Keamanan Jaringan Komputer



Disusun Oleh :

Nadya Rahma Noviyanti

09011281520127

Jurusan Sistem Komputer

Fakultas Ilmu Komputer

Universitas Sriwijaya

2019

1. **Tentang Remote Access Trojan (RAT)**

Remote Access Trojan (RAT) adalah Trojan yang memungkinkan monitor penyerang dan mengendalikan PC korban dari jarak jauh melalui jaringan. RAT biasanya terdiri dari sisi klien dan sisi server. Berlawanan dengan pengetahuan umum, sisi server dari RAT adalah korban. Dari layar operasi RAT. Kami mengonfirmasi bahwa RAT tidak hanya dapat mengunduh file dari PC korban, tetapi juga dapat memonitor keylogger dan layar sistem. Ada dua pola komunikasi RAT. Salah satunya dimulai dari sisi klien penyerang. Sisi klien berada di luar jaringan target, sehingga lalu lintas tidak dapat melewati firewall dengan mudah. Yang lain dimulai dari sisi server korban. Di dalam pola, lalu lintas bahkan dapat melewati server proxy.

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.

1. **Analisa Remote Access Trojan (RAT)**

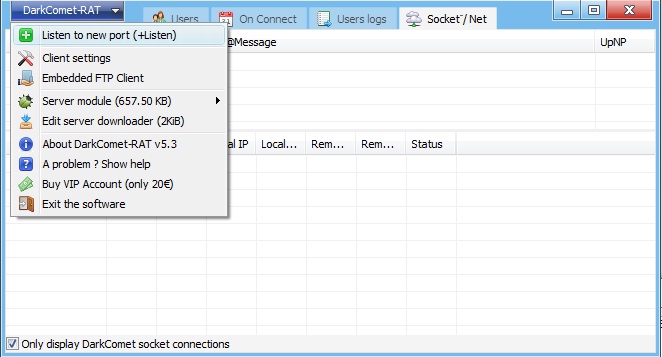
Karena kecelakaan kebocoran data terjadi setiap tahun, maka keamanan informasi rahasia penting semakin meningkat. Remote Access Trojan (RAT), sejenis spyware, digunakan untuk menyerang PC korban melalui serangan yang ditargetkan. Setelah intruksi, penyerang dapat memonitor dan mengontrol PC korban dari jarak jauh, untuk menunggu kesempatan mencuri informasi rahasia. Karena sulit untuk mencegah intruksi RAT sepenuhnya, mencegah informasi rahasia bocor kembali ke penyerang adalah masalah utama. Berbagai ada pendekatan memperkenalkan perilaku jaringan RAT yang berbeda membangun sistem deteksi. Sayangnya, dua tantangan terkait utama: satu adalah untuk mendeteksi sesi RAT sedini mungkin, itu lainnya adalah tetap memiliki akurasi tinggi untuk mendeteksi sesi RAT, sementara ada aplikasi normal yang lalu lintasnya berperilaku mirip dengan RAT.

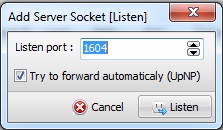
Dalam tulisan ini, diusulkan pendekatan baru untuk mendeteksi RAT sesi dalam tahap awal komunikasi. Untuk membedakan perilaku jaringan antara aplikasi normal dan RAT, kami ekstrak fitur dari lalu lintas dalam waktu singkat di awal mula. Setelah itu, kami menggunakan teknik pembelajaran mesin untuk melatih model pendeteksian, kemudian mengevaluasinya dengan K-Fold cross-validasi. Hasilnya menunjukkan bahwa pendekatan kami dapat mendeteksi Sesi RAT dengan akurasi tinggi. Secara khusus, pendekatan kami mencapai akurasi lebih dari 96% bersama dengan FNR sebesar 10% oleh Algoritma Random Forest, yang berarti bahwa pendekatan kami adalah valid untuk mendeteksi sesi RAT pada tahap awal komunikasi.

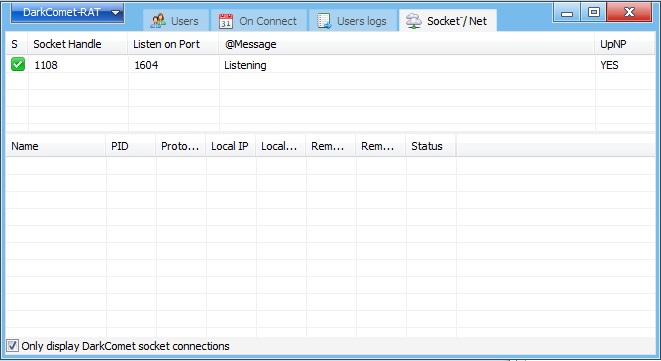
1. **Teknik Penggunaan Remote Access Trojan (RAT) dengan Tools Darkcomet RAT**

Darkcomet merupakan salah satu dari sekian banyak RAT yang beredar saat ini. Cara penggunaan darkcomet kurang lebih sama seperti RAT kebanyakan ,kita akan membuat server yang menjadi "inang" yang harus dijalankan pada komputer "korban" tujuan.

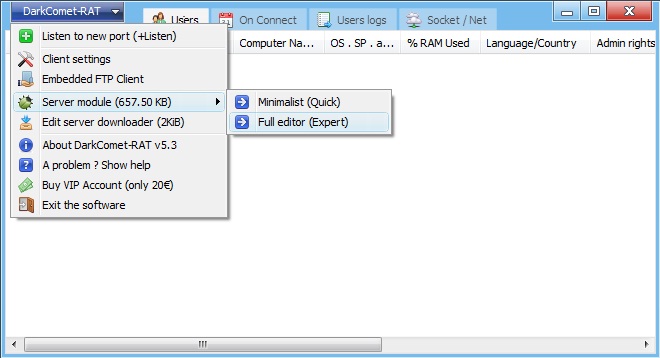
Hal yang pertama kita lakukan menentukan port yang akan dipakai ,yang nantinya digunakan untuk melakukan listen kepada port yang kita tuju. Selanjutnya ,kita melakukan listen ke port yang sudah kita tentukan sebelumnya.Dengan cara pilih menu Listen to the new port.



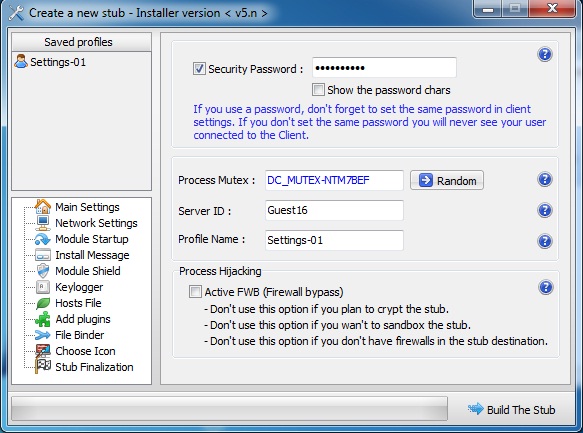




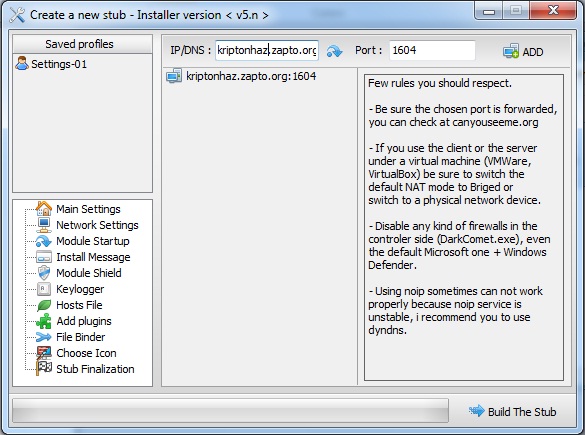
Lalu, kita akan membuat file server yang akan di jalankan pada komputer tujuan, dengan cara pilih server module pada menu, lalu pilih full editor.



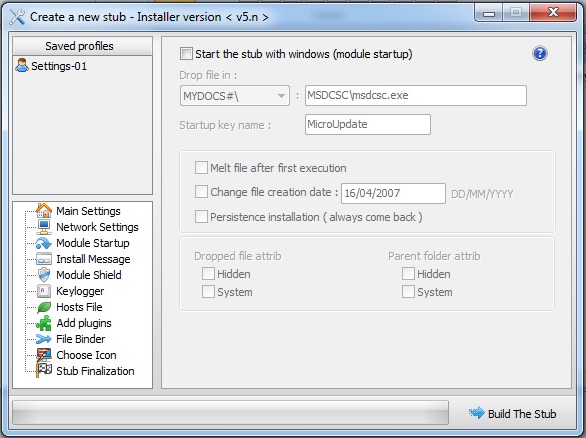
Pada security password terserah anda menggunakan atau tidak, pada contoh saya menggunakan password, dan untuk Process Mutex cukup klik random beberapa kali.

[](http://i.imgur.com/Ox2ka.jpg)

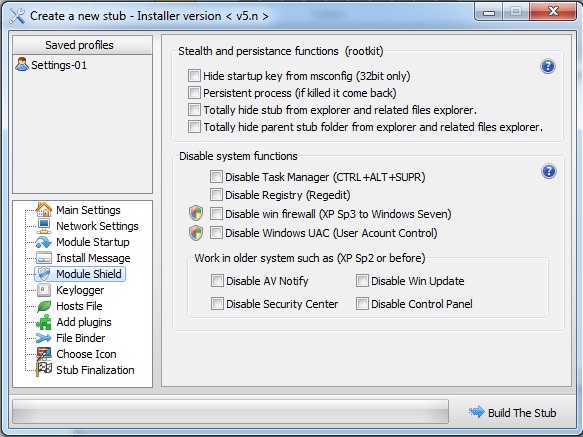
Selanjutnya di bagian network setting ingat di bagian awal kita membuat host di No-IP. Kita masukkan disana sesuai dengan port yang sudah di atur sebelumnya dan klik add hingga seperti ini

[](http://i.imgur.com/94ImF.jpg)

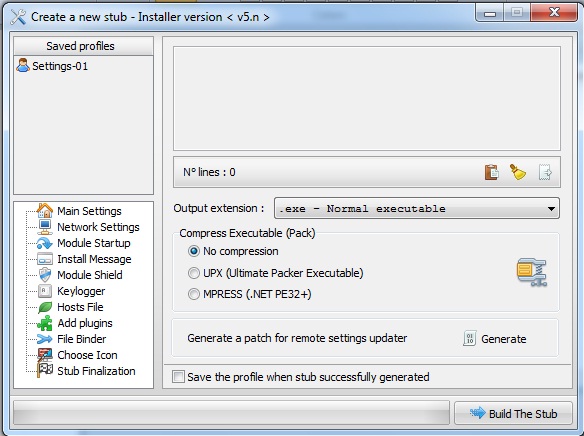
Pada bagian module startup ini tergantung anda mau menggunakan fitur startup disini atau pada crypter (akan dibahas nanti) namun harus memilih salah satu. Jika iya maka pilihan dibawahnya akan aktif.

[](http://i.imgur.com/PqfY6.jpg)

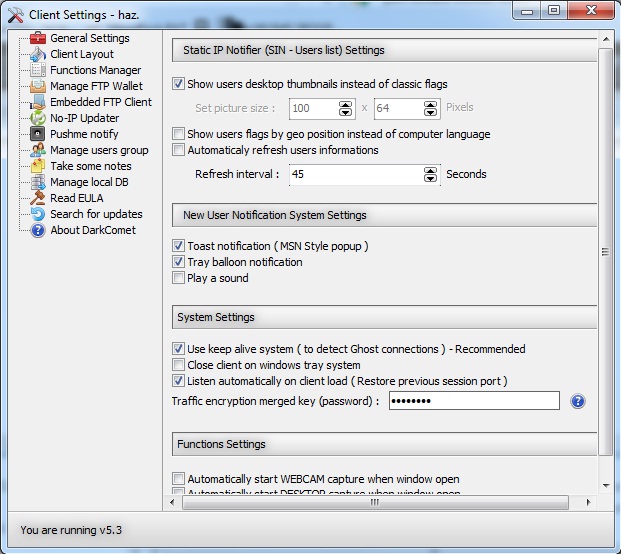
Pada bagian module shield cukup centang 4 opsi yang ada di bagian rootkit (paling atas)

[](http://i.imgur.com/fblZ1.jpg)

Save file server

[](http://i.imgur.com/0FRX0.jpg)

Sebelumnya kita harus  sesuai dengan server yang agan buat (berpassword atau tidak), jika berpassword sesuaikan dengan cara masukkan passwordnya pada menu > client setting

[](http://i.imgur.com/uprC8.jpg)

Setelah bagaimana kita menggunakan teknik trojan di atas, kita dapat melakukan beberapa pencegahan agar tidak ada trojan yang masuk ke dalam komputer kita.

1. Port
2. **Port dan Protokol yang Digunakan**

Dalam hah ini kami mencari sumber dari paper dimana tentang Trojan jenis HTTP. Menurut paper yang saya baca “A Method for HTTP-Tunnel Detection Based on Statistical Features of Traffic” di mana paper tersebut menggunakan port 80 sedangkan protokol yang digunakan ialah TCP/IP