ANALISIS HYBRID REVERSE ENGINEERING MALWARE WINDOWS BERBASIS LINGKUNGAN ISOLASI FLARE VM

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Teknik Komputer

disusun oleh

INDRA BAGAS PRATAMA

22.83.0859

Kepada

FAKULTAS ILMU KOMPUTER

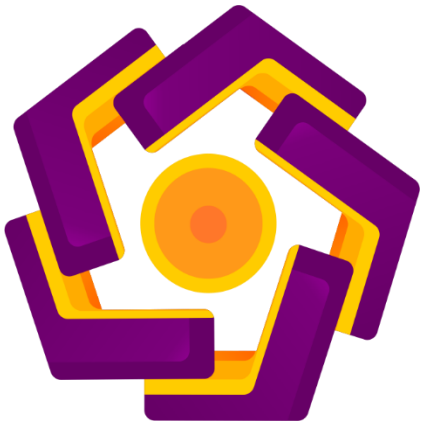
UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA 2026

ANALISIS HYBRID REVERSE ENGINEERING MALWARE WINDOWS BERBASIS LINGKUNGAN ISOLASI FLARE VM

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Teknik Komputer



disusun oleh

INDRA BAGAS PRATAMA

22.83.0859

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2026

HALAMAN PERSETUJUAN

SKRIPSI

ANALISIS HYBRID REVERSE ENGINEERING MALWARE WINDOWS BERBASIS LINGKUNGAN ISOLASI FLARE VM

yang disusun dan diajukan oleh

Indra Bagas Pratama

22.83.0859

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 28 Januari 2026

Dosen Pembimbing,

Muhammad Koprawi, S.Kom., M.Eng.
NIK. 190302454

HALAMAN PENGESAHAN

SKRIPSI

ANALISIS HYBRID REVERSE ENGINEERING MALWARE WINDOWS BERBASIS LINGKUNGAN ISOLASI FLARE VM

yang disusun dan diajukan oleh

Indra Bagas Pratama

22.83.0859

Telah dipertahankan di depan Dewan Penguji
pada tanggal 23 Februari 2026

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Wahid Miftahul Ashari, S.Kom., M.T **NIK. 190302452**	
Jeki Kuswanto, S.Kom., M.Kom **NIK. 190302456**	
Muhammad Koprawi, S.Kom., M.Eng **NIK. 190302454**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 23 Februari 2026

DEKAN FAKULTAS ILMU KOMPUTER

Prof. Dr. Kusrini, M.Kom.
NIK. 190302106

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Indra Bagas Pratama
NIM : 22.83.0859

Menyatakan bahwa Skripsi dengan judul berikut:

Analisis Hybrid Reverse Engineering Malware Windows Berbasis Lingkungan Isolasi Flare VM

Dosen Pembimbing : Muhammad Koprawi, S.Kom., M.Eng.

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 23 Februari 2026

Yang Menyatakan,

Indra Bagas Pratama

HALAMAN PERSEMBAHAN

Puji syukur ke hadirat Allah SWT atas segala limpahan karunia-Nya, sehingga penulisan skripsi ini dapat diselesaikan dengan baik. Tiada lembar yang paling bermakna dalam laporan skripsi ini selain lembar persembahan. Skripsi ini saya persembahkan kepada:

1. Teristimewa penulis ucapkan terima kasih kepada kedua orang tua tercinta. Untuk setiap tetes keringat dalam setiap kerja keras yang dilakukan, mengusahakan yang terbaik kepada penulis, selalu memberikan kasih sayang, dukungan, dan mendoakan sehingga penulis mampu menyelesaikan studi sampai sarjana. Penulis persembahkan gelar ini untuk bapak ibu dan saudari saya.
2. Kepada semua teman - teman penulis selama berkuliah. Terima kasih untuk kebesamaannya menjadi bagian dari cerita kehidupan dan perjalanan perkuliahan penulis hingga terselesaikannya skripsi ini.
3. Seluruh pihak yang memberikan bantuan kepada penulis namun tidak dapat disebutkan satu-persatu. Terima kasih atas bantuan, semangat, dan doa baik yang diberikan kepada penulis.

KATA PENGANTAR

Puji syukur kehadirat Tuhan Yang Maha Esa atas limpahan rahmat, ilmu, dan hidayah-Nya sehingga penulis dapat menyelesaikan penyusunan skripsi ini dengan baik dan lancar.

Skripsi ini disusun sebagai salah satu syarat untuk menyelesaikan program sarjana pada Fakultas Ilmu Komputer, Program Studi Teknik Komputer, Universitas AMIKOM Yogyakarta. Dalam proses penyusunan skripsi ini, penulis mendapatkan banyak dukungan, bantuan, dan bimbingan dari berbagai pihak, penulis menyampaikan terima kasih yang sebesar-besarnya kepada:

1. Kedua orang tua tercinta, atas doa, kasih sayang, dan dukungan moral maupun materi yang tiada henti sehingga penulis menyelesaikan pendidikan di Universitas Amikom Yogyakarta.
2. Bapak Prof. Dr. M. Suyanto, M.M, selaku Rektor Universitas Amikom Yogyakarta.
3. Ibu Prof. Dr. Kusrini, M.Kom selaku Dekan Fakultas Ilmu Komputer Universitas Amikom Yogyakarta.
4. Bapak Dr. Dony Ariyus, M.Kom. selaku Kepala Prodi Teknik Komputer
5. Bapak Muhammad Koprawi, S.Kom., M.Eng, selaku dosen pembimbing, atas waktu, bimbingan, dan arahan yang sangat berharga selama proses penyusunan skripsi.
6. Tim Dosen Penguji Skripsi, atas saran dan masukan yang telah membantu penyempurnaan karya ini.
7. Seluruh dosen Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta, atas ilmu, bimbingan, serta pelayanan yang diberikan selama masa studi.

Yogyakarta, 14 Februari 2026

Penulis

DAFTAR ISI

HALAMAN JUDUL i
HALAMAN PERSETUJUAN ii
HALAMAN PENGESAHAN iii
HALAMAN PERNYATAAN KEASLIAN SKRIPSI iv
HALAMAN PERSEMBAHAN v
KATA PENGANTAR vi
DAFTAR ISI vii
DAFTAR TABEL ix
DAFTAR GAMBAR x
DAFTAR SINGKATAN xii
DAFTAR ISTILAH xiii
INTISARI xv
ABSTRACT xvi
BAB I PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Rumusan Masalah 3
1.3 Batasan Masalah 3
1.4 Tujuan Penelitian 4
1.5 Manfaat Penelitian 4
1.6 Sistematika Penulisan 5
BAB II TINJAUAN PUSTAKA 6
2.1 Studi Literatur 6
2.2 Dasar Teori 11
BAB III METODE PENELITIAN 23
3.1 Objek Penelitian 23
3.2 Alur Penelitian 24
3.3 Alat dan Bahan 27

BAB IV HASIL DAN PEMBAHASAN 34
4.1 Persiapan Lingkungan Analisis 34
4.2 Hasil Analisis Statis 38
4.3 Hasil Analisis Dinamis 47
4.4 Hasil Integrasi Hybrid 56
4.5 Ekstraksi dan Validasi Indicators of Compromise (IoC) 66
4.6 Evaluasi Model Hybrid Reverse Engineering 67
BAB V PENUTUP 69
5.1 Kesimpulan 69
5.2 Saran 70
REFERENSI 71

DAFTAR TABEL

Tabel 3. 1 Daftar Sampel Malware 27
Tabel 3. 2 Komponen Perangkat Keras 28
Tabel 3. 3 Komponen Perangkat Lunak.....28
Tabel 4. 1 Komponen Alat Analisis.....36
Tabel 4. 2 Daftar Indicators of Compromise (IoC).....66

DAFTAR GAMBAR

Gambar 2. 1 Flare VM 18
Gambar 2. 2 Reverse Engineering 20
Gambar 3. 1 Alur Penelitian 24
Gambar 3. 2 Arsitektur Lingkungan Analisis 29
Gambar 4. 1 Arsitektur Lingkungan Analisis 34
Gambar 4. 2 Scanning Detect is Easy 38
Gambar 4. 3 Informasi entropy AgentTesla.....39
Gambar 4. 4 Hasil Analisis AgentTesla dengan Pestudio sebelum unpacking 39
Gambar 4. 5 Hasil Analisis AgentTesla dengan Pestudio sebelum unpacking 40
Gambar 4. 6 Hasil Analisis AgentTesla dengan Pestudio sebelum unpacking 40
Gambar 4. 7 Hasil Analisis AgentTesla dengan Pestudio sebelum unpacking 41
Gambar 4. 8 Hasil Analisis AgentTesla dengan Pestudio sebelum unpacking 41
Gambar 4. 9 Hasil Analisis AgentTesla dengan Pestudio 42
Gambar 4. 10 Proses Unpacking.....42
Gambar 4.11 Melakukan cek informasi file setelah unpacking.....43
Gambar 4. 12 Identifikasi file unpacking dengan pestudio 44
Gambar 4. 13 Identifikasi file unpacking dengan pestudio 44
Gambar 4. 14 Identifikasi file unpacking dengan pestudio 45
Gambar 4. 15 Perbandingan file malware dan file unpacked dengan pestudio.....46
Gambar 4. 16 Malware mendeteksi debug saat berjalan di x32dbg 47
Gambar 4. 17 Manipulasi nilai EAX 48
Gambar 4. 18 Malware membuat virtualalloc 48
Gambar 4. 19 Proses virtualalloc dijalankan pada modul kernel32.dll 49
Gambar 4. 20 proses virtualalloc malware.....50
Gambar 4. 21 Proses virtualalloc malware 50
Gambar 4. 22 Tampilan x32dbg dan proses hacker.....51
Gambar 4. 23 Child Proses baru dijalankan oleh malware 52
Gambar 4. 24 Melanjukkan proses debugging ada virtualalloc.....53

Gambar 4. 25 Capture aktivitas jaringan malware AgentTesla 54
Gambar 4. 26 Capture aktivitas malware AgentTesla 55
Gambar 4. 27 Ekstraksi memori pada child proses RegSvcs.exe 56
Gambar 4. 28 capture aktiivitas memori pada child proses RegSvcs.exe 57
Gambar 4. 29 Ditemukan blok memori “MZ” 58
Gambar 4. 30 Ditemukan blok memori 58
Gambar 4. 31 Rekonstruksi file PE malware 59
Gambar 4. 32 Temuan file mscoree.dll.....59
Gambar 4. 33 File .exe hasil *rekonstruksi* dianalisis dengan dnspy 60
Gambar 4. 34 Temuan fungsi GetLastInputInfo.....61
Gambar 4. 35 Temuan fungsi Pengambilan Informasi /Reconnaissance 61
Gambar 4. 36 Temuan fungsi SetwindowsHookex 62
Gambar 4. 37 Temuan fungsi informasi browser 63
Gambar 4. 38 Temuan fungsi ServerCertificateValidationCallback 63
Gambar 4. 39 Temuan fungsi *protocol* keamanan 64
Gambar 4. 40 Temuan fungsi SMTP 65

DAFTAR SINGKATAN

API
C2
CPU
DIE
DLL
DNS
FLARE VM
IOC
IP
MD5
PE
RAT
SMTP
UPX
VM
PROCMON
FAKENET-NG

DAFTAR ISTILAH

Analisis Statis	Metode analisis malware tanpa menjalankan program, dengan cara memeriksa struktur, kode, atau metadata file biner.
Analisis Dinamis	Metode analisis malware dengan menjalankan program dalam lingkungan terisolasi untuk mengamati perilaku runtime-nya.
Hybrid Reverse Engineering	Pendekatan gabungan antara analisis statis dan dinamis untuk memahami struktur dan perilaku malware secara menyeluruh.
Reverse Engineering	Proses membedah dan memahami cara kerja perangkat lunak dengan menganalisis kode biner atau perilakunya.
Malware	Perangkat lunak berbahaya yang dirancang untuk merusak, mengakses, atau mencuri data dari sistem komputer.
Obfuscation	Teknik penyamaran kode agar sulit dipahami atau dianalisis oleh peneliti maupun perangkat keamanan.
Packing	Proses kompresi atau penyamaran file executable untuk menyembunyikan kode asli dari analisis statis.
Sandbox	Lingkungan virtual yang aman dan terisolasi untuk menjalankan serta mengamati perilaku malware tanpa membahayakan sistem utama.

Debugger	Program yang digunakan untuk melacak, memantau, dan memodifikasi jalannya program secara langsung pada saat dijalankan.
Virtual Machine (VM)	Mesin virtual yang meniru komputer fisik untuk menjalankan sistem operasi dan perangkat lunak secara terisolasi.
Indicator of Compromise (IoC)	Tanda-tanda digital yang menunjukkan adanya aktivitas berbahaya, seperti alamat IP, domain, atau hash file.
Process Injection	Teknik di mana malware menyuntikkan kode berbahaya ke dalam proses lain untuk menghindari deteksi.
Command and Control (C2)	Server yang digunakan oleh penyerang untuk mengirim perintah dan menerima data dari malware.
FLARE VM	Lingkungan analisis malware berbasis Windows yang berisi kumpulan alat keamanan dan reverse engineering.
PE (Portable Executable)	Format file eksekusi standar pada sistem operasi Windows (.exe, .dll) yang memuat informasi struktur program.
Entropy	Ukuran acak data dalam file yang dapat menunjukkan adanya kompresi atau enkripsi pada malware.
Persistence	Teknik yang digunakan malware untuk tetap aktif atau berjalan setiap kali sistem dihidupkan kembali.
Anti-Debugging	Mekanisme yang digunakan malware untuk mendeteksi atau menghalangi aktivitas debugging oleh analis.

INTISARI

Perkembangan teknologi informasi yang pesat membawa dampak positif sekaligus meningkatkan potensi ancaman keamanan siber, terutama dari penyebaran malware pada sistem operasi Windows. Jenis malware seperti *Remote Access Trojan* (RAT) dengan objek penelitian *AgentTesla* yang mempunyai *impact* untuk mencuri data sensitif, mengendalikan sistem dari jarak jauh, serta menyembunyikan aktivitas berbahaya melalui teknik *packing* dan *obfuscation*. Ancaman ini menuntut adanya metode analisis yang efektif untuk memahami perilaku malware dan meningkatkan sistem pertahanan siber.

Penelitian ini menggunakan pendekatan Hybrid Reverse Engineering, yaitu kombinasi antara analisis statis dan analisis dinamis berbasis lingkungan isolasi FLARE VM. Lingkungan penelitian dibangun menggunakan sistem virtual terisolasi yang dilengkapi berbagai alat analisis seperti *Detect It Easy (DIE)*, *PE Studio*, *x32dbg*, *Process Hacker*, dan *FakeNet-NG*. Analisis statis digunakan untuk mengidentifikasi struktur internal dan fungsi berbahaya dalam kode biner malware, sedangkan analisis dinamis dilakukan untuk mengamati perilaku runtime malware terhadap sistem dan jaringan.

Hasil penelitian menunjukkan bahwa FLARE VM efektif sebagai platform analisis hybrid karena mampu mendeteksi dan memahami teknik penyamaran kode yang digunakan malware. Penelitian ini berhasil mengidentifikasi *Indicators of Compromise (IoC)* seperti domain, IP, dan aktivitas jaringan yang mencerminkan perilaku berbahaya. Temuan ini diharapkan dapat menjadi referensi bagi peneliti, analis keamanan, dan praktisi forensik digital dalam meningkatkan kemampuan deteksi serta mitigasi ancaman malware di lingkungan Windows.

Kata kunci: Malware, Reverse Engineering, FLARE VM, Analisis Statis, Analisis Dinamis.

ABSTRACT

The rapid development of information technology has brought significant progress while also increasing cybersecurity threats, particularly from the spread of malware targeting Windows operating systems. Malware such as Remote Access Trojan (RAT) for instance, AgentTesla are widely used to steal sensitive data, gain remote system control, and conceal malicious activities through packing and obfuscation techniques. These threats highlight the need for effective analysis methods to understand malware behavior and enhance cybersecurity defense mechanisms.

This research applies a Hybrid Reverse Engineering approach that combines both static and dynamic analysis using the FLARE VM isolation environment. The research environment was built within an isolated virtual system equipped with several analysis tools such as Detect It Easy (DIE), PE Studio, x32dbg, Process Hacker, and FakeNet-NG. Static analysis was conducted to identify internal structures and malicious functions within the malware binary code, while dynamic analysis observed the malware's runtime behavior on the system and network.

The results indicate that FLARE VM is effective as a hybrid analysis platform capable of detecting and understanding code obfuscation and packing techniques used by malware. This study successfully identified Indicators of Compromise (IoC), including domains, IP addresses, and network activities representing malicious behavior. The findings are expected to serve as a valuable reference for researchers, security analysts, and digital forensic practitioners in improving detection capabilities and mitigating malware threats within Windows environments.

Keywords: Malware, Reverse Engineering, FLARE VM, Static Analysis, Dynamic Analysis.