Dark Market

Van Misha Glenny verscheen eveneens bij uitgeverij Ambo

McMaffia. Misdaad zonder grenzen

Misha Glenny

Dark Market

Cybercriminelen, cyberpolitie en onze veiligheid in een digitale wereld

Vertaald door Rob Hartmans

Ambo|Amsterdam

ISBN 978 90 263 2274 7

Oorspronkelijke titel *DarkMarket. CyberThieves, CyberCops and You*
Oorspronkelijke uitgever The Bodley Head, Londen
Omslagontwerp Studio Jan de Boer
Foto auteur Ralph Glenny

Verspreiding voor België:
Veen Bosch & Keuning uitgevers n.v., Antwerpen

Voor Miljan, Alexandra en Callum

Inhoud

Proloog

crime@21stcentury.com

In de niet-aflatende hang naar gemak en economische groei heeft de mate waarin de mensheid afhankelijk is van netwerksystemen in zeer korte tijd een gevaarlijk peil bereikt: in minder dan twee decennia zijn in de meeste landen grote delen van de zogenoemde 'kritische nationale infrastructuur' (of CNI, Critical National Infrastructure, in nerdjargon) onder controle gekomen van steeds complexere computersystemen.

Computers bepalen een groot deel van ons leven, aangezien ze onze communicatie, onze voertuigen, onze interactie met bedrijven en de staat, ons werk, onze vrije tijd, kortom vrijwel alles reguleren. Tijdens een van de vele cybercrime-processen die ik de afgelopen jaren bijgewoond heb, eiste het Britse Openbaar Ministerie dat een hacker een preventiemaatregel opgelegd zou krijgen, die inhield dat hij na vrijlating uit de gevangenis slechts één uur per week, en onder toezicht van een politiefunctionaris, toegang tot het internet kreeg. 'Tegen de tijd dat mijn cliënt zijn straf heeft uitgezeten,' merkte de advocaat van de beklaagde op, 'is er nauwelijks nog een menselijke activiteit die niet op de een of andere manier via internet verloopt. Hoe wordt mijn cliënt geacht onder dergelijke omstandigheden een normaal leven te leiden?' luidde zijn retorische vraag. Inderdaad, hoe? Mensen die hun mobiele telefoon slechts een paar uur thuis hebben laten liggen bespeuren over het algemeen een intense ergernis en gemis, iets dat lijkt op de cold turkey van een drugsverslaafde. Interessant is echter dat als men drie dagen lang niet over het apparaatje kan beschikken, dit verlammende onrustgevoel plaatsmaakt voor een bevrijdingsroes, aangezien men terugverplaatst wordt naar een wereld die niet zo ver achter ons ligt,

waarin we niet beschikten over mobiele telefoons en ze dus ook niet nodig hadden om ons leven te leiden. Vandaag de dag denken de meeste mensen dat ze zonder deze kleine draagbare computers niet kunnen leven.

De computer is misschien nog het beste te vergelijken met de auto. Toen het vanaf de jaren veertig steeds gewoner werd dat gezinnen over een auto beschikten, begreep nog slechts een minderheid van de automobilisten wat er zich afspeelde onder de motorkap. Niettemin was er nog steeds een flink aantal autobezitters dat zijn auto kon repareren, ongeacht de soort pech die men had. Nog meer mensen konden aan de carburateur rommelen, zodat ze thuis konden komen, en de meesten konden in ieder geval een band verwisselen.

Als het alleen om een lekke band gaat, kun je ook nu je bestemming meestal nog wel bereiken. Een toenemend aantal mankementen is tegenwoordig echter het gevolg van computerfalen in de controlebox: het zwarte plastic omhulsel dat meestal achter de motor zit. Als het inderdaad de controlebox is, zul je zelfs als je een ervaren automonteur bent je auto niet meer aan de praat krijgen. Als je geluk hebt, kan een computermonteur de boel repareren, maar in de meeste gevallen zal de controlebox vervangen moeten worden.

Computersystemen zijn zoveel complexer en kwetsbaarder dan verbrandingsmotoren, dat alleen een uiterst kleine groep mensen meer hulp kan bieden dan de bekende mantra 'Heb je al geprobeerd te rebooten?'

We verkeren in een situatie waarin deze minuscule elite (noem ze nerds, techno's, hackers, codeurs, securocraten of wat je maar wilt) volledig begrijpt hoe de technologie werkt die ons leven elke dag meer en diepgaander beïnvloedt, terwijl de meesten van ons er werkelijk geen bal van snappen. De betekenis hiervan begon pas tot mij door te dringen toen ik onderzoek deed voor mijn vorige boek over wereldwijde georganiseerde misdaad, *McMaffia*. Om de computercriminaliteit te onderzoeken ging ik naar Brazilië, omdat dit fascinerende land naast zijn vele positieve eigenschappen ook een belangrijk centrum is waar veel rottigheid op internet vandaan komt – al was dat op dat moment nog nauwelijks bekend.

Hier ontmoette ik internetdieven die een spectaculair succesvol *phishing*-programma hadden ontworpen. Phishing is nog steeds een van de meest effectieve vormen van internetcriminaliteit. Er zijn twee eenvoudige varianten. Het slachtoffer opent een spam-e-mail. Het at-

tachment kan een virus bevatten dat een computer elders ter wereld in staat stelt alle activiteiten van de besmette computer te volgen, waaronder het invoeren van wachtwoorden voor bankrekeningen. De andere truc bestaat uit het opstellen van een e-mail die verzonden lijkt te zijn door een bank of andere instelling, waarin gevraagd wordt de gebruikersnaam en het wachtwoord te bevestigen. Als de ontvanger erin trapt kan de verzender van de e-mail deze gegevens gebruiken om zich toegang te verschaffen tot een of meer internetaccounts. De Braziliaanse hackers lieten stap voor stap zien hoe ze tientallen miljoenen dollars van bankrekeningen in Brazilië, Spanje, Portugal, Groot-Brittannië en de Verenigde Staten af haalden.

Vervolgens bezocht ik de Braziliaanse internetpolitie, die vier andere leden van deze misdaadorganisatie had gearresteerd (hoewel minstens tweemaal zoveel leden nooit werden opgespoord). Vervolgens interviewde ik het hoofd van X-Force, de afdeling Geheime Operaties van het Amerikaanse computerveiligheidsbedrijf ISS. Binnen een week tijd realiseerde ik me dat de conventionele of traditionele georganiseerde misdaad, hoe kleurrijk en gevarieerd die ook was, voor de daders aanzienlijk riskanter was dan internetcriminaliteit.

Ouderwetse misdaadsyndicaten, gebonden aan de technologie en middelen van de twintigste eeuw, moeten als zij in hun branche succesvol willen zijn, rekening houden met twee ontmoedigende hindernissen. Hun eerste bedrijfsrisico wordt gevormd door de politie. De doeltreffendheid van justitie varieert van tijd tot tijd en van plaats tot plaats. Misdaadorganisaties passen zich aan deze veranderende omstandigheden aan en kiezen voor een van de manieren waarop men kan omgaan met wetshandhavers. Ze kunnen proberen hen te overtreffen in kracht, ze kunnen hen corrumperen, ze kunnen de politici die gezag uitoefenen over de politie corrumperen, of ze kunnen proberen onopgemerkt te blijven.

Vervolgens worden ze geconfronteerd met een tweede probleem: de bedreiging door de concurrentie, door andere schurken die in dezelfde vijver vissen. Ook die kunnen ze proberen in kracht te overtreffen, ze kunnen voorstellen een bondgenootschap te sluiten, of ze kunnen ermee instemmen te worden overgenomen.

In geen van beide gevallen kan de misdaadorganisatie ze eenvoudig negeren – dan loopt het mis, en soms met fatale gevolgen. Cruciaal voor het overleven en het succes is de communicatie met je medecriminelen en met de politie – en uiteraard het versturen van de juiste boodschappen naar beide groepen.

In Brazilië kwam ik er snel achter dat de eenentwintigste-eeuwse criminaliteit anders is. Het belangrijkste is dat het veel moeilijker is om erachter te komen wanneer mensen op het internet van plan zijn rottigheid uit te halen. De wetgeving die het internetverkeer moet reguleren verschilt van land tot land. Dit maakt veel uit, omdat internetcriminaliteit over het algemeen wordt gepleegd vanaf een IP-adres (IP =Internet Protocol) in het ene land en gericht is tegen een persoon of onderneming in een tweede land, waarna het resultaat wordt geboekt (of uitbetaald) in een derde land. Een politiefunctionaris in Colombia kan er bijvoorbeeld achter komen dat het IP-adres vanwaar een aanval op een Colombiaanse bank is ondernomen afkomstig is uit Kazachstan. Maar dan ontdekt hij dat dit in Kazachstan niet als misdaad wordt beschouwd en dat zijn collega in de Kazachstaanse hoofdstad geen reden heeft om onderzoek te doen naar het misdrijf.

Veel internetcriminelen beschikken over de kennis om dergelijke discrepanties te ontdekken en te benutten. 'Ik gebruik nooit Amerikaanse creditcards of bankpassen,' vertelde een van de succesvolste Zweedse *carders* (creditcardfraudeurs) me, 'omdat ik hierdoor onder de jurisdictie van de Verenigde Staten zou vallen, waar ik ook verblijf op deze planeet. Daarom houd ik het gewoon bij Europese en Canadese kaarten en daar voel ik me goed en veilig bij – zij zullen me nooit te pakken krijgen.'

De waterscheiding tussen aan de ene kant de Verenigde Staten en aan de andere kant Canada en Europa is belangrijk, omdat dit de gebieden zijn waar de meeste slachtoffers van internetcriminaliteit wonen. De laatstgenoemde streken kennen veel strengere wetten waar het gaat om de bescherming van individuele vrijheden en rechten op het internet. Achtereenvolgende Amerikaanse regeringen hebben justitie grotere bevoegdheden gegeven dan Europese overheden zelfs maar in overweging zouden willen nemen, waardoor de politie in naam van de strijd tegen misdaad en terrorisme gemakkelijker toegang heeft tot gegevens die afkomstig zijn van particuliere ondernemingen.

De gevolgen hiervan zijn even diepgaand als ondoorgrondelijk. Zorgen over criminaliteit, toezicht, privacy, de accumulatie van informatie door zowel particuliere als overheidsinstanties, de vrijheid van meningsuiting (denk aan WikiLeaks), de toegankelijkheid van websites (het debat over de zogenaamde internetneutraliteit), de politieke bruikbaarheid van sociale netwerken, en nationale veiligheid botsen in cyberspace voortdurend op elkaar.

Men zou bijvoorbeeld kunnen stellen dat de alomtegenwoordigheid en de vele diensten van Google indruisen tegen de Amerikaanse anti-trustwetgeving en dat de opeenhoping van al die persoonlijke gegevens zowel een veiligheidsrisico als een kans voor criminelen betekent. Toch zou Google kunnen tegenwerpen dat de kern van zijn karakter en succes gelegen is in het feit dat het op verschillende gebieden met verschillende diensten aanwezig is en dat dit juist de strategische belangen van Amerika bevordert. Als zij dat wil kan de Amerikaanse overheid met juridische procedures binnen enkele uren toegang krijgen tot de data van Google. En omdat deze onderneming haar informatie in de gehele wereld verzamelt, hebben de Verenigde Staten hierdoor een immens strategisch voordeel. Andere regeringen mochten willen dat ze zoveel geluk hadden. Anders dan regeringen in China, Rusland of het Midden-Oosten hoeft de Amerikaanse overheid Google niet te hacken om achter zijn geheimen te komen. Zij kan een gerechtelijk bevel vragen. Zou je dat, in het kader van de anti-trustwetgeving, allemaal willen opgeven?

Het internet is één verzameling zeepbellen – als je één probleem oplost, doemt onmiddellijk elders een ander, ogenschijnlijk onhandelbaar probleem op.

En het grootste probleem voor alle wetshandhaving is de anonimiteit. Tot op heden is het voor iedereen die over de benodigde kennis beschikt mogelijk het internet op te gaan en de fysieke locatie van een computer te maskeren.

Er zijn twee manieren om dat te doen. De eerste *cyberwall* is het Virtual Private Network ofwel VPN, waardoor een verzameling computers hetzelfde IP-adres kan delen. Over het algemeen verwijst het IP-adres naar één apparaat, maar met een VPN kan het bijvoorbeeld zo lijken dat verschillende computers in verschillende delen van de wereld zich allemaal in Botswana bevinden.

Voor degenen die een VPN onvoldoende bescherming vinden bieden, kan er een tweede cyberwall worden gebouwd door middel van zogenaamde proxyservers. Een computer die zich op de Seychellen bevindt, kan gebruikmaken van een *proxy* (= gevolmachtigde) in, laten we zeggen, China of Guatemala. De proxy laat niet merken dat het oorspronkelijke IP-adres uitzendt vanaf de Seychellen of dat de computer onderdeel is van een op Groenland gestationeerd VPN.

Het opzetten van dergelijke netwerken vereist een hoge mate van vaardigheid en zodoende worden deze technieken over het algemeen