

Mire való a jelszó, mit ronthatunk el, mire figyeljünk?

Egy a jelszónk, a béke123

Sorozatunk 36. epizódja arra kívánja felhívni a figyelmet, hogy a jelszóválasztás mennyire fontos; kiderül, mikor csináljuk jól, melyek a tipikus elbaltázások, és hogyan lehet a bonyolult jelszavakat is könnyen megjegyezni. Néhány szemléletes példával azt is bemutatjuk, mi vár azokra, akik nem kezelik a kérdést súlyának megfelelően.

Tegyük fel, hogy van egy felhasználónk, valamennyire érdekli is a számítástechnika, hallott már az adathalásatról, és a vírusirtó, kémirtó, személyi tűzfal szentháromságát is szépen használja a gépén. Ez eddig nagyszerű – bár itt tartana már mindenki –, és ezzel sikeresen meg is védi a saját számítógépét. De vajon az adataiért is megtett mindent? Ez már azon is múlik, mennyire erős jelszavakat választott a különböző belépési helyein, és hogy minden helyen másikat használ-e. Van olyan hasznos biztonsági szokások, amelyek mellőzését egyetlen vírusirtó vagy tűzfal sem kompenzálhatja, ez pedig a használt jelszavak minősége, mennyisége és változtatási gyakorisága, továbbá ezek gondos és bizalmas kezelése.

Éljen és virágozzék az alapértelmezett jelszó!

A social engineering rejtelmek, módszerei naponta változnak, bővülnek új eszközökkel, illetve a kiemelt odafigyelést igénylik a begyepesedett pavlovi reflexek helyett. A legfontosabb dolgok, amiket észben kell tartani, a rendszeres jelszócsere, bizalmatlanság, a tanúsítványok kiemelt vizsgálata, csak ismert és megbízható forrásból történő szoftver telepítése, és még hosszasan lehetne sorolni. Sokféle hibát követhet el egy átlagfelhasználó; egy ilyen hiba például ha operációs rendszerében könnyen kitalálható, ergo szótárban szereplő jelszót választ. Emellett pedig sokan csak elhozzák a boltból Wi-Fi-routert, kicsomagol-



A Conficker féreg szótáralapú támadást indít a gyenge adminisztrátori jelszavak ellen. Így a fertőzés következményeinek kivédésében nagy szerep jut az erős jelszavak használatának

ják, és sem az alapértelmezett adminisztrációs jelszót (a www.routerpasswords.com oldalon bárki megkeresheti) nem változtatják meg azonnal, sem a forgalomhoz nem állítanak be titkosítást, vagy esetleg csak WEP-et. Aztán végül csodálkoznak, illetve ami talán még rosszabb, mindezt észre sem veszik. 2009 novemberében egy ausztrál fiatalember, visszaélve a jailbreakelt telefonokat használók tudatlanságával és/vagy lustaságával, az alapértelmezett SSH-jelszót felhasználva írt egy C nyelvű férget. Ez távolról belépett mások telefonjába, lezárta az SSH-portot és felmásolt néhány álmányt, többek közt lecserélte az inkriminált iPhone-ok háttérképét Rick Astley fotójára. A vírusíró, a 21 esztendő Ashley Towns csak egy jó balhénak tartotta az esetet, azonban a publikált forráskódnak köszönhetően később több kártevőváltozat is készült.

Az elnök emberei

2002. szeptember 25-én Friderikusz Sándor üzenetet kapott a mobiljára Lendvai Ildikótól, hogy őrá gondoltak az MTV elnöki székében (forrás: index.hu/belfold/lendvai0925/). „Mi a maga pályázatát támogatjuk első soron, tehát ebben az én véleményem nem változott, és ahogy látom, megegyezik a Péterével.” Az üzenet azonban kikerült a nyilvánosság elé és MP3 formátumban bejárta a netet. Friderikusz Sándor végül nem lett TV-elnök. Hogy történhetett meg mindez? Ebben az időben a Pannon GSM mindegyik postafiókjának alapértelme-

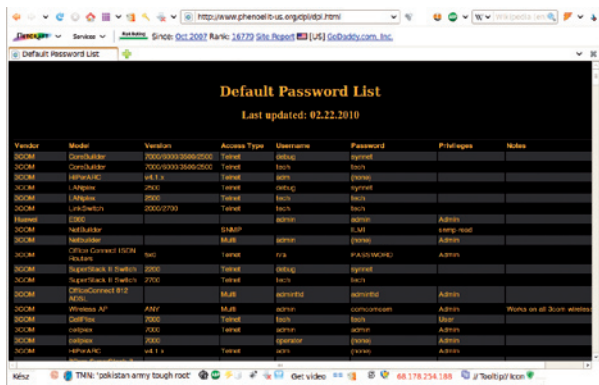
zett kódja – ha valaki nem állított be magának mást – „1111” volt. Mindenki ezt kapta automatikusan, és csak ennyit kellett beütnie az elkövetőnek is, bízva abban, hogy nem változtatták meg. A szerencse a behatoló mellett állt, a jelszó az alapértelmezett volt, így bárkinek a hangpostafiókjához hozzá tudott férni, meghallgathatta az üzeneteket.

2002. szeptember 28-án a Pannon lecserélte az összes hangpostakódot; ezzel a további hasonló eseteket kívánták megelőzni. Elvileg az ekkor hatályos büntető törvénykönyv az ilyen típusú bűncselekmények elkövetőit 5 évig terjedő szabadságvesztéssel sújthatta volna, de a történet végét, az esetleges nyomozás eredményét már nem ismerjük. Ennek ellenére konstataálhatjuk, hogy ha ismert emberek, közszereplők vagyunk, akkor különösen vonzó célpont lehetünk, és éppen ezért fokozott figyelemmel kell megelőzzük a biztonsági incidenseket. Ezt vagy saját magunknak kell megtenni, vagy megfelelő technikai segítséget kell kérni/alkalmazni hozzá.

Annak illusztrálására, hogy mennyire nem változik a világ, vagy talán a marketing legyőzi az ésszerűséget, álljon itt egy 2010. június 29-i hír. Az AT&T igyekszik felhívni az ügyfelei figyelmét, éljenek az egyedi hangpostakód lehetőségével, amelyet 4-14 jegyű számkombinációval védhetnek. Ellenkező esetben egy androidos telefonról bárkinek a hangpostafiókjá lehallgatható (forrás: hopp.pcworld.hu/7143).



Csak azok a feltört telefonok vannak ilyen veszélyben, amelyeken fut az SSH-démon. Ashley Towns nem akart kárt okozni, és a feltűnően lecserélt háttérkép is ez látszik igazolni



A Phenoelit az egyik legismertebb weboldal, ahol alapértelmezett jelszavakat találunk (www.phenoelit-us.org/dpl/dpl.html). A felhasználói listáságra jellemző, hogy ezek alkalmazása többször jár sikerrel, mint kudarccal

Steve Jobs is megvolt

Nem lehet elhanyagolni kulcsemberek, cégvezetők, és jól ismert IT-szereplők elleni próbálkozásokat sem, főleg ha sikeres a kísérlet. A „felhasználó” ahol tud, lazít, könnyít, post-ire jelszót írkal, illetve akár meg is adja azt egy idegennek a telefonban. 2009 májusában maga *Steve Jobs* Amazon áruház account-ja került horogra, pontosabban ennek kihorgászása az elkövető Orin0co szerint már az előző évben megtörtént, csak a nyilvánosságra hozatal volt a friss esemény. Emberünk időt és fáradságot nem kímélve, létrehozott egy hamis Amazon áruház weblapot belépési lehetőséggel, és várta az érkező adatokat. A sok hétköznapi felhasználó mellett azonban nagy meglepetésére egyszer csak maga Steve Jobs is figyelmetlen volt, és beszélt a csapdába: megadta a nevét, címét, bankkártyaadatait, telefonszámát, valamint az amazonos belépési nevét és jelszavát. A hiteles belépésről képernyőmentés is készült, és a támadó levelet is írt „bestseller” Jobsnak, amelyben azt is megemlítette, hogy 6-7 évre visszamenőleg elementette a korábbi vásárlásainak listáját. A levélben részletesen elmondta, hogyan

sikerült a fenti módon bejutnia és felajánlotta, hogy egyfajta váltságdíjként vegye meg tőle ezeket az adatokat, különben nyilvánosságra hozza azokat.

Game over

Az online játékosok is célpontok, sőt. Már 2008-as felmérések is megerősítették, hogy amíg egy lopott WoW- (World of Warcraft) login feketepiaci ára 10 dollár, addig egy „sima” bankkártyaadat mindössze csupán 50 centet kóstált a bűnözői körökben. A havi vírusstoplista eredményei alapján is úgy tűnik, a kártevő-terjesztők az elmúlt években a sebezhetőségek kihasználásával mind jobban ráfókuszáltak erre a területre is.

Jelszó- emlékeztető – jó és rossz ötletek

Bizonyára sokan emlékeznek még *Sarah Palin* Yahoo!-s postafiókjának feltörésére. A módszer nem feltörés, nem jelszótalálgatás volt, hanem új jelszó igénylése. A születési hely és idő megszerzése nem okozott gondot, a titkos ellenőrző kérdés pedig az volt, hol ismerkedett meg a férjével. A dolog érdekessége, hogy er-

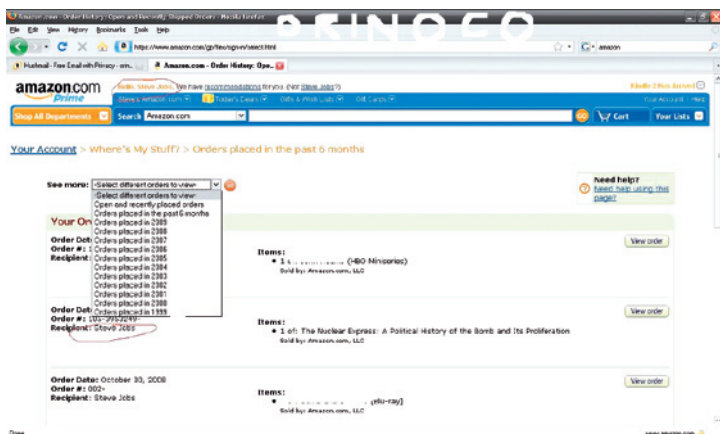
ről is beszélt már nyilvánosság előtt – és ez egy bizonyos középiskola neve volt. Innentől már meg is volt oldva a dolog.

Az ismert és kevésbé ismert embereknek komolyan el kellene gondolkodniuk, érdemes-e olyan adattal védeni bármit is, amit róluk a bulvárlapok hetente megírnak, vagy amit önként kiaplakáltak az iWiW-es, facebookos lapjukra.

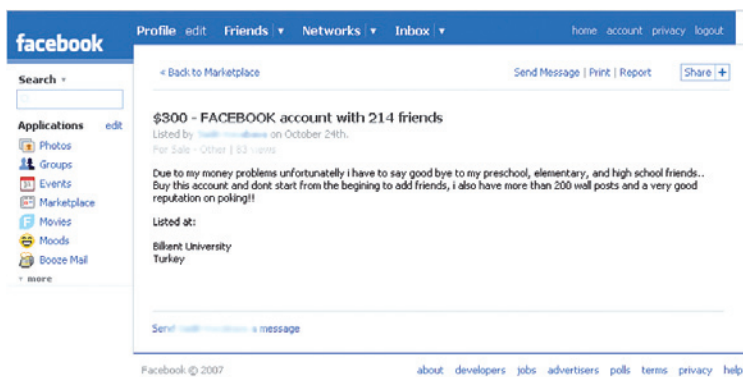
Sokszor nincs sok lehetőségünk, csak a rögzített standard jelszó-emlékeztető kérdések közül választhatunk: „your pet”, „your first teacher” stb. De ilyenkor sem kötelező ám az adott kérdésre vonatkozó választ adni! Persze sok helyen van lehetőség saját kérdést írni, ezt minden esetben érdemes is kihasználni, így jócskán csökkenthetjük a találgatásos módszer hatékonyságát. Hogy hívják a kedvenc tanárod? „Csütörtök_139” – hangzik a válasz, és ez egy jó válasz. Melyik kórházban születtél? „Lekváros palacsinta fahéjjal”. Dolgozzon csak meg a feltörő, ha akar valamit, ne mi nyújtsuk a tálcán a fejünket.

Egykulcsos jelszó

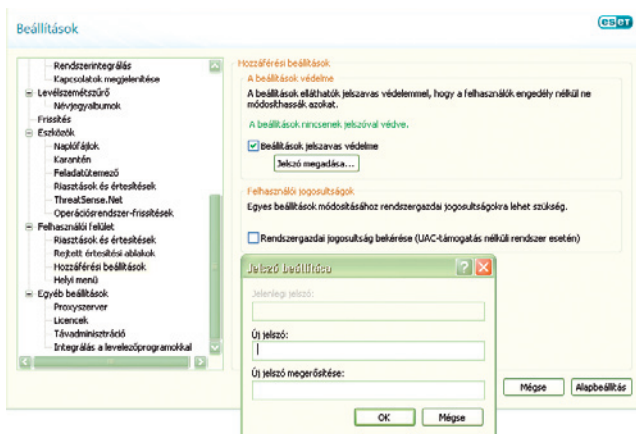
A mindenütt azonos jelszó használata is komoly veszélyt jelent, bár megjegyezni bizo-



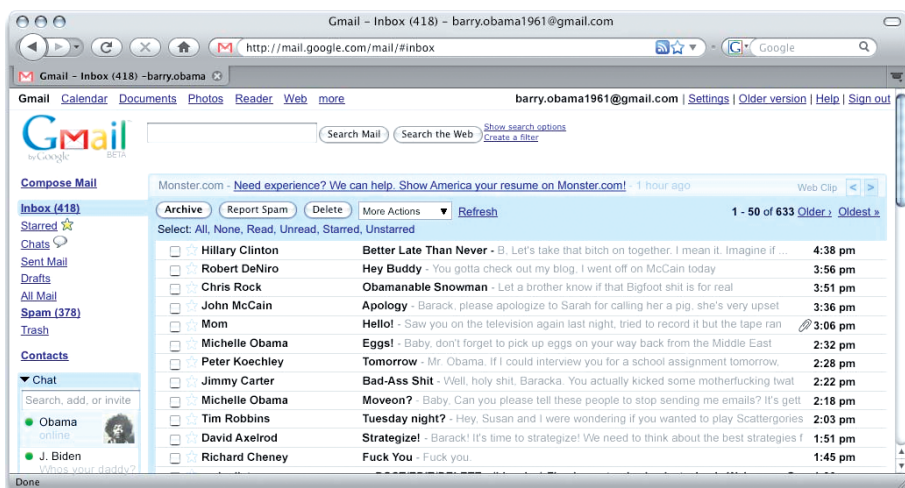
Egy jó példa arra, mihez kezdhetnek például egy ellopott belépéssel. Itt a támadó váltságdíját kért Steve Jobstól



Bár ez itt most csak egy ártalmatlan adásvétel, a bűnözői csoportok nagy tételben adják el a különböző ellopott banki, online játékhöz való és egyéb accountokat



Érdemes a jól konfigurált vírusvédelmi programunk beállításait is jelszóval védeni az illetéktelen módosítások ellen



Ez itt csak egy photoshoppolt vicces kép, de azért el lehet képzelni, milyen kalamajka származhat abból, ha illetéktelenek férnek hozzá egy befolyásos személy levelezéséhez

nyosan könnyű. Ha azonban ezek közül csak egyetlen helyszínen is kompromittálódik a belépési adatunk, gyakori forgatókönyv, hogy egy jelszó megszerzésekor végigpróbálgatják az illető minden egyéb publikus levelező, csevegő, közösségi, webes, FTP-eléréseit – és gyakran nem eredmény nélkül. Ezzel fokozhatják a veszteségeinket, dőlnek a további dominók. Ilyen baleset érte a propeller.hu-t is 2010 márciusában, amelynél egyszer csak azt vetették észre, hogy az oldal kikerült a Google-ből (forrás: hopp.pcworld.hu/7142). Mint később kiderült, a támadók úgy módosították a robots.txt fájlokat, hogy emiatt az kitiltotta a keresőrobotokat a weboldáról. Emellett a Propeller nevében beadtak egy törlési kérelmet is a Google-hoz. Az illetéktelen behatolók úgy jutottak be az oldalra, hogy az üzemeltető gmail-es fiókját törtek fel egy másik helyszínen meg-

szerzett jelszót kipróbálva. Ennek segítségével jutottak el a propelleres jelszavakhoz, és sajnálatos módon a fiókban benne volt két év levelezése, üzleti titkok, jelszavak, amelyeket a támadók elolvashattak, lemásolhattak.

Vajon mennyire működik a fantáziánk?

Negatív eredményt mutat a Bitkom németországi, 2010. júniusi vizsgálata, amelyből az derül ki, hogy a németek 41%-a sosem cserél kódot a banki, aukciós árverési helyszínein, sem a számítógépén, sem a mobiltelefonján. Kizárólag akkor változtatnak, amikor erre felszólítást kapnak, vagy ha technikailag elkerülhetetlen. A mind a magánszemélyeket, mint a vállalatokat érintő felmérés másik érdekessége, hogy a felhasználók 37 százaléka adja át a számítógépét vagy a belépési adatát valaki másnak is (forrás: hopp.pcworld.hu/7144).

A Webroot egy korábbi átfogó, mintegy ezer-ezres Facebook-, MySpace-, Twitter-, LinkedIn-oldal felhasználóját kérdezte ki egy felmérés keretében 2009 júniusában. Ebből többek között az derült ki, hogy egyharmaduk (36%) ugyanazt a közösségi portálon használt jelszavát máshol is alkalmazza. Ugyancsak 2009 februárjában az Errata Security is vizsgálta a jelszavak minőségét egy több ezer, PhpBB felhasználói csoport alapján, a végeredmény itt is siralmas és lesújtó volt. A két leggyakoribb választott jelszó az „123456” és a „password” volt. Íme a Top10-es lista további helyezettjei, a leggyakoribb találatokkal: „phpbb”, „qwerty”, „12345”, „12345678”, „letmein”, „1234”, „test”, „123”. A jelszóválasztási fantáziatlanság szembetűnő. Nyilván nem lehet figyelmen kívül hagyni ilyenkor azt sem, hogy az ESET Magyarországon terjedő számítógépes vírusok toplistájában első helyét 2009 októberé óta az a Conficker féreg tartja, amely az operációs rendszer frissítéseinek hiánya és

