4. fejezet - Tartalom

4 A trójaiak

4.1 A történelmi minta

Bizonyára mindenki ismeri a homéroszi történetet: *Párizs,* a trójai király megszöktette a szépséges görög *Helénát.* Erre a görögök évekig ostromolták eredménytelenül Trója városát. Amikor látták, hogy ostrommal nem tudják bevenni, a görög *Odüsszeusznak* támadt egy ötlete. Építtetett egy hatalmas falovat, a trójaiak isteni jelképét, és Trója kapuja elé állíttatta. Ezután a görögök visszahúzódtak. A trójaiak a biztos győzelem tudatában bevontatták a lovat a városba, és önfeledten ünnepeltek. De a ló belseje a legerősebb és legbátrabb görög harcosokat rejtette, akik azután éjszaka kimásztak a ló hasából, és kinyitották a város kapuit a görög seregnek, amely a város közelében rejtőzött. Trója elesett - a hackerek pedig a magukévá tették a trójai faló ötletét.

Trójainak tehát egy szoftvert nevezünk, amelyről azt sem tudjuk, hogy a számítógépünkre került, mégis mérhetetlen károkat okozhat. Hogy a trójai eltitkolja az elhelyezését, álcázást használ, akárcsak a görög katonák.

4.2 Miből áll egy trójai?

Először is tudni kell, hogy miből is áll egy trójai. Az *RFC 1244 (Site Security Handbook) így* írja le a trójait (a szerző fordítása): *Trójai lehet egy program, amely valami hasznosat vagy csak valami érdekeset csinál. Mindig valami váratlant tesz, például a tudtunk nélkül jelszavakat lop vagy fájlokat másol.*

Még egy kicsit világosabban leírva: a trójai egy meg nem engedett kód egy legitim programon belül - tehát az eredeti program megváltoztatása. Különböző műveleteket hajt végre, amelyekről a fertőzött rendszer felhasználója mit sem tud. A trójai lehet egy hasznos program, amelybe meg nem engedett kódot ágyaztak - ilyenkor a program a trójai program hordozójaként működik. De lehet egy olyan program is, amely látszólag hasznos funkciókat hajt végre, de az engedélyezetlen kódja alapján olyan funkciókat is elvégez, amelyekről a fertőzött rendszer felhasználójának nincsen tudomása.

A legegyszerűbb formájában a trójai *egyszerűen egy kémprogram* lehet, amely információkat közvetít úgy, hogy a bevitt adatokat egy előre megadott e-mail-címre küldi a következő online-kapcsolatnál. Ez a tipikus feladata egy keylogger-nek, amely egy fájlba naplózza felhasználói beviteleket, vagyis egy keyboard logfájlt készít. Jóval komplexebbek azok a programok, amelyek nemcsak adatokat küldenek el, hanem a számítógép távirányítását is lehetővé teszik. Itt mutatkozik meg a trójaiak és a klasszikus távkarbantartó programok hasonlósága, amelyek távoli számítógépek hálózaton vagy telefonvonalon keresztüli kezelését teszik lehetővé.

Hogy az akciók lehetőségei milyenek lehetnek, az kiderül a továbbiakban a különböző trójai programok leírásából. Azonban a trójai és a származási helye között minden esetben kapcsolatnak kell lennie. Ez a kapcsolat manapság legegyszerűbben az interneten vagy egy hálózaton keresztül valósítható meg.

4.2.1 A szerver kiosztása

Ahhoz, hogy egy számítógép vagy annak az adatai elérhetővé váljanak, telepíteni kell a szervert a cél-, illetve áldozat PC-re. A szerver a központi program, amely lehetővé teszi az idegen számítógép „távirányítását". Csak akkor lehet egy (internetes vagy hálózati) kapcsolaton keresztül az IP-cím segítségével az idegen számítógépet elérni, ha a szerver - mint program - aktív. Úgy képzelhető el, hogy a hacker megpróbálja elhelyezni vagyis „szórni" a szervert a célrendszereken, hogy később egy klienssel célzottan érhesse el a kitelepített szervereket. Az elérés csak akkor jöhet létre, ha a fertőzött számítógépet az IP-címén keresztül sikerül megszólítania.

A hacker ilyenkor többnyire a következő problémákkal szembesül:

- A szervert el kell juttatni a felhasználóhoz, azaz „rá kell sózni".
- A felhasználót rá kell venni arra, hogy el is indítsa a szervert.
- A hackernek meg kell kapnia a fertőzött PC aktuális IP-címét.

Az elhelyezésre a hackereknek és az ilyen eszközök programozóinak is rengeteg ötletük van. A trójaik lehetnek programba integrálva vagy fájlokhoz fűzve (erről később többet). Az egyik legismertebb eset egy trójai elrejtése a Linux *SÁTÁN 1.0* programkódjában. Egy programozó hozzáfért egy fejlesztői géphez, amelyen a SÁTÁN 1.0 forráskódja volt, módosította a main()-funkcókat, megváltoztatta az *Fpinget* úgy, hogy a SÁTÁN indításakor a jelszófájlba egy bejegyzés került, amellyel egy új felhasználót jegyzett be, aki ezzel elérést kapott. Szerencsére a programozás nagyon hibás volt, így nem keletkeztek jelentősebb károk. Ez az eset is mutatja, hogy a hackerek nem csak az ismert módokat, mint pl. az e-mail mellékleteket, választják, hogy az áldozataikhoz jussanak.

A szerver futtatása általában két lépésből áll. Először is aktiválni, majd telepítem és konfigurálni kell a szervert a rendszeren. Ez a lépés többnyire az elhelyezéssel egybekötve történik, a szerverfájl mindjárt el is indul. A második lépésben el kell érni, hogy a szerver az operációs rendszerrel együtt automatikusan elinduljon, és a háttérben aktív legyen. Csak ezután lehet célzottan megszólítani.

Az IP-címet a trójaitól és az eljárás módjától függően különböző utakon kapja meg a hacker: az ICQ-val történő elhelyezés esetén a következő kapcsolatnál közvetlenül lekérdezheti az áldozat aktuális IP-címét. A komplex trójai programok, amelyeket később még bemutatunk, automatikus értesítést adnak, ha a fertőzött számítógép a hálózatra, illetve az internetre lép. Már csak az kell, hogy maga a hacker is online legyen a megfelelő időben, és megkapja a támadáshoz szükséges IP-címet.

4.2.2 A kliens otthon marad, és vezérli a szervert

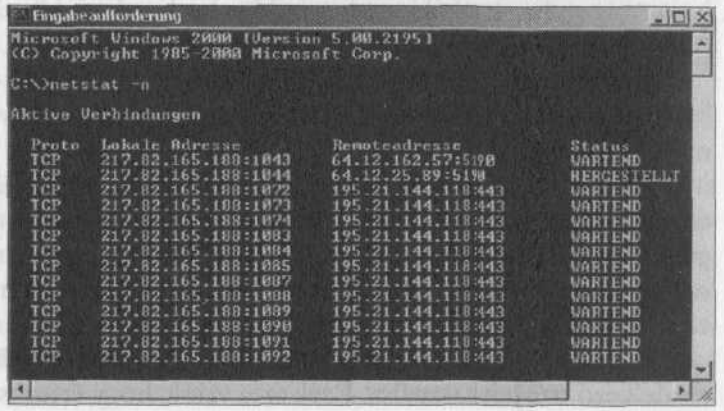
Ha egy trójai távirányítási funkciókat kínál, a támadónak egy vezérlőprogramra is szüksége van. Ezzel a programmal tud akciókat kiváltani a szerverrel a számítógépek között fennálló kapcsolaton keresztül. A kliens ehhez célzottan a fertőzött számítógép IP-címén szólítja meg a szervert. Az akciók lehetnek viszonylag ártalmatlanok, mint a CD-ROM-meghajtó nyitása, de kártékonyak is (adatok törlése) vagy kémkedők (adatok átadása).

Hogy a kliens milyen funkciókat tud vezérelni, az a felhasznált szoftvertől függ. A szerver konfigurálásánál meg lehet határozni a klienshez küldés módjait és az akciós lehetőségeket is, amelyeket a kliens el tud indítani. Ezzel a kliens az idegen számítógép irányítócentruma lesz. Hogy hogyan használja ki ezt a veszélyes potenciált, az a támadótól függ.

4.2.3 Hogyan szerzik meg a hackerek az IP-t?

A trójai használatához tehát szükség van a fertőzött számítógép IP-jére. Mivel a legtöbb felhasználó szolgáltatón keresztül létesít internetkapcsolatot, minden kapcsolódásnál egy másik, *dinamikus IP-címet* kap. Ez megnehezíti a trójai szerver elérését, mert nem lehet tudni, hogy a fertőzött számítógép egyáltalán online-ban van-e, és ha igen, milyen IP cím alatt. A legkönnyebben úgy lehet megkaparintani az aktuális IP-t, ha mondjuk átvitel közben IRC-n vagy ICQ-n keresztül, tehát amikor fennáll a kapcsolat a fertőzött számítógéppel, *DOSparancssor-ra* váltunk, és ott beírjuk: *netstat - n*. Ezután igen könnyű kiolvasni remote címekből a trójai szerver IP-jét.

A kapcsolat könnyen felismerhető



Egy másik lehetőség, ha nincs fennálló közveden online-kapcsolat, *válogatás nélkül címeket szkennelni.* Ehhez a legtöbb trójainak *integrált szkenneré* is van, amellyel meghatározott IP-tartományokat lehet tapogatni. És már meg is lehet fogni a klienssel egy fertőzött számítógép szerverét, és irányítani lehet azt. Ez így nagyon egyszerűen hangzik, de nem leéli feltétlenül annak lennie. A különböző trójaiak leírása a továbbiakban következik.

Ha a szerver automatikus értesítésre van beállítva, az IP-keresés viszonylag egyszerű. Amint a fertőzött számítógép kapcsolatba lép a hálózat-

tál, illetve az internettel, a szerver átküldi az aktuális IP-t a kliensnek, amennyiben az éppen online van, vagy mail-ben küldi el az aktuális IP-t. így tud a hacker célzottan rajtaütni a fertőzött számítógépen.

4.3 így álcázzák és terjesztik a trójaiakat

A veszélyes kis programok terjesztésére a legkülönbözőbb lehetőségeket agyalták ki a programozók. A profik például más programokba integrálják a trójaiakat, hogy könnyen és gyorsan tudják terjeszteni. A hobby-hackerek, ha hiányoznak a programozási ismereteik, inkább más utakat választanak. A trójaiak minden esetben veszélyesek, mert annak a szándékait uralják, aki a szervert vezérli.

A következőkben nemcsak az egyszerű álcázásokkal ismerkedünk meg, hanem a hobby-hackerek eljárásaiba is betekintünk. Erről az internet idevágó fórumain olyan rengeteg információ gyűlt össze, hogy abból már igazi „gyűjtemény" áll össze. A stratégiák egy része valóban profinak is mondható, míg mások inkább csak a hobby-hackerek eszközei közé sorolhatók. PC-felhasználóként mindenesetre ismernünk kell ezeket.

Hogy egy pillantást vethessünk a dolgok menetére, egy *Defcon4* nevű hackercsoport (csak csekély mértékben módosított) szövegét fogjuk használni.

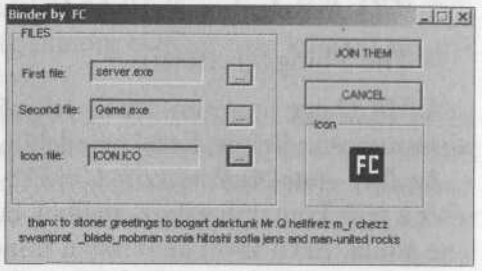
„A szervert mail-ekén, ICQ-n vagy IRC-n keresztül küldjük. Képnek álcázzuk (valami nem gyereknek való mindig jól jön) vagy toolnak, attól függően, hogy az áldozat mit kíván. Tedd fel hasznos programként a honlapodra, vagy kérj meg egy baráti webmestert, hogy kínálja a honlapján, azt persze nem kell elmondani, hogy trójait rejtettél bele. Ha már így elterjeszted a szervert a nép körében, akkor nem rossz, ha megfelelő értesítőfunkciókkal rendelkező trójait használsz. Ezek arra valók, hogy értesítsenek, amint az áldozat online van, és mail-ben vagy ICQ-n keresztül üzenetet küldjenek neked, amelyben bizonyos információkat kapsz az áldozatról és számítógépéről, pl. az IP-t, amire szükséged van, hogy bekösd a szervert."

4.3.1 A trójaiakat fájlokba integrálják

A szervert össze lehet kötni különböző fájlokkal, pl. .GiF, JPG, tehát képekkel, vagy be lehet építeni segédprogramokba, tehát *EXE* fájlokba. Ehhez a hálón nagyon sok program áll rendelkezésre. Egyes trójai kiteknek, mint például a *Sub7*-nek, olyan funkcióik vannak speciális konfigurációs fájlokban (Editserver), amelyekkel a legkülönbözőbb fájlokkal lehet összekötni a konfigurált szervert, sőt még a szerver ikonját is meg lehet változtatni. Ez akkor célszerű, ha az áldozatot valóban meg akarjuk téveszteni egy fájllal. Ehhez minden ikon felhasználható, amelyeket a programok egyébként is használnak: a képek JPEG fájlként megtévesztően hasonlítanak az eredetire, így a vélt DOC fájlok egy megnyugtató Winword ikont tudnak prezentálni.

A szerver fájlokhoz fűzése a következő előnnyel jár: ki lehet indulni abból, hogy az áldozat nem fogja gyanúsnak találni vagy rossz szándékot feltételezni arról a programról vagy a képről, amelybe a szerver be van ágyazva.

Ikon-kiosztás a szervernek



Olyan programnak, amelybe a szervert ágyazzák, különösen alkalmasak az animációk és a gag-programok. Ezeket mindenki szívesen küldi és nézegeti.

4.3.2 Álcázás a WinZip-pel

A trójai ügyes elhelyezéséhez a világ leggyakrabban használt tömörítő programjának, a W*inZip-nek* a programbeállításait is használják egyes hackerek. Ilyenkor egy új WinZip archívot készítenek, és más fájlokkal (képek stb.) együtt csomagolják össze a szervert. A *run command after unzipping* parancs az archívból történő kicsomagolás után azonnal elindítja a szervert. Ezután a *melt server after installation* szerver opció segít, mert ez a sikeres telepítés után azonnal törli a szervert. Az archív ártalmatlan önkicsomagoló fájllá változik, és máris van egy tökéletesen álcázott trójai.

4.3.3 A trójaiakat az ICQ-val is tovább lehet adni

Ön is kedveli ezt a kényelmes kommunikációs szolgáltatást az interneten? Van már egy listája kedvelt „beszélgetőpartnereiről"? Akkor valószínűleg érdekelni fogják azok a lehetőségek, amelyek az ICQ-nak köszönhetően adódnak a hackereknek.

Nos, ez így megy (megint a Defcon4 „információi" szerint):

Először begyűjtünk minden eszközt, amire szükségünk lesz. Ezek az alábbiak lennének:

- A Sub7 trójai (magyarázat 1. lent)
- MICQ (többször elindítja az ICQ-t)
- ICQ-AutoAuthorize/IP-Unhider Patch
- The Thing (kis trójai)

A *MICQ* egy program, amely lehetővé teszi az ICQ több példányának a párhuzamos indítását. Ezzel egyidejűleg lehet online két vagy több UIN.

Az *ICQ Auto-Authorize/IP-Unhider-Patch* megengedi UIN-ek hozzáfűzését a saját kontaktlistához, anélkül, hogy a másiknak ehhez engedélyt kellene adnia. Ezen kívül az infóban minden személy IP-jét megmutatja, akkor is, ha ez a funkció nálunk nincs aktiválva (az IP-ről és kiosztásáról lásd az alapismeretekről szóló fejezetet).

A *The Thing* egy kis trójai. A legtöbb trójai a sok szolgáltatás miatt már eleve akár 400 Kbájt is lehet. Tehát akinek van egy kis tapasztalata, az könnyen kiszámolhatja magának, hogy mi rejtőzik egy ilyen fájl mögött. A The Thing ezzel szemben csak kb. 40 Kbájt (nagyjából annyi, mint egy nagyobb kép). Amint ez a fájl az áldozat gépén egyszer lefutott, megnyílik egy hátsó kapu, amelyen át más fájlokat lehet feltölteni és végrehajtani.

Álcázás az ICQ-val

Ha lehet, akkor amilyen jól csak lehet, álcázzuk a saját identitásunkat. A legjobb, ha generálunk egy új ICQ-UIN-t (a MICQ-val többel is online lehetünk egyszerre). Férfi áldozatokhoz általában a női identitás az ideális.

Megkeressük az áldozatot a trójai terjesztéséhez, és hozzáfűzzük a kontaktlistához. Ekkor reális az esélye annak, hogy az áldozat észreveszi a támadást, hiszen a kontaktlistát a beleegyezése nélkül bővítették. Ilyen esetben már csak ártatlan kifogások segítenek, amelyben olyan fogalmak, mint hacker meg hasonlók garantáltan nem fordulnak elő.

Ha a fájl küldéséhez az ICQ-t használjuk, a régebbi ICQ-verziók egy kis búgját is kihasználhatjuk: ezek általában nem mutatják meg a fájlvégződéseket. Ha egy fájlt *photo.jpg.exe* nek nevezünk el, átvitelkor csak a *photo.jpg* jelenik meg, és ez nem különösebben feltűnő.

A hacker ráér

A szervert általában nem az első kapcsolatfelvételnél küldjük el az ICQ-n keresztül. Sokkal jobb, ha kezdetnek elküldünk egy pár tiszta fájlt. Egy pár nap múlva azután már sokkal kisebb feltűnést kelt bármilyen állomány.

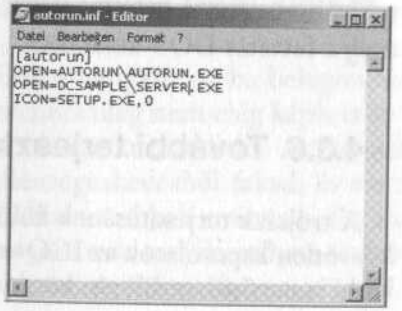
Az áldozatot persze nem kényszerítjük, hogy elfogadja a fájlt. Ha a fájlt visszautasítja az ICQ-n keresztül, még mindig el lehet neki küldeni egy pár nappal később egy anonim mail-fiókról.

„Ha az áldozat tényleg gyanítja, hogy egy fájl mögött vírus vagy trójai rejtőzik, egyszerűen várni kell pár napot, valamit fecsegni, és aztán egy nagyon kicsi fájllal megpróbálkozni, amilyen például a The Thing. Mint már mondtuk, ez a trójai túl kicsi ahhoz, hogy feltűnjön."

4.3.4 Elég egy CD és az automatikus lejátszás funkció

A trójai kihelyezésének egyik kedvelt módja a CD-n keresztüli terjesztés. Ezt többnyire a közeli környezetben található célok megtámadásához választják. Ehhez egy program vagy egy játék kalózmásolatát használja a hacker. A CD-ROM-on megváltoztatja *az Autorun.inf fájlt.*

Egy Autorun.inf szövege, amely egy trójaira utal



Az alapelv a következő: a felhasználó beteszi a CD-ROM-ot a meghajtójába, és a szerver automatikusan elindul a játék bevezetőjével együtt, anélkül, hogy észrevehető lenne. Ehhez a Windows 9.x automatikus lejátszás funkcióját használja ki a hacker. Ez egy CD-ROM felismerése után azonnal kiértékeli a megfelelő *Autorun.inf* fájl adatait és végrehajtja a fájlt. Esetünkben tehát a szervert is.

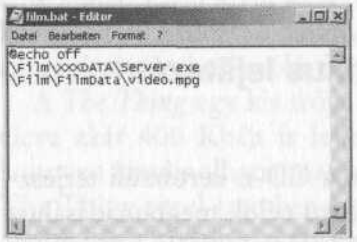
4.3.5 A lemezek majdnem ugyanígy működnek

Ez az alapelv a lemezekre is átvihető, és ekkor a következőképpen működik.

A hacker létrehoz egy mappát a lemezen, amelynek például *Film* a neve. Ebben a mappában létrehoz még két további mappát; az egyik neve mondjuk *Film Data,* a másiké *Xxdata.*

A *Film Data* mappába másolja a tulajdonképpeni filmet (*.AVI vagy *.MPEG fájlt), a *másik Xxdata* mappába másolja a szervert.

Most az editorral készít egy batch-fájlt (kötegelt parancsfájlt) a lemez főkönyvtárában, és *Film.bat* néven menti.



A batch-fájl **elindítja a szervert**

Ha ezt a lemezt most megkapja a felhasználó, és elindítja a *Film.bat-ot,* a trójai is elindul. Az *@echo* parancs szolgál arra, hogy a user előtt ne jelenjen meg a futtatás DOS-ablakban.

4.3.6 További terjesztési stratégiák

A trójaiak terjesztésének különböző stratégiái immár világossá váltak. A közvetlen kapcsolatok az ICQ-n keresztül elsősorban a közelebbi és a távolabbi ismerősök területén könnyítik meg a terjesztést, az internet-kapcsolat anonimitása védi a tettest, és támadhatóvá teszi az áldozatot. A terjesztés CD-n keresztül is inkább a hobby-hackereknek való, mert a hordozó csak a tartalma révén (játék, feltört program stb.) válik igazán vonzóvá.

A talán legfontosabb és legsikeresebb eljárás *a letöltésre kínált anyagokkal és a vírusokkal* való terjesztés. Ebben a két esetben más késztetések vannak a háttérben, mert az ilyen tömeges fertőzések mind a tervezés, mind a kiértékelés/felhasználás szempontjából sokkal ráfordítás-igényesebbek.

Egy trójait gyorsan nagy számban elhelyezni nemcsak ideális álcázást kíván - a Kurnyikova-vírus jó példa a sikert ígérő környezetekre, amelyek magas rákattintási és ezzel installálási arányt garantálnak. Emellett természetesen *terjesztési stratégiát* is kell fejleszteni, amely lehetővé teszi az elhelyezést világszerte több ezernyi számítógépen. Ez a legegyszerűbben *férgekkel (warm)* érhető el, amelyek úgy szaporodnak, hogy a levelezési címlisták minden címére elküldik magukat. Ezzel szemben egy letöltésre kínált anyagot először fáradságosán ismertté kell tenni, mielőtt a megfelelő számú kihelyezés megtörténhetne. Addig pedig a terv még csődöt is mondhat.

Egy nagy számban kihelyezett trójaiból beérkező adatokat természetesen ki is kell értékelni, mert nem minden trójai kínál valóban érdekes adatokat a hackereknek. Az olcsó szörfözésre utaló jelszavak viszonylag érdektelenek. Fontosabbak a hálózati hozzáférési jelszavak stb.

Természetesen egy trójaival jelentős károkat lehet okozni, de ha csupán a nagy mértékű pusztítás a cél, egy vírus végülis sokkal sikeresebb. Ez utóbbinál nem kell célzott támadásokkal és hasonlókkal bajlódnia a hackernek, hanem egyszerűen az időfaktorra (dátumvezérlés) vagy a használati gyakoriságra (a rombolás x fájlindítás után indul) épít. A trójai tulajdonképpen minden esetben olyan támadási technikát jelent, amelynél *fontosabb a hozzáférés, mint a rombolás.*

4.3.7 Mit csinálnak a hobby-hackerek a trójaiakkal?

A kérdés az első hallásra figyelemreméltóan hangzik, de ha belegondolunk, a legtöbb ember ugyan kíváncsi, de technikailag nem elég képzett ahhoz, hogy célzottan jelszavakat vagy hasonlókat kutasson ki. Az adatok azonnali tönkretétele inkább személyes ellenségeskedésből fakad, és erre, mint azt majd a következő fejezet mutatja, alkalmasabbak a vírusok. Persze azért ez a motívum sem zárható ki. És mostanra már tudják, milyen stratégiákkal tudja egy hacker célzottan megközelíteni az áldozatát.

A legtöbben azonban, akik csak úgy kísérletezgetnek egy kicsit ezzel, tulajdonképpen nem is tudják, hogy valójában mit is akarnak kezdeni az áldozat gépén. Általában kíváncsiság és egy adag vandalizmus rejtőzik a háttérben, amint azt a következő, az interneten található „szabályokból" is láthatjuk.

„Ha sok fantáziával és több ICQ-UIN-nal végre sikerült egy trójait elültetnünk az áldozat számítógépén, nem kell mindjárt nekikezdeni a mulatságnak. Először túrd át pár napig az áldozat gépét, és nézd meg az összes adatát. Áthelyezhetnél fájlokat, információkat fűzhetnél dokumentumokhoz, megváltoztathatnád a startlapját, és tovább tanulmányozhatnád a trójai sok funkcióját.

Legyetek szívesek, ne nagyon bántsátok az áldozat adatait. Mindannyian tudjuk, hogy az már nem túl vidám dolog, ha fontos adatokat veszítünk el.

Amint hozzáférünk az áldozat adataihoz, elsőként töröljük a C. *\windows\netstat.exe-t.* Én személy szerint teljes mértékben az adatmegsemmisítés ellen vagyok. Ezzel a Windows programmal viszont minden hálózati kapcsolatot meg lehet nézni...azért ez förtelmes lenne, nem?"

Önfertőzés ügyetleneknek

Azoknak a hobby-hackereknek, akik kísérletezés közben saját magukat fertőzik meg trójaival, a következő tanácsot tartja készenlétben az internet: „Ha az ember az első fertőzési kísérleteknél saját magát fertőzi meg, akkor egyszerűen kliensként összeköttetésbe lép saját magával (a saját gép IP-je mindig 127.0.01!), fogja, és törli a szervert!"

4.4 Sub7 - egy trójai rémisztő lehetőségekkel

A *Sub7,* egy backdoor-trójai, 1999 márciusában került a hálóra az első verziókban, egy *Mobman* álnéven működő programozó „válaszaként" a *NetBusra* és a *BackOrifice-vz.* Azóta ez a backdoor-tool folyamatosan tökéletesedik és új funkciókkal bővül. A Sub7 a legkomolyabb és a neten legelterjedtebb trójaiak közé tartozik. Hogy világszerte milyen sok rendszer volt Sub7-tel fertőzött, illetve hogy még most is az, azt az úgynevezett *portszkennek* mutatják, amelyek „több mint elég" fertőzött rendszert jelentenek.

```
0000CB90 AD39 AB6E 670E 6613 5047 4692 53C8 25BC .9.ng.f.PGF.S.%.
0000CBA0 5804 1672 C734 B175 801B 0DC8 6F0B 4342 X..r.4.u....o.CB
0000CBB0 F8E1 CC93 9472 406D 6F76 AD18 CF5D 4252 .....r@mov...]BR
0000CBC0 4D19 09A9 6B1F 215D 4173 4973 4224 C786 M...k.!]AsIsB$..
0000CBD0 4452 1B50 616C 0941 C898 0468 7192 4D9A DR.Pal.A...hq.M.
0000CBE0 10A2 0C0E 1000 6C93 1841 6B29 6401 E1C6 ......l..Ak)d...
0000CBF0 BF3D 19AD 7DDB 2AC6 6788 4490 BF56 D212 .=..}.*.g.D..V..
0000CC00 6623 3F15 6320 7DC4 2616 4124 C910 C17B f#?.c }.&.A$...{
0000CC10 0592 145A 4913 262E CF24 A409 2E08 9643 ...ZI.&..$.....C
0000CC20 339B F57B 8311 8454 6F6C 0E73 6C13 3618 3..{...Tol.sl.6.
0000CC30 4428 4499 0C36 8111 D6DE 215D 9B31 4260 D(D..6....!].1B`
0000CC40 2EDF C338 B8C3 0641 0F4D C273 0152 EBC2 ...8...A.M.s.R..
0000CC50 FD6F A408 626D 9CE5 0901 C029 67FD 04F0 .o..bm.....)g...
0000CC60 0E31 FDB3 11D6 2002 435A F40E 9033 171B .1.... .CZ...3..
0000CC70 390F 36F4 04D8 1B52 3F25 46DC C062 B3CD 9.6....R?%F..b..
0000CC80 2110 21C3 009B CD0E B877 A44E B305 E155 !.!......w.N...U
0000CC90 73A0 8516 D0A9 B5AD D04B 1AD0 7427 382B s........K..t'8+
0000CCA0 1500 87C6 4FBA 02B3 D962 DF25 233C 1332 ....O....b.%#<.2
0000CCB0 14DA 2B1D 533D 2023 A0B3 6CAE 2F01 C4D9 ..+.S= #..l./...
0000CCC0 C79B 11EE 6C72 0941 9104 8644 D450 9D6A ....lr.A...D.P.j
0000CCD0 9166 34DC 40E5 EB82 1FAF 1566 0AE4 641B .f4.@......f..d.
0000CCE0 D56D 756C A749 AAF1 B572 E064 310B D696 .mul.I...r.d1...
0000CCF0 2E07 5ED3 728F 3800 5F97 0FB2 EDB2 56E6 ..^.r.8._.....V.
0000CD00 0D1D 50BB 6B0D AC7D 38D8 0942 6F0C 4B69 ..P.k..}8..Bo.Ki
0000CD10 C166 15B5 33D3 A15B 5649 0A68 B253 0210 .f..3..[VI.h.S..
0000CD20 450F C725 CDCA 9954 B7F6 BB25 2964 B27A E..%...T...%)d.z
0000CD30 626E 751E F22D 7B01 0A8E 0C44 C20B D8D2 bnu..-{....D....
0000CD40 6B9A 701E B916 2818 361B 701C DCB2 0B26 k.p...(.6.p....&
0000CD50 0B4B 6368 403D 5984 6417 8A6F 7920 ED73 .Kch@=Y.d..oy .s
0000CD60 4BC6 63F2 4465 66C4 B3C7 C162 1006 78A4 K.c.Def....b..x.
```

Pillanatkép egy trójairól

4.4.1 Támad a Sub7

A *Sub7* tágabb értelemben egyfajta távkarbantartó programhoz hasonlítható. A távkarbantartó szoftver, azaz a *remote access tool* vagy *remote administration tool,* a rendszergazdák távkarbantartó és konfigurációs munkáját könnyíti meg a hálózatba kötött számítógépeken, nagyobb hálózatokban. Ismert remote access program pl. a *PCAnywher* a *Symantectől.*

Destruktív módon felhasználva, egy ilyen szoftverrel a teljes ellenőrzést át lehet venni egy fertőzött számítógép felett. Ez azt jelenti, hogy a megfelelő kliens tulajdonosa minden olyan funkciót végrehajthat a fertőzött gépen, amit a gép tulajdonosa is megtehet. Az egyes funkciók későbbiekben történő említése bizonyosan hozzá fog járulni az ilyen szoftverből eredő potenciális veszélyek felméréséhez.

Egy olyan trójai, mint a Sub7, több fájlból áll, amelyek egymáshoz kapcsolódva gondoskodnak a támadó gép és a fertőzött gép kapcsolatáról.

A Sub7 szervere

A szerver ahhoz szükséges, hogy a műveleti konzolok (kliens) között kapcsolatot teremtsen, és irányítsa a fertőzött gépet. Ennek a modulnak tehát feltétlenül telepítve kell lennie az irányítandó rendszerre ahhoz, hogy Sub7-es fertőzöttségről lehessen beszélni.

Minden működést a kliens irányít

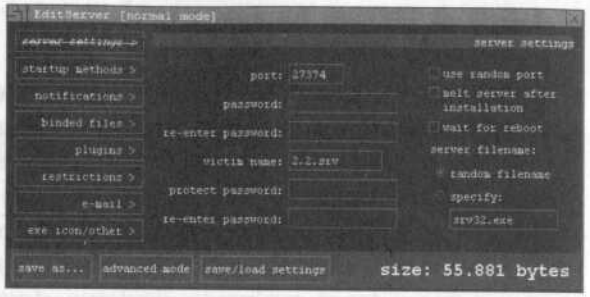
A kliensre azért van szükség, hogy a trójai egyes funkcióit inicializálja, és ezzel irányítóközpontként működhessen. A klienst teljesen hagyományos Windows-programként kell elképzelni, grafikus felülettel, gombokkal, menükkel és kiválasztómezőkkel, amelyekről egészen kényelmesen el lehet indítani az egyes funkciókat.

A Sub7-nek kapcsolata van a szerverre!

Edit-Server

Az *Edit-Server* egy kiegészítő program, amellyel a szervert lehet konfigurálni. Itt lehet például rögzíteni, hogy miként telepítse magát a célgépre a szerver, továbbá itt lehet meghatározni a szerver nevét is. Ehhez jönnek egyes ICQ-beállítások (értesítés, jelszókikémlelés, UIM-kicsomagolás), a port, amelyről a trójai kommunikál (az újabb verziókban véletlenszerű is lehet - itt a port a futási időben derül ki), és hogy a felhasznált port rejtve legyen-e. Azt is meg lehet adni, hogy a szerver közvetlenül a telepítés után azonnal elinduljon-e, és hogy egy másik futtatható fájlhoz kapcsolódjon-e, hogy az a szervert az installáció előtt elrejtse.

Pillantás a Sub7 váltóközpontjára



így előkészítve sokféleképpen közelíti meg a támadó az áldozatát, és megkísérli a célrendszerre telepíteni a szervert.

4.5 BackOrifice 2K - Hálózati eszköz vagy támadás a Microsoft ellen

1998. augusztus elején mutatta be a texasi *Cult of the Dead Cow* hackercsoport a *BackOrifice Windows Remote Administration Tool-t* egy hackertalálkozón, Las Vegasban. Egy ügyesen programozott kliens/szerver alkalmazásról volt szó, amely trójai falóként észrevétlenül tudott futni egy Windows 9x operációs rendszeren. Ugyanezen év augusztus 7-ig a programot több mint 35 ezerszer töltötték le a CDC honlapjáról.

A BackOrifice célja - állította a hackercsoport - a Windows 95/98 alatti súlyos biztonsági hiányosságok feltárása. És ehhez a program nem a Windows operációs rendszer valamiféle búgjait vagy belső dokumentálatlan API-jeit használja, hanem kizárólag dokumentált Windows funkcióhívásokat.

A Microsoft válasza nem váratott magára sokáig, bár azt nem ismerték el, hogy Windows 9x alatt biztonsági problémák lennének.

A 2000-ben a Cult of the Dead Cow (CDC) kihozta a BackOrifice új verzióját: a *BO2K-t.* A CDC ezzel a verzióval „trójainak" kikiáltott programjának a hírén akart javítani, és új képességekkel bővítette, így például a magasfokú titkosítással, amely csaknem lehetetlenné teszi, hogy az átvitt adatok egy harmadikhoz kerüljenek. Különösen ennek kellett a BO2K-t érdekessé tenni a hálózati rendszergazdák számára. A hackereket azonban ezek a dolgok nem nagyon érdekelhették, mert a BackOrifice ezután is az egyik legkedveltebb trójai maradt.

4.5.1 A BO2K és összetevői

íme egy áttekintés a legfontosabb fájlokról és funkcióikról a távkarbantartási funkciók és a trójai működés komplex együttműködésében.

Fájl	Funkció
bo2k.exe	Ez a szerver. Ha elindul, automatikusan a C:\Windows\System könyvtárba másolja magát. A Registry-be is bejegyzi magát úgy, hogy minden Windows-indításkor automatikusan aktiválódjon. Ha a szerver csak egyszer is elindul, a gép már megfertőződött. A szervert kiegészítő részekkel (pluginek) még bővíteni lehet.
bo2kgui.exe	A kliens a BO2K „látható" része. A grafikus felhasználói felületen keresztül lehet a fertőzött PC-t távirányítani, anélkül, hogy különösebb ismeretekre lenne szükség róla. Mielőtt a kliens a szerverrel kapcsolatba tudna lépni, néhány dolgot még be kell állítani rajta (jelszó stb.). Az IP (ez a címe egy PC-nek az interneten) is szükséges a kliens és a szerver összekötéséhez.
bo2kcfg.exe	Ezzel a programmal lehet fontos beállításokat (kódolás, port, amelyen a szerver és a kliens összekapcsolódnak, a szerver neve, amelyen a rendszerkönyvtárba másolódik stb.) végezni a szerveren, és kisebb bővítéseket (pluginek) hozzáfűzni.

Fájlok és funkcióik együttműködése

A BO2K legfontosabb fájljaihoz jön még néhány plugin:

Fájl	Funkció
bo2k_inetcmd.dll	Lényegében ezek a szerver alapfunkciói. Ez a plugin gondoskodik arról, hogy fájlokat lehessen kicserélni.
enc_serpent.dll	A SERPENT feladata, hogy az adatok kódoltan közlekedjenek a kliens és a szerver között.
io_stcpio.dll	Ez a plugin az első pillantásra ugyan nem nyújt új lehetőségeket, de ez kódolja a TCP-csomagok headerét. így ezeket nem lehet BO2K-adatforgalomként (Traffic) felismerni.
srv_rattler.dll	Ez a plugin látja el az értesítési funkciókat: ha a szerver elindult, a Rattler mailben elküldi az áldozat IP-jét.

BO2K pluginek

4.6 így ismerjük fel a trójait a rendszerünkben

Most, hogy a trójai falovak bevetésének a lehetőségei és potenciális veszélyei ismertté váltak, felmerül a kérdés, nem vagyunk-e már magunk is fertőzöttek. Ezért szeretnék itt néhány lehetőséget bemutatni, hogyan lehet felismerni és leküzdeni egy rendszerben a trójai vírusokat. A gyakorlatlan felhasználónak ez nehéznek tűnhet, mivel az ilyen programok keresése gyakran beavatkozásokat igényel a rendszerbe, illetve a Registry-be. Vannak azonban olyan programok, amelyek jelentősen megkönnyítik a standard trójaiak felkutatását.

4.6.1 Vírus- és trójai-szkenner

Alapvetően minden rendszerben mindig kell *telepített vírusvizsgálónak* lennie. Továbbá feltétlenül szükséges, hogy ez állandóan aktualizálva legyen, hiszen szinte naponta fedeznek fel új trójaiakat.

Az első vizsgálat előtt figyeljünk arra, hogy a *Minden fájl ellenőrzése* vagy hasonló funkció aktív legyen. Ezt a gyártók gyakran nem állítják be előzetesen, mert a szkennelés így túl sokáig tarthat. Arra is figyelnünk kell, hogy a szkenner ne törölje azonnal a fertőzött fájlokat, mert egyes trójaiak szerzői biztonsági intézkedéseket építettek a programjaikba az eltávolításnak e módja ellen, és ez a vírusvizsgálónak jelentős problémákat okozhat, Sőt bizonyos esetekben még ahhoz is vezethet, hogy a rendszer használhatatlanná válik - vagy jobban mondva: a gép totál lefagy. *Mobman* például beépített egy ilyen funkciót a Sub7-be.

Ha a vírusvizsgáló fertőzést talál, a megtisztítás különböző lehetőségeit fogja javasolni. Először - mint mondtuk - tekintsünk el az érintett fájlok törlésétől, hogy elkerüljük az esetleges károkat. Próbáljuk meg a fájlokat izolálni, illetve karanténba tenni.

Ha a vírusvizsgáló nem talál fertőzött fájlokat, az még messze nem jelenti azt, hogy a számítógép tiszta. A trójai rejtőzködhet - és megtéveszteti a víruskeresőt. Hogy az ilyen esetekben mit tehetünk, azt a következő szakasz részletezi.

A trójaiak leküzdésének most következő módjánál nagyon óvatosnak kell lennünk. Ha nem vagyunk biztosak magunkban, inkább kérjünk tanácsot szakembertől.

4.6.2AutoRunbejegyzések

Egy trójai csak akkor működik, ha a rendszerindítással együtt elindul. Ez azt jelenti, hogy a szervernek a rendszer hátterében állandóan futnia kell, hogy online kapcsolat esetén kész legyen parancsokat fogadni a klienstől.

Autostart (Indítópult)-mappa - kevésbé valószínű

Klasszikus változat az automatikusan indítandó programok indítására az *autostart (Indítópult)-mappa.* Ez az indítási lehetőség azonban nagyon valószínűtlen, mert nagyon nagy a felfedezés valószínűsége.

Az *Indítópultot* a következőképpen lehet ellenőrizni: közvetlenül a *Start* menüből: *Start Programok Indítópult* vagy *C:\Windows\Startmenu\ProgramokMndítópult.* Az olyan rendszereknél, mint a Windows NT, a mappát a felhasználói profilokon keresztül lehet megtalálni *(C:\WinNT\Profiles\ Username \Startmenü\Programok \Indítópult).*

Itt aztán szokatlan dolgok után kell kutatni, és esetleg programokat, illetve parancsikonokat kell törölni, amelyeket nem ismerünk, és egy trójait indíthatnának el.

A Win.ini a Windows 3.x-es időkben volt érdekes

Régebben nagyon kedvelt módszer volt a *Win.ini* bejegyzésein keresztül indítani a trójaiakat. Hogy ezt kizárjuk, írjuk be a *Start/Futtatásba* a *sysedit.exe-t.*

Nézzük meg a *Load* és a *Run* paraméterek mögötti bejegyzéseket. De persze a parancsokat többnyire rengeteg üres karakterrel álcázzák a paraméter-megnevezések mögött, hogy ne legyenek rögtön láthatóak. Gördítsük az alsó gördítősávot egyszerűen jobbra, míg a sor végét is látjuk.

Szükség esetén távolítsuk el a gyanús bejegyzéseket.

System.ini - elég ritka

Ebben a fájlban a *shell=* paraméter alatt fordulhat elő bejegyzés. Óvatosan! Itt már van egy *Explorer.exe* nevű bejegyzés, ezt semmiképpen se töröljük! Az *Explorer.exe* után azonban még további bejegyzések következhetnek. A *System.ini-t* ugyanúgy nyitjuk meg szerkesztésre, mint a *Win.ini-t.*

autoexec.bat - DOS-os hulladék, kis rizikófaktorral

Itt is óvatosnak kell lenni a törléssel, mert ide is bejegyzi magát néhány ártalmatlan program. A trójaiak ritkán használják ezt a lehetőséget. Mivel azonban ez a lehetőség is adott, hát megemlítjük. Az *autoexec.bat-ot* is a *sysedit.exe-vel* lehet megnézni és szerkeszteni.

config.sys - csak a szokatlan eszközmeghajtók veszélyesek

Néhány ritka trójai a Windows 95/98-s rendszerek eszköz-meghajtójaként is álcázza magát. Ezeket a trójaiakat azonban nehéz realizálni, és szerencsére nagyon ritkák is. A *config.sys* szintén a *sysedit.exe-vel* lelhető fel.

winstart.bat vagy control.ini - lehetséges, de nagyon ritka

Ha a w*instart.bat-ban* felismerhető egy bejegyzés, ez rendszerint azt jelenti: egy parancssor egy fájl másolását írja elő, amelyet az utolsó rendszerindítás előtt töröltek. Eddig alig ismertek olyan trójaiak, amelyek ezt az utat használnák. A *control.ini-ben* is el lehet helyezni egy bejegyzést az automatikus indítás céljából- de ez is nagyon ritka.

4.6.3 Windows Registry - ez már izgalmas

A regisztrációs adatbázisban megnevezett útvonalak mappákként jelennek meg, az illető ikonra duplán kattintva érjük el őket. Itt megintcsak ajánlatos az óvatosság, mielőtt bármit is törölnénk. Az indulásnak ezt a lehetőségét a rendszerindítással együtt sok ártalmatlan program (pl. uninstall-programok, vírusvizsgálók, backup programok stb.) is használja, de a trójaiak is. Számos más Registry-bejegyzési lehetőség is előfordul autorun célból, de persze ezeket (szerencsére) csak ritkán használják a trójaiak.

Hasznos segítség a Windows saját *msconfig* programja is. Menjünk egyszerűen a *Start* gombra, aztán a *Futtatás*-ra, és írjuk be *msconfig.* Ezzel a programmal a fent nevezett bejegyzések közül sokat ellenőrizhetünk, és kényelmesen megváltoztathatunk. A sysedit-tel is sokat megtalálhatunk a fentiek közül. Járjunk el úgy, mint az *msconfig-nál,* helyette azonban ezt írjuk be: *sysedit.* Több ablak is megnyílik szövegszerkesztő formában.

Következőként hívjuk meg a *Rendszerleíró adatbázis-szerkesztőt* a *Start/Futtatás/Regedit*-tel. Megnyílikegy program félelmetesen sok bejegyzéssel. Ezek közül csak néhány útvonal érdekes:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion
➥RunServices
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion
➥RunServicesOnce
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion
➥Run
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion
➥RunOnce
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion
➥Run
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion
➥RunOnce
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion
➥RunServices

Vannak még az úgynevezett „Unknown-módszerek", illetve a Windows-regisztráció, a shell paraméterrel.

Itt is a Windows Registryt használják a program automatikus indításához. Ezek alatt az útvonalak alatt a következő bejegyzések találhatók:

HKEY_CLASSES_ROOT\exefile\shell\open\command\ @="%1"%"*
HKEY_CLASSES_ROOT\comfile\shell\open\command\ @="\"%1\"%"*
HKEY_CLASSES_ROOT\batfile\shell\open\command\ @="\"%1\"%"*
HKEY_CLASSES_ROOT\htafile\shell\open\command\ @="\"%1\"%"*
HKEY_CLASSES_ROOT\piffile\shell\open\command\ @="\"%1\"%"*
HKEY_LOCAL_MACHINE\Software\CLASSES\batfile\shell\open
➥command\ @="\"%1\"%"*
HKEY_LOCAL_MACHINE\Software\CLASSES\ comfile\shell\open
➥command\@="\"%1\"%"*
HKEY_LOCAL_MACHINE\Software\CLASSES\ exefile\shell\open
➥command\ @="%1"%"*
HKEY_LOCAL_MACHINE\Software\CLASSES\` htafile\shell\open
➥command\ @="\"%1\"%"*
HKEY_LOCAL_MACHINE\Software\CLASSES\ piffile\shell\open
➥command\ @="\"%1\"%"*

A „%1" %*" karakterek elé be lehetne írni még egy programot. Rendszerint azonban csak az itt megnevezett bejegyzések vannak. Ha valamelyik kulcs még egy futtatható fájlt is tartalmaz, amögött egy trójai rejtőzhet. Gyanú esetén ne az egész bejegyzést távolítsuk el, hanem csak a program nevét!

ICQ-usereknél fennáll egy további lehetőség a következő bejegyzésnél:
HKEY_CURRENT_USER\Software\Mirabilis\ICQ\Agent\Apps\test
„Path"=test.exe" „Startup"="c:\\test" „Parameters"="" „Enable"="YES"

Registry Installed Components

HKEY_LOCAL_MACHINE\Software\Microsoft\Active Setup\Installed Components

A default érték: *„Trójai"\StubPath – C:\WINDOWS\SYSTEM\"trójai".exe*

Registry Common Startup kulcs

HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsqCurrentVersion\explorer\User shell folders.

A bejegyzés általában *C:\WINDOWS\SYSTEM\dv*.

Ez alatt az útvonal alatt található a szerver is.

Eszközmeghajtónak álcázás

Egy trójai, mint már említettük, eszközmeghajtónak is álcázhatja magát. Ilyen esetben nem egyszerű a pontos azonosítás. Végülis lehet az egy valódi meghajtó is, aminek a törlése rendszerproblémákat okoz. Itt is egy Registry-be került bejegyzést keresünk, azonban egy „szokatlan" path-on:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\ervices\VxD\InrLD

4.6.4 Módszerek az Explorer.exe-vel a C:\ meghajtóra

Egy bug miatt a Windows először mindig az első, megtalált *explorer.exe*-t futtatja le (kétséges esetben a C:\ könyvtárban), mielőtt a tulajdonképpeni *explorer.exe (C:\windows\)* elindulna. Az *explorer.exe* a C:\ -n azt eredményezhetné, hogy legközelebb egy trójai töltődik be, amely a *C:\windows\system* könyvtárban vagy máshol található.

4.6.5 A runonce.exe kicserélése

Csak a *Schoolbm* trójainál ismert. Az eredeti Windows *runonce.exe-t* egy módosított fájlra cseréli, amely így lehetővé tesz egy autorun eljárást. Az eredeti *runonce.exe* mérete a Windows 95 alatt 11264 bájt, Windows 98/ME alatt pedig 40960 bájt. Tehát ha találunk egy *runonce.exe-t,* amelynek más a mérete, akkor itt is el lehet rejtve egy trójai. Hangsúlyozzuk, LEHET! Ennek a módszernek a további magyarázatához az angolul értők olvassák el a *Schoolbus 2.0* trójai leírását, amely a **http://serdarka.8m.com/** weboldalon található.

„Futó folyamatok ellenőrzése" módszer

Gyakran lepleződik le egy trójai úgy, hogy a „futó feladatokat" ellenőrizzük. Itt futtatható fájlokról van szó, amelyek a rendszerrel „együtt futnak". Ezeket különböző módokon lehet megfigyelni.

Például a **Ctrl+Alt+Del** billentyűkkel. Megjelenik egy ablak, amely mutatja a futó programokat, amelyeket ennek megfelelően be is lehet zárni. Ez a módszer azonban egyáltalán nem biztos, mert a legtöbb trójai „tudja", hogy kell elrejtőzni a *Taskmanager* elől.

A Windows-zal azonban egy jó kis eszközt is kapunk a futó folyamatok ellenőrzéséhez. A program neve: *DrWatson*. A *Start* menü *Futtatás-ba* írjuk be: *drwatson*. A program elindul, és először elvégez néhány vizsgálatot. Menjünk a *Nézet* menüpontra, és válasszuk a *Mindent megmutat* opciót. Kezdőknek azonban a *DrWatson* bonyolultnak tűnhet, mert tényleg mindent könyörtelenül megmutat, ami a Windows alatt adódik. A Windows 2000-be is integráltak egy nagyon jó folyamat-nézőkét, amelyet a *Taskmanager-rel* együtt lehet elindítani.