ANALISIS MODIFIKASI KONFIGURASI ACCESS CONTROL LIST PADA USB FLASH DISK STUDI KASUS PADA PENYEBARAN MALWARE TROJAN SHORTCUT

Nugroho Budhisantosa
Fakultas Ilmu Komputer Universitas Esa Unggul
Jalan Arjuna Utara no. 9, Kebun Jeruk, Jakarta 11510
nugroho.budhisantosa@esaunggul.ac.id

Abstract

This research is conducted to find a solution to prevent the spreading the Shortcut Trojan malware using the Access Control List modification method which is applied on USB Flash Disk (UFD) external storage. Shortcut Trojan infects UFD by injecting AutoRun.inf and AntiSys.exe files in the root directory of UFD which is connected to infected computers. Once the infected UFD is connected to another unprotected host, the AutoRun.inf file in UFD will be run automatically executed its AntiSys.exe file in the victim host and the Trojan's payload will compromise the host. The simply method to prevent Trojan malware which is inject AutoRun.inf file to UFD root directory is to protect the UFD root directory against the writing activities, as a consequence some sub-folder should be created under the root directory with no restriction so that the UFD still can be use properly. Access Control List (ACL) is a security policy feature provide by Microsoft Windows Operating System which is allow users to protect folder using a series of permission configuration. Applying ACL policy on UFD is implemented in this research where two UFD with ACL modification and with factory standard is compared its behavior against Shortcut Trojan infection.The result of this research shown that the Access Control List modification method on UFD effectively performed its functions in order to prevent the spreading of Shortcut Trojan where the Shortcut Trojan has lost its ability to infect the UFD which was modified on its ACL

Keywords:

Abstrak

Penelitian ini bertujuan untuk menemukan suatu cara pencegahan penyebaran *malware* trojan Shortcut melalui pengontrolan *Access Control List* (ACL) pada media penyimpanan eksternal berupa *USB Flash Disk* (UFD). Trojan shortcut menginfeksi UFD dengan cara menginjeksi file *AutoRun.inf* dan *AntiSys.exe* pada *root directory* UFD yang terhubung dengan computer yang terinfeksi. Ketika UFD yang terinfeski terhubuhng dengan komputer yang tidak terlindungi, file *AutoRun.inf* akan berjalan mengeksekusi file *AntiSys.exe* nya pada komputer korban dan muatan Trojan akan menguasai komputer tersebut. Cara sederhana untuk mencegah penyebaran malware Trojan yang menginjeksi file *AutoRun.inf* pada *root directory* adalah dengan melindungi *root directory* UFD dari upaya aktivitas penulisan, sebagai konsekuensinya beberapa *sub-folder* tanpa pembatasan perlu dibuat di bawah *root directory* sehingga UFD tersebut dapat tetap digunakan selayaknya. *Access Control List* (ACL) adalah fitur keamanan Sistem Operasi Microsoft Windows yang memungkinkan pengguna untuk melindungi *folder* dengan serangkaian konfigurasi perijinan. Mengaplikasikan aturan ACL pada UFD diimplementasikan pada penelitian ini dimana dua UFD dengan modifikasi ACL dan dengan kondisi standar dibandingkan perilakunya terhadap infeksi Trojan Shortcut. Hasil penelitian menunjukkan bahwa metode modifikasi ACL pada UFD secara efektif dapat mencegah penyebaran *malware* trojan Shortcut, dimana Trojan Shortcut tidak lagi memiliki kemampuan untuk menginfeksi UFD dengan ACL yang telah dikontrol pengkasessannya

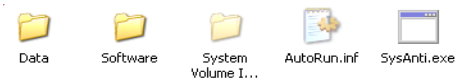
Kata kunci: *root directory*, mencegah penyebaran, *access control list*

Pendahuluan

Pola penyebaran *malware* seperti virus dan trojan komputer dalam 7 tahun belakangan ini tampaknya tidak banyak mengalami perubahan yaitu melalui media penyimpanan eksternal seperti *USB Flash Disk* yang terkoneksi dengan komputer yang memiliki akses bersama.
Melalui komputer publik yang terinfeksi *malware* inilah, dengan ketidak tahuan pengguna, *malware* menyebar dengan cepatnya bukan saja kebanyak komputer personal tetapi juga menyebar ke dalam suatu jaringan komputer.

Berbeda dengan Trojan Brontox, Trojan shorcut, adalah salah satu *malware* yang penyebarannya sampai saat ini tampaknya masih sulit untuk dicegah di dalam sistem operasi Microsoft Windows.Trojan Shortcut ditemukan pertama kali keberadaannya pada tahun 2011, namun hingga kuartal pertama tahun 2014, keberadaan *malware* ini masih cukup dapat mudah ditemui pada banyak komputer dan media penyimpanan eksternal.

Melihat kemampuan trojan Shortcut dalam bertahan dalam tenggang waktu yang cukup lama, maka peneliti melakukan penelitian pada teknik penyebaran *malware* ini guna mencari cara paling efektif untuk menghentikan penyebarannya.



Gambar 1
File Induk Trojan Shortcut – SysAnti.exe

Tujuan dan Manfaat

1. Mempelajari cara penularan malware trojan Shortcut
2. Mempelajari modifikasi ACL *USB Flash Disk* terhadap perilaku penyebaran infeksi *malware* pada *USB Flash Disk*
3. Menentukan cara melindungi sistem komputer atas penyebaran *malware* trojan Shortcut melalui media *USB Flash Disk*
4. Memberikan referensi pada pihak-pihak yang ingin mempelajari teknik penginfeksian *malware*

Malware

Malware di dalam Ensiklopedia Britanica didefinisikan sebagai ,semua perangkat lunak jahat, program komputer jahat, atau perangkat lunak jahat, seperti virus (komputer), trojans, spyware, dan worm.

Virus komputer bekerja dengan cara menempel pada suatu file komputer yang biasanya berupa file executable, trojan bekerja dengan cara melakukan social engineering pengkamuflasean file-file berbahaya dengan menampilkannya seperti file-file yang terlihat tidak berbahaya, spyware adalah perangkat lunak yang disisipi kode untuk mendapatkan informasi penting dari pengguna seperti akun bank, password, dan informasi lainnya yang diinginkan oleh pembuatnya, sedangkan worm adalah perangkat lunak jahat yang dibuat dengan memanfaatkan celah lubang keamanan pada sistem operasi untuk tujuan tertentu.

File AutoRun.inf

File *AutoRun.inf*adalah file teks di dalam sistem operasi Microsoft Windows yang dapat digunakan komponen *AutoRun*dan*AutoPlay*dari sistem operasi tersebut untuk di eksekusi secara otomatis jika file *AutoRun.inf* tersebut diletakkan pada direktori utama.

File *AutoRun.inf* pertama kali diperkenalkan oleh Microsoft pada produk sistem opeasi Microsoft Windows 95 yang memungkinkan CD-ROM untuk secara otomatis menjalankan suatu progam untuk proses instalasinya.

Ke depan file *AutoRun.inf* bukan saja dapat diletakkan di dalam CD-ROM untuk secara otomatis menjalankan program, tetapi dapat juga diletakkan pada perangkat penyimpanan internal seperti hardisk dan perangkat penyimpanan eksternal seperti USB Flash Disk, Micro-SD, dan lainnya. Kondisi seperti ini menyebabkan file *AutoRun.inf* juga sering digunakan oleh programmer pembuat *malware* untuk menjalankan program jahatnya secara otomatis melalui file *AutoRun.inf* yang didalamnya telah disisipkan kode pemanggilan file induk program.

Sitem file NTFS

Sitem file NTFS (*New Technology File System*) adalah sistem file yang dikembangkan oleh Microsoft dimana versi awalnya diperkenalkan kepada public tahun 1993 melalui sistem operasi Windows 3.1.

Berbeda dari sistem file produk Microsoft sebelumnya yaitu sistem FAT 32. Sistem file NTFS v3.0 seperti yang sekarang digunakan pada penelitian ini telah memiliki fitur keamanan*access control lists (ACL)*.

Menggunakan fitur ACL, hak akses membaca (*Read*), Menulis (*Write*), menghapus (*Delete*), Memodifikasi (*Modify*) suatu file untuk setiap pengguna dapat dikonfigurasi sesuai kebutuhannya.

Metodologi

Selain dilakukannya studi pustaka, pada penelitian ini, analisa perilaku cara penginfeksian malware pada *USB Flash Disk*akan diamati secara langsung dan juga melakukan pengamatan pada *USB Flash Disk* yang telah dilakukan modifikasi ACL dan yang tidak dilakukan modifikasi ACL atasnya.

Penelitian menggunakan 2 (dua) buah *USB Flash Disk* dengan kapasitas 8GB dimana *USB Flash Disk* pertama akan difungsikan sebagai *USB Flash Disk* kontrol yaitu *USB Flash Disk* tanpa perlakuan modifikasi ACL dan *USB Flash Disk* kedua sebagai*USB Flash Disk* H1 yang telah mendapat perlakuan modifikasi ACL.

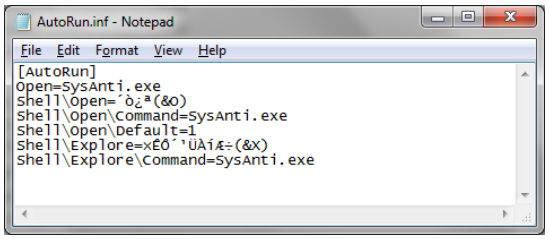
Pengamatan dilakukan pada *USB Flash Disk* kontrol dan *USB Flash Disk* H1 setelah keduanya dihubungkan pada komputer yang telah diinfeksikan *malware* trojan Shortcut.

Hasil dan Pembahasan

Mekanisme Penginfeksian Trojan Shortcut

Trojan Shortcut adalah *malware* yang memanfaatkan metode klasik penginjeksian *script* di dalam file *AutoRun.inf* kedalam direktori utama dari *USB Flash Disk*beserta file-file pendukung lainnya.

File *AutoRun.inf* dari trojan Shortcut terdiri dari serangkaian baris koding dimana baris-baris koding tersebut secaraspesifik digunakan untuk menjalankanfile *SysAnti.exe* yang merupakan file induk *malware* secara otomatis dengan beberapa cara.



Gambar 2
Isi File AutoRun.inf

```
[AutoRun]
Open=SysAnti.exe
Shell\Open=´ò¿ª(&O)
Shell\Open\Command=SysAnti.exe
Shell\Open\Default=1
Shell\Explore=×ÊÔ´¹ÜÀíÆ÷(&X)
Shell\Explore\Command=SysAnti.exe
```

Baris koding dari file *AutoRun.infmalware*trojan shortcut di atas dapat digunakan untuk menjalankan file *SysAnti.exe* dengan menggunakan *key* ***Open*** dan ***Shell***.

key ***Open=SysAnti.exe*** adalah perintah untuk secara otomatis menjalankan file *SysAnti.exe* yang terletak pada direktori utama/*root directoryUSB Flash Disk* (lihat Gambar 1) dimana file *AutoRun.inf* juga diletakkan.

Penggunaan *Key* ***Shell*** didalam file *AutoRun.inf* ditujukan untuk menampilkan *shortcut* ketika klik kanan dilakukan pada drive yang bersangkutan.

*key****Shell\Open\Command=SysAnti.exe*** adalah perintah untuk menjalankan file *SysAnti.exe* ketika klik kanan pada tetikus (*mouse*) dilakukan pada drive *USB Flash Disk*

SysAnti.exe

Seperti telah disebutkan di atas, file *SysAnti.exe* adalah file induk trojan shortcut yang berisi *malware payload* yang disamarkan keberadaannya dengan menggunakan teknik attribute hiding.

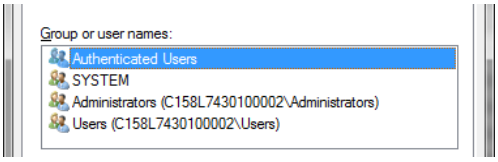
Trojan Shortcut akan menyembunyikan semua file dan folder dengan menggunakan nama drive dari komputer dengan tampilan shortcut. Jika shortcut tersebut di eksekusi melalui dua kali klik maka semua folder dan file yang disembunyikan akan ditampilkan, namun pada saat yang bersamaan payload dari malware juga akan ikut diaktifkan.

Melihat cara kerja penginfeksian klasik seperti ini, maka tindakan pencegahan penulisan pada direktori utama dapat dicoba dilakukan untuk mencegah Trojan Shortcut melakukan penulisan file *AutoRun.inf*dan file *AntiSys.exe* atas direktori utama tersebut.

Modifikasi ACL Format NTFS Pada USB Flash Disk

Tujuan utama dari perlakuan modifikasi ACL pada *USB Flash Disk*adalah melakukan pencegahan penulisan file pada *USB Flash Disk* khususnya pada direktori utama *USB Flash Disk* oleh pengguna komputer.Hal ini dilakukan karena komputer yang telah terinfeksi *malware*trojan Shortcut akan menjalankan proses untuk melakukan penulisan file *AutoRun.inf*, AntiSys, dan shortcut pada direktori utama dari *USB Flash Disk*.Modifikasi ACL secara efektif akan mengatur ijin akses *Read*, *Write*, *Delete*, dan *Modify* dari pengguna komputer.

Pada kondisi standar, sistem operasi Microsoft Windows 7 mendefinisikan 4 grup atau pengguna komputer yaitu *Authenticated Users*, *SYSTEM*, *Administrators*, dan *Users*



Gambar 3
Grup atau Pengguna pada sistem operasi Microsoft Windows 7

- *Authenticated Users* adalah kelompok dari pengguna komputer yang melakukan *logged in*ke sistem komputer dengan menggunakan *username*dan *password*.

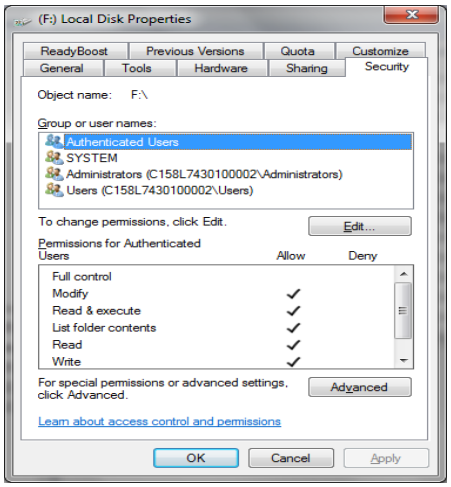
- *SYSTEM*merujuk padaproses-proses sistem operasi yang dikenali sebagai bagian dari pengguna
- *Administrators* adalah kelompok dari pengguna komputer yang memiliki hak untuk melakukan aktivitas administrasi pada sistem komputer
- *Users* merujuk pada semua pengguna komputer baik itu penggunan yang melakukan *logged in*kedalam komputer dengan menggunakan password juga yang non-passwordseperti Guest dan LOCAL_SERVICE.

Secara default *USB Flash Disk* yang tersedia di pasaran saat ini dijual dengan menggunakan format file FAT32 dimana modifikasi ACL pada media penyimpanan dengan format ini tidaklah dapat dilakukan. Untuk dapat melakukan modifikasi ACL pada *USB Flash Disk*, maka pada *USB Flash Disk* perlu dilakukan pemformatan menggunakan format file NTFS yang dapat dilakukan secara manual maupun dengan bantuan perangkat lunak pihak ke tiga.

Melihat bahwa rekayasa modifikasi ACL yang akan dilakukan pada *USB Flash Disk* pada dasarnya adalah rekayasa penguncian direktori utama dari*USB Flash Disk*terhadap segala bentuk penulisan file seperti file *AutoRun.inf* dan file-file induk *malware* maka pada*USB Flash Disk* perlu disiapkan sejumlah sub-folder yang pada sub folder tersebut tidakdilakukan rekayasa modifikasi ACLagar pengguna dapat melakukan penulisan file di dalamnya.Pada penelitian ini, peneliti menyiapkan 2 sub-folder yaitu sub-folder Data dan Sub-folder Program untuk lokasi penyimpanan file.

Untuk mempelajari perilaku *malware* trojan Shortcut, peneliti menyiapkan 2 *USB Flash Disk*dengan tipe dan merek yang sama dimana 1 *USB Flash Disk* yang telah diformat menggunakan format file FAT32 sebagai *USB Flash Disk*kontrol dan 1 *USB Flash Disk*H1 yang diformat menggunakan format file NTFS dengan cara berikut:

1. Login ke dalam komputer yang menggunakan sistem operasi Windows 7 dengan menggunakan akun Administrator atau setara
2. Biarkan 1 (satu) *USB Flash Disk*sebagai *USB Flash Disk* kontrol pada kondisi aslinya setelah di dalamnya dibuat folder Data dan Software
3. Hubungkan *USB Flash Disk* H1 dengan komputer
4. Format *USB Flash Disk* H1 menggunakan sistem file NTFS
5. Buat folder Data dan Software di dalam *USB Flash Disk*
6. Lakukan modifikasi ACL *USB Flash Disk* H1 dengan melakukan klik kanan pada mouse dan memilih tab Security

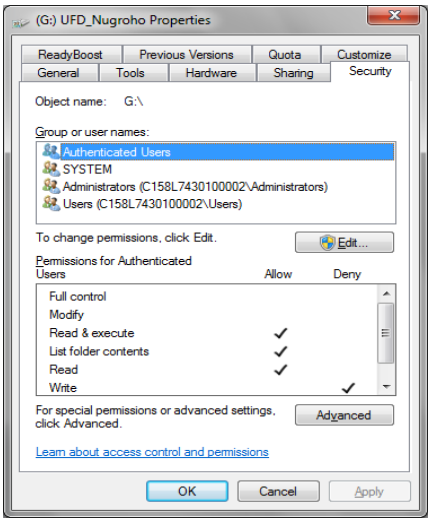


Gambar 4
Tab Security

7. Lakukan modifikasi ACL. Modifikasi ACL pada *USB Flash Disk* H1 sepertipada tabel di bawah:
   - Pengaturan ACL untuk *Authenticated Users* – Modifikasi ini dilakukan untuk mencegah semua *Authenticated Users* melakukan penulisan pada direktori utama*USB Flash Disk* H1

Tabel 1
Konfigurasi ACL *Authenticated Users*

ACL	UFD Kontrol		UFD H1	
	Allow	Deny	Allow	Deny
Full Control				
Modify	√			
Read & Execute	√		√	
List Folder Content	√		√	
Read	√		√	
Write	√			√
Special Permission				

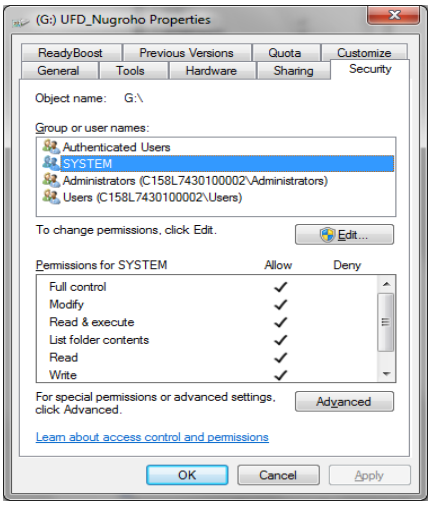


Gambar 5
Konfigurasi ACL pada Authenticated Users dari UFD H1

   - Pengaturan ACL untuk*SYSTEM*– Modifikasi ini dilakukan untuk mengijinkan SYSTEM melakukan penulisan pada direktori utama*USB Flash Disk* H1

Tabel 2
Konfigurasi ACL *System*

ACL	UFD Kontrol		UFD H1	
	Allow	Deny	Allow	Deny
Full Control	√		√	
Modify	√		√	
Read & Execute	√		√	
List Folder Content	√		√	
Read	√		√	
Write	√		√	
Special Permission				

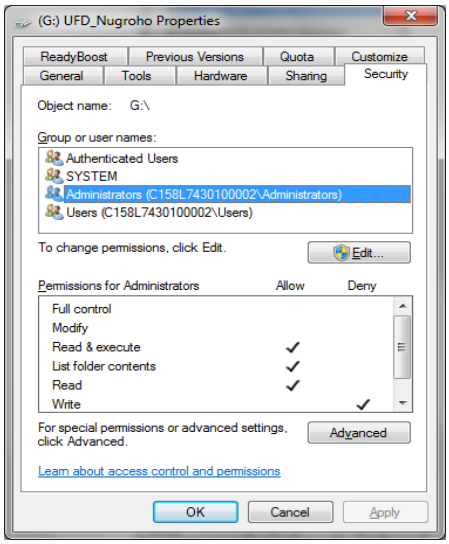


Gambar 6
Konfigurasi ACL pada SYSTEM dari UFD H1

- Pengaturan ACL untuk*Administrator*– Modifikasi ini dilakukan untuk mencegah semua *Administrators* melakukan penulisan pada direktori utama*USB Flash Disk* H1

Tabel 3
Konfigurasi ACL *Administrator*

ACL	UFD Kontrol		UFD H1	
	Allow	Deny	Allow	Deny
Full Control				
Modify	√			
Read & Execute	√		√	
List Folder Content	√		√	
Read	√		√	
Write	√			√
Special Permission				

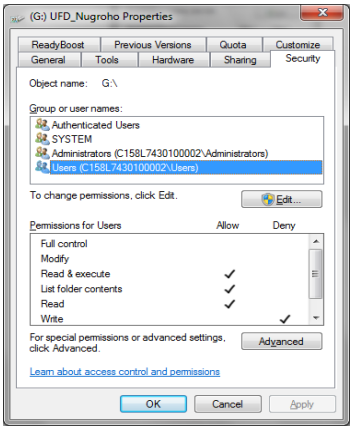


Gambar 7
Konfigurasi ACL pada Administrators dari UFD H1

- Pengaturan ACL untuk *Users*– Modifikasi ini dilakukan untuk mencegah semua *Users* melakukan penulisan pada direktori utama *USB Flash Disk* H1

Tabel 4
Konfigurasi ACL *Users*

ACL	UFD Kontrol		UFD H1	
	Allow	Deny	Allow	Deny
Full Control				
Modify	√			
Read & Execute	√		√	
List Folder Content	√		√	
Read	√		√	
Write	√			√
Special Permission				



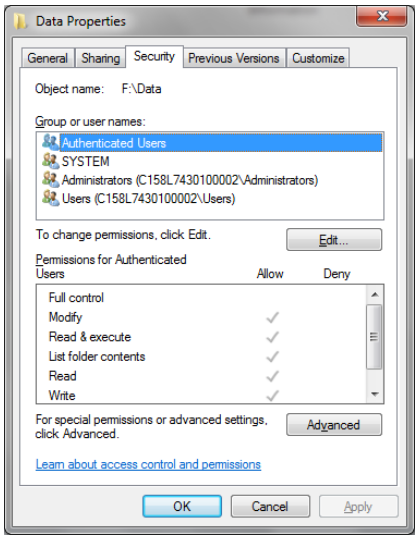
Gambar 8
Konfigurasi ACL pada Users dari UFD H1

8. Langkah modifikasi ACL di atas akan membuat seluruh isi *USB Flash Disk* tidak dapat digunakan untuk penyimpanan file. Untuk menjadikan folder Data dan Software yang ada didalamnya agar dapat digunakan untuk menyimpan file, maka modifikasi ACL pada kedua folder tersebut perlu dilakukan sesuaidengankondisi defaultnya seperti pada table dibawah:

- Pengaturan ACL untuk *Authenticated Users*

Tabel 5
Konfigurasi ACL *Authenticated Users*

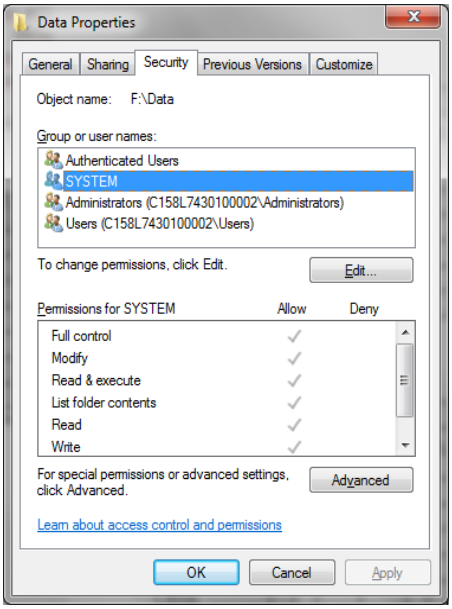
ACL	UFD Kontrol		UFD H1	
	Allow	Deny	Allow	Deny
Full Control				
Modify	√		√	
Read & Execute	√		√	
List Folder Content	√		√	
Read	√		√	
Write	√		√	
Special Permission				



- Pengaturan ACL untuk*SYSTEM*

Tabel 6
Konfigurasi ACL *System*

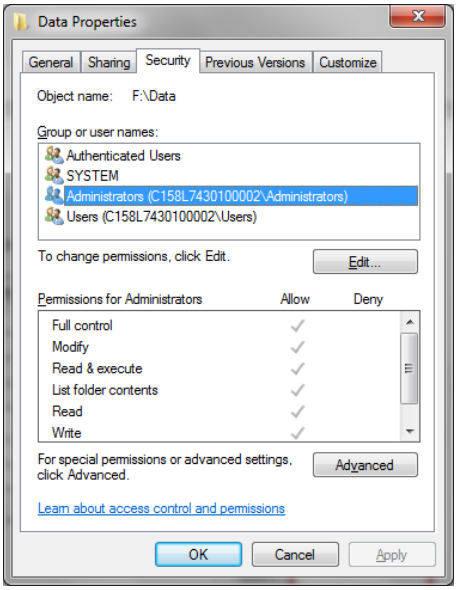
ACL	UFD Kontrol		UFD H1	
	Allow	Deny	Allow	Deny
Full Control	√		√	
Modify	√		√	
Read & Execute	√		√	
List Folder Content	√		√	
Read	√		√	
Write	√		√	
Special Permission				



9. Pengaturan ACL untuk*Administrators*

Tabel 7
Konfigurasi ACL *Administrator*

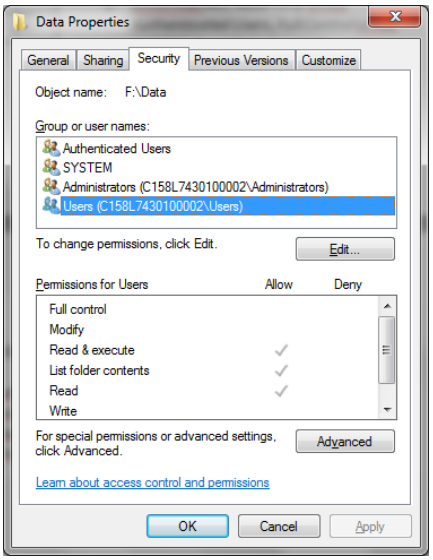
ACL	UFD Kontrol		UFD H1	
	Allow	Deny	Allow	Deny
Full Control	√		√	
Modify	√		√	
Read & Execute	√		√	
List Folder Content	√		√	
Read	√		√	
Write	√		√	
Special Permission				



- Pengaturan ACL untuk*Users*

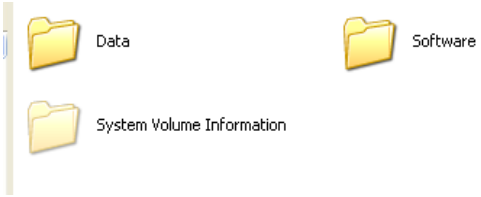
Tabel 8
Konfigurasi ACL *Users*

ACL	UFD Kontrol		UFD H1	
	Allow	Deny	Allow	Deny
Full Control				
Modify				
Read & Execute	√		√	
List Folder Content	√		√	
Read	√		√	
Write				
Special Permission				

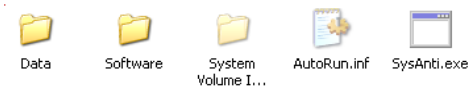


10. Hubungkan ke dua *USB Flash Disk* pada komputer yang telah terinfeksi malware Trojan Shortcut
11. Lakukan pengamatan pada kedua *USB Flash Disk*

Dari hasil pengujian didapati bahwa *USB Flash Disk* H1 ternyata memiliki ketahanan terhadap payload dari Trojan Shortcut dimana tidak ada satu file pun yang berhasil Trojan Shortcut tuliskan ke dalam direktori utama *USB Flash Disk*



Sementara *USB Flash Disk*Kontrol yang tidak mendapat perlakuan pemodifikasian ACL akan langsung terinfeksi Trojan Shortcut pada saat UFB pertama kali dihubungkan pada komputer yang terinfeksi



Kesimpulan

Tojan Shorcut yang yang dikenali oleh anti virus McAffe versi 4.6.0.3122 sebagai trojan *Exploit-CVE-2010-2586* merupakan *malware* trojanyang menggunakan metode penyebaran penginfeksian klasik menggunakan file *AutoRun.inf* dan file Induk, file SysAnti.exe adalah file induk *malware* yang digunakan pada *malware*trojan Shortcut. Modifikasi ACL *Read Only*untuk *Authenticated Users*,*Full Control* untuk*SYSTEM*,*Read Only* dan *Write*untuk Administrator, dan *Read Only* untuk Users dapat melindungi direktori utama *USB Flash Disk.* Dari penelitian dapat disimpulkan bahwa teknik modifikasi ACL yang diaplikasikan pada *USB Flash Disk* secara efektif dapat melindungi *USB Flash Disk* dari infeksi *malware* trojan Shortcut dan penyebarannya

Daftar Pustaka

Abraham Silberschatz, Peter Baer Galvin, Greg Gagne, "*Operating System Concept*", 6th, Wiley, 2001

Britannica Encyclopedia, "*Malware"*, www.britannica.com, 4 Juli 2014

Microsoft, "*Access Control Lists"*, http://msdn.microsoft.com/en-us/library/windows/desktop/aa374872%28v=vs.85%29.aspx