

DAFTAR ISI

HALAMAN SAMPUL	i
HALAMAN JUDUL.....	ii
HALAMAN PERSETUJUAN.....	iii
HALAMAN PENGESAHAN.....	iv
HALAMAN PERNYATAAN KEASLIAN	v
HALAMAN PERSEMBAHAN.....	vi
HALAMAN MOTTO	viii
KATA PENGANTAR	ix
DAFTAR ISI.....	xi
DAFTAR TABEL.....	xiii
DAFTAR GAMBAR	xiv
DAFTAR LAMPIRAN.....	xv
INTISARI.....	xvi
<i>ABSTRACT</i>	xvii
BAB I PENDAHULUAN	
A. Latar Belakang Masalah	1
B. Rumusan Masalah.....	5
C. Batasan Masalah	5
D. Tujuan Penelitian	6
E. Manfaat Penelitian	6
BAB II TINJAUAN PUSTAKA	
A. Landasan Teori.....	7
B. Penelitian Sebelumnya.....	16
BAB III METODE PENELITIAN	
A. Tempat dan Waktu Penelitian.....	22
B. Metode Pengumpulan Data.....	22
C. Alat dan Bahan Penelitian.....	23
D. Konsep Penelitian	25

BAB IV HASIL DAN PEMBAHASAN

A. Pengumpulan Data 28
B. Penerapan metode analisis packed malware 28

BAB V PENUTUP

A. Kesimpulan 50
B. Saran 51

DAFTAR PUSTAKA

LAMPIRAN



DAFTAR TABEL

Tabel 2. 1 Perbandingan Penelitian Terdahulu	19
Tabel 4. 1 Hasil identifikasi <i>Hybrid analysis</i>	37
Tabel 4. 2 <i>File Section malware</i> xinchao.....	39
Tabel 4. 3 <i>File Import malware</i> xinchao.....	41
Tabel 4. 4 Nilai <i>string</i> yang didapat dari <i>malware</i> xinchao.exe	45
Tabel 4. 5 <i>Library</i> yang digunakan pada <i>malware</i> xinchao.....	47



DAFTAR GAMBAR

Gambar 1. 1 Jumlah serangan <i>malware</i> dalam 5 tahun terakhir	2
Gambar 2. 1 <i>Hybrid analysis</i>	10
Gambar 2. 2 PE Studio.....	12
Gambar 2. 3 CFF Explorer.....	13
Gambar 2. 4 Alur Teknik <i>Reverse engineering</i>	14
Gambar 4. 1 <i>Virtualbox</i>	28
Gambar 4. 2 <i>Windows 10</i>	29
Gambar 4. 3 <i>VirusTotal</i>	29
Gambar 4. 4 PE Studio.....	30
Gambar 4. 5 <i>Hybrid analysis</i>	31
Gambar 4. 6 CFF Explorer.....	32
Gambar 4. 7 Pengujian <i>Packed Malware</i>	33
Gambar 4. 8 <i>Unpacked Malware</i>	33
Gambar 4. 9 CPU Overrun.....	34
Gambar 4. 10 Hasil Identifikasi <i>VirusTotal</i>	36
Gambar 4. 11 Tampilan <i>hybrid analysis</i>	37
Gambar 4. 12 <i>File sections malware xinchao</i>	38
Gambar 4. 13 <i>File Import malware xinchao</i>	40
Gambar 4. 14 <i>Contacted Hosts</i>	43
Gambar 4. 15 Tampilan <i>string</i> pada PE Studio.....	44
Gambar 4. 16 <i>Library</i> yang digunakan oleh <i>xinchao</i>	47
Gambar 4. 17 Hasil Disassembler CFF Explorer	48

DAFTAR LAMPIRAN

Lampiran 1 Kartu Bimbingan 1

Lampiran 2 Kartu Bimbingan 2

Lampiran 3 Website sampel *malware* MalShare.com

Lampiran 4 Link sampel *malware* yang digunakan

