IMPLEMENTASI PENDETEKSI VIRUS MAKRO MENGGUNAKAN VIPERMONKEY

[1]Ardiansyah Eka Septian, [2]Setia Juli Irzal Ismail, [3]Anang Sularsa.

[1] Computer Engginering, Telkom University, Bandung, Indonesia.

[1] arditian@student.telkomuniversity.ac.id, [2]jul@tass.telkomuniversity.ac.id, [3]anang@tass.telkomuniversity.ac.id.

Abstrak: File yang terinfeksi Virus Makro atau dikenal dengan *maldoc (Malicious Document)* adalah virus yang dibuat dengan memanfaatkan fasilitias pemrograman modular pada suatu program aplikasi seperti Ms Word, Ms Excel dan sebagainya. Dengan cara ini virus makro ini sulit untuk diketahui ketika disusupkan kedalam suatu *file* dokumen. Virus makro berbahaya karena mempunyai kemampuan untuk menggandakan dirinya, menghapus dokumen, mengubah pengaturan komputer, reset password, dan menyelipkan perintah berbahaya. Vipermonkey dapat melakukan deteksi pada virus makro, yang kemudian akan memberikan hasil berupa laporan yang menyatakan bahwa *file* terinfeksi oleh virus makro. Proyek akhir ini menggunakan Vipermonkey sebagai perangkat lunak untuk mendeteksi virus makro/*maldoc*. Vipermonkey juga dapat memberikan hasil berupa source code, hash malware, dan perintah yang ada dalam virus makro tersebut.

Kata Kunci *: ViperMonkey*

1. Pendahuluan

1.1 Latar Belakang

Pada Perkembangan kemajuan teknologi komputer dalam hal keamanan semakin meningkat. Tetapi kelebihan ini juga digunakan untuk hal-hal yang bersifat merugikan, akibatnya kerugian yang diderita akibat penyalahgunaan atau kejahatan menggunakan komputer/jaringan komputer (*cyber crime*) mencapai milyaran setiap tahunnya. Serangan terhadap komputer/jaringan di seluruh dunia seperti *virus*, *worms*, *spam* dan malware semakin meningkat. Salah satunya adalah virus makro. File yang terinfeksi Virus Makro atau dikenal dengan maldoc adalah virus yang dibuat dengan menggunakan fasilitas pemrograman modular pada program aplikasi *seperti Ms Word, Ms Excel, Corel WordPerfect* dan lainnya. Maldoc sendiri artinya adalah *Malicious Office documents* atau dokumen office berbahaya. Makro virus memiliki kemampuan untuk menggandakan dan menyebarkan dirinya, dan juga dapat menghapus dokumen words, mengubah pengaturan komputer, *reset password*, ,dan menyelipkan perintah berbahaya di CONFIG.SYS atau AUTOEXEC.BAT. Dokumen microsoft *office* menyumbang pengiriman hampir setengah dari semua makro berbahaya pada Agustus 2018, menurut Cofense.com. Pada web tersebut dilaporkan bahwa lampiran email merupakan salah satu pilihan yang sering digunakan untuk mengirimkan virus makro yang berbahaya. Dari semua mekanisme yang dianalisis, 45% dari penyerang menggunakan dokumen-dokumen ini untuk mengirimkan makro jahat, termasuk contohnya seperti virus makro Geodo, Chanitor, AZORult, dan GandCrab.

Menurut para peneliti keamanan, makro adalah pilihan utama karena itu diaktifkan pada mesin atau hanya membutuhkan satu klik mouse untuk diaktifkan. Virus makro dijalankan sangat mudah dengan hanya dengan 1 kali klik.

ViperMonkey adalah *software* yang ditulis dengan Bahasa Phyton, yang dirancang untuk mendeteksi virus makro yang berbahaya yang terdapat dalam file *Malicious Document*. ViperMonkey mengecek file tersebut aman atau tidak terinfeksi virus makro yang berbahaya bagi komputer user. Jika ternyata *file maldoc* yang dianalisa terinfeksi virus makro, maka *file* tersebut harus segera dihapus.

Berdasarkan hal tersebut penulis akan melakukan deteksi dan analisa virus makro pada file *doc* atau dokumen dengan menggunakan *ViperMonkey*.
.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang terdapat diatas, maka rumusan masalah pada proyek akhir ini adalah cara mendeteksi virus makro pada file atau dokumen terinfeksi virus makro/*maldoc*.

1.3 Tujuan

Tujuan dari proyek akhir ini adalah menggunakan Vipermonkey untuk mendeteksi pada *file* dokumen yang dicurigai terinfeksi virus makro/*maldoc.*

1.4 Batasan Masalah

Batasan masalah yang digunakan dalam proyek akhir ini adalah :

1. Menggunakan Vipermonkey sebagai alat untuk mendeteksi virus makro.
2. Menggunakan Operasi sistem Ubuntu.
3. Menggunakan *Virtual, Machine* sebagai *software* pendukung untuk pengujian.
4. Menguji 4 sampel virus makro/*Maldoc*.

1.5 Definisi Operasional

Definisi operasional pada proyek akhir ini adalah :

1. **Keamanan**. keadaan bebas dari bahaya. Istilah ini bisa digunakan dengan hubungan kepada kejahatan, segala penyalahgunaan, dan lain-lain**.**
2. **Aplikasi.** dapat diartikan sebagai suatu program berbentuk perangkat lunak yang berjalan pada suatu sistem tertentu yang berguna untuk membantu berbagai kegiatan yang dilakukan oleh manusia.
3. **Virus Makro.** virus yang dibuat dengan memanfaatkan fasilitas pemrograman modular pada suatu program aplikasi seperti Ms Word, Ms Excel, Corel WordPerfect dan sebagainya
4. **ViperMonkey.** ViperMonkey adalah Emulator Visual Basic for Applications yang ditulis dengan Phyton, yang dirancang untuk mendeteksi dan menyamarkan virus makro yang berbahaya yang terdapat dalam file Microsoft *Office* (Word, Excel, PowerPoint, Publisher, dll).

2. Tinjauan Pustaka

2.1 Virus Makro

Virus makro atau maldoc, merupakan dokumen office berbahaya yang mengandung serangkaian program didalamnya. Hanya membutuhkan 1x klik dari user untuk mengaktifkan makro tersebut. Virus makro atau maldoc adalah alat virus yang dibuat dengan pemrograman pada suatu program aplikasi seperti Microsoft Word, Microsoft Excel, dan sebagainya.

2.2 Identifikasi Virus Makro

Identifikasi virus makro adalah proses studi tentang Virus makro dengan membedah komponen-komponen yang berbeda untuk memahami perilaku dan karakteristik dari virus makro untuk mendeteksi dan mengetahui caranya tersebut bekerja dan mencari celah dalam keamanan.

2.3 ViperMonkey

Dikembangkannya vipermonkey github untuk mendeteksi virus macro/maldoc. Aplikasi ini bersifat opensource bagi user. Tersedia di github dan dapat digunakan di Sistem Operasi Windows ataupun Linux/Ubuntu. ViperMonkey adalah Emulator Visual Basic for Applications yang ditulis dengan Phyton, yang dirancang untuk menganalisis dan menyamarkan virus makro yang berbahaya yang terdapat dalam file Microsoft *Office* (Word, Excel, PowerPoint, Publisher, dll).

2.4 Ubuntu

Ubuntu sering kali digunakan dalam hal security, karena lebih aman dari windows. Ubtuntu ini dijalankan menggunakan virtual machine, sebagai tempat implementasi aplikasinya. Karena mudah digunakan sebagai tempat implementasinya. Ubuntu 16.04 adalah Operasi Sistem yang dilengkapi dengan berbagai platform dengan versi terbaru, seperti Firefox 45, Thunderbird 38, Libre*Office* 5.1, Files 3.14.2, Videos 3.18, Rhythmbox 3.3, GNOME Terminal 3.18 dan banyak lagi.

2.5 Oletools

Vipermonkey memerlukan beberapa fitur dari oletools sebagai pendukungnya.Aplikasi ini sama-sama ditulis dengan Bahasa phyton.
Oletools adalah paket salah satu fitur dari python untuk menganalisis file Microsoft OLE2 (juga disebut Penyimpanan Terstruktur, File Compound Binary Format atau Compound Document File Format), seperti dokumen Microsoft *Office* atau pesan Outlook, terutama untuk analisis malware, forensik, dan debugging.

2.6 Bahasa Pemrograman Python

Python adalah bahasa pemrograman interpretatif multiguna. Tidak seperti bahasa lain, *python* lebih memudahkan user dalam membaca dan memahami Bahasa pemrogramannya.
Bahasa *Python* mendukung semua sistem operasi, bahkan sistem operasi Linux, hampir semuanya sudah menyertakan *Python*.

3. Analisis Dan Perancangan

3.1 Analisis

Pada bab ini menjelaskan mengenai proses analisis terkait dengan cara kerja sistem yang sedang berjalan, kemudian pada bab ini juga akan dibahas penjelasan mengenai gambaran umum sistem, dan blok diagram.

3.1.1 Gambaran Sistem Saat Ini

Gambar 3. 1 Gambaran Sistem Saat Ini.

Pada Gambar 3.1 merupakan gambaran sistem saat ini, file *document* yang terinfeksi virus makro

langsung dibuka oleh user tanpa dicek terlebih dahulu, akibatnya ketika file akan dibuka komputer terinfeksi virus makro.

3.1.2 Blok Diagram

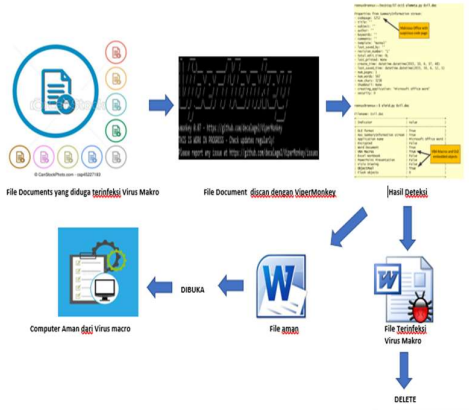
Gambar 3. 2 Blok Diagram.

Pada gambar 3. 2 merupakan block diagram File *Documents* yang diduga terinfeksi virus makro akan dianalisa dengan ViperMonkey. Jika *file* tersebut aman maka *file* dapat dibuka, tetapi jika *File* terinfeksi virus makro maka *file* akan dihapus.

3.2 Perancangan

Perancangan menjelaskan mengenai proses cara kerja sistem yang akan dibuat, Kemudian juga akan dibahas penjelasan mengenai gambaran umum sistem usulan, blok diagram, cara kerja, dan analisis kebutuhan fungsional dan *non* fungsional.

3.2.1 Gambaran Sistem Usulan



Gambar 3. 3 gambaran Sistem Usulan.

Gambar 3.3 merupakan gambaran sistem. File *Documents* yang terinfeksi virus makro di Analisa terlebih dahulu dengan menggunakan ViperMonkey, setelah hasil Analisa keluar jika file aman, maka file dapat dibuka, tetapi jika hasil menunjukkan *file Document* terinfeksi, maka file tersebut harus dihapus. Untuk menjalankan sistem ini diperlukan beberapa alat yang sudah tersedia di dalam sistem operasi, serta diperlukan beberapa alat atau *software* tambahan dan juga beberapa konfigurasi.

3.2.2 Blok Diagram

Pada gambar 3. 4 merupakan blok diagram sistem saat ini ketika menganalisis *malware* adalah seperti berikut.

Gambar 3. 4 Blok Diagram.

1. *Input*

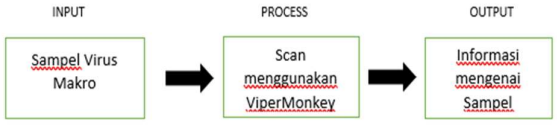
Pada tahap ini pengguna melakukan instalasi *Vipermonkey* terlebih dahulu.

2. *Process*

Pada tahap ini akan dilakukan konfigurasi terlebih dahulu pada *ViperMonkey* dengan menginstal beberapa program yang diperlukan seperti *oletools* dan *Virtual Machine* yang akan dijelaskan lebih lanjut pada bagian implementasi.

3. *Output*

Pada tahap ini akan dihasilkan *output* berupa *ViperMonkey* yang siap digunakan untuk mendeteksi virus makro .



Gambar 3. 5 Blok Diagram.

1. *Input*

Pada tahap ini digunakan perangakat keras yaitu laptop yang menggunakan *sistem operasi Kali linux*. Kemudian *ViperMonkey* dijalankan untuk melakukan analisis virus makro. Dilakukan dengan memasukkan sampel virus makro yang didapat dari web.

2. *Process*

Pada tahap ini akan dilakukan identifikasi dengan memasukkan sampel virus makro yang sudah disediakan sebelumnya yang kemudian dianalisis dengan *ViperMonkey*.

3. *Output*

Pada tahap ini akan dihasilkan *output* berupa laporan yang berisi mengenai informasi tentang isi yang terkandung dalam sampel yang diperiksa.

3.2.3 Cara Kerja

Berikut ini adalah cara kerja sistem yang akan dibuat dalam Proyek Akhir ini adalah sebagai berikut.

1. Pengguna mengambil beberepa sampel virus makro, kemudian dilakukan analisis dengan menggunakan *ViperMonkey*.

2. *ViperMonkey* dijalankan dan melakukan deteksi terhadap virus makro, Kemudian akan memberikan hasil deteksi dari sampel tersebut berupa laporan berisi source code.

3. Hasil dari deteksi akan berupa laporan mengenai informasi sampel virus makro tersebut.

3.2.4 Analisis Kebutuhan Fungsional Dan Non Fungsional

A. Kebutuhan Fungsional

Berikut ini adalah kebutuhan sistem yang diperlukan untuk menyelesaikan Proyek Akhir ini adalah sebagai berikut.

1 ViperMonkey dibangun untuk dapat menganalisis virus makro pada maldoc.
2 *Oletools* sebagai aplikasi paket pendukung untuk ViperMonkey.
3 Mesin virtual.
4 Virus Makro yang yang akan dijadikan sampel untuk uji coba didapatkan dari web.

B. Kebutuhan *Non* Fungsional

Kebutuhan non fungsional pada sistem yang akan dibangun terdiri dari dua bagian yaitu *hardware* dan *software*, adapun rincian dari kedua bagian tersebut adalah sebagai berikut.

1 *Hardware*

Pada Tabel 3. 1 merupakan kebutuhan *hardware* atau perangkat keras yang dibutuhkan untuk membangun sistem adalah sebagai berikut.

Tabel 3. 1 Spesifikasi *Hardware*.

No	Hardware User	Jumlah	Spesifikasi	Keterangan
1	*Laptop User*	1	*RAM* 8 GB, *Storage* 1 TB	*Hardware* yang digunakan untuk menjalankan sistem operasi *kali linux*

2 *Software*

Pada Tabel 3. 2 merupakan kebutuhan *software* atau perangkat lunak yang dibutuhkan untuk membangun sistem adalah sebagai berikut.

Tabel 3. 2 Spesifikasi *Software*.

No	Software User	Fungsi
1	*Ubuntu 16.04*	Sistem operasi yang digunakan untuk menjalankan *ViperMonkey*.
2	*ViperMonkey*	*Software* yang digunakan untuk menganalisis virus makro.
3	*Virtual Machine*	Mesin yang digunakan untuk menjalankan Ubuntu.
4	Virus Makro	Sampel maldoc yang terinfeksi virus makro yang didapat dari *Web* yang kemudian dijadikan sampel untuk menganalis virus makro.
5	*Oletools*	salah satu paket aplikasi yang diperlukan untuk konfigurasi dan menjalankan *ViperMonkey*.
6	*Python*	Bahasa Pemrograman *Python* digunakan untuk konfigurasi dalam penggunaan *ViperMonkey*.

4 Pengujian

Pada Tabel 4. 1 merupakan sampel yang didapat dari *web* yang akan diujikan untuk analisis virus makro menggunakan ViperMonkey.

Tabel 4. 1 Uji Sampel Makro.

Sampel	Temuan	Hash
Sampel 1	VBA Macro	a5e14eecf6beb956732790b05df001ce4fe0f001022f75dd1952d529d2eb9c11
Sampel 2	VBA macro	165342352beed89530e07fab934f28102731a4139ce15e63a39f7b2521723a76
Sampel 3	VBA macro	26de80e3bbbe1f053da4131ca7a405644b7443356ec97d48517f1ab86d5f1ca5

Sampel 4	No VBA macro found	-

5 Kesimpulan

Proyek akhir ini menyimpulkan bahwa ciri-ciri file yang merupakan virus makro yaitu terdapat hash dari VBA macro dan fungsi-fungsi yang dienkripsi. Hasil ini berdasarkan pengujian pada ViperMonkey yang menunjukkan 75% sampel *file Malicious Document* yang diuji mengandung virus makro. Selain itu, berdasarkan verifikasi dengan Virustotal, 30 antivirus mendeteksi sampel sebagai virus makro/malware dan 28 antivirus tidak mampu mendeteksi.

Daftar Pustaka

[1] Github, "Decalage2 ViperMonkey," [Online]. Available: https://github.com/decalage2/ViperMonkey.

[2] Ubuntu, "Ubuntu," [Online]. Available: https://ubuntu.com/download.

[3] Github, "Oletools," [Online]. Available: https://github.com/decalage2/oletools. [Accessed 24 12 2019].

[4] Wikipedia, "Macro virus," [Online]. Available: https://en.wikipedia.org/wiki/Macro_virus. [Accessed 24 12 2019].

[5] M. R. ZULFIKAR, ANALISIS MALWARE MENGGUNAKAN METODE REVERSE ENGINEERING PADA REMNUX, Bandung: Open Library, 2017.

[6] A. D. MULADI, MEMBANGUN SISTEM ANALISIS MALWARE DENGAN MENGGUNAKAN FAME, Bandung: Open Library, 2018

[7] N. A. ISMIYUSHAR, ANALISIS DAMPAK MALWARE BERDASARKAN API CALL DENGAN METODE ANOMALI, Bandung: Open Library, 2018.

[8] S . C. Y. HUTAURUK, Malware Analysis Pada Sistem Operasi Windows untuk Mendeteksi Trojan, Bandung: Open Library, 2016.

[9] Virusshare. [Online]. Available: https://virusshare.com/