

# **TUGAS KEAMANAN JARINGAN KOMPUTER**

## **“FTP TROJAN”**



**Disusun Oleh:**

Nama : MUHAMMAD FAJAR PUTRA  
NIM : 09011181520009  
Kelas : SK8

**JURUSAN SISTEM KOMPUTER  
FAKULTAS ILMU KOMPUTER  
UNIVERSITAS SRIWIJAYA  
2019**

## Pengertian Trojan

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 perusakan. 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 menjalankan 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.

## Cara kerja Trojan

Trojan bersifat "*stealth*" (siluman dan tidak terlihat) dalam operasinya dan seringkali berbentuk seolah-olah program tersebut merupakan program baik-baik, sementara virus komputer atau worm bertindak lebih agresif dengan merusak sistem atau membuat sistem menjadi crash.

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.

## **FTP ( FILE TRANSFER PROTOCOL)**

File Transfer Protocol (FTP) adalah suatu protokol yang berfungsi untuk tukar-menukar file dalam suatu network yang menggunakan TCP koneksi bukan UDP. Dua hal yang penting dalam FTP adalah FTP Server dan FTP Client. FTP server adalah suatu server yang menjalankan software yang berfungsi untuk memberikan layanan tukar menukar file dimana server tersebut selalu siap memberikan layanan FTP apabila mendapat permintaan (request) dari FTP client.

FTP client adalah computer yang merequest koneksi ke FTP server untuk tujuan tukar menukar file. Setelah terhubung dengan FTP server, maka client dapat men-download, meng-upload, merename, men-delete, dll sesuai dengan permission yang diberikan oleh FTP server.

## **FTP TROJAN**

FTP Trojan Generator adalah trojan yang tersembunyi di dalam program jahat. Setelah Anda menginstal program sumber (operator), trojan ini mencoba untuk mendapatkan akses "root"(akses tingkat administrator) ke komputer kita tanpa sepengetahuan kita.

Trojan FTP adalah jenis Trojan khusus yang memungkinkan penyerang mengakses mesin menggunakan Protokol FTP. Umumnya, Trojan adalah jenis virus yang memasuki sistem dengan cara yang tidak terdeteksi dan mengakses semua data rahasia, sehingga menyebabkan masalah dengan mengkompromikan atau mengekspos data. Salah satu cara Trojan dapat memanifestasikan dirinya adalah dalam bentuk program asli yang melakukan fungsi jahat.

Trojan FTP menginstal server FTP pada mesin korban yang memungkinkan penyerang mendapatkan akses ke data sensitif melalui Protokol FTP. Trojan membuka port 21 dan membuatnya dapat diakses oleh penyerang atau sekelompok individu. Beberapa serangan kata sandi juga dapat digunakan di mana hanya penyerang mendapatkan akses ke sistem. Sistem mencoba mengunduh dan mengunggah file dari sistem korban. Jenis-jenis informasi yang terpengaruh meliputi: Informasi kartu kredit Semua jenis informasi nama pengguna dan kata sandi data rahasia alamat email untuk disebarluaskan menggunakan komputer korban sebagai sumber untuk menyebarkan serangan lain.

Trojan seperti FTP Generator Trojan sulit dideteksi karena mereka menyembunyikan diri dengan mengintegrasikan ke dalam sistem operasi. Setelah menginfeksi komputer kita, FTP Trojan Generator mengeksekusi setiap kali komputer Anda melakukan boot dan mencoba mengunduh dan menginstal file berbahaya lainnya. Setelah eksekusi berhasil, ia menghapus program sumber, membuatnya lebih sulit untuk dideteksi.

## **Bagaimana Cara FTP Trojan mengakses Komputer Kita ?**

Seperti trojan lainnya, FTP Trojan Generator memperoleh entri melalui program sumber yang membawa muatan trojan yang tanpa sadar kita instal. Sumber umum dari program tersebut adalah:

- Situs web berbahaya yang dirancang khusus untuk menyuntikkan Trojans
- Situs web resmi yang terinfeksi Trojans
- Lampiran email
- Pembaruan palsu disajikan untuk perangkat lunak yang diinstal
- Perangkat lunak berbagi peer-to-peer
- Pemutar video dan codec berbahaya
- Game yang dapat diunduh gratis
- Software Chatting
- Saluran IRC
- Tautan media sosial yang menunjuk ke file atau situs web yang terinfeksi

## **Gejala Infeksi Generator Trojan FTP**

Gejala utama infeksi FTP Trojan Generator adalah:

- Aktivitas jaringan yang tidak alami: Anda mungkin mengalami aktivitas jaringan yang tidak wajar yang mengakibatkan kecepatan jaringan (Internet) lambat karena trojan mencoba mengakses jaringan Anda untuk mengunduh program jahat lainnya.
- Modifikasi registri. FTP Trojan Generator berupaya menambah entri registri baru dan memodifikasi yang sudah ada. Akibatnya, Anda secara bertahap akan melihat perilaku komputer yang lambat dan tidak biasa.
- Perubahan dalam pengaturan browser: FTP Trojan Generator menginstal file jahat, terutama dengan fungsi memodifikasi pengaturan terkait browser kita. Akibatnya, akses Internet melambat dan situs web yang tidak diinginkan terus dimuat melalui jendela pop-up atau langsung di jendela peramban aktif.
- Komputer lambat: kita mungkin mengalami boot komputer lambat, karena program startup yang tidak diketahui diunduh oleh FTP Trojan Generator. Anda mungkin juga mengalami kinerja komputer yang lambat karena program-program berbahaya yang diunduh

## **Cara Menghapus Trojan FTP dari Komputer**

FTP Trojan r sulit untuk dideteksi dan dihapus secara manual. Namun, sebagian besar program anti-malware dapat mendeteksi dan menghapusnya dengan sukses. Memindai komputer dengan satu anti-malware semacam itu akan menghapus Generator Trojan FTP dan semua file yang terinfeksi olehnya..

Sayangnya, memindai dan menghapus ancaman saja tidak akan memperbaiki modifikasi yang dibuat FTP Trojan Generator untuk Windows Registry kita. Kita harus membersihkan Windows Registry dengan menghapus entri registri yang tidak valid menggunakan program pembersih registri.

Mengamankan Komputer Terhadap Serangan Trojan Perlindungan gateway antivirus dapat digunakan untuk mendeteksi Trojan yang masuk melalui HTTP, email atau FTP. Disarankan untuk menggunakan beberapa mesin antivirus untuk memastikan bahwa berbagai jenis Trojan mudah dikenali dan ditangani. Mesin antivirus tunggal tidak akan pernah bisa mengenali semua Trojan. Berikut ini adalah beberapa langkah untuk mencegah atau mengurangi keberadaan Trojan: Unduh hanya dari situs web tepercaya.,Periksa ekstensi file sebelum membukanya. (Mungkin saja file jpg telah dimask dengan ekstensi .exe, yang dapat mengaktifkan Trojan dengan mengkliknya.), Hindari mengeksekusi skrip berbasis web dan perintah otomatis yang disebutkan online tanpa sepenuhnya memahami efeknya. Unduh file .exe hanya dari sumber tepercaya.

Jika komputer terinfeksi dengan FTP Trojan Generator, lakukan langkah-langkah berikut untuk menghapusnya :

- Gunakan program anti-malware untuk memindai dan menghapus ancaman malware maupun Trojan
- Bersihkan Registry Windows secara rutin