DIENST COMMUNICATIE
AFDELING NIEUWS
OUDE MARKT 13
3000 LEUVEN

PERSBERICHT

Webgebruikers worden vaker stiekem gevolgd dan eerder gedacht

Voor elke 10 000 websites die dagelijks het meest bezocht worden zijn er 145 die hun bezoekers volgen, ook al geeft deze bezoeker expliciet aan dit niet te willen. Recent doken maar liefst 16 nieuwe toepassingen op die toelaten de gebruiker te volgen op het web. Daarmee is dit probleem veel groter dan aanvankelijk gedacht. Dit blijkt uit onderzoek van KU Leuven en iMinds.

Elk toestel waarmee iemand online gaat beschikt over een webbrowser. Deze browser heeft specifieke eigenschappen, zoals de grootte van het scherm, de softwareversies die gebruikt worden of de geïnstalleerde lettertypes. Bij de meeste browsers vormen deze eigenschappen samen een combinatie die uniek is voor elk toestel, een digitale 'vingerafdruk'. Bezoekers van een website die een dergelijk volgsysteem gebruikt, worden geïdentificeerd aan de hand van deze vingerafdruk, waarna het systeem hun verdere doen en laten op het net kan volgen. Recent doken maar liefst 16 nieuwe toepassingen op die deze 'vingerafdruk'-dienst aanbieden.

De meeste volgsystemen maken een vingerafdruk op basis van Flash. Het systeem zet een onzichtbaar flash-object, zoals een filmpje, op de website. Dit object geeft het volgsysteem vervolgens de kans om allerhande informatie over de browser te verzamelen. Sommige Flash-objecten gebruiken zelfs twijfelachtige technieken om het originele IP-adres van de bezoeker te achterhalen. Apple-producten zoals de iPad en iPhone werken niet met Flash, maar zijn daarom niet beter beschermd. Nieuwere volgsystemen schrijven een onzichtbaar bericht op je scherm. Ze zetten dit bericht in verschillende lettertypes en kunnen aan de hand van de veranderende afmetingen van het bericht achterhalen welke lettertypes al dan niet beschikbaar zijn in je browser. Daar waar voordien slechts één bedrijf deze dienst aanbood, groeide dat aantal intussen aan tot 13.

Officieel zouden deze vingerafdrukken dienen om bijvoorbeeld fraude op te sporen, botnets te blokkeren die je computer inzetten als 'zombiecomputer' voor hun eigen doeleinden, en bescherming te bieden tegen het stelen van accounts. Onderzoek suggereert echter een groeiend gebruik van deze methoden voor het profileren van gebruikers voor marketing doeleinden. In deze logica is het ook opmerkelijk dat de systemen zelfs gebruikers volgen die expliciet aangeven dit niet te willen. De meest recente browsers maken immers gebruik van een 'do-not-track header' die aan de volgsystemen duidelijk maakt dat deze gebruiker niet gevolgd wil worden. Bovendien kwamen de onderzoekers er ook achter dat 'Tor Browser' en 'Firegloves', twee tools die gebruikt worden om de privacy te beschermen, kwetsbaar zijn voor deze volgsystemen.

Onderzoekers van KU Leuven en iMinds ontwikkelden software om deze online volgsystemen te detecteren. Deze software zal binnenkort vrij beschikbaar zijn voor andere onderzoekers op http://homes.esat.kuleuven.be/~gacar/fpdetective/

Contact:
Gunes Acar (engelstalig), Afdeling Computerbeveiliging en Industriële Cryptografie KU Leuven, tel: 0487 125 633, e-mail: gunes.acar@esat.kuleuven.be
Professor Bart Preneel, Afdeling Computerbeveiliging en Industriële Cryptografie KU Leuven, tel: 016 32 11 48, e-mail: bart.preneel@esat.kuleuven.be