PENGARUH KERUSAKAN PERANGKAT PENYIMPANAN HARDISK DAN FLASHDISK TERHADAP VIRUS KASPERSKY INTERNET SECURITY

Tri Yusnanto[1)], Moch Ali Machmudi[2)], Khoirul Mustofa[3)]
[1),2)]Manajemen Informatika STMIK Bina Patria
[3)] Universitas Duta Bangsa
Email : yusnanto@gmail.com[1)],aliadhinata@gmail.com[2)],Khoirul_Mustofa@gmail.com[3)]

Abstract

Security at this time is one very important thing an effort is made to protect organizational data or other personal files against threats such as tapping or misuse of third people or misuse that causes intentional or unintentional losses caused by computer viruses. To choose and use antivirus is very important, in this study try to find out the effect of damage to hardware and flashdisk storage devices on the Kesperskay Internet Security virus. In this research, the experiment is carried out and observations in the storage system both those affected by the virus and those that have not been affected by the virus. By trying to change some file formats that are affected by the virus. The results of the observations obtained that the hard drive is more immune than flasdisk because it must be formatted to be able to normalize the work of the flashdisk again.

Keywords *: Antivirus, Virus, Kaspersky Internet Security*

Abstrak

Kemanan pada saat ini merupakan satu hal yang sangat penting upaya yang dilakukan untuk melindungi data organisasi ataupun file pribadi lainya terhadap ancaman seperti penyadapan ataupun penyalah gunaan orang ketiga atau penyalahgunaan yang menyebabkan kerugian yang disengaja maupun tidak disengaja yang dikarenakan oleh virus komputer. Untuk memilih dan menggunakan antivirus sangatlah penting, Dalam penelitian ini mencoba mengetahui Pengaruh Kerusakan Perangkat penyinpanan Hardisk dan Flashdisk terhadap virus Kesperskay Internet Security. Dalam penelitian ini yang dilakukan adalah melakukan percobaan serta pengamatan didalam sistem penyimpanan baik yang terkena virus maupun yang belum terkena virus tersebut. Dengan mencoba mengubah beberapa format file yang terkena virus. Hasil dari pengamatan didapat bahwa hardisk lebih kebal dibandingkan dengan flasdisk karena harus di format untuk dapat menormalkan kembali kerja dari flashdisk tersebut.

Kata kunci : Antivirus, Virus, Kesperskay Internet Security

1. Pendahuluan

Di era sekarang ini dan sebuah keamanan menjadi perhatian utama bagi teknologi elektronik (Niranjanamurthy and Chahar 2013) agar tetap aman seiring meningkatnya penggunaan sistem komputer yang sealu di akses oleh berbagi user (Jang 2010). Maka Peningkatan kemanan adalah upaya yang dilakukan untuk melindungi data sebuah organisasi atupun data penting lainya terhadap ancaman seperti penghancuran atau penyalahgunaan yang dikarenakan oleh virus yang meyebabkan kerugian yang disengaja maupun tidak disengaja. Keamanan yang dianjurkan adalah menggunakan anti virus yang handal dan selau uptodate. Dengan pesatnya perkembangan teknologi jaringan, serangan melalui internet juga bermacam-macam, sehingga anti virus yang hanya di installl tanpa update sudah tidak bisa membendung adanya ancaman virus lagi pada saat ini.

Untuk memilih Anti virus yang terbaik pada saat ini adalah hal yang tidak susah karena banyak sekali anti virus yang di tawarkan oleh berbagi vendor pembuat anti virus , Dalam penelitian kami mencoba membandingkan antara pc yang dinstalll

dengan anti virus dengan yang belum dinstall antivirus baik yang berbayar maupun tidak dengan mengaplikasikan flasdisk yang sudah terkena virus. Virus adalah suatu program yang aktif dan menyebar dengan memodifikasi program atau file lain didalam memory baik memori komputer ataupaun penyimpanan external. Virus tidak bisa aktif dengan sendirinya, melainkan perlu dibantu pengaktifannya. Sekali diaktifkan, dia akan mereplikasi dirinya dan menyebar keseluruh memori yang ada didalam sistem yang berjalan. Meskipun sederhana, virus ini sangat berbahaya karena dapat dengan cepat menggunakan semua memori yang tersedia dan dapat berakibat fatal karena dapat membuat mesin komputer tak bisa berjalan sebagaimana mestinya atau bahkan dapat berjalan sendiri. Virus dibuat untuk menghapus atau merusak file tertentu, yang disebarluaskankan biasa melalui email, downolad file, media storage non permanen, alat penyimpan data lainya virus tersebut diselipkan kedalamnya,mungkin kita tidak trasa mengaktifkan sebuah virus yang berada didalm sebuah file yang sudah kita download. Virus pada mulanya diperkenalkan oleh Len Adleman pada November 1983 dalam sebuah seminar yang membahas tentang cara membuat virus serta memproteksi diri dari ancaman sebuah virus. Namun orang-orang sering menganggap bahwa virus yang pertama kali muncul adalah virus *Brain* yang justru lahir tahun 1986. Maka kebanyak orang-orang beranggapan seperti itu karena virus ini yang paling menggemparkan dan paling luas penyebarannya karena menjalar melalui disket DOS yang pada saat itu sedang popular. Virus ini juga lahir bersamaan dengan PC-Write Trojan dan *Vindent*. Setelah itu, virus mulai merambat dengan sangat cepat serta meluas dan perkembangannya sangat pesat. Berselang beberapa tahun muncul virus pertama yang menginfeksi file. Biasanya virus ini menyerang file yang berekstensi *.exe. Virus ini bernama *Suriv* . Virus ini termasuk dalam golongan virus 'jerussalem'. Kecepatan penyebaran virus ini sangatlah pesat. Virus ini menyerang mainframe dari IBM cukup lama, yaitu sekitar 1 tahun lamanya didalam proses penyeranganya tersebut.

Menurut (Hanif M. D , Ravie C. M,Iman T. A,, Abdolhossein S) 2014 definisi untuk varian malware ada berbagi macam jenisnya , dibawah ini merupakan jenis malware dari berbagai referensi.

a. Worm

Worm adalah program yang menyebar sendiri di Internetjaringan deengan menggunakan kelemahan atau kebijakan keamanan dalamlayanan korban. Dia dapat perbanyakan diri, worm bisa replikasi diri dan mandiri. Replikasi diri ini berarti bahwa ia menyalin dirinya sendiri dan mandiri artinya worm dieksekusi tanpa perlu menempel program lain. Worms dapat dideteksi dengan menggunakan perangkat lunak antimalware yang berisi definisi untuk worm. Worm yang paling penting, harus dihentikan penyebarannya. Untuk melakukan ini, administrator mungkin perlu mematikan sistem. Praktik terbaik untuk membersihkan worm dari sebuah sistem jaringan yaitu pertama-tama lepaskan komputer dari jaringan dan kemudian jalankan perangkat lunak keamanan ataupun anti virus untuk membersihkan Worm tersebut.

b. Virus

Virus adalah program yang menempel pada program lain untuk disebarkan. Program yang tempelkan oleh virus itu sendiri adalah program korban.

c. Botnet

Botnet adalah platform paralel yang berbahaya. Istilah botnet digunakan untuk mendefinisikan jaringan host jahat yang disebut bot dan dikendalikan oleh operator manusia bernama botmaster.

d. Spyware

Spyware adalah program perangkat lunak yang ditempatkan di mesin Internet korban dan tanpa informasi dan izin pengguna mengirimkan informasi pribadi pengguna ke pihak ketiga yang berupa, katasadi, dokumen penting dan lain sebagainya.

e. Trojan Horse

Trojan horse: Ini adalah program perangkat lunak yang melakukan tindakan yang tidak diinginkan atau tidak dikenal pada korban saat itu dikenal sebagai program yang sah. Trojan horse adalah virus yang tidak mereplikasi. Trojan adalah program jahat yang menyamar sebagai sesuatu yang tidak berbahaya. Dalam banyak kasus, Trojan muncul untuk melakukan fungsi yang diinginkan untuk pengguna tetapi sebenarnya memungkinkan akses hacker ke sistem komputer pengguna. Trojan juga dapat digunakan sebagai titik peluncuran untuk serangan lain, seperti distributed denial of service (DDoS). Banyak Trojan digunakan untuk memanipulasi file di komputer korban, mengelola proses, menjalankan perintah dari jarak jauh, mencegat penekanan tombol, menonton gambar layar, dan memulai kembali atau mematikan host yang terinfeksi. Trojan canggih dapat menghubungkan diri mereka ke pencetusnya atau mengumumkan infeksi Trojan pada saluran Internet Relay Chat (IRC).

f. Rootkit

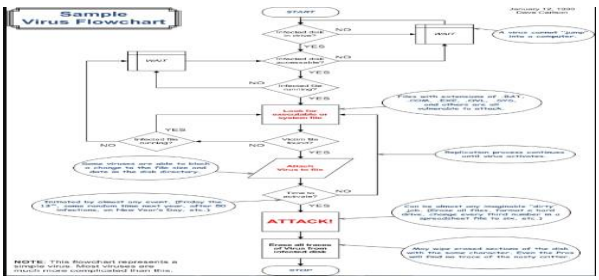
Rootkit adalah program yang dirancang untuk menyembunyikan proses, file, dan aktivitas penyerang dari sistem operasi dan pengguna yang sah guna mengakses sistem. Rootkit dapat memasang handler yang dapat menghilangka catatan audit dan catatan lain dari siatem pendeteksi virus rootkit

g. Backdoor

Backdoor adalah program perangkat lunak yang diinstal oleh penyerang pada sistem yang dikenali untuk memfasilitasi akses lebih lanjut yang tidak sah dari penyerang pada sistem tersebut untuk kepentingan penyerang. Backdoor dapat disematkan dalam Trojan jahat. Tujuan menginstal backdoor pada suatu sistem adalah untuk memberikan akses hacker ke dalam sistem pada saat yang mereka pilih. Kuncinya adalah bahwa peretas tahu cara masuk ke pintu belakang tanpa terdeteksi dan dapat menggunakannya untuk meretas sistem lebih jauh dan mencari informasi penting.

h. Remote Access Trojans (RATs)

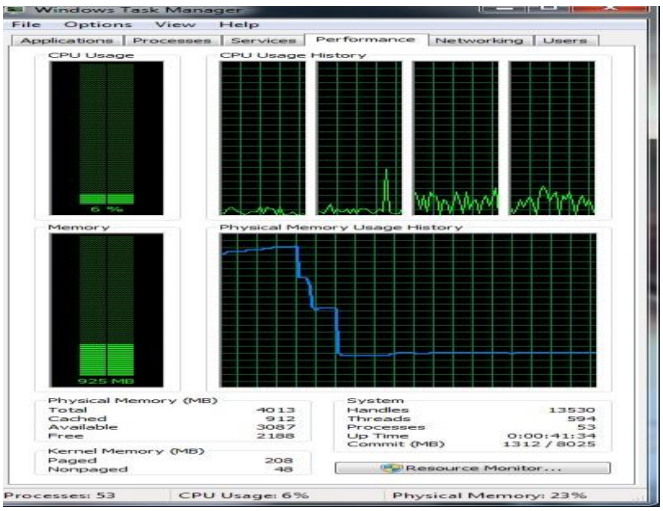
Remote Access Trojans (RATs) adalah kelas pintu belakang yang digunakan untuk memungkinkan remote control melalui mesin yang dikompromikan. Mereka memberikan fungsi yang tampaknya bermanfaat bagi pengguna dan, pada saat yang sama, membuka port jaringan pada komputer korban. Setelah RAT dimulai, ia berperilaku sebagai file yang dapat dieksekusi, berinteraksi dengan kunci Registry tertentu yang bertanggung jawab untuk memulai proses dan terkadang membuat layanan sistemnya sendiri. Tidak seperti pintu belakang biasa, RAT menghubungkan diri mereka ke sistem operasi korban dan selalu dikemas dengan dua file: file klien dan file server. Server diinstal di mesin yang terinfeksi, dan klien digunakan oleh penyusup untuk mengontrol sistem yang dikendalikannya



Gambar 1. *Alur penyebaran virus (Dave Carlson - January 12, 1990)*

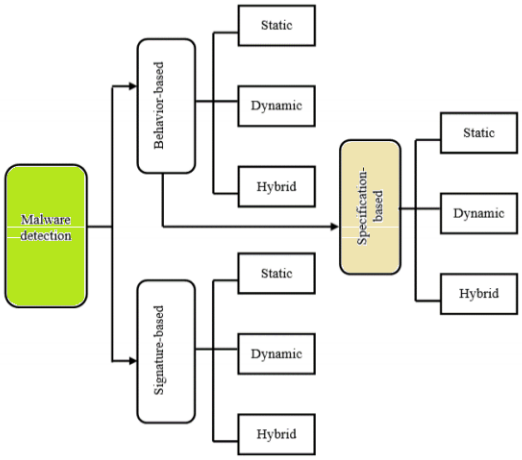
Flowchart diatas merupakan contoh dari logika yang ada di dalam program virus komputer. Diatas merupakan alur virus yang sangat sederhana. Sebagian besar virus jauh lebih rumit dari pada ini. Virus komputer dapat berjalan pada semua keadaan yang bisa tidak dibayangkan karena mereka dapat menghapus semuafile penting pada email kita, menghapus semua file pada hard drive, mengubah setiap angka di semua file spreadsheet dan lain sebagainya.

Teknik deteksi berbasis perilaku berfokus pada analisa dengan perilaku yang diketahui dan dicurigai ataupun kode berbahaya. Perilaku seperti itu meliputi faktor-faktor seperti sumber dan alamat tujuan malware, di mana mereka menyematkan dan anomali statistik dalam sistem yang terinfeksi malware semisalkan pada task manager.
(Goertzel, 2009)



Gambar 2. Task manager Untuk Mengecek Pengunaan CPU.

Bo Y, Ying F, Qiang Y, Yong T, Liu L (w2017).Analisis perilaku malware adalah salah satu cara yang paling banyak dilakukan dalam mengetahui malware yang akan mengancam didalam dunia maya. Meski banyak penelitian telah dilakukan untuk menganalisis perilaku malware,dan juga lebih banyak upaya masih dilakukan untuk memahami mekanisme,tren dalam perilaku malware itu sendiri.



Gambar 3. Ecosystem of malware detection Khalid M. A.Y .A(2012)

Deteksi berbasis anomali merupankan suatu cara dengan memanfaatkan informasi dasar untuk menentukan keberadaan yang normal suatu perilaku untuk memutuskan kekuatan malware di didalam penyelidikan. Bentuk lain dari berbasis anomali:

1. Deteksi Berbasis Spesifikasi
Untuk menangani insiden pendektesian palsu yang terjadi dengan banyak prosedur yaitu deteksi berbasis anomali, deteksi berbasis spesifikasi, yang mirip dengan Unit berbasis anomali. Karena kenyataan itu deteksi berbasis spesifikasi berasal dari deteksi berbasis anomal digunakan untuk memperkirakan persyaratan dalam suatu sistem. Apalagi di deteksi berbasis spesifikasi situasi, menentukan atau memperkirakan semua hasil bahwa setiap perilaku suatu program dapat menunjukkan sistem tertentu sedang dijaga atau di bawah penyelidikan. Kelemahan utama dari deteksi berbasis spesifikasi adalah tidak mudah didalam memprediksi semua hasil yang dapat diterima sepenuhnya oleh sistem.

2.Signature-Based Detection
Memanfaatkan kepribadian berbasis teknologi untuk membedakan malware dan akibatnya dalam mengkonfirmasi sifat jahat sebuah program yang sedang diselidiki. Dengan kata lain, deteksi berbasis tanda tangan mencoba membuat *benchmark* menggunakan malware dan selanjutnya menggunakan ini sebagai referensi untuk mendeteksi malware lain didalam perangkat lunak.Dalam mengelompokkan semua model ini, deteksi menghasilkan database untuk dirinya sendiri. Secara sempurna sistem, sangat penting yang dapat mengenali setiap program yang dimanifestasikan dengan menyesuaikanan perilaku basis data yang berbahaya. Database ini berisi semua informasi yang dibutuhkan untu kmendeteksi perangkat lunak berbahaya.

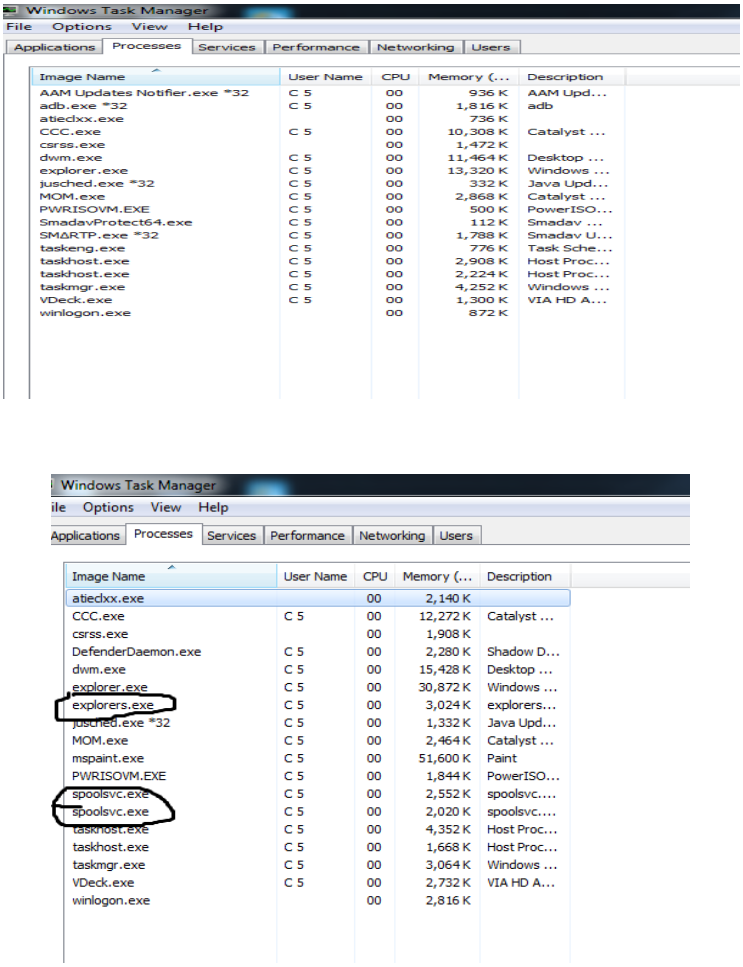
Namun, semua deteksi diatas dapat dijalankan dengan menggunakan prosedur satu dari tiga variasi
metodologi.
1). Statis: Seperti dalam bahasa, analisis statis menggunakan struktur atau format pemrograman ke mengungkap malware yang sedang diselidiki. Umumnya, metodologi statis berusaha mengungkapmalware sebelum program dalam penyelidikan sedang dilaksanakan.
2). Dinamis: Selama pra atau pasca program malware implementasi dapat dideteksi dengan memanfaatkanmetodologi yang dinamis.
3). Hibrid: Tersedia prosedur hibridmenggabungkan dua metodologi, yang berarti keduanyadatabase statis dan dinamis digunakan untuk mengungkap perangkat lunak berbahaya

2. Metode Penelitian

Jenis penelitian ini adalah eksperimental didalam penelitian ini yang dilakukan adalah melakukan pengamatan serta membandingkan antara hardisk dan flashdisk yang belum terkena virus serta yang terkena virus. Dengan dengan membuka file serta mengubah ataupun merename file yang terinfeksi oleh virus kayspersky internet security. Untuk pcnya kita lihat didalam local disk atau program file sedangkan pada flashdisk kita lihat pada tampilan awalnya dan folder yang ada didalamnya. Komputer yang dipakai untuk program ini menggunakan komputer dengan spesifikasi *Intel Pentium core i5 2320 Processor* 3.00 GHz, RAM 4 GB, dan AMD *Radeon* HD 5500 *memory size* 2048 MB serta flash disk 4GB kingstone

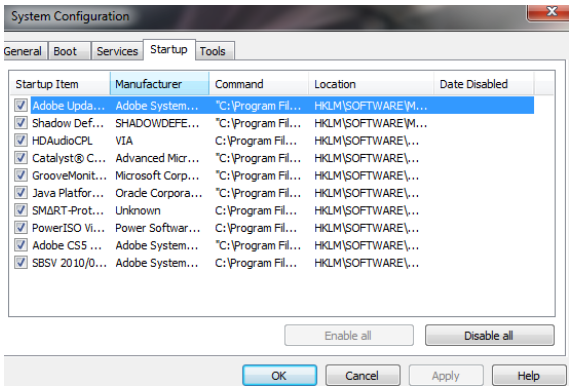
3. Hasil dan Pembahasan

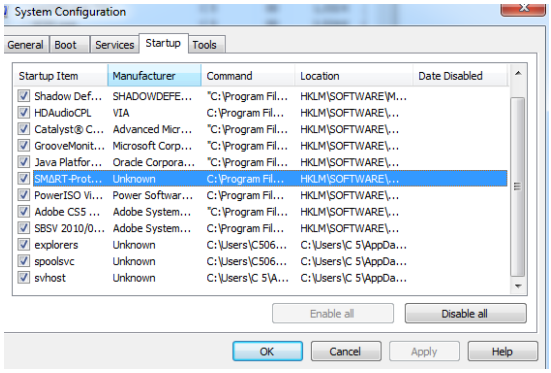
Setelah melakukan ujicoba dalam beberapa kali perubahan file baik hardisk ataupun flashdisk dengan anti virus maupun yang yang belum ada anti virusnya.



Gambar 4. *Gambar task manager*

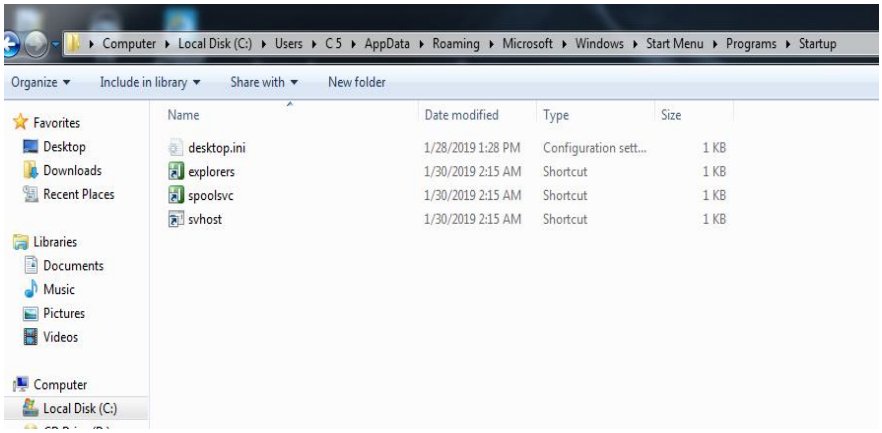
Pada gambar 3 diatas merupakan gambar pc yang belum ada virus kaspersky internet security dan sesudah terkena virus tersebut





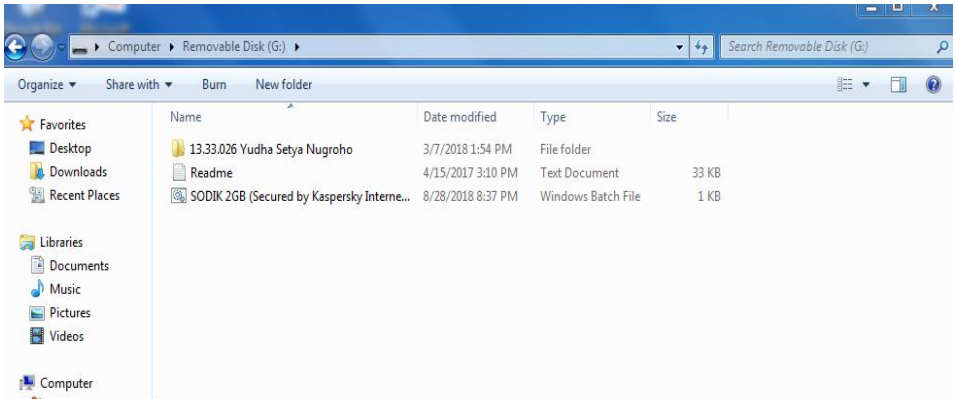
Gambar 5. *Gambar System Konfigurasi*

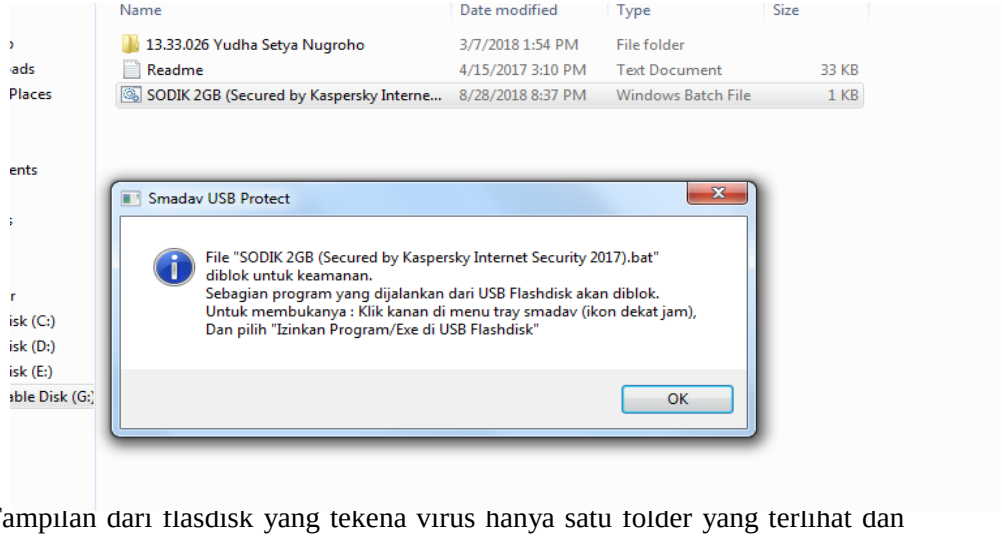
Pada Gambar 4 system Konfigurasi yang belum dan sesudah terkena virus kaspersky internet security



Gambar 6. *Didalam Folder startup localdisck C:/*

Pada Gambar 5 didalam Local disk C pada folder startup terdapat shorcut dari virus yang masuk yaitu ada spoolsvc ,explorers dan svhost.





Gambar.7 Tampilan dari flasdisk yang tekena virus hanya satu folder yang terlihat dan folder lainya di sembunyikan .

Pada gamabar diatas menunjukan pada saat akan membuka dengan di klik ada tampilan bahwa flashdisk akan di blok oleh anti virus yang meminta klik kanan dan mengizinkan program atau exe di flasdik dijalankan maka baru bisa tampil seluruh folder yang ada didalam flasdisk tersebut.

Tabel 1. *Perbandingan file hardisk dan flashdisk yang terinfeksi*

File atau folder	Hardisk	Flashdisk
.exe	bisa diedit, renama dan disimpan	File bisa diedit akan tetapi tidak bisa di rename sehabis derename akan hilang file tersebut
.word	bisa diedit, renama dan disimpan	File bisa diedit akan tetapi tidak bisa di rename sehabis derename akan hilang file tersebut
.xls	bisa diedit, renama dan disimpan	File bisa diedit akan tetapi tidak bisa di rename sehabis derename akan hilang file tersebut
.rtf	bisa diedit, renama dan disimpan	File bisa diedit akan tetapi tidak bisa di rename sehabis derename akan hilang file tersebut
.ppt	bisa diedit, renama dan disimpan	File bisa diedit akan tetapi tidak bisa di rename sehabis derename akan hilang file tersebut
.jpeg	bisa diedit, renama dan disimpan	File bisa diedit akan tetapi tidak bisa di rename sehabis derename akan hilang file tersebut
.png	bisa diedit, renama dan disimpan	File bisa diedit akan tetapi tidak bisa di rename sehabis derename akan hilang file tersebut

Pada tebel 1 diatas terlihat bahwa semua file yang berada di hardisk masih bisa diedit didelete dan juga bias di rename sedangkan pada flashdisk semua file tidak bisa didelete ataupun di rename walaupun sudah ada anti virusnya pada saat di rename bisa akan tetapi file akan hilang walaupun kalau folder dari file tersebut ditutup kemudian dibuka kembali filtadi yang hilang akan kembali seperti semula.

4. Kesimpulan

Dengan adanya anti virus yang selalu terupdate maka paling tidak meminimalisir terjadinya virus baru karena sudah ada didalam daftar data antivirus tetapi lebih baik kita membeli antivirus karena lebih komplit dibandingkan dengan yang free, serta kita diharapkan sesering mungkin melalukan backup data karena apabila ada fileyang rusak pada saat kena virus paling tidak kita sudah mempunyai file cadangannya. Caralain untuk Sistem Operasi Windows, yaitu dengan klik Start>Run… Ketik gpedit.msc dan tekan Enter/OK.Masuk ke bagian Administrative Templates>System (ada dua, yang satu Computer Configuration,yang satu User Configuration). Cari bagian Turn off Autoplay dan klik 2 kali.Pilih Enable dan All drive ini merupakan cara pencegahan yang bersifat basic saja karena virus bias saja lewan jaringan internet.

Daftar Pustaka

Ajit N, Yi C, Shaoning P, and Ban T. 2013. The Effects of Different Representations on Static Structure Analysis of Computer Malware Signatures. 26 February /2013/671096

Anjik Sukmaaji, S.Kom, Rianto, S,Kom, 2008, Jaringan Komputer (Konsep Dasar Pengembangan Jaringan dan Keamanan Jaringan), Andi , Yogyakarta

Aat Shadewa, 2006. Rahasia Membuat Antivirus Menggunakan Visual Basic. Yogyakarta : DSI Publishing.

Amperiyanto, Tri, 2003. Bermain-main dengan Virus Macro 2 : Menjelajah Word dan Excel. PT Elex Media Komputindo, Kelompok Gramedia, Jakarta.

Bo Y, Ying F, Qiang Y, Yong T, Liu L (2017). A survey of malware behavior description and analysis. Yu et al. / Front Inform Technol Electron Eng 2018 19(5):583-603

Dave Carlson - January 12, 1990. http://www.dynotech.com/articles/virusflowchart.shtml' Sample Virus Flowchart ' di akses tanggal 6 Januari 2019

Goertzel, K.M., 2009. Tools on Anti Malware. Technical Information Center.

Hartini. 2006. Analisis Dengan Diagram Aliran Data (DFD). Materi Kuliah, Ilmu Komputer, Universitas Sriwijaya.

Hossain, Monjur Ahmed and Mohammad Ashraf. 2014. ―Cloud Computing S Ecurity in Business.‖ *International Journal of Network Security and Its Applications* 6(1): 25–36.

Jang, Seung-ju. 2010. ―Developing File Security for Windows Operation System.‖ 10(5): 36–39.

Leo Hendrawan. 2004. Virus Komputer : Sejarah Dan Perkembangannya.

Marko Helenius. 2002. A System to Support the Analysis of Antivirus Products' VirusDetection Capabilitie

Martin Karresand, Seperating Trojan hourses, viruses, and worms – A proposed taxonomy of software weapons, IEEE workshop on information assurance, 2003.

Niranjanamurthy, M., and Dharmendra Chahar. 2013. ―The Study of E-Commerce Security Issues and Solutions.‖ International Journal of Advanced Research in Computer and Communication Engineering 2(7): 2885–95

Naqqash A, Yasir S, Fahim H. A, Farrukh S. 2017. A Hybrid Approach For Malware Family Classification

Tala T , Seyed H. S . 2008.- Malware fuzzy ontology for semantic web IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.7, July