ICQ als Trojaner by MiGa

Hi,
ist euch auch schon das kleine Häuschen aufgefallen, dass manche ICQ Benutzer neben ihrem Namen haben ?
Es bedeutet, dass sie einen Webserver am laufen haben. Wenn ihr so einen findet könnt ihr tolle Sachen machen:

1. ICQ schließen
2. Dateien angucken

zu 1.

IP Adresse des USERS

Ihr brauch zuerst die IP Adresse des Users. Entweder über "INFO", wenn sie freigeschaltet ist oder ihr schickt dem User eine Message und fürht danach direkt "netstat -a" ind der MS-DOS Eingabeaufforderung aus. Dort seht ihr unter "Foreign Address" eine Adresse mit :1054 am ende.
Jetzt müsst ihr nur noch "ping *.*.*.*.*:1054" (wobei *.*.*.*.* die Adresse ist, die vor :1054 in der Tabelle stand) schreiben. Dan habt ihr die IP Adresse.

ICQ des USERS schließen

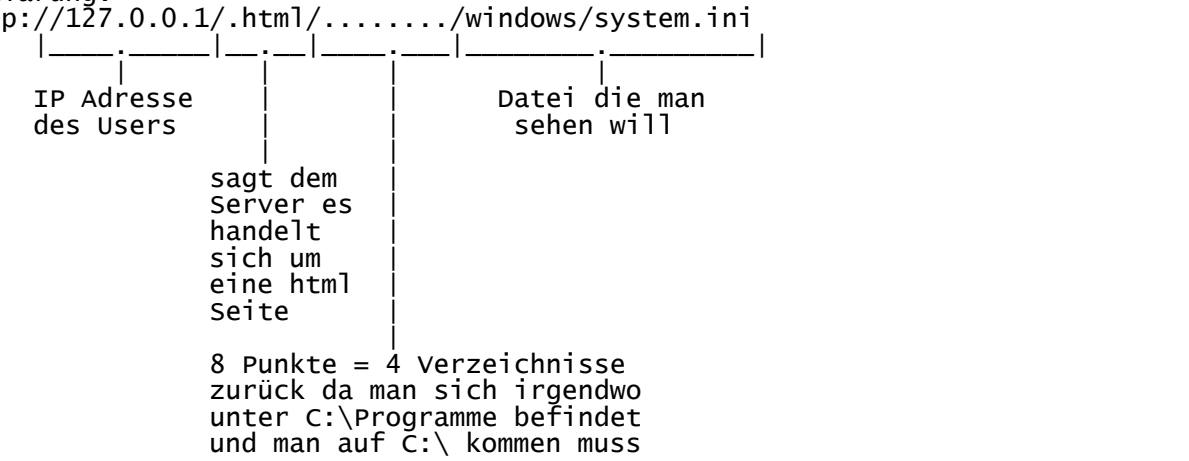
Jetzt drückt ihr auf START und gebt bei AUSFÜHREN folgendes ein:
Telnet 127.0.0.1 80 (127.0.0.1 ersetzt ihr natürlich durch die gefundene IP Adresse)
Danach müsst ihr ENTER drücken und warten bis ihr drin seit.
Jetzt schreibt ihr "QUIT" und wartet etwas...
Danach sollte der USER nicht mehr online sein !

zu 2.

Dateien angucken

Also, zuerst braucht ihr wieder die IP Adresse (s. oben)
Danach geht ihr in euren Browser und schreibt:
"http://127.0.0.1/.html/...../windows/system.ini"

Erklärung:



Dann kommt eine Meldungsbox, wo ihr die Datei speichern wollt und ihr könnt sie euch angucken.

Tipps:

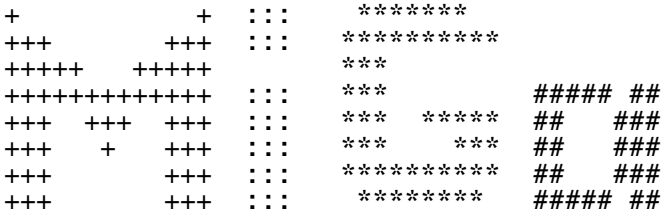
Manche User sind zu faul für dauernd ihre Passwörter (z.B. Mailpasswörter) einzugeben und speichern die dann ab. Wenn ihr die Passwörter haben wollt, müsst ihr euch die system.dat und die user.dat von dem Computer runter laden. Als

nächstes geht ihr unter die Eingabeaufforderung (nicht das Fenster sonder ihr müsst euren Computer entweder runter fahren als "Im MS-Dos Modus neu starten" oder ihr drück am Start F8 und geht auf "Eingabeaufforderung"). Dort müsst ihr eure system.dat + user.dat irgendwo anders hin sichern und die Dateien dann durch die gestohlenen system.dat + user.dat ersetzen. Dann könnt ihr euren Computer noch mal neu starten und geht in den regediät von Windows. Jetzt könnt ihr etwas rumgucken und nach Passwörtern suchen!
Nicht vergessen, dass ihr eure eigene system.dat + user.dat nachher wieder zurück kopiert!

Es kann sein, dass es nicht bei allen Versionen von ICQ klappt.

-

Das war's



Visit us at http://www.dch.de.cx oder http://dch.areCool.net