

TROJAN HORSE

Anharku

v_maker@yahoo.com

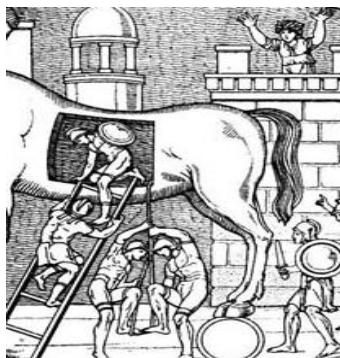
<http://anharku.freevar.com>

Lisensi Dokumen:

Copyright © 2003-2009 IlmuKomputer.Com

Seluruh dokumen di IlmuKomputer.Com dapat digunakan, dimodifikasi dan disebarkan secara bebas untuk tujuan bukan komersial (nonprofit), dengan syarat tidak menghapus atau merubah atribut penulis dan pernyataan copyright yang disertakan dalam setiap dokumen. Tidak diperbolehkan melakukan penulisan ulang, kecuali mendapatkan ijin terlebih dahulu dari IlmuKomputer.Com.

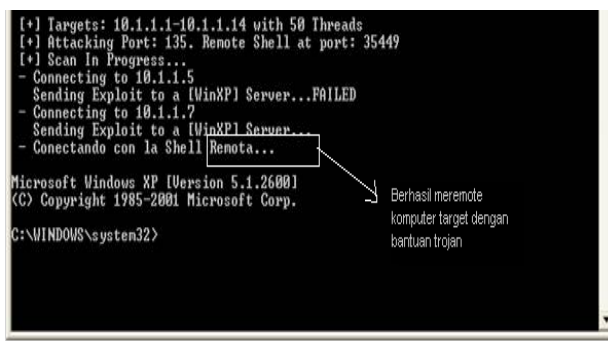
Sejarah Trojan Horse



Untuk mengetahui apa itu Trojan Horse mari kita pelajari terlebih dahulu sejarah dari nama Trojan Horse itu sendiri. Nah sejarahnya Nama Trojan Horse berasal dari sejarah Yunani Kuno dimana terjadi peperangan antara bangsa Yunani dengan Troy selama lebih dari 10 tahun. Penyusup dari Yunani dipanggil Sinon menawarkan hadiah Trojan yang berbentuk Kuda dari kayu berukuran besar dan berhasil menyakinkan Troy bahwa Kuda Kayu (Trojan) tersebut dapat memberi kekuatan abadi kepada bangsa Troy. Setelah Kuda Kayu tersebut masuk ke kota Troy , tidak disangka telah banyak pasukan Yunani yang bersembunyi di dalamnya, Yunani berhasil melumpuhkan dan membakar habis kota Troy dari dalam. Kisah tersebut mengilhami para *hacker* untuk menciptakan “penyusup” ke

komputer orang lain yang disebut dengan Trojan Horse. Daniel Edwards dari *National Security Agency* (NSA) yang diakui mencetuskan istilah Trojan Horse untuk program jahat yang menyelip dalam komputer korban (detik.com,12/06/2008)

Trojan Horse dalam dunia IT?



Trojan Horse (Kuda Troya), Trojan Horse bukanlah sebuah virus, karena Trojan Horse tidak memiliki kemampuan untuk menggandakan diri. Namun demikian, Trojan Horse tidak kalah berbahaya jika dibandingkan dengan virus. Trojan Horse umumnya dikemas dalam bentuk sebuah software yang menarik. Namun dibalik daya tarik software tersebut, tersembunyi fungsi lain untuk melakukan kerusakan. Misalkan saja software Keygen /key generator atau software pencari

Serial Number(SN)/ kunci, nah tentunya kita tertarik bukan untuk menjalankan software tersebut? Karena kadang-kadang software meminta kita melakukan registrasi dengan memasukkan SN untuk

menghilangkan masa trialnya. Pengguna komputer yang mendapatkan file yang telah mengandung Trojan Horse ini umumnya akan terpancing untuk menjalankannya yah Karena daya tarik tadi. Akibatnya tentu fatal, karena dengan demikian si pengguna telah meenjalankan rutin-rutin perusak yang siap menebar bencana di komputernya. *Trojan* bisa berupa program perusak maupun program kendali. Contoh *trojan* misalnya kaHt, *Back Orifice* dan *Netbus*. Apabila korban telah terkena salah satu dari program ini maka apabila korban terhubung ke jaringan atau *internet*, si pengirim *trojan* dapat mengendalikan komputer korban dari jauh,karena trojan membuka port-port tertentu agar komputer dapat diremote, bahkan tidak mustahil untuk mematikan atau merusak dari jauh. Itu sama halnya dengan penduduk kota Troy yang terlambat menyadari bahwa kota mereka sudah di masuki oleh tentara musuh.

Bagaimana Cara kerja Trojan Horse?

Trojan masuk melalui dua bagian, yaitu bagian *client* dan *server*. Jadi hacker kadang harus berjalan menanamkan trojannya di komputer korban ataupun memancing agar sang korban mengeksekusi/membuka file yang mengandung Trojan, namun ada juga Trojan yang langsung menginfeksi korbannya hanya dengan berbekal ip korban misalnya Kaht. Ketika korban (tanpa diketahui) menjalankan file yang mengandung Trojan pada komputernya, 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 membuka beberapa *port* untuk melakukan koneksi, memodifikasi *registry* dan atau menggunakan metode lain yaitu metode *autostarting* agar trojan menjadi otomatis aktif saat komputer dihidupkan. Trojan sangat berbahaya bagi pengguna komputer yang tersambung jaringan komputer atau internet, karena bisa jadi hacker bisa mencuri data-data sensitif misalnya password email, *dial-up passwords*, *webservices passwords*, *e-mail address*, dokumen pekerjaan, internet banking, paypal, e-gold,kartu kredit dan lain-lain.

Jenis-jenis Trojan?

Jenis-jenis Trojan antara lain:

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 dikomputer korban dan BOGUI.EXE yang dijalankan oleh penyerang untuk mengakses komputer korban.

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.

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*.

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.

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.

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. Wintrino 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.

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.

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.

Lalu bagaimana cara mengatasi bahaya Trojan?

Pertama lakukan langkah pendeteksian keberadaan Trojan pada komputer. Pendeteksian Trojan dapat dilakukan dengan cara-cara sebagai berikut

1. Task List

Pendeteksiannya dengan melihat daftar program yang sedang berjalan dalam *task list*. Daftar dapat ditampilkan dengan menekan tombol CTRL+ALT+DEL atau klik kanan pada toolbar lalu klik task manager. 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.

Langkah penghapusan Trojan

Trojan dapat dihapus dengan:

- Menggunakan Software Anti-Virus. Sebagian antivirus dapat digunakan untuk mengenali dan menghapus Trojan.
- Menggunakan *Software Trojan Scanner*, software yang di khususkan untuk mendeteksi dan menghapus Trojan
- Cara yang paling sadis yah diinstal ulang komputernya.

Langkah pencegahan Trojan

Untuk mencegah Trojan menyusup di komputer anda, pastikan anda memasang antivirus yang selalu ter-update, mengaktifkan Firewall baik bawaan dari Windows atau dari luar. Selalu waspadalah jika komputer anda mengalami sesuatu kejanggalan. Hindari penggunaan software ilegal karena sering tanpa kita sadari software tersebut mengandung Trojan, downloadlah software dari situs-situs yang benar-benar dapat dipercaya.

Semoga yang saya tuliskan diatas dapat membuka pengetahuan kita mengenai Trojan Horse... ☺

Referensi:

Apa itu trojan horse-ZonaKita.net

Deteksi Trojan dan Penangannannya,Rohmadi Hidayat

Konsep perlindungan komputer terhadap virus, Minnarto Djojo

Biografi Penulis



Anharku. Pertama mengenal komputer saat SMP pertamanya kenal komputer hanya bermain game bawaan window's lambat laun karna pergaulan dan pertumbuhan, merasakan anehnya cinta monyet...patahhati lalu melampiaskannya pada bermain Game online namun karena satu persatu game itu servernya runtuh (gameOver kali) jadi aku memutuskan vakum dari dunia gamer waktu itu juga saat aku masih UAS jadi aku fokus ke skull dulu.Lanjut mengenal dunia internet

sejak hobi main di warnet untuk sekedar mengecek e-mail, fs, dan sekedar chatting ga jelas..Dari temanku bernama DNZ lah aku mulai mengenal dunia virus..lalu aku belajar secara otodidak karna temanku DNZ lebih suka dunia Hacking. Belajar algoritma dan pemrograman, membuat flowchart, dan belajar bahasa pemrograman seperti visual basic, delphi, C++, pascal, asmbly. Belajar tentang micro, website, PHP, Basis data, MySQL, belajar tentang Jaringan Komputer..belajar tentang segala sesuatu yang berbau komputer.