

DAFTAR ISI

ABSTRACT	i
ABSTRAK	ii
KATA PENGANTAR	iii
DAFTAR ISI	v
DAFTAR TABEL	vii
DAFTAR GAMBAR	vii

BAB I PENDAHULUAN

1.1 Latar Belakang	I-1
1.2 Rumusan Masalah	I-2
1.3 Batasan Masalah.....	I-3
1.4 Tujuan Penelitian.....	I-3
1.5 Manfaat Penelitian.....	I-3
1.6 Metodologi Penelitian	I-4
1.7 Sistematika Penulisan.....	I-5

BAB II LANDASAN TEORI

2.1 Android	II-1
2.1.1 Arsitektur Sistem Android	II-1
2.1.2 Aplikasi	II-2
2.1.3 Kerangka Kerja Aplikasi.....	II-2
2.1.4 <i>Libraries</i>	II-4
2.1.5 <i>Android RuntimeI</i>	II-6
2.1.6 <i>Linux Kernel</i>	II-6

2.2 Malware	II-7
2.2.1 Pengertian Malware	II-7
2.2.2 Jenis Jenis Malware.....	II-7
2.2.3 <i>Spynote</i> Malware.....	II-10
2.3 Teknik Analisis Malware.....	II-11
2.3.1 Analisis Dinamik	II-12
2.3.2 Analisis Statik	II-12
2.3.3 Analisis <i>Hybird</i>	II-13
2.4 <i>Virtual Box</i>	II-13
2.5 ANDROL4B	
2.5.1 <i>Mobile Scurity Framework (MobSF)</i>	II-14
2.6 Penelitian Terkait.....	II-14

BAB III METODOLOGI

3.1 Metode Penelitian.....	III-1
3.2 Perumusan Masalah	III-2
3.3 Pengumpulan Data	III-2
3.3.1 Studi Literatur.....	III-2
3.3.1 Observasi	III-2
3.4 Analisis Malware.....	III-3
3.4.1 <i>Code Review</i>	III-3
3.4.2 <i>Live Testing</i>	III-3
3.5 <i>Documentation</i>	III-4

BAB IV HASIL DAN PEMBAHASAN

4.1 <i>Code Review</i>	IV-1
4.2 <i>Decompile file Apk</i>	IV-3
4.3 <i>Decompile file Dex</i>	IV-8
4.3.1 <i>Analisis Class dan Source</i>	IV-9
4.3.2 <i>Analisis Source Class A</i>	IV-9
4.3.3 <i>Analisis Source Class B</i>	IV-18
4.3.4 <i>Analisis Source Class C</i>	IV-19
4.3.5 <i>Analisis Source Class D</i>	IV-21
4.3.6 <i>Analisis Source Class G</i>	IV-22
4.3.7 <i>Analisis Source Class M</i>	IV-23
4.3.8 <i>Analisis Source Class S</i>	IV-24
4.3.9 <i>Analisis Source Class B</i>	IV-25
4.4 <i>Live Testing</i>	IV-28
4.4.1 <i>File Patch Malware Apk Spynote</i>	IV-31
4.4.2 <i>Proses Install Pada Emulator Android</i>	IV-33
4.3.1 <i>Proses Sniffing Aplikasi Spynote</i>	IV-36
4.5 <i>Pencegahan Malware Spynote</i>	IV-40

BAB V KESIMPULAN DAN SARAN

V.1 <i>Kesimpulan</i>	V-1
V.2 <i>Saran</i>	V-2

DAFTAR PUSTAKA

LAMPIRAN.....

DAFTAR TABEL

Tabel 2.1 Tabel Penelitian Terdahulu Mengenai Investigasi Malware.....	II-14
Tabel 4.1 Informasi <i>Patch</i> Malware <i>Spynote</i>	IV-2
Tabel 4.2 Analisis File <i>AndroidManifest.xml</i>	IV-5
Tabel 4.3 Arsitektur Lokasi Fungsi Service Malware <i>Spynote</i>	IV-27
Tabel 4.4 Spesifikasi <i>Hardware</i> Emulator Android	IV-29
Tabel 4.5 Spesifikasi <i>Software</i>	IV-30
Tabel 4.6 Perbandingan Penggunaan <i>RAM</i> Malware <i>Spynote</i>	IV-38
Tabel 4.7 Karakteristik Malware <i>Spynote</i>	IV-39
Tabel 4.8 Hasil Scanning Malware <i>Spynote</i> menggunakan Antivirus	IV-41

DAFTAR GAMBAR

Gambar 2.1 Arsitektur Sistem Android	II-2
Gambar 2.2 Taksonomi Malware Menurut Wisnu Nurdianto	II-8
Gambar 2.3 Representasi <i>Hierarchal</i> Berbagai Teknik Deteksi Malware	II-11
Gambar 3.1 Tahapan Penelitian.....	III-1
Gambar 4.1 Data Builder <i>Spynote</i>	IV-1
Gambar 4.2 Alur Pengerjaan <i>Code Review</i>	IV-3
Gambar 4.3 Hasil Ekstrak Aplikasi Malware <i>Spynote</i>	IV-3
Gambar 4.4 Isi file <i>AndroidManifest.xml</i> Malware <i>Spynote</i>	IV-4
Gambar 4.5 Hasil <i>decompile</i> file <i>classes.dex</i>	IV-8
Gambar 4.6 <i>Source</i> Informasi <i>Device Info</i> pada <i>Class A</i>	IV-10
Gambar 4.7 <i>Source</i> Informasi <i>System Info</i> dan <i>Sim Info</i> pada <i>Class A</i>	IV-11

Gambar 4.8 <i>Source</i> Informasi Wifi pada <i>Class A</i>	IV-12
Gambar 4.9 <i>Source</i> Informasi status batrai pada <i>Class A</i>	IV-13
Gambar 4.10 <i>Source</i> Pengaktifan wifi Audio pada <i>Class A</i>	IV-14
Gambar 4.11 <i>Source</i> Informasi Kontak pada <i>Class A</i>	IV-15
Gambar 4.12 <i>Source</i> History panggilan telepon pada <i>Class A</i>	IV-16
Gambar 4.13 <i>Source</i> Informasi <i>Pengiriman SMS</i> pada <i>Class A</i>	IV-17
Gambar 4.14 <i>Source</i> Informasi Kamera pada <i>Class A</i>	IV-18
Gambar 4.15 Menjalankan Service Tertentu pada <i>Class A</i>	IV-19
Gambar 4.16 Proses Melakukan Panggilan Telepon	IV-20
Gambar 4.17 <i>Source</i> Fitur DeviceAdmin.....	IV-21
Gambar 4.18 <i>Source</i> Akses Lokasi	IV-22
Gambar 4.19 <i>Source</i> Pemanggilan Menjalankan <i>Package</i>	IV-23
Gambar 4.20 <i>Source</i> Pemanggilan <i>Service</i> sebagai <i>Activity</i>	IV-24
Gambar 4.21 <i>Source</i> Proses Pengiriman Sms	IV-25
Gambar 4.22 Pemanggilan <i>Class A</i> sebagai <i>RunningActiviry</i>	IV-26
Gambar 4.23 Skema Pengujian Malware.....	IV-29
Gambar 4.24 Alur Pengerjaan <i>Live Testing</i>	IV-30
Gambar 4.25 Skema Penyebaran Malware Spynote	IV-31
Gambar 4.26 Proses Build Malware <i>Spynote</i>	IV-32
Gambar 4.27 Hasil Instalasi Aplikasi Malware <i>Spynote</i>	IV-33
Gambar 4.28 Proses <i>Running</i> Aplikasi Malware <i>Spynote</i>	IV-34
Gambar 4.29 <i>Package</i> Malware <i>Spynote</i> pada <i>tools Inspecakge</i>	IV-35
Gambar 4.30 Service <i>Package yps.etos.application</i> yang berjalan	IV-36
Gambar 4.31 Hasil <i>Sniffing</i> Malware <i>Spynote</i> Menggunakan <i>Inspeckage</i>	IV-37

Gambar 4.32 Proses Cara Kerja Malware Spynote..... IV-38

Gambar 4.33 Informasi *Disable Uninstall* Malware..... IV-40