Samuel Sembiring, dr

Arsip Perangkat Jahat:

Buku#3: 12 Langkah Menjadi Virus Analyst Lokal Terbaik

Diterbitkan secara mandiri

melalui Nulisbuku.com

Arsip Perangkat Jahat#3: 12 Langkah Menjadi Virus Analyst Lokal Terbaik

Oleh: *Samuel Sembiring, dr*

Penerbit

Penerbit Sam's Books

http://www.samuelkarta.com

dokter@samuelkarta.com

Desain Sampul:

Samuel Sembiring, dr

Untuk kedua orang tuaku

DAFTAR ISI

Pendahuluan

Sekarang banyak sekali kita lihat hasil-hasil analisis dari virusanalyst yang tersebar di blog-blog/web virologist. Ada yang hasilnya mengesankan dan ada juga yang hasilnya 'omong kosong'.

Tapi perlu diketahui, semua orang bisa menganalisis malware. Siapa saja! Apalagi setelah kamu baca buku ini. Kamu akan tahu apa yang kamu perlukan untuk menganalisis malware.

Dan satu hal lagi yang kamu perlu tahu. Tidak semua orang yang menganalisis virus itu pintar. Malah ada virusAnalyst yang copy paste dari web debugger asing. Tidak usah muluk-muluk dan tidak perlu ada yang ditutup-tutupi, banyak sekali saya lihat di beberapa blog/web hasil analisisnya dicopypaste dari web debugger asing. Dan yang lebih parahnya lagi, mereka yang mengepost/mempublish artikel (hasil analisis) itu menyebut dirinya virusanalyst. Wah, wah, banyak sekali kasus seperti itu.

Mereka itu kita sebut saja "VTC", Virus Analyst Tukang Contek

Kalau hanya copy paste *sih*, siapa pun bisa! Tetapi ada yang tidak bisa 'mereka' lakukan. Nanti saya akan beri tahu apa yang VTC tidak bisa lakukan. Untuk itu bacalah buku ini hingga tuntas. Oke!

Saya juga akan beritahu bagaimana dan apa saja web malware debugger yang sering digunakan VTC. Saya tidak mengajarkan kamu untuk memanfaatkannya, tapi saya hanya akan memberitahu apa yang mungkin kamu tidak tahu.

Di dalam tutorial ini, saya juga akan jelaskan bagaimana menganalisis virus/malware. Nah, sebelumnya saya beritahu sesuatu dulu (supaya tidak simpang siur).

Sebenarnya apa yang akan kita analisis nantinya?

Jawabnya adalah malware. Saya rasa semua sudah tahu apa itu malware. Malware terdiri dari banyak kelas seperti virus, worm, trojan ,spyware dan lain-lainnya. Istilah awam malware atau *malicious ware* ini adalah virus.

Memang cukup membingungkan. Para virologist menyebutnya malware sedangkan orang awam menyebutnya virus.

Perhatikan kalimat-kalimat berikut.

• Para virologist mendefinisikan virus sebagai malware yang membutuhkan file untuk bisa hidup atau menular, sedangkan orang awam mendefenisikan virus sebagai program apa saja yang merusak.

• Para virologist mengetahui perbedaan antara virus dan worm, sedangkan orang awam tidak tahu perbedaan virus dan worm. Kadang mereka menyebut worm juga termasuk virus.

• Para virologist tahu bahwa trojan juga berbeda dari virus dan worm, sedangkan orang awam menyebutkan bahwa trojan termasuk salah satu jenis virus. Malah kadang ada teman kita yang mengatakan "virus Trojan"

Sekarang yang menjadi pertanyaan adalah siapa yang benar? Para virologist tidaklah salah. Mereka benar. Tapi orang awam juga tidak salah. Jadi untuk apa pertanyaan ini ditanyakan?

Para virologist memang sudah tahu betul dan tahu selukbeluk malware sendiri. Mereka juga tahu pembagian kelas-kelas malware.

Tapi pernahkah kamu sadari bahwa sebenarnya kebanyakan virologist memihak istilah orang awam? Kamu mengerti yang saya katakan?

Nah, begini. Pernahkah kamu mendengar istilah Norton Antimalware atau Norton Antiworm? Yang ada adalah Norton Antivirus (tanpa bermaksud untuk menyebutkan merek).

Norton Antivirus bisa memberantas virus, worm, trojan dan kelas-kelas malware lainnya.

Begitu juga dengan Norman Virus Control, Morphost Antivirus, Wedash Antivirus dan lain-lain. apakah ada istilah Norman Worm Control, Morphost Antitrojan, Wedash AntiSpyware? Semuanya memakai istilah "virus", padahal mereka tidak hanya memberantas virus saja, akan tetapi memberantas virus, worm, trojan dan lain-lain.

Meskipun sebenarnya ada juga tools/software lain yang menyebutkan antitrojan dan antispyware. Kebetulan untuk istilah yang seperti itu memang dikhususkan untuk beberapa kelas malware saja.

Nah, di dalam tutorial ini saya memakai istilah "virus" untuk mencakup seluruh kelas malware. Saya mengikuti istilah awamnya saja. Sengaja saya jelaskan ini di bagian pendahuluan supaya tidak ada virologist yang menentang atau memprotes dan supaya semuanya sama-sama mengerti.

Buku ini sengaja saya tulis supaya meningkatkan keinginan para virusAnalyst yang kebetulan mungkin belum tahu ada tools-tools lain yang belum mereka gunakan. Dan supaya virusAnalyst tidak meniru VTC.

Arga Makmur, April 2016

Penulis