PEMANFAATAN *SPYWARE* UNTUK MONITORING AKTIVITAS KEYBOARD DALAM JARINGAN MICROSOFT WINDOWS

Mulki Indana Zulfa, Erfan Subiyanta
Teknik Elektro Fakultas Teknik Universitas 17 Agustus 1945 Cirebon
Jln. Perjuangan No.17 Kota Cirebon Telp.0231-481945
mulki_indanazulfa@yahoo.com

ABSTRAKSI

Pengawasan terhadap penggunaan teknologi informasi sangat diperlukan terlebih semakin berkembangnya ilmu tentang pembuatan virus, worm, atau spyware. Memasang antivirus bisa juga menjadi solusi untuk mencegah virus masuk ke dalam jaringan atau sistem komputer. Tetapi antivirus tidak bisa melakukan monitoring terhadap aktivitas user contohnya aktivitas keyboard.

Keylogger adalah perangkat lunak yang mampu merekam segala aktivitas keyboard. Keylogger harus diinstal terlebih dahulu terhadap target komputer (client) yang akan direkam aktivitas keyboard-nya. Kemudian untuk mengambil file hasil rekamannya, file log, harus mempunyai akses fisik ke komputer tersebut dan hal ini akan menjadi masalah jika komputer target yang akan dimonitoring cukup banyak.

Metode control keylogger-spy agent dengan memanfaatkan teknologi spyware menjadi solusi dari masalah tersebut. Spy agent akan secara aktif merekam aktivitas keyboard seseorang. File log yang dihasilkan akan disimpan didalam cache-nya sehingga tidak akan menimbulkan kecurigaan user dan tidak perlu mempunyai akses fisik jika ingin mengambil file lognya. Control keylogger dapat menghubungi spy agent mana yang akan diambil file lognya. File log yang berhasil diambil akan disimpan dengan baik di komputer server. Dari hasil pengujian lima komputer yang dijadikan target spy agent semuanya dapat memberikan file log kepada control keylogger.

Kata kunci: keylogger, control keylogger-spy agent, microsoft winsock control.

1. PENDAHULUAN

Serangan virus, *spyware* dan program membahayakan lainnya semakin meningkat kuantitas maupun kualitasnya. Hal tersebut terjadi karena semakin berkembangnya ilmu tentang *security komputer* dan kelemahan – kelemahan yang ditemukan dalam sebuah sistem.

Spyware adalah program yang mampu memata-matai aktivitas pengguna komputer, dimana salah satunya adalah dapat merekam ketukan *keyboard* yang disebut *keylogger*.

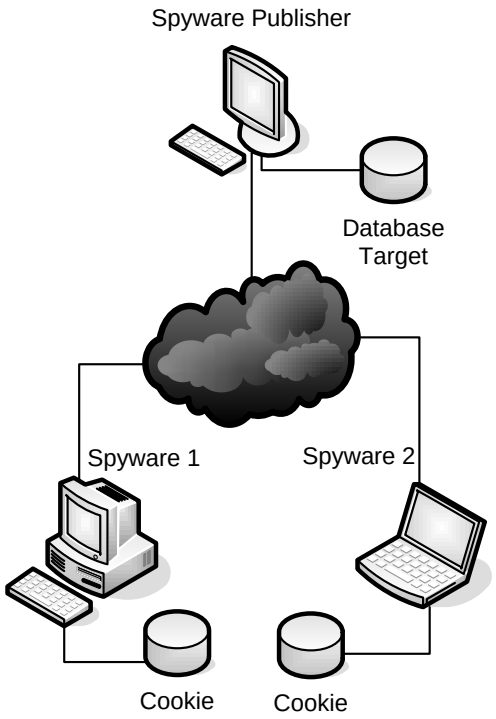
Ada lima metode yang banyak digunakan oleh perangkat lunak *keylogger* diantaranya *hypervisor-based, kernel-based, hook-based, passive-method,* dan *form grabber based*. Kemudian diantara lima metode tersebut *passive method* adalah teknik yang paling banyak digunakan oleh pembuat *keylogger*. Metode ini banyak menggunakan fungsi Windows API (*Appication Programming Interface*).

Jika *keylogger* tersebut dapat dimanfaatkan untuk aktivitas positif yaitu monitoring jaringan area lokal (LAN), maka hal itu akan memudahkan seorang Administrator dalam mengawasi jaringan komputer yang dikelolanya. Aktivitas yang diawasi misalnya untuk mengawasi bawahannya saat bekerja hingga memang berniat untuk mencuri data pribadi seseorang.

Ada dua istilah lain yang berkaitan dengan *spyware* yaitu *trojan horse* dan *Remote Administration Tool* (RAT). *Trojan horse* adalah program yang disamarkan dengan file lain yang tidak dianggap berbahaya contohnya icon program yang sama dengan icon MS.Word ditambah dengan nama file yang sangat menarik sehingga memancing user untuk mengeksekusi file tersebut.

Biasanya tiap *spyware* yang disebarkan diberikan kode yang unik untuk membedakan informasi dari tiap target dengan menggunakan metode *Globally Unique IDentifier* (GUID). GUID akan menyimpan informasi *cookie* dan perangkat keras pada *harddisk* komputer target. *Spyware* secara periodik akan terus – menerus mengirimkan informasi tersebut sehingga informasi yang dimiliki oleh pemilik *spyware* akan diperbarui terus. (Ari, 2006)

Gambar dibawah ini menjelaskan bagaimana *spyware* bekerja pada tiap komputer target.



Gambar 1. Ilustrasi cara keja *spyware*

Keylogger adalah salah satu jenis *spyware* yang memiliki kemampuan untuk memata – matai (merekam) ketukan *keyboard* yang bekerja secara sembunyi tanpa diketahui oleh pengguna komputer. *Keylogger* banyak dimanfaatkan oleh *hacker* untuk mencuri data – data penting seperti user dan *password* email, no rekening bank atau kartu kredit serta banyak informasi penting lainnya yang dapat direkam oleh *keylogger*.

Keylogger ada yang berbentuk perangkat lunak maupun perangkat keras. Perangkat keras *keylogger* susah untuk dideteksi oleh antispyware atau antivirus sekalipun tetapi justru lebih mudah dilihat oleh mata karena biasanya perangkat ini akan dipasang diantara konektor kabel *keyboard* dan *port* PS2 atau USB pada komputer. (S'to, 2009)

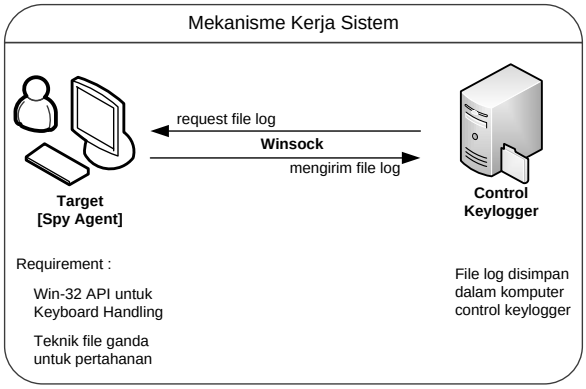
Ada lima metode yang banyak digunakan oleh perangkat lunak *keylogger* diantaranya *hypervisor-based*, *kernel-based*, *hook-based*, *passive-method*, dan *form grabber based.* Dalam paper ini keylogger yang dibuat menggunakan *passive-method*.

Passive-Method keylogger adalah teknik yang paling banyak digunakan oleh pembuat *keylogger* yaitu dengan banyak memanfaatkan fungsi windows *Application Programming Interface* (API). Fungsi – fungsi API yang digunakan diantaranya *GetAsyncKeyState(), GetForegroundWindow(), GetWindowText(), GetCapsState(), dan GetShiftState()*.

2. METODE PENELITIAN

Sistem yang dibuat adalah aplikasi yang mampu merekam aktivitas *keyboard* melalui *spy agent* yang sengaja dijalankan di komputer target dalam jaringan LAN kemudian mampu mengirimkan file lognya jika *control keylogger* memintanya.

Mekanisme kerja sistem digambarkan yang ditunjukkan pada gambar 2

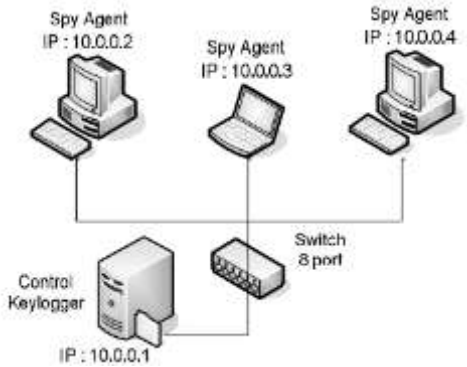


Gambar 2. Gambaran umum sistem

Adapun metodologi yang digunakan adalah sebagai berikut :

1. Identifikasi masalah
2. Studi literatur
3. Analisis dan perancangan
4. Implementasi
5. Pengujian Sistem

Untuk memudahkan implementasi maka topologi yang digunakan adalah Star dengan bentuk sebagai berikut :



Gambar 3. Topologi Pengujian Sistem

Adapun skenario pengujiannya adalah sebagai berikut:

Skenario pada komputer client :

1. *Spy agent* akan dijalankan disetiap komputer client.
2. User akan diminta melakukan aktivitas yang menggunakan *keyboard* seperti mengetik sebuah dokumen.
3. Komputer client yang menjadi target *spy agent* akan diinstal antivirus yang berbeda – beda.

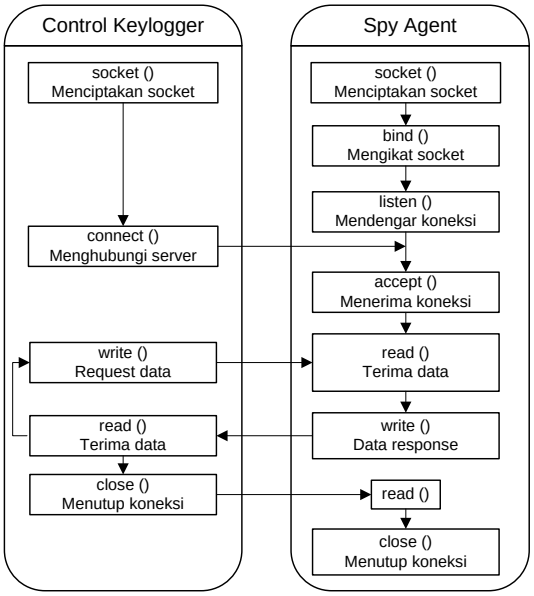
Skenario pada komputer server :

a) *Control keylogger* akan dijalankan pada komputer server.
b) *Control keylogger* akan melakukan koneksi dengan salah satu komputer client dan me-request terhadap file log yang telah direkam sebelumnya oleh *spy-agent*.
c) File log yang telah berhasil dikirim oleh *spy agent* akan disimpan di komputer server sehingga mudah untuk dikelola.

3. HASIL DAN PEMBAHASAN

Mekanisme kerja ini dimulai dari *control keylogger* dan *spy agent* yang membuat *socket* terlebih dahulu sebelum menjalin komunikasi. *Spy agent* dalam hal ini yang bertindak sebagai *server* akan *binding* (mengikat) terlebih dahulu *socket* yang telah dibuat, hal ini mencegah port yang digunakan agar tidak digunakan oleh aplikasi lain dalam komputer yang sama. Setelah *socket* telah dibuat dan diikat kemudian *spy agent* akan menunggu koneksi dari *control keylogger* dan melakukan apa yang dimintanya.

Untuk mengambil file log hasil rekaman aktivitas *keyboard*, *control keylogger* akan melakukan koneksi ke salah satu *spy agent* yang telah berada di komputer target. *Spy agent* yang telah menerima koneksi tersebut akan menunggu perintah *control keylogger* berikutnya. *Control keylogger* dapat meminta file log hasil rekaman aktivitas *keyboard*, mengaktifkan atau menonaktfikan monitoring aktivitas *keyboard*, dan dapat menghapus *spy agent* pada komputer target, semuanya dilakukan secara *remote* melalui LAN.



Gambar 4 : Mekanisme kerja *control keylogger* dan *spy agent*

Jika tidak ada lagi perintah yang diberikan, *control keylogger* dapat mengakhiri komunikasi dengan *spy agent* dengan memberi notifikasi terlebih dahulu kepada *spy agent* bahwa koneksi yang ada akan diakhiri. Pada saat itu *control keylogger* akan menutup koneksinya yang kemudian diikuti oleh *spy agent* dengan melakukan hal yang sama.

Sistem ini diuji dengan user dan antivirus. Antivirus yang digunakan ditunjukkan pada tabel 1.

Tabel 1. Daftar antivirus yang menguji sistem

No	Nama antivirus	Versi	Produksi
1	Avast! Free Antivirus	5.0.545	Luar
2	AVIRA AntiVir Personal	9.0.0.457	Luar
3	ESET NOD32	4.2.22.0	Luar
4	Commodo Internet Security	3.13.120417	Luar
5	SmadAV	rev.8.1	Lokal
6	PC Media	3.0 build 3	Lokal

Hasil percobaan menunjukkan bahwa antivirus lokal dan luar tidak mampu menemukan keberadaan spy agent. Hanya antivirus yang berjenis firewall yang mampu mendeteksi adanya koneksi ilegal dari dalam sistem menuju luar sistem.

Gambar 5. *Alert firewall* terhadap koneksi *control keylogger* dan *spy agent*

4. KESIMPULAN

Berdasarkan hasil penelitian yang dilakukan didapatkan kesimpulan sebagai berikut :

1. Baik antivirus lokal maupun luar, keduanya tidak dapat menemukan *spyware* yang dijalankan pada komputer target.
2. Kemampuan antivirus akan lebih lengkap jika mempunyai kemampuan *form scanning* dan *behavior detection* secara sekaligus. Sehingga jika antivirus tidak mampu melihat dan mengerti instruksi yang mencurigakan pada sebuah file, maka antivirus ini dapat menganalisis melalui perilakunya ketika file tersebut dieksekusi.
3. Dengan menginstal *firewall* tambahan akan mengurangi bahaya dari serangan virus atau *spyware* yang kadang tidak bisa dideteksi oleh antivirus.

5. DAFTAR PUSTAKA

Darmal, Achmad, 2007, “Computer Worm 1”, Jasakom, Jakarta.

Darmal, Achmad, 2007, “Computer Worm 2”, Jasakom, Jakarta.

Saputra, Johan, 2005, “Eksplorasi Kekuatan WIN-32 API dengan Visual Basic”, PT. Elex Media Komputindo, Jakarta.

S’to, 2007, ”Seni Teknik Hacking 2”, Jasakom, Jakarta.

S’to, 2009, “CEH Certified Ethical Hacker 200% Illegal”, Jasakom, Jakarta.

Wardana, Ari, 2006, “Pemrograman Virus dan Spyware”, Jasakom, Jakarta.