BAB V

PENUTUP

5.1 Kesimpulan

Kesimpulan pokok mengenai Aplikasi Pertahanan Terhadap Serangan Malcode Dalam Sistem Operasi Microsoft Windows XP Profesional SP2 yang dapat diambil dari uraian penjelasan dan pembahasan pada bab sebelumnya antara lain:

1. Aplikasi antivirus memerlukan database atau signature malcode untuk mendeteksi nama malcode yang beredar untuk menjaringnya dan mengeksekusi malcode tersebut.
2. Malcode atau tepatnya suatu file memiliki karakter yang berbeda satu sama lainnya, agar bisa di baca oleh mesin atau computer, karakter ini yang disebut nilai HexaDecimal (*HexaDecimal value*), untuk mendapatkan nilainya aplikasi ini menggunakan standar M31 Pattern.
3. Pendeteksian suatu malcode tidak hanya dengan signature malcode berdasarkan HexaDecimalnya, karena jika suatu file yang terinfeksi yang diambil sampel maka kemungkinan salah deteksi besarnya 50-70%, oleh karena itu penanaman heuristik diberlakukan agar lebih akurat dalam menjaring malcode karena menggunakan string karakter malcode itu sendiri.
4. Penggunaan API (*Application Programming Interface*) dicanangkan untuk memudahkan kinerja antivirus itu sendiri dikraenakan API adalah

suatu kode rekomendasi langsung dari pembuat system operasi windows untuk menjelajahi, mengeksplorasi, dan memanipulasi system tersebut.

5. Proses pemindaian(*scanning*) didasarkan atas signature malcode dan heuristik, yaitu mendeteksi nilai HexaDecimal terlebih dahulu setelah cocok maka nama malcode akan ditampilakan, namun jika suatu file tidak ada kecocokan dengan signature maka heuristik diberlakukan disini untuk dicocokan string karakternya.
6. Hasil yang diberikan berupa nama malcode, alamat malcode tersebut berada, ukuran filenya, keterangan tambahan, dan proses eksekusi serta pembenahan segera dilakukan.

5.2 Saran

Aplikasi ini memang belum stabil dan memiliki banyak kekurangan, oleh karena itu dimungkin setelah menggunakan aplikasi ini hendaknya menggunakan antivirus lokal yang sudah memiliki kredibilitas tinggi antara lain PCMAV, CMC(Codenesia Malware Cleaner), SmadAV, MorphostAV dll. Berikut adalah saran yang harus diperhatikan jika suatu saat ada yang ingin mengembangkannya lagi.

1. NugAV ver Alpha 0 untuk menu pembenahan registry(*registry fixer*) sudah dapat melakukan pembenahan terhadap registry yang rusak, namun kondisinya belum stabil, sehingga harus di restart dahulu agar dapat melihat hasilnya.

2. NugAV ver Alpha 0 dalam proses pemindaian(*scanning*) belum dapat menembus file archiver(RAR, ZIP, RAX).
3. NugAV ver Alpha 0 dalam proses pemindaian(*scanning*) baru dapat menjelajahi subfolder hingga tahap 3, yaitu (folder→subfolder→ subfolder→....).
4. NugAV ver Alpha 0 belum dapat melakukan pemindaian sistem secara langsung, dan pemindaian dilakukan bertahap atau path-perpath.
5. Heuristik Conficker belum stabil, dalam artian belum menggunakan karakteristik string sensitif(*sensitivity string character*).
6. Struktur pengkodean(*coding*) belum tertata rapi alias meloncat-loncat letak fungsi-fungsinya.

Seluruh hal yang perlu diperhatikan untuk NugAV ver Alpha 0 saat akan dikembangankan ulang semuanya telah dijabarkan, oleh karena itu untuk adik-adik angkatanku hendaknya loyal dalam memberikan dan mengajarkan ilmumu, karena semakin banyak orang yang kau ajari maka semakin banyak pula ilmu baru yang kau dapatkan.

Hendaknya jangan disobek draft skripsi ini hargai karya saya dan hormati saudara yang lain yang ingin belajar.