ANALISIS DAN DETEKSI FILE PDF YANG TERINFEKSI MALWARE MENGGUNAKAN METODE STATIC ANALYSIS

SKRIPSI

Disusun oleh:

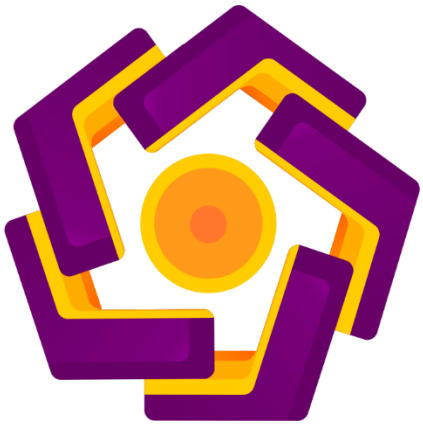
Rio Saputra
17.83.0051

PROGRAM SARJANA
PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2021

ANALISIS DAN DETEKSI FILE PDF YANG TERINFEKSI MALWARE MENGGUNAKAN METODE STATIC ANALYSIS

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:

Rio Saputra
17.83.0051

PROGRAM SARJANA
PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2021

HALAMAN PERSETUJUAN

SKRIPSI

ANALISIS DAN DETEKSI FILE PDF YANG TERINFEKSI MALWARE MENGGUNAKAN METODE STATIC ANALYSIS

yang dipersiapkan dan disusun oleh

Rio Saputra
17.83.0051

Telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal <08 februari 2021>

Dosen Pembimbing

DONY ARIYUS, M.KOM
NIK. 190302128

HALAMAN PENGESAHAN

SKRIPSI

ANALISIS DAN DETEKSI FILE PDF YANG TERINFEKSI MALWARE MENGGUNAKAN METODE STATIC ANALYSIS

yang dipersiapkan dan disusun oleh

Rio Saputra

17.83.0051

Telah dipertahankan di depan Dewan Penguji
pada tanggal <22 februari 2021>

Susunan Dewan Penguji

Nama Penguji	**Tanda Tangan**
Uyock Anggoro Saputro, M.Kom **NIK. 190302419**	_____
Nila Feby Puspitasari, S.Kom, M.Cs **NIK. 190302161**	_____
Dony Ariyus, M.Kom **NIK. 190302128**	_____

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal < 22 februari 2021>

DEKAN FAKULTAS ILMU KOMPUTER

Krisnawati, S.Si, M.T.
NIK. 190302038

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Rio Saputra
NIM : 17.83.0051

Menyatakan bahwa Skripsi dengan judul berikut:

Analisis Dan Deteksi File PDF Yang Terinfeksi Malware Menggunakan Metode Static Analysis

Dosen Pembimbing : DONY ARIYUS, M.KOM

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 februari 2021>

Yang Menyatakan,

Rio Saputra

HALAMAN MOTTO

“***Kunci sukses*** itu ada tiga, yang pertama itu ***jangan ambisi*** saat sudah nyampai step yang di inginkan, yang kedua ***jangan syrik/iri*** kepada orang lain,
Dan yang ketiga ***jangan lupa untuk bersedekah*** karena sebagian harta kita itu milik orang lain juga.”

(H. Bolot)

“Anda ingin mengetahui siapa diri Anda? Jangan bertanya. Beraksilah!”

(Thomas Jefferson)

“Pekerjaan-pekerjaan kecil yg selesai dilakukan lebih baik daripada rencana-rencana besar yang hanya didiskusikan.”

(Peter Marshall)

"Beberapa orang memimpikan kesuksesan, sementara yang lain bangun setiap pagi untuk mewujudkannya."

(Wayne Huizenga)

HALAMAN PERSEMBAHAN

Puji syukur kepada Allah SWT atas segala nikmat, hidayah, dan kesempatan menimba ilmu, sehingga penulis dapat menyelesaikan laporan ini. Dalam penyusunan laporan ini penulis banyak dibantu, dibimbing, dan didukung oleh berbagai pihak. Laporan ini penulis persembahkan kepada :

1. Kedua orang tua, Bapak Basuki dan Ibu Listiana yang selalu mendo'akan, memberi dukungan, fasilitas serta memberikan hasil kerja kerasnya kepada saya.
2. Bapak Dony Ariyus, M.Kom selaku dosen pembimbing saya yang telah membantu dalam penyusunan skripsi ini.
3. Kepada keluarga besar Bapak Mujiono yang telah memberikan semangat dan dukungan, baik secara material atau secara visual.
4. Kepada Sahabat dan teman-teman yang ada di saat suka maupun duka selama masa perkuliahan.
5. Semua pihak yang mendukung saya secara langsung ataupun tidak langsung.

KATA PENGANTAR

Puji dan syukur penulis panjatkan kehadirat Tuhan Yang Maha Esa atas karunia. Yang telah melimpahkan kasih dan sayang-Nya kepada kita semua, sehingga penulis bisa menyelesaikan skripsi dengan tepat waktu, yang diberi judul "*Analisis Dan Deteksi File PDF Yang Terinfeksi Malware Menggunakan Metode Static Analysis*" .

Tujuan dari penyusunan skripsi ini guna memenuhi syarat memperoleh gelar Sarjana pada program studi S1 Teknik Komputer, Fakultas Ilmu Komputer, Universitas Amikom Yogyakarta.

Didalam pengerjaan skripsi ini telah melibatkan banyak pihak yang sangat membantu dalam banyak hal. Oleh sebab itu disini penulis sampaikan rasa terimakasih sedalam-dalamnya kepada:

1. Allah SWT karena atas karunia-Nya, sehingga penulis dapat menyelesaikan skripsi ini dengan baik dan semoga dapat memberikan mamfaat di kemudian hari.
2. Bapak Prof. Dr. M. Suyanto, M.M. selaku Rektor Universitas AMIKOM Yogyakarta.
3. Bapak Dony Ariyus, M.Kom. selaku Ketua Program Studi S1 Teknik Komputer Universitas AMIKOM Yogyakarta, dan sekaligus selaku Dosen pembimbing yang telah bersedia memberikan pengarahan dan masukan dalam menyelesaikan Skripsi saya.
4. Bapak Joko Dwi Santoso, M.kom. selaku Dosen yang telah bersedia memberikan pengarahan dan bimbingan dalam penyususnan Skripsi ini.
5. Segenap Dosen, Staff, dan Karyawan Universitas AMIKOM Yogyakarta yang telah memberikan ilmu kepada penulis di bangku kuliah dan juga membantu penulis dalam kelancaran administrasi sampai terselesaikannya Skripsi ini.
6. Orang tua, saudara-saudara beserta keluarga yang selalu mendoakan dan memberikan dukungan penuh kepada penulis.

7. Serta kepada semua pihak yang telah membantu dalam penyusunan Skripsi ini yang tidak dapat penulis sebutkan satu per satu.

Penulis berharap semoga skripsi ini dapat bermamfaat bagi semua pihak yang terkait dalam penulisan ini. Dalam penulisan skripsi ini penulis menyadari masih banyak kekurangan karena terbatasnya pengetahuan dan pengalaman penulis. Karena itu, dengan lapang hati penulis mengharapkan kritik dan saran yang membangun guna menyempurnakan skripsi ini.

Yogyakarta, 22 februari 2021

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

Portable Document Format (disingkat *PDF*) adalah sebuah format berkas yang dibuat oleh Adobe Systems pada tahun 1993 untuk keperluan pertukaran dokumen digital. Format *PDF* digunakan untuk merepresentasikan dokumen dua dimensi yang meliputi teks, huruf, citra dan grafik vektor dua dimensi. Pada Acrobat 3-D, kemampuan PDF juga meliputi pembacaan dokumen tiga dimensi. Sekitar bulan september 2007, file PDF mulai dimanfaatkan oleh pembuat *virus* untuk menyertakan kode-kode tertentu dalam dokumen tersebut. Biasanya berupa *trojan*. Seperti juga diberitakan Avira tanggal 6 Mei 2008, kelemahan *PDF* dimanfaatkan untuk menyisipkan kode virus, sehingga ketika *PDF* dijalankan *virus* yang berupa *trojan* tersebut bisa menginstall dirinya ke komputer. Untuk mengetahui bagaimana *malware* dapat melakukan infeksi pada *File PDF* maka dari itu di perlukan analisis.

Analisis dilakukan dengan melakukan implementasi penyusupan *malware* pada sampel *File PDF* yang terjangkit *malware*. Penyusupan *malware* pada sampel File menggunakan *tools MSFvenom*. Dalam melakukan scaning, file akan dilakukan injeksi dengan tujuan menyusupkan *malware* yang diciptakan menggunakan *MSFvenom*.

Hasil implementasi yaitu *file PDF* yang berhasil diinfeksi malware. Selanjutnya dilakukan analisis statis guna mengetahui dampak dari hasil infeksi malware. *Analisis statis* menggunakan *tool VirusTotal dan App Any Run*. selanjutnya ditemukan perbedaan *ukuran file* dari sebelum *infeksi malware*.

Kata kunci: File PDF, Malware, Analisis Malware, Analisis Static.

ABSTRACT

Portable Document Format (abbreviated as PDF) is a file format created by Adobe Systems in 1993 for the purpose of exchanging digital documents. The PDF format is used to represent two-dimensional documents which include text, letters, images and two-dimensional vector graphics. In Acrobat 3-D, PDF capabilities also include reading three-dimensional documents. Around September 2007, PDF files began to be used by virus authors to include certain codes in the document. Usually a trojan. As Avira also reported on May 6, 2008, PDF weaknesses were used to insert virus code, so that when the PDF was run the virus in the form of a trojan could install itself on the computer. To find out how malware can infect PDF files, analysis is needed.

The analysis was carried out by implementing malware infiltration on a sample PDF file which was infected by malware. Infiltration of malware in the sample file using MSFvenom tools. In scanning, the file will be injected with the aim of infiltrating the malware created using MSFvenom.

The result of the implementation is a PDF file that was successfully infected with malware. Furthermore, a static analysis is carried out to determine the impact of the malware infection results. Static analysis using VirusTotal and App Any Run tools. furthermore found differences in file size from before malware infection.

Keyword:*File PDF, Malware, Malware Analysis, Analysis Static.*