

## Webbanalys

Hemsidan  
Webbanalys artiklar

### Se upp för ful-cookies

Cookies sänds ut från de flesta webbplatser för olika syften, men det är skillnad på vanliga cookies och s.k. "ful-cookies" när det gäller webbstatistik där de används för att räkna ut bl.a. antalet unika besökare. Den senare typen utgör ett dolt hot mot din integritet och möjliggör att 3:de part som exempel kan se vilka webbplatser som du besöker.

#### Vad är en cookie

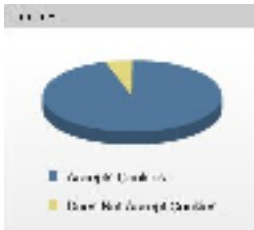
Enligt PTS är en cookie en textfil som webbplatsen du besöker begär att spara på din dator. Cookies används på många webbplatser för att ge en besökare tillgång till olika funktioner, men även i webbstatistik syften i samband med webbanalys. Statistikcooken i kombination med IP numret blir det möjligt att skilja olika webbläsare åt, speciellt då webbläsaren sitter bakom en brandvägg eller proxy server genom vilka anrop till webbplatsen passerar.

Det finns två typer av cookies, sessionscookies som är temporära och permanenta cookies vilka används i t.ex. webbstatistik sammanhang. Vad som avses med vanliga cookies är cookies (oavsett typ) som tas emot i samband med ett besök till en webbplats, och som är unika för webbplatsen ifråga. ful-cookies däremot är en och samma cookie som delas av många webbplatser, och det är dessa som utgör ett dolt hot mot den personliga integriteten för en webbplats besökare.

#### Hysterisk cookie radering

Det senaste året har hysterin kring radering av cookies ökat, och speciellt i dagspress har rapporteringen inte lyckats med att skilja åt de olika typer av cookies som finns. I kölvattnet på raderingen så har glöms det ofta bort att en cookie är nödvändig för att kunna få fram en rättvisande webbstatistik. Utan en korrekt webbstatistik blir det svårt att på ett professionellt sätt driva en webbplats, det skulle kunna liknas vid att köra en bil utan instrumentpanel.

Diverse program såsom Ad-Aware och Spybot är idag allt för grova i sin gallring, de är tyvärr oförmögna att kunna skilja en cookie för webbstatistik som endast används av en webbplats från en ful-cookie som används av flera olika webbplatser. I bilden nedan ser man 2 olika cookies som Ad-aware funnit vilka sånts ut tillsynes i webbstatistik syfte:



Hur många av dina besökare blockerar din statistik cookie?  
**Mät med HBX Analytics!**

| Obj.                     | Vendor          | Type          | Category   | Object                                 | Comment  |
|--------------------------|-----------------|---------------|------------|----------------------------------------|----------|
| <input type="checkbox"/> | Tracking Cookie | IECache Entry | Data Miner | Cookie: ...@imrworldwide.com/cgi-bin   | Hits:174 |
| <input type="checkbox"/> | Tracking Cookie | IECache Entry | Data Miner | Cookie: ...@ehg-salesforce.hitbox.com/ | Hits:52  |

Någon åtskillnad mellan dessa två cookies görs inte, utan båda anses vara kritiska objekt som skall tas bort. Detta utgör en stor brist i liknande verktyg, de presenterar dessvärre informationen på ett onyanserat sätt för användaren.

#### Description

This cookie is known to collect information that may be used either for targeted advertising, or tracking users across a particular website, such as page views or ad click-thrus.

Skillnaden i en cookie för webbstatistik och en ful-cookie ligger i varifrån den sänds och hur unik den är för webbplatsen. I ovanstående fall kommer ful-cooken från imrworldwide.com att delas mellan samtliga webbplatser där data insamlas av detta system för webbstatistik. Just användandet av en obskyr domän för insamling av data för webbstatistik är första tecknet på att man har att göra med en ful-cookie. Nyligen skrevs det om detta i [The Wall Street Journal Online](#), och kanske kommer svensk press snart att börja skärskåda de system som deras egna webbsidor nyttjar.

Den andra cookien som anges i Ad-aware rapporten är unik för Salesforce webbplats, d.v.s. denna cookie kommer endast att kunna identifiera besökande webbläsare till den webbplatsen. Eftersom denna cookie ur ett insamlingsperspektiv är unik för webbplatsen kommer ägaren av webbplatsen inte kunna se vilka andra webbplatser en specifik webbläsare t.ex. besöker under en given tidsperiod i och med detta. Insamlingspunkten i detta fall blandar inte ihop besöksinformation från ett flertal webbplatser, vilket är fallet med det system som sänder ut ful-cooken.

System för webbstatistik vilka använder ful-cookies saknar påfallande ofta en tydlig deklaration på hur den personliga integriteten hanteras, och även om det finns deklarationer på detta så strider per automatik användandet av en enda cookie för samtliga webbplatser de samlar in data ifrån mot trovärdigheten i deklarationen. Ett exempel på en omfattande deklaration finner du [här](#).

#### ful-cookiens födelse

Men hur har en så pass simpel sak som en liten text fil orsakat så mycket skrivelser och för den vanlige surfaren ett behov av att regelbundet ta bort dessa?

Problemet uppstod troligen ur behovet av att veta mer om besökarnas beteende och surfande, men även av ren slöhet och uselt utformade arkitekturer i vissa lösningar för webbstatistik. Exempelvis så ville annonsföretag undvika att samma annons visades till en besökare om denne besökte flera webbplatser som annonsföretaget försåg med annonser. Kontrollen kom då att styras av en gemensam cookie från annonsföretagets server, och ful-cooken var född. Med den kunde ett annonsföretag kontrollera vilka annonser på en given webbplats som en given cookie från deras server blivit exponerad för.

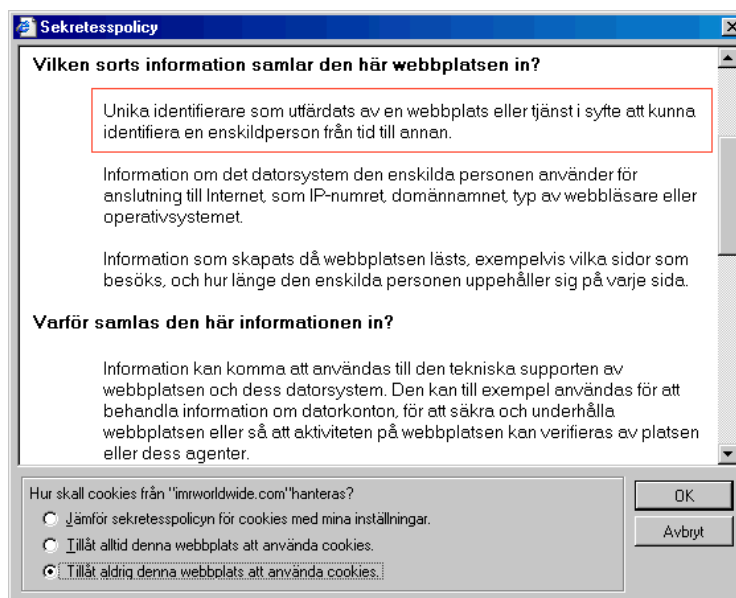
Baksidan på denna effektiva styrning av annonser med hjälp av cookies blev dessvärre att annonsföretaget kunde se vilka webbplatser om varje enskild webbläsare besökte, vilket direkt ledde till ett direkt hot mot den personliga integriteten. I USA kom företaget att hamna inför domstolar på grund av vad man ansåg vara intrång i den personliga integriteten, ett exempel kan du läsa om [här](#).

Visst kan man påstå att det är en "win-win" att kunna styra hur många gånger en annons visas för en webbläsare som en representant för ett annonsföretag gör i en [artikel i InternetWorld](#), men deras egen webbplats saknar idag (2005AUG16) en tydlig cookie förklaring trots att de använder cookies för att styra annonserna. Och det är knappast så att de webbplatser på vilka annonserna exponeras tydliggör att externa cookies vilka de saknar kontroll över används.

I samma artikel påstår en företrädare för ett annat företag att de för varje webbplats de mäter besöksstrafiken på sätter en unik cookie, men verkligheten visar något helt annat. Det är enkelt att se att detta inte stämmer, testa själv genom att rensa bort samtliga kritiska objekt enligt Ad-aware och besök webbplatserna för Sveriges fyra största dagstidningar så blir resultatet att det endast är 1 enda cookie dolt under det obskyra namnet ...@cgi-bin[1].txt som återfinns. Detta är signaturen på en ful-cookie, att en och samma cookie används av ett flertal webbplatser.

#### Selektiv blockering av cookies

Värre ändå är att cookien ifråga har en cookie policy som borde ha satt fart på debatten om den personliga integriteten på internet. Microsoft Internet Explorer har en mycket bra funktion (som tyvärr saknas i Firefox) där man för varje given sida kan ta fram en sekretessrapport (klicka på visa | sekretessrapport) så får man upp en lista på samtliga objekt som sidan består av.



Med två klick kan man permanent förhindra att webbläsaren tar emot denna ful-cookie, och på så sätt bättre selektera bort dessa. Liknande funktion för att blockera en sådan cookie finns även i Firefox och andra webbläsare.

#### Selektiv radering av cookies

Att blint radera alla cookies leder till att webbplatsägare får sämre möjlighet att kunna analysera den egna trafiken, kunskap om detta ger dem möjlighet att bättre utforma och tillhandahålla information till dig som besöker webbplatsen. En selektiv radering är att föredra, speciellt då de cookies som på ett korrekt sätt sänds ut från de webbplatser som besöks regelbundet och värnar om din integritet bör vara kvar av den anledningen. Det gäller att skilja agnarna från vetet.

#### Framtida hot och möjligheter

I ett av våra grannländer har det till och med förts på tal av medlemmar i en mätorganisation om att använda den interna adressen till datorns nätverkskort (MAC-adressen) för att unikt särskilja webbläsare, förhoppningsvis så är gällande lagstiftning i Sverige tillräckligt klar på den punkten att vi kommer att slippa liknande intrångsliknande försök.

Om de branschliknande mätorganisationer och större webbplats ägarna gör rätt och städar upp i cookie träsket kommer detta att radikalt minska mängden ful-cookies, frågan är bara om de vill och kan.

«««