

Vajon létezik biztonságos böngésző?

Biztonságos böngészés? Na persze...

Mi lesz a Google-keresésekkel? Kitörölt sütik után is maradhatnak nyomaink? Valóban teljesen anonim az anonim böngészés? Lehetséges-e, hogy egy számítógépes kártevő a böngészőből kiolvasható személyes adataink és böngészési előzményeink nyilvánosságra hozatalával zsarol meg minket? Ilyen kérdések jártak a fejünkben a 39. epizód kapcsán.

Ha a „Létezik-e biztonságos böngésző?” kérdésre keressük a választ, jó támpontot adhatnak az alábbiak: „A böngészők ma már nemcsak egyszerű, HTML-megjelenítésre alkalmas programok. A weben szörfölve ezer szállal függünk a különböző, harmadik félről származó alkalmazásoktól, beépülő moduloktól és magától az operációs rendszertől, amelyeknek szintén hibátlanak kellene lenniük ahhoz, hogy biztonságban érezhessük magunkat. Mindez persze nevetséges illúzió. Azt hiszem, el kell fogadnunk, hogy böngészés közben sebezhetőek vagyunk” – véli a *Buherátor*. Nincs olyan böngésző, amelynek ne lenne tucatnyi felfedezett és felfedezetlen biztonsági sebezhetősége. A webalapú kártevőkről, az ajánlott és a biztonságot szolgáló pluginekről már értekezünk egyszer a 14. részben, az URL-ek rövidítéséből és egyéb linkekkel kapcsolatos veszélyekről pedig a 35-ös epizód adott részletes tájékoztatást.

Ahová nézek, szörny terem

Nincs már berlini fal méretű éles elválasztó a megbízható weboldalak és a gyanús webhelyek között, szemben azzal a régi megközelítéssel, hogy aki warez vagy pornó oldalakra látogat, az van kiemelt veszélyben. Ma már bármilyen weboldalról kaphatunk támadást,

The screenshot shows the F-Secure Browsing Protection interface. At the top, it says "F-Secure" and "BROWSING PROTECTION". There's a language selection dropdown set to "Magyar". Below that, there's a search bar with the URL "http://browsingprotection.f-secure.com/swp/" and a magnifying glass icon. The main content area has a "Kezdőlap" tab selected. It shows a large green circle with a white checkmark, indicating a secure site. To the right of the icon, it says "Meglátogatás biztonságos" and "Az F-Secure semmilyen gyanús működést nem talált a webhelyen. Legjobb tudomásunk szerint ez a webhely biztonságosan látogatható.". Below this, there's a link "Webhely tulajdonosának visszaelzése".

Az F-Secure Browsing Protection (browsingprotection.f-secure.com) bármilyen linkről megmutatja, hogy megbízható-e szerintük. Érdemes tisztában lenni azzal, hogy minden kártekony oldal esetében el kell tennie egy bizonyos időnek, amíg az adatbázisba bekerül és riasztást kapunk rá

és sokszor a manipulált keresőtalálatok is igyekeznek minket ezek felé terelni, ráadásul nincs ez másként a közösségi oldalak esetében sem. Az AVG végzett ilyen irányú kutatásokat, és az eredmények közel sem megnyugtatók: „Az ismertebb közösségi terek átvizsgálásával több mint 20 ezer olyan oldalra bukkantunk, amely valamilyen szempontból fenyegetést jelent az internezőkre. Ezek közül 11 701 darabot a Facebookon fedeztünk fel. Emellett a YouTube is igen elő-

kelő helyet foglal el: a felmérés szerint 7163 olyan oldal szerepelt a honlapon a tesztelés időszakában, amely veszélyt hordoz.” Ezen a helyzetben segíthet valamelyest, ha vírusvédelmi programunkban szerepel valamilyen kártekony URL-szűrő, illetve böngészőnkben is használhatunk ilyen plugineket. Ezek jól rosszul, időben vagy késve, de próbálják a nyilvántartott linkekkel és a kártekony tartalmakat blokkolni. Természetesen azért a gyanús helyek prívilégiuma nem szűnt meg teljesen; ha valaki például warez vírusirtót vagy ingyenes iWorks-csomagot tölt le, trójai kártevő-beltartalomra számíthat.

Nyuszika, van neked papírod az anonim böngészésről? Akkor azt akár szét is tépheted!

Ha valaki úgy gondolja, hogy semmilyen nyomat nem akar hagyni maga után, akkor általában a ma már minden böngészőben elérhető anonim módot szokta választani. Ilyenkor a böngészőkliens elvileg csak minimális adatot tárol, és szintén elvileg ezeket is elfelejtíti, ha kilépünk ebből a bizonyos módból. Ezzel kapcsolatban nemrégiben egy érdekes tanulmány jelent meg, amelynek az a lényege, hogy ilyenkor az anonimnak gondolt netezés után a könyvjelzők és a letöltött állományok eltüntetése mégsem történik meg, illetve sok eset-

The screenshot shows the Facebook registration page. At the top, there's a blue header with the Facebook logo. Below it, there's a form with fields for "E-mail cím" and "Jelszó", and a checkbox "Emlékezz rám". A button "Bejelentkezés" is next to it. Below the form, a note says "Elfelejtettek a jelszavat?". In the center, there's a large "Kisemmillzett Bvm" button. To its left is a placeholder image of a person's face. To its right, there's text about becoming friends with a friend on Facebook. At the bottom, there's a note about being a friend on Facebook and a "Regisztráció" button.

„Like-olását kegyelettel megőrzük.” Egy lehetséges jövőbeni üzleti modell, amelyben nem az amerikai adóhivataltól kérík le az évi 100 és 200 ezer dollár között kereső ügyfelek címlistáit, hanem majd a Facebooktól rendelik meg az adott pártprefencia szerinti klubtagságokkal és teljes like-történettel rendelkező ügyfelek adatait. Ki tudja, meddig sci-fi ez, és mikortól lesz valóság?



iGoogle

Gadgets installed 4 gadgets
Most recently added:
Tabs 1 tab
Most recently added: Kezdőlap

Talk
Contacts 3 contacts
Sample Contact: [REDACTED]@gmail.com

Web History
Web History: Enabled for searches only
Web Most recent: [REDACTED] AG on Sep 23, 2010
Images Most recent: totó lottó kártyanaptár on Jul 9, 2009
Maps Most recent: South Ealing Road, Ealing, London W5 4QB on [REDACTED]

A Google Dashboardjában (www.google.com/dashboard/) nemcsak a korábbi keresések naplózódnak, de a belépés alatti YouTube-videók és Google Maps-keresések is megőrződnek

ben a privát böngészésnél begyűjtött sütiket (cookie), SSL- és más tanúsítványokat is megőrizik, illetve a gyorsítótárat (cache) sem ürítik ki. Emiatt aztán a privát üzemmódból kilépve ezek később is visszakereshetők lesznek egy helyi vagy online támadó számára. Ugyancsak gyenge pont még, hogy a beépülő modulok sem támogatják minden esetben a privát módot, így az végül nem tud teljes értékűen működni. Ez a veszély szinte minden böngészőt érint, például a Firefox privát módjának védelme bizonyult a Stanford Egyetem tanulmánya szerint a leggyengébbnek.

Maradj csak bejelentkezve, Piroskám, hogy jobban halljalak és lássalak

Eddig jobbára a szoftverek tulajdonságairól beszélgettünk, persze azért szóba kerültek olyan dolgok is, ahol mi, felhasználók is te-

Web Képek Térkép Hírek Fordító Blogok Gmail továbbiak ▾ [REDACTED] @gmail.com | Fiók

Google Keresési előzmények Keresés az interneten

Internettes előzmények [REDACTED]@gmail.com címre vonatkozóan

Minden előzmény

- Web
- Képek
- Hírek
- Termékek
- Szponzorált linkek

Internettes tevékenységek	okt. 2		
H	K	Sz	K
27	28	29	30
4	5	6	7

Az óvatos netező megőrzött keresési előzménye ezt mutatja: semmi!

hetünk magunkért, például válogatott pluginekkel stb. Létezik egy olyan szokás is, amely a kényelem kontra biztonság mérlegelésben a kényelmet szolgálja, ám nem várt mellékhatásokkal is szolgálhat, amivel nem árt tisztában lenni. Ha valakinek gmailes postafiója van, és a leveleit webes felületen éri el, az biztosan találkozott már azzal, hogy belépve a kereséseinek a története is megőrződik, igaz, szerencsére ezt ki is lehet kapcsolni. Aki kíváncsi arra, hogy nála bekapcsolt volt-e ez a funkció, mit őrzött meg a Google a keresései ből, az látogasson el a www.google.com/history/ címre. Emellett a www.google.com/dashboard/ linken a belépve nézett Google Maps-keresések, továbbá az így megtekinntett YouTube-videók előzménye is elolvasható. Emiatt itt is, de minden más webhelyen is javasolt az azonnali kilépés, ha befejeztük a szolgáltatás használatát, illetve ha jót akarunk magunknak, soha ne ikszeljük be bejelentkezéskor a Maradjon belépve opciót. (Forrás: hopp.pcworld.hu/7368)

Flash sütik és egyéb fincsi nyárlánkságok

Léteznek a hagyományos sütiktől eltérő, úgynevezett Flash vagy Super sütik is, amelyek egy korrektül beállított, minden előzmény, cookie stb. törlést követően a böngészőből kilépéskor továbbra is megőrződnek. Természetesen

nem minden irányul ez ellenünk, a Flash-játékok például ebben tárolják el a high score listát, ami persze szép és jó. Azonban az a helyzet, hogy egyrészt a különböző reklámozó cégek is tudják ezt és már régóta ki is használják, valamint a HTML-sütik 4 kilobájtos méretéhez képest ezek akár 100 KB-osak is lehetnek. Nem rendelkeznek semmiféle lejáratú idővel, és a böngészőkliens helyileg is elkülönítve tárolja ezeket egy SOL kiterjesztésű fájlban. Tovább súlyosítja a helyzetet, hogy az ezekben tárolt személyes adatokkal a Flash cookie képes helyreállítani a korábban törölt webes süti tartalmát. (Forrás: hopp.pcworld.hu/7367)

Aki meg akarja kímélni magát ettől a reklámozócégeknek biztosan kiváló módszertől, annak érdemes lehet a **Better Privacy** kiegészítőt (hopp.pcworld.hu/7361) feltelepítenie, amelynek segítségével teljes körű sütiellenőrzés és -védelem valósítható meg, és természetesen rendelkezhetünk úgy is, hogy az általunk kiválasztott vagy akár az összes LSO-(Locally Shared Objects) elemek minden egyes kilépéskor teljes körűen töröljenek a gépünkről.

A Jó, a Rossz és a Profilalkotó

Tovább árnyalhatja a korábbi anonim böngészésben felvett képet az is, hogy az Electronic Frontier Foundation (EFF) 2010 tavaszán végzett egy kutatást, amelyben azt vizsgálták,

Google Keresési előzmények Keresés az interneten

Minden előzmény törlése

Törlendő időtartomány: minden

Minden előzmény törlve lesz.
Ez a művelet nem visszavonható.

Részletek

Böngészési és letöltési előzmények

Ürlapok és keresőmezők előzményei

Sütik

Gyorsítótár

Aktív bejelentkezések

Webhely beállításai

DownThemAll! előzmények és letöltési sorok

Mégse Töröl most

A böngészőkliensből való kilépés egy ajánlott módja: törölni minden tárolt elemet. Természetesen nyomozati eszközökkel a helyi gépen így is előtávolítható minden látogatott webhely

Web Képek Térkép Hírek Fordító Blogok Gmail továbbiak ▾ [REDACTED] @gmail.com | Fiók | Kilépés

Google Keresési előzmények Keresés az interneten

Internettes előzmények [REDACTED]@gmail.com címre vonatkozóan

Minden előzmény

- Web
- Képek
- Hírek
- Termékek
- Szponzorált linkek
- Videó
- Térkép
- Blogok
- Könyvek
- Szünet
- Elemek eltávolítása
- Trendek
- Könyvjelek

2009. dec. 7. (szerda)

10:45	Keresés: [REDACTED] Megtekintve 1 eredmény blog&topic=pet&func=list&tag=anon... [REDACTED]
10:35	Keresés: eldobható email cím -mpp Megtekintve 2 eredmény No-Spam.hu Eldobható e-mail cím [beta] - no-spam.hu techline.hu - Eldobható email-cím - techline.hu
10:34	Keresés: eldobható email cím Megtekintve 1 eredmény http://szoftvertipp.info/windows,egyszer-hasznalatos-email-clm/
09:28	Keresés: Alvaro@wes-up.org Megtekintve 1 eredmény Wes Alvaro - home - utk.edu

2009. szept. 16.

15:06	Keresés: [REDACTED] Ealing, London W5 4QB
15:06	Keresés: West Union Group

Osszes Google keresés: 69

Több oldalnyi nyomat, keresési előzményt hagyhat maga után az, aki óvatlanul, Google-fiókjába bejelentkezve keresgél a neten

A Firefox beállításai

- Figyelmeztetés kiegészítők telepítése előtt
- Bejelentett támadó webhelyek blokkolása
- Bejelentett hamisított webhelyek blokkolása

Jelszavak

- Webhelyjelszavak mentése
- Mesterjelszó használata

Figyelmeztetések
Válassza ki, hogy milyen figyelmeztetéseket szeretne kapni webböngészés közben

Kivételek... **Mesterjelszó megváltoztatása...** **Mentett jelszavak...** **Beállítások...**

Kártékony és hamisított honlapok figyelése alapértelmezett a Firefoxban. A bejelentett támadó webhelyek blokkolása jó dolog, bár késve jelenik meg nemcsak a figyelmeztetés, de a már tiszta állapot utáni visszavonás is

hogy IP-cím és egyebek nélkül, pusztán egy JavaScript segítségével lekérdezhető környezetben mennyire lehet azonosítani a névtelen netezőt. Ezek lehetnek például olyan alapvető információk, hogy milyen operációs rendszer alatt milyen böngészőverzióval neteznek, de akár olyan információk is kiderülhetnek, hogy mi a rendszerben alapértelmezettként beállított nyelv, vagy milyen betűtípusokat telepített, esetleg minden böngészőpluginet használnak a számítógépen. A tanulmány szerint ezzel a módszerrel a látogatók 94 százalékában megállapítható volt a látogató személye – számítógép-használat esetén. Mobilos böngészés esetén ugyanis sokkal kevesebb ilyen

egyedi extra jellegzetesség szerezhető meg – legalábbis egyelőre.

Ha kicsi a tét, kedvem sötét

Kezdetben voltak, sőt sajnos azóta is vannak a hamis vírusirtók. Aztán új találomány jött meg: a hamis szerzői jogi büntetés. A naiv ügyfél letölt valamit a BitTorrent-hálózatról, és ezek után a felugró JavaScript ablak nem ál-vírusfertőzésekkel tájékoztat, hanem illegális letöltésről, pénzbüntetésről. Valódinak látszó hivatalos pecsétben nincs hiány, és az állítólagos svájci székhelyű ICCP Foundation felszólít bennünket összesen négyszáz dollár befizetésére, amellyel elkerülhetjük az esetleges pert a maga zord következményeivel: 5 év börtön, 250 ezer USD bírság.

Vatera.hu Üdvözöljük a Vatera piactérén!

Kategóriák: kopogtató cédua | Minden kategóriában

Főoldal > Keresés: "kopogtató cédua"

Találatok Kategóriánként: Egyebek (2)

Hirdetés: 4 MILLIÓ VAN A PAKLIBAN! Nyerjen minden nap!

Ezeket mutassa: minden termék | Aukciós termékek | eladók termékek

2 db termék a(z) "kopogtató cédua" kulcsszóra

A keresés mentéséhez kattintson ide » Csak szöveg | Kis képekkel | Nagy képekkel

Áru neve: Kiemelt ajánlatok

Növelte értékesítési esélyeit! Emelje ki termékéit a többi cédban!

Kopogtató cédua | Kopogtató cédua

Google Hirdetések

Csak egy példa, hogy a szolgáltatók sosem tudnak azonnal reagálni az eseményekre. Mindig eltelik bizonyos idő, mire bejelentést kapnak, vagy pedig monitorozással, naplóelemzéssel észlelik, hogy be kell avatkozniuk. Ugyanez áll a kártékony linkek nyilvántartására is

Bár az ICCP azt sugallja, hogy munkakapcsolatban áll a valódi jogvédő szervezetekkel (RIAA-val, MPAA-val stb.), ez nem igaz. Sőt berezelni sem kell, és színtúgym nem javasolt turkálni a Visa vagy Mastercard kártyánk után, mert ez az egész egy nagy csalás. Ám itt nem állt meg a bűnözők fantáziája: megjelent ugyanis a Kenzo (Kenzero) trójai. Ez nem tesz mást, mint a fertőzött gépről ellopja a böngészés adatait, majd egy publikus weboldala kitéve azért követel váltságdíjat, hogy azt onnan eltávolítsa. A Japánban felbukkanó vírus a 200 milliós táborral rendelkező Winny

VIRUS TOTAL

VirusTotal is a service that analyzes files and URLs and facilitates the sharing of viruses, worms, trojans, and malware detected by antivirus information...

0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this URL is benign. 0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this URL is malicious.

Submission date: 2010-10-01 08:26:09 (UTC)
Current status: finished
Antivirus report: View downloaded file analysis
WebScan result: 2 / 7 (25.6%)

[Compact](#)

URL analysis tool	Result
Firefox	Malware site
Google Safebrowsing	Malware site
Opera	Clean site
ParetoLogic	Clean site
PhishTank	Clean site
TRUSTe	Clean site

Additional information

Normalized URL: <http://rev570.com/>
URL MD5: bfde4d45c4950f08d820ee8db24531af
Content-Type: text/html

VT Community

This URL has never been reviewed by any VT Community member. Be the first one to comment!

0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is goodware. 0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is malware.

File name: .rar
Submission date: 2009-12-22 11:26:00 (UTC)
Current status: finished
Result: 22 / 41 (53.7%)

[Print results](#)

There is a [more up-to-date report](#) (35/41) for this file.

Antivirus	Version	Last Update	Result
a-squared	4.5.0.43	2009.12.22	-
AhnLab-V3	5.0.0.2	2009.12.22	-
AntiVir	7.9.1.122	2009.12.22	TR/Drop.Agent.BD
AntiY-AVL	2.0.3.7	2009.12.22	Trojan/MSIL.Agent.gen
Authentium	5.2.0.5	2009.12.22	-

Egy ideje már URL-eket is tudunk vizsgálni a VirusTotal.com-on. A több különböző adatbázis, illetve a felhasználói kommentek is segíthetik az eligazodást

„Pénzt, vagy a böngészési előzményeid egy publikus weboldalon landolnak!” – ez lehetne a Kenzo trójai mottója. Ha valaki korábban pornót nézett, akkor most kellemetlen meglepetésben lehet része



PORT.hu | Napi ajánló | TV | Mozi | DVD | Színház | Fesztivál | Zene | Klállítás | Gyerek | Sport | Rádió | Étterem
 Hotel | Játék | Tudás

PORT.hu > TV (Budapest) > A mamut | Összes értesítőm | Összes eseményem | Személyes ajánló | Kijelentkezés

Idő szerint | Hely szerint

Vetítik:
FILM: Vasárnap (Október 3.) 2:55 4

Vélemény | Összes hozzájárulás (58)

[anakin@globonet.hu](#) | Válasz | Borzasztó! Nem ajánlom senkinek a film megtékinését, maximum a mazochistáknak! 1/10 | szep. 28. 14:24 | 58/58

[tomiloki](#) | Válasz | Előzmény (Tskull) | olyan jó horrott áltadtam és benne volt a kedvenc színészem Mike Epps akiről kiderült hogy álcázta magát hogy velem jöjjön d e egy szörny volt és pesze én is meghaltam és kívülről néztem végig | máj. 29. 21:11 | 57/58

[víziócs](#) | Válasz | Pusztulat! Az ovisok harsányan röhögnek rajta! Miért kell a film+nak ilyen ürléket megvásárolnia, ahelyett hogy néhány többször is leforgatható, de nem unalomig játszott igazi filmet vetítének le! Igaz a mai nap, "A sárkány közelbelé" című moziival valamelyest javítottak, kategóriájának egyik csúcsfilmje, de egy 1973-as film amit már mindenki látott, aki meg akarta tekinteni! Az utóbbi időben ez a csatorna is többször leadta már! Ma tuti nem a film+ a nyerő csatorna! | márc. 04. 19:31 | 56/58

[Kivagyok?](#) | Válasz | A ZS kategória szégyene. | márc. 04. 18:28 | 55/58

[Rahar](#) | Válasz | Egyetértek az előttem írókkal, gagyi történet, primitív kivitelezés és a színész munka hiánya jellemzi. Szinte bármit érdemes csinálni az életben mert ezen film megtékinése szerintem totális időpazarlás, mindenki kerülje el. | 2009. nov. 10. 03:50 | 54/58

Hogy segítenek-e, vagy letérítenek a tisztaítás ösvényéről a közösségi vélemények, ezt nehéz megmondani általánosságban, konkrét esete válogatja. Mindenesetre, ha a kom mentelők többsége a Zs kategória szégyenének, vagy kártékony állománynak tart valamit, az azért intő jel lehet

fájlcserei honlap felhasználói közül azokat vette célba, akik a megosztóoldalról erotikus tartalmakat töltötték le. Nyilván ennek világába kürtölése mellett az azonosításhoz ele gendő minden bongészési adatának nyilvánosságra hozatala kellemetlen lehet a letöltőnek. A lényeg minden esetre maradt: fizessen itt a felhasználó tulajdonképpen a semmi-

ért. (Források: hopp.pcworld.hu/7364, hopp.pcworld.hu/7365)

A nagy testvér nem is titkolja

Gyakran szoktuk mondogni, hogy „én okosan bongészek”, viszont tudnivaló, hogy bármelyik weboldal vagy banner tartalmazhat ismeretlen kódot, szkriptet. Összegzésképpen biztonságos

böngésző vagy böngészés nincs, inkábbjó kom promisszum, és hasznos óvatos szokások, meg felelő hozzájárás, hadra fogható pluginok gyűjt eménye létezik. Ilyen hasznos szokások lehetnek a minden böngészés utáni cache-ürítés, a session cookie-k törlése (amelyek bizonyos körülmények között ellenőrizték), néhány alap plugin, például a *Finjan SecureBrowsing* (finjan.com), *NoScript*, *NetCraft*, *ShowIP*, *Adaptive Referrer remover*, *Cache Status*, *Cookie Safe*, *JS View*, *Secure Login*, *XSS Guardian* és az *XSS Warning* használata. Utóbbiak az addons.mozilla.org oldalon kereshetők meg. Emellett persze a rendszeres jelszócsere is ilyen okosság. (Forrás: hopp.pcworld.hu/7366)

Zárógondolatnak következzen a Google-el nök, Eric Schmidt véleménye a keresések nap lózásáról: „Senki ne csináljon semmi rosszat, és akkor eleve nem is lesz oka félni. Ha valakinek nem tetszik, hogy a cégek keresője és más weboldalak segítségével több évtizedre visz számenőleg is kikereshetők adatai róla, akkor egyszerűen csak változtassa meg a nevét.” (Forrás: hopp.pcworld.hu/7363)

Kérjük kedves olvasónkat, ha a témaban kér désük, hozzájárulásuk van, juttassák el hozzánk (velemeny@pcworld.hu).

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

Kapcsolódó weboldalak

Tanácsok a biztonságos Facebook használathoz:

www.facebook.com/biztonsag

Antivirusburgi Ünnepi Játékok:

hopp.pcworld.hu/7266

Hamis profilk:

hopp.pcworld.hu/7267

Zaklatás a gépből:

hopp.pcworld.hu/7268

10+ Tips To Identify Fake Profiles

On Facebook:

hopp.pcworld.hu/7269

Fake Facebook Profiles:

hopp.pcworld.hu/7270

Fake Facebook Profile Equals Jail Time?:

hopp.pcworld.hu/7271



A kártevőterjesztők fantáziája kiapadhatatlan. A hamis antivirusok után megjelent a hamis szerzői jogi felszólítás, persze a befizetett „büntetés” itt is a bűnözök zsebébe vándorol