

**PAPER TUGAS AKHIR (EC 7010)**  
**KEAMANAN SISTEM LANJUT**

---



**DETEKSI TROJAN DAN  
PENANGANANNYA**

Disusun Oleh

**ROHMADI HIDAYAT**  
**23203124**

**BIDANG KHUSUS TEKNOLOGI INFORMASI**  
**DEPARTEMEN TEKNIK ELEKTRO**  
**INSTITUT TEKNOLOGI BANDUNG**

2004

---

## DAFTAR ISI

	Halaman
DAFTAR ISI	i
DAFTAR GAMBAR	iii
ABSTRAK	iv
BAB I. PENDAHULUAN	1
1.1 Latar Belakang Masalah	1
1.2 Tujuan	2
1.3 Sistematika Pembahasan	2
BAB II. PENGERTIAN UMUM TROJAN	3
2.1 Definisi Trojan	4
2.2 Fungsi Trojan	4
2.3 Cara Kerja trojan	6
2.4 Jenis-jenis Trojan	9
2.4.1 Trojan Remote Akses	10
2.4.2 Trojan Pengirim Password	10
2.4.3 Trojan FTP	10
2.4.4 Keyloggers	10
2.4.5 Trojan Penghancur	11
2.4.6 Trojan Denial of Service (DoS) Attack	11
2.4.7 Trojan Proxy/Wingate	12
2.4.8 Software Detection Killers	12
2.5 Sumber-sumber Trojan	12
2.5.1 ICQ	12
2.5.2 IRC	13
2.5.3 Attachment	13
2.5.4 Physical Access	14
2.5.5 Lubang Software Browser dan E-mail	14
2.5.6 Netbios (File Sharing)	15

	Halaman
2.6 Program Gadungan, Situs Yang Tidak Dapat Dipercaya dan Software Freeware	15
2.7 Port Yang Digunakan Trojan	16
2.8 Apa Yang Dicari Penyerang	16
 BAB III. DETEKSI TROJAN DAN PENANGANANNYA	 18
3.1 Deteksi Trojan	18
3.2 Menghapus Trojan	20
3.2.1 Anti-Virus Scanner	21
3.2.2 Trojan Scanner	21
3.3 Penanganan Pengobatan (Recovery)	22
3.4 Pencegahan Agar Terhindar Dari Trojan	24
 BAB IV. ANALISIS DAN KESIMPULAN	 28
4.1. Analisis	28
4.2. Kesimpulan	29
 DAFTAR PUSTAKA	 30
 LAMPIRAN	 31

## DAFTAR ISI

	Halaman
Gambar 2.1 Penyusupan Trojan dalam Belanja <i>Online</i>	6

# DETEKSI TROJAN DAN PENANGANANNYA

*Rohmadi Hidayat*  
NIM 23203124  
rohmedi\_hdy@yahoo.com

## ABSTRAK

Trojan Horse atau lebih dikenal dengan “Trojan” dalam sistem komputer adalah bagian dari infeksi digital yang kehadirannya tidak diharapkan oleh pemilik komputer. Trojan terdiri dari fungsi-fungsi yang tidak diketahui tujuannya, tetapi secara garis besar mempunyai sifat merusak. Trojan masuk ke suatu komputer melalui jaringan dengan cara disisipkan pada saat berinternet dengan media fisik.

Trojan tidak membawa pengaruh secara langsung seperti halnya virus komputer, tetapi potensi bahayanya dapat jauh lebih besar dari virus komputer. Trojan dapat diaktifkan dan dikendalikan secara jarak jauh atau menggunakan timer. Pengendalian jarak jauh seperti halnya *Remote Administration Tools*, yaitu versi *server* akan dikendalikan oleh penyerang lewat versi *client*-nya. Banyak hal yang dapat dilakukan oleh penyerang jika komputer korban yang telah dikendalikan. *Port* tertentu yang tidak lazim terbuka mengindikasikan adanya kegiatan aktif trojan

Penanganan Trojan dapat dilakukan dengan dua cara, yaitu pencegahan (*preventif*) dan pengobatan (*recovery*). Usaha pencegahan dilakukan sebelum terjadinya infeksi, yaitu usaha agar sistem tidak mempunyai lubang keamanan. Usaha pengobatan dilakukan setelah sistem terinfeksi, yaitu usaha untuk menutup lubang kemanan yang telah dieksploitasi dan menghilangkan penyebab infeksi.

Pemahaman tentang seluk beluk Trojan perlu diketahui oleh pemakai Internet untuk menghindari atau meminimalkan serangan terhadap dirinya serta mampu melakukan pengobatan jika terinfeksi.



## BAB I PENDAHULUAN

### 1.1 Latar Belakang Masalah

Perkembangan teknologi informasi yang sangat pesat khususnya teknologi Internet, menyebabkan teknologi ini menjadi salah satu media utama pertukaran informasi. Tidak semua informasi dalam Internet bersifat terbuka, sedangkan Internet sendiri merupakan jaringan komputer yang bersifat publik. Dengan demikian diperlukan usaha untuk menjamin keamanan informasi terhadap komputer yang terhubung dengan jaringan Internet.

Dalam jaringan Internet terdapat dua sisi yang saling bertentangan dalam hal akses informasi. Di satu sisi, banyak usaha-usaha dilakukan untuk menjamin keamanan suatu sistem informasi, di sisi lain ada pihak-pihak dengan maksud tertentu yang berusaha untuk melakukan eksploitasi sistem keamanan tersebut. Eksploitasi keamanan adalah berupa serangan terhadap keamanan sistem informasi. Bentuk serangan tersebut dapat dikelompokkan dari hal yang ringan, misalnya hanya mengesalkan sampai dengan yang sangat berbahaya.

Salah satu bentuk eksploitasi keamanan sistem informasi adalah dengan adanya infeksi digital. Virus, Worm, Trojan Horse adalah bagian dari infeksi digital yang merupakan ancaman bagi pengguna komputer, terutama yang terhubung dengan Internet. Infeksi digital disebabkan oleh suatu perangkat lunak yang dibuat atau ditulis seseorang dengan tujuan untuk menjalankan aksi-aksi yang tidak diinginkan oleh pengguna komputer. *Software* tersebut sering disebut dengan *Malicious software* (disingkat dengan “*malware*”). *Malicious software* mempunyai arti program pendendam atau program jahat. Aksi *malicious software* tergantung selera pembuatnya [3][9].

Trojan Horse atau disebut dengan Trojan adalah bagian dari *malicious software* yang terdiri dari fungsi-fungsi yang tidak diketahui tujuannya, tetapi secara garis besar mempunyai sifat merusak. Trojan memang tidak membawa pengaruh secara langsung seperti halnya virus, namun potensi bahayanya dapat jauh lebih besar.



Oleh karena itu diperlukan pemahaman dan pengetahuan tentang Trojan dalam konteks keamanan (*security*) agar luput dari bahaya yang ditimbulkannya. Jika hal tersebut tidak dikuasai maka yang akan dirasakan adalah kekhawatiran dan rasa takut saat terhubung dengan Internet.

## 1.2 Tujuan

Berdasarkan latar belakang di atas, maka pembuatan paper tugas akhir EC 7010 ini bertujuan untuk :

1. mempelajari dan memahami hal-hal yang berkaitan dengan Trojan, yaitu cara kerja, jenis dan sumbernya,
2. memahami proses pendeteksian keberadaan Trojan, melakukan penanganan dan pencegahan.

## 1.3 Sistematika Penulisan

Sistematika pembahasan di dalam tesis ini adalah sebagai berikut.

### 1. BAB I. Pendahuluan

Dalam bab ini berisi latar belakang perlunya dilakukan penulisan paper, tujuan penulisan dan sistematika penulisan.

### 2. BAB II. Pengertian Umum Trojan

Bagian ini membahas tentang hal-hal yang berkaitan dengan Trojan, yaitu jenis-jenis Trojan, cara kerja Trojan, sumber-sumber Trojan, *port* yang digunakan berbagai macam Trojan dan motivasi penyerang.

### 3. BAB III. Deteksi Trojan dan Penanganannya

Bagian ini berisi cara pendeteksian Trojan, penghapusan Trojan, Anti Virus Scanner, Anti Trojan *Software* dan penanganan pasca terinfeksi Trojan.

### 4. BAB IV. Analisis dan Kesimpulan

Bagian ini berisi analisis dan kesimpulan penulisan yang berasal dari pembahasan bagian sebelumnya.



## BAB II

### PENGERTIAN UMUM TROJAN

Istilah Trojan Horse (Kuda Troya) berasal dari mitologi Yunani pada saat perang Troya. Dalam peperangan tersebut pasukan Yunani melawan pasukan kerajaan Troya. Pasukan Yunani telah mengepung kota Troya selama sepuluh tahun, namun karena pasukan kerajaan Troya cukup tangguh, maka pasukan Yunani sulit mengalahkannya. Akhirnya, pasukan Yunani membuat strategi yaitu dengan membuat sebuah kuda raksasa yang terbuat dari kayu. Kuda dari kayu ini cukup unik, di dalamnya berongga sehingga dapat diisi pasukan Yunani. Pasukan Yunani pura-pura mundur dan sambil memberikan hadiah kuda kayu raksasa tersebut. Dengan bantuan seorang spionase Yunani yang bernama Sinon, penduduk kota Troya berhasil diyakinkan untuk menerima kuda kayu raksasa itu dan memasukkannya ke dalam kota. Pada malam harinya, pasukan Yunani yang berada di dalam kuda kayu keluar, kemudian membuka gerbang dan kota Troya diserang. Dengan cara tersebut kota Troya dapat dikuasai oleh Yunani [9].

Kisah epik di atas telah mengilhami para *hacker* untuk menciptakan “penyusup” ke komputer orang lain yang disebut dengan Trojan Horse. Trojan pada saat ini berkaitan dengan masalah keamanan komputer yang cukup serius. Trojan dapat masuk ke komputer dengan melalui beberapa cara dan dari berbagai sumber yang kurang dapat dipercaya di Internet atau dari orang lain [1].

Seperti halnya virus, jumlah trojan yang semakin lama semakin bertambah banyak, karena *hacker* atau pembuat program Trojan (*programmer*) yang selalu bereksperimen untuk mengembangkannya. Trojan tidak mempunyai masa aktif, maksudnya Trojan akan ada selamanya (bersarang) dan tidak pernah akan habis. Ada banyak hal yang dapat dikembangkan oleh *programmer* agar program yang dibuat tidak terdeteksi oleh *anti-virus* atau *trojan scanner*. *Programmer* akan selalu bereksperimen untuk menciptakan Trojan yang unik dengan fungsi-fungsi baru dengan metode enkripsi yang lebih hebat [7].

Secara teknis, Trojan dapat muncul di mana saja dan kapan saja, di sistem operasi manapun dan berbagai *platform*. Kecepatan peredaran Trojan secepat virus. Secara



umum Trojan berasal dari program-program yang di *download* dari Internet, terutama *freeware* atau *shareware* yang mencurigakan dan tidak berasal dari situs aslinya [7].

Salah satu indikasi komputer yang terinfeksi oleh Trojan dapat digambarkan sebagai berikut. Pada saat komputer terhubung dengan Internet, misalnya saat mengobrol (*chatting*) atau memeriksa *e-mail*, tetapi hardisk bekerja dengan sibuk (*busy*) dalam waktu yang lama. Selain itu pemakai juga tidak sedang menjalankan program aplikasi besar atau men-*download* sesuatu yang mengharuskan piringan hardisk berputar cukup lama. Kejadian tersebut termasuk kejadian aneh yang patut dicurigai adanya penyusupan [10].

## 2.1 Definisi Trojan

Trojan di dalam sistem komputer adalah suatu program yang tidak diharapkan dan disisipkan tanpa sepengetahuan pemilik komputer. Program ini kemudian dapat diaktifkan dan dikendalikan dari jarak jauh, atau dengan menggunakan *timer* (pewaktu). Akibatnya, komputer yang disisipi Trojan Horse tersebut dapat dikendalikan dari jarak jauh [5] [6] [9].

Definisi lain mengatakan bahwa Trojan adalah program apapun yang digunakan untuk melaksanakan suatu fungsi penting dan diharapkan oleh pemakai, namun kode dan fungsi di dalamnya tidak dikenal oleh pemakai. Selanjutnya program melaksanakan fungsi tak dikenal dan dikendalikan dari jarak jauh yang tidak dikehendaki oleh pemakai [8].

## 2.2 Fungsi Trojan

Trojan bersembunyi di latar belakang dengan cara membuka *port* tertentu dan menunggu diaktifkan oleh penyerang. Komputer yang telah terinfeksi dapat dikendalikan oleh penyerang melalui versi *client*-nya [10].

Cara kerja Trojan mirip dengan *remote administration tool*, dengan sifat dan fungsi yang sama. Program *remote administration* misalnya *pcAnywhere*, digunakan untuk keperluan yang benar dan sah (*legitimate*), sedangkan Trojam digunakan untuk keperluan yang negatif [5].



Jika sebuah komputer terinfeksi oleh Trojan dan telah dikendalikan oleh penyerangnya, maka beberapa kemungkinan dapat terjadi. Sebagai contoh, sebuah Trojan dengan nama NetBus dapat melakukan banyak hal ke komputer yang telah dikendalikan antara lain : [10]

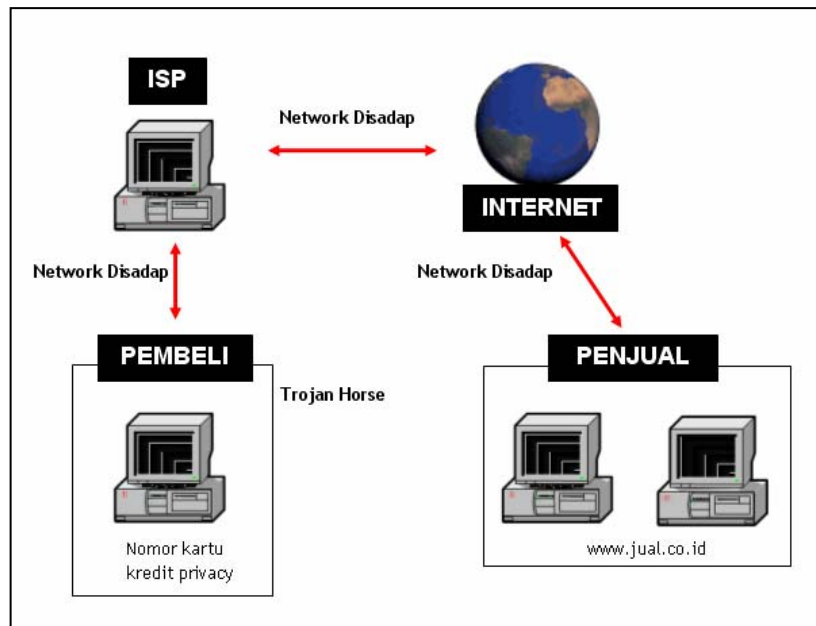
- menghapus *file*,
- mengirim dan mengambil *file*,
- menjalankan program-program aplikasi,
- menampilkan gambar,
- mengintip program-program yang sedang dijalankan,
- menutup program-program yang dijalankan,
- melihat apa saja yang sedang diketik,
- membuka dan menutup CD-ROM drive,
- mengirim pesan dan mengajak untuk bicara (*chat*),
- mematikan komputer.

Contoh di atas adalah hanya sebagian yang dapat dikerjakan oleh sebuah Trojan. Trojan lain kemungkinan mempunyai fungsi yang berbeda bahkan mungkin lebih berbahaya dan lebih susah dideteksi.

Dalam aplikasi belanja *online*, Trojan adalah salah satu ancaman bagi penjual dan pembeli. Trojan dapat digunakan untuk mencuri nomor kartu kredit dengan cara menangkap ketikan saat dilakukan proses transaksi *online* [6].

Cara lain adalah memanfaatkan lubang keamanan pada operating system di sisi penjual atau pemberi jasa (*server*) dimanfaatkan untuk menyadap data-data pelanggannya (*client*). Jika lubang ini dieksploitasi, kemungkinan data seluruh pelanggan dari *server* tersebut jatuh ke tangan penyadap [6].

Contoh dari penyusupan Trojan dalam belanja *online* terdapat dalam Gambar 2.1.



Gambar 2.1 Penyusupan Trojan dalam Belanja *Online* <sup>[6]</sup>

### 2.3 Cara Kerja Trojan

Trojan masuk melalui dua bagian, yaitu bagian *client* dan *server*. Ketika korban (tanpa diketahui) menjalankan komputer, kemudian penyerang akan menggunakan *client* untuk koneksi dengan *server* dan mulai menggunakan trojan. Protokol TCP/IP adalah jenis protokol yang umum digunakan untuk komunikasi. Trojan dapat bekerja dengan baik dengan jenis protokol ini, tetapi beberapa trojan juga dapat menggunakan protokol UDP dengan baik. Ketika *server* mulai dijalankan (pada komputer korban), Trojan umumnya mencoba untuk menyembunyikan diri di suatu tempat dalam sistem komputer tersebut, kemudian mulai “mendengarkan” di beberapa *port* untuk melakukan koneksi, memodifikasi *registry* dan atau menggunakan metode lain yaitu metode *autostarting* [8].

Hal yang penting untuk diketahui oleh penyerang adalah mengetahui IP *address* korban untuk menghubungkan komputernya ke komputer korban. Banyak varian Trojan mempunyai kemampuan mengirimkan IP *address* korban ke penyerangnya, misalnya media ICQ maupun IRC. Hal ini digunakan bagi korban yang mempunyai



IP *address* dinamis, yang berarti setiap kali menghubungkan ke Internet didapatkan IP *address* yang berbeda. Untuk pemakai yang memanfaatkan Asymmetric Digital Subscriber Line (ADSL) berarti selalu memakai IP *address* yang tetap (statis) sehingga mudah diketahui dan mudah untuk dikoneksikan dengan komputer penyerang [8].

Sebagian besar Trojan menggunakan metode *auto-starting*, yaitu Trojan akan secara otomatis aktif saat komputer dihidupkan. Walaupun komputer dimatikan dan kemudian dihidupkan lagi, Trojan mampu bekerja kembali dan penyerang mengakses kembali ke komputer korban [8].

Metode baru *auto-starting* dan trik lain telah ditemukan sejak semula. Jenis Trojan ini bekerja mulai dari koneksi trojan ke dalam beberapa *file executable* yang sering digunakan misalnya explorer.exe dan kemudian memodifikasi *file* sistem atau Windows Registry. *File* sistem ditempatkan di direktori Windows. Dari direktori ini penyerang melaksanakan penyerangan atau penyalahgunaan. Penyalahgunaan penyerang melewati *file* sistem adalah sebagai berikut [8].

- Autostart Folder.  
Autostart folder berada di lokasi C:\Windows\Start Menu\Programs\Startup dan sesuai dengan namanya akan bekerja secara otomatis bagia *file* sistem yang ditempatkan di folder tersebut.
- Win.Ini.  
*File* sistem Windows menggunakan load=trojan.exe dan run=trojan.exe untuk menjalankan Trojan.
- System.Ini.  
Menggunakan shell=explorer.exe trojan.exe. Hal ini diakibatkan oleh eksekusi setiap *file* setelah menjalankan explorer.exe.
- Wininit.Ini.  
Sebagian besar *setup* program menggunakan *file* ini. Sekali dijalankan maka menjadi *auto-delete*, akibatnya Trojan sangat cekatan atau cepat untuk bekerja kembali.



- **Winstart.Bat.**  
Bertindak seperti *batch file* yang normal, ketika ditambahkan@ trojan.exe mampu menyembunyikan korbannya.
- **Autoexec.Bat.**  
Autoexec.Bat adalah *file auto-starting Disk Operating System (DOS)*. File tersebut digunakan sebagai metode *auto-starting*, yaitu dengan memasang `c:\trojan.exe`.
- **Config.Sys.**  
Config.Sys juga dapat digunakan sebagai suatu metode *auto-starting* untuk Trojan.
- **Explorer Startup.**  
Explorer Startup adalah suatu metode *auto-starting* untuk Windows95, 98, ME dan jika `c:\explorer.exe` ada, hal itu akan dimulai maka akan menggantikan yang umum, yaitu `c:\Windows\Explorer.exe`.

*Registry* sering digunakan dalam berbagai metode *auto-starting*. *Registry* sebagai jalan untuk *auto-starting* yang diketahui antara lain: [7]

- [HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]  
"Info"="c:\directory\Trojan.exe"
- [HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce]  
"Info"="c:\directory\Trojan.exe"
- [HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices]  
"Info"="c:\directory\Trojan.exe"
- [HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce]  
"Info"="c:\directory\Trojan.exe"
- [HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run]  
"Info"="c:\directory\Trojan.exe"
- [HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce]  
"Info"="c:\directory\Trojan.exe"



- Registry Shell Open

```
[HKEY_CLASSES_ROOT\exefile\shell\open\command]
[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\exefile\shell\open
\command]
```

Suatu kunci dengan nilai "% 1%\*" harus ditempatkan disana dan jika terdapat beberapa *file* yang *executable*. Setiap kali *file* dieksekusi maka akan membuka suatu *binary file*. Jika di *registry* ini terdapat trojan.exe "% 1%\*", maka akan digunakan sebagai *auto-starting* untuk Trojan.

- Metode Deteksi ICQ Net

```
[HKEY_CURRENT_USER\Software\Mirabilis\ICQ\Agent\Apps\]
```

Kunci dari metode ini adalah semua *file* akan dieksekusi jika ICQ mendeteksi koneksi Internet. Perlu diketahui, bahwa cara kerja dari ICQ adalah sangat mudah dan sering digunakan pemakai, sehingga ICQ dimanfaatkan oleh penyerang mediana.

- ActiveX Component

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Active Setup
\Installed Components\KeyName]
StubPath=C:\directory\Trojan.exe
```

## 2.4 Jenis jenis Trojan

Trojan seperti halnya virus, mempunyai jumlah yang cukup banyak dan berkembang seiring dengan berjalannya waktu. Terdapat kurang lebih 650 buah Trojan yang telah beredar saat ini [4]. Pendapat lain mengatakan bahwa di tahun 2002 sudah terdapat sekitar 800 buah Trojan [7]. Jumlah tersebut adalah jumlah yang diketahui atau terdeteksi keberadaannya, sedangkan yang tidak terdeteksi tidak diketahui jumlahnya.

Dari berbagai macam Trojan yang telah beredar dan menginfeksi pemakai Internet, dapat diklasifikasikan berdasarkan ciri-cirinya. Menurut Dancho Danchev (2004), Trojan dapat diklasifikasikan menjadi delapan jenis, antara lain sebagai berikut.



### 2.4.1 Trojan Remote Access

Trojan Remote Access termasuk Trojan paling populer saat ini. Banyak penyerang menggunakan Trojan ini dengan alasan fungsi yang banyak dan sangat mudah dalam penggunaannya. Prosesnya adalah menunggu seseorang menjalankan Trojan yang berfungsi sebagai *server* dan jika penyerang telah memiliki IP *address* korban, maka penyerang dapat mengendalikan secara penuh komputer korban. Contoh jenis Trojan ini adalah Back Orifice (BO), yang terdiri dari BOSERVE.EXE yang dijalankan di komputer korban dan BOGUI.EXE yang dijalankan oleh penyerang untuk mengakses komputer korban.

### 2.4.2 Trojan Pengirim Password

Tujuan dari Trojan jenis ini adalah mengirimkan *password* yang berada di komputer korban atau di Internet ke suatu *e-mail* khusus yang telah disiapkan. Contoh *password* yang disadap misalnya untuk ICQ, IRC, FTP, HTTP atau aplikasi lain yang memerlukan seorang pemakai untuk masuk suatu *login* dan *password*. Kebanyakan Trojan ini menggunakan *port 25* untuk mengirimkan *e-mail*. Jenis ini sangat berbahaya jika dalam komputer terdapat *password* yang sangat penting.

### 2.4.3 Trojan File Transfer Protocol (FTP)

Trojan FTP adalah paling sederhana dan dianggap ketinggalan jaman. Satu-satunya fungsi yang dijalankan adalah membuka *port 21* di komputer korban yang menyebabkan mempermudah seseorang memiliki FTP *client* untuk memasuki komputer korban tanpa *password* serta melakukan *download* atau *upload file*.

### 2.4.4 Keyloggers

Keyloggers termasuk dalam jenis Trojan yang sederhana, dengan fungsi merekam atau mencatat ketukan tombol saat korban melakukan pengetikan dan menyimpannya dalam *logfile*. Apabila diantara ketukan tersebut adalah mengisi *user name* dan *password*, maka keduanya dapat diperoleh penyerang dengan membaca *logfile*. Trojan ini dapat dijalankan pada saat komputer *online* maupun *offline*.



Trojan ini dapat mengetahui korban sedang *online* dan merekam segala sesuatunya. Pada saat *offline* proses perekaman dilakukan setelah Windows dijalankan dan disimpan dalam hardisk korban dan menunggu saat *online* untuk melakukan transfer atau diambil oleh penyerang.

#### 2.4.5 Trojan Penghancur

Satu-satunya fungsi dari jenis ini adalah untuk menghancurkan dan menghapus *file*. Trojan penghancur termasuk jenis yang sederhana dan mudah digunakan, namun sangat berbahaya. Sekali terinfeksi dan tidak dapat melakukan penyelamatan maka sebagian atau bahkan semua *file* sistem akan hilang. Trojan ini secara otomatis menghapus semua *file* sistem pada komputer korban (sebagai contoh : \*.dll, \*.ini atau \*.exe). Trojan diaktifkan oleh penyerang atau bekerja seperti sebuah *logic bomb* dan mulai bekerja dengan waktu yang ditentukan oleh penyerang.

#### 2.4.6 Trojan Denial of Service (DoS) Attack

Trojan DoS Attack saat ini termasuk yang sangat populer. Trojan ini mempunyai kemampuan untuk menjalankan Distributed DoS (DDoS) jika mempunyai korban yang cukup. Gagasan utamanya adalah bahwa jika penyerang mempunyai 200 korban pemakai ADSL yang telah terinfeksi, kemudian mulai menyerang korban secara serempak. Hasilnya adalah lalu lintas data yang sangat padat karena permintaan yang bertubi-tubi dan melebihi kapasitas *band width* korban. Hal tersebut menyebabkan akses Internet menjadi tertutup. Wintrinoo adalah suatu *tool* DDoS yang populer baru-baru ini, dan jika penyerang telah menginfeksi pemakai ADSL, maka beberapa situs utama Internet akan *collaps*. Variasi yang lain dari sebuah trojan DoS adalah trojan *mail-bomb*, tujuan utamanya adalah untuk menginfeksi sebanyak mungkin komputer dan melakukan penyerangan secara serempak ke alamat *e-mail* yang spesifik maupun alamat lain yang spesifik dengan target yang acak dan muatan/isi yang tidak dapat disaring.



### 2.4.7 Trojan Proxy/Wingate

Bentuk dan corak yang menarik diterapkan oleh pembuat trojan untuk mengelabui korban dengan memanfaatkan suatu Proxy/Wingate *server* yang disediakan untuk seluruh dunia atau hanya untuk penyerang saja. Trojan Proxy/Wingate digunakan pada Telnet yang tanpa nama, ICQ, IRC, dan untuk mendaftarkan *domain* dengan nomor kartu kredit yang telah dicuri serta untuk aktivitas lain yang tidak sah. Trojan ini melengkapi penyerang dengan keadaan tanpa nama dan memberikan kesempatan untuk berbuat segalanya terhadap komputer korban dan jejak yang tidak dapat ditelusuri.

### 2.4.8 Software Detection Killers

Beberapa Trojan telah dilengkapi dengan kemampuan melumpuhkan fungsi *software* pendeteksi, tetapi ada juga program yang berdiri sendiri dengan fungsi yang sama. Contoh *software* pendeteksi yang dapat dilumpuhkan fungsinya adalah Zone Alarm, Norton Anti-Virus dan program *anti-virus/firewall* yang lain berfungsi melindungi komputer. Ketika *software* pendeteksi dilumpuhkan, penyerang akan mempunyai akses penuh ke komputer korban, melaksanakan beberapa aktivitas yang tidak sah, menggunakan komputer korban untuk menyerang komputer yang lain.

## 2.5 Sumber-sumber Trojan

Banyak pemakai komputer/Internet yang mempunyai sedikit pengetahuan tentang asal muasal sebuah Trojan, mereka beranggapan bahwa sumber Trojan hanya dari proses *download* dan menjalankan *server.exe*. Sebenarnya banyak jalan atau sumber Trojan untuk menginfeksi komputer seseorang yang berawal dari menggunakan Trojan untuk aktivitas yang tidak sah [8].

Komputer korban dapat disusupi Trojan dengan berbagai macam cara atau berasal dari sumber-sumber tertentu. Sumber-sumber tersebut adalah sebagai berikut [8].

### 2.5.1 ICQ

ICQ adalah media komunikasi yang populer, namun sebenarnya merupakan media yang sangat mungkin mengakibatkan seseorang terkena Trojan, terutama sewaktu



seseorang mengirimkan *file*. Terdapat bug pada ICQ yang memungkinkan seseorang mengirimkan *file* \*.exe ke orang lain, namun *file* tersebut akan seperti *file* \*.bmp atau \*.jpg atau jenis *file* lain sesuai keinginan. Hal ini sangat berbahaya, pengirim dapat mengirimkan *file* \*.exe tetapi dengan bentuk \*.jpg atau \*.bmp dan mengatakan bahwa ini foto si pengirim. Penerima akan menerima *file* tersebut dan menjalankannya dengan rasa aman, karena *file* yang diterima berupa *file* gambar. Jika pengirim adalah seorang penyerang, maka dengan mudah menyusupkan *file* Trojan ke dalam komputer penerima (korban). Hal inilah yang menyebabkan orang ragu menggunakan ICQ.

### 2.5.2 IRC

Media yang digemari banyak orang adalah chatting menggunakan IRC. Seperti halnya ICQ, IRC media penyebaran Trojan yang efektif. Cara yang digunakan juga hampir sama dengan ICQ, yaitu dengan cara mengirimkan *file-file* tertentu yang menarik bagi pemakai IRC dan di dalam *file* tersebut telah disisipkan program Trojan. Tawaran dari pengirim yang sekaligus sebagai penyerang misalnya dengan hal-hal yang bersifat pornografi, *software* untuk melakukan akses Internet secara bebas, hacking program Hotmail dan sebagainya. Target utama penyerang biasanya adalah pemakai baru Internet (*newbies*) maupun pemakai lama tetapi belum mengetahui tentang keamanan dalam berinternet.

### 2.5.3 Attachment

*Attachment* dalam *e-mail* juga merupakan media penyebaran Trojan. Banyak penyerang menggunakan media *attachment*, karena media ini adalah salah satu media yang efektif untuk menyerang korban secara massal dengan cara mengirimkan *e-mail*. *Attachment* yang dikirimkan berisi hal-hal yang menarik misalnya pornografi, layanan bebas berinternet, *password* dan sebagainya. Selain dengan cara tersebut, penyerang juga menggunakan cara lain yaitu dengan menyadap *e-mail address* dan *attachment* dari seseorang yang sedang mengirimkan *e-mail* ke temannya. Setelah disadap oleh penyerang, *attachment* disisipi program Trojan dan kemudian dikirimkan ke target *e-mail*. Penerima *e-mail* akan merasakan



bahwa *e-mail* yang dikirimkan berasal dari temannya dan tanpa ragu-ragu membuka *attachment* yang telah tersisipi Trojan.

#### 2.5.4 Physical Access

Akses fisik dalam komputer adalah hal yang sangat vital. Media akses fisik adalah dengan disket, Compact Disc (CD) maupun flash ROM. Dengan media tersebut, Trojan dapat menyusup ke dalam komputer dan dapat mengaktifkan dirinya ketika terkoneksi dengan Internet. Caranya adalah dengan menyebar melalui komputer yang telah terinfeksi, kemudian komputer digunakan untuk meng-*copy file* ke dalam media. Selanjutnya *file* yang berada dalam media di-*copy*kan lagi ke komputer lain, sehingga komputer tersebut juga terinfeksi. Cara lainnya adalah dengan memanfaatkan fasilitas *autorun* dalam fungsi pembacaan CD. Saat CD dimasukkan ke CDROM drive, secara otomatis akan membaca fasilitas *autorun* yang berada dalam *Autorun.inf* dalam CD, yaitu :

```
[autorun]
open=setup.exe
icon=setup.exe
```

Jika sebuah CD dengan fasilitas *autorun* dan telah disisipi program Trojan, maka sangat mudah bagi penyerang untuk menyusupkan Trojan ke dalam komputer orang lain.

#### 2.5.5 Lubang Software Browser dan E-mail

Dalam penggunaan *software* aplikasi untuk browser dan *e-mail*, seringkali pemakai tidak memperhatikan masalah *update software*. Pemakai enggan memperbaharui versi *softwarena* padahal mereka seharusnya melakukan *update* setiap saat. Hal ini membawa keuntungan bagi penyerang karena pemakaian *software* versi lama lebih mudah untuk disusupi. *Software* versi lama tentunya mempunyai banyak kelemahan atau bug jika dibandingkan dengan versi barunya. Misalnya kasus pemakaian *software* versi lama Internet Explorer yang digunakan untuk mengunjungi sebuah situs *malicious*, kemudian secara otomatis menginfeksi komputer tanpa melakukan proses *download* atau menjalankan program apapun. Situs *malicious* tersebut akan memeriksa secara otomatis *software* yang digunakan dan mencari kelemahannya.



Hal yang sama juga terjadi dalam pemakaian *software* untuk memeriksa *e-mail* misal pemakaian Outlook Express versi lama. Oleh karena itu, *update software* atau menggunakan *software* versi terbaru perlu dilakukan. Hal ini dapat menekan atau meminimalkan kemungkinan terinfeksi komputer yang melewati *software browser* dan *e-mail*.

### **2.5.6 Netbios (File Sharing)**

*File sharing* dapat dilakukan dengan cara membuka *port* 139 . Jika *port* tersebut terbuka dan diketahui oleh penyerang, maka dapat digunakan sebagai jalan untuk menyusupkan Trojan. Caranya adalah dengan meng-*install* trojan.exe dan memodifikasi *file* sistem di komputer korban. Trojan yang telah disisipkan akan aktif setiap kali komputer dihidupkan.

Kadang-kadang penyerang juga melengkapi dengan DoS yang digunakan melumpuhkan kerja komputer. Komputer dipaksa untuk *booting* ulang, sehingga Trojan dapat mengaktifkan sendiri bersama proses *booting*.

## **2.6 Program Gadungan, Situs Yang Tidak Dapat Dipercaya dan Software Freeware**

Dari keterangan sebelumnya telah dijelaskan tentang sumber-sumber Trojan yang digunakan sebagai media penyebarannya. Beberapa cara dilakukan oleh penyerang untuk mengelabui korbannya saat menggunakan Internet. Tawaran yang dilakukan untuk mengelabui adalah dengan menggunakan program gadungan (*fake program*), situs yang tidak dapat dipercaya (*untrusted sites*) dan *software* yang didapatkan secara gratis (*freeware*). Pemakai komputer perlu berhati-hati dengan tawaran tersebut. Sebagai contoh dari ketiga tawaran diatas adalah sebagai berikut [7].

1. Pemanfaatan fasilitas *freeware* SimpleMail. *Software* ini sengaja dibuat menarik namun didalamnya telah disisipi Trojan. Komputer korban yang telah diproteksi dengan *software* proteksi tetapi tidak dapat mendeteksi keberadaan Trojan. Saat SimpleMail digunakan, maka fungsi Trojan yang tersembunyi akan membuka *port* 25 atau 110 untuk POP 3 dan menghubungkan komputer korban ke komputer penyerang. Selanjutnya penyerang dapat menyadap



apapun yang diketik korban, misalnya nomor kartu kredit, *user id*, *password* dan sebagainya. Selanjutnya data-data tersebut digunakan oleh penyerang untuk aktivitas yang tidak sah.

2. Pemanfaatan fasilitas *free web space*. Fasilitas ini memungkinkan seseorang untuk menempatkan situsnya secara gratis. Penyedia layanan ini misalnya Xoom, Tripod dan Geocities. Banyak pemakai yang memanfaatkan layanan ini, termasuk para *hacker* yang memanfaatkan fasilitas ini sebagai media penyebaran Trojan. Melakukan *download* menjadi berbahaya jika situs di layanan ini telah terinfeksi oleh Trojan.
3. *Download* untuk mendapatkan *software freeware*. Dalam mendapatkan *software* yang gratis perlu dipertimbangkan, karena dengan media ini Trojan dapat disusupkan. Ada pepatah bahwa “gratis tidak selalu yang terbaik”. Jika memang diperlukan, maka perlu dipastikan bahwa *file* di-*download* dari sumber aslinya.

## 2.7 Port Yang Digunakan Trojan

Trojan sesuai dengan fungsinya akan membuka pintu belakang berupa *port* dengan nomor tertentu. Adanya *port* yang tidak lazim terbuka mengindikasikan adanya kegiatan aktif Trojan [7].

*Port-port* yang telah diketahui sebagai media koneksi trojan terlampir pada lampiran Trojan Port List yang diambil dari sumber <http://www.glocksoft.com>, pada tanggal 11 September 2004.

## 2.8 Apa Yang Dicari Penyerang

Sebagian pemakai Internet beranggapan bahwa Trojan hanya bersifat merusak saja. Anggapan tersebut tidak benar, karena Trojan dapat digunakan alat untuk mata-mata dan melakukan penyadapan pada beberapa komputer korban. Data yang disadap berupa data pribadi maupun informasi yang sensitif (misalnya spionase dalam industri) [8].



Contoh hal-hal yang diminati penyerang adalah sebagai berikut [8].

- Informasi Kartu Kredit.
- Data akuntansi (*e-mail passwords*, *dial-up passwords* dan *webservices passwords*).
- *E-mail Addresses*.
- *Work Projects* (dokumen pekerjaan).
- Nama anak-anak dengan foto dan umurnya.
- Dokumen sekolah.



## BAB III

### DETEKSI TROJAN DAN PENANGANANNYA

Dalam bab sebelumnya telah dipaparkan tentang hal-hal yang berkaitan dengan Trojan. Selanjutnya dalam bab ini akan dibahas tentang pengamanan sistem yang membahas pendeteksian Trojan dan penanganannya.

Pada dasarnya, pengamanan sistem dapat dibedakan menjadi dua cara, yaitu pencegahan (*preventiv*) dan pengobatan (*recovery*). Keduanya dibedakan berdasarkan waktu terjadinya infeksi. Usaha pencegahan dilakukan sebelum terjadinya infeksi, yaitu usaha agar sistem tidak mempunyai lubang keamanan. Usaha pengobatan dilakukan setelah sistem terinfeksi, yaitu usaha untuk menutup lubang keamanan yang telah dieksploitasi dan menghilangkan penyebab infeksi [5].

#### 3.1 Deteksi Trojan

Kadang-kadang pemakai komputer menganggap normal perilaku komputer yang menjalankan program tertentu dan memakai hardisk dengan kapasitas yang besar. Bahkan tidak curiga karena telah terpasang *software anti-virus* yang dianggap telah mampu menangkal keberadaan Trojan. Banyak yang mengira bahwa dengan *anti-virus* yang selalu di *update* dari situs pembuatnya, maka pemakai telah aman dari masalah di Internet dan tidak akan terinfeksi trojan atau komputernya diakses orang lain. Anggapan tersebut tidak benar, karena banyak jalan dilakukan oleh penyerang untuk menyusup ke komputer korban [7].

Tanda-tanda terserangnya komputer oleh Trojan dapat diketahui dengan melihat perilaku tampilan komputer dan melakukan deteksi dengan *anti-virus* maupun *trojan scanner*. Tanda-tanda yang diperlihatkan oleh tampilan komputer dan patut dicurigai adalah sebagai berikut [1][8].

- Saat mengunjungi suatu situs, terdapat beberapa *pop-up* yang muncul dan telah mengunjungi salah satu *pop-up*. Tetapi ketika akan mengakhiri kunjungan (tidak sepenuhnya dikunjungi), tiba-tiba *browser* mengarahkan dan membuka secara otomatis beberapa halaman tidak dikenal.



- Tampilan Kotak Pesan yang tak dikenal dan tampak di layar monitor. Pesan berisi beberapa pertanyaan yang bersifat pribadi.
- Tampilan Windows mengalami perubahan dengan sendirinya, misalnya teks *screensaver* yang baru, tanggal/waktu, perubahan volume bunyi dengan sendirinya, pointer mouse bergerak sendirinya, CD-ROM drive membuka dan menutup sendiri.
- Outlook Express menggunakan waktu yang cukup lama saat menutup (*close*) atau terlihat *hang* (menggantung) ketika melihat *preview*-nya,
- Adanya *file* yang rusak atau hilang,
- Program yang tidak diketahui aktif terlihat di *task list*,
- Tanda atau informasi dari *firewall* tentang *outbound* komunikasi dari sumber yang tidak diketahui.

Sebagian tanda-tanda diatas biasanya dilakukan oleh penyerang tingkat pemula dengan ciri memberikan tanda atau pesan di layar monitor. Hal ini berbeda dengan penyerang tingkat lanjut, ia akan berusaha untuk menutupi dirinya dan menghilangkan jejaknya saat melakukan penyusupan. Penyerang tingkat lanjut melakukan penyadapan dan menggunakan komputer yang infeksi untuk beberapa alasan yang spesifik, serta tidak menggunakan cara-cara seperti penyerang tingkat pemula. Sehingga aktivitasnya diam-diam dan tidak mencurigakan.

Pendeteksian Trojan dapat dilakukan dengan cara-cara sebagai berikut [1].

#### 1. Task List

Cara pendeteksiannya adalah dengan melihat daftar program yang sedang berjalan dalam *task list*. Daftar dapat ditampilkan dengan menekan tombol CTRL+ALT+DEL. Selain dapat mengetahui program yang berjalan, pemakai dapat melakukan penghentian terhadap suatu program yang dianggap aneh dan mencurigakan. Namun beberapa Trojan tetap mampu menyembunyikan dari *task list* ini. Sehingga untuk mengetahui secara program yang berjalan secara keseluruhan perlu dibuka System Information Utility (*msinfo32.exe*) yang berada di C:\Program files\common files\microsoft shared\msinfo. *Tool* ini dapat melihat semua proses itu sedang berjalan, baik yang



tersembunyi dari *task list* maupun tidak. Hal-hal yang perlu diperiksa adalah path, nama *file*, properti *file* dan berjalannya *file \*.exe* serta *file \*.dll*.

## 2. Netstat

Semua Trojan membutuhkan komunikasi. Jika mereka tidak melakukan komunikasi berarti tujuannya sia-sia. Hal ini adalah kelemahan yang utama dari Trojan, dengan komunikasi berarti mereka meninggalkan jejak yang kemudian dapat ditelusuri. Perintah Netstat berfungsi membuka koneksi ke dan dari komputer seseorang. Jika perintah ini dijalankan maka akan menampilkan IP *address* dari komputer tersebut dan komputer yang terkoneksi dengannya. Jika ditemukan IP *address* yang tidak dikenal maka perlu diselidiki lebih lanjut, mengejar dan menangkapnya.

## 3. TCP View

TCPVIEW adalah suatu *free utility* dari Sysinternals yang mempunyai kemampuan menampilkan IP *address* dan menampilkan program yang digunakan oleh orang lain untuk koneksi dengan komputer pemakai. Dengan menggunakan informasi tersebut, maka jika terjadi penyerangan dapat diketahui dan dapat melakukan serangan balik.

### 3.2 Menghapus Trojan

Trojan sering memodifikasi *file startup*, menambahkan atau mengubah baris di sistem *registry* dan bahkan melakukan *overwrite* terhadap sistem *file* untuk meyakinkan mereka dapat dijalankan setiap kali komputer *booting*. Dengan alasan tersebut, maka untuk menghapus Trojan diperlukan waktu yang cukup lama, kesabaran dan suatu pemahaman apa yang harus dilakukan. Proses menghapus Trojan adalah proses yang penuh dengan bahaya, termasuk membuang *registry* atau kehilangan kemampuan untuk menjalankan program [1].

Langkah-langkah sederhana yang dilakukan untuk menghapus Trojan dari komputer adalah : [8]

1. Mengidentifikasi *file* Trojan di dalam hardisk,



2. Menemukan bagaimana Trojan mengaktifkan dirinya dan mengambil tindakan yang perlu untuk mencegahnya berjalannya Trojan setelah *reboot*,
3. *Reboot* komputer dan menghapus Trojan,
4. Mengamati proses penyembuhan dari suatu halaman System Compromise dan membantu penyembuhannya.

Langkah di atas adalah salah satu pilihan untuk membuang Trojan dari komputer. Ada pendapat lain yang intinya juga menghapus keberadaan Trojan dengan beberapa pilihan. Pilihan-pilihan tersebut memang tidak sempurna, karena varian Trojan sangat banyak. Cara tersebut adalah sebagai berikut [3].

1. Membersihkan dengan cara instalasi ulang.
2. Pemakaian *Software Anti-Virus*.
3. Pemakaian *Software Trojan Scanner*.
4. Memanfaatkan bantuan dari *IRC Channels*.

### 3.2.1 Anti Virus (AV) Scanner

*Anti-virus* berfungsi untuk mendeteksi virus, bukan untuk mendeteksi Trojan. Namun ketika Trojan mulai populer dan menyebabkan banyak masalah, pembuat *anti-virus* menambahkan data-data trojan ke dalam *anti-virusnya*. *Anti-virus* ini tidak dapat mencari dan menganalisa Trojan secara keseluruhan. *Anti-virus* dapat mendeteksi Trojan berdasarkan nama-namanya yang telah dimasukkan ke database *anti-virus* [7][8].

*Anti-virus* juga tidak termasuk dalam kategori *firewall* yang mencegah seseorang yang tidak diundang mengakses komputer orang lain. Program *anti-virus* tidak dapat sepenuhnya melindungi sistem komputer seseorang dari serangan Trojan tetapi hanya meminimalkan kemungkinan itu [7].

### 3.2.2 Trojan Scanner

Sebagian *anti-virus* dapat mendeteksi keberadaan Trojan melalui pendeteksian nama-nama *filenya*. Pendeteksian yang efektif adalah menggunakan *Trojan Scanner*,



yang khusus digunakan untuk mendeteksi Trojan. Proses pendeteksian dilakukan dengan cara melakukan scanning terhadap *port-port* yang terbuka [7].

Trojan membuka *port* tertentu sebagai jalan belakang (*backdoor*) untuk menyerang targetnya. Salah satu contoh *trojan scanner* adalah Anti-Trojan. *Scanner* ini memeriksa Trojan dengan melakukan proses :

- *port scanning*,
- memeriksa *registry*,
- memeriksa hardisk.

Jika ditemukan adanya Trojan, maka dilakukan penanganan dengan beberapa pilihan untuk menghapus Trojan.

### **3.3 Penanganan Pengobatan (Recovery)**

Jika dalam suatu komputer telah ditemukan adanya hacking oleh Trojan, maka menghapus atau menutup fasilitas *sharing* tidaklah cukup. Karena suatu penyerang dapat dengan mudah menciptakan jalan lain (*backdoors*) ke dalam sistem atau memodifikasi sistem operasi untuk dirinya sendiri. Oleh karena itu hanya ada satu jalan yang nyata untuk mengamankan suatu yang sistem, yaitu meng-*install* ulang dengan menggunakan program yang asli [1].

Berikut ini akan disampaikan uraian langkah-langkah yang diperlukan dalam rangka pengobatan/penyembuhan suatu sistem. Langkah-langkah yang diperlukan adalah sebagai berikut [1]

1. Mengisolasi komputer yang telah terinfeksi.

Untuk mengisolasi komputer, maka semua hubungan dengan komputer tersebut harus diputuskan, baik dengan Internet maupun jaringan lokalnya. Melepaskan kabel jaringan dan mematikan kerja modem. Cara ini berarti memutuskan hubungan antara komputer dengan penyerang. Sebagian orang beranggapan bahwa membiarkan kabel tetap terpasang dan modem dalam kondisi *standby* telah mengisolasi suatu komputer. Dalam beberapa kasus anggapan tersebut adalah tidak benar. Sebab kondisi tersebut memungkinkan komputer tetap tersambung dengan jaringan.



2. Menemukan masalah-masalah yang serius.

Jika sebuah komputer terpasang dalam suatu jaringan maka ada beberapa resiko yang harus dihadapi. Resiko yang dihadapi mencakup :

- lamanya waktu eksploitasi keamanan yang tidak diketahui,
- tipe jaringan yang digunakan,
- pemakaian dan pemeliharaan *anti-virus* atau *firewall*,
- kepastian bahwa suatu program yang akan di-*install* belum dirubah.

3. Mengawali dengan proses pembersihan

Menggunakan dan memastikan bahwa program yang akan digunakan asli. Proses pembersihan diawali dengan *backup* data, kemudian format ulang hardisk dan *install* ulang program. Dalam penanganan *backup* data diperlukan prosedur :

- melepaskan hubungan dengan jaringan lain,
- meng-*copy file* data ke dalam disket atau CD, dan memastikan bahwa Program Files tidak ter-*copy*,
- memberikan label atau tulisan terhadap data yang telah terinfeksi dan menyimpan di tempat yang aman.

4. Mengamankan sistem dan menggunakan *software* tambahan

Setelah melakukan proses pembersihan, maka dalam komputer diperlukan tambalan keamanan dengan memasang *software anti-virus*, *trojan scanner* atau *firewall* mutakhir yang berfungsi mengamankan sistem. Sistem operasi yang digunakan menggunakan fasilitas *update* yang secara otomatis meng-*update* sistemnya.

5. *Restore backup* data

Setelah proses instalasi dan pengaturan semua *software* selesai, proses selanjutnya adalah menempatkan kembali data yang telah di *backup*. Sebelum data disimpan kembali ke komputer, perlu dilakukan pembersihan dan membuang semua bentuk infeksi. Setelah selesai, maka komputer siap digunakan lagi untuk berinternet. Banyak pengetahuan yang harus diketahui untuk memastikan bahwa selama memakai Internet terbebas dari serangan dari luar atau infeksi lain.



### 3.4 Pencegahan Agar Terhindar Dari Trojan

Beberapa cara dapat dilakukan untuk menghindari agar tidak terinfeksi Trojan. Salah satu cara masuk Trojan untuk menginfeksi suatu sistem adalah melewati *file* yang di *download*. Maka perlu ada perlakuan khusus dengan cara mengkarantina hasil *download* sebelum yakin bahwa *file* tersebut benar-benar aman [7].

Cara lain yang bersifat mencegah (*preventif*) dan merupakan informasi yang umum yang dapat dilakukan oleh seseorang yang menggunakan komputer untuk berinternet, adalah sebagai berikut [3].

1. Memilih situs yang benar-benar dapat dipercaya untuk melakukan *download*. Jangan pernah melakukan *download* secara sembarangan yang berasal dari seseorang atau situs yang tidak dapat dipercaya.
2. Memastikan bahwa *file* yang dikirimkan belum pernah dibuka oleh orang lain.
3. Mewaspada *file-file* yang ekstensinya disembunyikan.
4. Memastikan bahwa di dalam komputer tidak ada program yang berjalan secara otomatis atau mode *file preview*.
5. Jangan selalu merasa aman bila di komputer telah terpasang *software anti-virus/trojan scanner*,
6. Memastikan bahwa tidak melakukan *download* program *executable* “*check it out*”. Ini adalah sebuah Trojan. Jika program ini dijalankan, maka komputer telah terinfeksi Trojan.

Selain pengetahuan di atas, maka pengetahuan tentang proses berjalannya komputer juga perlu dipahami, khususnya saat sistem komputer menjalankan program untuk pertama kalinya. Dalam beberapa kasus, hal ini digunakan oleh Trojan untuk mengeksekusi dirinya. Paparan berikut sekaligus melengkapi bagian sebelumnya.



Cara komputer menjalankan program untuk pertama kalinya (secara otomatis) adalah sebagai berikut. [2]

1. Start Up Folder

Semua program yang berada di folder ini akan dijalankan secara otomatis ketika Windows dijalankan.

`C:\windows\start menu\program\startup`

Direktori tersebut tersimpan di dalam registry key :

`HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell`

2. Win.ini

```
[windows]
load=file.exe
run=file.exe
```

Pada *load* dan *run* dapat diisi dengan nama program yang akan dijalankan saat pertama kali Windows dijalankan.

3. System.ini [boot]

`Shell=Explorer.exe file.exe`

Nama program diletakkan setelah `explorer.exe`.

4. C:\windows\winstart.bat

Program yang dapat dijalankan di `winstart.bat` adalah yang mempunyai perilaku seperti *bat file*.

5. Registry

`[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunSevices]`

`[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce]`

`[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]`

`[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce]`

`[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]`

`[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce]`

`[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices]`



Program yang terdapat pada *registry key* di atas semuanya dijalankan saat pertama kali Windows berjalan.

#### 6. C:\windows\wininit.ini

Program ini digunakan untuk *setup*, yaitu akan dijalankan sekali lalu akan dihapus oleh Windows. Sebagai contoh isi dari *file* ini adalah :

```
[Rename]
```

```
NUL=c:\windows\file.exe
```

Perintah tersebut akan mengirim `c:\windows\file.exe` ke proses NUL, yang berarti dihapus. Ini tidak membutuhkan interaksi dari pemakai dan berjalan sepenuhnya di *background*.

#### 7. Autoexec.bat

Program ini akan berjalan secara otomatis dalam DOS *level*.

#### 8. Registry Shell Spawning

```
[HKEY_CLASSES_ROOT\exefile\shell\open\command]
@="\"%1"%"
```

```
[HKEY_CLASSES_ROOT\comfile\shell\open\command]
@="\"%1"%"
```

```
[HKEY_CLASSES_ROOT\batfile\shell\open\command]
@="\"%1"%"
```

```
[HKEY_CLASSES_ROOT\htafile\shell\open\command]
@="\"%1"%"
```

```
[HKEY_CLASSES_ROOT\piffile\shell\open\command]
@="\"%1"%"
```

```
[HKEY_LOCAL_MACHINE\Software\CLASSES\batfile\shell\open\
command] @="\"%1"%"
```

```
[HKEY_LOCAL_MACHINE\Software\CLASSES\comfile\shell\open\
command] @="\"%1"%"
```

```
[HKEY_LOCAL_MACHINE\Software\CLASSES\exefile\shell\open\
command] @="\"%1"%"
```

```
[HKEY_LOCAL_MACHINE\Software\CLASSES\htafile\shell\open\
command] @="\"%1"%"
```

```
[HKEY_LOCAL_MACHINE\Software\CLASSES\piffile\shell\open\
command] @="\"%1"%"
```

*Value key* yang sesungguhnya adalah `"\"%1"%"` , jika telah diubah menjadi

`"file.exe %1%"`, maka file yang berekstensi `exe/pif/com/bat/hta` akan



dijalankan. Sebagian Trojan juga menggunakan *registry* ini untuk mengaktifkan dirinya.

#### 9. ICQ Net

```
[HKEY_CURRENT_USER\Software\Mirabilis\ICQ\Agent\Apps\test]
"Path"="test.exe"
"Startup"="c:\test"
"Parameters"=""
"Enable"="Yes"
```

*Registry key* di atas akan dijalankan jika ICQ net mendeteksi adanya koneksi Internet.

#### 10. Lain-lain

```
[HKEY_LOCAL_MACHINE\Software\CLASSES\ShellScrap]
@"Scrap object" "NeverShowExt"=""
```

Bagian *key* "NeverShowExt" mempunyai fungsi menyembunyikan ekstensi aslinya. Hal ini dapat dimanfaatkan oleh Trojan untuk menyembunyikan dirinya.

Pemakai dapat melakukan pemeriksaan terhadap komputernya dengan cara melihat *setting* sistem saat pertama kali berjalan. Jika terdapat nama-nama *file* yang mencurigakan dan bukan merupakan bagian dari sistem yang diinginkan maka patut dicurigai.



## BAB IV ANALISIS DAN KESIMPULAN

### 4.1. Analisis

Dari paparan yang telah dituliskan di bagian sebelumnya, maka dapat dianalisis tentang hal-hal yang berkaitan dengan Trojan sebagai berikut.

1. Trojan termasuk dalam kategori program yang berbahaya. Hal ini berdasarkan fungsi-fungsi yang telah diketahui. Hal yang sederhana, misalnya hanya dengan indikasi pesan di layar monitor, tetapi sesungguhnya korban tidak tahu apa yang dikerjakan oleh penyerang di dalam komputernya. Bahkan penyerang yang lain tidak menampilkan sesuatupun dan berusaha untuk bersembunyi. Selanjutnya korban akan merasakan akibatnya secara langsung maupun tidak langsung.
2. Sesuai dengan fungsi Trojan yang telah diketahui, maka pemakai Internet perlu waspada dan hati-hati. Serangan Trojan mengakibatkan hal-hal yang sangat fatal, misalnya penghapusan file, melakukan format hardisk, mencuri informasi yang sensitif (nomor kartu kredit, *password*, *user id*, data perusahaan) dan sebagainya. Hilangnya informasi atau jatuhnya informasi ke orang lain akan menyebabkan kerugian yang besar bagi pemilik informasi.
3. Pemakai Internet perlu membentengi sistem komputernya dengan cara memasang penangkal serangan dengan versi terbaru (*trojan scanner* atau *firewall*) dan sistem operasi yang selalu dapat di *update* untuk mendapatkan penangkalan yang optimal. Selain itu, juga ditambahkan pengetahuan tentang seluk beluk Trojan dan setting sistem komputer untuk proses pencegahan dan pengobatan.
4. Diperlukan suatu prosedur khusus untuk menangani suatu sistem yang telah terinfeksi oleh Trojan.



## 4.2. Kesimpulan

Beberapa kesimpulan yang dapat diambil dari paper ini adalah :

1. Pemahaman tentang Trojan perlu diketahui oleh pemakai Internet, karena Trojan mempunyai potensi bahaya yang besar pada saat komputer terhubung dengan Internet maupun jaringan lokal. Pemahaman meliputi cara kerja, jenis, sumber dan motivasi penyerang. Dengan pengetahuan awal ini, pemakai dapat meminimalkan serangan terhadap dirinya.
2. Pemahaman untuk mendeteksi keberadaan Trojan sangat diperlukan, karena sebagian pemakai Internet tidak mengetahui bahwa komputernya telah terinfeksi Trojan dan lubang keamanannya telah dieksploitasi oleh penyerang. Pemahaman ini diharapkan mampu menghantarkan pemakai untuk dapat mendeteksi sekaligus menghilangkan pengaruh Trojan dari komputernya.
3. Pemahaman untuk pencegahan juga diperlukan untuk mencegah terinfeksinya kembali komputer oleh Trojan. Pengetahuan untuk pencegahan meliputi pemakaian operating sistem, pemasangan penangkal infeksi dan serangan (*anti-virus, trojan scanner* dan *firewall*), serta cara-cara yang baik saat berinternet. Dengan pengetahuan tersebut, pemakai komputer akan lebih berhati-hati dan teliti saat terkoneksi dengan Internet.



## DAFTAR PUSTAKA

- [1] -----, *Detecting and Removing Trojan Horse*, <http://www.nohack.net/trojans.htm>, 11 September 2004, 21.08 WIB.
- [2] -----, “Menjalankan Program Saat Pertama Kali Windows Dijalankan” *Neotek*, Vol. II - No.11, pp 37, 2002.
- [3] -----, *Trojan Horse Attack*, <http://www.irchelp.org/irchelp/security/trojan.html>, 11 September 2004, 19.51 WIB.
- [4] -----, *Trojan Port List*, [http://www.glocksoft.com/trojan\\_port.htm](http://www.glocksoft.com/trojan_port.htm), 11 September 2004, 19.46 WIB.
- [5] Budi Rahardjo, *Keamanan Sistem Informasi Berbasis Internet*, PT Insan Komunikasi Indonesia Bandung & PT INDOCISC Jakarta, 2002.
- [6] Budi Rahardjo, *Memahami Teknologi Informasi*, PT. Elex Media Komputindo, Jakarta, 2002.
- [7] David Sugianto, “Trojan Horse, Apakah Sebenarnya Kuda Yang Satu Ini?” *Neotek*, Vol. II - No.11, pp 16 – 19, 2002.
- [8] Danchev, Dancho, *The Complete Windows Trojans Paper*, [http://www.frame4.com/content/pubs/comp\\_trojans.pdf](http://www.frame4.com/content/pubs/comp_trojans.pdf), 12 September 2004, 09.10 WIB.
- [9] Happy Chandraleka, *Virus Worm dan Trojan Horse*, Penerbit Andi Yogyakarta, 2004.
- [10] Sitorus, Eryanto, *Teknik Penetrasi Kemampuan Hacker Untuk Menguji Sekuriti*, Penerbit Indah, Surabaya, 2004.

# LAMPIRAN

---

## TROJAN PORT LIST

Diambil dari sumber : [http://www.glocksoft.com/trojan\\_port.htm](http://www.glocksoft.com/trojan_port.htm)

Tanggal 11 September 2004.

**Default Port****Trojan Horse**

1 (UDP) - Sockets des Troie  
2 Death  
20 Senna Spy FTP server  
21 Back Construction, Blade Runner, Cattivik FTP Server, CC Invader, Dark FTP, Doly Trojan, Fore, Invisible FTP, Juggernaut 42, Larva, MotIv FTP, Net Administrator, Ramen, Senna Spy FTP server, The Flu, Traitor 21, WebEx, WinCrash  
22 Shaft  
23 Fire HackeR, Tiny Telnet Server - TTS, Truva Atl  
25 Ajan, Antigen, Barok, Email Password Sender - EPS, EPS II, Gip, Gris, Happy99, Hpteam mail, Hybris, I love you, Kuang2, Magic Horse, MBT (Mail Bombing Trojan), Moscow Email trojan, Naebi, NewApt worm, ProMail trojan, Shtirlitz, Stealth, Tapiras, Terminator, WinPC, WinSpy  
30 Agent 40421  
31 Agent 31, Hackers Paradise, Masters Paradise  
41 Deep Throat, Foreplay  
48 DRAT  
50 DRAT  
58 DMSetup  
59 DMSetup  
79 CDK, Firehotcker  
80 711 trojan (Seven Eleven), AckCmd, Back End, Back Orifice 2000 Plug-Ins, Cafeini, CGI Backdoor, Executor, God Message, God Message Creator, Hooker, IISworm, MTX, NCX, Reverse WWW Tunnel Backdoor, RingZero, Seeker, WAN Remote, Web Server CT, WebDownloader  
81 RemoConChubo  
99 Hidden Port, NCX  
110 ProMail trojan  
113 Invisible Identd Deamon, Kazimas  
119 Happy99  
121 Attack Bot, God Message, JammerKillah  
123 Net Controller  
133 Farnaz  
137 Chode  
137 (UDP) - Msinit  
138 Chode  
139 Chode, God Message worm, Msinit, Netlog, Network, Qaz  
142 NetTaxi  
146 Infector  
146 (UDP) - Infector  
170 A-trojan  
334 Backage  
411 Backage  
420 Breach, Incognito  
421 TCP Wrappers trojan  
455 Fatal Connections  
456 Hackers Paradise  
513 Grlogin  
514 RPC Backdoor  
531 Net666, Rasmin  
555 711 trojan (Seven Eleven), Ini-Killer, Net Administrator, Phase Zero, Phase-0, Stealth Spy  
605 Secret Service  
666 Attack FTP, Back Construction, BLA trojan, Cain & Abel, NokNok, Satans Back Door - SBD, ServU, Shadow Phyre, th3r1pp3rz (= Therippers)  
667 SniperNet  
669 DP trojan  
692 GayOL  
777 AimSpy, Undetected  
808 WinHole  
911 Dark Shadow  
999 Deep Throat, Foreplay, WinSatan  
1000 Der Späher / Der Spaeher, Direct Connection



1001 Der Späher / Der Spaeher, Le Gardien, Silencer, WebEx  
1010 Doly Trojan  
1011 Doly Trojan  
1012 Doly Trojan  
1015 Doly Trojan  
1016 Doly Trojan  
1020 Vampire  
1024 Jade, Latinus, NetSpy  
1025 Remote Storm  
1025 (UDP) - Remote Storm  
1035 Multidropper  
1042 BLA trojan  
1045 Rasmin  
1049 /sbin/initd  
1050 MiniCommand  
1053 The Thief  
1054 AckCmd  
1080 WinHole  
1081 WinHole  
1082 WinHole  
1083 WinHole  
1090 Xtreme  
1095 Remote Administration Tool - RAT  
1097 Remote Administration Tool - RAT  
1098 Remote Administration Tool - RAT  
1099 Blood Fest Evolution, Remote Administration Tool - RAT  
1150 Orion  
1151 Orion  
1170 Psyber Stream Server - PSS, Streaming Audio Server, Voice  
1200 (UDP) - NoBackO  
1201 (UDP) - NoBackO  
1207 SoftWAR  
1208 Infector  
1212 Kaos  
1234 SubSeven Java client, Ultors Trojan  
1243 BackDoor-G, SubSeven, SubSeven Apocalypse, Tiles  
1245 VooDoo Doll  
1255 Scarab  
1256 Project nEXT  
1269 Matrix  
1272 The Matrix  
1313 NETrojan  
1338 Millenium Worm  
1349 Bo dll  
1394 GoFriller, Backdoor G-1  
1441 Remote Storm  
1492 FTP99CMP  
1524 Trinoo  
1568 Remote Hack  
1600 Direct Connection, Shivka-Burka  
1703 Exploiter  
1777 Scarab  
1807 SpySender  
1966 Fake FTP  
1967 WM FTP Server  
1969 OpC BO  
1981 Bowl, Shockrave  
1999 Back Door, SubSeven, TransScout  
2000 Der Späher / Der Spaeher, Insane Network, Last 2000, Remote Explorer 2000, Senna Spy Trojan Generator  
2001 Der Späher / Der Spaeher, Trojan Cow  
2023 Ripper Pro  
2080 WinHole



2115 Bugs  
2130 (UDP) - Mini Backlash  
2140 The Invasor  
2140 (UDP) - Deep Throat, Foreplay  
2155 Illusion Mailer  
2255 Nirvana  
2283 Hvl RAT  
2300 Xplorer  
2311 Studio 54  
2330 Contact  
2331 Contact  
2332 Contact  
2333 Contact  
2334 Contact  
2335 Contact  
2336 Contact  
2337 Contact  
2338 Contact  
2339 Contact, Voice Spy  
2339 (UDP) - Voice Spy  
2345 Doly Trojan  
2565 Striker trojan  
2583 WinCrash  
2600 Digital RootBeer  
2716 The Prayer  
2773 SubSeven, SubSeven 2.1 Gold  
2774 SubSeven, SubSeven 2.1 Gold  
2801 Phineas Phucker  
2989 (UDP) - Remote Administration Tool - RAT  
3000 Remote Shut  
3024 WinCrash  
3031 Microspy  
3128 Reverse WWW Tunnel Backdoor, RingZero  
3129 Masters Paradise  
3150 The Invasor  
3150 (UDP) - Deep Throat, Foreplay, Mini Backlash  
3456 Terror trojan  
3459 Eclipse 2000, Sanctuary  
3700 Portal of Doom  
3777 PsychWard  
3791 Total Solar Eclypse  
3801 Total Solar Eclypse  
4000 SkyDance  
4092 WinCrash  
4242 Virtual Hacking Machine - VHM  
4321 BoBo  
4444 Prosiak, Swift Remote  
4567 File Nail  
4590 ICQ Trojan  
4950 ICQ Trogen (Lm)  
5000 Back Door Setup, Blazer5, Bubbel, ICKiller, Ra1d, Sockets des Troie  
5001 Back Door Setup, Sockets des Troie  
5002 cd00r, Shaft  
5010 Solo  
5011 One of the Last Trojans - OOTLT, One of the Last Trojans - OOTLT, modified  
5025 WM Remote KeyLogger  
5031 Net Metropolitan  
5032 Net Metropolitan  
5321 Firehotcker  
5333 Backage, NetDemon  
5343 wCrat - WC Remote Administration Tool  
5400 Back Construction, Blade Runner  
5401 Back Construction, Blade Runner



5402 Back Construction, Blade Runner  
5512 Illusion Mailer  
5534 The Flu  
5550 Xtcp  
5555 ServeMe  
5556 BO Facil  
5557 BO Facil  
5569 Robo-Hack  
5637 PC Crasher  
5638 PC Crasher  
5742 WinCrash  
5760 Portmap Remote Root Linux Exploit  
5880 Y3K RAT  
5882 Y3K RAT  
5882 (UDP) - Y3K RAT  
5888 Y3K RAT  
5888 (UDP) - Y3K RAT  
5889 Y3K RAT  
6000 The Thing  
6006 Bad Blood  
6272 Secret Service  
6400 The Thing  
6661 TEMan, Weia-Meia  
6666 Dark Connection Inside, NetBus worm  
6667 Dark FTP, ScheduleAgent, SubSeven, Subseven 2.1.4 DefCon 8, Trinity, WinSatan  
6669 Host Control, Vampire  
6670 BackWeb Server, Deep Throat, Foreplay, WinNuke eXtreame  
6711 BackDoor-G, SubSeven, VP Killer  
6712 Funny trojan, SubSeven  
6713 SubSeven  
6723 Mstream  
6771 Deep Throat, Foreplay  
6776 2000 Cracks, BackDoor-G, SubSeven, VP Killer  
6838 (UDP) - Mstream  
6883 Delta Source DarkStar (??)  
6912 Shit Heap  
6939 Indoctrination  
6969 GateCrasher, IRC 3, Net Controller, Priority  
6970 GateCrasher  
7000 Exploit Translation Server, Kazimas, Remote Grab, SubSeven, SubSeven 2.1 Gold  
7001 Freak88, Freak2k  
7215 SubSeven, SubSeven 2.1 Gold  
7300 NetMonitor  
7301 NetMonitor  
7306 NetMonitor  
7307 NetMonitor  
7308 NetMonitor  
7424 Host Control  
7424 (UDP) - Host Control  
7597 Qaz  
7626 Glacier  
7777 God Message, Tini  
7789 Back Door Setup, ICKiller  
7891 The ReVeNgEr  
7983 Mstream  
8080 Brown Orifice, RemoConChubo, Reverse WWW Tunnel Backdoor, RingZero  
8787 Back Orifice 2000  
8988 BacHack  
8989 Rcon, Recon, Xcon  
9000 Netadministrator  
9325 (UDP) - Mstream  
9400 InCommand  
9872 Portal of Doom



9873 Portal of Doom  
9874 Portal of Doom  
9875 Portal of Doom  
9876 Cyber Attacker, Rux  
9878 TransScout  
9989 Ini-Killer  
9999 The Prayer  
10000 OpwinTRojan  
10005 OpwinTRojan  
10067 (UDP) - Portal of Doom  
10085 Syphillis  
10086 Syphillis  
10100 Control Total, Gift trojan  
10101 BrainSpy, Silencer  
10167 (UDP) - Portal of Doom  
10520 Acid Shivers  
10528 Host Control  
10607 Coma  
10666 (UDP) - Ambush  
11000 Senna Spy Trojan Generator  
11050 Host Control  
11051 Host Control  
11223 Progenic trojan, Secret Agent  
12076 Gjamer  
12223 Hack '99 KeyLogger  
12345 Ashley, cron / crontab, Fat Bitch trojan, GabanBus, icmp\_client.c, icmp\_pipe.c, Mypic, NetBus, NetBus Toy, NetBus worm, Pie Bill Gates, Whack Job, X-bill  
12346 Fat Bitch trojan, GabanBus, NetBus, X-bill  
12349 BioNet  
12361 Whack-a-mole  
12362 Whack-a-mole  
12363 Whack-a-mole  
12623 (UDP) - DUN Control  
12624 ButtMan  
12631 Whack Job  
12754 Mstream  
13000 Senna Spy Trojan Generator, Senna Spy Trojan Generator  
13010 Hacker Brasil - HBR  
13013 PsychWard  
13014 PsychWard  
13223 Hack '99 KeyLogger  
13473 Chupacabra  
14500 PC Invader  
14501 PC Invader  
14502 PC Invader  
14503 PC Invader  
15000 NetDemon  
15092 Host Control  
15104 Mstream  
15382 SubZero  
15858 CDK  
16484 Mosucker  
16660 Stacheldraht  
16772 ICQ Revenge  
16959 SubSeven, Subseven 2.1.4 DefCon 8  
16969 Priority  
17166 Mosaic  
17300 Kuang2 the virus  
17449 Kid Terror  
17499 CrazyNet  
17500 CrazyNet  
17569 Infector  
17593 Audiodoor



17777 Nephron  
18753 (UDP) - Shaft  
19864 ICQ Revenge  
20000 Millenium  
20001 Millenium, Millenium (Lm)  
20002 AcidkoR  
20005 Mosucker  
20023 VP Killer  
20034 NetBus 2.0 Pro, NetBus 2.0 Pro Hidden, NetRex, Whack Job  
20203 Chupacabra  
20331 BLA trojan  
20432 Shaft  
20433 (UDP) - Shaft  
21544 GirlFriend, Kid Terror  
21554 Exploiter, Kid Terror, Schwindler, Winsp00fer  
22222 Donald Dick, Prosiak, Ruler, RUX The Tic.K  
23005 NetTrash  
23006 NetTrash  
23023 Logged  
23032 Amanda  
23432 Asylum  
23456 Evil FTP, Ugly FTP, Whack Job  
23476 Donald Dick  
23476 (UDP) - Donald Dick  
23477 Donald Dick  
23777 InetSpy  
24000 Infector  
25685 Moonpie  
25686 Moonpie  
25982 Moonpie  
26274 (UDP) - Delta Source  
26681 Voice Spy  
27374 Bad Blood, Ramen, Seeker, SubSeven, SubSeven 2.1 Gold, Subseven 2.1.4 DefCon  
8, SubSeven Muie, Ttfloader  
27444 (UDP) - Trinoo  
27573 SubSeven  
27665 Trinoo  
28678 Exploiter  
29104 NetTrojan  
29369 ovasOn  
29891 The Unexplained  
30000 Infector  
30001 ErrOr32  
30003 Lamers Death  
30029 AOL trojan  
30100 NetSphere  
30101 NetSphere  
30102 NetSphere  
30103 NetSphere  
30103 (UDP) - NetSphere  
30133 NetSphere  
30303 Sockets des Troie  
30947 Intruse  
30999 Kuang2  
31335 Trinoo  
31336 Bo Whack, Butt Funnel  
31337 Back Fire, Back Orifice 1.20 patches, Back Orifice (Lm), Back Orifice russian, Baron  
Night, Beeone, BO client, BO Facil, BO spy, BO2, cron / crontab, Freak88, Freak2k,  
icmp\_pipe.c, Sockdmini  
31337 (UDP) - Back Orifice, Deep BO  
31338 Back Orifice, Butt Funnel, NetSpy (DK)  
31338 (UDP) - Deep BO  
31339 NetSpy (DK)



31666 BOWhack  
31785 Hack´a´Tack  
31787 Hack´a´Tack  
31788 Hack´a´Tack  
31789 (UDP) - Hack´a´Tack  
31790 Hack´a´Tack  
31791 (UDP) - Hack´a´Tack  
31792 Hack´a´Tack  
32001 Donald Dick  
32100 Peanut Brittle, Project nEXT  
32418 Acid Battery  
33270 Trinity  
33333 Blakharaz, Prosiak  
33577 Son of PsychWard  
33777 Son of PsychWard  
33911 Spirit 2000, Spirit 2001  
34324 Big Gluck, TN  
34444 Donald Dick  
34555 (UDP) - Trinoo (for Windows)  
35555 (UDP) - Trinoo (for Windows)  
37237 Mantis  
37651 Yet Another Trojan - YAT  
40412 The Spy  
40421 Agent 40421, Masters Paradise  
40422 Masters Paradise  
40423 Masters Paradise  
40425 Masters Paradise  
40426 Masters Paradise  
41337 Storm  
41666 Remote Boot Tool - RBT, Remote Boot Tool - RBT  
44444 Prosiak  
44575 Exploiter  
47262 (UDP) - Delta Source  
49301 OnLine KeyLogger  
50130 Enterprise  
50505 Sockets des Troie  
50766 Fore, Schwindler  
51966 Cafeini  
52317 Acid Battery 2000  
53001 Remote Windows Shutdown - RWS  
54283 SubSeven, SubSeven 2.1 Gold  
54320 Back Orifice 2000  
54321 Back Orifice 2000, School Bus  
55165 File Manager trojan, File Manager trojan, WM Trojan Generator  
55166 WM Trojan Generator  
57341 NetRaider  
58339 Butt Funnel  
60000 Deep Throat, Foreplay, Sockets des Troie  
60001 Trinity  
60068 Xzip 6000068  
60411 Connection  
61348 Bunker-Hill  
61466 TeleCommando  
61603 Bunker-Hill  
63485 Bunker-Hill  
64101 Taskman  
65000 Devil, Sockets des Troie, Stacheldraht  
65390 Eclypse  
65421 Jade  
65432 The Traitor (= th3tr41t0r)  
65432 (UDP) - The Traitor (= th3tr41t0r)  
65534 /sbin/initd  
65535 RC1 trojan