JOEICT (Jurnal of Education and Information Communication Technology)
Volume 1, Nomor 1, Tahun 2017: 37 – 43

MALWARE DYNAMIC

Retno Adenansi[1)], Lia A. Novarina[2)]
[1, 2)]Jurusan Pendidikan Teknologi Informasi
e-mail: ade_nansii@yahoo.com[1)], lianugroholiem@gmail.com[2)]

ABSTRAK

Dalam kehidupan di era teknologi sekarang ini semua aktivitas manusia telah dipengaruhi oleh internet. Berbagai informasi, komunikasi, sosialisasi, belanja, menjalankan bisnis, pendidikan dan banyak hal lain yang dapat dilakukan menggunakan internet. Seiring dengan berkembangnya internet berbagai macam ancaman keamanan menjadi lebih beragam.Virus adalah musuh internet nomor satu. Virus memanfaatkan berbagai metode untuk dapat menghindari anti-virus, salah satunya dengan malware. Malware adalah salah satu kode berbahaya yang dapat mengakibatkan dampak buruk bagi sebuah computer maupun pengguna computer. Program ini dapat ,mengubah, merusak, mencari celah, mencuri data pribadi seseorang yang tentu sangat merugikan. Untuk itu diperlukan pengetahuan tentang penyebaran berbagai macam virus dan cara penyebarannya supaya terhindar dari berbagai macam virus. Dalam artikel ini akan dibahas tentang cara penyerang menyebarkan kode berbahaya malware dan cara pendeteksian malware dalam computer. Penulisan artikel ini untuk para pengguna computer lebih mengenal metode yang biasa dilakukan penyerang dalam menyebarkan malware dan cara mengantisipasi serangan malware yang semakin hari semakin beragam. Dalam artikel ini juga dibahas tentang tools yang digunakan untuk analisis malware.

***Kata Kunci**: Cara pendeteksian malware, malware, malware dynamic*

ABSTRACT

In life in today's technological era of all human activities have been effected by internet. Information, communication, socializing, shopping, running abusiness,education and many other things that can be done using the internet. Along with the development of a wide range of internet security threats become more diverse. Virus is the number one enemy of the internet. Viruzes utilize a variety of methods in order to avoid anti-virus, one of them with malware. Malware is one of the malicious code that could result in adverse effects for a computer or computer user. This program can change, break, look for cracks, steal personal data of person who is very detrimental. It is necessary for the deployment of wide range of knowledge about the virus and how it could contribute to avoid the wide variety of viruses. In this article will discuss how attackers to spread malicious code malware and malware detection method in computer. Writing this article for the computer users more familiar with methods used to do attacker in spreading malware and how to anticipate malware. In this article also discussed about the tools used for malware analysis.

***Kata Kunci**: Malware detection method, malware, malware dynamic*

I. PENDAHULUAN

Modus kejahatan di dunia cyber saat ini sangat beragam. Teknik yang digunakan oleh penyerang pun semakin beragam dan kompleks. Berbagai serangan tersebut melibatkan malicious software atau yang biasa disebut malware yang merupakan suatu program jahat. Ancaman malware dan penyebarannya bisa melalui berbagai cara. Salah satu cara yang sering dilakukan untuk menyebarkan malware dengan cara menyisipkannya di sebuah aplikasi ataupun file tertentu.

Malware dapat menyebar dengan cepat di jaringan tanpa campur tangan dari pengguna. Sistem pendektesian malware masih menjadi masalah karena varian malware baru yang selalu berkembang dengan menggunakan teknik yang berbeda untuk menghindari metode pendeteksian. Untuk itu diperlukan mengembangkan teknik pendeteksian malware supaya malware dapat dideteksi secara akurat. Sasaran utama dari malware adalah untuk memata-matai seseorang, mencuri informasi atau data pribadi (rahasia) orang lain seperti m-banking, membobol security program dan lain-lain.

Pada umumnya, sebuah malware diciptakan untuk merusak atau membobol suatu software atau sistem operasi melalui script yang dirahasiakan, dalam arti lain disisipkan secara tersembunyi oleh penyerang. Perkembangan malware yang semakin pesat mengharuskan pengguna computer semakin waspada agar informasi pribadi ataupun file yang penting tidak diambil oleh orang yang tidak berhak. Demikian juga bagi para pelaku bisnis baik perusahaan maupun perorangan yang bergantung dengan sistem computer untuk pekerjaannya agar lebih

menambah pengetahuan tentang malware untuk pencegahan dan antisipasi dari serangan malware yang merugikan. Pemasangan antivirus juga diperlukan sebagai upaya pencegahan malware masuk ke dalam sistem computer.

II. PEMBAHASAN

A. Malware

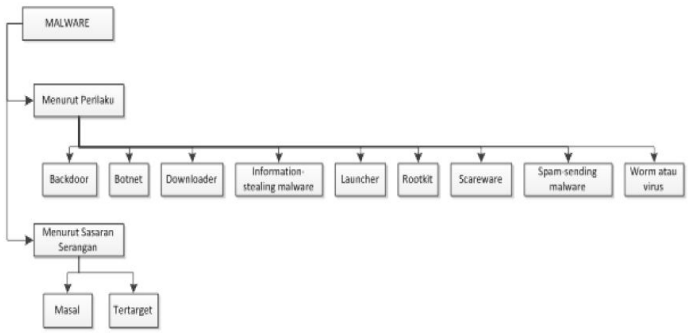
Dalam kecanggihan internet seperti sekarang ini, berbagai macam keamanan menjadi lebih kompleks dan beragam. Penyerang memanfaatkan berbagai macam celah untuk dapat mengambil keuntungan dari korban. Malware merupakan singkatan dari "Malicious Software" yang berarti perangkat lunak mencurigakan. Malware mempunyai beberapa pengerian yang intinya sama, berikut merupakan beberapa pengertian yang dapat kami tulis berdasarkan jurnal yang kami baca [1-3] :

1. Malware adalah perangkat lunak berbahaya dengan tujuan jahat.
2. Malware adalah program yang diinstal pada sistem tanpa pengetahuan pemilik sistem
3. Malware adalah segala bentuk software yang membahayakan baik bagi pengguna, computer atau jaringan.

Jadi dari beberapa pengertian malware di atas dapat disimpulkan bahwa malware merupakan suatu software yang dibuat untuk tujuan tertentu dengan mencari celah keamanan sistem. Malware dapat mengakibatkan dampak buruk bagi computer maupun penggunanya karena penyerang dapat mencuri informasi ataupun data pribadi seseorang.
Tujuan malware diciptakan oleh penyerang untuk merusak atau membobol suatu sistem operasi melalui script rahasia atau dapat dikatakan disisipkan oleh penyerang secara tersembunyi.

B. Taksonomi Malware

Malware dapat dibedakan menurut perilaku dan sasaran serangannya. Menurut perilakunya, malware dibagi menjadi 9 kelompok sedangkan menurut sasaran serangannya, malware dibagi menjadi dua kelompok [3].



Gambar 1. Taksonomi malware menurut Wisnu Nurdiyanto [3]

Berikut beberapa jenis malware menurut perilakunya :

1. Backdoor

Backdoor adalah suatu teknik hacker yang dapat mengakses ke suatu sistem tanpa melalui autentifikasi normal (login) terlebih dahulu dan berusaha tidak terdeteksi

2. Botnet

Botnet adalah teknik membuka akses suatu sistem oleh penyerang dengan semua computer yang terinfeksi botnet akan menerima suatu Intruksi yang sama dari server milik penyerang

3. Downloader

Downloader adalah suatu kode jahat yang bertugas untuk mengunduh kode jahat lainnya. Penyerang menginstal downloader ketika mendapatkan akses ke sebuah sistem. program downloader ini akan menginstal kode jahat tambahan

Information-stealing malware

Information-stealing malware adalah suatu malware yang mengumpulkan berbagai mcam informasi korban dan mengirimkannya ke penyerang. Malware jenis ini biasa digunakan penyerang untuk mendapatkan akeses akun online seperti internet banking

4. Launcher

Launcher adalah suatu program jahat yang digunakan penyerang untuk menjalankan program jahat lainnya. Launche ini menggunakan teknik non-tradisional untuk menjalankan program jahat lainnya agar tidak terdeteksi dan penyerang bisa mendapat akses lebih dalam ke suatu sistem.

5. Rootkit

Rootkit adalah suatu kode yang didesain untuk menyembunyikan keberadaaan kode lainnya. Rootkit dipasang oleh penyerang bersama malware lainnya untuk dapat mengakses jarak jauh serta membuat kode sulit terdeteksi oleh korban.

6. Scareware

Scareware adalah suatu jenis malware yang dibuat untuk menakuti korban agar mau membeli sesuatu. Scareware mempunyai interface yang menyerupai antivirus, biasanya scareware memberi informasi ke pengguna bahwa ada kode jahat dalam sistemnya dan satu-satunya cara dengan membeli software tersebut. Namun kenyataannya software tersebut hanya mampu menghapus scareware tersebut

7. Spam-sending malware

Spam-sending malware adalah suatu malware yang menginfeksi mesin pengguna dan kemudian menggunakanya untuk mengirimkan spam. Malware jenis ini dapat menghasilkan uang bagi penyerang dengan cara menjual layanan pengiriman spam

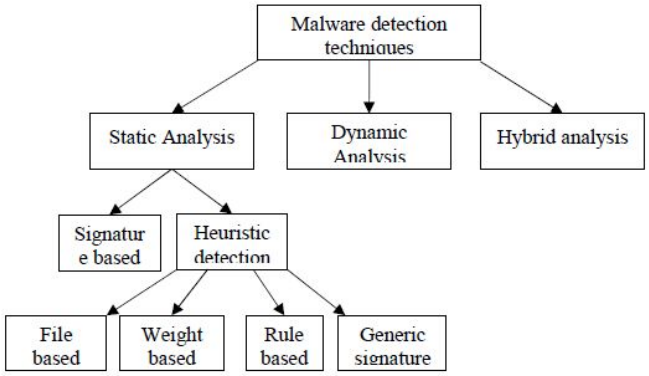
8. Worm atau virus

Worm atau virus adalah sebuah program yang memiliki kemampuan untuk menggandakan dirinya secara mandiri dan menyebar dengan cepat pada jaringan komputer melalui port keamanan yang terbuka. Worm dapat dikatakan evolusi dari virus karena worm memiliki karakteristik yang hampir sama dengan virus, perbedaannya virus bergantung pada program sedangkan worm tidak.

Malware dapat diklasifikasikan berdasarkan tujuan penyerang, yaitu malware masal dan malware tertarget [3]. Malware masal, misalnya berupa launcher didesain untuk menyerang sebanyak mungkin computer korban. Malware masal termasuk dalam malware yang banyak dijumpai dan lebih mudah dideteksi karena banyak software keamanan yang sudah mengantisipasi jenis malware masal. Malware tertarget misalnya information-stealing malware dibuat khusus untuk suatu organisasi tertentu. Malware jenis ini merupakan malware yang lebih berbahaya daripada malware masal karena tidak disebarluaskan dan produk keamanan yang diapakai korban tidak terlindung dari malware tertarget ini.

C. Teknik Analisis Malware

Analisis malware merupakan dasar untuk mendapatkan informasi dalam rangka mengatasi serangan dalam sistem korban. Dari informasi tersebut, dapat dikembangkan signature untuk mendeteksi infeksi malware. Tujuan akhir dari analisis adalah menggambarkan secara tepat cara kerja sebuah malware.



Gambar 2. Representasi Hierarchal berbagai teknik deteksi malware [2]

Teknik yang digunakan untuk analisis ini sebagai berikut :

1. Analisis Statis

Analisis statis adalah analisis yang dilakukan dengan cara mengamati secara langsung source code malware tanpa mengeksekusi malware tersebut. Dalam mengamati source code malware dapat menggunakan program seperti program analyze, debugger dan disassembler. Berikut meupakan beberapa teknik analisis statis :

a) Teknik deteksi berbasis signature

Teknik ini menggunakan pencocokan pola atau string atau teknik fingerprinting [2]. Penyerang menyisipkan signature ke dalam suatu aplikasi dan signature ini digunakan untuk mengidentifikasi jenis malware tertentu. Untuk dapat mencari kode malware, detector malware akan mencari signature yang sudah ada dalam kode.

b) Teknik deteksi heuristic

Teknik ini juga dikenal sebagai teknik proaktif [2]. Teknik ini hampir mirip dengan teknik deteksi berbasis signature. Perbedaannya teknik heuristic ini mencari perintah atau intruksi dalam suatu program aplikasi. Hasil akhirnya adalah mudah untuk mendeteksi varian baru dari malware yang semakin banyak jenisnya.

Keuntungan Analisis Statis

Analisis statis cepat dan aman, pengumpulan struktur kode program di bawah pemeriksaan.jika analisis statis dapat menghitung perilaku berbahaya dalam aplikasi, maka analisis ini dapat digunakan dalam mekanisme keamanan di masa depan [2].

Kerugian Analisis Statis

Source code sumber sulit diketahui karena masih banyak aplikasi yang tidak menyediakannya, untuk melakukan analisis statis, peneliti harus memiliki pengetahuan yang baik tentang bahasa assembly dan juga harus memiliki pemahaman yan tinggi tentang fungsi dari suatu sistem operasi [2].

2. Analisis dinamic

Analisis dinamik merupakan metode analisa yang mengamati kerja suatu sistem yang dapat terlihat dari perilaku suatu sistem sebelum malware dijalankan dengan perilaku setelah malware tersebut dijalankan atau dieksekusi dalam sistem tersebut. Metode analisis ini biasanya menggunakan software seperti VirtualBox, sehngga apabila malware yang dieksekusi tersebut merusak sistem maka sistem utama tidak mengalami kerusakan akibat malware yang dijalankan

Keuntungan Analisis Dinamic
Dapat dengan mudah mendeteksi suatu malware yang tidak diketahui hanya dengan menganalisis perilaku dari suatu program atau aplikasi.

Kerugian Analisis Dinamic
Analisis ini membutuhkan waktu untuk melakukan eksekusi suatu program atau aplikasi sehingga menjadi lama dan tidak aman. Analisis ini gagal untuk melakukan pendeteksian multipath malware [2]

3. Analisis hybrid

Teknik analisis ini adalah teknik analisis kombinasi dari analisis statis dan analisis dinamis. Teknik ini menggabungkan keunggulan teknik statis dan dinamis yaitu melakukan pengecekan untuk setiap signature malware jika ditemukan kode di bawah pemeriksaan dan kemudian memonitor perilaku kode.

D. Teknik dalam Analisis Dinamic

1. Monitoring Function Call

Monitoring ini merupakan panggilan yang dikontrol oleh subroutine, setelah dieksekusi melewati control eksekusi kemudian kembali ke instruksi pada program utama. Seluruh proses akan dipantau oleh program yang membantu untuk menganalisis perilaku. Fungsi hook ini bertanggung jawab melaksanakan fungsi analisis seperti menganalisis parameter input.

2. Analysis of Function Parameter

Teknik ini sangat penting dalam analisis dinamis karena analisis ini memantau nilai yang sebenarnya. Output dari sistem call CreateFile digunakan sebagai input ke WriteFile. Fungsi ini menggelompokkan menjadi set logis yang menyediakan informasi rinci tentang perilaku program.

3. Information Flow Tracking

Pendekatan utama fungsi panggilan pemantauan pelaksanaan program adalah menganalisis tentang bagaimana program bekerja pada data. Teknik ini merupakan metodologi inti yang digunakan oleh tools analisis dinamis yang bekerja pada berbagai tingkatan sistem operasi.

Table 1. Tools dalam Malware Dynamic [6]

No	Process explorer	monitor currently runnng process
1.	Filemon	Monitor file operation
2.	Regmon	Monitor operation on registry
3.	Regshot	Takes snapshot of the registry and associated file
4.	Tcpview	Display all tcp & udp open connections and the process that opened and using the port
5.	Tdimon	Network connectivity is logged, but packet contents are not logged
6.	Ethereal	Packet sniffer, helps in viewing of contents/payload

D. MALWARE TOOLS

Di bawah ini merupakan alat-alat yang digunakan untuk pendekatan yang disajikan untuk menganalisis software berbahaya.
Malware tools yang dihasilkan oleh alat-alat sampel memberikan pengetahuan yang penting. Pengetahuan ini diperlukan untuk mengembangkan penanggulangan secara tepat waktu.

1. Anubis : Anubis mengeksekuksi sampel yang terdiri dari sistem operasi Windows XP yang berjalan sebagai tamu di Qemu. Analisis ini dilakukan untuk memantau fungsi API Windows serta layanan sistem panggilan ke jendela asli API. Parameter yang dikirim pada fungsi-fungsi ini diperiksa dan dilacak.

2. CWSandbox: dibuat untuk mengeksekusi pada analisis baik native atau dalam lingkungan Windows Virtual. Sistem dirancang untuk menangkap perilaku sampel software berbahaya terhadap sistem file dan manipulasi registry, jaringan komunikasi, dan interaksi sistem operasi. Sistem virtual meruapakn sistem instalasi penuh dari kelas operasi Win32 di mana sampel analisis dijalankan bersama-sama dengan komponen analisis.

3. Norman Sandbox: Analisis malware dinamis yang mengeksekusi sampel dan di simulasikan pada sistem operasi windows . Norman Sandbox dibuat untuk menggantikan semua fungsi yang diperlukan oleh sampel untuk dianalis dengan versi simulasi. Sistem simulasi harus menyediakan sistem operasi pendukung yang relevan seperti memory protection dan multi-threading support. Norman Sandbox ini memfokuskan pada deteksi worm yang menyebar melalui e-mail atau jaringan peer-to-peer serta mendeteksi software berbahaya lainnya.

4. JoeBox: JoeBox merupakan log yang berisi informasi tindakan tingkat tinggi yang dilakukan sistem file, registry, sistem dan kegiatan. JoeBox dirancang secara khusus untuk berjalan pada perangkat keras nyata dan tidak bergantung pada virtualisasi. Sistem ini dirancang sebagai model client server dimana controller tunggal dapat mengkoordinasi beberapa client untuk melakukan analisis. Semua data yang akan dianalisis dikumpulkan oleh mesin pengendali.

III. KESIMPULAN

Dalam makalah ini telah dibahas berbagai macam klasifikasi jenis malware yang digunakan oleh penyerang. Hacker memanfaatkan berbagai macam celah untuk dapat menginfeksikan malware ke dalam sistem computer pengguna. Dengan adanya berbagai jenis malware, penyerang selalu berusaha mencari keuntungan dari pengguna. Agar komputer terhindar dari serangan malware, perlu adanya kesadaran untuk selalu mengantisipasi, menjaga dan mengatasi malware di dalam komputer. Salah satu pencegahan dan pengamanan adalah dengan melakukan scanning komputer melalui antivirus secara berkala. Pengetahuan tentang malware juga diperlukan untuk antisipasi penyebaran malware yang semakin kompleks dengan berbagai macam cara. Analysis malware digunakan untuk mendeteksi malware terhadap suatu program yang terindikasi terkena malware. Pada malware dynamic terdapat beberapa tools yang dapat digunakan dan menambah pengetahuan penting bagi para pengguna computer.

DAFTAR PUSTAKA

[1] Monika Agrawal,Heena Singh, Nidhi Gour, Mr. Ajay Kumar, *Evaluation on Malware Analysis,* International Journal of Computer Science and Information Technologies (IJCSIT) 2014

[2] Dolly Uppal, Vishakha Mehra and Vinod Verma, *Basic survey on Malware Analysis Tools and Techniques,* International Journal on Computational Sciences & Applications (IJCSA) 2014

[3] Wisnu Nurdiyanto, *Skenario Kombinasi Tools yang Efektif dalam Analisis Malware* 2013

[4] Ekta Gandotra Divya Bansal Sanjeev Sofat**,** *Malware Analysis and Classification:A Survey* Journal of Information Security, 2014

[5] Savan Gadhiya, Kaushal Bhavsar, *Techniques for Malware Analysis IJARCSSE 2013*

[6] Navroop Kaur, Amit K. Bindal, PhD, *A Complete Dynamic Malware Analysis* , International Journal of Computer Applications *2016*