

# mIRC Trojan

(tutorial by ircboy)

mIRC Trojan adalah trojan dengan memakai mIRC sebagai client dan IRC sebagai media server dengan beberapa fungsi umum seperti

- join channel
- part channel
- private dan channel msg
- spam (untuk penyebaran trojan) bisa juga di gunakan sebagai inviter channel / server
- proxy / bnc
- xdcc / file server
- mencuri user ID / nick / password dll

## Penting

bagi yang belum memahami mIRC script disarankan untuk mempelajari dulu mIRC script untuk menghasilkan trojan yang memiliki fungsi yang lengkap dan sesuai keinginan kamu mirc.hlp sudah cukup untuk panduan. Dalam membuat mIRC Trojan dengan keterbatasan/belum ada nya script untuk beberapa tujuan, biasanya di pergunakan beberapa file bantuan apakah berupa file \*.exe \*.bat \*.vbs dll untuk mendukung kinerja trojan

Berikut adalah panduan membuat mIRC Trojan

## 1. mIRC Trojan Setting dan Script

Buatlah script mIRC Trojan kamu sesuai keinginan kamu dengan fungsi yang kamu inginkan (bot kontrol, spam kontrol, xdcc, dll) dan setting **mirc.ini** sesuai kebutuhan (seperti flood protection, auto dcc get, dll). Test script secara online/offline. Untuk test secara offline gunakan software irc server seperti

- **WIRCSRV, copyright 1996 by John Joseph**
- **mIRC Based IRC Services for Win95 By Boris Dinkevich**

### tips

- gunakan untuk trojan **mirc.exe** yang unregistered or udah di hacked register nya
- edit **mirc.exe** dengan program Resource Hacker untuk menghapus resources yang tidak di gunakan
- compress **mirc.exe** untuk mendapatkan ukuran file yang lebih kecil berkisar 400 s/d 500 bytes
- gunakan beberapa irc server untuk mengontrol bot hal ini untuk menjaga apabila server tidak bisa connect atau channel bot kamu di tutup admin server  
gunakan variabel untuk mengontrol bot seperti variabel server admin, channel admin, ick admin, website download trojan dll. Variabel ini dapat menggunakan variabel pda mIRC script atau disimpan pada file **mirc.ini** Penggunaan variabel adalah untuk memudahkan apabila kita melakukan perubahan.
- check system operasi dan diretory windows untuk simpan trojan di drive c:\windows atau c:\winnt
- unload / replicated trojan installer ke drive trojan
- auto update versi script atau variabel
- manfaatkan fasilitas DDE dari mirc script untuk membuat relay / kontrol user yang online ke mIRC

## 2. Menyembunyikan mIRC di layar monitor

Untuk membuat korban tidak curiga adalah penting untuk menyembunyikan trojan kamu atau membuat trojan berjalan invisible. Adapun beberapa cara untuk mebuat mIRC invisible adalah sebagai berikut

### program hide window

Beberapa program seperti hide.exe sudah terdeteksi banyak anti virus jadi tidak disarankan. Cobalah cari referensi di internet program hide window lainnya yang belum terdeteksi oleh anti virus. Atau buatlah program hide sendiri melalui bahasa pemrograman seperti VB atau JS.

### mIRC always minimize dan place mIRC in tray

mIRC Options / Display / Tray

Check pilihan | on startup minimize mIRC to tray

Check pilihan | palce mIRC on tray when minimize

Pilih icon minimize lain yang tidak menunjukkan mIRC program

di awal script jadi mIRC selalu minimize

/timer 0 0 /showmirc -t

## **dll**

Penggunaan DLL dalam script untuk membuat mIRC invisible. Beberapa versi DLL sudah terdeteksi beberapa anti virus tapi masih bagus dan untuk DLL lainnya dengan fungsi sama silahkan di cari di internet atawa tanya Om Google ama Tante Yahoo or collector mirc trojan  
Tambahkan di script perintah contoh dll swf.dll do\_ShowWindow \$window(-2).hwnd 0

### **3. Upload trojan ke komputer korban**

Untuk membuat korban terkena trojan kamu tentu saja kamu harus menanam trojan kamu ke komputer korban. Ada beberapa cara menanam trojan antara lain sebagai berikut :

**HTML exploit code (VBS.Karma)** sudah banyak terdeteksi oleh banyak anti virus.

**Installer** (Winzip Self Extractor, Astrum Installer, dll)

**Exploit JPEG** (JPEG of Death)

**Exploit lainnya**

#### **tips**

Penting untuk langsung menjalankan trojan saat korban membuka website / file hal ini karena penggunaan program sejenis DeepFreeze yang tidak memungkinkan apabila trojan di jalankan pada next restart. Namun penggunaan autostart tetap di perlukan untuk komputer yang tidak terproteksi Deep Freeeze (**ada yang udah tahu cara ngalahin Deep Freeze please email me**). Autostart trojan dapat dibuat pada registry, win.ini, system.ini dan lokasi lainnya.

### **4. Penyebaran Trojan**

Penyebaran trojan dapat di lakukan dengan beberapa cara

- **spamming** (mIRC script)

gunakan spamming yang kreatif untuk menghindari bot check spam dan flooding, caranya pakai timer dan jangan spam nick yang join tapi nick lain di channel. Untuk bot check spam buat beberapa kalimat sebelum ngasih alamat website atau langsung halt kalo ada kalimat berbau check spam dari bot. Paling efektif adalah bot yang bisa chat so korban yakin chat sama user dan mau kalau di suruh buka / upload /run file installer trojan. Jangan spam Dalnet karena mereka punya nohack team yang bikin website trojan kamu cepat ditutup. Mau spam juga tapi pake smooth spam deh

- **DCC Send** (mIRC script)

- **XDCC / Fserve** (mIRC script)

bot trojan join xdcc / fserv / trade channel dan mengadaptasi command di channel tersebut

- **internet / LAN Infecting** (psexec.exe dari pstool)

menggunakan kelemahan drive / printer sharing. Kombinasi mIRC script, bat file dan psexec.exe.

- **e-mail** (vbs) cara paling efektif . **kalo yang punya versi mirc script nya please e-mail me**

- **copy ke disket dan flash disk** (mIRC script)

check drive aktif per N menit so trojan installer bisa ke komputer lain dengan bantuan user.

**Kalo ada yang punya cara buat autorun di flash disk please e-mail me**

Nah dah siap buat mIRC Trojan !!!! Lets do IT

ircboy

e-mail novitasarita@yahoo.com

ircboy / #aceh / irc.allnetwork.org

This document was created with Win2PDF available at <http://www.daneprairie.com>.  
The unregistered version of Win2PDF is for evaluation or non-commercial use only.