Az új süti szörny: a Privacy Badger

Írta: Paul Arnote (parnote)

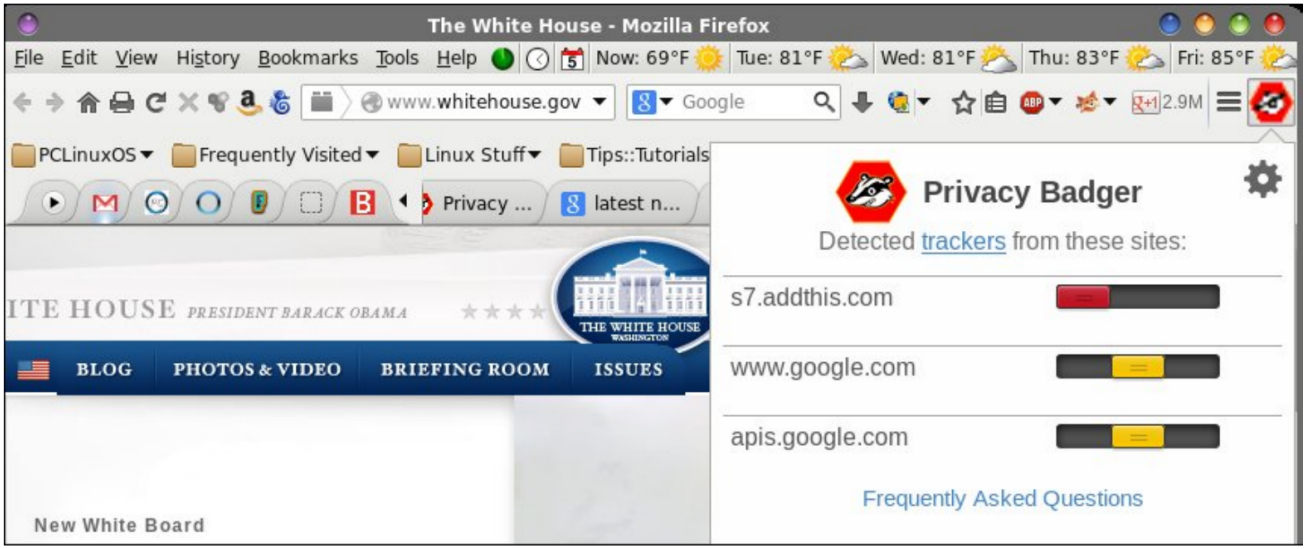
Ha a tolakodó online hirdetések és az internet kémkedés nem lett volna elég, most aggódhatunk a megfigyelés egy új formája miatt. A „Canvas fingerprint”-nek (ujjlenyomat) hívott ronda trükk az, amit egyes weboldalak a felhasználóik internetes tevékenységének megfigyelésére használnak.

Íme, így működik. Amikor a böngésző betölti a lap kódját beágyazott JavaScript módosítja a canvas API-t, ami a modern böngészők többségében megtalálható. Ez az API hozzáfér a felhasználói gép grafikus chipjéhez. A weblap kéri a böngészőt, hogy olvasson be egy rejtett képet. Mivel minden gép a képeket eltérő, a számítógép hardverétől részben függő módon olvassa be, a kép egy egyedi sorszámot kap, ami később felhasználható az adott felhasználó azonosítására az Interneten való mozgása közben.

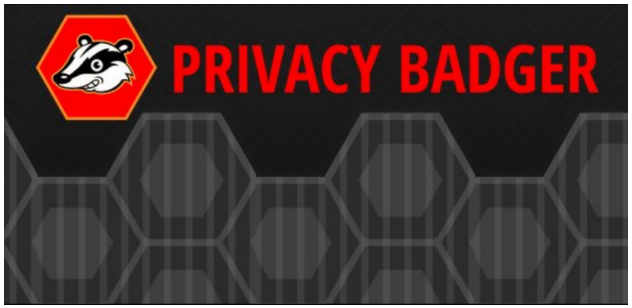
Hirdetők és mások, akik a felhasználókat az Interneten követni akarják, szeretnének a sütiktől megszabadulni. A végfelhasználó a sütiket blokkolhatja és fizikailag is törölhetők a felhasználó által. Sütik betöltése használhatatlan a felhasználók követésére, különösen, ha célzott hirdetést kellene küldeni az adott felhasználónak.

A canvas (festővászon) ujjlenyomatozása sokkal lopakodóbb. SEMMI SEM tárolódik a felhasználó gépén, vagyis sokkal nehezebb az átlagos felhasználónak törölni. Igazából a legtöbb felhasználó talán azt sem veszi észre, hogy megfigyelik, vagy hogy az ujjlenyomat létezik.

Sajnálatos módon az ujjlenyomat olyan oldalakra is befurakodott, amikről sosem tételeznéd fel, mint például a Fehér Ház honlapja. Az AddThis nevű



nyomkövető widget kimondottan notórius a canvas ujjlenyomat alkalmazásában. Az AddThis készítői állítják, hogy a canvas fingerprint kódot jólius elején eltávolították a widget-jükből, de bevallották, hogy kísérleteztek vele egy öt hónapos tesztfuttatás során. Természetesen ezt nem hozták az átlagos internethasználók tudomására, a teljes nyomkövetési tevékenység úgy folyt, hogy a használó nem tudta, figyelik. Egy időben több, mint 5000 jelentős oldal használta az AddThis nyomkövető widget-et. A fenti kép mutatja, hogy a Fehér Ház oldala még mindig használja.



Nos, mit tehet a felhasználó a magánélete védelmére? Nos, köszönetet mondhat az Electronic Frontier Foundation-nak. Elkészítették a Privacy Badger-t, ami sütiket eszik reggelire, ebédre, vacsorára és esti falatozáskor. A canvas fringerprinting blokkolása olyan tulajdonság, aminek a jövő verziókba be kívánnak építeni. Jelenleg az AddThis widget-et blokkolja, mivel nem képes kezelni a felhasználók „Do Not Track” (ne kövess) kérését.

Íme a Privacy Badger leírása a letöltési oldalon:

A Privacy Badger blokkolja a kém hirdetéseket és láthatatlan nyomkövetőket. Célja, hogy megakadályozza a cégeket a böngészésed engedély nélküli megfigyelésében.

Ez a kiterjesztés arra való, hogy automatikusan védje a magánéletedet a harmadik fél böngészés közben láthatatlanul betöltődő megfigyelőitől.

Minden egyes kéréssel elküldjük a Do Not Track fejlécet és a kiterjesztésünk elemzi az esetleges nyomkövetés fennmaradását. Ha az algoritmus úgy találja, hogy a valószínűsége túl magas, automatikusan blokkolja a kérés továbbküldését a szolgáltató felé. Meg kell érteni, hogy a Privacy Badger még béta és az algoritmus megállapítása az adott nyomkövetéséről nem perdöntő.

A kiterjesztésnek három állapota van. Vörös azt jelenti, hogy a Privacy Badger szerint a domain nyomkövető és blokkolta. Sárga, ha a domain vélhetően nyomkövető, de a lap működéséhez szükséges, ezért a Privacy Badger engedi, de a sütijeit blokkolja. Zöld, ha a Privacy Badger számára nem tűnik nyomkövetőnek. Ha felülírnád az automatikus blokkolás beállításait, akkor böngésződben a Privacy Badger ikonjára kell kattintani. Egyébként békésen böngészhetsz, mivel a Privacy Badger felkutatja és elfogyasztja a webes nyomkövetőket egyenként.

Semmi sem állíthatja meg a Privacy Badger-t a sütik fogyasztásában, amikor éhes!

Privacy Badger az Electronic Frontier Foundation projektje.

A Privacy Badger „jelentése” a The PCLinuxOS Magazine weboldaláról.

A Privacy Badger jelenleg Firefox-ra és Chrome-hoz érhető el. Telepítése könnyű, a többi böngészőhöz való kiterjesztés, vagy kiegészítő telepítésének menetét követi. A nyomkövetők tevékenysége az adott nyomkövetőhöz tartozó csúszka mozgatásával beállítható, engedélyezve (zöld), engedve, de a sütiket blokkolva (sárga), vagy teljesen blokk (piros).

Összegzés

Az átlag állampolgár elleni illegális kormányzati internetkémkedésnek korán sincs vége. Szerintem még csak közel sincs a csúcshoz. A netes állampolgárnak a legkevésbé hiányzik egy újabb fenyegetés a magánéletére. Emellett a magánélet az Interneten és másfajta kommunikációban (pl. mobiltelefon) a közösségi öntudat frontvonalában van.

Ha NoScript-et futtatsz, akkor viszonylag biztonságban **kell** lenned a canvas fingerprintektől, mivel a NoScript megakadályozza a JavaScript kód futását és az egyedi ujjlenyomat létrehozását. Azt pedig a többieknek jó tudni, hogy van a nyomkövetőket automatikusan a háttérben lerendező, a Privacy Badger. A EFF magánéleti minden vetülete melletti elkötelezettségét ismerve, senkiben sem bízhatok meg jobban, mint bennük a magánélet és az internetes lábnyomok kezelésének kérdésében.

Screenshot Showcase

Posted by gseaman, on August 21, 2014, running KDE.