Vigyázat! Botok!

Napjainkban tömegesen bukkannak fel a vírusok a neten, ha egy nap nem fedeznek fel újat, akkor mindenki meglepődik.

Az IRC-én van egy olyan kifejezés, amibe lépten-nyomon belebotlunk. Ez a szó a következő: bot. A robot rövidítéséből származik. Egyszerűen egy automatizált IRC klienst jelent, ami bizonyos eseményekre reagál.

Hogyan kapcsolható össze a két dolog? Nagyon könnyen. Gondoljuk csak el, hogy valaki egy sereg gépet szeretne irányítani, amelyeket valamire fel szeretne használni. Persze azt akarja, hogy egyszerre cselekedjenek. Itt jön képbe az IRC, mint ideális felület. Ha egy csapat botról van szó, amik egy meghatározott csatornán tömörülnek, akkor egyetlen szó beírásával, mintegy parancsszóra nekiindul a sereg, és teszi a dolgát.

Sokan alábecsülik ezeknek a jelentőségét, mondván, hogy ezek csupán egyszerű vírusok vagy hátsó kapuk. Viszont ha jobban a dolgok mögé nézünk, akkor megdöbbentő tényeket fedhetünk fel. A vírusos gépek számáról készülnek felmérések, mindenki tisztában van a veszéllyel. Az ilyen „alvó bestiák” számáról egészen sokáig semmiféle adat nem volt. Napjainkban viszont, amikor számuk hihetetlenül megnőtt, már kellő figyelmet fordítanak erre a problémára is.

A CERT egyszer, különös késztetést érezve utánanézett a dolognak. Pár napos munkával találtak két olyan bot-hálózatot, amik több ezer gépet foglaltak magukban. Erről írtak is, közzétették, mit tapasztaltak, és kértek mindenkit, hogy ha lehet, tegyen ez ellen. Ez volt talán az első ilyen hivatalos felmérés.

Az év elején egy amerikai IRC szolgáltatót zártak be, mert a tulajdonos egy DDoS-bérlő rendszert működtetett. Több embernek is fizetett azért, hogy azok a saját 5-10 ezer gépből álló hálózatukkal ellehetetlenítsék a konkurencia Internet elérését és megjelenését.

Nemrégiben egy norvég Internet szolgáltató (a Telenor) emberei találtak és hatástalanítottak egy tízezer botból álló hálózatot. A hálózatot arra használták, hogy DDoS támadást indítsanak weblapok ellen.

A Symantec az év elején napi 2000 botot futtató gépet fedezett fel. Júniusban ez a szám már 30 ezer volt naponta! Ez természetesen nem azt jelenti, hogy ezek egy kézben vannak. De mindenképpen elgondolkodtató a számuk növekedése.

Egyre több hasonló botnet van, amelyek „zombi” gépekből állnak össze. Ezeket a gépeket valamilyen módon ellátják egy bot programmal, ami a felhasználó számára szinte észrevétlenül lapul, de a megfelelő parancsokkal aktivizálni lehet. Ezeknek a programoknak a terjedését nagyon elősegíti a sok trójai vírus és biztonsági rés, amiknek a segítségével bejutnak az adott gépre.

A rosszindulatú botok általában a rendszer ismert sebezhetőségeit használják fel arra, hogy bejussanak a gépbe. A legismertebb botok szinte napról napra változnak, mindig újabb támadási lehetőségekkel látják el „valakik”.

Egy az ilyen ismertebb botok közül például a Gaobot-család, amik több ismert Windows sebezhetőséget kihasználva terjednek. Megjegyzem ezeknek a sebezhetőségeknek nagy részére már létezik javítócsomag, csak nem mindenki használja ki a lehetőséget, hogy feltelepítse.

Ha bekerült a gépbe, akkor szintén több fronton „jeleskedik”. Mondhatni teljesen szokásos, hogy DoS támadást lehet vele véghezvinni. Ezen kívül a változatai nagyon sokrétűek: némelyik játékok kulcsait próbálja ellopni az áldozat gépéről, némelyik FTP vagy email szervert tartalmaz, némelyik elmenti a felhasználó billentyűleütéseit, más pedig azzal kezdi tevékenységét, hogy az ismertebb antivírus-programok működését lehetetlenné teszi. Ez csak pár kiragadott példa volt sajnos, ennél sokkal veszélyesebbek.

A védekezés ellenük nem kíván sok erőfeszítést. Ha minden nap csak öt percet törődünk ezzel, máris védettnek, vagy legalábbis jobban védettnek mondhatjuk magukat. Ha csak annyit teszünk, hogy az operációs rendszerünket rendszeresen frissítjük, máris sokat tettünk. Ha ezután felteszünk még valamilyen antivírus programot is (megéri rászánni azt a kis összeget) esetleg a gépünkre valamilyen PFW (Personal FireWall) programot is telepítünk, akkor nyugodtabban aludhatunk, mert a mi gépünkön kevesebb támadási felület van, mint egy átlagos felhasználói gépen.

Ez a helyzet ma. Hogy mi lesz holnap, senki sem tudja. Újabb operációs rendszer sebezhetőségeket fedeznek majd fel, a botok ezeket kihasználják, egyre több dologra lesznek képesek… ez mind csak feltevés, de nagyon reális. Egy azonban teljesen biztos: a számuk növekedni fog.

Többször említettem a cikkben a **DoS**-t. Szerintem manapság már mindenki tisztában van vele, mit jelent. Ha mégsem, akkor röviden: a Denial of Service rövidítése. Olyan támadások gyűjtőneve, amiknek az a célja, hogy egy szolgáltatás vagy egy gép ne tudja elvégezni azt a munkát, amire szánták. Webszerverek esetén ne tudja a honlapot megmutatni, FTP esetén ne tudja a felhasználó elérni, „mezei” felhasználó esetén ne tudjon az internetre kapcsolódni. Ezt általában úgy érik el, hogy a megtámadott gépet olyan mennyiségű vagy minőségű adattal árasztják el, amitől az vagy teljesen válaszképtelen lesz, vagy a kapott adatok feldolgozása tölti ki minden idejét. A DDoS támadás a DoS egy speciális fajtája, amikor a támadás nem egy gépről érkezik, hanem több gépről egyszerre, megosztva (Distibuted Denial of Service). Az ilyen támadások sokkal hatékonyabbak és sokkal gyorsabban célt érnek a támadók.

Balla Imre - ircmania@talpak.org