de Correspondent

Explainer

07.10.2013 • Leestijd 4 minuten

De NSA probeert al jaren om de populaire privacytool Tor te kraken, zo maakten The Guardian en de Washington Post afgelopen weekend bekend. Maar wat is Tor en waarom is dit belangrijk nieuws?

Wat is Tor?

Correspondent Veiligheidsindustrie

Dimitri **TOKMETZIS**

Wat is Tor?

Tor staat voor The Onion Router en is een netwerk van computers waarop je anoniem kunt surfen. Het is ongeveer tien jaar geleden ontworpen met steun van de Amerikaanse marine om veilige communicatie over het internet mogelijk te maken. Later is Tor, met financiële steun van de Amerikaanse regering en veel

vrijwilligers, uitgebouwd tot een mondiaal netwerk.

Waarom zou je Tor willen gebruiken?

Simpel. Om anoniem te blijven. Daar kunnen verschillende motieven voor zijn. Sommige Tor-gebruikers houden zich bezig met illegale activiteiten. Naar onder andere die mensen is de NSA op zoek. Maar Tor wordt ook veel gebruikt door dissidenten en journalisten in autoritaire regimes. Bedrijven en overheidsdiensten gebruiken Tor soms voor gevoelige communicatie. Maar ook voor minder spannende zaken kan Tor nuttig zijn. Als je bijvoorbeeld naar een medische aandoening zoekt op internet en je wilt geen spoor achterlaten (en later lastig gevallen worden door allerlei advertenties), dan kan de anonimiseringsdienst uitkomst bieden.

Waarom staat het ineens in de belangstelling?

Afgelopen weekend publiceerden The Guardian en de Washington Post tegelijkertijd een verhaal over jarenlange pogingen van de NSA om het Tor-netwerk te kraken. De kranten baseren zich op gelekte NSA-documenten die door Edward Snowden zijn geleverd.

Hoe werkt Tor?

Al het verkeer op internet bestaat uit twee onderdelen: de inhoud en de verpakking. Wanneer je contact maakt met een website verloopt dat via verschillende schakels, routers genoemd. Die lezen niet de inhoud van het bericht, maar alleen welk adres er op de verpakking staat, dus waar het pakketje heen moet en van wie het afkomstig is. Tor pakt het bericht in meerdere verpakkingslagen tegelijk in. Iedere keer dat het bericht langs een Tor computer komt, wordt er een verpakkingslaag weggehaald. De laatste computer, de

zogenoemde exit node, haalt de laatste verpakking weg en stuurt het bericht door naar de gewenste computer met als afzender de exit node. Op die manier is al snel niet meer te reconstrueren waar het oorspronkelijke bericht vandaan kwam. Je bent geheel anoniem. De servers van Tor worden door vrijwilligers geleverd en onderhouden. In principe kan iedereen hier aan meehelpen en zijn eigen computer beschikbaar stellen voor Tor. Hoe het precies werkt, zie je hieronder .

Is Tor 100 procent veilig?

Nee. De verpakking wordt geanonimiseerd, maar de inhoud blijft ongewijzigd. Wie na de laatste Tor-computer, de zogenoemde *exit node,* een tap plaatst, kan de inhoud alsnog onderscheppen. Veel opsporings- en veiligheidsdiensten hebben daarnaast exit nodes geïnstalleerd. Tor is dus alleen veilig als ook de inhoud versleuteld is.

Hoe probeert de NSA Tor te kraken?

Met brute kracht en door de zwakste schakel te vinden. Als het aankomt op brute kracht, probeert de NSA het hele netwerk te verzwakken door veel verkeer te genereren. Tor gaat daardoor langzamer werken en wordt minder aantrekkelijk voor gebruikers. Uit de onthullingen van Snowden blijkt dat de NSA deze methode nauwelijks gebruikt. De NSA probeert ook computers van gebruikers te infecteren met een virus. Zij richt computers in die zich voordoen als *Google servers*. Ze plaatsen die computers echter op de zogenoemde *backbone* van het internet, de grote verkeersaders waar haast niemand toegang toe heeft. Als een gebruiker vervolgens Google probeert te bereiken, zijn deze servers net iets sneller dan die van Google. Ze

plaatsen vervolgens een virus waarmee de NSA gebruikers blijft volgen.

Daarnaast zoekt de NSA de zwakste schakel in het netwerk, in de meeste gevallen is dat de gebruiker. Uit de onthullingen van The Guardian en de Washington Post bleken er veiligheidsproblemen te zijn met de Firefox-browser die Tor aanbiedt als toegangspoort naar het netwerk. Die problemen zijn inmiddels verholpen, maar werken alleen als iedere gebruiker de laatste Firefox-versie heeft geïnstalleerd. Een andere slimme truc is het plaatsen van cookies. Niet iedereen denkt eraan de Tor-browser cookies te laten weigeren. De NSA heeft via Google advertenties opgekocht om zelf cookies te kunnen plaatsen. Op die manier kan de dienst gebruikers blijven volgen.

Waarom is dit nieuws belangrijk?

Een aantal van de bovengenoemde zwakten is al langer bekend en inmiddels verholpen. Door de onthullingen van The Guardian en de Washington Post is duidelijk geworden welke zwakten er nog meer in het Tor-systeem zitten. Die kunnen nu worden aangepakt. Het goede nieuws is dat de NSA Tor niet heeft kunnen kraken. Tor voorziet in een belangrijke behoefte van activisten, journalisten, maar ook bedrijven en overheidsdiensten om ongezien te kunnen communiceren. Als er problemen zijn in de veiligheid van Tor, kan dat nare gevolgen hebben voor de gebruikers. De NSA zal daarom ook in conflict komen met een aantal andere overheidsdiensten die Tor juist financieren, zoals het Amerikaanse ministerie van Buitenlandse Zaken. De NSA zal vermoedelijk een manier moeten verzinnen om met een minder groot sleepnet kwaadwillende Tor-gebruikers te ontmaskeren.

Met dank aan @koenrh voor het meelezen.

Update 14.20 uur. Lezer Jaap-Henk Hoepman wees op een storende fout in het stuk. Het gaat om de volgende oorpsronkelijke passage: 'In het Tor-netwerk wordt dit pakketje onderweg verder ingepakt. Bij iedere computer die het aandoet, komt er een extra verpakking omheen. Die nieuwe verpakking verhult de oorspronkelijke bestemming, het geeft als retouradres de vorige computer aan in het Tor-netwerk.' Het moet juist andersom zijn. Het bericht wordt in verschillende pakketten gestopt, waarna iedere node in het netwerk een pakketlaag verwijderd.

Update 19.33 uur. Ik heb deze zin geschrapt, na de passage dat de FBI en de NSA exit nodes beheren. 'Daarmee zijn in het verleden bijvoorbeeld verspreiders van kinderporno opgespoord.' Dit gebeurde niet na de exit nodes, maar door een zwakte in de browser. Dank aan @conflictmedia voor de oplettendheid.
