

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 Tuesday, azaz „Foltozó Kedd” – hivatott arra, hogy a Microsoft kijavítsa a rendszeresen összegyűlt és támadásokhoz kihasználható hibákat. Az, hogy a hiba észlelésétől kezdve mennyi idő telik el a „javított” megjelenéséig, igen változó lehet.

Ha arra gondolunk, a „gyerekszájál” 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 kisé ködbe veszhet a tapasztalat, mert ugyebár ki tudja, mit, hol és mennyien 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 per-

szé 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 érdemesebbek között. Ilyesmiket láthatunk, ha a Metasploit Framework (www.metasploit.com/framework/) weboldalát meglátogatjuk. Ezeket a weboldal készítői persze csak és kizárólag „tesztelési” célból tesztik 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 szászszázelekosan biztosak lehetünk, hogy a honlapot nem csak a Grál-lovagok fogják használni.

2006 májusában olvashattunk egy Safari böngésző hibáról, amit bár a felfedezője kritikusnak tartott, az Apple nem értett ezzel egyet és nem tartotta sürgősnek javított kiadást. 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 hasonlító (el nem ismerő és halogató) taktikát folytató Microsoft állt a sarkára és igyekezett a hibára jobban felhívni a figyelmet, nem véletlenül. Ugyanis a Sa-

[\[home \]](#)
[\[contents \]](#)
[\[platforms \]](#)
[\[shellcode \]](#)
[\[search \]](#)
[\[cracker \]](#)
[\[links \]](#)
[\[rss \]](#)
[\[archive \]](#)

MILWORM

[remote]

DATE	DESCRIPTION	HITS	AUTHOR
2009-01-01	Megacube 5.0.7 (mega-//) Remote File Download and Execute Exploit	1594	R D X Junior
2008-12-30	Megacube 5.0.7 (mega-//) Remote eval() Injection Exploit	2141	R D X Nine/Situations Group
2008-12-29	SaxCam WebCam Server 2.6.5 ActiveX Remote BOF Exploit	1487	R D X callAX
2008-12-28	Chilkat FTP ActiveX (SaveLastErr) Insecure Method Exploit	1208	R D X callAX
2008-12-28	Amaya Web Browser <= 11.0.1 Remote Buffer Overflow Exploit (wida)	1136	R D SKD
2008-12-26	MS Internet Explorer XML Parsing Buffer Overflow Exploit	3542	R D Jeremy Brown

[local]

DATE	DESCRIPTION	HITS	AUTHOR
2008-12-29	Linux Kernel <= 2.6.26.4 SCTP Kernel Memory Disclosure Exploit	2923	R D Jan Oberheide
2008-12-29	IntelliTampor 2.07/2.08 (ProxyLogin) Local Stack Overflow Exploit	836	R D Hisoka
2008-12-28	IntelliTampor 2.07/2.08 (MAP File) Local SEH Overflow Exploit	930	R D Co@phus

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

metasploit

ALWAYS NOT EXPLOITS. ALWAYS.

[HOME](#) [FRAMEWORK](#) [SHELLCODE](#) [OSPOC/OSB](#) [RESEARCH](#) [BLOG](#)



The Metasploit Project

Metasploit provides useful information to people who perform penetration testing, IDS signature development, and exploit research. This project was created to provide information on exploit techniques and to create a useful resource for exploit developers and security professionals. The tools and information on this site are provided for legal security research and testing purposes only. Metasploit is a community project managed by Metasploit LLC.

**Jan-01-2009: Happy New Year!**

The Metasploit Project is celebrating the new year with a series of updates to the metasploit.com web site and services. Stay tuned as updates are rolled out.

**Oct-10-2008: Metasploit 3.2 Released**

Quick Links

-  [Metasploit 3.2 \(LUMX\)](#)
-  [Metasploit 3.2 \(WIN32\)](#)
-  [Conference Materials](#)
-  [Shellcode Generator](#)

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

fariban 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.

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

Click here to Install Silverlight | United States Change | All Microsoft Sites



[TechNet Home](#) | [Downloads](#) | [TechNet Program](#) | [Subscriptions](#) | [Security Bulletins](#) | [Archive](#)

[TechNet Home](#) > [TechNet Security](#) > [Security Advisories](#)

Microsoft Security Advisory (961509)

Research proves feasibility of collision attacks against MD5

Published: December 30, 2008

Microsoft is aware that research was published at a security conference proving a successful attack against X.509 digital certificates signed using the MD5 hashing algorithm. This attack method could allow an attacker to generate additional digital certificates with different content that have the same digital signature as an original certificate. The MD5 algorithm had previously shown a vulnerability, but a practical attack had not yet been demonstrated.

This new disclosure does not increase risk to customers significantly, as the researchers have not published the cryptographic background to the attack, and the attack is not repeatable without this information. Microsoft is not aware of any active attacks using this issue and is actively working with certificate authorities to ensure they are aware of this new research and is encouraging them to migrate to the newer SHA-1 signing algorithm.

While this issue is not a vulnerability in a Microsoft product, Microsoft is actively monitoring the situation and has worked with affected Certificate Authorities to keep customers informed and to provide customer guidance as necessary.

Mitigating Factors:

- Microsoft is not aware of specific attacks against MD5, so previously issued certificates that were signed using MD5 are not affected and do not need to be revoked. This issue only affects certificates being signed using MD5 after the publication of the attack method.

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

The screenshot shows a Windows XP desktop environment. On the left, a terminal window displays the output of a netstat -an command, showing active connections to various IP addresses on ports 80 and 8080. On the right, a Windows 2000 Advanced Server installation window is open, showing the 'Use the Windows' screen with a progress bar and a 'Next' button. The desktop background is a blue and white abstract pattern, and several icons are visible on the right side, including 'My Computer', 'Recycle Bin', and various application shortcuts.

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.



Dancho Danchev's Blog - Mind Streams of Information Security Knowledge

In the overwhelming sea of information, access to timely, insightful and independent open-source intelligence (OSINT) enables it crucial for maintaining the necessary situational awareness to stay on top of emerging security threats. This blog covers trends and facts, tactics and strategies, interacting with third-party research, speculation and relative CYBERINT assessments, all packed with satirical attitude.

WEDNESDAY, DECEMBER 17, 2008

Cyber Jihadists part of the GDMF Bust?

In one of those "better late than never" type of situations, last month members of the Global Islamic Media Front were busted in Germany. The group is largely known due to their releases and propaganda of the *Technical Mujahideen* (GDMF) and the *Muslimah Security Association* (GDMF). GDMF was distributing its materials through popular Web 2.0 sites sharing sites, perfectly fitting into the profile of the majority of cyber jihadist groups.

GDMF used to be one of my favorite sources of raw OSINT regarding various cyber jihadist activities due to its centralized nature and lack of any operational security in place, in particular the way it was unknowingly exposing their social networks online.

About Me

Dancho Danchev

Independent Security Consultancy, Threat Intel Analysis and Competitive Intelligence research on Demand. Insightful, unbiased, and client-tailored assessments, neatly communicated in the form of interactive reports - because anticipating the emerging threat is what shapes the big picture at the end of the day. Approach me at dancho.danchev@gmail.com

[View my complete profile](#)

Add Feed to RSS Reader

RSS Feed

Feeds from FeedBurner

3,200 subscribers

Related posts:

- GDMF Switching Blogs
- GDMF Now Permanently Shut Down
- GDMF - "We Will Remain"
- Islamic Jihadist - Come Out, Come Out Wherever You Are
- A List of Terrorist Blogs
- Cyber Jihadist Blog Switching Locations Again
- Windows of the Anti Cyber Jihadist Crowd
- Analysis of Cyber Jihadist Forums and Blogs
- Terror on the Internet - Conflict of Interest

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

zó weboldalt kellett előtte a windows Safari böngészővel felkeresni a bemutatkozó 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 fájletöltési 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 befolytassa a versenytársaihoz képest sokkal kevesebb biztonsági hibát, és ezzel igyekezett nimbuszát megőrizni. Emiatt aztán végképp érthetetlen volt részükről ez a hozzáállás.

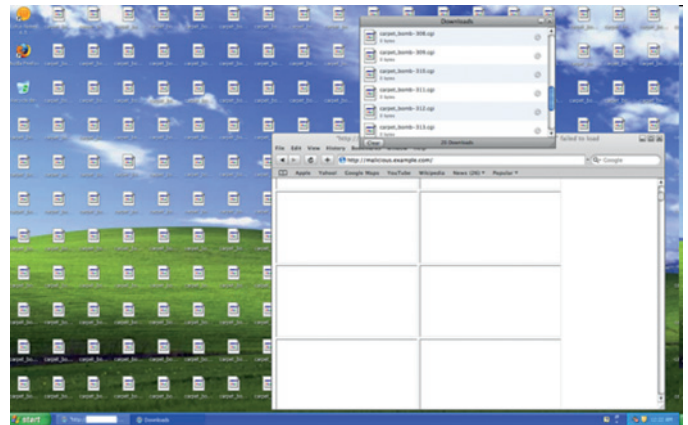
Mikortól kereshetjük?

Ha már egy kihasználható hibára épülő kísérleti támadás forráskódja nyilvánosan is megjelent vagy már észlelték ilyen kártevőt valós környezetben (In The Wild, ITW), akkor a konkrét kártevőminta birtokában kezdenek el ténykedni a víruslaboratóriumok is. A víruskereső nem sebezhetőséges (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,

	IE MDAC - Знаменитый спloit обеспечивающий пробив на Internet Explorer 6 траффике
	IE SNAPSHOT - Уникальный спloit обеспечивающий пробив на Internet Explorer 6 и 7 траффике. Срабатывает сразу без перезагрузки!
	FF EMDDE - Спloit обеспечивающий пробив Firefox траффика вплоть до последней версии браузера! *
	OPERA OLD/NEW - Сплойты обеспечивающие отличный пробив браузера OPERA всех версий включая последнюю 9.62!
	PDF OLD - Спloit использующий уязвимость Adobe Reader v. < 8.1.1 обеспечивает отличный пробив Internet Explorer, Opera и Firefox. Спloit выдается только при наличии установленного Adobe Reader!
	PDF NEW - Новая версия уязвимости Adobe Reader v. < 8.1.2, обеспечивает еще более высокий пробив на Internet Explorer, Opera и Firefox траффике. В паре с PDF OLD работает непревзойденно и выдается только при наличии установленного Adobe Reader!
	XLS - Уникальный спloit использующий уязвимость Microsoft Excel обеспечивает неплохой пробив практически на всех видах трафика
	SWF - Реинкарнация знаменитого сплота! Новый почищенный SWF с определением версии плагина для выдачи обеспечивает пробив на всех видах трафика превосходящий PDF в 1,5-2 раза! Работает тихо и бесшумно, не выносит ни один браузер!

* Пробив зависит от версии установленного в системе Windows Media Player

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

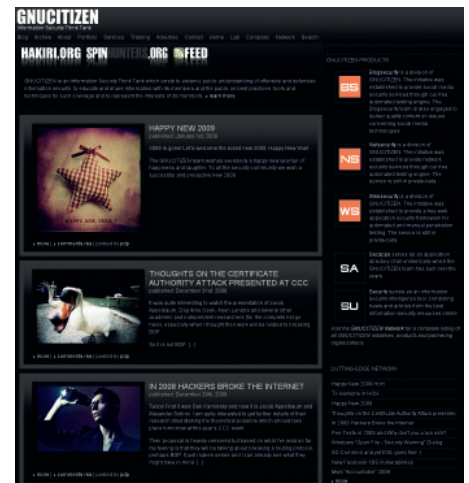
hogy bekerülhessen a felismertek közé.

Zorro day

Ebből nagyjából már azt is látni lehet, hogy ez az időbeli eltérés mindig egy kicsit a támadóknak kedvez, és lépéskényszer 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 Foltzó Kedvet 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 emlékeztet, 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.

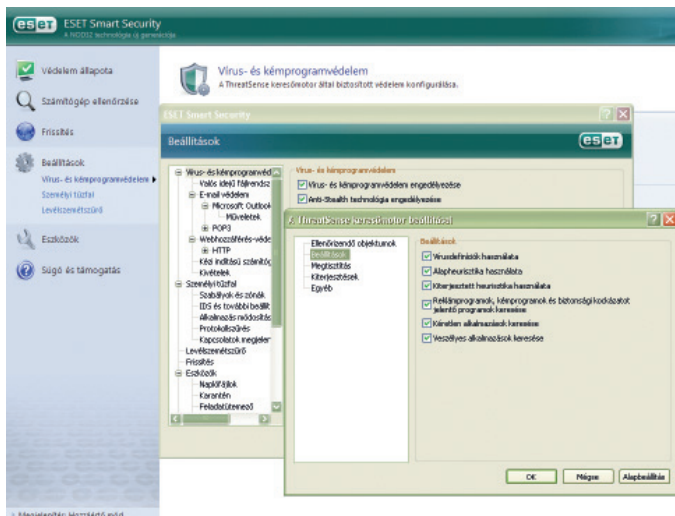
Éljen a nyilvánosság!

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 elzárkoznak, vagy azt nyilatkozzák, még vizsgálják a bejelentést – ezt néha észvesztően sokáig is képesek elhú-



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 segítőkézségét

ni. 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 cikkekkben írják. Meg lehet még ezt tolni 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 hozzáteszik, hogy a következő öt éves tervben vagy „május és november között az esti órákban” majd valóban megjelenik egyszer egy esetleges javítás, valamint kéri, 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 vírusserű 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 képesek elkészíteni és nyilvánosságra hozni a javítást, hiszen itt már re-noméjuk a tét – nem merik megkockáztatni azt, hogy vásárlóik elpártoljanak tőlük, vagy esetleg elcsábítsa őket a konkurencia.

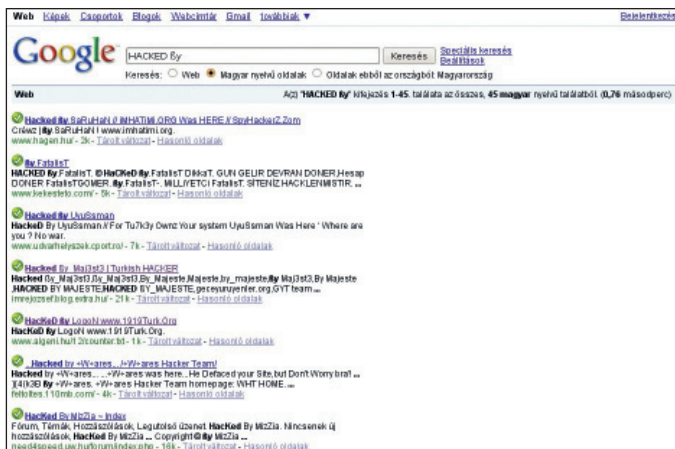
Etikus hackerek, sebezhetőségi információs oldalak

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. Láthatunk persze ennek a hozzáállásnak az ellenkezőjét is, elég csak a WabiSabiLabi oldalra gondolni (www.wslabi.com), ahol árverési portált szerveztek a felderített sebezhetőségekhez. Álnaiva és álságosan a kutatók megsegítése volt

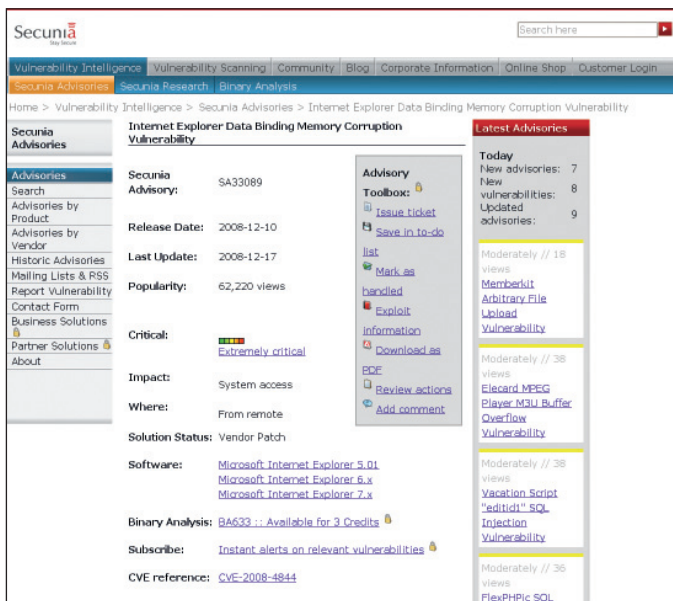
a hangoztatott cél, de azt azért mindenki sejtetheti, kiknek éri meg igazán az ilyeneket megvásárolni. A hamis antivírus programok fejlesztőinek például biztosan, és még csak nem is kellett nagyon mélyen a zsebükbe nyúlniuk ehhez. Emlékeztet, hogy egy orosz botnetes támadásokban résztvevő bűnöző a Bakasoftware 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, kértelen levelek mellékleteire kattintunk, nem frissítjük rendszeresen



Egy december 26-i weblapokat módosító támadássorozat saját webszövegeiben szerepelt a „HACKED By” karakterfüzér. A Google-be beütve meglepően sok magyar találatot is kapunk, és az érintett oldalak tulajdonosai sokszor nem is veszik észre a velük történt malört



A Secunia oldala (www.secunia.com) nemcsak a Personal Security Inspectorral igyekszik segíteni programjainak 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 végigdőlnek ezeken.

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 sürke hétköznapi mellett minden különleges alkalom, ünnep kihasználható eseményt jelent, lehetőséget a kártevőterjesztőknek, hogy különféle módszerekkel célba juttassák a kódjikat. 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 komlett, azonnal használatba vehető kártevőterjesztő készleteket kínálnak, amelyek segítségével „biztosan meg lehet keresni a karácsonyi ajándékre való”. Az interneten orosz weboldalakon hirdetett eszköz Basic, Standard és Professional változatban kapható, és természetesen a legdrágább, profi ver-

zió 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 tévézés 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 kérdései, hozzászólásuk van, juttassák el hozzánk (velemen@pcworld.hu).

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

KAPCSOLÓDÓ WEBOLDALAK

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