Daftar Isi

METODE KLASIFIKASI DAN ANALISIS KARAKTERISTIK MALWARE MEGGUNAKAN ONTOLOGI i
HALAMAN PENGESAHAN PEMBIMBING ..... **Error! Bookmark not defined.**
HALAMAN PENGESAHAN PENGUJI ..... **Error! Bookmark not defined.**
ABSTRAK….. iv
ABSTRACT…..... v
PERNYATAAN KEASLIAN KARYA vi
PUBLIKASI SELAMA MASA STUDI..... vii
PUBLIKASI YANG MENJADI BAGIAN DARI TESIS..... viii
HALAMAN PERSEMBAHAN vix
KATA PENGANTAR…..... x
DAFTAR ISI……..... xii
DAFTAR TABLE…. xv
DAFTAR GAMBAR……..... xvi
Bab 1 Pendahuluan 1
1.1 Latar Belakang Penelitian..... 1
1.2 Rumusan Masalah 4
1.3 Batasan Masalah..... 4
1.4 Tujuan Penelitian..... 5
1.5 Manfaat Penelitian..... 5
1.6 Review Penelitian..... 5
1.7 Metode Penelitian..... 10
1.8 Sistematika Penulisan..... 10
Bab 2 Landasan Teori..... 12
2.1 Defenisi *Malware* 12
2.2 Analisis *Malware*..... 13
2.2.1 Analisis Statis 13
2.2.2 Analisis Dinamis 14
2.3 Kategori *Malware*..... 15
2.4 Masalah Pada Analisis *Malware* 16
2.5 Ontologi..... 16
2.6 Kategori Ontologi..... 16
2.7 Komponen Ontologi 17
2.8 Konstruksi Ontologi 20
2.9 *Protégé* 22

2.9.1 Ontograf 22
2.10 Penelitian Terkait 23
Bab 3 Metodologi 25
3.1 Analisis Penelitian 25
3.1.1 Objek Penelitian 25
3.1.2 Metode Pengumpulan Data 25
3.1.3 Kebutuhan Perangkat 25
3.2 Pemodelan Sistem 26
3.2.1 Analisis Sistem 26
3.2.2 Metode Pengembangan Sistem 26
3.3 Rancangan Pemodelan Sistem 27
3.3.1 Rancangan Model *Owl Viz* Ontologi Karakteristik *Malware* 28
3.3.2 Rancangan Model Ontograf Ontologi Karakteristik *Malware* 29
3.3.3 Tahapan Pengujian 30
Bab 4 Hasil Dan Pembahasan 31
4.1 Skema Analisis 31
4.1.1 Tahapan Pra Analisis 33
4.1.2 Tahapan Proses Analisis 34
4.1.3 Skenario Analisis 34
4.2 Hasil Analisis *Malware* 35
4.2.1 Analisis *Malware* Trojan 35
4.2.2 Analisis Virus 44
4.2.3 Analisis Exploit 54
4.2.4 Analisis Worm 65
4.2.5 Analisis Adware 74
4.3 Karakteristik *Malware* 83
4.4 Hirarki Karakteristik *Malware* 83
4.4.1 Karakteristik *Payload* / Muatan 83
4.4.1.1 *Integrity Violating* 84
4.4.1.2 *Confidentiality Violating* 84
4.4.1.3 *Avialability Violating* 84
4.4.1.4 *Safety Violating* 85
4.4.2 Karakteristik *Vector* 85
4.4.2.1 *Plurality* 85
4.4.2.2 *Transivity* 85
4.4.2.3 *Instiuacy* 85
4.4.2.4 *Locality* 86
4.4.2.5 *Invocation* 86

4.4.3 Karakteristik *Obfuscation* 86
4.4.3.1 *Stealth* 86
4.4.3.2 *Tunneling* 86
4.4.3.3 *Polymorphism* 87
4.4.3.4 *Metamorphic* 87
4.4.4 Karakteristik *Packer* 87
4.4.4.1 *Encryption Algorithms* 87
4.4.4.2 *Compression Algorithms* 88
4.5 Ontologi *Malware* 88
4.5.1 *Properties* 88
4.5.2 *Class* 89
4.5.3 Struktur Karakteristik Trojan Horse 89
4.5.4 Struktur Karakteristik Virus 89
4.5.5 Struktur Karakteristik Exploit 90
4.5.6 Struktur Karakteristik Worm 90
4.5.7 Struktur Karakteristik Adware 91
4.6 Implementasi Ontologi 91
4.7 Ontograf 95
Bab 5 Kesimpulan Dan Saran 100
5.1 Kesimpulan 100
5.2 Saran 101
Daftar Pustaka 102
LAMPIRAN 104

Daftar Tabel

Table 1.1 Review Paper Penelitian 7
Table 4.1 Tabel Perbandingan Penelitian 99

Daftar Gambar

Gambar 1.1 *Mobile Malware Category* 2013 1
Gambar 1.2 *New Varian Malware* (G Data, 2015) 2
Gambar 1.3 *New sample Malware* (Av-Test.org, 2016) 2
Gambar 2.1 Jenis *Malware* (http://www.transiskom.com/2013) 12
Gambar 2.2 Representasi *Individual* 17
Gambar 2.3 Representasi *class* (terdapat *Individual)* 18
Gambar 2.4 *Functionl Property* 18
Gambar 2.5 *Inverse Function Property* 19
Gambar 2.6 *Transitive Properties* 19
Gambar 2.7 *Symetric Properties* 20
Gambar 2.8 Ontologi struktur model (Thunkijjanukij and Kawtrakul 2009) 21
Gambar 3.1 Metode *Malware Analysis Body of Knowledge* 26
Gambar 3.2 Metode Usulan Ontologi Analisis Karakteristik *Malware* 27
Gambar 3.3 Rancangan Model *Owl Viz* Karakteristik Analisis *Malware* 28
Gambar 3.4 Rancangan Ontograf Analisis Karakteristik Malware 29
Gambar 4.1 Analisis Paket Trojan Horse Sougou PY 35
Gambar 4.2 Header File Trojan Horse Sougou PY 36
Gambar 4.3 Analisis Dependensi Modul Trojan Horse Sougou PY 37
Gambar 4.4 Analisis Fungsi Call Trojan Horse Sougou PY 37
Gambar 4.5 Analisis fungsi Push Trojan Horse Sougou PY 38
Gambar 4.6 Analisis Teknik Penyamaran Malware Config.exe 38
Gambar 4.7 Analisis Header File Malware Config.exe 39
Gambar 4.8 Analisis Dependensi Modul Malware Config.exe 40
Gambar 4.9 Analisis Kode Malware Config.exe 40
Gambar 4.10 Analisis Teknik Penyamaran Trojan.Win32.Midgare.jnk 41
Gambar 4.11 Analisis Header File Trojan.Win32.Midgare.jnk 42
Gambar 4.12 Analisis Dependensi Modul Trojan.Win32.Midgare.jnk 42
Gambar 4.13 Analisis Kode Trojan.Win32.Midgare.jnk 43
Gambar 4.14 Analisis Paket Virus.Win32.MTV.a 44
Gambar 4.15 Header File Wirus.Win32.MTV.a 45
Gambar 4.16 Analisis Dpenedensi Modul Virus.Win32.MTV.a 45
Gambar 4.17 Analisis Kode Virus.Win32.MTV.a 46

Gambar 4.18 Virus.Win9x.Chimera.1542 47
Gambar 4.19 Analisis Header File Virus.Win9x.Chimera.1542 47
Gambar 4.20 Analisis Dependensi Modul Virus.Win9x.Chimera.1542 48
Gambar 4.21 Analisis Kode Virus.Win9x.Chimera.1542 49
Gambar 4.22 Analisis Teknik Penyamaran Virus.Win9x.Sillywr.180.c 49
Gambar 4.23 Analisis Header File Virus.Win9x.Sillywr.180.c 50
Gambar 4.24 Analisis Dependensi Modul Virus.Win9x.Sillywr.180.c 51
Gambar 4.25 Analisis Kode Virus.Win9x.Sillywr.180.c 52
Gambar 4.26 Lanjutan Analisis Kode Virus.Win9x.Sillywr.180.c 53
Gambar 4.27 Analisis Paket/Penyemaran Exploit.IIS.Danet 54
Gambar 4.28 Analisis Header File Exploit.IIS.Danet 54
Gambar 4.29 Analisis Header File Exploit.IIS.Danet 55
Gambar 4.30 Analisis Kode Exploit.IIS.Danet 56
Gambar 4.31 Lanjutan Analisis Kode Exploit.IIS.Danet 56
Gambar 4.32 Website Yang Disisipkan pada Exploit.IIS.Danet 57
Gambar 4.33 Analisis Teknik Penyamaran Exploit Cndcom 57
Gambar 4.34 Analisis Header File Exploit Cndcom 58
Gambar 4.35 Analisis Dependensi Modul Exploit Cndcom 59
Gambar 4.36 Analisis Kode Exploit Cndcom 60
Gambar 4.37 Analisis Teknik Penyamaran Exploit.Win32.Serv-u 61
Gambar 4.38 Analisis Teknik Penyamaran Exploit.Win32.Serv-u 61
Gambar 4.39 Analisis Dependensi Modul Exploit.Win32.Serv-u 62
Gambar 4.40 Analisis Kode Exploit.Win32.Serv-u 63
Gambar 4.41 Lanjutan Analisis Kode Exploit.Win32.Serv-u 64
Gambar 4.42 Analisis Paket Worm.Win32.Pikachu 65
Gambar 4.43 Analisis Header File Worm.Win32.Pikachu 65
Gambar 4.44 Analisis Dependensi Modul Worm.Win32.Pikachu 66
Gambar 4.45 Analisis Kode Worm.Win32.Pikachu 67
Gambar 4.46 Analisis Teknik Penyamaran Email-Worm.Win32.Locksky.al 68
Gambar 4.47 Analisis Header File Email-Worm.Win32.Locksky.al 68
Gambar 4.48 Analisis Dependensi Modul Email-Worm.Win32.Locksky.al 69
Gambar 4.49 Analisis Kode Email-Worm.Win32.Locksky.al 70
Gambar 4.50 Analisis Teknik Penyamaran Worm.Win32.Sonic.a 70
Gambar 4.51 Analisis Teknik Penyamaran Worm.Win32.Sonic.a 71
Gambar 4.52 Analisis Dependensi Modul Worm.Win32.Sonic.a 72

Gambar 4.53 Analisis Kode Worm.Win32.Sonic.a 72
Gambar 4.54 Lanjutan Analisis Kode Worm.Win32.Sonic.a 73
Gambar 4.55 Analisis Paket Adware.Hotbar 74
Gambar 4.56 Analisis Header File Adware.Hotbar 74
Gambar 4.57 Analisis Dependensi Modul Adware.Hotbar 75
Gambar 4.58 Analisis kode Adware.Hotbar 76
Gambar 4.59 Analisis Teknik Penyamaran Adware.Cinmus-2777 77
Gambar 4.60 Analisis Header File Adware.Cinmus-2777 77
Gambar 4.61 Analisis Dpendensi Modul Adware.Cinmus-2777 78
Gambar 4.62 Analisis Kode Adware.Cinmus-2777 79
Gambar 4.63 Analisis Teknik Penyamaran W32.Adware an 80
Gambar 4.64 Analisis Header File W32.Adware an 81
Gambar 4.65 Analisis Modul W32.Adware an 81
Gambar 4.66 Analisis Kode w32.adware an. 82
Gambar 4.67 Karakteristik Malware 83
Gambar 4.68 Karakteristik Payload 84
Gambar 4.69 Struktur karakteristik Trojan Horse 89
Gambar 4.70 Struktur Karakteristik Virus 89
Gambar 4.71 Struktur Karakteristik Exploit 90
Gambar 4.72 Struktur Karaktersitik Worm 90
Gambar 4.73 Struktur Karakteristik Adware 91
Gambar 4.74 *Class* dan *Sub Class* Ontologi Analisis *Malware* 91
Gambar 4.75 *Object Property* Ontologi Analisis *Malware* 92
Gambar 4.76 *Owl Viz* Diagram Ontologi Analisis *Malware* 92
Gambar 4.77 *Owl Viz* Diagram Karakteristik Analisis *Malware* 93
Gambar 4.78 *Owl Viz* Diagram Ontologi Analisis *Malware* 94
Gambar 4.79 Proses Perancangan Ontograf Analisis *Malware* 96
Gambar 4.80 Ontograf Diagram Analisis *Malware* 97