DOOR: RONALD SMIT

DARKNET

Legale én illegale avonturen in de cloud

Je hebt mogelijk de termen Darknet of Deepnet wel eens horen vallen. Een compleet verborgen internet waar je in een handomdraai aan illegale producten en diensten kunt komen. Of volledig anoniem het net op kunt.

We gaan in dit artikel wat dieper in op deze 'duistere kant' van internet. Zijn alle wilde verhalen rond Darknet (of Deepnet, wat hetzelfde is) fabels? Ja en nee. Ten eerste gebruiken mensen de route via Darknet vooral om gewoon anoniem en nagenoeg ontraceerbaar te surfen op internet. Dat kan door gebruik te maken van bijvoorbeeld het meest bekende 'alternatieve' netwerksysteem: TOR.

TOR staat voor The Onion Router en deze naam is zeer toepasselijk. Wat er gebeurt is dat je na het installeren van een TOR-browser (daarover straks meer) niet meer rechtstreeks vanaf je eigen pc websites bezoekt, maar via een scala aan tussenpersonen. Peer-to-peer heet dat, en tegelijkertijd zorgt versleuteling ervoor dat meelezen nagenoeg tot het verleden behoort.

Denk overigens niet dat je, áls je eenmaal via TOR aan het browsen bent, volledig ontraceerbaar bent. Er zijn complexe trucs te verzinnen om TOR-gebruikers alsnog te achterhalen, maar daarover in een volgend artikel veel meer. Om

het verhaal helemaal compleet te maken: er is meer dan TOR om het 'Darknet' mee te ontsluiten. Zo zijn er FreeNet (*https://freenetproject.org/*), I2P (*https://geti2p.net/en/*) en het nog erg jonge ZeroNet (*https://github.com/HelloZeroNet/ZeroNet*). TOR werkt dankzij het kant-en-klaar-pakket Tor Browser echter verreweg het simpelst.

VERSTOPPERTJE SPELEN

Wat browsen via de Tor Browser precies inhoudt? Voor nu houden we het even bij een simpele omschrijving: browsen via een TOR-browser betekent dat voor de website die je bezoekt, je oorspronkelijke IP-adres (ofwel het 'huisnummer' van je computer dat iedere internetgebruiker via zijn of haar provider krijgt toegewezen) verstopt blijft. Ideaal als je eens een website wilt bezoeken waarvan je niet wilt dat jouw IP-adres gelogd wordt. Denk dan aan iets heel simpels, bijvoorbeeld een collega die een blog bijhoudt over misstanden op het werk. Als je niet wilt dat jij daar als bezoeker op de één of andere manier mee in verband wordt gebracht, dan is TOR een oplossing. Ga je ook nog zelf misstanden aan zo'n blog toevoegen en wil je niet dat de collega of je baas ooit achter je identiteit komt, dan is de TOR-route eveneens een optie.

.ONION

Tot zover is TOR dus eigenlijk vooral een stuk gereedschap om je anoniem over het internet te bewegen. De meeste gebruikers houden het daar ook bij en zijn gelukkig met alleen deze functionaliteit. TOR biedt echter óók toegang tot eigen, specifieke websites met de extensie .onion. En dát is waar het Darknet begint. Deze .onion-sites zijn namelijk zónder TOR-koppeling onbereikbaar. Onbereikbaar voor iedereen die een normale internetverbinding gebruikt, maar ook onbereikbaar voor traditionele zoekmachines als Google & co. Bovendien is het moeilijk (maar ook weer niet helemaal onmogelijk) om de makers van dergelijke .onion-sites te achterhalen.

Op veel van die .onion-sites vind je dan ook zaken die het daglicht eigenlijk niet kunnen verdragen. Dat kan iets 'onschuldigs' zijn als een handleiding voor het hacken van een of ander systeem, maar ook tref je er leveranciers van allerlei smaken harddrugs aan en behoort het bestellen van een huurmoordenaar tot de mogelijkheden.
Wat dat betreft kloppen de 'wilde verhalen' in de media dus wel. Alleen geldt natuurlijk dat niet iedere gebruiker van het TOR-netwerk (of een van de hier links genoemde alternatieven) direct kwade bedoelingen heeft. Als je je TOR-browser alleen maar inzet om anoniem vanuit een hotel-

De basis van het Darknet: vertrouw niks en niemand

kamer of internetcafé te kunnen internetten, ben je niet bepaald met iets 'spannends' of illegaals bezig. Slechts het beschermen van je identiteit en het voorkomen van (al dan niet lokale) meelezers is dan je hoofddoel.

NADELEN

Browsen via TOR heeft ook nadelen. Ten eerste is het een stuk trager dan 'gewoon' browsen. Logisch, want voor de door jou opgevraagde site uiteindelijk bij jou op het scherm verschijnt zijn de gegevens via een complex netwerk van andere computers ('peers') gelopen. Dat kost (veel) tijd, al moet gezegd worden dat het netwerk langzaamaan sneller is geworden omdat er steeds meer deelnemers bij zijn gekomen.
De inhoud van Darknet kan voor gebruikers overigens ook aanstootgevend zijn. Als volwassene kun je er simpelweg voor kiezen om gewoon geen specifieke .onion-sites te bezoeken, maar met bijvoorbeeld kinderen in huis kan de controle moeilijk zijn. Omdat op het verborgen internet als vanzelfsprekend ook lieden met minder edele bedoelingen rondlopen, is het dan ook meer dan ooit oppassen geblazen. Installeer vooral ook een up-to-date virusscanner en download bij voorkeur gewoon niets van .onion-sites. Kijken, maar niet aankomen, is het devies wat ons betreft.

DUIK IN DARKNET

Toegang realiseren tot Darknet is niet echt ingewikkeld, zeker niet als je kiest voor TOR als toegangspoort. Hiervoor zijn bijvoorbeeld browser ▶

add-ons te vinden, maar eigenlijk adviseren we je om deze niet te installeren in je browser voor dagelijks gebruik. Gewoon, om de zaken netjes gescheiden te houden én om te voorkomen dat specifieke add-ons (denk aan Java, Javascript, Flash enzovoorts) tijdens het bezoek van .onion-sites actief zijn. Deze extraatjes barsten vaak van de veiligheidslekken en de kans is levensgroot dat een criminele site direct probeert wat er zoal aan achterdeurtjes beschikbaar is in jouw browser.

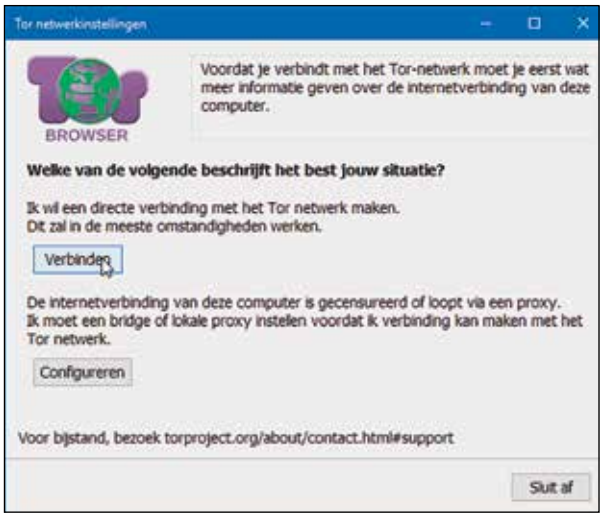
TOR BROWSER

We kiezen in dit artikel dan ook voor Tor Browser (*www.hcc.nl/tor*), leverbaar voor diverse besturingssystemen, waaronder Windows. Zelfs in het Nederlands, dus pik deze versie op van de site en installeer de TOR-browser. Deze laatste is overigens gebaseerd op een streng gelimiteerde (zo ongeveer alle add-ons zijn uitgeschakeld en privacysettings zijn tot het hoogste beschermingsniveau aangepast) versie van Firefox.

Het eerste teken van leven na de start van Tor Browser is een keuzevenster. In vrijwel alle gevallen klik je hierin op de knop *Verbinden*, zeker als het gaat om een thuisnetwerk. Wacht even tot de koppeling gerealiseerd is, waarna wellicht een enigszins teleurgesteld gevoel ontstaat: eigenlijk zie je namelijk een doodgewoon browservenster à la Firefox verschijnen. Wel verschijnt na maximaliseren van het browservenster bovenin een geel balkje met een bijzondere melding. Hier wordt namelijk afgeraden om het browservenster te maximaliseren, omdat de schermresolutie gebruikt kan worden om je alsnog te traceren. Laat de vensergrootte van Tor Browser dus ongewijzigd. Inderdaad: tamelijk paranoïde, maar dat is dan ook precies de basis van het hele Darknet: vertrouw niks en niemand.

WIE BEN IK?

Om te checken of je TOR-netwerkverbinding veilig is, klik je op de homepage van de browser op de link *Test Tor Netwerkinstellingen*. Eventueel kun je hier – voor nog meer veiligheid – kiezen voor een melding in het Engels. Op de geopende pagina zie je – als het goed is – een melding dat de browser geconfigureerd is voor TOR. Tegelijkertijd wordt een IP-adres vermeld: dát is het adres waarmee je websites bezoekt binnen deze



Klik hier in negen van de tien gevallen op Verbinden

TOR-sessie. Dit is niet het IP-adres dat je van je provider hebt gekregen, maar een heel ander. Om dat te bewijzen breng je – met de TOR-browser – een bezoekje aan *http://www.ipligence.com/geolocation*, kwestie van dit adres in de adresbalk intikken. Tijdens onze test kregen we een Frans IP-adres toegewezen, maar dat had net zo goed iets uit de Russische Federatie, Vietnam of IJsland kunnen zijn. Dat kán overigens ook zo z'n nadelen hebben, want als een bezochte website adaptief is en informatie toont in de taal van het land van je IP-adres, is dat niet praktisch. Maar deze kleine ongemakken nemen we voor lief als het gaat om onze privacy.

VERBORGEN BROWSEN

Tot zover eigenlijk weinig nieuws onder de zon qua browsen: alles werkt zoals je normaal gewend bent, zij het iets trager. Het eerste teken van 'verandering' is dat de standaard zoekmachine is ingesteld op DuckDuckGo, een zoekmachine die

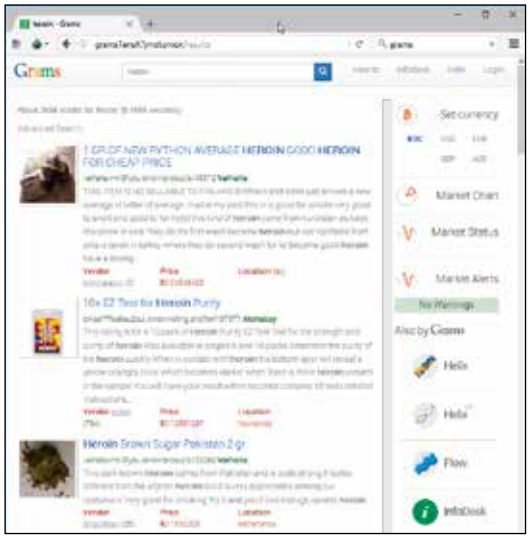
We zijn gekoppeld aan het TOR-netwerk

In deze sessie gaan we als Fransman m/v door het leven

resultaten van andere zoekmachines verzamelt en anonimiseert. Alweer een extra laagje veiligheid dus, maar niets staat je in de weg om gewoon Google te gebruiken. Kwestie van *www.google.nl* in de adresbalk tikken en gaan. In ieder geval geldt dat het, zolang je binnen de TOR-browser actief bent, verdraaid moeilijk zal zijn voor wie dan ook om je oorspronkelijke IP-adres te achterhalen. Onmogelijk is het ook weer niet, maar het vergt flink wat werk, zoals beloofd daarover meer in het aansluitende artikel dat in het volgende nummer van PC-Active verschijnt.

PAAR KILO HEROÏNE ERBIJ?

Dan nu een duik in het échte Darknet. Een prima startpunt is de verborgen zoekmachine Grams, deze bereik je door in het adres van de Onion-browser *http://grams7enufi7jmdl.onion/* te tikken. Dit adres werkt *niet* in een gewone browser!



Voor de liefhebbers, zullen we maar zeggen

Voordat we verder gaan willen we wel even duidelijk stellen dat het níet onze bedoeling is je in dit artikel aan te zetten tot allerlei illegale activiteiten. Alles wat we nu tonen is puur educatief bedoeld, wederom geldt dus: kijken en verder afblijven.

Hoe dan ook, stel je bent ineens dringend op zoek naar wat heroïne om die arme verslaafde die aanbelde een beetje te kunnen helpen. Tik daarvoor simpelweg in het zoekveld 'heroin' en je krijgt ineens toch héél andere zoekresultaten te zien dan wat je normaliter in bijvoorbeeld Google ziet. Enerzijds schokkend, anderzijds kun je dat spul natuurlijk ook gewoon op straat kopen als je de weg weet. Veel van de getoonde links brengen je rechtstreeks in contact met de leveranciers, kies uit grammen of kilogrammen. Veel van deze 'Darkshops' zijn overigens alleen toegankelijk na registratie en dát hebben wij fijn achterwege gelaten. Ook het bestellen van een huurmoordenaar of andere illegale diensten gaan we maar niet uitproberen.

NUTTIG, NOODZAKELIJK ÉN GEVAARLIJK

Feit is dat Darknet (of Deepnet als je het zo wilt noemen) bestaat. En ja, je kunt er de meest bizarre diensten en dingen bestellen. Is er wat dat betreft iets nieuws onder de zon? Ja en nee, want net als met het heroïne-voorbeeld van net, wisten bijvoorbeeld verslaafden en dealers elkaar sowieso wel te vinden, ook voor de komst van Darknet. Tegelijkertijd geldt dat de toegang tot criminaliteit nu wel een heel stuk makkelijker is geworden, net als de toegang tot drugs. Experimenteren was nog nooit zo makkelijk, alleen is het wel jammer dat pubers hierdoor verleid kunnen worden tot het uitproberen van extreem verslavende middelen. Gewoon even wat spulletjes bestellen vanachter je laptop is toch heel wat laagdrempeliger dan 's avonds een ongure achterbuurt doorstruinen om aan je gram te komen.

Het is allemaal dubbel, want tegelijkertijd zorgt datzelfde Darknet (of in ieder geval de basis in de vorm van TOR) ervoor dat activisten en ondergrondse bewegingen in bijvoorbeeld dictatoriale staten min of meer vrij met elkaar kunnen communiceren en censuur kunnen omzeilen. Ook door overheidsinternetfilters is met behulp van het TOR-netwerk (eventueel in combinatie met een VPN-server) wel heen te breken. ■