ANALISIS MALWARE MENGGUNAKAN METODE MEMORY FORENSIK DAN YARA RULE PADA SISTEM OPERASI WINDOWS 10

SKRIPSI

Disusun oleh:

Bagus Aji Saputro
17.83.0119

PROGRAM SARJANA
PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA

2022

ANALISIS MALWARE MENGGUNAKAN METODE MEMORY FORENSIK DAN YARA RULE PADA SISTEM OPERASI WINDOWS 10

SKRIPSI

Diajukan kepada Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta
untuk memenuhi salah satu syarat memperoleh gelar Sarjana Komputer
Pada Jenjang Program Sarjana – Program Studi Teknik Komputer

Disusun oleh:

Bagus Aji Saputro
17.83.0119

PROGRAM SARJANA
PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2022

HALAMAN PERSETUJUAN

SKRIPSI

ANALISIS MALWARE MENGGUNAKAN METODE MEMORY FORENSIK DAN YARA RULE PADA SISTEM OPERASI WINDOWS 10

yang dipersiapkan dan disusun oleh

Bagus Aji Saputro
17.83.0119

Telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal <25 Februari 2022>

Dosen Pembimbing,

Banu Santoso, S.T., M.Eng
NIK. 190302327

HALAMAN PENGESAHAN

SKRIPSI

ANALISIS MALWARE MENGGUNAKAN METODE MEMORY FORENSIK DAN YARA RULE PADA SISTEM OPERASI WINDOWS 10

yang dipersiapkan dan disusun oleh

Bagus Aji Saputro
17.83.0119
Telah dipertahankan di depan Dewan Penguji
pada tanggal <22 Maret 2022>

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Muhammad Koprawi S.Kom., M.Eng **NIK. 190302454**	
Banu Santoso S.T., M.Eng **NIK. 190302327**	
Anggit Ferdita Nugraha, S.T., M.,Eng **NIK. 190302480**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal < 22 Maret 2022 >

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta,S.Kom., M.Kom.
NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,
Nama mahasiswa : Bagus Aji Saputro
NIM : 17.83.0119

Menyatakan bahwa Skripsi dengan judul berikut:

Analisis Malware Menggunakan Metode Memori Forensik Dan Yara Rule Pada Sistem Operasi Windows 10

Dosen Pembimbing : Banu Santoso, S.T., 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, <22 Maret 2022>

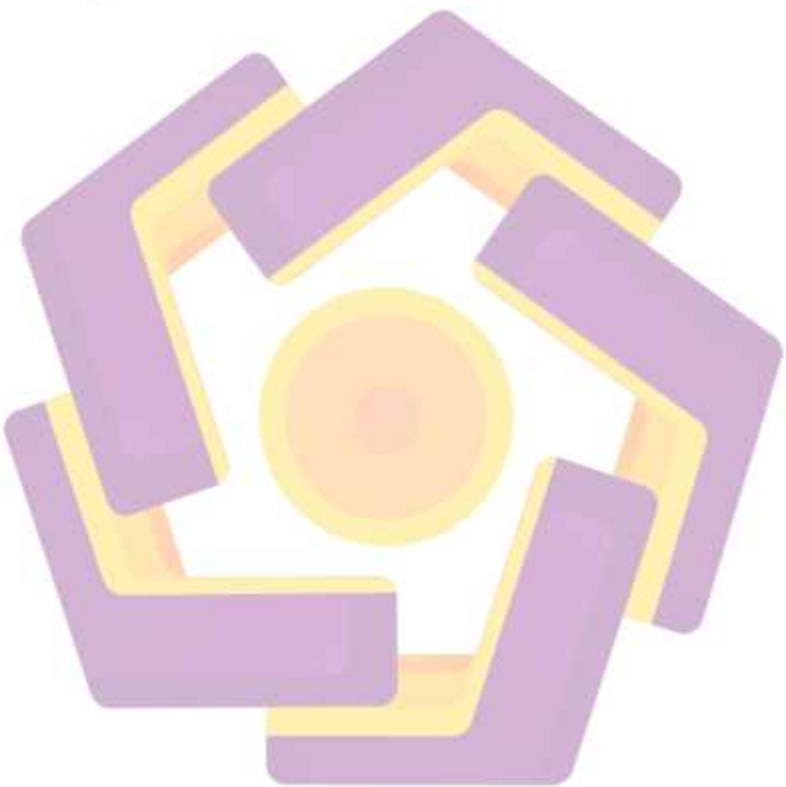
Yang Menyatakan,

Bagus Aji Saputro

v

HALAMAN MOTTO

Jadilah bagian dari perubahan yang ingin Anda lihat di dunia ini (Mahatma Gandhi)



HALAMAN PERSEMBAHAN

Segala puji bagi Allah subhanahu wa ta'ala yang telah memberi kemudahan untuk menyelesaikan skripsi ini, atas kehendak mu saya bisa menjadi pribadi yang berilmu, berpikir dan sabar. Semoga ini menjadi langkah awal untuk meraih cita-cita di masa depan, dan terima kasih atas dukungan dan doa dari orang-orang tercinta sehingga skripsi ini dapat diselesaikan dengan baik. Oleh karena itu, dengan bangga dan rasa syukur saya ingin mengucapkan terimakasih saya kepada:

1. Allah *subhanahu wa ta'ala,* atas izin dan ridha-Nya saya dapat menyelesaikan Skripsi ini dengan baik dan selesai dengan tepat waktu.
2. Orang tua saya, telah memberi banyak dukungan semasa perkuliahan hingga selesai mengerjakan skripsi ini. Semoga Allah *subhanahu wa ta'ala* senantiasa memberi kebahagiaan dan kemudahan untuk kedua orang tua.
3. Dosen pembimbing skripsi, bapak Banu Santoso, S.T., M. Eng, selaku dosen pembimbing yang dengan sabar telah memberikan banyak masukan, kritikan, dan saran untuk kelancaran pengerjaan skripsi.
4. Teman – teman 17 Teknik Komputer 2, yang telah memberi banyak dukungan dan semangat selama 3 tahun belajar bersama di kampus dengan banyak episode kehidupan, banyak kenangan yang tak akan terlupakan semasa perkuliahan atas canda tawa yang telah kita buat kurang lebih selama 3 tahun lalu.

KATA PENGANTAR

Sujud syukur penulis kepada Allah *subhanahu wa ta'ala* yang telah memberikan karunia, nikmat, dan hidayah kepada seluruh hamba-Nya. Skripsi ini disusun untuk memperoleh gelar Sarjana Komputer (S. Kom) sebagai salah satu syarat kelulusan Program Strata 1 Program Studi Teknik Komputer. Dengan selesai nya skripsi berjudul **"Analisis Malware Menggunakan Metode Memori Forensik Dan Yara Rule Pada Sistem Operasi Windows 10"**, Penghargaan dan terima kasih yang setulus-tulusnya kepada Ayah dan Ibu saya tercinta yang telah mencurahkan segenap cinta dan kasih sayang serta perhatian moril maupun material. Semoga Allah SWT selalu melimpahkan Rahmat, Kesehatan, Karunia dan keberkahan di dunia dan di akhirat atas budi baik yang telah diberikan kepada penulis.

Penghargaan dan terima kasih penulis berikan kepada Bapak Banu Santoso S.T., M.Eng. selaku Dosen Pembimbing yang membantu kelancaran penulisan skripsi ini ingin mengucapkan terimakasih kepada:

1. Allah subhanahu wa ta'ala yang dengan karunia dan hidayah-Nya penulis dapat menyelesaikan skripsi dengan baik.
2. Prof. Dr. M. Suyanto, MM, selaku Rektor Universitas Amikom Yogyakarta.
3. Bapak Hanif Al Fatta, S. Kom., M. Kom. selaku Dekan Fakultas Ilmu Komputer.
4. Bapak Dony Ariyus, M. Kom. selaku Ketua Program Studi S1 Teknik Komputer.
5. Bapak dan Ibu dosen S1 Teknik Komputer yang telah memberikan banyak pengalaman ketika perkuliahan di kelas maupun di laboratorium.
6. Keluarga besar Teknik Komputer angkatan 2017.
7. Teman-teman dan kenalan yang tidak dapat saya sebutkan satu per satu yang telah membantu dalam proses penyelesaian skripsi ini.

Yogyakarta, <25 Februari 2022>

Bagus Aji Saputro

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

Perkembangan teknologi yang sangat cepat membuat banyak orang memanfaatkan sebuah teknologi untuk melakukan tidak kejahatan, banyak pengguna komputer ataupun laptop kurang mewaspadai bahaya dalam menggunakan produk bajakan maupun mendownload sebuah aplikasi dari sumber yang kurang terpercaya sehingga memungkinkan untuk sebuah aplikasi yang digunakan tersebut disusupi sebuah *malware* tanpa sepengetahuan oleh pengguna. Sehingga memungkinkan aplikasi tersebut dapat digunakan oleh orang untuk melakukan pencurian sebuah data dari komputer pengguna tersebut.

Analisis memori forensik digunakan untuk mendapatkan artefak atau bukti digital pada laptop korban dengan cara mengakuisisi RAM dari laptop tersebut, sedangkan analisis *Yara rule* digunakan untuk mendapatkan string *malware* untuk menganalisis perilaku *malware* yang disisipkan pada aplikasi *sample malware* digunakan.

Hasil dari penelitian ini terdapat PID 4996 yang terinfeksi *malware* melakukan komunikasi dengan IP 2.56.59.42 dan aplikasi Gcleaner melakukan banyak injeksi aplikasi tanpa sepengetahuan pengguna yang memungkinkan dapat digunakan untuk melakukan pencurian data.

Kata kunci: memori forensik, *malware*, *Yara rule*,

ABSTRACT

The rapid development of technology encourages many people to use technology to not commit any crime, many computer or laptop users are less aware of the dangers of using pirated products or downloading an application from an untrusted source, which allows an application used to be infiltrated by malware without their knowledge by the user. This allows the app to be used by people to steal data from the user's computer.

Forensic memory analysis is used to obtain artifacts or digital evidence on the victim's laptop by acquiring RAM from the laptop, while Yara rules analysis is used to obtain malware strings to analyze the behaviour of malware inserted into the sample malware application used.

The result of this search is that the malware infected PID 4996 communicates with the IP 2.56.59.42 and the Gcleaner application performs many application infections without the knowledge of the user which allows it to be used to commit data theft.

Keyword: *forensics memory, malware, Yara rule*