ANALISIS MALWARE TROJAN PADA DOCUMENT MICROSOFT EXCEL MENGGUNAKAN METODE STATIK

SKRIPSI

disusun oleh

Mohammad Rivan zhafran

17.83.0004

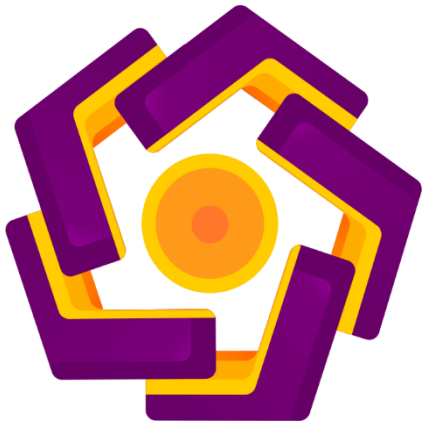
PROGRAM SARJANA
PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA

2023

ANALISIS MALWARE TROJAN PADA DOCUMENT MICROSOFT EXCEL MENGGUNAKAN METODE STATIK

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai gelar Sarjana
pada Program Studi Informatika



disusun oleh

Mohammad Rivan zhafran

17.83.0004

PROGRAM SARJANA
PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2023

PERSETUJUAN

SKRIPSI

ANALISIS MALWARE TROJAN PADA DOCUMENT MICROSOFT EXCEL MENGGUNAKAN METODE STATIK

yang dipersiapkan dan disusun oleh

Mohammad Rivan zhafran

17.83.0004

telah disetujuai oleh Dosen Pembimbing Skripsi

pada tanggal 24 Januari 2023

Dosen Pembimbing,

Joko Dwi Santoso, M.Kom

NIK. 190302181

PENGESAHAN

SKRIPSI

ANALISIS MALWARE TROJAN PADA DOCUMENT MICROSOFT EXCEL MENGGUNAKAN METODE STATIK

yang dipersiapkan dan disusun oleh

Mohammad Rivan zhafran

17.83.0004

telah dipertahankan di depan Dewan Penguji
pada tanggal 17 Januari 2023

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Joko Dwi Santoso, M.Kom **NIK. 190302181**	
Andika Agus Slameto, M.Kom **NIK. 190302109**	
Senie Destya, M.Kom **NIK. 190302312**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 17 Januari 2023

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta, M.Kom
NIK. 190302096

PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu institusi pendidikan tinggi manapun, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggungjawab saya pribadi.

Yogyakarta, 24 Januari 2023

Mohammad Rivan zhafran

NIM. 17.83.0004

PERSEMBAHAN

Puji syukur saya panjatkan kepada Allah SWT yang telah memberikan berkat, rahmat dan hidayah-Nya sehingga saya dapat menyelesaikan Skripsi ini dengan baik. Saya juga merasa berterima kasih kepada orang-orang disekitar saya yang telah secara langsung maupun tidak langsung membantu saya dalam mengerjakan Skripsi ini. Skripsi ini saya persembahkan kepada :

1. Ayah saya, Talidi, Ibu saya Yaumawati, Kakak saya Suryadi yang selalu mendoakan, memberi semangat, dan dukungan kepada saya.
2. Bapak Joko Dwi Santoso, M.Kom selaku dosen pembimbing yang selalu memberikan masukan dan bimbingan dalam menyelesaikan Skripsi.
3. Sahabat-sahabat kontrakan dan sobat tercinta saya.
4. Teman-teman kelas, yang telah menjadi teman saya semasa kuliah.
5. Serta semua pihak yang telah membantu serta mendukung saya yang tidak bisa saya sebutkan satu persatu.

KATA PENGENTAR

Puji syukur kita panjatkan kepada Allah SWT atas berkat dan karunia-Nya sehingga penulis dapat menyelesaikan laporan skripsi tepat pada waktunya dengan judul "Perancangan Aplikasi Pedoman Tata Cara mengemudi Mobil Berbasis Andorid Menggunakan Adobe Flash" Skripsi ini disusun untuk melengkapi tugas akhir kuliah dan memenuhi syarat kelulusan program Pendidikan S1 Informatika di Universitas Amikom Yogyakarta. Selama mengikuti pendidikan Strata 1 Informatika sampai dengan proses penyelesaian Skripsi, berbagai pihak telah memberikan fasilitas, membantu, membina, dan membimbing penulis untuk itu khususnya kepada :

1. Bapak Prof. Dr. M. Suyanto, MM selaku Rektor Universitas Amikom Yogyakarta yang telah banyak memberikan kemudahan dalam menyelesaikan pendidikan.
2. Bapak Joko Dwi Santoso, M.Kom selaku dosen pembimbing yang telah banyak meluangkan waktu dan tenaga untuk membimbing penulis selama penyusunan Skripsi ini.
3. Bapak/Ibu Dosen di Universitas Amikom Yogyakarta yang telah membekali penulis dengan beberapa disiplin ilmu yang berguna.
4. Teman–teman seperjuangan Mahasiswa S1 Informatika 2017, yang telah banyak berdiskusi dan bekerjasama dengan penulis selama masa Pendidikan.

Penulis menyadari, Skripsi ini masih banyak kelemahan dan kekurangan. Karena itu kritik dan saran yang membangun akan diterima dengan senang hati, semoga keberadaan Skripsi ini dapat bermanfaat dan menambah wawasan kita, khususnya tentang Tata cara mengemudi mobil.

Yogyakarta, 24 Januari 2023

Penulis

DAFTAR ISI

PERNYATAAN ..... **IV**

MOTTO ..... **VI**

PERSEMBAHAN ..... **VII**

DAFTAR ISI ..... **IX**

DAFTAR TABEL ..... **XII**

DAFTAR GAMBAR ..... **XIII**

INTISARI ..... **XIV**

ABSTRACT ..... **XV**

BAB I PENDAHULUAN ..... **1**.

1.1 LATAR BELAKANG ..... **1**.

1.2 RUMUSAN MASALAH ..... **2**.

1.3 BATASAN MASALAH ..... **2**.

1.4 TUJUAN PENELITIAN ..... **3**.

1.5 MANFAAT PENELITIAN ..... **3**.

1.6 METODOLOGI PENELITIAN ..... **4**.

1.7 SISTEMATIKA PENULISAN ..... **4**.

BAB II TINJAUAN PUSTAKA ..... **5**.

2.1 MALWARE ..... **5**.

2.1.1 Trojan ..... *7*.

2.2 METODE MALWARE ANALISIS ..... **11**.

2.2.1 Malware Analisis Statis ..... *11*.

2.3 KEAMANAN INFORMASI DAN TEKNIK MALWARE ANALYSIS ..... **12**.

2.3.1 Elemen Keamanan Informasi ..... *15*.

2.3.2 Teknik Malware Analysis ..... *17*.

2.4 MICROSOFT EXCEL ..... **20**.

2.4.1 Sejarah ..... *20*.

2.4.2 Fungsi ..... *22*.

2.8.3 Kelebihan ..... *23.*

2.4.4 Kekurangan ..... *24.*

BAB III METODOLOGI ..... **25.**

3.1 SANS INSTITUTE ..... **26.**

3.2 METODOLOGI PENELITIAN ..... **27.**

3.2.1 Static (Code) Analysis ..... *28.*

3.2.2 Dynamic (Behavioral) Analysis ..... *28.*

3.3 PENENTUAN TARGET ..... **30.**

2.1.2 Virus Scanning ..... *31.*

2.1.3 File Fingerprinting ..... *31.*

2.1.4 Extraction Of Hard Coded Strings ..... *32.*

2.1.5 Inside PE Format ..... *32.*

2.1.6 Extract Linked Libraries and Function ..... *32.*

2.1.7 Disassembly ..... *32.*

3.4 APLIKASI YANG DIGUNAKAN ..... **33.**

3.4.1 Virustotal ..... *33.*

3.4.2 Bintext ..... *34.*

3.4.3 Hashmyfiles ..... *34.*

3.4.4 CFF Explorer ..... *34.*

3.4.5 PEview ..... *34.*

3.4.6 Dependency Walker ..... *34.*

3.4.7 IDA Pro ..... *34.*

BAB IV IMPLEMENTASI DAN HASIL PENELITIAN ..... **47.**

4.1 VIRUS SCANNING ..... **47.**

4.2 FILE FINGERPRITING ..... **48.**

4.3 EXTRATION OF HARD CODED STRINGS ..... **48.**

4.4 INSIDE PE FORMAT ..... **49.**

4.5 EXTRACT LINKED LIBRARIES AND FUNCTION ..... **49.**

4.6 DISASSEMBLY ..... **50.**

BAB V PENUTUP ..... **52.**

5.1 KESIMPULAN ..... 52.
5.2 SARAN ..... 52.
DAFTAR PUSTAKA ..... 53.

DAFTAR TABEL

Tabel 2. 1 Elemen Keamanan Informasi ..... 17.
Tabel 4. 1 *Hash PlutoCrypt* ..... 48.
Tabel 4. 2 Header PlutoCrypt ..... 49.

DAFTAR GAMBAR

Gambar 3. 1 SANS INSTITUTE ..... 26.
Gambar 3. 2 Website Virustotal ..... 33.

Gambar 4. 1 Tahapan Penelitian ..... 47.
Gambar 4. 2 Hasil Virus Scanning PlutoCrypt ..... 47.
Gambar 4. 3 Hasil Virus Scanning Malware 2 ..... 47.
Gambar 4. 4 Hasil Strings PlutoCrypt ..... 48.
Gambar 4. 5 Libraries dan Function PlutoCrypt ..... 49.
Gambar 4. 6 Assembly Code PlutoCrypt ..... 50.
Gambar 4. 7 Assembly Code PlutoCrypt ..... 50.
Gambar 4. 8 Assembly Code PlutoCrypt ..... 50.
Gambar 4. 9 Assembly Code PlutoCrypt ..... 51.

INTISARI

Saat ini masih banyak perangkat lunak yang ditawarkan secara gratis (freeware). Perangkat lunak freeware biasanya dapat di download pada internet secara gratis. Perangkat lunak yang di download secara gratis biasanya memiliki tingkat resiko yang sangat tinggi. Mengapa demikian, karena saat ini sudah banyak perangkat lunak gratisan yang dengan sengaja di buat. Tetapi perangkat lunak tersebut adalah sebuah Malware (Malicious Software).

Malicious Software atau malware adalah sebuah software yang di buat untuk merusak sistem pada komputer. Peningkatan pengguna internet juga seiring dengan peningkatan penggunaan software. Namun, masih banyaknya pengguna yang masih menggunakan software bajakan karena relative gratis dan gampang didapatkan. Software bajakan biasanya sudah ditanamkan sebuah malware berbahaya seperti Trojan. Trojan merupakan jenis malware yang paling sering ditemukan dalam sistem komputer dengan berbagai banyak kasus.

Perkembangan malware yang ada memicu seseorang untuk melakukan sebuah penelitian atau analisa dari sebuah teknologi yang sudah ada, baik dari sektor kenyamanan sampai pada sektor keamanan, penulis melakukan analisis model serangan dan fungsi malware trojan dengan metode static analysis pada sistem operasi windows. Pada penelitian ini penulis melakukan analisa dengan metode SANS INSTITUTE yang diharapkan dapat memberikan pengetahuan dalam malware analysis.

Kata Kunci: malware, Trojan, analisis statis, Microsoft excel

ABSTRACT

Currently there is still a lot of software that is offered for free (freeware). Freeware software can usually be downloaded on the internet for free. Software that is downloaded for free usually has a very high level of risk. Why is that, because currently there is a lot of free software that is deliberately created. But the software is Malware (Malicious Software).

Malicious Software or malware is software that is created to damage a computer system. The increase in internet users is also in line with the increase in software use. However, there are still many users who still use pirated software because it is relatively free and easy to obtain. Pirated software is usually embedded with dangerous malware such as Trojans. Trojans are the type of malware that is most often found in computer systems in many cases.

The development of existing malware triggers someone to carry out research or analysis of existing technology, both from the comfort sector to the security sector. The author analyzes the attack model and function of trojan malware using the static analysis method on the Windows operating system. In this research, the author carried out analysis using the SANS INSTITUTE method which is expected to provide knowledge in malware analysis.

Keywords: malware, Trojan, analisis statis, Microsoft excel