

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PERSETUJUAN	ii
HALAMAN PENGESAHAN	iii
HALAMAN PERSEMBAHAN	iv
HALAMAN MOTTO	v
INTISARI	vi
KATA PENGANTAR	vii
DAFTAR ISI	x
DAFTAR TABEL	xiv
DAFTAR GAMBAR	xv
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	3
1.3 Ruang lingkup	3
1.4 Tujuan Penelitian	3
BAB II TINJAUAN PUSTAKA DAN DASAR TEORI ..	4

2.1 Tinjauan Pustaka	4
2.2 Dasar Teori	5
2.2.1 Malware	5
2.2.2 Jenis Jenis Malware	6
2.2.2.1 Virus	6
2.2.2.1 Worm	6
2.2.2.1 Trojan	6
2.2.3 Windows	7
2.2.4 Windows API	8
2.2.4.1 Kernel API	8
2.2.4.2 User API	9
2.2.5 Analisis Malware	9
2.2.6 Teknik Analisis Malware	10
2.2.6.1 Analisis Statis	10
2.2.6.1 Analisis Dinamis	10
2.2.7 Disassembly	11
BAB III ANALISIS SISTEM	12

3.1 Analisis Sistem	12
3.1.1 Menyiapkan dan Melakukan Instalasi	
System Operasi	12
3.1.2 Melakukan Instalasi Tools untuk pro-	
Ses Analisis	12
3.1.3 Melakukan Analisis Statis	13
3.1.3.1 Proses Disassembly Terhadap	
File Biner Trojan	14
3.3.4 Melakukan Analisis Dinamis	15
BAB IV IMPLEMENTASI DAN PEMBAHASAN	
SISTEM	18
4.1 Pembahasa Sistem	18
4.1.1 Menginstal Tools Analisis Malw-	
are Pada SO Windows	18
4.1.2 Mencari File Malware Trojan ...	21
4.1.3 Melakukan Karantina Terhadap	
File Malware Trojan	23

4.2 Pembahasa Sistem	24
4.2.1 Analisis Statis	24
4.2.2 Analisis Dinamis	44
BAB V PENUTUP	47
5.1 Kesimpulan	47
5.2 Saran	47

DAFTAR TABEL

Tabel 4.1 Daftar String	33
-------------------------------	----

Tabel 4.2 Tabel Windows API	35
Tabel 4.3 Daftar String	36
Tabel 4.3 Variabel dan Data	36

DAFTAR GAMBAR

Gambar 3.1 Flowchart Proses disassembly	14
Gambar 3.4 Flowchart Proses analisis dinamis	15

Gambar 3.5 flowchart A proses analisis dinamis	16
Gambar 3.6 flowchart B proses analisis dinamis	17
Gambar 4.1 kotak pilihan license	18
Gambar 4.2 kotak pilihan lokasi install	19
Gambar 4.3 tampilan tool regshot	20
Gambar 4.4 tampilan tool process monitor	20
Gambar 4.5 hasil properties dari file program yang dicurigai	22
Gambar 4.6 hasil properties dari file program yang asli ..	22
Gambar 4.7 membandingkan file menggunakan md5sum..	23
Gambar 4.8 sharing file Trojan dari linux ke windows ...	24
Gambar 4.9 proses load file Trojan IEXPLORE.exe	25
Gambar 4.10 kode assembly dari file Trojan IEXPLORE.exe	26
Gambar 4.11 kode assembly dari file Trojan IEXPLORE.exe	26
Gambar 4.12 kode assembly dari file Trojan IEXPLORE.exe	27
Gambar 4.13 kode assembly dari fungsi sub_408E80	28
Gambar 4.14 kode assembly Trojan IEXPLORE.exe	29

Gambar 4.15 fungsi yang terdapat di dalam Trojan	31
Gambar 4.16 fungsi yang terdapat di dalam Trojan	31
Gambar 4.17 string yang terdapat di dalam Trojan	33
Gambar 4.18 fungsi yang menggunakan string prettysky.com	34
Gambar 4.19 string yang terdapat di dalam Trojan	36
Gambar 4.20 code assembly dari string	37
Gambar 4.21 kode dalam bentuk bahasa c++	37
Gambar 4.22 string dipanggil oleh fungsi	38
Gambar 4.23 kode assembly dari fungsi sub_408E0C ..	40
Gambar 4.25 konversi fungsi sub_408E0C ke c++	41
Gambar 4.26 Keadaan registry sebelum eksekusi <i>Trojan</i>	43
Gambar 4.27 pembuatan file md5 dari IEXPLORE.exe	43
Gambar 4.28 Regshot sebelum eksekusi	44
Gambar 4.29s capture paket dengan wireshark	45
Gambar 4.30 key registry yang ditambahkan	46
Gambar 4.31 key registry yang ditambahkan	46

Gambar 4.32 validasi file dengan md5sum setelah eksekusi 47

Gambar 4.33 hasil compare regshot sebelum dan sesudah eksekusi

..... 47

Gambar 4.34 monitoring proses dengan process monitor. 48

Gambar 4.35 pemantauan jaringan menggunakan wireshark 48