

Másvilág

2013.10.08. kedd

Vannak, akik szerint nem a világ lett rosszabb, csak a hírszolgáltatás lett jobb. A magunk részéről ezt másképp látjuk, a hírek gyorsabb és tömeges áramlása mellett az egy emberre jutó csalások, átverések száma is exponenciálisan növekedett az utóbbi években, és nincs ez másképp a számítógépes felhasználók esetében sem.

Ha megnézzük az ezzel kapcsolatos felméréseket, kutatásokat, sok érdekességet találhatunk. Először is, ha a Halon amerikai internetezők körében 2013 augusztusában végzett vizsgálatának adatait elolvassuk, látható, hogy döntő többségük, egészen pontosan 94,7 százalékuk kapott már olyan e-mailt, amelyben vírus, kémprogram vagy valamilyen kártevő volt. Ez következik a nagy számok törvényéből, a maradék 5,3 százalék meg valószínűleg nem értette a kérdést. Nagyjából 8,8 százalékuk meg is nyitotta az ilyen mellékletet megfertőzve ezzel a számítógépet, és ezzel ismét egy fontos mérföldkőhöz érkeztünk. Ugye, sok számmal kapcsolatos szabályt szoktunk emlegetni itt az informatikában, például a 20-80-as Pareto elvet, vagy a Moore törvényt a 18 havonta megduplázódó teljesítményről. A számítógépes csalásokkal kapcsolatban is létezik egy 5 százalékos elvi határ, ha az adathalászattal, vagy más elektronikus csalással megtévesztettek száma eléri az 5 százalékot, a bűnözőknek már megéri spamekkel, kártékony URL-ekkel, mérgezett kereső találatokkal bombázni a tömegeket. És akkor ehhez képest látjuk a fenti 8.8 százalékot.

A jobb-rosszabb szűrés ellenére beeső spamek, kéretlen üzenetek már régen nem reklámról, kéretlen értékesítési csatornákról szólnak, ahol hasonlóan Rolex órát vagy olcsó Viagrát akarnak ránk sózni. Az ilyen üzenetek fő csapásiránya inkább a megtévesztés, sebezhetőséget tartalmazó melléklet vagy link felkínálása, adatlopás, vírusfertőzés, kémkedés. Persze azt is meg kell mondani, ebből egy eset is lehet sok, ha az például éppen mivelünk történik. De hasonlóan szomorúak lehetnek a New York Times szerkesztőségében is, ahol a kritikus kémkedési események szintén egy gyanútlan, kíváncsi alkalmazott által e-mailben kapott PDF állományra való kattintással kezdődtek.

Még a fenti vizsgálatra visszatérve minden harmadik amerikai beismerte, hogy simán megnyitja a gyanúsnak látszó leveleket is, ha az üzenet tárgya számára érdekesnek hangzik. A nők inkább a közösségi oldalak nevében érkezőkre harapnak, míg a férfiak jobbra a pénzkereséssel, illetve szexuális témák esetén esnek kísértésbe. Gyors haszon a tőzsdén, különleges gyógyszer akció, azonnali adó-visszatérítés, Windows crack, kiemelkedő jövedelem napi egy óra otthoni munkával, univerzális szériaszám generátor minden víruskeresőhöz, vagy Kurnyikova meztelen fotói. Vegyük észre, hogy itt viszont már egyáltalán nem 5%-nál, nem 8,8-nál, hanem 33%-nál járunk.

És akkor a gyakoriságra is térjünk még vissza. Egyetlen perc, azaz hatvan másodperc alatt 216 ezer fényképet osztanak meg a felhasználók az Instagramon, 1,8 millió lájk és 41 ezer új poszt keletkezik a Facebookon, és 83 ezer USD forgalmat bonyolít le az Amazon webáruház. 204 millió e-mail üzenetet küldenek világszerte, 278 Twitter bejegyzés születik, de új weblapok is keletkeznek, szám szerint 571 darab. Az egy perc időtartam alatt 70 új domén bejegyzése is megtörténik, 72 órányi videót töltenek fel a felhasználók a YouTube rendszerébe, 15 ezer dalt töltenek le ezalatt az iTunes-ból, de Google keresésből is 2 milliót indítanak a netezők.

Szóval igaz a hírszolgáltatás javulása, de a támadások, kártevők, átverések szempontjából drámai átrendeződés zajlott le, és aki nem a klasszikus "kavarja ez most, vagy nem kavarja" gondolatával közelít az ártalmatlan közösségi üzenetekhez, ártatlannak tűnő e-mailekhez, látszólag hivatalos szervektől, banktól érkező adatbekérő levelekhez, az könnyen áldozattá válhat. Tetszik, nem tetszik, van a védekezési feladatoknak olyan szegmense is, ami nem delegálható tovább a pusztá technikának, számítógépnek, védelmi programoknak, hanem a mi aktív közreműködésünket,

biztonságtudatos hozzáállásunkat, gondolkodásunkat igényli, és ezt a képességet mindenkinek egy életen át csiszolgatnia, fejlesztenie kell.

És még egy utolsó adalék, ami szemünk fényeiről, gyermekeinkről szól. Egy 2013-as felmérés – melyben tízezer 13 és 22 év közötti megkérdezett válaszait összesítették – azt írja, a fiatalok szerint az internetes zaklatás nagyon is gyakori, 20%-uk akár napi szinten tapasztal valamilyen durva hangvételi fenyegetést, és ez egyaránt fenyegeti a lányokat és a fiúkat is. A rosszindulatú, lejárató tartalmak víruszerű gyorsasággal terjednek, ami rengeteg emberhez eljut, és ez nagyon lehangoló lehet az áldozatok számára, nem is beszélve arról, hogy ami egyszer felkerül a netre, az gyakorlatilag később már eltávolíthatatlan. A megfélemlítések, titkos webkamerás kukkolások, megszegyenyítések gyakran katasztrofális hatást gyakorolnak az önbecsülésükre, vagy borítják fel fenekestül korábbi megszokott társadalmi életüket. Ami talán ebből megint előremutató fontos gondolat lehet, hogy nem csak egyedül a bántalmazott baja mindez, hanem a történet minden egyes szereplője is tehet, vagy tehetne ellene, itt is van még tanulni valónk. A szülők, a tanárok, az osztálytársak mind-mind viselnek ebben valamekkora felelősséget, és az elhallgatás a lehető legrosszabb, leghibásabb stratégia ebben a kérdésben.

Összességében az események, incidensek sűrűsége nyilvánvalóan változóban van. Az, hogy a számítógépes bűnözésből már 2007-ben az USA-ban több bevétel keletkezhetett, mint a kábítószer-kereskedelemből, valóban riasztó. A 2001 és 2009 évek internetes bűncselekmények számainak összevetéséből már akkor 667,8 százalékos növekedést mutattak ki a szakemberek, és persze a válság sem tett jót ennek a közegnek, a víruslaborok mára napi 60-200 ezer egyedi mintát dolgoznak fel. Az előző évszázad lassúságához, betárcsázós BBS és ADSL internetjéhez képest ma már egész más, felfokozott, állandóan online és kissé túlságosan inger gazdag világ van. Mindenesetre egy biztos: amíg egyetlen ember is akad, aki elhiszi egy böngészőben kéretlenül felugró ablaknak, hogy valóban ő nyerte az ingyen iPhone-t, iPadet vagy az 1000 dolláros kupont, a nyeremény reményében pedig kész kiadni személyes adatait, kéretlen üzenetek linkjeire kattint, kártevőt telepít, addig lesz tennivaló az oktatás és képzés vonalon.