Samuel Sembiring, dr

Arsip Perangkat Jahat:

Buku#1: 16 Teknik Terbaik Ciptakan Virus Paling Berbahaya!

Diterbitkan secara mandiri

melalui Nulisbuku.com

Arsip Perangkat Jahat#1: 16 Teknik Terbaik Ciptakan Virus Paling Berbahaya!

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

	Daftar Isi	4
	Pendahuluan	5
1	Trik Lolos dari Heuristik Icon Antivirus	8
2	Trik Agar Virus Sulit Dibunuh	14
3	Teknik Mutasi Virus	19
4	Mempercepat Eksekusi Virus	22
5	Tutorial *Encrypted* VBS	27
6	Trik Mengelabui Caption	30
7	Tutorial Membuat Virus Macro	35
8	Tutorial Membuat Virus Macro (2)	53
9	Teknik Automacros Pada Virus Macro	59
10	Mungkinkah Virus Macro Ber-polymorphic?	66
11	Teknik Virus Mengetik Sendiri	73
12	Trik Virus Batch yang *Bikin* Jahil	76
13	Pemrograman Virus Batch	78
14	Membuat Virus Vinorika Tiruan	86
15	Teknik Menembus Smad-Lock	106
16	Mungkinkah Proteksi Smadav di-nonaktifkan?	114
	Tentang Penulis	119

Pendahuluan

Isi buku ini merupakan sekumpulan arsip yang telah saya tulis pada tahun 2008 hingga 2011. Saat itu adalah masa-masa kejayaan virus lokal maupun asing. Tak sedikit juga antivirus lokal yang bermunculan pada saat itu.

Teknik-teknik baru sering mencuat di dunia maya. Setiap programmer memiliki cara dan teknik masing-masing dalam mengekspresikan kemampuannya. Tentunya dalam bentuk virus ataupun antivirus. Hingga terbentuk opini virus versus antivirus merupakan perang intelektual para programmer.

Para pembuat virus tidak berhenti di satu teknik. Semua berlomba menemukan ide-ide baru. Motif mungkin berbeda-beda, entah itu popularitas, iseng, mengisi waktu atau mengembangkan skill.

Sebuah virus dapat ditulis dengan berbagai bahasa pemrograman. Salah satu yang populer adalah bahasa visual basic. Berdasarkan perkiraan saya, sekitar 80% virus lokal yang beredar ditulis dengan bahasa ini. Sebab bahasanya mudah dipelajari. Mungkin di zaman

yang modern saat ini visual basic sudah tidak lagi populer.

Aplikasi atau software saat ini cenderung berubah dari visual basic hingga ke java dan bahasa lain. Sehingga virus-virus visual basic sebenarnya tidak lagi populer. Ditambah lagi kemampuan heuristik antivirus sekarang yang semakin baik dan juga system operasi komputer sekarang yang tingkat keamanannya sudah semakin tinggi.

Istilah "virus" sebenarnya tidak tepat. Yang tepat adalah malware atau *malicious ware* yang dalam bahasa Indonesia artinya "perangkat jahat." Malware sendiri banyak jenisnya, mulai dari virus, worm, Trojan, backdoor dan lain-lainnya. Namun para ahli sepakat menggunakan kata "virus" agar lebih mudah dipahami masyarakat umum.

Sebagian besar isi buku ini merupakan teknik dan trik yang saya temukan secara otodidak, selebihnya adalah teknik-teknik virus yang beredar yang saya coba bongkar.

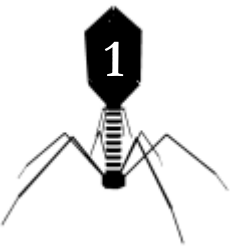
Buku ini mungkin tidak seluruhnya dapat diaplikasikan pada saat ini, sebab sebagian besar tekniknya menggunakan bahasa visual basic. Alasan buku ini saya buat hanya untuk peng-arsip-an artikel-artikel lama yang telah saya tulis dulu. Juga berguna untuk mereka yang ingin mempelajari lagi ide-ide virus yang unik.

Dalam buku ini saya tidak mengajarkan bagaimana langkah-langkah membuat virus mulai dari dasar hingga menjadi virus ganas. Karena tujuan buku ini bukan untuk itu. Sehingga buku ini mungkin tampak sulit bagi mereka yang pemula atau ingin mulai belajar.

Semoga buku ini dapat memberikan manfaat.

Arga Makmur, Februari 2016

Penulis



Trik Lolos dari Heuristik *Icon* Antivirus

Belakangan ini metode heuristik antivirus semakin canggih saja. Mulai dari pengecekan string tubuh virus hingga pengenalan tingkah laku virus. Salah satu metode heuristik yang cukup terkenal adalah heuristik *icon*.

Metode heuristik ini sebenarnya dapat dikatakan metode lama. Antivirus asing-asing rata-rata sudah memiliki metode ini. Sementara antivirus lokal mungkin belum semua, tetapi saya yakin sudah banyak yang menggunakan teknik ini. Karena metode ini mampu

mendeteksi banyak virus virus (sebenarnya worm, tetapi kita pakai istilah virus saja) baru.

Saya akan memaparkan bagaimana cara agar virus kamu tidak terdeteksi oleh heuristik *icon* antivirus. Hal ini perlu sebab sudah banyak antivirus yang memiliki teknik heuristik untuk mendeteksi *icon-icon* palsu.

Begini caranya supaya virus kamu bisa lolos. Teknik ini saya beri nama teknik Icon-phic. Teknik ini saya temukan sendiri dan kecil kemungkinan akan kamu dapatkan dari buku lain.

FAKTA:
Icon folder sering dijadikan *icon* yang paling banyak digunakan pada virus oleh *Virus Maker*. Sebenarnya *icon* folder pun berbeda-beda. Mulai dari icon folder yang berwarna terang hingga ke warna yang dianggap pas menyerupai folder biasanya. Dan ada juga virus yang menggunakan icon folder lama.

KELEBIHAN
Mampu mengelabui pengguna PC dengan sangat mudah. Banyak pengguna PC tidak mengira file ber-*icon* folder itu adalah virus. Apalagi kalau file tersebut

memiliki nama file-file yang dapat menarik pengguna untuk membukanya. Nama-nama file berbau porno, tugas, film dan lain-lain sering berhasil mengelabui pengguna PC.

KEKURANGAN

Antivirus lokal sekarang umumnya dilengkapi dengan heuristik pembandingan *icon* jadi umumnya virus yang menggunakan *icon* folder biasanya akan terdetesi dengan mudah. Bayangkan saja! Virus yang sudah dibuat dengan susah payah ternyata mudah ditangkap oleh antivirus!

Teknik Icon-phic: *Icon* folder memang diakui sebagai *icon* yang paling ampuh meski dianggap meniru. Penggunaan *icon* folder juga dianggap sebagai metode tua pada virus. Meski begitu yang terpenting adalah virus buatan kita sukses!

Ada cara supaya virus kamu lolos dari *scanning* antivirus yang berheuristik *Icon Compare*. Yaitu dengan menggunakan software editor untuk *icon*. Saya sendiri biasanya menggunakan microsoft Visual C++ untuk mengedit icon.