OPTIMASI ACCESS CONTROL LIST SEBAGAI BAGIAN REAKSI CEPAT TANGGAP ATAS GANGGUAN INFEKSI MALWARE SKYPEE PADA MEDIA PENYIMPANAN JARINGAN KOMPUTER PADA PT. KYZ

Nugroho Budhisantosa
Fakultas Ilmu Komputer, Universitas Esa Unggul
Nugroho.budhisantosa@esaunggul.ac.id

Abstrak

Tulisan ini merupakan studi pengaplikasian optimasi *Access Control List* sebagai bagian dari reaksi tanggap gangguan atas infeksi *Trojan Skypee* yang diaplikasikan dalam bentuk perangkap Malware pada media penyimpanan Jaringan.Hasil menunjukkan bahwa malware yang menginfeksi perangkat media penyimpanan jaringan akan terisolasi dan terperangkap di dalamnya tanpa dapat menyebar ke host lainnya di dalam jaringan komputer dan sistem akan menunjukkan komputer sumber penyebaran infeksi yang akan memudahkan tindakan pembersihan sistem komputer terhadap infeksi *Trojan Skypee* secara menyeluruh.

Kata Kunci: Access Control List, Malware Skypee, Jaringan Komputer

Abstract

This paper is an application study of the Access Control List optimization as part of the response reaction to the disruption of Skypee Trojan infection which is applied in the form of traps Network Malware on the storage media.The results showed that the malware that infects the network storage media device will be isolated and trapped without being able to spread to other hosts on the network and the computer system will show the source of the spread of infection that will help to facilitate the cleaning action of computer systems against Trojan infection Skypee thoroughly.

Keywords: *Access Control List , Malware Skypee , Computer Networking*

Pendahuluan

Tidak terpengaruh oleh seberapa baiknya sistem pertahanan keamanan jaringan komputer telah disiapkan, suatu insiden keamanan dapat terjadi kapan saja. Demikian juga halnya yang terjadi pada PT. XYZ yang telah melengkapi sistem pertahanan jaringan komputernya dengan sistem antivirus kelas dunia yang ternyata tidak mampu melindungi sistem secara 100% terhadap ancaman infeksi malware.

Bermula dari perangkat media penyimpanan milik pengguna yang sebelumnya telah terinfeksi malware yang signature nya belum dikenali oleh database sistem anti virus terpasang, dalam hitungan detik malware ini langsung menginfeksi sistem media penyimpanan jaringan berikut puluhan host komputer yang mencoba mengakses media penyimpanan jaringan yang telah terinfeksi malware ini.

Adalah trojan Skypee, nama yang digunakan penulis untuk mengedentifikasi keberadaan malware ini di dalam sistem media pentimpanan PT. XYZ. Penamaan ini diberikan berdasarkan ciri khusus dari trojan ini yang akan membentuk folder Skypee di dalam direktori utama dari media penyimpanan komputer.

Trojan Skypee adalah sejenis trojan yang menyebar dengan sangat cepat nya di dalam sistem media penyimpanan sehingga perlu dilakukan pembersihan secara keseluruhan bukan saja pada host komputer dan media penyimpanan dari infeksi trojan ini, tetapi juga pada semua perangakat penyimpanan yang akan terhubung pada komputer PT. XYZ

Standar Operating Prosedur pada insiden keamanan seperti ini pada PT. XYZ adalah mengirimkan contoh malware ke rekanan vendor anti virus dan menunggu upgrade database terbaru dari anti virus yang telah memuat signature dari malware ini sehingga pembersihan dan pencegahan infeksi lanjutan dapat dilakukan.

Masalah yang dihadapi oleh PT. XYZ adalah kenyataan bahwa rekanan vendor anti virus tidak dapat memberikan solusi pertahanan yang dapat memblok infeksi malware melainkan hanya terbatas melakukan penghapusan pada berkas-berkas malware di dalam media penyimpanan, sementara proses malware akan tetap berjalan pada memori host komputer yang terinfeksi kemudian. Sehingga infeksi malware selalu berulang setiap ada pengguna yang menghubungkan media penyimpanan eksternal seperti USB Flash Disk atau

perangkat smarthphone yang telah terinfeksi pada komputer yang digunakannya.

Kondisi ini membuat PT. XYZ perlu mengembangkan suatu teknik pendeteksian asal sumber infeksi ketika sistem jaringan telah dibersihkan dari infeksi dan melakukan pengejaran malware langsung dari sumbernya untuk melakukan pembersihan sambal menunggu update database yang berisi digital signatures dari malware terbaru.

Rumusan Masalah

Masalah yang ditemukan dan perlu diberikan solusi dari kasus di atas adalah:

1. Bagaimanakan cara menonaktifkan *payload* dari malware ketika malware telah menginfeksi media penyimpanan dan meletakkan berkas-berkas induk di dalamnya?
2. Bagaimanakah cara mengetahui host komputer asal infeksi malware agar tindakan pembersihan dapat segera dilakukan.

Manfaat

1. Mempelajari cara kerja *trojan Skypee*
2. Memberikan referensi pada pihak-pihak yang tertarik untuk mendalami pengetahuan tentangtanggap gangguan *malware*.

Tinjauan Teori

*Malware*adalah istilah yang merupakan kependekan dari kata *malicious software* dimana istilah ini mengacu pada satu kelompok perangkat lunak yang diciptakan untuk tujuan mengganggu pengoperasian dari komputer, mencuri informasi penting di dalam komputer, mendapatkan akses ke dalam sistem komputer, atau menampilkan iklan yang tidak diingikan oleh penggunanya.

Malware dapat hadir dalam bentuk virus komputer, *worm*, *Trojan*, *rootkit*dan perangkat lunak lainnya yang dibuat dengan maksudjahat.

Berbeda dengan virus komputer, *worm*, dan *rootkit*, malware yang berada dalam kelompok Trojan komputertidak dirancang secara khusus untuk memiliki mekasime pengaktifan diri sendiri–*self activated*, agar dapat aktif *malware Trojan* akan menggunakan teknik *social engineering*pada user sehingga secara tidak sadar melakukan aktifasi *payload* nya.

Terkadang*malware Trojan*juga menggunakan berkas *autorun.inf* sebagai berkas pengaktifan*payload* nya.Berkas *autorun.inf* adalah berkas yang akan dieksekusi secara otomatis oleh sistem operasi Windows ketika sistem operasi Windows menemukan keberadaan berkas ini di dalam direktori utama dari media penyimpanan ketika media penyimpanan terhubung pada komputer yang aktif, jadi apa yang diperlukan oleh malware Trojan adalah membuat satu set perintah pengaktifan diri yang dibuat di dalam format berkas *autorun.inf*.

Sistem operasi Microsoft Windows sebenarnya bukanlah sistem operasi yang mengabaikan keamanan pengoperasiaan.Sistem operasi Windows telah dilengkapi dengan beberapa fitur keamanan seperti *Access Control List* (ACL).

ACL secara umum banyakdiimplementasikan untuk keperluan pengontrolan aksespengguna komputer atas media penyimpanan.

ACL sendiri telah menjadi fitur dari Sistem berkas NTFS yang dibawa oleh keluarga Sistem Operasi dari Microsoft yang memungkinkan sistem operasi melakukan:

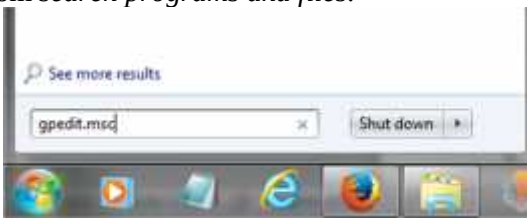
1. Pencegahan eksekusi program di dalam media penyimpanan jaringan komputer.
2. Pencegahan user untuk mengakses berkas yang tidak diperuntukkan untuknya.
3. Perlindungan reabilitas keberadaan informasi pada perangkat penyimpanan di dalam jaringan komputer.

Di dalam konteks Microsoft, ACL adalah suatu tabel yang berisi informasi keamanan obyek yang mendefinisikan hak akses terhadap sumber daya seperti *users*, *groups*, proses-proses atau perangkat-perangkat yang dapat berupa berkas, folder, atau sumber daya jaringan yang lainnya. Pengaturan ACL pada Sistem Operasi Microsoft Windows

Gambar 1
Property ACL pada sistem operasi Microsoft Windows

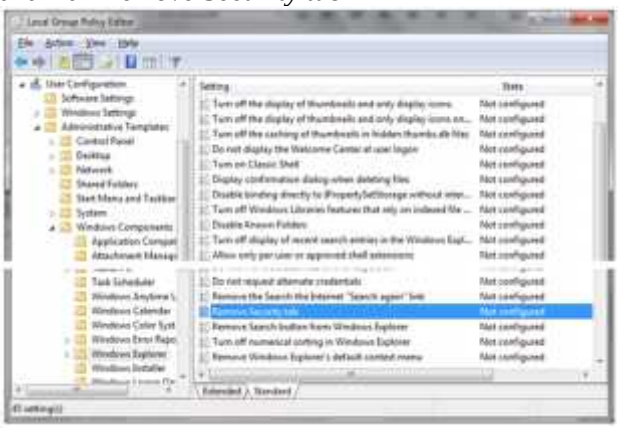
Untuk dapat mengakses ACL, pengguna sistem operasi perlu menonaktifkan seting *Remove Security Tab*melalui*Local Group Policy*

*Editor*dengan cara mengetikkan gpedit.msc pada kolom *search programs and files*.



Gambar 2
Aktifasi *Security Tab*

Pada jendela *Group Policy* lakukan navigasi ke *User Configuration ->Administrative Templates ->Windows Components ->Windows Explorer* non aktifkan *Remove Security tab*



Gambar 3
Penonaktifan *Remove Security Tab*

Tinjauan Sistem Terpasang

PT. XYZ secara adalah perusahaan otomotif yang memiliki kantor di 3 (tiga) lokasi yang berbeda.

Dalam pengoperasian kegiatannya, PT. XYZ menggunakan perangkat teknologi informasi berupa 3 (tiga) unit *network storage* yang masing-masing lokasi memiliki 1 unit network storage yang ketiganya saling terhubung melalui Internet untuk keperluan sinkronisasi *e-collaboration* berbagi berkas.

Menggunakan script *auto mapping*, maka setiap pengguna komputer akan terkoneksi ke network storage melaui *drive mapping* berikut:

1. Drive H:\ - Merupakan drive personal dimana pengguna komputer dapat meletakkan berkas-berkas penting di dalamnya. Drive H:\ ini secara otomatis akan dilakukan backup harian oleh sistem *cron job* sehingga berkas-berkas yang ada di dalamnya dapat terjaga ketersediaannya.
2. Drive P:\ - Drive ini adalah drive yang berisi berkas-berkas informasi proyek dimana berkas-berkas yang digunakan secara bersama oleh banyak departemen diletakkan di dalamnya dalam struktur folder sesuai dengan nama proyeknya. Drive P:\ adalah subyek *back up* harian oleh sistem.
3. Drive T:\ - Biasa disebut drive sementara – *temporary* dimana didalamnya, semua user dapat meletakkan berkas-berkas yang bersifat sementara dan secara otomatis akas dihapus oleh sistem *cron job* pada jam 8 malam
4. Drive Y:\ - Drive ini adalah drive milik divisi dimana pengguna komputer yang berada di dalam divisi yang sama dapat berbagi berkas pekerjaan di dalamnya. Drive Y:\ adalah subyek untuk dilakukan back up harian oleh proses *cron job*.
5. Drive Z:\ - Drive ini adalah drive milik Departemen dimana pengguna komputer yang berada di dalam departemen yang sama dapat berbagi berkas pekerjaan di dalamnya. Drive Z:\ adalah subyek untuk dilakukan back up harian oleh proses *cron job*

Pembahasan

Melihat sistem mapping berkas di atas, maka apa yang terjadi ketika malware yang tidak terdeteksi oleh aplikasi pertahanan Anti Virus yang memiliki kemampuan menginfeksi *network storage*tereksekusioleh pengguna komputer, maka secara otomatis *malware Trojan*akan langsung menginfeksi semua driver yang terhubung.

Hal inilah yang terjadi ketika salah seorang pengguna komputer menghubungkan media penyimpanan eksternal yang telah terinfeksi *Trojan Skypee* pada komputer yang terhubung ke dalam jaringan komputer. Dalam waktu singkat Trojan komputer ini menyebar dengan sangat cepat ke dalam media penyimpanan jaringan dan menginfeksi komputer lainnya yang kemudian mengakses media penyimpanan jaringan yang sama.

Trojan Skypee menggunakan file *autoun.inf* sebagai mekanisme penginfeksian dirinya ke dalam sistem komputer. *autorun.inf* adalah berkas yang akan dieksekusi secara otomatis oleh sistem operasi Windows ketika sistem operasi Windows menemukan keberadaan berkas ini si dalam direktori utama dari media penyimpanan ketika media penyimpanan terhubung pada komputer yang aktif.

Berkas *autorun.inf* dari *trojan Skypee* berisi instruksi untuk menjalankan file induk malware yang diletakkan secara tersamar di dalam direktori utama dari media penyimpanan yang telah terinfeksi.

Strategi

Dalam kondisi pertahanan sistem Anti Virus yang tidak dapat melakukan pemblokiran terhadap

lalulintas berkas Trojan yang belum dikenali ini di dalam jaringan komputer membuat situasi pembersihan menjadi sulit karena infeksi ulang dapat kembali terjadi disebabkan Trojan Komputer ini sekarang telah menginfeksi lebih banyak perangkat seperti smartphone dan perangkat media penyimpanan eksternal yang terhubung pada sistem dan kelak akan kembali dihubungkan oleh pengguna.

Untuk menghadapi situasi seperti ini maka strategi berikut diterapkan:

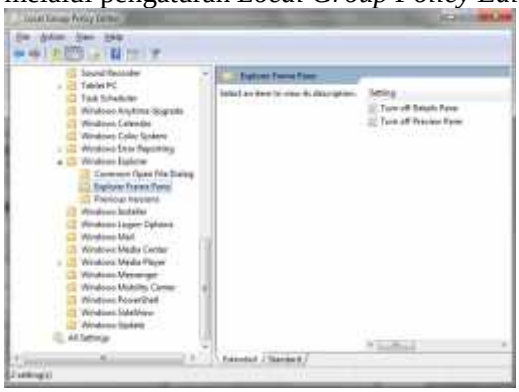
1. Memahami cara penyebaran *Trojan Skypee* pada peinyimpanan jaringan
2. Melakukan konfigurasi perangkap berdasarkan mekanisme penyebaran *Trojan Skypee* pada peinyimpanan jaringan
3. Pengujian perangkat
4. Pengaplikasian perangkap

Setelah mempelajari mekanisme kerja *Trojan Skypee* di atas maka perangkap Trojan Skypee dibuat pada jaringan komputer dengan tahap-tahap sebagai berikut:

1. Memutuskan semua *mapping* drive ke media penyimpanan jaringan kecuali pada *drive* T:\ yang merupakan drive media penyimpanan sementara (temporary). *Drive* T:\ adalah *drive* yang dapat diakses oleh semua user sehingga *drive* ini dipilih sebagai *drive* perangkat *Trojan Skypee*.
2. Pada drive T:\ dilakukan modifikasi *ACL* yang tidak mengijinkan segala bentuk eksekusi terhadap berkas yang tersimpan di dalamnya. Melalui modifikasi ini maka berkas Trojan yang berasal dari komputer pengguna ketika menginfeksi drive T:\ tidak akan dapat dieksekusi oleh pengguna siapapun (*Everyone*)

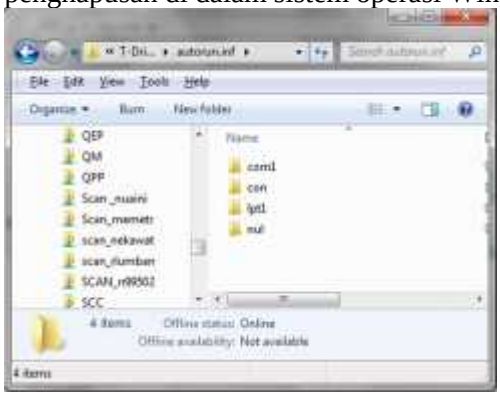
Gambar 4
Penonaktifan opsi *Read & Execute* pada *ACL*

3. Untuk mengetahui asal sumber penyebar berkas *Trojan Skypee*, panel *Details* perlu diaktifkan melalui pengaturan *Local Group Policy Editor*



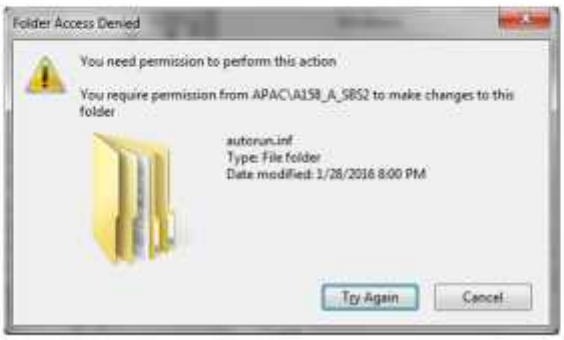
Gambar 5
Pengaktifan panel Details melalui*Local Group Policy Editor*

4. Mencegah penulisan berkas autorun.inf dapat dilakukan dengan membuat folder dengan menggunakan nama*autorun.inf*. Sistem operasi Windows tidak mengijinkan folder dan berkas untuk memiliki nama yang sama. Ketika pada driver telah ada folder dengan nama autorun.inf maka sistem operasi tidak akan mengijinkan penulisan berkas dengan nama autorun.inf di dalam folder tersebut.
5. Folder *autorun.inf* yang dibuat pada langkah sebelumnya adalah folder yang memiliki kelemahan yang rentan terhadap upaya penghapusan oleh malware, untuk ini beberapa subfolder seperti com1, Con, lpt1, *nul* perlu ditambahkan di dalamnya yang akan membuat folder autorun.inf menjadi kebal upaya penghapusan. Hal ini dimungkinkan karena penamaan sub folder diatas bukan merupakan penamaan yang diijinkan didalam sistem operasi Windows sehingga tidak dapat dihapus dengan cara yang umum dilakukan pada penghapusan di dalam sistem operasi Windows.



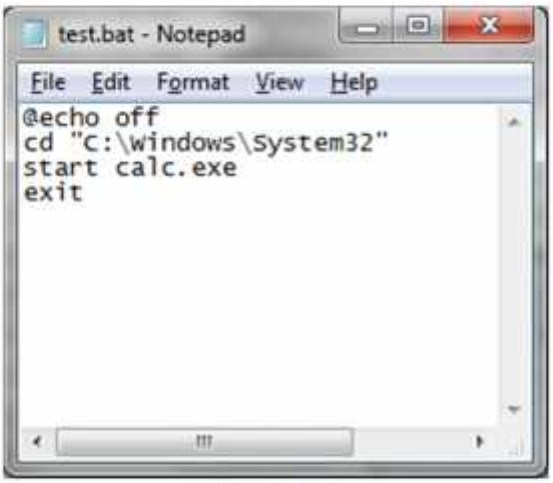
Gambar 6
Sub folder khusus yang tidak dapat dihapus menggunakan cara penghapusan biasa di dalam sistem operasi Windows

Ketika upaya penghapusan konvensional dilakukan pada folder autorun.inf di atas yang telah mengalami modifikasi maka pesan kesalahan akan muncul.



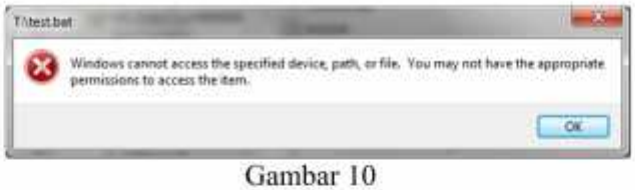
Gambar 7
Pesan kesalahan ketika folder autorun.inf coba dihapus

Setelah langkah konfigurasi perangkap maka pengujian dilakukan menggunakan berkas test.bat yang berisi instruksi untuk mengaktifkan aplikasi kalkulator dan aplikasi bereksistensi .exe.Hasil pengujian menunjukkan baik berkas test.bat maupun aplikasi bereksistensi .exe tidak dapat dieksekusi dan memunculkan pesan kesalahan. Hal ini menunjukkan bahwa perangkap*Trojan Skypee* telah bekerja sesuai dengan yang diinginkan.



Gambar 8
Program test.bat untuk menjalankan aplikasi kalkulator

Gambar 9
Program test.bat untuk menjalankan aplikasi kalkulator



Gambar 10
Pesan kesalahan yang muncul ketika berkas test.bat dan aplikasi berekstensi .exe dieksekusi

Langkah terakhir adalah langkah pengaplikasian yang menunjukkan malware *Trojan Skypee*akan terperangkap di dalam perangkap dan menunjukkan sumber komputer host asal infeksi untuk kemudian akan dilakukan langkah pembersihan secara manual.

Gambar 11
Malware Trojan Skypee yang dan menunjukkan sumber komputer host asal infeksi

Kesimpulan

Dari kasus di atas dapat dipelajari bahwa dengan pengaturan *ACL* yang tepat, pekerjaan penanganan infeksi *malware Trojan Skypee* dapat dilakukan dengan cara yang mudah

Saran

Untuk melindungi dan membersihkan Sistem Operasi dari serangan malware adapat dilakukan langkah-langkah berikut:

1. Lakukan updates
2. Memperhatikan proses-proses yang aktif ketika sistem dinyalakan
3. Gunakan perangkat lunak pemindai malware terbaru
4. Gunakan digital signatures untuk memastikan bahwa berkas yang diterima sama tidak mengalami infeksi malware.
5. Buatlah Back up sistem secara berkala dan *repair disks*
6. Buat dan implementasikan kebijakan-kebijakan penggunaan sistem komputer.

Daftar Pustaka

Mark Ciampa. (2003). *Security+ Guide to Network Security Fundamentals* (1st Edition). Course Technology.

Michael Palmer. (2003).*Guide to Operating Systems Security* (1st Edition). Course Technology.