

„Az internet egy veszélyes üzem”

Csizmazia István, IT biztonsági szakértő, Siccontact Kft.

Kikre jelentik a legkomolyabb veszélyt az internetes csalók?

A mai világban annyira gyakoriak a csalások minden téren, hogy nagyszüleink már elvesznének, az ő jóhiszeműségük ma már öngyilkosság lenne. Elég az ál-villanyóraleolvasókra, a porszívót több százezerért részletre eladó cégekre, a nyugdíjasokat ingyenes termékbemutatóval erőszakosan vásárlásra kényszerítő vállalkozásokra vagy a „nyertes” telefonkártya sorszáma után érdeklődő telefonos csalókra gondolni. Egy mai fiatal azonban már annyira sokféle csalásról hallott, olvasott, hogy gyanakvóbban, gyakorlatiasabban áll hozzá a kétes ajánlatokhoz.

Mely országok eladóival érdemes különösen óvatosnak lenni?

Románia már rég felkerült az árverési portálok feketelistájára az említett „kifizetik, előre utalják a pénzt, de aztán végül nem küldenek semmit” trükk miatt.

Emellett gyakori, hogy az ígért Macbook vagy számítástechnikai eszköz helyett csak egy téglá, zsák krumpli, kő, fadarab van a csomagokban. Ha nem is ilyen rossz megítélés alá esik, de sajnos Magyarország renoméja is bizonytalan a Magyar Posta megbízhatatlansága miatt: Ghánával, Indonéziával, Malajziával, azaz kiszámíthatatlan országokkal soroltak minket egy kategóriába a rengeteg elveszett, ellopott küldemény miatt.

A Russian Business Network és más hasonló orosz, ukrán, román bűnszervezetek magas szakértelemmel, jól szervezeten dolgoznak, és folyamatosan új ötletekkel, trükkökkel, bérbe adható botnet-hálózatokkal, szaktudás nélkül is használható kártevőterjesztő készletekkel árasztják el a piacot. De az ellopott személyes adatok folyamatos adásvételével is busás nyereségre tesznek szert. Vannak országok, pl. Kína, Vietnam, Románia, Ukrajna, Oroszország, ahol a törvénykezés lassabb, engedékenyebb, lazább. Illetve ha nemzetközi, több országon átívelő, vagy nemzetközi bűnbanda által végrehajtott a bűncselekmény, úgy a bizonyítási eljárás is sokkal nehezebb, körülményesebb.

Mennyire képesek megvédeni bennünket az erre hivatott programok?

A vírusirtók közül már jó néhány képes a gyanús szkriptet tartalmazó weboldalak blokkolására, így a NOD32, illetve az ESET Smart Security is ilyen. Ha egy weboldal kódjában kártékony átirányítás (pl. *Iframe elem*) található, a program azonnal figyelmeztet. Emellett létezik egy külön adatbázis is, amely a kártékony webcímek listáját tárolja, és ha egy hivatkozás ilyen helyre mutat, arra is kapunk külön riasztást. Ez az adatbázis, a vírusismereti szignatúrákhoz hasonlóan, szintén rendszeresen frissül. A legtöbb védő-



program az MSN és más üzenőprogramok mellékleteit, linkjeit is képes hatékonyan ellenőrizni, hiszen a közösségi és csevegőoldalakon különösen sok adathalász, illetve kártevőre mutató linket tartalmazó üzenetet kaphatunk.

Természetesen böngészőből érdemes a biztonságosabb változatokat (például Opera, Firefox) választani. Hasznos szokás lehet a böngészés utáni rendszeres cache-ürítés, a session cookie-k törlése (amik bizonyos körülmények közt ellophatók), valamint néhány kiegészítő biztonsági plugin használata is például az alábbiak közül: NoScript, NetCraft Toolbar, ShowIP, Finjan, Adaptive Referrer remover, Cache Status, Cookie Safe, Live HTTP headers, JS View, Secure Login, XSS Guardian, XSS Warning.

Mit tehetünk még megelőzőképpen?

Akármiilyen jó is a gép automatikus védelme, mindig sok múlik a felhasználón. Gyanús linkekre például még akkor sem szabad rákattintani, ha az azt tartalmazó levél vagy üzenet látszólag ismerőstől érkezett.

A webes vásárlásokat is viszonylag könnyen lehet biztonságosabban intézni, külön erre a célra kért webes kártyával – ez többnyire csak egy darab papír, amelynek azonban saját Mastercard-száma és lejáratát ideje van. Egyáltalán nem kell rajta pénzt tartani, hanem csak és kizárólag az egyes tranzakciók előtt pár perccel átutalni az éppen szükséges összeget a normál banki számláról. Nagy előnye ennek a módszernek, hogy a webes kártya száma nyugodtan kiadható a netes vásárlásoknál, E-bay-en vagy bármilyen webáruház regisztrációnál.

A mottó lehetne egy Rejtő Jenő-idézet: „Jobb egy pillanatig gyávának lenni, mint halottnak életünk végéig.” Amint a cikkből is látható, az internet egy veszélyes üzem, érdemes tehát óvatosnak lenni, folyamatosan tanulni. És rendszeresen olvasni híreket és cikkeket az internetes védekezésről, kockázatokról – ehhez jó muníciót ad például az antivirus.blog.hu oldal is.