



**ANALISIS *RANSOMWARE* STOP/DJVU DENGAN
MENGUNAKAN METODE *STATIC ANALYSIS* DAN
*DYNAMIC ANALYSIS***

NAMA : RAKHA TRI FADILLAH

NPM : 18360011

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS SAINS DAN TEKNOLOGI INFORMASI
INSTITUT SAINS DAN TEKNOLOGI NASIONAL
JAKARTA
MARET 2022**



**ANALISIS RANSOMWARE STOP/DJVU DENGAN
MENGUNAKAN METODE *STATIC ANALYSIS* DAN
*DYNAMIC ANALYSIS***

SKRIPSI

**Diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana
Komputer**

NAMA : RAKHA TRI FADILLAH

NPM : 18360011

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS SAINS DAN TEKNOLOGI INFORMASI
INSTITUT SAINS DAN TEKNOLOGI NASIONAL
JAKARTA**

MARET 2022

HALAMAN PERNYATAAN ORISINALITAS

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

NAMA : Rakha Tri Fadillah

NPM : 18360011

TANGGAL : 8 Maret 2022

TTD di atas MATERAI



HALAMAN PERNYATAAN NON PLAGIAT

Yang bertanda tangan di bawah ini:

Nama : Rakha Tri Fadillah
NPM : 18360011
Mahasiswa : Strata Satu (S1)
Tahun Akademik : 2018

Dengan ini menyatakan bahwa skripsi yang telah saya buat dengan judul **“Analisis Ransomware STOP/DJVU Dengan Menggunakan Metode *Static Analysis* dan *Dynamic Analysis*”** adalah hasil karya sendiri, dan semua sumber baik yang kutip maupun yang di rujuk telah saya nyatakan dengan benar dan skripsi belum pernah di terbitkan atau di publikasikan di manapun dalam bentuk apapun.

Demikian surat pernyataan ini saya buat dengan sebenar benarnya . Apabila dikemudian hari ternyata saya memberikan keterangan palsu dan atau ada pihak lain yang mengklaim bahwa skripsi yang telah saya buat adalah hasil karya milik seseorang atau badan tertentu, saya bersedia diproses baik secara pidana maupun perdata dan kelulusan saya dari Program Studi Teknik Informatika Institut Sains dan Teknologi Nasional dicabut/dibatalkan.

Jakarta, 8 Maret 2022

1


Rakha Tri Fadillah

Rakha Tri Fadillah

HALAMAN PENGESAHAN

Skripsi ini diajukan oleh :
Nama : Rakha Tri Fadillah
NPM : 18360011
Program Studi : Teknik Informatika
Judul Skripsi : Analisis *Ransomware* STOP/DJVV Dengan Menggunakan Metode *Static Analysis* dan *Dynamic Analysis*

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh Sarjana Komputer (S.Kom.) pada Program Studi Teknik Informatika, Fakultas Sains dan Teknologi Informasi, Institut Sains dan Teknologi Nasional

DEWAN PENGUJI

Pembimbing : B. Sumardiyono, S.T, M.Kom
NIDN. 0323067503

(B. Sumardiyono)

Penguji : Aryo Nur Utomo, S.T. M.Kom.
NIDN. 0319046803

(Aryo Nur Utomo)

Penguji : Neny Rosmawarni, S.Kom. M.Kom.
NIDN. 0312018701

(Neny Rosmawarni)

Penguji : Siti Madinah L., S.Kom. M.Kom.
NIDN. 0307107201

(Siti Madinah L.)

Ditetapkan di : Jakarta
Tanggal : 8 Maret 2022

KATA PENGANTAR

Puji syukur penulis ucapkan kehadirat Allah SWT yang telah memberikan rahmat dan karunia-Nya kepada penulis, sehingga penulis dapat menyelesaikan Skripsi yang berjudul “Analisis *Ransomware* STOP/DJVU Dengan Menggunakan Metode *Static Analysis* Dan *Dynamic Analysis*”. Skripsi ini disusun untuk memenuhi salah satu syarat kelulusan.

Dalam pelaksanaan penyusunan skripsi ini, penulis mendapat banyak bantuan, bimbingan, serta arahan dari berbagai pihak. Oleh sebab itu, dalam kesempatan ini penulis ingin menyampaikan rasa terima kasih yang tulus kepada:

1. Bapak B. Sumardiyono, S.T, M.Kom, selaku dosen pembimbing yang telah menyediakan waktu, tenaga, dan pikiran untuk mengarahkan saya dalam penyusunan skripsi ini;
2. Ibu Neny Rosmawarni, S.Kom., M.Kom selaku Kepala Program Studi Teknik Informatika yang telah memberikan bantuan serta perhatian bagi penulis;
3. Para Dosen yang sudah memberikan pengetahuan kepada penulis guna menyelesaikan skripsi ini;
4. Keluarga yang selalu membantu penulis dengan Do’a dan dukungan dalam berbagai hal; dan
5. Sahabat yang telah banyak membantu saya dalam menyelesaikan skripsi ini.

Semoga arahan, motivasi, dan bantuan yang telah diberikan menjadi amal ibadah bagi keluarga, bapak, dan rekan-rekan, sehingga memperoleh balasan yang lebih baik dari Allah SWT.

Depok, 8 Maret 2022



Rakha Tri Fadillah

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademika Institut Sains dan Teknologi Nasional, saya yang bertanda tangan di bawah ini:

Nama : Rakha Tri Fadillah
NPM : 18360011
Program Studi : Teknik Informatika
Fakultas : Fakultas Sains dan Teknologi Informasi
Jenis Karya : Skripsi

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Institut Sains dan Teknologi Nasional **Hak Bebas Royalti Noneksklusif** (*Non-exclusive Royalty-Free Right*) atas karya ilmiah saya yang berjudul:

“Analisis *Ransomware* STOP/DJVU Dengan Menggunakan Metode *Static Analysis* dan *Dynamic Analysis*”.

Dengan Hak Bebas Royalti Noneksklusif ini Institut Sains dan Teknologi Nasional berhak menyimpan, mengalihmedia/format-kan, mengelola dalam bentuk pangkalan data (*database*) *soft copy* dan *hard copy*, 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 : Jakarta
Pada Tanggal : 8 Maret 2022

Yang menyatakan



Rakha Tri Fadillah

DAFTAR ISI

SKRIPSI	i
HALAMAN PERNYATAAN ORISINALITAS	ii
HALAMAN PERNYATAAN NON PLAGIAT	iii
HALAMAN PENGESAHAN	iv
KATA PENGANTAR	v
HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS	vi
ABSTRAK	vii
ABSTRACT	viii
DAFTAR ISI	ix
DAFTAR GAMBAR	xi
DAFTAR TABEL	xii
1. PENDAHULUAN	Error! Bookmark not defined.
1.1 Latar Belakang	Error! Bookmark not defined.
1.2 Rumusan Masalah	Error! Bookmark not defined.
1.3 Batasan Masalah	2
1.4 Manfaat	Error! Bookmark not defined.
1.5 Tujuan Penulisan	2
1.6 Sistematika Penulisan	3
2. TINJAUAN PUSTAKA	4
2.1 Pengertian <i>Malware</i>	4
2.2 Sejarah <i>Malware</i>	4
2.3 Jenis-jenis <i>Malware</i>	7
2.3.1 Virus	7
2.3.2 <i>Ransomware</i>	8
2.3.3 Worm	9
2.3.4 <i>Trojan</i>	9
2.3.5 Spyware	9
2.3.6 Rootkit	10
2.4 STOP <i>Ransomware</i>	10
2.5 Cuckoo Sandbox	10
2.6 Process Explorer	10
2.7 Pestudio	11
2.8 CryptoTester	11
2.9 RegShot	11
2.10 Teknik Analisis <i>Malware</i>	11
2.10.1 Analisis Statis	12
2.10.2 Analisis Dinamis	12
2.10.3 Hybrid	Error! Bookmark not defined.
3. METODOLOGI PENELITIAN	13
3.1 Pendahuluan	Error! Bookmark not defined.
3.2 Tahapan Penulisan	Error! Bookmark not defined.
3.2.1 Studi Literatur	14
3.2.2 Perancangan Dan Konfigurasi Sistem	14
3.2.3 Pengumpulan Data	14

3.2.4 Analisis Sistem.....	14
3.2.5 Pembuatan Laporan.....	16
3.3 Persiapan Sampel	Error! Bookmark not defined.
3.4 Konsep Rancangan Analisis.....	Error! Bookmark not defined.
3.5 Alat Penulisan	Error! Bookmark not defined.
4. HASIL DAN PEMBAHASAN.....	19
4.1 Tahapan Cuckoo Sandbox	19
4.2 Hasil Analisis	21
4.2.1 Analisis Statis	21
4.2.2 Analisis Dinamis.....	Error! Bookmark not defined.
5. KESIMPULAN DAN SARAN.....	35
5.1 Kesimpulan	35
5.2 Saran	35
DAFTAR PUSTAKA.....	36

DAFTAR GAMBAR

Gambar 3.1 Tahapan Penulisan	13
Gambar 3.2 Konsep Analisis Ransomware	16
Gambar 4.1 Menjalankan Perintah cuckoo	19
Gambar 4.2 Server cuckoo saat berjalan.....	20
Gambar 4.3 Proses Submit	20
Gambar 4.4 Hasil Analisis	21
Gambar 4.5 VirusTotal	22
Gambar 4.6 HexDump	24
Gambar 4.7 Strings	25
Gambar 4.8 Header dan Section	25
Gambar 4.9 Resources	26
Gambar 4.10 Imports	26
Gambar 4.11 Ransomware Popup	27
Gambar 4.12 File yang terinfeksi	29
Gambar 4.13 _readme file dari pembuat ransomware	29
Gambar 4.14 Perbandingan file Kalimba.mp3	30
Gambar 4.15 Perbandingan file Chrysanthemum.jpg.....	31
Gambar 4.16 Perbandingan file Wildlife.wmv.....	31
Gambar 4.17 HTTPS	32
Gambar 4.18 DNS	33
Gambar 4.19 Value	33
Gambar 4.20 Value file registry	34

DAFTAR TABEL

Tabel 4.1 Signatures.....	22
Tabel 4.2 Perbandingan proses CPU, Memory, I/O Usage.....	28