

|| FŐOLDAL

|| SZOLGÁLTATÁSUNKRÓL

|| SZAKÉRTŐK KERESÉSE

|| FELTALÁLUNK! ÉRDEMES?

|| MINDENKIT ÉRDEKELHET

|| RENDEZVÉNY RÁDIÓ ÉS
TELEVÍZIÓ

Szakértőt keres? Mi megtaláljuk Önnek!

Szolgáltatásunkról bővebben [ide kattintva olvashat!](#)



Index

< 2009 >

Február

Január

< 2008 >

December

November

Október

Szeptember

Augusztus

Július

Június

Május

Április

Március

Február

Január

< 2007 >

December

November

Október

Szeptember

Augusztus

Július

Június

Május

Április

Március

Február

Január

Ajánlott böngészők: Internet Explorer 7+
Mozilla FireFox 2+

Nyomtatás

Mindenkit érdekelhet

2009. Február

A bankok vagy adataink biztonsága. Ez itt a kérdés?

Február 5.-én az Országos Rendőrfőkapitány és a bankok biztonsági vezetőinek értekezletén javaslatok hangzottak el a bankoknak a bankrablások elleni védelmével kapcsolatban.

Ezek közül néhányról az országos televíziós csatornák is beszámoltak.

Többek közt arról, hogy a bankok ne csak a saját belső területet figyeljék kamerákkal, hanem a bejáratok távolabbi külső környékét is. Ezek a külső kamerák olyan sűrűn készítsenek képeket, hogy minden bankba érkezőről készüljön kép. Ezt azzal indokolták, hogy a tettesek a bank előtt szokták felvenni a sisakot, símaszkot, harisnyanadrágot, kendőt az arcuk eltakarására, nem távolabb, mivel ha nem így tennének az igencsak feltűnő lenne.

Az egyik adásban viszont az Adatvédelmi Biztos ezt a személyes adatok védelme szempontjából aggályosnak tartotta.

Valóban jogos ez a félelem?

Amennyiben az így gyűjtött adatokat korlátlan ideig őriznék a bankok, úgy természetesen igen, hiszen minden arra járóról nyilvántarthatnák, mikor volt ott.

A nyomozás számára azonban csak az esetleges bankrablást közvetlenül megelőző egy-két percben érkezők képei lehetnek fontosak. Elég tehát a gyűjtött képeket igen rövid ideig őrizni. Ez lehet pl. egy óra, ami után letörölődne. (Azért nem csak egy-két perc, mert akkor már a rablás alatt megtörténne a törlés.) Egy ilyen rendszer tehát még kevésbé lenne veszélyes személyes adataink biztonságára, mint a térfelügyelő kamerák.

Azt kell tehát csak ellenőrizni, hogy az adatok valóban törlésre kerüljenek. Ez pedig ugyanúgy történhet, mint a térfelügyelő kameráknál.

Nem kérdés tehát, hogy a bankok vagy a személyes adatok biztonsága a lehetséges.

(Ezen a jogi természetű akadályon felül elhangzott az is, hogy az angliai tapasztalatok szerint ez nem hatékony intézkedés, mert ott van a legtöbb bankrablás Európában. Lehet, de ez nem megelőzi a rablást, hanem elősegíti a rabló megtalálását. Amennyiben ez sikeres lesz, talán a rabló jelöltek is jobban meggondolják, hogy próbálkozzanak-e? Akkor mégiscsak kevesebb lesz a rablás. Ez pedig fontos eredmény.)

Simonyi Endre

A Google-on hirdetőik adataira utaznak

Google-on hirdetőik adataira utaznak - a Virtumonde és kilenc másik kémprogram okozza a fertőzések 25%-át - Az amerikai Sunbelt Software kutatócsoportja, a Sunbelt Threat Research Center 2009 februárjában is megjelentette toplistáját a 2009 januárjában legfertőzöttbb kémprogramokról és számítógépes vírusokról. A listát a Sunbelt szakemberei a VIPRE

Antivirus+Antispysware vírusirtót használó és a Sunbelt ThreatNet™ káros alkalmazásokat regisztráló hálózatában résztvevő felhasználók automatikus visszajelzései alapján készítik. A kutatásban bárki részt vehet, aki használja a VIPRE antivírust, vagy a plusz védelmi réteggként is alkalmazható CounterSpy kémprogram-eltávolítót. A fertőzések negyedét tíz kártevő okozza. Az újévben tovább folytatódott a tavalyi év második felében elkezdődött fertőzés-koncentráció: a januári fertőzések immár közel 25%-át csupán tíz kémprogram okozza. Közülük is kiemelkedik a Virtumonde, amely tavalyi év végén került a toplista élére, letaszítva a sokáig egyeduralkodó Zlob.MediaCodecet. Ez a kémprogram egymaga a fertőzések közel 5%-áért felelős. Korábban egy-egy listavezető trójai mindössze a fertőzések 1%-áért volt okolható. A Sunbelt toplistája egyébként őrzi az év végén kialakult képet: eltűntek róla a trójai letöltők és a komplex károkozók uralják. A toplista második helyén a böngésző keresési eredményét megváltoztató Explorer32.Hijacker található, míg a harmadik helyre a többfunkciós Zango reklámprogram került fel, a negyedik helyen pedig a reklámlablakokat megjelenítő Hyperlinks Rotator helyezkedik el. Az ötödik helyet az Adware.Agent reklámprogram család, míg a hatodikat egy újdonság foglalta el: a Plus18Point reklámokat jelenít meg és eltéríti a böngészőt – például átírja a kezdőoldalt, illetve manipulálja a keresési eredményeket. A hetedik és nyolcadik helyen a meglátogatott honlappal konkurens hirdetések megjelenítő Hotbar.ShopperReports reklámprogram, illetve a programcsalád többi tagja együttesen található. A kilencedik helyre a C2.Lop böngésző eszköztár csúszott le, míg a tízedik helyre a WhenU.Save kémprogram került, amely folyamatosan figyeli a felhasználó böngészési szokásait, és a meglátogatott oldalak függvényében jelenít meg a tartalomhoz többé-kevésbé illő hirdetéseket. Adathalászok utaznak a Google és a Yahoo hirdetői felületére. Nem érezhetik magukat biztonságban azok, akik a Google, vagy a Yahoo hirdetési szolgáltatásait veszik igénybe. Az elmúlt héten olyan lánclevelekre figyeltek fel a Sunbelt szakemberei, amelyek megtévesztő módon az adwords-noreply@google.com címről érkeztek, s arra kérték a felhasználókat, hogy látogassák meg az adwords.google.com honlapot, ott pedig ellenőrizzék a felhasználónevékhöz kapcsolódó jelszavakat. A hamis portált felkereső egy olyan úrlappal találták szembe magukat, amelyen részletesen meg kellett adniuk nevüket, cégük nevét, telefonos és e-mail-es elérhetőségeiket, illetve országukat. A hamis oldal továbbá különböző .eu végű ödésű, hitelesnek tűnő domainekre irányította a látogatókat, ezzel is erősítve a valódiság látszatát. A Google felhasználók olcsón megúszták a Yahoo Marketing Solutions ügyfeleit ért levelekhez képest: ők ugyanis olyan üzenetet kaptak, hogy hirdetési egyenlegük elérte a 0-át, aminek következtében nem jelenik meg többé az általuk megrendelt reklám. A lánclevél továbbá azzal fenyegette a felhasználókat, hogy ha nem lépnek be az e-mailben megadott linken található számlára, törlik a számlájukat. A hivatalosság látszatát ebben az esetben azzal próbálták elérni, hogy a Yahoo Customer Support oldalra vezető linket is elhelyezték. Természetesen az összes megadott link hamis belépési, illetve ügyfélszolgálati oldalra vezetett. Sokan bedőltek és jelentős összegeket helyeztek el a bűnözők által üzemeltetett honlapokon megadott számlákra. „Hiába gondolnánk, hogy Google hirdetési felületeit igénybe vevő vállalkozókat nem lehet egy ilyen átlátszó trükkel becsapni. Sokan bedőltek a trükköknek, akik az átverést komolyan véve jelentős összegeket utaltak át a bűnözőknek, amelyeket már soha nem látnak viszont.” – mondja Bódis Ákos, a Sunbelt magyarországi képviselőjének vezetője. Hasonló átverés érte az egyéni szoftvervásárlókat is, akiknek az így feltört számlákkal népszerű termékeket hirdettek – így például a WinRAR fejlesztői adták ki figyelmeztetést, hogy a cég nevében megjelenő Google-hirdetések ál-webshopokba irányították a felhasználót, ahol pénzt kértek a WinRAR letöltéséért – ám az összeg végül nem a WinRAR-t fejlesztő német cég, hanem az orosz Roshal testvérek számláján landolt. A legfertőzösebb vírusok és kémprogramok 2009. januárjában Magyarországon:

1. Virtumonde (reklámprogram) A Virtumonde felugró ablakokban különböző kénytelen reklámokat jelenít meg, a háttérben pedig további károkozók letöltésére, és különböző összegyűjtött adatok elküldésére is képes. A fertőzést általában nehéz eltávolítani, több módszerrel is próbál a kémprogram-eltávolítók ellen küzdeni.

2. Explorer32.Hijacker (reklámprogram) A webböngésző önk honlapját és kereső oldalát is módosító kémprogram eltéríti a valódi kereséseket és a reklámprogram hirdetőinek megfelelő találati listát ad, valamint csökkenti a böngésző védelmi szintjét, ezáltal újabb fertőzések előtt nyitja meg a számítógépet. Ezt a reklámprogramot gyakran terjesztik más trójai letöltő szoftverek is, amelyeket ha nem azonosít védelmi rendszerünk, akkor általában egymás után számtalan ismétlődő vírusriasztást kapunk, amíg csak el nem sikerül távolítanunk a fertőzések valódi okát.

3. Zango (reklámprogram) A Zango az egyik legelterjedtebb és az egyik legszokásosabb reklámprogram család az interneten, ami szinte kivétel nélkül ingyenes programok mellé települ fel, sokszor a felhasználó tudta és beleegyezése nélkül. Legtöbbször böngésző beépülő modulként illetve keresési asszisztensként működik, és ingyenes alkalmazások, játékok, képernyővédők ök mellé „jár”. Működése során felugró reklámlablakokat jelenít meg, befolyásolja a keresési találatokat és különféle módokon zavarja a felhasználót a mindennapi munkában.

4. Hyperlinks Rotator (reklámprogram) A reklámprogram különböz ő hirdetéseket jelenít meg felváltva a felhasználó számítógépén. Általában az Internet Speed Monitor nevű alkalmazás telepítésére veszi rá a felhasználót, de lényegében mindegy, melyik reklámlablakra kattintunk, az legtöbbszőr további károkozók telepítéséhez vezet.

5. Adware.NetAdware (reklámprogram) A reklámprogram eltéríti a böngész ő honlapját és kéretlen eszköztárat is telepít, amivel különböz ő ál-antivírusok és hamis kémprogram-eltávolító szoftverek megvásárolására próbálja rávenni a felhasználót. Az ál-antivírusok letöltése és telepítése további fert őzésekkel jár, a programok esetleges megvásárolásával pedig hasznos hitelkártya adatokat gyűjtenek be a bűnöz ők. Sajnos a kiadott hitelkártyát többszőr is leterhelik különböz ő, általában kisebb, néhány ezer forintos összegekkel, így a már megtörtént vásárlást követ ően a védekezésre a legjobb módszer a kiadott hitelkártya adatainak minél el őbbi letiltása.

6. Plus18Point (reklámprogram, böngész ő eltérít ő) A böngész ő eltérítés mestere, a Plus18Point különböz ő károkozói a legváltozatosabb módokon épülnek be a böngész őbe, és „eltérítik”, vagyis módosítják a keresési találatokat, a meglátogatott oldalakat, vagy egyes variánsai akár a beírt honlapcímekeket. A meglátogatott oldalakat kéretlen reklámokkal is gazdagíthatják, vagy a szokásos keresési találatok helyett egy alternatív, a hirdet ők üzleti érdekeinek megfelel ő keresési találatokat jelenít meg. A kéretlen keres őoldalak tipikusan nagyságrendekkel lassabbak a népszerű internetes keres őknél, ezért a meghamisított keresési eredményekre már a hosszú másodpercekig tartó, szokatlanul lassú keresés is utalhat.

7. Hotbar.ShopperReports (böngész ő eszköztár) A böngész őbe kéretlenül beépül ő ShopperReports eszköztár a teljes, hasznosnak tűn ő Hotbar programcsomagot is feltelepíti, ami id őjárás jelent őt, asztali háttérkép letölt őt, Outlook Tools néven az Outlook levelez őkliensekbe beépül ő modult és az internetes vásárlásokat „segít ő” böngész ő oldalát, ami vásárláskor a konkurencia reklámjait jeleníti meg a weboldal mellett. A program kézi eltávolítása nehézkes, többszőr próbálja a felhasználót lebeszélteni a valós eltávolításról, és teljesen csak kémprogram-eltávolító használatával tüntethet ő el. Az eszköztár működése során megváltoztatja a böngész ő keres ő és saját honlap beállításait, böngészési beállításait, és gyűjtött adatokat jelent a böngészési és kommunikációs szokásokról.

8. többi Hotbar fert őzés (reklámprogram-család) A Hotbar reklámprogram család többi tagja is sok számítógépen megtalálható, köztük név szerint az AccuWeather id őjárás jelent ő, a WOWPapers háttérkép kezel ő, az Outlook Tools néven levelez őbe beépül ő kéretlen kiegészít ő és a Hotbar Web Tools reklámprogram, ami a böngész őben több helyen beépül, majd például a meglátogatott oldal tartalmától, vagy a keresett kifejezést ől függ ően próbál kapcsolatos reklámokat megjeleníteni.

9. C2.Lop (reklámprogram) A C2 Media érdekeltségébe tartozó Lop.com honlap az átkattintás alapon fizet ő hirdetésekre specializálódott, a cég a károkozói segítségével hirdet ői számára garantált mennyiségű látogatót szállít. A C2.Lop reklámprogram a böngész őket teljesen átalakítja, ami gyakorlatilag minden hibaüzenet, könyvjelz őt vagy keres ő oldalt ezen túl a lop.com honlapon keresztül fog csak megjeleníteni. A reklámprogramot leggyakrabban MP3 zenék vagy erotikus tartalmú videók keres őjeként tüntetik fel, és fájlcsere ő hálózatokon, a böngész ő sebezhet ősegeit kihasználó honlapokon valamint más alkalmazások, például fájlcsere ő kliensek, vagy MSN Messenger beépül ő modulok „segédprogramjaként” települ fel.

10. WhenU.Save (reklámprogram) A kémprogram folyamatosan figyeli a felhasználó böngészési szokásait, és a meglátogatott oldalak függvényében jelenít meg a tartalomhoz többé-kevésbé ill ő hirdetéseket. A reklámprogram működését a végfelhasználói szerz ődésben is felvállalja, elméletileg teljesen eltávolítható kézzel is, de ezt minden lépésben megnehezítik a fejleszt ők. Olyan apróságokra is figyeltek, hogy a program eltávolításkor fordított értelmű kérdést tesz fel és arra kérdez rá, hogy a programot szeretné-e megtartani, amikor az eltávolítók szinte mindig az alkalmazás törlésére kérnek meger ősítést. Kapcsolódó honlap: www.sunbelt.hu A Sunbelt Software-r ől A floridai székhelyű, 1994-ben alapított Sunbelt Software, a Windows-biztonság szakért ője, a kémprogram- és vírusvédelem, spamszűrés, archiválás és hálózati biztonsági megoldások területeinek vezet ő szállítója. A Yellow Cube 2000. Kft.-r ől A Yellow Cube 2000. Kft. egyéni és vállalati ügyfeleknek fejleszt és kínál biztonságtechnikai szoftvereket. A cég a piacon egyedülállóként magyar nyelvű spamszűr ő megoldást fejleszt, továbbá a Sunbelt Software és a Message Partners termékeinek kizárólagos hazai disztribútoraként spamszűr őket, antivírust, kémprogram-eltávolítót és tűzfalat kínál otthoni felhasználóknak és vállalatoknak.

