MI KÖZE A BIZTONSÁGNAK A BIZTONSÁGI RÉSHEZ?

# E, mint Exploit

Sorozatunk tizennyolcadik epizódjában megpróbáljuk összefoglalni, hogyan lesz a sebezhetőségből kártevő. Az alaptétel az, hogy nem elég csupán a vírusirtót frissíteni, a szoftverkörnyezetünket is állandóan naprakészen kell tartani ahhoz, hogy elkerüljük a fertőzéseket. Bizonyított az összefüggés, ugyanis a biztonsági incidensek java része elavult, nem frissített környezetben történik.

Sokszor és sokat hallottunk sérülékenységekről, sebezhetőségekről az utóbbi években. Ha csak a Microsoft operációs rendszerét és fő alkalmazásait nézzük, láthatjuk, rákényszerültek a rendszeresen kibocsátott hibajavításokra. Minden hónap második keddje – népszerű nevén Patch Thuesday, azaz „Foltozó Kedd" – hivatott arra, hogy a Microsoft kijavítsa a rendszeresen összegyűlő és támadásokhoz kihasználható hibákat. Az, hogy a hiba észlelésétől kezdve menynyi idő telik el a „javítófolt" megjelenéséig, igen változó lehet.

## Exploit, ami nem egy hangszer, amit három darabból raknak össze

Ha arra gondolunk, a „gyerekszájnál" mi a szél meghatározása: „Olyan levegő, amelyiknek sürgős dolga van...", akkor az exploitnál is lehet hasonlót alkotni. Ez körülbelül úgy hangzana: „az exploit olyan sebezhetőség, amit egy, külön erre a célra szánt támadókóddal ki is használnak". Aztán itt már kissé ködbe veszhet a tapasztalat, mert ugyebár ki tudhatja, mit, hol és menynyien használnak ki aztán tényleg a gyakorlatban. Mindenesetre ha már komolyabb portálokon osztják meg az ilyen kódot – ilyen például a Milw0rm –, akkor az internet természetéből adódóan ezt többé nem lehet titokban tartani, és a sebezhetőségről szóló információ könnyedén eljut azokhoz is, akik ezt szándékos támadásra kívánják felhasználni. Ezen tevékenységet persze nem okvetlenül úgy kell elképzelni, hogy külön erre a hibára írnak mindig egy külön kártevőt – bár ez is gyakran előfordul –, hanem úgy, hogy az adott kihasználható sebezhetőség bekerül a többi használt támadási módszer közé, és egy lesz a lehetséges, detektálásra érdemesek között. Ilyesmiket láthatunk, ha a Metasploit Framework (**www.metasploit.com/framework/**) weboldalát meglátogatjuk. Ezeket a weboldal készítői persze csak és kizárólag „tesztelési" célból teszik fel, amire külön figyelmeztetési szöveg is megjelenik: „The tools and information on this site are provided for legal security research and testing purposes only." Abban azért százszázalékosan biztosak lehetünk, hogy a honlapot nem csak a Grál-lovagok fogják használni.

## Amikor nem adnak ki (idejében) frissítést

2006 májusában olvashattunk egy Safari böngésző hibáról, amit bár a felfedezője kritikusnak tartott, az Apple nem értett ezzel egyet és nem tartotta sürgősnek javítófolt kiadását. A hiba szerintük nem volt jelentős, és éppen csak azt nem mondták, hogy addig is böngésszünk kizárólag megbízható forrásból származó weblapokat. A sebezhetőség azonban később úgy tűnt, mégis komolyabb a vártnál.

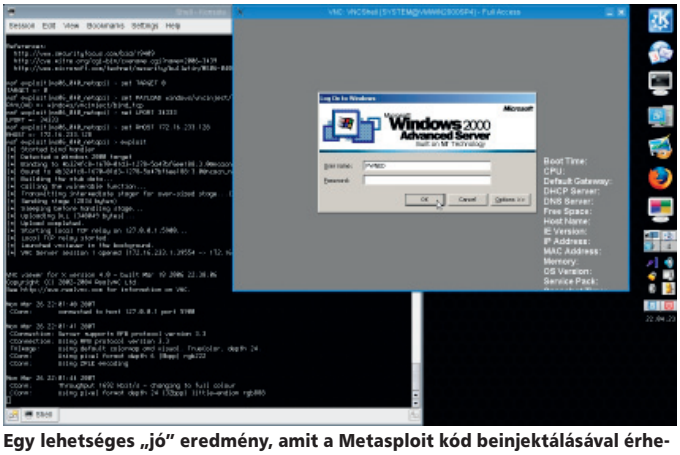
Érdekes módon most a korábban hasonló (el nem ismerő és halogató) taktikát folytató Microsoft állt a sarkára és igyekezett a hibára jobban felhívni a figyelmet, nem véletlenül. Ugyanis a Safariban a *Nitesh Dhanjani* biztonsági kutató által május 15-én talált hiba és egy, az Internet Explorerben lévő másik sebezhetőség együttes hatásaként tetszőleges program vált futtathatóvá.


**Ha már itt is feltűnik egy exploit forráskódja, felgyorsulnak az események**


**Nem véletlenül népszerű a moduláris Metasploit eszközkészlet, a program segítségével Windows és Linux alól is „tesztelhetünk"**

Az IDG News Service munkatársai ezt demonstrálva képesek voltak az áldozat számítógépén futtatni a Windows Calculator programot. A végrehajtáshoz egy rosszindulatú kódot tartalma-


**A Microsoft Biztonsági Értesítőkből sok hasznos információ szerezhető, olvasása egyes esetekben szinte nélkülözhetetlen**




**Egy lehetséges „jó" eredmény, amit a Metasploit kód beinjektálásával érhetünk el: belépési ablakot kapunk egy Windows 2000 szerverre, aminek az igazi admin valószínűleg nem igazán örülne.**

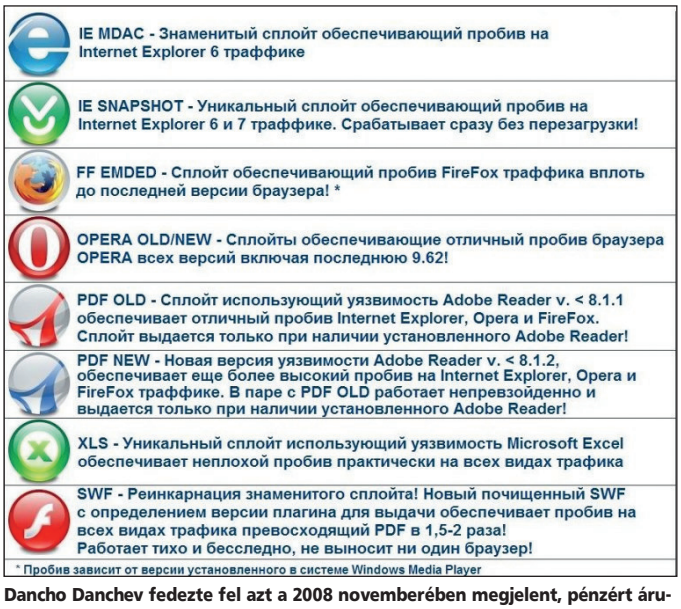

**Izgalmas olvasmány Dancho Danchev független biztonsági szakértő blogja (ddanchev.blogspot.com)**

zó weboldalt kellett előtte a windowsos Safari böngészővel felkeresni a bemutató kedvéért.

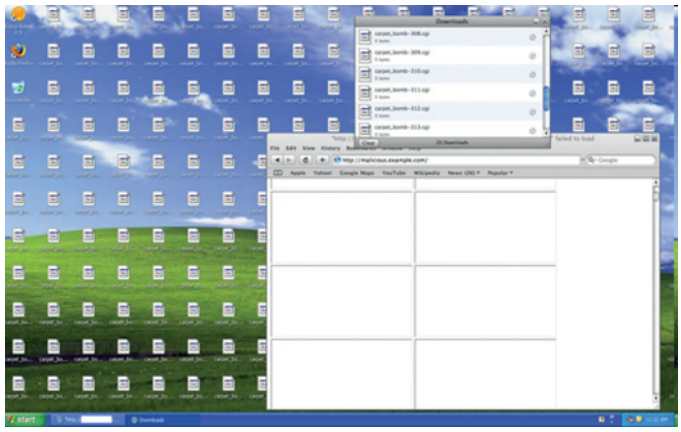
A Microsoft ezúttal komolyan vette az esetet, hiszen az XP és Vista alatt is jelentkezett, és a cég rövidesen kibocsátott egy biztonsági értesítőt. Ellenben az Apple júniusban még mindig félvállról kezelte az automatikus fájlletöltési esetet – némiképp csalódást okozva saját felhasználóinak is -, pedig még a **StopBadware.org** is felszólította, hogy vegye komolyan a „szőnyegbombázás" nevű sérülékenységet és adja közre mielőbb a biztonsági hiba javítását. Érdekes momentum, hogy a korábbi böngészőbiztonsági összehasonlításokon a Safari mindig büszkén hozakodott elő azzal, hogy extra rövid idő alatt befoltozza a versenytársaihoz képest sokkal kevesebb biztonsági hibát, és ezzel igyekezett nimbuszát megóvni. Emiatt aztán végképp érthetetlen volt részükről ez a hozzáállás.

## Mikortól kereshetjük?

Ha már egy kihasználható hibára épülő kísérleti támadás forráskódja nyilvánosan is megjelent vagy már észleltek ilyen kártevőt valós környezetben (In The Wild, ITW), akkor a konkrét kártevőminta birtokában kezdenek el ténykedni a víruslaboratóriumok is. A víruskereső nem sebezhetőségkereső (fuzzer), ezért vagy a begyűjtött kártevő kódja alapján készített szignatúrával, vagy a heurisztikus keresés segítségével a gyanús viselkedése alapján ismerheti fel ezeket. Magyarul, pusztán a sebezhetőség kihasználása nem okoz riasztást, hanem csak ha már létezik erre épülő támadó kód, amely meg is próbál végrehajtani nem kívánt lépéseket (jelszólopás, fertőzés, állományok törlése, cseréje, nem kívánt új állományok létrehozása, további kártevő komponensek letöltése, stb.). Vagyis kevés kivételtől eltekintve a kártevőnek büntető rutinnal (payload) kell rendelkeznie, hogy bekerülhessen a felismertek közé.




**Dancho Danchev fedezte fel azt a 2008 novemberében megjelent, pénzért árusított exploitkészletet, amellyel már az ünnepi szezonra készültek a bűnözők**



**A nevezetes szőnyegbombázási hiba, amit Nitesh Dhanjani fedezett fel. Nem igazán érthető, miért húzódott el a javítás végül olyan hosszú ideig**

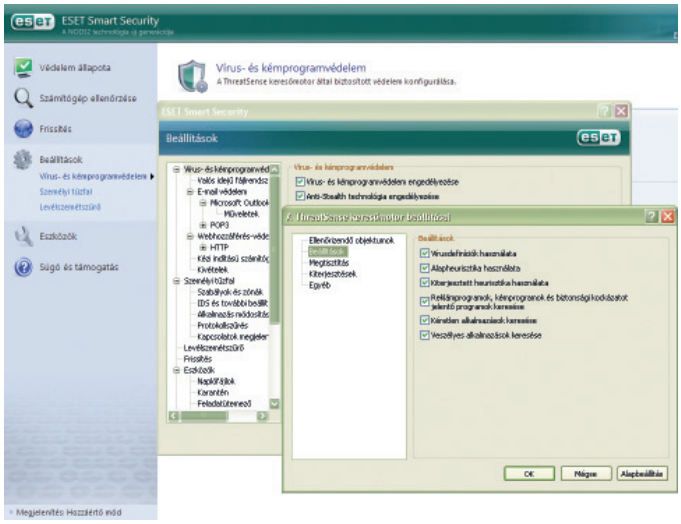

**A GNUCITIZEN (www.gnucitizen.org) egy nagyon hasznos weboldal biztonsági szakembereknek. Petko Petkov nagyon sok érdekes felfedezést tett már, és a Microsoft külön köszönetnyilvánításban is elismeri a szakember segítőkészségét**

## Zorro day

Ebből nagyjából már azt is látni lehet, hogy ez az időbeli eltérés mindig egy kicsit a támadóknak kedvez, és lépéskényszert okoz a védelmi programok fejlesztőinél. Ezért is veszélyesek egyébként az úgynevezett nulladik napi – más néven zero day – exploitok, hiszen a kihasználásra relatíve igen sok ideje marad a támadóknak. Sokszor fordult elő például az az eset, hogy a Foltozó Keddet követő szerdán ismertek fel egy új sérülékenységet, amelylyel jó esetben egy teljes hónapig lehetett visszaélni, mire a következő rendszeres havi biztonsági javítás megjelent. Rossz esetben akár több havi csúszás is elképzelhető. Néhány kivételes esetben rendkívüli azonnali javítás is megjelenhet, legutóbb ilyen volt például az Internet Explorer hibája. Mint emlékezetes, állítólag véletlenül hozták nyilvánosságra a sebezhetőséget konkrétan kihasználó kódot kínai biztonsági kutatók, akik azt hitték, hogy a kód egy már javított hibát aknázott ki. A Microsoft patch ez esetben példás sebességgel, napok alatt elkészült és letölthető lett. Az már persze egy másik kérdés, hány számítógépen fogják ezt majd valóban telepíteni.

## Éljen a nyilvánosság!

A fenti példából már világosan kiderült, hogy a sebezhetőségi harc résztvevőinél konrad lorenzi megfigyeléseket tehetünk: többé-kevésbé szabályszerűen, kiszámíthatóan ténykednek. Kitudódik egy hiba, és figyelmeztetik a céget, a fejlesztőket. Ott először vagy elzárkóznak, vagy azt nyilatkozzák, még vizsgálják a bejelentést – ezt néha észvesztően sokáig is képesek elhúzni. Ha időközben egy vagy több szakértő is megerősíti, hogy valóban létező és igencsak súlyos hibáról van szó, akkor először az a kijelentés következik, hogy megvizsgálták az esetet, de az korántsem olyan súlyos, mint azt a cikkekben írják. Meg lehet még ezt toldani azzal, hogy „nincs tudomásunk olyan konkrét esetről, amelynél éppen ezt a hibát használták volna ki", illetve „a hiba valóban kihasználható, azonban annyira ritka és extrém körülmények között, hogy ez semmilyen veszélyt nem jelent az átlagfelhasználókra nézve". Pluszban esetleg hozzátesszik, hogy a következő ötéves tervben vagy „május és november között az esti órákban" majd valóban megjelenik egyszer egy esetleges javítás, valamint kérik, hogy „a javítás megjelenéséig kizárólag biztonságos forrásból származó állományokat nyissanak meg, illetve csak biztonságos weblapokat látogassanak". Ekkor előfordulhat, hogy az elégedetlen és türelmetlen hibafelfedező – ha teljesen bizonyos a dolgában – kiteszi a blogjába az exploit mintakódot, hogy jó, hát ha harc, legyen harc, nézzük meg, valóban olyan ritka/ártalmatlan/extrém-e ez a bizonyos hiba. Ekkor




**Ha már valami vírusszerű viselkedést produkál, hiába nincs benne a felismerés a vírusismereti adatbázisban, a heurisztika jó eséllyel képes detektálni az új támadásokat is, amennyiben ehhez megfelelően választottuk ki a beállításokat**

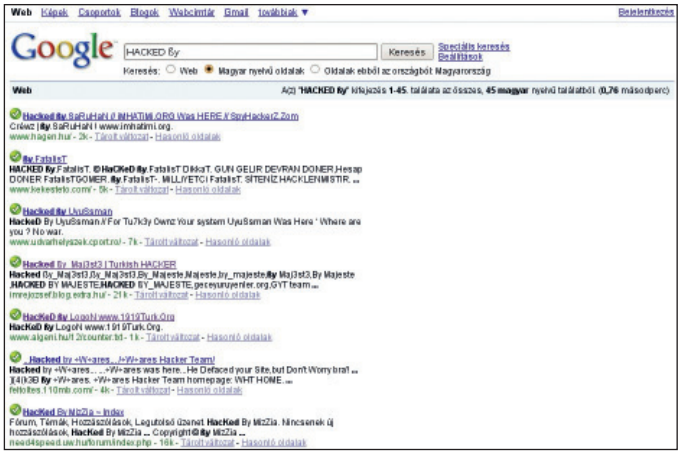
aztán általában hihetetlenül felgyorsulnak az események. Az eddig vitatkozó, lomha léptű fejlesztőcégek akár órák alatt is képes elkészíteni és nyilvánosságra hozni a javítást, hiszen itt már renoméjuk a tét – nem merik megkockáztatni azt, hogy vásárlóik elpártoljanak tőlük, vagy esetleg elcsábítsa őket a konkurencia.

## Etikus hackerek, sebezhetőségi információs oldalak

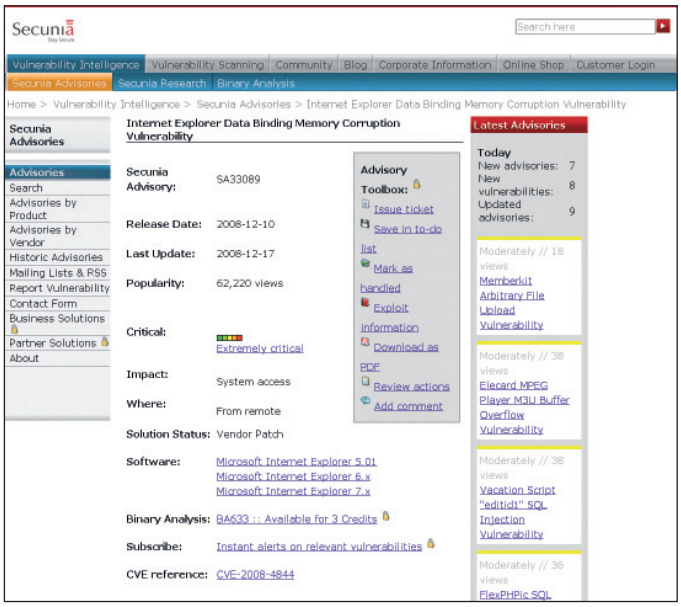
Az olyan neves cég, mint például a dán Secunia portál (**www.secunia.com**), minden esetben először a gyártókat figyelmezteti, és csak és kizárólag ezután hoz nyilvánosságra technikai részleteket, ha már azok kibocsátották a sebezhetőséget javító foltot. Láthattuk persze ennek a hozzáállásnak az ellenkezőjét is, elég csak a WabiSabiLabi oldalra gondolni (**www.wslabi.com**), ahol árverési portált szerveztek a felderített sebezhetőségekhez. Álnaivan és álságosan a kutatók megsegítése volt a hangoztatott cél, de azt azért mindenki sejtheti, kiknek éri meg igazán az ilyeneket megvásárolni. A hamis antivírus programok fejlesztőinek például biztosan, és még csak nem is kellett nagyon mélyen a zsebükbe nyúlniuk ehhez. Emlékezetes, hogy egy orosz botnetes támadásokban résztvevő bűnöző a Bakasoftware nevű cégnél kishalként is heti 158 ezer dollárt keresett (mintegy 32 millió forintot). Fogalmazzuk diplomatikusan úgy, hogy a furcsa árverési oldal működése erőteljesen megosztotta a szakmát.

## Hol bukkannak fel a művek?

Sajnos minden olyan esetben, ahol hiányzik a megfelelő szakértelem, beleütközhetünk károkba. Ha újonnan vettünk egy routert, és nem változtatjuk meg az alapértelmezett jelszót, nem védjük megfelelő titkosítással a Wi-Fi internetkapcsolatunkat, kéretlen levelek mellékleteire kattintunk, nem frissítjük rendszeresen




**Egy december 26-i weblapokat módosító támadássorozat saját webes szövegeiben szerepelt a „HACKED ßy" karakterfüzér. A Google-be beütve meglepően sok magyar találatot is kapunk, és az érintett oldalak tulajdonosai sokszor nem is veszik észre a velük történt malőrt**




**A Secunia oldala (www.secunia.com) nemcsak a Personal Security Inspectorral igyekszik segíteni programjaink naprakészen tartását, de kiterjedt adatbázist is vezet a sebezhetőségekről, azok veszélyességéről és az adott javítófolt megjelenéséről**

a használt operációs rendszert és alkalmazásainkat, nincs naprakész biztonsági csomagunk, vagy fertőzött weboldalra, esetleg fertőzött bannerhirdetésre kattintunk. Ha weboldalt vagy fórumszoftvert üzemeltetünk, ott is fontos a megfelelő hozzáértés és a megjelenő biztonsági frissítések mielőbbi futtatása. Ellenkező esetben a botok automatikusan felderítik az ilyen oldalakat, és a támadók végigdúlják ezeket.

Sok fórumszoftver és még több weboldal esik áldozatul az ilyen jellegű támadásoknak, és a legrosszabb, amit ilyenkor tehetünk, ha csak bambán visszamásoljuk az oldalt mentésből – már akinek van ilyenje. A támadásról alaposan tájékozódni kell a keletkezett logokból, az okot kell megszüntetni, és a hiányosságokat pótolni, a közben keletkezett biztonsági javításokat, frissítéseket pedig haladéktalanul telepíteni.

## Érdek a világ ura

Nem kell különösebb jóstehetség vagy üveggömb hozzá, hogy elképzeljük, a szürke hétköznapok mellett minden különleges alkalom, ünnep kihasználható eseményt jelent, lehetőséget a kártevőterjesztőknek, hogy különféle módszerekkel célba juttassák a kódjaikat. A repertoár széles: fertőzött weblapok, manipulált webáruházak, ünnepi üdvözlőlapok stb. *Dancho Danchev* (**ddanchev.blogspot.com**) 2008 novemberében például egy olyan hirdetést fedezett fel, ahol a rosszfiúk komplett, azonnal használatba vehető kártevőterjesztő készleteket kínálnak, amelyek segítségével „biztosan meg lehet keresni a karácsonyi ajándékra valót". Az interneten orosz weboldalakon hirdetett eszköz Basic, Standard és Professional változatban kapható, és természetesen a legdrágább, profi verzió képes kihasználni a legtöbb sebezhetőséget. A szoftver leírásában IE6, Opera, Firefox, PDF, XLS és SWF állományok elleni támadások szerepelnek, és a készítő a weboldalán még azzal is dicsekedett, hogy 37 antivírus programból mindössze 6 látta a kártevőt, amely TDSSserv.sys néven egy rootkit komponenst is megkísérel a rendszerbe juttatni. Ha igaz is volt az akkori említett felismerési arány, ez mostanra biztosan megváltozott.

Mindenesetre minden számítógép-felhasználónak fel kell kötnie a felkötendőt, hiszen a biztonsági cégek 2009-es jóslatait olvasva olybá tűnik, a sakkozás, focizás és tévénézés mellett sajnos az exploitkészítés és -terjesztés is össznépi elfoglaltsággá válik; mindent támadnak, ami szembejön. A frissítés és a szoftverek naprakészen tartása nem úri passzió, nemcsak a vállalati környezet követelménye, hanem minden magánfelhasználó számára is olyan lehetőség, amivel minimalizálhatja a számítógépe ellen irányuló sikeres támadásokat.

***

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**

### KAPCSOLÓDÓ WEBOLDALAK

Az ESET magyar nyelvű víruslexikona:
**www.eset.hu/virus**
Isodor Biztonsági Központ:
**www.isbk.hu**