Még olcsóbb a botneted

2013.08.01. csütörtök

Ahogy Bruce Willisnek moziepizódról epizódra még drágább lett az élete, a számítógépes kártevők feketepiacán ezzel szemben sajnos egyre olcsóbban lehet munícióhoz jutni.

Mielőtt egyáltalán belekezdünk a témába, írjunk le annyit, hogy a kártevővel fertőzött számítógépek távolról vezérelhető botnetes hálózata a felhasználó tudta nélkül vesz részt különféle számítógépes támadásokban, jellemzően ilyen például a DDoS és a spamküldés. De természetesen a gépen levő bizalmas anyagokat, adatokat, jelszavakat, banki belépéseket is ellopják ezzel a módszerrel. Ilyen kártékony hálózatokat már jó néhány - talán nyolc - éve lehet bérelni, és az egyik leghírhedtebb a SpyEye botnet volt, amely elsősorban banki adatokra utazott. Egy ilyen botnetes banda általában teljes körű "szolgáltatást" nyújt az ügyfeleinek, vagyis tetszőleges időtartamra bérelni lehet a fertőzött gépekből álló botnetes hálózatot, természetesen nonstop technikai támogatással, egységesített adminisztrációs felületről vezérelve, saját statisztikai modullal, sőt a vevők különféle pénzintézetek online webbanki oldalai ellen már előre elkészített támadókódokat is kaphatnak.

Talán az egyik első jelentősebb, vagy talán csak valóban széles körben publikált eset az volt, mikor a BBC televíziócsatorna 2009-ben a Click! című számítástechnikai műsorában egy felettébb furcsa kísérletre szánta el magát: botnetet béreltek és szemfelnyitási, figyelmeztetési céllal bemutatták mindezt. Azt az aspektust, miszerint bármilyen - esetünkben demonstratív céllal - tették is ezt, egyes megítélések szerint akkor is ezzel már törvénytelenséget követtek el, sőt még saját etikai kódexüket is megsértették, most tegyük félre. Tegyük emellett félre azt is, vajon valóban hasznos-e ennyire részletesen bemutatni, milyen egyszerű mindezt véghez vinni, és nem pont tanfolyam vagy kedvcsináló lesz-e inkább egy ilyen riport, és ezzel éppen hogy kontraproduktívvá válik. Sőt, hagyjuk figyelmen kívül azt is, hogy a közszolgálati TV, azaz az adófizetők pénze ebben az esetben a bérbe vett botnetes üzlet miatt közvetlenül a bűnözőkhöz került.

Szóval nézzük kizárólag csak azt a részt, mibe került ott a "szolgáltatás". Már az akkori árak is erőteljes mélyrepülésben voltak a korábbiakhoz képest, hiszen javában kezdődött-mélyült a világméretű pénzügyi válság, egymás alá ígértek a bűnözői csoportok, sőt lopták is egymás forráskódjait. Nos tehát 2009-ben jóval a korábbi ezer dolláros ár alatt, már 400 USD - mai árfolyamon körülbelül 90-100 ezer forint - kellett egy ezer gépes botnet bérléséhez. A feketepiacon folyamatosan egyre olcsóbban beszerezhető kártékony kódok, botnetek és exploit kitek miatt már a 2010-es esztendőt is a "botnetek évének" titulálták egyes szakértők, ha azonban az idei ajánlatokat nézzük meg, akkor még jobban meglepődünk. Az EU-n belüli országokban található ezer gépes botnet ma már egy hónapra csak 50 dollár, azaz nagyjából tízezer forint.

És ha ehhez hozzávesszük a webkamerán keresztül titokban megfigyelt lány, a 20 éves glasgow-i *Rachel Hyndman* esetét, és szembesülünk azzal, hogy 1, azaz EGY dollárért már vásárolható száz férfi webkamerához vagy egy nőihez való illegális hozzáférés, talán mindenki érzi, mennyire nagy a veszély. Annyi mindenesetre bizonyos, hogy arra semmiképpen nem lehet naivan számítani, hogy holmi magasabb erkölcsi aggályok vagy éppen az árfekvés visszatartaná az ilyen tömeges támadásokat.
