensors Journal*, 1(1), pp. 1-14.
- FEDAK, A. & STULRAJTER, J., 2020. Fundamentals of Static Malware Analysis: Principles, Methods and Tools. *Science & Military*, 1(1), pp. 45-53.
- Hafiz, A. et al., 2020. ANALISIS CELAH KEAMANAN JARINGAN DAN SERVER MENGGUNAKAN SNORT INTRUSION DETECTION SYSTEM. *JURNAL INFORMASI DAN KOMPUTER*, 8(2), pp. 59 - 66.
- Haque, M. M., 2019. SLACKBOT DESIGN AND DEVELOPMENT. *BACHELOR'S THESIS TURKU UNIVERSITY OF APPLIED SCIENCES*, 1(1), pp. 1-36.
- Jung, B., Bae, S., Choi, C. & Im, E., 2018. Packer Identification Method Based on Byte Sequences. *Concurrency Computat Pract Exper*, pp. 1-11.
- Kabakus, A. T. & Dogru, I. A., 2018. An in-depth analysis of Android Malware using Hybrid Techniques. *Digital Investigation*, pp. 1-9.
- Kara, I. & Aydos, M., 2019. The Ghost in the System: Technical Analysis of Remote Access Trojan. *International Journal of Information Technologies & Security*, 11(1), pp. 73-84.

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumpulkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta



© Hak Cipta milik Jurusan TK Politeknik Negeri Jakarta

- Kara, I. & Aydos, M., 2019. THE GHOST IN THE SYSTEM: TECHNICAL ANALYSIS OF REMOTE ACCESS TROJAN. *International Journal on Information Technologies & Security*, 11(1), pp. 73-84.
- Li, Y. et al., 2018. DeepPayload: Black-Box Backdoor Attack on Deep Learning Models through Neural Payload Injection. *International Telecommunication Networks and Applications Conference (ITNAC)*, 28(12), pp. 50-62.
- Mohanta, A. & Saldanha, A., 2020. *Malware Analysis and Detection Engineering*. Manglore: Apress.
- Panjanian, F., Ydiastuti, H. & Ulfa, M., 2021. Analisis Malware dengan Metode Surface dan Runtime Analysis. *Jurnal Ilmiah MATRIK*, 23(1), pp. 1 - 11.
- Sheng, P., Yang, L., Song, L. & Wang, G., 19. Opening the Blackbox of VirusTotal: Analyzing Online Phishing Scan Engines. *IMC*, pp. 478 - 485.
- Seppens, J., 2018. *Creating a Malware Analysis Lab and Basic Malware Analysis*, Iowa: Iowa State University.
- Qubeitah, M. A. & Aldwairi, M., 2018. Dynamic Malware Analysis of Phishing Emails. *International Conference on Information and Communication Systems (ICICS)*, 9(9), pp. 18-24.
- Schrohleder, R., 2019. Hands-On Ghidra - A Tutorial about the Software Reverse Engineering Framework. *SPRO'19*, pp. 77 -78.
- Sari, I. Y. et al., 2020. *Keamanan Data & Informasi*. 1st penyunt. s.l.:Yayasan kita Menulis.
- Sauder, D., 2015. Why Anti-Virus Software Fails. *Magdeburger Journal zur Sicherheitsforschung*, 1(1), pp. 541-546.
- Sopaheluwakan, C. R. & Chandra, D. W., 2020. ANTI-WEBSHELL PHP BACKDOOR SCANNER PADA LINUX SERVER. *ILKOM Jurnal Ilmiah*, 12(2), pp. 143-153.

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumpulkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta



© Hak Cipta milik

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumpulkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta



Politeknik Negeri Jakarta

LAMPIRAN

DAFTAR RIWAYAT HIDUP

TRISYA TALIA DAVID

Lahir pada tanggal 4 Desember 1999 di Karawang. Lulus dari SMAN 99 Jakarta pada tanggal 2017, SMAS YP-IPPI CAKUNG pada tahun 2016 dan Diploma II program studi Network Administrator Professional di CCIT – FTUI pada tahun 2019. Saat ini sedang menempuh Pendidikan Diploma IV Program Studi Information Security Jurusan Teknik Informatika dan Komputer di Politeknik Negeri Jakarta.

POLITEKNIK
NEGERI
JAKARTA