Samuel Sembiring, dr

Arsip Perangkat Jahat#2

# Buku#2: 13 Metode Wajib Antivirus Untuk Deteksi Virus Terbaru

Diterbitkan secara mandiri

melalui Nulisbuku.com

ARSIP PERANGKAT JAHAT
Buku#2: 13 Metode Wajib Antivirus Untuk Deteksi Virus Terbaru

Oleh: *Samuel Sembiring, dr*



**Penerbit**

*Penerbit Sam's Books*

*http://www.samuelkarta.com*

*dokter@samuelkarta.com*

Desain Sampul:

*Samuel Sembiring, dr*

diterbitkan melalui:

**www.nulisbuku.com**

*Untuk kak Iski dan Endang*

## DAFTAR ISI


| | | |
|---|---|---|
| | Daftar Isi | 4 |
| | Pendahuluan | 5 |
| 1 | Teknik DeepScan Antivirus | 9 |
| 2 | Teknik FastScanning Morphost | 15 |
| 3 | Bagaimana Cara Antivirus Mendeteksi virus Sality? | 21 |
| 4 | Source Code Deteksi Virus RunOnce | 35 |
| 5 | Teknik Enkripsi Database | 41 |
| 6 | Trik Scanning File Shortcut | 47 |
| 7 | Metode Heuristik Ganda | 51 |
| 8 | Metode Heuristik No Shortcut dan Missing Target | 55 |
| 9 | Modifikasi Baru Teknik ReadString: Cepat, Tepat, dan Akurat! | 59 |
| 10 | Ilmu Kompres Karantina Pada Antivirus | 65 |
| 11 | Nyalakan Alarm Antivirusmu | 71 |
| 12 | Parameter Command Untuk Antivirus | 73 |
| 13 | Penerapan Menu Konteks "Send to" Pada Antivirus | 77 |
| | Tentang Penulis | 85 |

## Pendahuluan

Antivirus dari waktu ke waktu semakin canggih. Canggih dari segi kecepatan, pendeteksian, penuntasan maupun perbaikan PC paska terinfeksi virus. Setiap antivirus menawarkan keunggulannya masing-masing agar pengguna PC mau memakainya. Dalam hal ini, memakai artinya membeli. Dan dari sinilah para vendor antivirus mendapat penghasilan.

Tidak sedikit antivirus yang berbayar, walaupun ada juga yang gratis. Ada harga ada rupa. Antivirus dari perusahaan terkenal terkadang mematok harga yang tinggi. Tetapi ada juga antivirus canggih yang dapat diunduh secara gratis. Kecanggihan suatu antivirus tidak dapat ditentukan berdasarkan harga.

Teknik-teknik canggih diciptakan oleh programmer-progrrammer antivirus handal, agar tidak kalah saing dengan virus-virus baru yang terus bermunculan. Setiap antivirus memiliki teknik masing-masing dalam menangani virus. Dan tentunya mereka pastinya tidak akan membocorkan tekniknya sendiri.

Memang antivirus lokal mungkin belum dapat menyaingi antivirus luar, tetapi kalau soal urusan virus lokal antivirus kita tidak kalah lebih baik. Antivirus tanah air sendiri saat ini jumlahnya sangat banyak. Dan hampir semua merupakan buatan programmer lokal secara individu. Mungkin hanya dua atau tiga yang berupa suatu kelompok atau organisasi komersil. Menurut catatan yang pernah saya dapatkan, saat ini Indonesia memiliki antivirus buatan lokal terbanyak di Asia.

Buku ini saya tulis mulai pada tahun 2008, dimana isinya merupakan sekumpulan arsip tentang teknik-teknik antivirus. Sebagian besar adalah teknik yang saya kembangkan sendiri. Dan hampir semua teknik yang aa di buku ini telah saya terapkan pada antivirus buatan saya, Morphost.

Buku ini tidak mengajarkan kepada kamu bagaimana membuat antivirus mulai awal, atau langkah-langkah membuat antivirus. Di sini kita bercerita soal "teknik" atau metode. Jadi sangat diharapkan pembaca sebaiknya sudah memiliki kemampuan programming atau sudah memiliki antivirus buatan pribadi sebelumnya.

Mungkin tidak semua metode yang ada di dalam buku ini yang bisa kamu terapkan. Tetapi setidaknya saya berharap dengan adanya buku ini, banyak ide cemerlang yang muncul sehingga kamu bisa membuat antivirus yang canggih.

Terima kasih dan selamat membaca.

Arga Makmur, Februari 2016

Penulis

# Teknik DeepScan Antivirus

Sekarang banyak pembuat antivirus yang masih menggunakan teknik pendeteksian dengan metode basis data / checksum saja, ditambah dengan beberapa teknik heuristik. Pendeteksian dengan checksum merupakan hal wajib bagi antivirus, karena dinilai cukup mudah, cepat dan tepat. Contoh checksum yang digunakan antivirus lokal diantaranya CRC32, CRC16, MD5, M31 dan checksum-checksum lainnya. Sebagian lagi membuat checksum sendiri. Sedangkan metode heuristik karena pembuatannya juga cukup rumit dan butuh ide yang baik maka tidak semua antivirus memiliki metode heuristik yang sama. Salah satu metode heuristik yang populer di kalangan antivirus tanah air adalah pendeteksian menurut icon folder.

Pengertian heuristik sebenarnya cukup luas. Tetapi pada bidang antivirus, heuristik ini berarti pendekatan-pendekatan yang didasarkan kepada tingkah laku atau kebiasaan virus. Pendekatan-pendekatan ini kemudian diperkuat karena kekerapan yang terjadi pada virus-virus lokal. Misalnya, virus-virus lokal yang menggunakan icon folder untuk mengelabui pengguna PC.

Dalam tulisan kali ini, metode yang saya paparkan termasuk metode heuristik. Saya perhatikan belum banyak antivirus yang menggunakannya. Padahal teknik ini lumayan ampuh.

Memang Morphost belum menggunakan teknik ini. Karena saya sendiri masih belum banyak mengumpulkan string-string virus. Tapi yang jelas pada versi berikutnya, trik ini akan saya gunakan.

Teknik ini fungsinya untuk melihat ke dalam tubuh file. Yaitu untuk melihat string-string sensitif virus yang ada di dalam tubuh file.