Daftar Isi

Daftar Isi i

Daftar Tabel xii

Daftar Gambar xiii

BAB 1 Pendahuluan 15

1.1 Latar Belakang 15

1.2 Rumusan Masalah 18

1.3 Batasan Maslah 18

1.4 Tujuan Penelitian 18

1.5 Manfaat Penelitian 18

1.6 *Review* Penelitian 19

1.7 Metodologi Penelitian 25

1.8 Sistematika Penulisan 26

BAB 2 Tinjauan Pustaka 27

2.1 Malware 27

2.1.1 Sejarah malware 27

2.1.2 Jenis-Jenis Malware 28

2.1.3 Perkembangan Malware 29

2.2 Metode-Metode Deteksi 33

2.2.1 *Signature Based Detection* 33

2.2.2 *Behavior Based Detection* 34

2.2.3 *Statistic Based Detection* 34

BAB 3 Metodologi Penelitian 35

3.1 Pendahuluan 35

3.2 Tinjauan Pustaka 35

3.3 Analisis 36

3.3.1 Malware dan Aplikasi yang dianalisis 36
3.3.2 Sistem dan *Tools* Analisis 36
3.3.3 Analisis dan *Extract Behavior Features* 37
3.4 Perancangan Skema Deteksi 37
3.5 Implementasi dan Testing Skema Deteksi 39
3.5.1 Implementasi 39
3.5.2 Testing sistem 39
3.6 Hasil 39
3.7 Kesimpulan 40
BAB 4 Hasil dan Pembahasan 41
4.1 Penerapan Metode *Behavior Approach* 41
4.1.1 *Behavior Operations* dan *Behavior Features* 42
4.1.2 User Sebagai Target *Behavior operations* 43
4.2 Komputer dan Sistem yang digunakan 43
4.3 Analisis 44
4.3.1 Malware yang digunakan 44
4.3.2 Sistem dan *Tools* yang Digunakan 44
4.3.3 Analisis Dinamis 44
4.3.4 *Extract Behavior Features* 48
4.4 Implementasi Sistem Deteksi Malware 48
4.4.1 Instalasi Python 2.7 48
4.4.2 Implementasi kedalam Script Python 49
4.5 Pengujian Sistem dan Hasil 52
4.5.1 Testing Untuk Aplikasi 53
4.5.2 Testing Untuk Malware Locky Ransomware 57
4.5.3 Hasil Testing Rata-Rata 58
4.6 Analisis Hasil dan Penerapan Metode 60

4.6.1 Analisis Hasil Testing 60
4.6.2 Analisis Hasil Penerapan Metode *Behavior* 61
4.6.3 Hasil 61
BAB 5 Kesimpulan dan Saran 62
5.1 Kesimpulan 62
5.2 Saran 62
Daftar Pustaka 63
LAMPIRAN A.1 67
LAMPIRAN A.2 68
LAMPIRAN A.3 69
LAMPIRAN A.4 70
LAMPIRAN B.1 71
LAMPIRAN B.2 80
LAMPIRAN B.3 101

Daftar Tabel

Tabel 1. 1 Kelebihan dan kekurangan signature dan behavior 15
Tabel 1. 1 Kelebihan dan kekurangan signature dan behavior (Lanjutan) 16
Tabel 1. 3 Literatur Review Penelitian 21
Tabel 1. 4 Literatur Review Penelitian (Lanjutan) 22
Tabel 1. 5 Literatur Review Penelitian (Lanjutan) 23
Tabel 1. 6 Literatur Review Penelitian (Lanjutan) 24
Tabel 4. 1 Spesifikasi komputer yang digunakan 43
Tabel 4. 2 Data hasil testing *application behavior* MsWord 53
Tabel 4. 3 Data hasil testing *application behavior* MsExcel 55
Tabel 4. 4 Data hasil testing malware Locky Ransomware behaviour 57
Tabel 4. 5 Data rangkuman hasil testing rata-rata aplikasi normal dan malware 58

Daftar Gambar

Gambar 1.1 Gambaran penelitian yang sudah ada dan yang akan diusulkan. 16
Gambar 1.2 Alur Metode Penelitian. 25
Gambar 2.1 Malware baru dalam angka sejak tahun 1984 – 2017 30
Gambar 2.2 Total Malware dalam kurun waktu 10 (sepuluh) tahun terakhir. 31
Gambar 3.1 Alur metode penelitian 35
Gambar 3.2 Skema sistem deteksi malware 37
Gambar 3.3 Monitoring proses 38
Gambar 3.4 Proses Komparasi *Behavior* 39
Gambar 4.4 Perintah *cuckoo* untuk menjalankan *cuckoo sandbox* 46
Gambar 4.5 Screenshot hasil analisis *cuckoo* pada malware 47
Gambar 4.6 Proses debugging pada malware di cmd 48
Gambar 4.7 Flowchart dari script utama sistem deteksi malware. 51
Gambar 4. 8 Data perbedaan *behaviour* aplikasi normal dan malware 59