



**UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA**  
**ANALISIS TROJAN DAN *SPYWARE* MENGGUNAKAN**  
**METODE *HYBRID ANALYSIS***

**SKRIPSI**

**ANNISA RIZKY DAMANIK**  
**1810511102**

**PROGRAM STUDI INFORMATIKA**  
**FAKULTAS ILMU KOMPUTER**  
**UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN**  
**JAKARTA**

**2023**



**UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA**

**ANALISIS TROJAN DAN *SPYWARE* MENGGUNAKAN  
METODE *HYBRID ANALYSIS***

**SKRIPSI**

**Diajukan Sebagai Salah Satu Syarat Untuk Memperoleh Gelar  
Sarjana Komputer**

**ANNISA RIZKY DAMANIK**

**1810511102**

**PROGRAM STUDI INFORMATIKA**

**FAKULTAS ILMU KOMPUTER**

**UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN  
JAKARTA**

**2023**

## PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya saya sendiri, dan sumber yang dikutip maupun yang dirujuk telah saya nyatakan dengan benar.

Nama : Annisa Rizky Damanik  
NIM : 1810511102  
Tanggal : 22 Desember 2022

Bilamana dikemudian hari ditemukan ketidaksamaan dengan pernyataan ini, maka saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku.

Jakarta, 22 Desember 2022



Annisa Rizky Damanik

## LEMBAR PENGESAHAN

Tugas Akhir ini diajukan oleh:

Nama : Annisa Rizky Damanik  
NIM : 1810511102  
Program Studi : SI Informatika  
Judul Tugas Akhir : Analisis Trojan Dan Spyware Menggunakan Metode Hybrid Analysis

Telah berhasil dipertahankan dihadapan Tim Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana pada Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta.



Dr. Ermatita, M.Kom.  
Penguji I



Anita Muliawati, S.Kom., MTI.  
Penguji II



Henki Bayu Seta, S.Kom., MTI.  
Pembimbing



Dr. Widva Cholil, M.I.T.  
Kepala Program Studi

Ditetapkan di : Jakarta  
Tanggal Pengesahan : 18 Januari 2023



## LEMBAR PERSETUJUAN

Dengan ini menyatakan bahwa Skripsi/Tugas Akhir berikut:

Nama : Annisa Rizky Damanik  
NIM : 1810511102  
Program Studi : S1 Informatika  
Judul : Analisis Trojan dan Spyware Menggunakan Metode Hybrid  
Analysis

Sebagai bagian persyaratan yang diperlukan untuk mengikuti ujian Sidang Tugas Akhir/Skripsi pada Program Studi S1 Informatika Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta.

Menyetujui,

Dosen Pembimbing

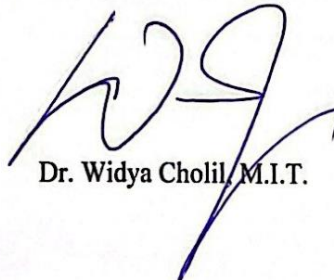


Henki Bayu Seta, S.Kom, MTI.

Mengetahui,

an. Ketua Program Studi

Wakil Dekan Bidang Akademik



Dr. Widya Cholil, M.I.T.

Ditetapkan : Jakarta  
Tanggal Persetujuan : 22 Desember 2022

## SURAT PERNYATAAN / PERSETUJUAN PUBLIKASI SKRIPSI

Sebagai civitas akademika Universitas Pembangunan Nasional Veteran Jakarta, saya yang bertandatangan dibawah ini:

Nama : Annisa Rizky Damanik  
NIM : 1810511102  
Fakultas : Ilmu Komputer  
Program Studi : Informatika  
Jenis Karya : Skripsi

Demi pengembangan ilmu pengetahuan, menyetujui skripsi saya untuk dipublikasikan Bersama Dosen Pembimbing dengan keterangan sebagai berikut:

Judul Skripsi :

**ANALISIS TROJAN DAN SPYWARE MENGGUNAKAN METODE HYBRID ANALYSIS**

Dosen Pembimbing : Henki Bayu Seta, S.Kom., MTI.  
NIDN : 0309118104

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta

Pada Tanggal : 24 Januari 2023



Annisa Rizky Damanik

# **ANALISIS TROJAN DAN *SPYWARE* MENGGUNAKAN METODE *HYBRID ANALYSIS***

**ANNISA RIZKY DAMANIK**

## **ABSTRAK**

*Malicious Software* atau *malware* merupakan sebuah *software* yang diciptakan untuk merusak sistem komputer. Peningkatan pengguna internet juga seiring dengan peningkatan penggunaan *software*. Namun, masih banyaknya pengguna yang masih menggunakan *software* bajakan karena relative gratis dan gampang didapatkan. *Software* bajakan biasanya sudah ditanamkan sebuah malware berbahaya seperti Trojan dan *spyware*. Trojan merupakan jenis malware yang paling sering ditemukan dalam sistem komputer dengan berbagai banyak kasus. Dan *spyware* adalah jenis malware yang sulit di terlihat aktivitasnya di sistem komputer, bahkan anti-virus sering tidak bisa mendeteksi jenis malware ini. Semua tindak kejahatan penyebaran malware ini selalu berkaitan dengan mencuri informasi kartu kredit, internet banking dan tindak *cybercrime* lainnya. Untuk membuktikan bahwa *software* yang diinstal dan digunakan pada *computer* adalah *software* berbahaya, dibutuhkan tindak forensic digital dengan menganalisis *software*. Teknik analisis hybrid merupakan analisis statis dan dinamis dikombinasikan yang sesuai untuk menganalisis aktivitas malware. Penulis mengharapkan dengan menggunakan metode analisis ini dapat membuktikan jejak aktivitas Trojan dan *spyware* berbahaya pada *software* yang digunakan.

***Kata kunci:*** *Malware, Trojan, Spyware, Cybercrime, Malware Hybrid Analysis, Dynamic Analysis, Static Analysis*

# **TROJAN AND SPYWARE ANALYSIS USING HYBRID ANALYSIS METHOD**

**ANNISA RIZKY DAMANIK**

## **ABSTRACT**

Malicious Software or malware is software created to damage a computer system. The increase in internet users is also in line with the increase in the use of software. However, there are still many users who still use pirated software because it is relatively free and easy to obtain. Pirated software is usually embedded with dangerous malware such as Trojans and spyware. Trojans are the most common type of malware found in computer systems with many cases. And spyware is a type of malware that is difficult to see its activity on a computer system, even anti-virus often cannot detect this type of malware. All crimes of spreading this malware are always related to stealing credit card information, internet banking and other cybercrimes. To prove that the software installed and used on a computer is malicious software, digital forensics is required by analyzing the software. Hybrid analysis technique is a combination of static and dynamic analysis which is suitable for analyzing malware activity. The author hopes that using this analysis method can prove traces of malicious Trojan and spyware activity in the software used.

**Keywords:** Malware, Trojan, Spyware, Cybercrime, Malware Hybrid Analysis, Dynamic Analysis, Static Analysis



## **KATA PENGANTAR**

Puji dan syukur penulis panjatkan kehadiran Allah SWT atas nikmat dan karunia beserta rahmat-Nya, sehingga penulis dapat menyelesaikan skripsi sebagai syarat kelulusan yang berjudul “Analisis Trojan Dan Spyware Menggunakan Metode Hybrid Analysis”.

Pada kesempatan ini penulis mengucapkan terima kasih kepada Bapak Henki Bayu Seta, S.Kom., MTI. Selaku pembimbing yang telah membimbing dan memberikan saran serta arahan dalam penyusunan skripsi ini. Serta tak lupa pula penulis sampaikan terima kasih kepada kedua orang tua yang selalu memberikan dukungan dan motivasi kepada penulis. Dan juga kepada saudara penulis dan teman-teman yang juga memberikan dukungan, bantuan dan doa selama ini.

Semoga skripsi ini dapat memberikan manfaat dan ilmu yang berguna di masa mendatang.

Jakarta, 24 Januari 2023

Annisa Rizky Damanik

## DAFTAR ISI

PERNYATAAN ORISINALITAS LEMBAR PENGESAHAN.....	i
LEMBAR PERSETUJUAN.....	iii
SURAT PERSETUJUAN PUBLIKASI SKRIPSI .....	iv
ABSTRAK .....	v
ABSTRACT .....	vi
KATA PENGANTAR .....	vii
DAFTAR ISI.....	viii
DAFTAR GAMBAR .....	xi
DAFTAR TABEL.....	xiv
DAFTAR LAMPIRAN.....	xv
BAB 1 PENDAHULUAN .....	1
1.1 Latar Belakang Masalah.....	1
1.2 Rumusan Masalah .....	3
1.3 Ruang Lingkup .....	3
1.4 Tujuan Penelitian.....	3
1.5 Manfaat Penelitian.....	3
1.6 Luaran Yang Diharapkan .....	4
1.7 Sistematika Penulisan.....	4
BAB 2 LANDASAN TEORI.....	6
2.1 Cybercrime .....	6
2.2 Malware.....	6
2.2.1 Definisi Malware.....	6
2.2.2 Klasifikasi Malware .....	7
2.2.2.1 Klasifikasi berdasarkan jenis malware .....	8
2.2.2.2 Klasifikasi berdasarkan perilaku Malware .....	9

2.3	Sampel Malware.....	12
2.4	Metode Malware Analisis .....	13
2.3.1	Metode Analisis Statis .....	13
2.3.2	Metode Analisis Dinamis.....	15
2.3.3	Metode Analisis Hybrid .....	15
2.5	Penelitian Terdahulu.....	15
BAB 3 METODOLOGI PENELITIAN.....		18
3.1	Kerangka Pikiran .....	18
3.2	Tahapan Penelitian .....	19
3.2.1	Identifikasi Masalah .....	19
3.2.2	Pengumpulan Data .....	19
3.2.3	Tahapan dalam pembuatan sampel malware.....	19
3.2.3.1	Membuat malware skripsi01.exe berjenis trojan malware .....	19
3.2.4	Tahap Analisis Malware .....	22
3.2.5	Dokumentasi .....	26
3.3	Peralatan Operasional.....	26
3.3.1	Hardware Yang Digunakan.....	26
3.3.2	Software Yang Digunakan .....	26
3.4	Jadwal Penelitian .....	27
BAB 4 HASIL DAN PEMBAHASAN.....		28
4.1	Pembuatan Sampel Malware .....	28
4.1.1	Pembuatan sampel skripsi01.exe .....	28
4.1.2	Pembuatan sampel money.exe .....	32
4.2	Analisis Statis .....	34
4.2.1	Membangun Lingkungan Kerja Analisis Statis .....	34
4.2.2	Sampel <i>Spyware</i> : Money.exe .....	36

4.2.3	Sampel Trojan: skripsi01.exe.....	41
4.3	Analisis Dinamis .....	47
4.4	Hybrid Analysis.....	52
4.4.1	Sampel <i>Spyware</i> : money.exe .....	53
4.4.2	Sampel Trojan: Skripsi01.exe .....	55
4.5	Hasil Dari Analisis .....	56
BAB 5 KESIMPULAN DAN SARAN .....		59
5.1	Kesimpulan.....	59
5.2	Saran .....	59

#### DAFTAR PUSTAKA

#### LAMPIRAN

## DAFTAR GAMBAR

Gambar 1. 1 Data Grafik pertumbuhan populasi pengguna internet setiap tahun ...	1
Gambar 2. 1 Variasi taksonomi malware .....	7
Gambar 2. 2 Metode analisis malware .....	13
Gambar 3. 1 Tahapan Penelitian .....	18
Gambar 3. 2 Tahapan Analisis Malware Statis .....	23
Gambar 3. 3 Alur Analisis Dinamis .....	25
Gambar 4. 1 Tampilan OS Kali Linux .....	28
Gambar 4. 2 Command kali linux: instalisasi TheFarrat .....	29
Gambar 4. 3 Checking kebutuhan dalam tool TheFarrat .....	30
Gambar 4. 4 TheFarrat .....	30
Gambar 4. 5 Membuat malware farrat dengan ip addr .....	31
Gambar 4. 6 Letak File Malware yang telah dibuat .....	31
Gambar 4. 7 Malware skripsi01.exe .....	32
Gambar 4. 8 root sistem kali linux .....	32
Gambar 4. 9 Metasploit .....	33
Gambar 4. 10 perintah pembuatan file money.exe .....	33
Gambar 4. 11 Instalasi OS windows 7 .....	34
Gambar 4. 12 Tampilan dari PeStudio .....	35
Gambar 4. 13 Pengecekan sampel skripsi01.exe .....	35
Gambar 4. 14 Pengecekan sampel money.exe .....	36

Gambar 4. 15 Struktur dari malware money.exe .....	37
Gambar 4. 16 String malware money.exe .....	38
Gambar 4. 17 Lybrary malware money.exe.....	39
Gambar 4. 18 Import yang digunakan spyware money.exe.....	40
Gambar 4. 19 Struktur dari malware skripsi01.exe.....	42
Gambar 4. 20 String malware skripsi01.exe .....	43
Gambar 4. 21 Lybrary pada malware skripsi01.exe .....	44
Gambar 4. 22 Import pada malware skripsi01.exe .....	46
Gambar 4. 23 Instalasi OS windows 7 .....	48
Gambar 4. 24 menjalankan malware money.exe .....	48
Gambar 4. 25 tampilan metasploit kali linux .....	49
Gambar 4. 26 informasi komputer pengguna.....	49
Gambar 4. 27 Trace malware spyware money.exe .....	49
Gambar 4. 28 Lanjutan trace malware money.exe.....	50
Gambar 4. 29 Process hacker menjalan money.exe.....	51
Gambar 4. 30 Trace malware skripsi01.exe.....	52
Gambar 4. 31 Tampilan dari Tool hybrid analysis .....	53
Gambar 4. 32 hybrid analisis pada money.exe .....	53
Gambar 4. 33 Beberapa daftar antivirus yang mendeteksi malware pada file.....	54
Gambar 4. 34 tipe perilaku pada malware .....	54
Gambar 4. 37 hybrid-analysis.com pada malware skripsi01.exe.....	55

Gambar 4. 38 hasil scan anti virus pada malware skripsi01.exe..... 55

## DAFTAR TABEL

Tabel 2. 1 Penelitian sebelumnya.....	16
Tabel 3. 1 Jadwal Penelitian.....	27
Tabel 4. 1 Rangkuman sampel spyware Regasm.bin.....	37
Tabel 4. 2 Hasil String spyware money.exe.....	38
Tabel 4. 3 Library dari spyware money.exe.....	39
Tabel 4. 4 Import yang digunakan spyware money.exe.....	40
Tabel 4. 5 Rangkuman sampel trojan skripsi01.exe .....	42
Tabel 4. 6 String pada trojan skripsi01.exe.....	44
Tabel 4. 7 Library dan import pada malware skripsi01.exe.....	45
Tabel 4. 8 Data import malware skripsi01.exe .....	46
Tabel 4. 9 Jumlah String, Library dan Import pada sampel.....	56
Tabel 4. 10 Hasil data yang didapat dari metode dinamis .....	57
Tabel 4. 11 Hasil data yang didapat dari metode statis.....	57
Tabel 4. 12 Hasil data yang didapat dari metode hybrid analysis.....	57



## DAFTAR LAMPIRAN

Lampiran 1 Virtual Lab Machine yang digunakan .....	62
Lampiran 2 Operasi Sistem yang Digunakan: OS Windows 7 .....	62
Lampiran 3 Operasi Sistem yang digunakan: Kali Linux .....	63
Lampiran 4 Tools yang digunakan dalam analisis .....	63
Lampiran 5 Tools Membuat Sampel Malware .....	66