



Analisa Malware

Prof. Richardus Eko Indrajit

Email: indrajit@post.harvard.edu Website: <http://www.EkoIndrajit.com>

Pendahuluan

Modus operandi kejahatan di dunia siber sangatlah beragam dan bervariasi. Teknik yang dipergunakan oleh para kriminal pun semakin lama semakin mutakhir dan kompleks. Berdasarkan kejadian-kejadian terdahulu, hampir seluruh serangan melibatkan apa yang disebut sebagai “malicious software” atau “malware” – yang dalam terjemahan bebasnya adalah program jahat (karena sifatnya yang merusak atau bertujuan negatif).

Analisa malware adalah suatu aktivitas yang kerap dilakukan oleh sejumlah praktisi keamanan teknologi informasi untuk mendeteksi ada atau tidaknya komponen sub-program atau data yang bertujuan jahat dalam sebuah file elektronik. Analisa atau kajian ini sangat penting untuk dilakukan karena:

- Malware sering diselundupkan melalui file-file umum dan populer seperti aplikasi (.exe), pengolah kata (.doc), pengolah angka (.xls), gambar (.jpg), dan lain sebagainya – sehingga jika pengguna awam mengakses dan membukanya, akan langsung menjadi korban program jahat seketika;
- Malware sering diselipkan di dalam kumpulan file yang dibutuhkan untuk menginstalasi sebuah program atau aplikasi tertentu – sehingga jika sang pengguna melakukan instalasi terhadap aplikasi dimaksud, seketika itu juga malware diaktifkan;
- Malware sering disamarkan dengan menggunakan nama file yang umum dipakai dalam berbagai keperluan, seperti driver (.drv), data (.dat), library (.lib), temporary (.tmp), dan lain-lain – sehingga pengguna tidak sadar akan kehadirannya di dalam komputer yang bersangkutan;
- Malware sering dikembangkan agar dapat menularkan dirinya ke tempat-tempat lain, dengan cara kerja seperti virus atau worms – sehingga komputer pengguna dapat menjadi sarang atau sumber program jahat yang berbahaya;
- Malware sering ditanam di dalam sistem komputer tanpa diketahui oleh sang pengguna – sehingga sewaktu-waktu dapat disalahgunakan oleh pihak yang tidak berwenang untuk melakukan berbagai tindakan kejahatan; dan lain sebagainya.

Model Analisa

Pada dasarnya malware adalah sebuah program, yang disusun berdasarkan tujuan tertentu dengan menggunakan logika dan algoritma yang relevan dengannya. Oleh karena itulah maka model analisa yang biasa dipergunakan untuk mengkaji malware sangat erat kaitannya dengan ilmu dasar komputer, yaitu: bahasa pemrograman, algoritma, struktur data, dan rekayasa piranti lunak.

Secara umum, ada 3 (tiga) jenis analisa terhadap sebuah program untuk mendeteksi apakah yang bersangkutan merupakan malware atau bukan. Ketiga pendekatan dimaksud akan dijelaskan dalam masing-masing paparan sebagai berikut.

Surface Analysis

Sesuai dengan namanya, “surface analysis” adalah suatu kajian pendeteksian malware dengan mengamati sekilas ciri-ciri khas sebuah file program tanpa harus mengeksekusinya. Untuk melihat ciri khas tersebut dapat dilakukan dengan menggunakan bantuan software atau perangkat aplikasi pendukung. Analisa ini memiliki ciri-ciri sebagai berikut:

- Program yang dikaji tidak akan dijalankan, hanya akan dilihat “bagian luarnya” saja (sebagai analogi selayaknya orang yang ingin membeli buah-buahan, untuk mengetahui apakah buah yang bersangkutan masih mentah atau sudah busuk cukup dengan melihat permukaan kulitnya, membaunya, dan meraba-raba tekstur atau struktur kulitnya). Dari sini akan dicoba ditemukan hal-hal yang patut untuk dicurigai karena berbeda dengan ciri khas program kebanyakan yang serupa dengannya; dan
- Sang pengkaji tidak mencoba untuk mempelajari “source code” program yang bersangkutan untuk mempelajari algoritma maupun struktur datanya (sebagaimana layaknya melihat sebuah kotak hitam atau “black box”).

Saat ini cukup banyak aplikasi yang bebas diunduh untuk membantu melakukan kegiatan surface analysis ini, karena cukup banyak prosedur kajian yang perlu dilakukan, seperti misalnya: HashTab dan digest.exe (Hash Analysis), TrID (File Analysis), BinText dan strings.exe (String Analysis), HxD (Binary Editor), CFF Explorer (Pack Analysis), dan 7zip (Archiver).

Runtime Analysis

Pada dasarnya ada kesamaan antara runtime analysis dengan surface analysis, yaitu keduanya sama-sama berada dalam ranah mempelajari ciri-ciri khas yang selayaknya ada pada sebuah program yang normal. Bedanya adalah bahwa dalam runtime analysis, dipersiapkan sebuah prosedur dan lingkungan untuk mengeksekusi atau menjalankan program yang dicurigai mengandung atau sebagai malware tersebut.

Model analisa ini menghasilkan kajian yang lebih mendalam karena selain dihilangkannya proses “menduga-duga”, dengan mengeksekusi malware dimaksud akan dapat dilihat “perilaku” dari program dalam menjalankan “skenario jahatnya” sehingga selanjutnya dapat dilakukan analisa dampak terhadap sistem yang ada.

Oleh karena itulah maka aplikasi pendukung yang dipergunakan harus dapat membantu mensimulasikan kondisi yang diinginkan, yaitu melihat ciri khas dan karakteristik sistem, sebelum dan sesudah sebuah malware dieksekusi. Agar aman, maka program utama yang perlu dimiliki adalah software untuk menjalankan virtual machine, seperti misalnya: VMWare, VirtualBoz, VirtualPC, dan lain sebagainya. Sementara itu aplikasi pendukung lainnya yang kerap dipergunakan dalam melakukan kajian ini adalah: Process Explorer, Regshot, Wireshark, TCPView, Process Monitor, FUNdelete, Autoruns, Streams/ADSSpy, dan lain-lain. Keseluruhan aplikasi tersebut biasanya dijalankan di sisi klien; sementara di sisi server-nya diperlukan FakeDNS, netcat/ncat, tcpdump/tshark, dan lain sebagainya.

Static Analysis

Dari ketiga metode yang ada, static analysis merupakan model kajian yang paling sulit dilakukan karena sifat analisisnya yang “white box” alias pengkajian melibatkan proses melihat dan mempelajari isi serta algoritma program malware dimaksud, sambil mengamati sekaligus menjalankan/mengeksekusinya.

Karena sifat dan ruang lingkupnya yang cukup luas dan mendalam, strategi khusus perlu dipersiapkan untuk melakukan kajian ini. Disamping itu, kajian ini juga memerlukan sumber daya yang khusus – misalnya adalah SDM yang memiliki pengetahuan dan pengalaman dalam membuat serta membaca program berbahasa

mesin atau rakitan (assembly language) serta ahli arsitektur dan organisasi piranti komputasi seperti komputer, PDA, tablet, mobile phone, dan lain sebagainya.

Cukup banyak aplikasi pendukung yang diperlukan, tergantung dari kompleksitas malware yang ada. Contohnya adalah: IDA Pro (Disassembler); Hex-Rays, .NET Reflector, and VB Decompiler (Decompiler); MSDN Library, Google (Library); OllyDbg, Immunity Debugger, WinDbg/Syser (Debugger); HxD, WinHex, 010editor (Hex Editor); Python, Lunux Shell/Cygwin/MSYS (Others); dan lain-lain.

Hasil Analisa

Terlepas dari berbagai metode yang dipergunakan, apa sebenarnya hasil dari analisa yang dilakukan? Secara umum berdasarkan kajian yang dilakukan terhadap sebuah program yang dicurigai sebagai atau mengandung malware akan diambil kesimpulan:

1. Benar tidaknya program dimaksud merupakan malware atau mengandung unsur malware;
2. Jika benar, maka akan disampaikan jenis atau tipe malware dimaksud dan cara kerjanya;
3. Dampak yang terjadi akibat adanya malware tersebut dalam sebuah sistem;
4. Kiat cara mengurangi dampak negatif seandainya malware tersebut telah terlanjur dieksekusi dalam sebuah sistem atau cara mengeluarkan malware tersebut dalam sebuah sistem untuk mencegah terjadinya efek negatif;
5. Rekomendasi mengenai apa yang harus dilakukan untuk menghindari masuknya malware tersebut di kemudian hari, atau paling tidak cara-cara melakukan deteksi dini terhadap keberadaannya; dan
6. Menyusun panduan atau prosedur dalam menghadapi hal serupa di kemudian hari sebagai referensi (lesson learnt).

--- oOo ---