ANALISIS MALWARE GANDCRAB RANSOMWARE PADA WINDOWS MENGGUNAKAN METODE STATIS

SKRIPSI

Disusun oleh:

Anisa Oktaviani
17.83.0063

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

2021

ANALISIS MALWARE GANDCRAB RANSOMWARE PADA WINDOWS MENGGUNAKAN METODE STATIS

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:

Anisa Oktaviani
17.83.0063

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

HALAMAN PERSETUJUAN

SKRIPSI

ANALISIS MALWARE GANDCRAB RANSOMWARE PADA WINDOWS MENGGUNAKAN METODE STATIS

yang dipersiapkan dan disusun oleh

Anisa Oktaviani

17.83.0063

Telah disetujui oleh Dosen Pembimbing Skripsi

pada tanggal 30 Agustus 2021

Dosen Pembimbing,

Melwin Syafrizal, S.Kom, M.Eng.
NIK. 190302105

HALAMAN PENGESAHAN

SKRIPSI

ANALISIS MALWARE GANDCRAB RANSOMWARE PADA WINDOWS MENGGUNAKAN METODE STATIS

yang dipersiapkan dan disusun oleh

Anisa Oktaviani

17.83.0063

Telah dipertahankan di depan Dewan Penguji
pada tinggal 24 Agustus 2021

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Wahyu Sukestyastama Putra, S.T., M.Eng **NIK. 190302328**	
Nila Feby Puspitasari, S.Kom.,M.Cs **NIK. 190302161**	
Melwin Syafrizal, S.Kom.,M.Eng **NIK. 190302105**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Ahli Madya Komputer
Tanggal 30 Agustus 2021

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta, M.Kom
NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Anisa Oktaviani
NIM : 17.83.0063

Menyatakan bahwa Skripsi dengan judul berikut:

ANALISIS MALWARE GANDCRAB RANSOMWARE PADA WINDOWS MENGGUNAKAN METODE STATIS

Dosen Pembimbing : Melwin Syafrizal, 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, 24 Agustus 2021
Yang Menyatakan,

Anisa Oktaviani

HALAMAN MOTTO

Teruslah berbuat baik selagi engkau masih di beri kesempatan untuk berbuat baik di dunia ini.

HALAMAN PERSEMBAHAN

Dengan mengucapkan puji syukur kepada Allah SWT atas limpahan rahmat dan hidayah serta karunia-Nya sehingga skripsi ini dapat diselesaikan dengan sebaik-baiknya. Skripsi ini saya persembahkan untuk:

1. Allah SWT, yang telah meridhoi dan mengabulkan doa-doa saya sehingga saya dapat menyelesaikan skripsi ini tepat pada waktunya. Puji syukur yang tak terhingga saya panjatkan kepada Allah SWT Tuhan semesta alam.
2. Kedua orang tua saya. Bapak Muslihuddin dan Ibu Nila Wati yang tak pernah bosan menyemangati dan mendoakan serta memberikan dukungan moral maupun material kepada saya untuk meraih kesuksesan. Terimakasih untuk semua kasih saying yang tak akan pernah habis.
3. Kakak saya, Arief Setya Budi M.Kom. yang selalu memberikan dukungan dan sangat saya sayangi.
4. Dosen pembimbing saya. Bapak Melwin Syafrizal, S.Kom, M.Eng. yang tak bosan membimbing dan mengarahkan saya dalam pembuatan skripsi ini. Serta seluruh jajaran dosen teknik komputer Universitas Amikom Yogyakarta yang sudah memberikan ilmunya kepada saya.
5. Sahabat dan teman-teman yang selalu menemani saya dalam pembuatan skripsi ini.

KATA PENGANTAR

Alhamdulillah, Dengan mengucapkan puji syukur kehadirat Allah SWT, yang telah melimpahkan rahmat dan karunia-Nya, sehingga pada akhirnya penulis dapat menyelesaikan skripsi ini dengan judul "Analisis Malware GandCrab Ransomware Pada Windows Menggunakan Metode Statis".

Skripsi ini disusun sebagai syarat memperoleh gelar Sarjana Komputer pada program Studi S1 Teknik Komputer Fakultas Ilmu Komputer Unniversitas Amikom Yogyakarta.

Selesainya skripsi ini tidak terlepas dari dukungan berbagai pihak yang telah memberikan dorongan moril maupun spiritual dan juga bimbingan ilmu pengetahuan. Oleh karena itu penulis mengucapkan terimakasih 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. Orang tua dan kakak yang selalu mendoakan dan memberikan dukungan penuh kepada penulis
3. Bapak Prof. Dr. M. Suyanto, M.M. selaku Rektor Universitas AMIKOM Yogyakarta.
4. Bapak Dony Ariyus, M.Kom. selaku Ketua Program Studi S1 Teknik Komputer Universitas AMIKOM Yogyakarta.
5. Bapak Melwin Syafrizal, S.Kom, M.Eng. selaku Dosen Pembimbing yang telah bersedia memberikan pengarahan dan bimbingan dalam penyusunan skripsi ini.
6. 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.
7. Sahabat serta teman-teman kelas 17-S1TK-01. Serta kepada semua pihak yang telah membantu dalam penyusunan skripsi ini yang tidak dapat penulis sebutkan satu per satu.

Akhir kata penulis berharap semoga skripsi ini dapat memberikan manfaat bagi pembaca. Penulis menyadari bahwa masih banyak kekurangan dalam penulisan skripsi ini. Untuk itu, penulis mohon kritik dan saran yang bersifat membangun demi kesempurnaan penulisan dimasa yang akan datang.

Yogyakarta, 24 Aguustus 2021

Anisa Oktaviani

DAFTAR ISI

HALAMAN JUDUL i
HALAMAN PERSETUJUAN ii
HALAMAN PENGESAHAN iii
HALAMAN PERNYATAAN KEASLIAN SKRIPSI iv
HALAMAN MOTTO v
HALAMAN PERSEMBAHAN vi
KATA PENGANTAR vii
DAFTAR ISI viii
DAFTAR TABEL xi
DAFTAR GAMBAR xii
INTISARI xiv
ABSTRACT xv
BAB I PENDAHULUAN 1
2.1 Latar Belakang Masalah 1
2.2 Rumusan Masalah 2
2.3 Batasan Masalah 2
2.4 Tujuan Penelitian 2
2.5 Sistematika Penulisan 2
BAB II Landasan Teori 4
2.1 Kajian Pustaka 4
2.2 Malware 8
2.2.1. Virus 8
2.2.2. Worm 8
2.2.3. Trojan 9
2.2.4. Rootkit 9
2.2.5. Spyware 9

2.2.6. Keyloggers 9
2.3 Ransomware 10
2.3.1. Deteksi Jenis Ransomware 10
2.4 Gandcrab 11
2.4.1. Gandcrab version 1 12
2.4.2. Gandcrab version 2 12
2.4.3. Gandcrab version 3 12
2.4.4. Gandcrab version 4 12
2.4.5. Gandcrab version 5 13
2.5 Nefilim 13
2.6 Analisis Malware 13
2.7 Analisis Statis 14
2.8 Analisis Dinamis 15
2.9 Analisis Hybrid 15
BAB III Metode Penelitian 18
3.1 Gambaran Umum 18
3.2 Alur Penelitian 18
3.3 Alat dan Bahan Penelitian 19
3.3.1. Perangkat keras (*hardware*) 19
3.3.2. Perangkat lunak *(software)* 19
BAB IV Hasil dan Pembahasan 21
4.1 Rancangan Sistem 21
4.1.1. Instalasi Virtual Machine Environment 21
4.1.2 Instalasi *Tools* 23
4.1.2.1 PeStudio 23
4.1.2.2 *ExeInfo PE* 23
4.1.2.3 PE.Explorer 24
4.1.2.4 Dependency Walker 28
4.2 Implementasi Sistem 28
4.2.1. *Analysis With Virustotal* 28
4.2.2. *Analysis With PeStudio* 30

4.2.3. *Analysis With PEexplorer* 31
4.2.4. *Analysis With Exeinfo* 32
4.2.5. *Analysis String Indicators* 33
4.2.6. *Analysis With Dependency Walker* 34
4.2.7. *Record Analysis Result* 43
BAB V Penutup 45
5.1 Kesimpulan 45
4.2 Saran 46
Daftar Pustaka 47

DAFTAR TABEL

Tabel 2.1 Penelitian Terkait..... 6

Table 2.2 Perbandingan Gandcrab dan Nefilim.....13

Tabel 3.1 Spesifikasi Hardware..... 15

Tabel 3.2 Spesifikasi Software..... 15

Tabel 3.3 Penjelasan Tools..... 16

Tabel 4.1 Perbandingan nilai checksum gandcrab antara virustotal dan PeStudio.27

Tabel 4.2 Strings Function..... 33

DAFTAR GAMBAR

Gambar 2.1 Teknik Deteksi Malware 13
Gambar 3.1 Alur Penelitian 17
Gambar 4.1 Import File OVA Kali-Linux-2020.1-vbox-amd64 20
Gambar 4.2 Proses Import File OVA 21
Gambar 4.3 Import File OVA Windows 7 64-bit 21
Gambar 4.4 Proses Import File OVA 21
Gambar 4.5 Download PeStudio 22
Gambar 4.6 Isi Folder PeStudio 22
Gambar 4.7 Download Exeinfo PE 23
Gambar 4.8 Isi Folder Exeinfo PE 23
Gambar 4.9 Download PE.Explorer 24
Gambar 4.10 setup PE.Explore 24
Gambar 4.11 Tampilan Awal Instalasi 25
Gambar 4.12 License Agreement 25
Gambar 4.13 "Ready to Install" 26
Gambar 4.14 Akhir Proses Instalasi PE.Explorer 26
Gambar 4. 15 Download Depencency Walker 27
Gambar 4.16 Dependency Walker 27
Gambar 4.17 Informasi Gandcrab menggunakan virustotal 28
Gambar 4.18 checksum file malware 29
Gambar 4.19 Informasi Gandcrab dengan PeStudio 29
Gambar 4.20 PE explorer result 30

Gambar 4.21 Exeinfo Result 1 31
Gambar 4.22 Exeinfo Result 2 31
Gambar 4.23 String Indicators 32
Gambar 4.24 Strings Malware Gandcrab Ransomware 32
Gambar 4.25 Tampilan awal dependency walker 33
Gambar 4.26 MFC24.DLL 34
Gambar 4.27 SHELL32.DLL 34
Gambar 4.28 KERNEL32.DLL 34
Gambar 4.29 USER32.DLL 35
Gambar 4.30 USER32.DLL 35
Gambar 4.31 ADVAPI32.DLL 36
Gambar 4.32 GDI32.DLL 36
Gambar 4.33 MSVCRT.DLL 36

INTISARI

Malware atau *malicious software* adalah suatu program yang dibuat khusus untuk menginfeksi perangkat lunak atau aplikasi atau dokumen yang tersimpan dalam sebuah sistem. Sistem operasi yang terinfeksi *malware* dapat mengalami kerusakan sistem, file atau kehilangan data-data penting. *Ransomware* merupakan salah satu jenis *malware* yang bekerja dengan cara menyerang jaringan internet kemudian mengenkripsi computer korban. Agar korban dapat mengakses komputernya lagi, korban diminta unutk menebus *(ransom)* dengan sejumlah uang dalam bentuk *Bitcoin*. Salah satunya yaitu *GandCrab*. *Gandcrab* merupakan *ransomware* yang sangat kuat dan hanya pembuat *gandcrab* yang mengetahui deskripsi dari file yang terenkripsi.

Analisis statis dilakukan dengan mengimpor *sample malware* kedalam tools Virustotal, Dependency walker, PEStudio, Exeinfo PE, dan PEexplorer untuk mendapatkan fungsi *strings* yang kemudian *strings* tersebut akan dianalisa untuk mengetahui cara kerja dari *GandCrab Ransomware*.

Penelitian ini melakukan analisis terhadap *malware ganderab ransomware* dengan menggunakan metode statis. Pada *tool* Virustotal, didapatkan bahwa file *sample malware* terdeteksi sebagai *malware* dengan rasio 60 dari 70 *antimalware*. Selanjutnya ditemukan bahwa GandCrab berformat PE *(portable executable)* dan dikompilasi menggunakan Microsoft Visual C++ dan GndCrab mengakses beberapa fungsi DLL *(dynamic link-library)*.

Kata kunci: GandCrab, Malware, Ransomware, Analisis Statis

ABSTRACT

Malware or malicious software is a program created specifically to infect software or applications or documents stored on a system. Malware-infected operating systems may experience system damage, files or loss of important data. Ransomware is a type of malware that works by attacking the internet network and then encrypting the victim's computer. So that the victim can access his computer again, the victim is asked to redeem (ransom) with some money in the form of Bitcoin. One of them is GandCrab. Gandcrab is a very powerful ransomware and only the creators of Gandcrab know the description of the encrypted files.

Static analysis is done by importing malware samples into Virustotal, Dependency walker, PEStudio, Exeinfo PE, and PEexplorer tools to get the strings function, which will then be analyzed to find out how the GandCrab Ransomware works.

This study analyzes the gandcrab ransomware malware using a static method. In the Virustotal tool, it was found that the malware sample file was detected as malware with a ratio of 60 out of 70 antimalware. Furthermore, it was found that GandCrab is in PE (portable executable) format and compiled using Microsoft Visual C++ and GndCrab accesses some DLL (dynamic link-library) functions.

Keywords: *GandCrab, Malware, Ransomware, Static Analysis*