ANALISA DAN DETEKSI FILE PDF YANG TERINFEKSI MALWARE MENGGUNAKAN METODE HYBRID

SKRIPSI

Disusun oleh:

Bobby Nur Febriyanto
17.83.0020

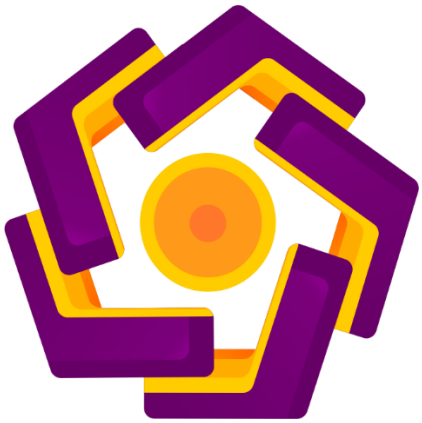
PROGRAM SARJANA
PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA

2021

ANALISA DAN DETEKSI FILE PDF YANG TERINFEKSI MALWARE MENGGUNAKAN METODE HYBRID

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:

Bobby Nur Febriyanto
17.83.0020

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

HALAMAN PERSETUJUAN

SKRIPSI

ANALISA DAN DETEKSI FILE PDF YANG TERINFEKSI MALWARE MENGGUNAKAN METODE HYBRID

yang dipersiapkan dan disusun oleh

Bobby Nur Febriyanto

17.83.0020

Telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 16 September 2021

Dosen Pembimbing,

Joko Dwi Santoso, M.Kom.
NIK. 190302181

HALAMAN PENGESAHAN

SKRIPSI

ANALISA DAN DETEKSI FILE PDF YANG TERINFEKSI MALWARE MENGGUNAKAN METODE HYBRID

yang dipersiapkan dan disusun oleh

Bobby Nur Febriyanto

17.83.0020

Telah dipertahankan di depan Dewan Penguji
pada tanggal 26 April 2021

Susunan Dewan Penguji

Nama Penguji	**Tanda Tangan**
Joko Dwi Santoso, M.Kom. **NIK. 190302181**	_____
Banu Santoso, S. T, M.Eng. **NIK. 190302248**	_____
Andika Agus Slameto, M.Kom. **NIK. 190302105**	_____

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 26 April 2021

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta, M.Kom.
NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Bobby Nur Febriyanto
NIM : 17.83.0020

Menyatakan bahwa Skripsi dengan judul berikut:

ANALISA DAN DETEKSI FILE PDF YANG TERINFEKSI MALWARE MENGGUNAKAN METODE HYBRID

Dosen Pembimbing : Joko Dwi Santoso, 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, 20 September 2021

Yang Menyatakan,

Bobby Nur Febriyanto

HALAMAN MOTTO

“Mungkin kamu bisa mengandalkan semua orang, tapi orang yang paling bisa kamu andalkan adalah dirimu sendiri.”

(Junghwan Treasure)

HALAMAN PERSEMBAHAN

Segala puji bagi Allah SWT atas limpahan rahmat dan hidayah serta karunia-Nya sehingga skripsi ini selesai dengan sebaik-baiknya. Skripsi ini saya persembahkan untuk :

1. Kedua orang tua, Bapak Sumarno dan Ibu Sumiyem yang selalu mendo'akan, memberi dukungan, fasilitas serta memberikan hasil kerja kerasnya kepada saya.
2. Bapak Joko Dwi Santoso, M.Kom selaku dosen pembimbing saya yang telah membantu dalam penyusunan skripsi ini.
3. Kepada Bibi saya Pujo Lestari dan kakak saya 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. Sesorang yang sangat berharga dan memberikan banyak arti dalam hidup saya, Mayza Monita Lutfitasari. Terima kasih atas cinta, dukungan, kebaikan, perhatian, dan kebijaksanaan serta telah mengajarkan arti kedewasaan.

KATA PENGANTAR

Puji dan syukur dipanjatkan kehadirat Tuhan Yang Maha Esa atas karunia yang telah dianugerahkan kepada penulis, sehingga penulis dapat menyelesaikan skripsi yang berjudul "Analisa Dan Deteksi File Pdf Yang Terinfeksi Malware Menggunakan Metode Hybrid".

Penulis menyadari bahwa tanpa bantuan dan bimbingan dari berbagai pihak, skripsi ini tidak mungkin dapat terselesaikan. Oleh karena itu, penulis menyampaikan terima kasih kepada :

1. Allah SWT karena atas karunia-Nya, sehingga penulis dapat menyelesaikan skripsi ini dengan baik dan semoga dapat memberikan manfaat 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.
4. Bapak Joko Dwi Santoso, M Kom selaku Dosen Pembimbing 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, 16 September 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 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 determin 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