PENGEMBANGAN VOLATRIK UNTUK ANALISIS FILELESS MALWARE DENGAN TEKNIK MEMORY FORENSIC

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi S1 Teknik Komputer

diajukan oleh

MUCHTAR ARIF BASTIAN

18.83.0234

Kepada

PROGRAM SARJANA

PROGRAM STUDI S1 TEKNIK KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2022

PENGEMBANGAN VOLATRIK UNTUK ANALISIS FILELESS MALWARE DENGAN TEKNIK MEMORY FORENSIC

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi S1 Teknik Komputer

diajukan oleh

MUCHTAR ARIF BASTIAN

18.83.0234

Kepada

PROGRAM SARJANA

PROGRAM STUDI S1 TEKNIK KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2022

HALAMAN PERSETUJUAN

SKRIPSI

PENGEMBANGAN VOLATRIK UNTUK ANALISIS FILELESS MALWARE DENGAN TEKNIK MEMORY FORENSIC

yang disusun dan diajukan oleh

Muchtar Arif Bastian

18.83.0234

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 23 Agustus 2022

Dosen Pembimbing,
ii

Rini Indrayani, ST, M.Eng
NIK. 190302417

HALAMAN PENGESAHAN

SKRIPSI

PENGEMBANGAN VOLATRIK UNTUK ANALISIS FILELESS MALWARE DENGAN TEKNIK MEMORY FORENSIC

yang disusun dan diajukan oleh

Muchtar Arif Bastian

18.83.0234

Telah dipertahankan di depan Dewan Penguji
pada tanggal 23 Agustus 2022

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Muhammad Koprawi, S.Kom., M.Eng **NIK. 190302454**	
Subektiningsih, M.Kom **NIK. 190302413**	
Rini Indrayani, ST, M.Eng **NIK. 190302417**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 23 Agustus 2022

DEKAN FAKULTAS ILMU KOMPUTER

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

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Muchtar Arif Bastian
NIM : 18.83.0234

Menyatakan bahwa Skripsi dengan judul berikut:

PENGEMBANGAN VOLATRIK UNTUK ANALISIS FILELESS MALWARE DENGAN TEKNIK MEMORY FORENSIC

Dosen Pembimbing : Rini Indrayani, ST, 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 Agustus 2022

Yang Menyatakan,

Muchtar Arif Bastian

HALAMAN PERSEMBAHAN

Dengan rasa syukur yang mendalam, dengan telah diselesaikannya skripsi ini. Penulis mempersembahkan skripsi ini kepada :

1. Keluarga besar penulis yang senantiasa memberikan doa dan dukungan dalam menyelesaikan skripsi ini.
2. Segenap civitas akademika Universitas AMIKOM Yogyakarta, staf pengajar, karyawan, dan seluruh mahasiswa di Universitas AMIKOM Yogyakarta.
3. Semua pihak yang menanyakan skripsi saya.

Penulis menyadari bahwa masih banyak kekurangan salam penyusunan skripsi ini dikarenakan keterbatasan wawasan serta pengetahuan penulis. Penulis sangat mengharapkan kritik dan saran yang membangun dari pembaca sehingga skripsi ini menjadi lebih baik. Semoga skripsi ini berguna dan bermanfaat bagi yang membacanya.

KATA PENGANTAR

Puji syukur dipanjatkan kehadirat Allah SWT atas segala rahmat dan karunia-Nya, sehingga penulsi dapat menyelsaikan skripsi ini dengan baik. Penulis juga mengucapkan terimakasih terhadap pihak yang telah memberikan dukungan kepada penulis untuk segera menyelesaikan skripsi ini. Penulis berharap skripsi ini dapat bermanfaat untuk pembaca serta dapat menmabah wawasan dan pengetahuan lebih mengenai memory forensic.

Penulis menyadari bahwa masih banyak kekurangan salam penyusunan skripsi ini dikarenakan keterbatasan wawasan serta pengetahuan penulis. Penulis sangat mengharapkan kritik dan saran yang membangun dari pembaca sehingga skripsi ini menjadi lebih baik.

Yogyakarta, 23 Agustus 2022

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

DAFTAR LAMBANG DAN SINGKATAN

CLI	*Command Line Interface*
CMD	*Command Prompt*
CPU	*Central Processing Unit*
ELF	*Executable and Linkable Format*
GUI	*Graphical User Interface*
IP	*Internet Protocol*
LTS	*Long Term Support*
PID	*Process Identifier*
PPID	*Parent Process Identifier*
RAM	*Random Access Memory*
RAT	*Remote Access Trojan*
UUID	*Universally Unique Identifier*
VM	*Virtual Machines*
WMI	*Windows Management Instrumentation*

DAFTAR ISTILAH

Malware	Perangkat Lunak Berbahaya
Sandbox	Lapisan perlindungan yang bertujuan untuk mencegah kode dan perangkat lunak berbahaya yang menyerang dan membahayakan sistem

INTISARI

Tantangan terbesar yang dihadapi di internet saat ini salah satunya yaitu ancaman *malware*. Kebanyakan proses *malware* yang aktif dapat dipantau melalui *task manager* atau program file yang dapat terdeteksi antivirus yang terpasang. Sayangnya, kemunculan *fileless malware* dapat membuat pemindai antivirus kesulitan untuk mendeteksi *malware* jenis ini. Pendekatan analisis dinamis biasanya digunakan untuk mengatasi hal tersebut, karena *malware* tidak selamanya berada di sistem file kemungkinan *malware* tidak terdeteksi ketika sistem memulai ulang. Maka pendekatan analisis memori dibutuhkan untuk melakukan identifikasi aktifitas *fileless malware*. Penelitian ini mengusulkan volatrik sebagai alat untuk melakukan ekstrak digital artefak yang kemudian untuk mengidentifikasi komputer yang terindikasi terdapat *fileless malware* yang sedang berjalan. Hasil dari penelitian ini menemukan bahwa ditemukan *fileless malware* jenis keylogger yang merekam input dari keyboard yang disimpan pada folder temporary dan dikirim ke suatu alamat melalui ftp.

Kata kunci: fileless malware, memory forensic, volatility framework, virtualbox

Abstract

One of the biggest challenges faced on the internet today is the threat of malware. Most active malware processes can be monitored through the task manager or a file program that can detect the installed antivirus. Unfortunately, the emergence of fileless malware can make it difficult for antivirus scanners to detect this type of malware. A dynamic analysis approach is usually used to address this, as malware does not stay in the file system forever and it is likely that the malware will not be detected when the system restarts. So a memory analysis approach is needed to identify fileless malware activities. This study proposes volatrik as a tool to extract digital artifacts and then to identify computers that are indicated to have fileless malware running. The results of this study found that keylogger fileless malware was found which recorded input from the keyboard which was stored in a temporary folder and sent to an address via ftp.

Keyword: fileless malware, memory forensic, volatility framework, virtualbox