HIGH TECH CRIME

Criminaliteitsbeeldanalyse 2012

«waakzaam en dienstbaar»

POLITIE

High Tech Crime

Criminaliteitsbeeldanalyse 2012

« waakzaam en dienstbaar »

POLITIE
Korps landelijke politiediensten

Uitgave

Korps landelijke politiediensten (KLPD)
Dienst Nationale Recherche
Postbus 11
3970 AA Driebergen

Woerden, maart 2012

Auteurs

Frank Bernaards LL.M.
Eileen Monsma Msc.
Peter Zinn Msc.

Colofon

Vormgeving OSAGE / communicatie en ontwerp, Utrecht
Druk Thieme MediaCenter, Rotterdam

Inhoud

Voorwoord

Voor u ligt de criminaliteitsbeeldanalyse (CBA) high tech crime (HTC) 2012. Een document waarin een dynamisch en almaar groeiend aandachtsgebied en de ontwikkeling daarvan beschreven wordt. Een aandachtsgebied dat zichzelf steeds meer in het nieuws manifesteert en maatschappelijke aandacht vraagt. De uitdagingen voor de politie worden daarmee relevanter en intensiever en het belang van informatiedeling wordt steeds groter. In deze CBA wordt getracht op een gestructureerde manier overzicht te bieden van de relevante informatie ten aanzien van high tech crime en de daarmee samenhangende uitdagingen voor de politie.

De CBA 2012 is een document met verscheidene opdrachtgevers. In eerste instantie is het geschreven in opdracht van het Landelijk Parket (LP) van het Openbaar Ministerie (OM). Het moet de komende periode dienen als leidraad voor het nemen van de juiste beslissingen in de aanpak van high tech crime. Daarnaast moet de CBA input geven voor het Nationaal Dreigingsbeeld (NDB) 2012 ten behoeve van de strategische aanpak van criminaliteit in de komende jaren.

Deze CBA is overigens niet de enige publicatie van de overheid die de ontwikkelingen en trends op dit aandachtsgebied in beeld brengt. Zo werkt de politie, specifiek het Team High Tech Crime (THTC), nauw samen met het Nationaal Cyber Security Centrum (NCSC) en levert het ondersteuning bij het opstellen van het Cybersecuritybeeld Nederland. Elementen uit deze documenten zullen daarom ook terugkomen in deze CBA.

Steeds meer publieke en private partijen hebben de afgelopen periode trendanalyses gepubliceerd. Het THTC heeft bijvoorbeeld bijgedragen aan het Data Breach Investigations Report dat jaarlijks uitgebracht wordt door Verizon. Het verschil tussen de CBA en andere relevante publicaties is gelegen in het perspectief. In deze CBA wordt met een politiebril gekeken naar de ontwikkelingen op het gebied van specifiek high tech crime. Waar de meeste partijen primair geïnteresseerd zijn in beveiliging tegen dergelijke criminaliteit, is de politie de enige partij met een primaire interesse in de daders achter deze aanvallen. Om die reden wordt er in de CBA relatief meer aandacht besteed aan het analyseren van criminele ketens, daderprofielen en criminogene factoren.

1
Introductie

De snelheid waarmee informatie- en communicatietechnologie (ICT) verweven raakt met het dagelijkse leven blijft toenemen. Het internet biedt bijna onbegrensde mogelijkheden voor communicatie en het aanbieden en afnemen van diensten en producten. Maatschappelijke en economische processen zijn inmiddels in sterke mate afhankelijk geworden van de infrastructuren die ICT heeft voortgebracht.

Enkele cijfers die deze afhankelijkheid illustreren: Anno 2011 heeft 91 procent van de Nederlanders een (breedband) internetverbinding[1], zo'n 10 miljoen Nederlanders regelen hun bankzaken via het internet[2], en 77 procent van de Nederlanders die op internet actief zijn, doet wel eens aankopen online[3]. Hierbij werd in 2010 8,2 miljard euro omgezet[4]. Inmiddels beschikt twee op de vijf Nederlanders ook over mobiel internet[5]. In 2011 gaf 39 procent van de Nederlandse bedrijven aan dat hun bedrijf volledig stil staat zonder ICT[6]. Slechts 1 procent van diezelfde bedrijven geeft aan volledig onafhankelijk van ICT te opereren. Al deze cijfers zijn de afgelopen jaren gestegen en te verwachten is dat ze dat ook de komende jaren zullen doen.

Zowel hardware als software is niet immuun voor misbruik. Ontwikkelingen in de techniek worden mede daarom onmiddellijk gevolgd door hierop gebaseerde ontwikkelingen in de criminaliteit. Hoewel accurate cijfers ontbreken, kan geconstateerd worden dat criminele winst voor daders en schade voor slachtoffers zoals burgers, de private sector en de overheid aanzienlijk is.

De bestrijding van criminaliteit op of via ICT (opsporing, bewijsvoering, tegenhoudmaatregelen) is behoorlijk complex. De urgentie om de veiligheid en openheid van het internet te waarborgen is hoog. De huidige regering heeft dat onderkend en in 2011 een Nationale Cyber Security Strategie (NCSS) geformuleerd. Daarin is onder meer besloten tot de volgende versterkingen:

---

1 CBS - ICT, kennis en economie 2011, p. 13.
2 CBS - ICT, kennis en economie 2011, p. 8.
3 CBS - ICT, kennis en economie 2011, p. 8.
4 Thuiswinkel marktmonitor (TMM) 2011, De Nederlandse thuiswinkelmarkt 2005-2011, Thuiswinkel.org (2011).
5 OPTA - Marktcijfers tweede kwartaal 2011.
6 Ernst & Young - ICT barometer over cybercrime, p. 3.

- De oprichting van het Nationaal Cyber Security Centrum (NCSC). Daarbinnen brengen publieke en private partijen, op basis van hun eigen taken en binnen de wettelijke mogelijkheden, informatie, kennis en expertise bij elkaar. Zo kan inzicht verkregen worden in ontwikkelingen, dreigingen en trends en kan ondersteuning worden geboden bij incident-afhandeling en crisisbesluitvorming. Ook de politie, specifiek het THTC, is hierin vertegenwoordigd;
- Intensivering van de opsporing en vervolging van cybercrime. Het doel hiervan is om de aangiftebereidheid en de pakkans te doen stijgen en overtreders steviger aan te pakken. In de NCSS is aangegeven dat de politie een verschuiving moet realiseren binnen het huidige budgettaire kader om tussen 2011 en 2014 zo'n 500 cyberspecialisten meer in te kunnen zetten. Daarmee moet vanaf 2014 voldoende capaciteit zijn om 20 grote high tech crime onderzoeken per jaar uit te kunnen voeren bij het THTC. Om dat te kunnen bewerkstelligen moet het THTC groeien van 30 medewerkers naar 119 medewerkers. Daarnaast moeten er meer digitaal experts en cybercrime specialisten bij de verschillende politieregio's worden aangenomen voor de aanpak van veelvoorkomende/high volume cybercrime die het vertrouwen in ICT van burgers en het bedrijfsleven aantasten.

1.1 Definities en criteria

Het is haast niet mogelijk om cybercrime als één apart crimineel verschijnsel te onderscheiden, omdat veel vormen van criminaliteit tegenwoordig in meer of mindere mate met ICT verweven zijn. De verschijningsvormen zijn zeer divers, evenals de mate waarin het gebruik van ICT een rol speelt. Nationaal en internationaal bestaan verschillen in definities van gebruikte terminologie. Dit maakt het noodzakelijk om te bepalen wat binnen de context van deze publicatie met de verschillende termen bedoeld wordt en wat de focus van de CBA HTC is. De gebruikte definities worden gedragen door de politie, het Openbaar Ministerie en het Nationaal Cyber Security Centrum (NCSC).

1.1.1 Cyber security

Cyber security is het overkoepelende begrip voor beveiliging van informatie, systemen en netwerken. De dreigingen op dat gebied worden in het algemeen onder een van de volgende deelgebieden geschaard: cybercrime, cyberactivisme, cyberspionage, cyberterrorisme en cyberconflict/-warfare. De politie heeft daarbij primair een verantwoordelijkheid op het gebied van cybercrime. Bepaalde (strafbare) gedragingen binnen cyberactivisme en cyberspionage

zouden ook onder cybercrime geschaard kunnen worden. Signalering en bestrijding van cyberterrorisme is in beginsel geen politie-aangelegenheid. Partijen als de AIVD en MIVD zijn hiermee belast. Cyberconflict/-warfare is een (relatief nieuw) onderdeel van het diplomatieke arsenaal van een staat. Naast water, land, lucht en ruimte vormt cyber een nieuw domein voor staten. Dit deelgebied is voornamelijk een defensie-aangelegenheid. Alleen incidenten en dreigingen waar de politie en specifiek THTC bij betrokken is (geweest) worden in deze CBA beschreven. Om die reden blijven een aantal deelgebieden in deze publicatie onderbelicht.

1.1.2 Cybercrime

Het KLPD hanteert de volgende definitie van cybercrime:
Cybercrime omvat elke strafbare gedraging voor de uitvoering waarvan het gebruik van geautomatiseerde werken bij de verwerking en overdracht van gegevens van overwegende betekenis is.

In lijn met relevante wetgeving wordt de techniekneutrale term 'geautomatiseerde werken' gebruikt. Daaronder worden alle inrichtingen verstaan die bestemd zijn om langs elektronische weg gegevens op te slaan, te verwerken en over te dragen. Hier vallen niet alleen computers onder, maar bijvoorbeeld ook mobiele telefoons.

Dergelijke geautomatiseerde werken hoeven niet per definitie het doelwit van de criminaliteit zijn. Het kan ook gaan om ICT als plaats van of als hulpmiddel bij het delict. Vanwege de digitalisering van de maatschappij is er vaak sprake van digitalisering van diverse vormen van traditionele criminaliteit. Voorbeelden hiervan zijn grooming (het lokken van kinderen via chatsites), het publiceren van dreigtweets, cyberstalking, cyberoplichting, de online verkoop van geneesmiddelen, het gebruik van forums voor handel in grondstoffen voor drugs, het aanbieden van poker-websites en het uploaden van auteursrechtelijk beschermd materiaal zoals video's, muziek en software.

Daarnaast zijn er vormen van cybercrime waarbij geautomatiseerde werken naast middel ook doelwit zijn. In veel gevallen is er dan sprake van opzettelijk en wederrechtelijk binnendringen in geautomatiseerde werken (hacken, of in juridische termen: 'computervredebreuk'). Voorbeelden hiervan zijn skimmen en defacements (inbraak op een webserver om bestaande webpagina's te vervangen door andere).

1.1.3 High tech crime

Hoewel het onderscheid in de praktijk niet altijd even strikt te maken is, richt het THTC zich op bestrijding van een specifieke subcategorie van cybercrime: high tech crime. Onder high tech crime worden bijzondere vormen van cybercrime verstaan, die voldoen aan een aantal of alle van onderstaande kenmerken:

- ICT als doelwit, en;
- Innovatie (gebruik van relatief nieuwe, geavanceerde technieken en middelen), en;
- Ondermijning (functioneren van de Nederlandse staat of samenleving is in het geding), en/of;
- High impact (in termen van financieel-economische schade, inbreuk op de continuïteit van bedrijfsvoering en/of op het vertrouwen van burgers of consumenten).

Figuur 1.1

De vingerafdruk van high tech crime

Georganiseerde misdaad met een innovatief karakter
Bij doelwitten van high tech crime zijn vaak complexe ICT-systemen en -netwerken betrokken. Aangezien deze bovengemiddeld beveiligd (zouden moeten) zijn, gaat het in veel gevallen om gerichte aanvallen die hoge eisen stellen aan de organisatievorm en werkwijze van de daders. Het THTC richt zich op vormen van cybercrime die in georganiseerd verband plaatsvinden en waarbij relatief nieuwe, geavanceerde technieken en middelen toegepast worden.

Ondermijning en high impact
Bij high tech crime ligt de focus op vitale belangen. Dat betekent dat deze vorm van misdaad een (potentieel) ontwrichtend effect heeft op de nationale veiligheid, economische veiligheid en/of volksgezondheid zodat het functioneren van de Nederlandse staat of (delen van) de samenleving in het geding is. Bijvoorbeeld cybercrime die gericht is tegen de sectorale ordening of vitale knooppunten van virtuele en/of fysieke infrastructuren. Meestal zijn dit incidenten van internationale of mondiale orde en heeft het veel impact in termen van financieel-economische schade, inbreuk op de continuïteit van bedrijfsvoering en/of op het vertrouwen van burgers of consumenten.

Vereiste aanpak
Kenmerkend voor high tech crime is ook dat voor de aanpak een hoog niveau van recherche expertise in complexe digitale omgevingen gevraagd is. Daarnaast is in veel gevallen direct handelen op (inter)nationaal niveau noodzakelijk om bedreigende situaties te voorkomen danwel te doen stoppen, of om bewijs te verkrijgen.

Figuur 1.2

Verhouding tussen cyber security/cybercrime/high tech crime

Bovengenoemde kenmerken illustreren de unieke positie van high tech crime binnen het bredere criminaliteitsveld cybercrime. Ondanks dat andere vormen van cybercrime buiten de scope van het THTC en deze CBA vallen is het wel degelijk relevant. Vooral geaggregeerd vormt veelvoorkomende/high volume cybercrime een zeer grote schadepost voor de maatschappij. Bovendien is het onderscheid niet in alle gevallen duidelijk te maken. Zo wordt skimmen meestal niet als high tech crime aangemerkt, maar werden specifieke geavanceerde aanvallen op de EMV chipkaart daar de afgelopen periode wel onder geschaard. Gebruik van botnets wordt daarentegen vrijwel altijd als high tech crime aangemerkt, hoewel sommige tools voor ontwikkeling en gebruik tegenwoordig voor iedere leek toegankelijk zijn en op grote schaal toegepast worden. In het algemeen geldt dat high tech crime het topje van de ijsberg is en dat het THTC op het scherpst van de snede van de ontwikkelingen probeert te opereren.

1.2 Onderzoeksopzet

Binnen de politie in Nederland worden high tech crime onderzoeken uitsluitend door het THTC uitgevoerd en deze CBA is dan ook voornamelijk gebaseerd op diens dossiers. Hierbij dient opgemerkt te worden dat op andere plaatsen binnen de politie wel degelijk opsporingsonderzoek naar (andere) vormen van

cybercrime plaatsvindt. Die dossiers vallen echter buiten de scope van deze CBA. In de voorgaande paragraaf werd beschreven dat dit ook geldt voor andere deelgebieden van cyber security.

De politie is niet de enige partij die zich bezig houdt met high tech crime. Naast eigen dossiers zijn daarom ook uiteenlopende bronnen met informatie van diverse publieke en private partners geraadpleegd. Wetenschappelijk onderzoek en publicaties vanuit de security industrie zijn vooral gericht op technische malware analyses en bijbehorende statistieken. Deze cijfers worden hier en daar onder voorbehoud gebruikt, vooral om een kwantitatieve indicatie te geven van trendontwikkelingen. In deze CBA wordt het aandachtsgebied echter meer vanuit criminologisch perspectief benaderd. Effectieve bestrijding vereist kennis over ontwikkelingen in de aard van het criminele verschijnsel en de personen en criminele samenwerkingsverbanden die van betrokkenheid bij de criminaliteit worden verdacht. Hier wordt door andere partijen niet of nauwelijks aandacht aan besteed en de beperkt beschikbare informatie is voornamelijk kwalitatief van aard.

Aangezien high tech crime een internationale vorm van criminaliteit is, dient er ook op die manier naar gekeken te worden. Daarom wordt er in deze CBA ook aandacht besteed aan dossiers van buitenlandse (politie)partners. Deze CBA richt zich daarbij vooral op de internationale trends die relevant zijn voor Nederland. Het kan daarbij gaan om een (indirecte) dreiging op Nederlandse daders, slachtoffers of infrastructuur.

De gekozen onderzoeksperiode is 2009 tot en met 2011. Om tot een zo actueel mogelijke CBA te komen, is gepoogd om ook de (aller)laatste ontwikkelingen binnen het aandachtsgebied mee te nemen.

1.2.1 Onderzoeksvragen NDB

Om input te verkrijgen voor het Nationaal Dreigingsbeeld (NDB) 2012 zijn er door het KLPD een aantal onderzoeksvragen geformuleerd. Vanwege de leesbaarheid zullen de onderstaande onderzoeksvragen verspreid over verschillende hoofdstukken van deze CBA aan de orde komen.

1. Hoe heeft de aard van het criminele verschijnsel zich ontwikkeld voor wat betreft de wijze waarop die criminaliteit wordt gepleegd?
Voor de beantwoording van deze onderzoeksvraag worden in *hoofdstuk 3* de belangrijkste technieken en middelen voor het plegen van high tech crime beschreven. Deze basiselementen worden op uiteenlopende manieren ten

behoeve van uiteenlopende doeleinden ingezet. In *hoofdstuk 4* wordt vervolgens meer context gegeven door een aantal verschijningsvormen te beschrijven die als actuele dreigingen worden beschouwd. In beide hoofdstukken zal ook aandacht geschonken worden aan opvallende verschuivingen die de afgelopen periode hebben plaatsgevonden.

2. Hoe heeft de omvang van het criminele verschijnsel zich ontwikkeld in termen van hoeveelheid (frequentie, incidentie, prevalentie, schaalgrootte) van activiteit?
In *hoofdstuk 6* wordt getracht deze onderzoeksvraag te beantwoorden. Accurate en vergelijkbare kwantitatieve data met betrekking tot het aandachtsgebied zijn echter bijzonder schaars. Aan de hand van een aantal indicatoren voor hoeveelheid van activiteit zal toch enigszins een beeld geschetst worden van ontwikkelingen in de omvang van high tech crime.

3. Hoe heeft de aard van het criminele verschijnsel zich ontwikkeld voor wat betreft de kenmerken van personen respectievelijk criminele samenwerkingsverbanden die van (betrokkenheid bij) het plegen daarvan worden verdacht?
Deze onderzoeksvraag wordt expliciet beantwoord in *hoofdstuk 5*. Daarbij zal zowel aandacht besteed worden aan dadergroepen en criminele samenwerkingsverbanden die zich al langer met high tech crime bezighielden als aan kenmerken van actoren die zich recent prominenter op het speelveld gemeld hebben.

4. Wat zijn de gevolgen voor de Nederlandse samenleving van het criminele verschijnsel?
In *hoofdstuk 4* wordt vanuit een kwalitatieve benadering een indruk gegeven van de (mogelijke) gevolgen van high tech crime. In aanvulling daarop komen in *hoofdstuk 6*, waar mogelijk,gevolgen in termen van kwantiteit aan bod. Bijvoorbeeld door een indicatie te geven van financiële schade voor de Nederlandse samenleving.

5. Wat is de (logistieke) rol van Nederland op de (Noord/West)Europese markt van het betreffende criminele verschijnsel?
In de voorgaande CBA's werd de rol van Nederland al uitgebreid belicht en bleek dat er een infrastructuur aanwezig is die aantrekkelijk is voor high tech crime. Dit beeld wordt in de beschrijving van de verschillende deelonderwerpen in deze CBA wederom bevestigd. In *hoofdstuk 5 (paragraaf 5.3.1)* wordt specifiek de faciliterende rol van Nederlandse hosting providers uitgelicht.

6. Welke criminaliteitsrelevante factoren zijn, in welke mate en op wat voor wijze, van betekenis voor c.q. van invloed op het criminele verschijnsel?

Ontwikkelingen in technologie worden beschouwd als de belangrijkste aanjager voor ontwikkelingen in high tech crime. In *hoofdstuk 2* wordt daar een beknopt overzicht van gegeven. Ook maatschappelijke veranderingen in de manier waarop burgers, private organisaties en de overheid omgaan met ICT zijn van invloed op het criminele verschijnsel. Deze veranderingen worden in de gehele CBA omschreven.

7. Wat zijn de verwachtingen over omvang, toegepaste werkwijzen, betrokken criminele samenwerkingsverbanden en maatschappelijke gevolgen van het criminele verschijnsel in de komende jaren?

Middels een terugblik op de ontwikkelingen gedurende de afgelopen jaren, en in samenhang met de antwoorden op de eerdere onderzoeksvragen, worden in *hoofdstuk 8* voorspellingen gedaan voor de ontwikkeling van het criminele verschijnsel in de komende jaren. Daarbij is altijd voorzichtigheid geboden, want motieven zijn veranderlijk en het aandachtsgebied is voortdurend in beweging. Toch zijn er enkele duidelijk trends te voorspellen, die in de toekomst speciale aandacht verdienen.

2
Techologisch landschap

2.1 Inleiding

Het voortdurend op de markt brengen van nieuwe technologie ('technology push') zorgt ervoor dat er voortdurend nieuwe aanvalsvectoren voor criminelen ontstaan. Om deze aanvalsvectoren in volgende hoofdstukken goed te kunnen beschrijven wordt in dit hoofdstuk ingegaan op een aantal van de technologieën die eraan ten grondslag liggen.

In dit hoofdstuk worden belangrijke elementen uit het cyberlandschap beschreven, zonder al te diep in te gaan op de criminele mogelijkheden. Wel worden, waar van toepassing, risico's aangestipt. Bij de keuze van de opgenomen technologieën is de voorkeur gegeven aan die technologieën waarvan we verwachten dat ze in de nabije toekomst misbruikt zullen (blijven) worden door high tech criminelen.

2.2 Versleuteling

Versleutelingstechnieken spelen een belangrijke rol bij het garanderen van integriteit van vertrouwelijkheid van waardevolle gegevens en communicatie. Deze technieken verouderen echter snel. De groeiende rekenkracht van computers en de toegenomen mogelijkheid om grote aantallen computers massaal parallel in te zetten maakt het vandaag mogelijk om de versleuteling van gisteren door te rekenen. Daarnaast bevatten alle versleutelingstechnieken onvolkomenheden. Deze worden meestal gevonden door onderzoekers (dezelfde onderzoekers die ook de nieuwe versleutelingstechnieken bedenken). Vervolgens worden ze door aanvallers misbruikt. De versleuteling zal daarom van tijd tot tijd vernieuwd moeten worden. Zowel in de vorm van nieuwe technieken (te vergelijken met een nieuw type slot op de deur) als in de vorm van langere sleutels, die met de huidige rekenkracht nog niet door te rekenen zijn.

De inzet van betere technieken wordt uit kostenoverwegingen geregeld uitgesteld. Denk hierbij bijvoorbeeld aan de OV-Chipkaart met de gekraakte MiFare chip, of aan het breken van de GSM-encryptie, wat het mogelijk maakt om realtime mee te luisteren of zelfs namens anderen betalingen te doen. Daar staat tegenover dat criminelen vaak wel gebruik maken van de nieuwste technieken en hun data-(verkeer) daarmee verborgen weten te houden (voor de politie).

2.3 Infrastructuur

Hoewel het internet als geheel niet echt beheerd wordt zijn er toch een aantal partijen betrokken bij het in stand houden en reguleren van het net. Dit zijn vrijwel allemaal private instellingen. Denk bijvoorbeeld aan Internet Service Providers (partijen als XS4ALL) en hosting providers (b.v. Leaseweb). Dit zijn de knooppunten in het net die sites hosten en particulieren en bedrijven verbinden met het internet. Daarnaast zijn er de grote knooppunten zoals de AMS-IX (Amsterdam Internet Exchange), die voor het routeren van het internetverkeer van cruciaal belang zijn.

Regulering hoort thuis bij partijen als ICANN, RIPE-NCC en SIDN. Dit is waar het technische landschap vloeiend overloopt in een politiek en juridisch landschap. ICANN staat voor de International Cooperation for Assigned Names and Numbers en heeft als het ware een top-coördinatiefunctie over het internet, waaronder met betrekking tot de uitgifte van internet address space, regulatie van de top-level domain name systemen (DNS) en root server systemen en de ontwikkeling van basis internet-protocollen. ICANN maakt hierbij gebruik van vijf decentrale Regional Internet Registries (RIR's), die de registratie en toewijzing van IP-blokken en Autonomous System Numbers verzorgen aan bijvoorbeeld Internet Providers. RIPE NCC is de RIR voor Europa, het Midden-Oosten en delen van Centraal Azië. SIDN staat voor Stichting Internet Domeinnaam Registratie. Zij beheert de uitgifte van de .nl-domeinnamen.

Om online criminaliteit effectief te kunnen bestrijden is een nauwe samenwerking met deze partijen van belang. De afgelopen jaren zijn hierin zichtbare stappen genomen. Van oudsher hebben dergelijke organisaties een membership structuur met een lobby-model en zijn ze overheidsbemoeienis niet gewend en er vaak ook niet van gediend. Het bijsturen van het beleid van deze organisaties vergt daarom vaak jaren. Tegelijkertijd wordt afgetast waar de grenzen liggen van wat de politie kan vragen en deze partijen kunnen bieden. Zo is RIPE NCC in het kader van een rechtshulpverzoek door het OM gesommeerd om IP ranges te bevriezen. RIPE NCC heeft dit gedaan en vervolgens een proefproces aangespannen om uit te vinden of er voldoende wettelijke grondslag was voor het vervaardigen van dat bevel. Dit moet op den duur jurisprudentie opleveren zodat alle partijen weten waar ze aan toe zijn.

Het THTC vraagt tezamen met verscheidene buitenlandse high tech crime units ondertussen aan ICANN om een duidelijker 'due diligence' beleid op te zetten, waarbij Domain Name Registrars de verplichting hebben om de identiteit van hun klanten te controleren. Dit moet de kwaliteit van de whois data sterk verbeteren.

2.4 Domain Name System (DNS)

Het Domain Name System (DNS), is een systeem dat het mogelijk maakt om IP-adressen te koppelen aan domeinnamen. De huidige DNS implementatie stamt uit 1983, kort na de uitrol van het TCP/ IP protocol. De werking van DNS kan vergeleken worden met de werking van een telefoonboek in de analoge wereld. Wie op zoek is naar een telefoonnummer, kan in een telefoonboek de achternaam opzoeken van de persoon die hij wil bellen. Vervolgens wordt dan naast de getoonde naam het bijbehorende telefoonnummer gegeven. DNS werkt op gelijksoortige wijze. Iemand die in een webbrowser de domeinnaam www.politie.nl intikt, wordt met behulp van DNS geleid naar de bij het domeinnaam horende IP-adres. Dit is belangrijk omdat de domeinnamen die dagelijks gebruikt worden, omgezet moeten worden naar IP-adressen voordat een verbinding gemaakt kan worden met de computer waar informatie vanaf gehaald gaat worden. Er zijn diverse aanvallen mogelijk op of via het DNS systeem. Zo kunnen high tech criminelen door het besmetten van een DNS-server grote aantallen computers naar de door hen gewenste websites sturen.[7]

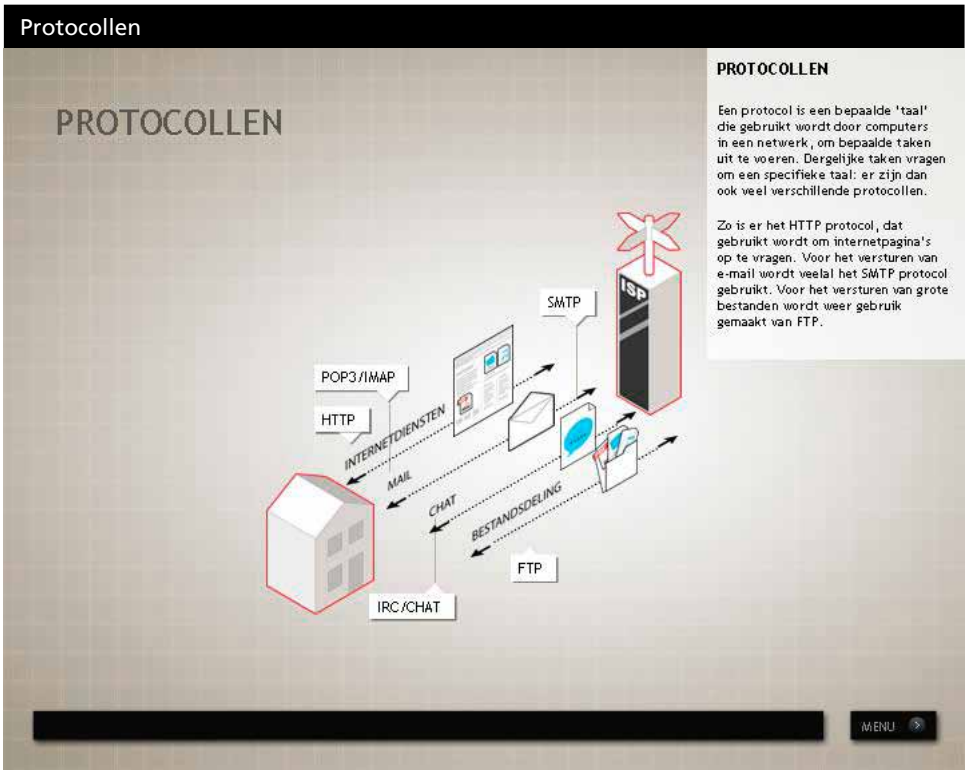
2.5 IPv6

IP staat voor Internet Protocol. Middels dit protocol zijn computers op internet bereikbaar en kunnen zij met elkaar communiceren. IPv4 is de huidige versie van dit protocol. Het biedt ruimte aan zo'n 4,3 miljard IP-adressen. Al in de jaren negentig werd duidelijk dat het aantal IP-adressen dat kon worden uitgegeven op een gegeven moment ontoereikend zou zijn, en werd begonnen aan een opvolger, IPv6 (de 5 was al vergeven aan een ander protocol). IPv6 biedt een vrijwel oneindig aantal adressen (21^{28} of ongeveer 3,4 x 10^{38}) en voert daarnaast een aantal verbeteringen door ten opzichte van IPv4.

---

[7] Zie bijvoorbeeld paragraaf 3.5.5.

Figuur 2.1



De brede invoering van IPv6 heeft echter lang op zich laten wachten. De oorspronkelijke raming was dat het protocol in 1996 zou worden ingevoerd. Echter werden er zelfs in 2011 nog steeds (de laatste) IPv4-blokken vergeven. Dat de IPv4-adressen nu feitelijk op zijn, betekent niet dat de overstap naar IPv6 volledig gemaakt is. Verwacht wordt dat IPv4 nog decennia meegaat terwijl de wereld gradueel overstapt op IPv6. Van alle netwerken in Nederland ondersteunt ongeveer 42% naast IPv4 ook IPv6 (2012). Dit percentage is vrij hoog in vergelijking met de andere landen in Europa (gemiddeld 18%).[8]

[8] Zie RIPE NCC via http://v6asns.ripe.net/v/6.

2.6 Certificaten

Een certificaat is een computerbestand dat beschouwd kan worden als het 'digitaal paspoort' van de eigenaar van dat bestand. Een certificaat heeft twee doelen. Ten eerste kan een website zijn berichten digitaal ondertekenen en hiermee zijn identiteit bewijzen. Ten tweede kan het berichtenverkeer tussen de bezoeker en de website versleuteld worden, waardoor er bescherming tegen meelezen ontstaat. Het certificaat bestaat uit 2 sleutels: een geheime privé-sleutel (die in het bezit is van de website) en een publieke sleutel (die algemeen bekend is). Gegevens die met de privé-sleutel zijn versleuteld, kunnen alleen met de publieke sleutel ontcijferd worden en vice versa.

Als een website zijn digitale handtekening zet met zijn privé-sleutel, dan kan de cliënt dit ontcijferen met de publieke sleutel. Omdat de website de enige is die de privé-sleutel kent, weet de bezoeker dus zeker dat dit de website is waar het om gaat. Andersom kan een bezoeker een bericht sturen naar de website, bijvoorbeeld met creditcard gegevens, die dan versleuteld wordt met de publieke sleutel. Alleen de website kan dit vervolgens met zijn privé-sleutel ontcijferen. Op deze manier kan niemand het bericht afluisteren.

Certificaten worden dus onder meer gebruikt om een beveiligde verbinding tussen een website en een bezoeker op te zetten. Zo'n verbinding heet een SSL (Secure Socket Layer)-verbinding en is herkenbaar aan het adres in de adresbalk. Dat begint met https in plaats van http. Daarnaast is er in de browser een slotje zichtbaar.

Certificaten worden uitgegeven door Certificate Authorities (CA's). Wereldwijd zijn er daar ongeveer 600 van. De CA's zijn vertrouwde derde partijen die instaan voor de validiteit van de certificaten en dus voor de identiteit van de websites. Als een van deze partijen zegt dat een bepaald certificaat klopt, dan nemen alle internetgebruikers ter wereld aan dat dit ook zo is. Het certificaten-systeem is gebouwd op vertrouwen. Dat stelt hoge eisen aan CA's, zoals wederom duidelijk werd na de hack op de Nederlandse CA DigiNotar in 2011.

2.7 Mobiele besturingssystemen

De ontwikkelingen op de smartphone- en tabletmarkt gaan razendsnel. Dat betekent, meer nog dan voor de PC-markt, dat nieuwe technologieën al worden uitgerold voordat ze volledig getest zijn. Het gebruik van bètaversies begint gemeengoed te worden. De producenten hebben er voor de smartphone- en

tabletmarkt voor gekozen om zich te baseren op nieuwe besturingssystemen zoals Android, iOS, Windows Phone en Blackberry OS. De besturingssystemen van PC's zijn te groot en te zwaar voor de beperkte rekenkracht van smartphones.

De ontwikkelaars van deze nieuwe besturingssystemen hebben de kans gehad om te leren van de fouten die gemaakt zijn bij het ontwikkelen van de besturingssystemen voor de PC. De vraag is of dit ook is gebeurd. Smartphones worden primair ontworpen op gebruikersgemak en beveiliging staat gebruikersgemak vaak in de weg. Het toestel staat altijd aan, virusscanners zijn schaars, de connectie met draadloze hotspots staat meestal default aan, en de besturingssystemen blijken slecht bestand te zijn tegen malware.

Een zorgelijke ontwikkeling op dit gebied is dat de verschillende smartphonefabrikanten hun telefoons leveren met een eigen variant van het besturingssysteem. We zien dit met name bij Android toestellen. De software in deze eigen distributies loopt vaak achter en wordt onvoldoende geüpdatet, wat betekent dat beveiligingslekken die al meer dan een jaar bekend zijn bij veel klanten nog niet gepatcht zijn. Het feit dat privé aangeschafte telefoons ook steeds meer voor het werk gebruikt gaan worden (bring your own device) levert een stevige uitdaging op voor IT security.

2.8 Draadloze technologie

Communicatie en dataoverdracht gaan in toenemende mate door de lucht. Draadloos internet, DECT-telefonie, bluetooth, RFID, satellietcommunicatie zijn allemaal radiogolven waarmee op verschillende golflengtes en met verschillende protocollen contact wordt gemaakt tussen twee of meer apparaten. Die signalen kunnen allemaal onderschept worden. Criminelen zijn in staat om ze af te luisteren of zelfs aan te passen indien er geen of geen goede versleuteling van die gegevens plaatsvindt.

Van verschillende protocollen is bekend dat de versleuteling in meer of mindere mate gebroken is. Zo zijn GSM[9] en DECT[10] met goedkope hulpmiddelen in realtime af te luisteren. Criminelen kunnen hier op diverse manieren misbruik van maken. Er kan geld verdiend worden door communicatie op te vangen en te

[9] Zie: GOVCERT.nl - Factsheet FS2009-05 (2009).

[10] Aangetoond op 25C3 (het 25e Chaos Communication Congress), december 2008.

veranderen (denk aan betaal-SMS) en het afluisteren van GSM past in contra-strategieën van georganiseerde criminelen. Ook de mogelijkheden voor (ontwrichtende) aanvallen lopen in de pas met het toenemende gebruik van radiosignalen voor dataoverdracht.

WiFi (draadloos internet) kent verschillende encryptiemogelijkheden. WEP kan met eenvoudige middelen in seconden gekraakt worden. Voor het veelgebruikte WPA / TKIP is aangetoond dat het te kraken is[11]. WPA2 is vooralsnog in de praktijk veilig. Het zwakste punt van WiFi-encryptie zijn overigens vaak de wachtwoorden.

Een ander zwak punt is de implementatie van de WiFi clients. Sommige apparaten verbinden automatisch met ieder access point dat dezelfde naam heeft als een hotspot waarmee ze eerder verbonden zijn geweest, soms zelfs als deze nieuwe hotspot geen encryptiewachtwoord nodig heeft terwijl de oorspronkelijke hotspot dat wel had. In combinatie met het actief uitzenden van de bekende hotspots maakt dit het erg eenvoudig om een gebruiker zonder dat deze het in de gaten heeft een onbetrouwbare internetverbinding aan te bieden.

2.9 De cloud

Bij cloud computing maakt men gedeeld gebruik van IT-middelen op het internet, bijvoorbeeld voor de opslag van data. Deze middelen worden alleen aangewend indien ze daadwerkelijk nodig zijn. Cloud computing drukt daarmee de kosten, maar het brengt tevens een aantal risico's met zich mee. De meeste personen en bedrijven die gebruik maken van de cloud, nemen die dienst af van een derde partij. Voorbeelden van dergelijke partijen zijn Google, Microsoft en Amazon. Het beheer van de data is daarmee ook uit handen gegeven aan deze partijen. Het is onduidelijk waar de data fysiek opgeslagen is (vaak verdeeld over diverse geografische locaties) en de beveiliging van de data ligt bij de aanbieder van de clouddienst. Zoals bij veel relatief nieuwe technologieën is de beveiliging in de cloud nog niet op het gewenste niveau.

Daarnaast worden ook volledige servers aangeboden. Dit zijn virtuele machines. Op één fysieke machine kunnen diverse virtuele machines draaien. De fysieke machines worden hierdoor efficiënter gebruikt, waardoor de cloud aanbieders

[11] Ohigashi en Morii - A Pratical Message Falsification Attack on WPA- Hiroshima University en Kobe University.

goedkoper kunnen werken. De gebruiker kan zijn virtuele machine naar eigen wens indelen, en naar eigen behoefte rekencapaciteit gebruiken. Hij weet echter niet met wie hij de machine deelt en waar de machine zich bevindt.

Voor de politie levert het gebruik van cloud diensten de vraag op hoe dergelijke data op een forensisch correcte methode kan worden veiliggesteld. De cloud provider zal in veel gevallen wel in staat zijn een kopie van de data te verschaffen, maar dat zal geen forensische kopie zijn.

2.10 Industriële systemen

Geautomatiseerde systemen brengen per definitie kwetsbaarheden mee. In veel vitale sectoren is procesautomatisering dermate complex en wijdvertakt dat speciale aandacht vereist is om de beveiliging van de bedrijfsprocessen te controleren en te waarborgen. Een goed preventiebeleid is daarom essentieel om de risico's zo laag mogelijk te krijgen en te houden.

Een belangrijk aandachtspunt vormt de beveiliging binnen het domein van de process control systemen. Deze systemen worden ook vaak SCADA-systemen (Supervisory Control And Data Acquisition) genoemd. Ze worden veelvuldig gebruikt om industriële systemen van uiteenlopende grootte te besturen. Ze sturen de verschillende machines aan en verzamelen en verwerken gegevens van meet- en regelsensoren om het proces stabiel te houden. De systemen worden onder meer gebruikt door elektriciteitscentrales, boorplatforms, gemalen, kerncentrales en drinkwaterbedrijven.

Omdat deze systemen hoge eisen stellen aan betrouwbaarheid en bedrijfszekerheid worden de computers in deze systemen zelden of nooit geüpdatet. Een update legt de productie namelijk stil en de werking van het systeem kan na een update niet altijd gegarandeerd worden. Als gevolg hiervan draaien sommige process control systemen op oude hardware, een oud besturingssysteem en zonder virusscanner. Dit is in beginsel geen bezwaar zolang gegarandeerd kan worden dat er geen verbindingen bestaan met kantoorautomatisering of computers die in contact staan met de buitenwereld. De afgelopen jaren is echter gebleken dat dergelijke verbindingen vaak wél bestaan.

2.11 Big data

Big data staat voor gegevenssets die zo groot zijn dat ze met behulp van de standaardprogramma's niet meer beheerd of binnen redelijke tijd verwerkt kunnen worden. Van big data is sprake vanaf enkele tientallen Terabytes, een grens die jaarlijks opschuift met het beschikbaar komen van grotere opslagmedia en snellere computers. Het werken met grotere datasets maakt het mogelijk om trends te ontdekken en verbanden te leggen die anders niet zichtbaar zouden zijn. Door de snelle groei van informatie en informatiebehoefte neemt big data toe.

3
Criminele techieken en middelen

3.1 Inleiding

In hoofdstuk 2 werd kort het huidige cyberlandschap beschreven, in dit hoofdstuk zullen we inzoomen op de technieken en middelen die high tech criminelen gebruiken om zich in dit landschap te bewegen. We kunnen hierin onderscheid maken tussen aanvalstechnieken, communicatietechnieken en anonimiseringstechnieken.

De technieken en middelen die high tech criminelen tot hun beschikking hebben zijn net zo veranderlijk als het aandachtsgebied zelf. Daarnaast kenmerken ze zich door een grote mate van variatie. Van geavanceerde, specialistische software die maar voor een beperkte groep mensen toegankelijk is tot algemeen en makkelijk verkrijgbare compleet ingerichte kits die iedereen van het internet kan halen. En natuurlijk niet te vergeten: social engineering, de aanval op de mens achter de computer. Het gaat niet in alle gevallen om technieken die op zichzelf aangemerkt worden als high tech crime, maar om middelen die onderdeel uit kunnen maken van high tech crime ketens. In veel gevallen zijn er dwarsverbanden tussen de technieken te leggen en is de inzet van meerdere technieken tegelijkertijd of achtereenvolgens noodzakelijk. Soms zijn de technieken op zichzelf al strafbaar, terwijl ze voor de cybercrimineel wellicht slechts als middel dienen om een (strafbaar) doel te bereiken. Het illegaal achterhalen van een wachtwoord is bijvoorbeeld slechts een middel om toegang te krijgen tot de bankaccount van een slachtoffer, waarmee de crimineel vervolgens zijn einddoel kan bereiken: de bankrekening leeghalen. De (mate van) strafbaarheid hangt af van wet- en regelgeving, die per land kan verschillen. In veel landen is cyberwetgeving op dit moment volop in ontwikkeling.[12]

3.2 Hacken

Hacken omvat een breed scala aan activiteiten en wordt vaak als containerbegrip gebruikt. In algemene zin kan het gedefinieerd worden als het binnendringen in geautomatiseerde werken. In de praktijk is hacken vaak een proces

[12] In hoofdstuk 7 wordt nader ingegaan op de strafbaarstellingen die in Nederland gelden.

van verscheidene stappen en lagen. In deze paragraaf worden een aantal belangrijke elementen uit dit spectrum beschreven. In veel gevallen zullen technieken ongericht ingezet worden: elke computer met de bewuste zwakheid wordt gehackt. Het gaat dan om geautomatiseerde processen die op grote (mondiale) schaal worden ingezet. Logbestanden van IDS's[13] of firewalls laten zien dat systemen dagelijks worden onderworpen aan zulke hack-pogingen. Daarnaast vinden er ook steeds vaker gerichte aanvallen op specifieke systemen plaats. Voor zulk maatwerk is meestal meer kennis vereist. Er moet bijvoorbeeld worden uitgezocht waar de zwakheden van het bewuste systeem liggen, om vervolgens een aanvalsmethodiek te ontwikkelen om het te kunnen binnendringen. Dit is een intensiever proces dan bij geautomatiseerde hacks. Immers worden de zwakheden bij een bepaalde computer gezocht, en niet de computers bij bepaalde zwakheden.

3.2.1 Exploits

Veel hackpogingen beginnen met een portscan. Hierbij worden alle netwerkpoorten van het doelsysteem systematisch en automatisch bevraagd door er datapakketjes heen te sturen. Op grond van de reacties kan opgemaakt worden welke poorten actief zijn (open staan) en welke versie van de netwerkservice erop draait. Aan de hand daarvan kunnen de kwetsbaarheden in kaart worden gebracht en kan de juiste exploit erbij gezocht worden.

Voorbeeld
Bij de portscan blijkt poort 80 open te staan (dit is de poort waarover onversleuteld web-verkeer gaat; de http-poort). Op poort 80 draait een Apache server (een veel gebruikte webserver), versie 2.0.63. Dit is een oude versie, met bekende kwetsbaarheden. Aan de hand van deze gegevens kan de hacker op zoek gaan naar een bestaande exploit die de betreffende kwetsbaarheden kan uitbuiten, of eventueel zelf zo'n exploit schrijven.

Een exploit is een stuk programmacode, een verzameling gegevens, of een opeenvolging van commando's om een specifieke kwetsbaarheid in software te misbruiken. In het bovengenoemde voorbeeld wordt de exploit bij de machine gezocht. Bij massale aanvallen gaat het vaak andersom. Daar wordt gebruik gemaakt van een bekend beveiligingslek in een versie van een programma en

[13] 'Intrusion Detection System' (inbraakdetectiesysteem). Dit is software die alarm slaat als het pogingen detecteert van ongeoorloofde toegang tot een netwerk.

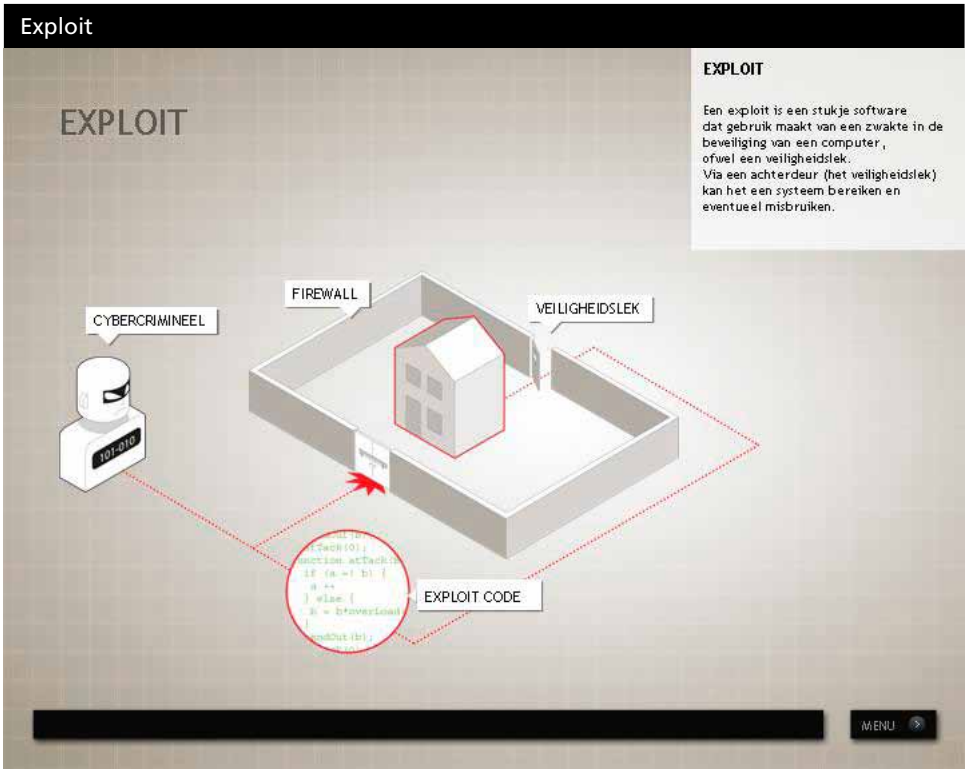
worden zoveel mogelijk systemen benaderd. De systemen met de bewuste versie raken besmet.

Voorbeelden

Internet Explorer 6 (al jaren niet meer ondersteund) bevat een groot aantal bekende kwetsbaarheden. Door gebruikers naar een webpagina te lokken die een exploit bevat voor een van deze kwetsbaarheden kan een kwaadwillende alle bezoekers die de pagina met Internet Explorer 6 bezoeken besmetten.

Een hacker bezit een exploit die misbruik maakt van een beveiligingslek in Adobe Reader, versie 10.1.1, en stopt deze in een pdf bestand. Het pdf-bestand wordt vervolgens via spam mail uitgestuurd naar miljoenen mailadressen. De geadresseerden die het bestand openen en hun Adobe Reader nog niet hebben geüpdatet naar versie 10.1.2 raken hierdoor besmet.

Figuur 3.1



Exploits worden meestal ontwikkeld met behulp van 'reverse engineering'[14] van updates die leveranciers hebben uitgebracht. Aangezien veel mensen de update niet installeren, kunnen de kwetsbaarheden zo vaak nog lang misbruikt worden.

Voorbeeld
Op 6 december 2011 brengt Adobe een security advisory uit waarin wordt aangegeven dat versie 10.1.1 een kritiek beveiligingslek bevat, en raadt gebruikers ten strengste aan te upgraden naar versie 10.1.2. Dezelfde dag gebruiken verschillende hackers wereldwijd de gegevens uit de security advisory om in de assembly[15] code van Adobe Reader gericht op zoek te gaan naar het lek en daar een exploit voor te schrijven.

Door techologische vooruitgang in kwaliteit van standaardsoftware en bijbehorende beschermingsmaatregelen is de waarde van werkende exploits voor veelgebruikte programma's de afgelopen jaren sterk gestegen.

IFrame injecties

Exploits kunnen verstopt worden op internetpagina's. Eén van de manieren om dit te doen is met behulp van IFrame injecties. IFrames zijn een soort vensters binnen de pagina en worden gebruikt om de pagina op te bouwen. Een besmette pagina kan een IFrame venster ter grootte van nul pixels bevatten (dus niet zichtbaar) die code aanroept van een andere, externe locatie. Dit heet cross site scripting. Deze code kan vervolgens een exploit bevatten die de computers van bezoekers kan besmetten. Dit is een voorbeeld van een zogeheten drive-by-download: een programma dat wordt geladen zonder medeweten of goedkeuring van de gebruiker.

0-day exploits
De gevaarlijkste, en duurste, exploits zijn de zogeheten 0-day (uitspraak zero-day of oh-day) exploits. Dit zijn exploits waarvan nog geen patch voorradig is. Meestal zijn de makers van de betreffende software zelf nog niet op de hoogte van de uitgebuite kwetsbaarheid of ze zijn er nog niet aan toe gekomen om de software te patchen. De term 0-day slaat op het aantal dagen dat de kwetsbaarheid (algemeen) bekend is. 0-day exploits worden gezien hun aard voor-

[14] Reverse engineering is het onderzoeken van een product om daaruit af te leiden wat de eisen zijn waaraan het product probeert te voldoen, of om de precieze interne werking ervan te achterhalen. Dit doet men meestal met het doel een concurrerend product te ontwerpen.

[15] Basale programmeertaal waarin elke instructie één op één overeenkomt met een instructie in machinetaal.

namelijk gebruikt voor gerichte aanvallen op een specifiek doelwit. Omdat de kwetsbaarheid nog niet bekend is bestaat er ook geen verweer tegen. In 2010 werd bekend dat de StuxNet-worm minimaal vier 0-day kwetsbaarheden in het Windows besturingssysteem uitbuitte.

3.2.2 SQL-injecties

Structured Query Language (SQL) is een taal die ontworpen is om databases te vullen en te bevragen. SQL-injecties zijn een zeer gebruikelijke manier om te hacken. Bij een SQL-injectie geeft de crimineel een SQL-opdracht aan de database via zijn browser. Op die manier kunnen bijvoorbeeld databases uitgelezen, aangepast of verwijderd worden. Een SQL-injectie is technisch gezien relatief eenvoudig. Om die reden kan het vaak ook makkelijk gestopt worden via speciale gestandaardiseerde controles in de applicatie. Desondanks is een groot percentage van de databases die online ontsloten is, niet afdoende beveiligd tegen deze injecties.

3.2.3 Sniffing

Sniffing is het afvangen van netwerkverkeer. De aanvaller kan hierdoor alle data die vanuit of naar een systeem wordt verzonden 'meelezen'. De internet-tap, die de politie onder bepaalde voorwaarden mag zetten bij internet service providers, is feitelijk ook een vorm van sniffing.

Versleutelde data kan met behulp van sniffing wel opgevangen maar niet geduid worden, hooguit kan worden vastgesteld wie de zender en de ontvanger zijn. Encryptie is echter nog niet de norm, vooral niet bij intern dataverkeer binnen bedrijfsnetwerken. Met behulp van sniffing kan zo bijvoorbeeld direct bedrijfsgevoelige informatie worden buitgemaakt. Hackers kunnen het ook inzetten om gebruikersnaam/wachtwoord combinaties af te vangen om daarmee vervolgens het netwerk verder binnen te kunnen dringen. Sniffing wordt meestal in combinatie met andere technieken voor gerichte aanvallen gebruikt.

Het toenemende gebruik van draadloze communicatie[16] (WiFi, bluetooth, etc.) gecombineerd met het gebruik van protocollen die vaak deels of geheel gebroken zijn maakt het voor criminelen mogelijk te sniffen zonder fysieke toegang.

---

[16] Zie paragraaf 2.8.

3.2.4 Wachtwoorden kraken

Een hacker kan zich verdiepen in de meest geavanceerde technologische mogelijkheden om een computersysteem binnen te dringen. Echter biedt het kraken van een wachtwoord vaak directe toegang tot allerlei cruciale (vertrouwelijke) systemen en data. Hackers maken gebruik van verschillende technieken om wachtwoorden te achterhalen. Hieronder volgen enkele voorbeelden.

‘Stratfor-wachtwoorden schokkend slecht’

03-01-2012 (op webwereld nl)

De gebruikte wachtwoorden op de site van beveiligingsbedrijf Stratfor zijn schrikbarend eenvoudig te kraken. “Het wachtwoordbeleid bevindt zich nog in de Middeleeuwen.”
Dat concludeert techsite The Tech Herald na een analyse van de 860.000 gelekte StratFor-accounts die de hackersgroep Anonymous vorige week publiceerde. Binnen 5 uur kraakte Tech Herald 81.000 wachtwoorden. Zelfs wachtwoorden van één karakter werden gevonden (59 stuks). “Dat is verrassend voor een bedrijf dat inlichtingen verzamelt en deelt,” meldt de site. Uit de analyse blijkt dat de gebruikers wachtwoorden gebruiken die eenvoudig te herinneren zijn en daarvoor persoonlijke gegevens gebruiken, zoals voornamen (James), favoriete muziekgroep (Blink 182) en data (19871987). Een medewerker van het Nationaal Coördinator Terrorisme-bestrijding gebruikte het wachtwoord ‘0000’ om in te loggen.

Raden
De meest eenvoudige techniek om achter een wachtwoord te komen is door er simpelweg naar te raden. Deze methode werkt alleen bij slecht beveiligde systemen, maar daar zijn er schrikbarend veel van. Lijsten met veelvoorkomende wachtwoorden circuleren overal op internet. Het gaat daarbij vooral om ‘default’ wachtwoorden die standaard bij producten of diensten worden geleverd, veelvoorkomende namen en toetsenbordcombinaties. Bovendien gebruiken mensen vaak precies hetzelfde wachtwoord voor verschillende applicaties. Daardoor kunnen hackers overal binnenkomen zodra ze één wachtwoord in handen hebben.

Rainbow tables

De meeste systemen slaan wachtwoorden niet letterlijk op (hoewel er verrassend veel systemen zijn die dat wel doen). In plaats daarvan versleutelen ze de wachtwoorden met behulp van een hashfunctie tot een hashwaarde[17]. Zo'n functie werkt maar één kant op; de hashwaardes kunnen dus niet teruggerekend worden naar het wachtwoord. Wel zijn er meerdere wachtwoorden mogelijk met dezelfde hashwaarde. Als een hacker zich toegang weet te verschaffen tot een wachtwoordenbestand met dergelijke hashwaardes dan weet hij nog niet wat de daarbij behorende wachtwoorden zijn. Hij zou ze één voor één moeten proberen en dat duurt een eeuwigheid. Rainbow tables kunnen dit werk echter aanzienlijk versnellen. Dit zijn enorme wachtwoordtabellen waarbij voor elk wachtwoord de bijbehorende hashwaarde is opgeslagen. Deze hashwaardes zijn vooraf berekend met behulp van dezelfde hashfunctie als die op het doelsysteem. De gevonden hashwaardes worden opgezocht in de rainbow table en als ze gevonden worden rolt het wachtwoord er direct uit. Goede rainbowtables zijn eenvoudig te vinden op het web.

Voorbeeld

Een hacker heeft zich toegang weten te verschaffen tot een Duits Windows XP systeem maar heeft daar te weinig privileges om verder te komen. Hij kan echter wel de gehashte wachtwoordentabel inzien. Hij gebruikt de tool ophcrack, speciaal bedoeld voor het kraken van Windows wachtwoorden, en downloadt de rainbow tables xp_free_fast (voor een eerste poging), xp_special (voor wachtwoorden met speciale karakters) en xp_german (voor wachtwoorden met umlauten), in totaal zo'n 16GB. Hiermee is hij in staat om praktisch elk wachtwoord tot en met 14 karakters in redelijke tijd te kraken. Voor het gebruik van specialistische (niet gratis) rainbow tables is geavanceerdere apparatuur nodig; de hacker in dit voorbeeld is derhalve waarschijnlijk een professional.

Men kan zich via verschillende technieken wapenen tegen het gebruik van rainbow tables, zowel aan de systeem-kant (salting) als aan de gebruikerskant (langere wachtwoorden), maar deze worden nog te weinig toegepast.

Naast systeemwachtwoorden kunnen rainbow tables ook ingezet worden voor het kraken van wachtwoorden van bijvoorbeeld Windows Office files.

---

[17] Een hashwaarde is een groot getal dat met behulp van een wiskundige functie (de 'hashfunctie') kan worden berekend uit een willekeurige invoer zoals een wachtwoord of een bestand. Hashfuncties zitten zo in elkaar dat de kans dat twee verschillende invoeren dezelfde hashwaarde opleveren extreem klein is.

Brute force
In het verlengde van het gebruik van een rainbow tables ligt de brute force aanpak. Hierbij worden alle mogelijke varianten één voor één uitgerekend door krachtige apparatuur. Voor een wachtwoord van acht karakters is dit binnen beperkte tijd te doen. Maar een wachtwoord van twintig karakters via brute force kraken zou eeuwen duren. Daarom wordt deze methode meestal pas gebruikt als andere methodes onbruikbaar zijn of gefaald hebben.

3.2.5 Fysieke toegang

Fysieke toegang tot een systeem biedt de aanvaller de meeste kansen op een succesvolle hack, vooral als het systeem aan staat. We geven hier twee voorbeelden. Overigens wil dat niet zeggen dat het beveiligen van computersystemen tegen fysieke aanvallen zinloos is. Net als in de fysieke wereld geldt dat een beter slot zorgt voor een kleinere kans op inbraak.

Evil maid
De beste beveiliging tegen fysieke aanvallen bestaat uit Full Disk Encryption (FDS). De naam doet vermoeden dat de volledige disk versleuteld is, maar in de praktijk zijn delen van de harddisk onversleuteld. Deze zijn nodig in de eerste fase van het opstarten (bootloading).

Voor een evil maid aanval is tweemaal toegang nodig tot de computer van het slachtoffer. De naam van de aanval komt van het scenario waarin een kamermeisje in een hotel zich tweemaal toegang weet te verschaffen tot een PC. Bij de eerste toegang wordt de PC opgestart met behulp van een geprepareerde USB-stick. Hierop staat een stukje code dat een aanval uitvoert op de Full Disk Encryption. De versleuteling zelf wordt niet opgeslagen, er wordt alleen voor gezorgd dat als het slachtoffer de volgende keer zijn PC opstart zijn wachtwoord onversleuteld op de harde schijf wordt opgeslagen. Bij de tweede toegang wordt de PC weer met de geprepareerde USB-stick opgestart. Het wachtwoord wordt op de stick geladen en de originele situatie weer teruggezet. De USB-stick bevat nu dus het wachtwoord voor de Full Disk Encryption.

De evil maid aanval werkt niet tegen elke vorm van Full Disk Encryption. Wel blijven er nieuwe varianten gevonden worden, bijvoorbeeld tegen bepaalde mobiele platforms.

Firewire
Firewire wordt vaak gebruikt bij audiovisuele apparaten en bij beeldbewerking, vanwege de optie tot hoge overdrachtssnelheid en compatibiliteit met lange

bekabeling. Door een kabel aan te sluiten op de Firewire-poort van een ingeschakelde computer kan een kwaadwillende volledige lees- en schrijfrechten bemachtigen. Dat betekent dat hij, ondanks wachtwoordbeveiliging, alles kan doen wat hij wenst. Ook laptops zonder Firewire-poort, maar met een PCMCIA-slot kunnen aangevallen worden. Dit is mogelijk door een Firewire PCMCIA-kaart in het slot te stoppen. De aanval kan binnen enkele seconden worden uitgevoerd. Er is geen andere oplossing voor de problemen met de kwetsbaarheid van Firewire, behalve het uitzetten van het protocol. Het betreft hier namelijk geen onvolkomenheid in de techniek; het is bewust op deze manier ontworpen.

3.3 Malware - besmetting

Bij veel, maar niet alle, vormen van high tech crime worden op enig moment één of meerdere computers besmet met malware. Er bestaat een uitgebreid arsenaal aan technieken en middelen om een dergelijke besmetting te realiseren. In de meeste gevallen gaat het om een combinatie van hacken en social engineering[18].

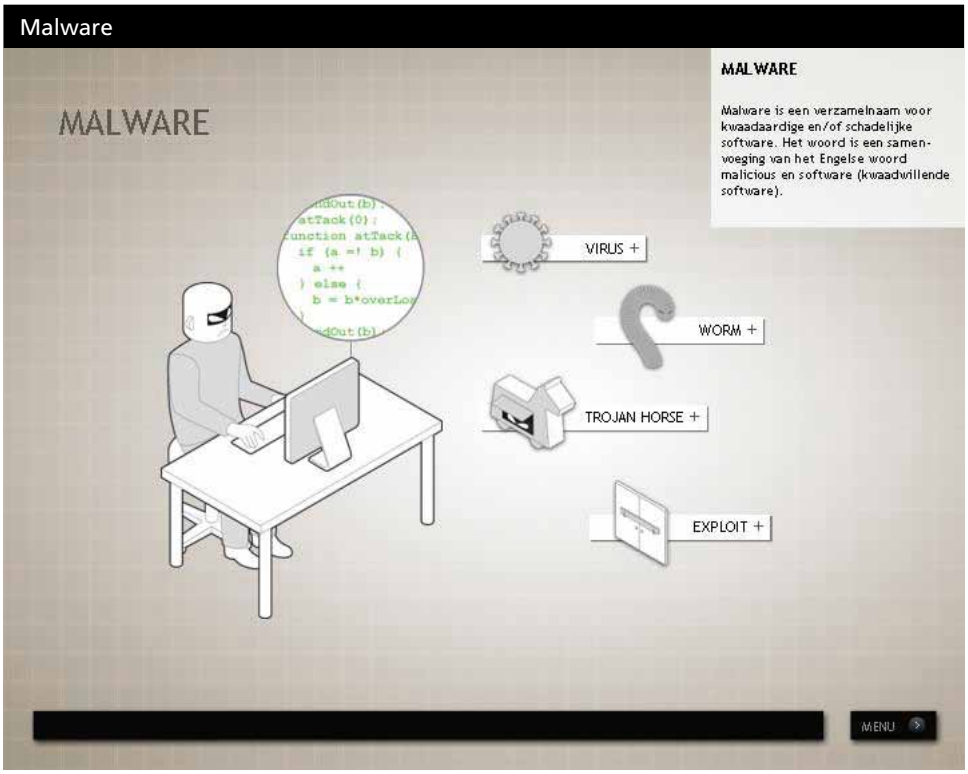
Malware (of: crimeware) is de verzamelnaam voor alle vormen van software met kwaadaardige bedoelingen. De term is een samenvoeging van de Engelse woorden 'malicious' en 'software' (kwaadwillende software). In deze paragraaf zullen we aandacht besteden aan malware die erop gericht is veel systemen te besmetten. Als dit eenmaal gebeurd is wordt vaak de achterdeur opengezet om de crimineel de mogelijkheid te bieden uitgebreidere programma's te installeren zoals keyloggers of botnetsoftware.

We behandelen achtereenvolgens trojans, virussen en wormen. Ook IFrame injecties zouden in de categorie 'ongerichte besmettingsmalware' ondergebracht kunnen worden. Deze zijn reeds omschreven in paragraaf 3.2.1. De scheidslijnen tussen deze vormen van malware zijn in de loop van de tijd steeds vager geworden en in het algemene spraakgebruik voldoet de term malware prima. Om een duidelijk beeld te houden van de trends in malware gebruiken antivirusbedrijven de onderverdeling echter nog wel. De verschillende vormen worden overigens ook dikwijls in combinatie ingezet (blended threats).

---

[18] Zie paragraaf 3.6.

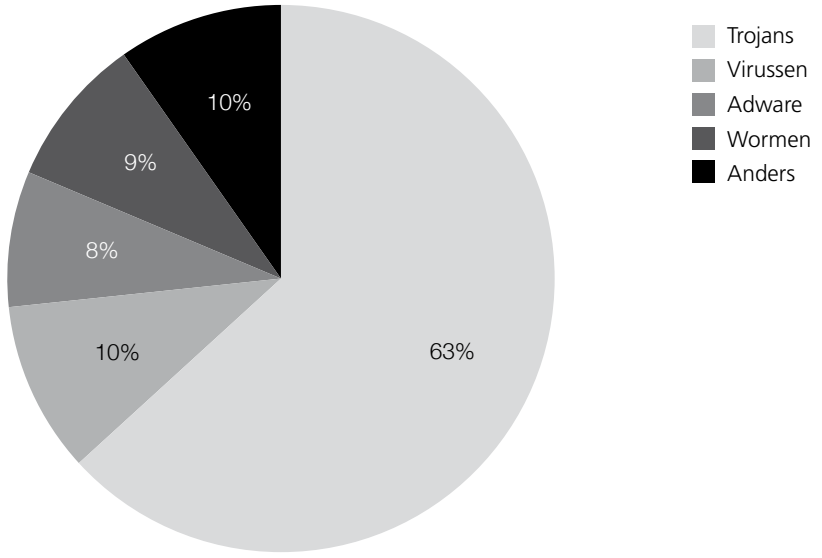
Figuur 3.2



Varianten van malware, afzonderlijk of als blended threat, vormen een serieuze bedreiging voor ICT-systemen. En daarmee natuurlijk ook voor de huidige samenleving, die in grote mate afhankelijk is van dergelijke systemen. De impact wordt ook steeds groter: malware beperkt zich niet meer tot het verzenden van onschuldige mailtjes, maar is in staat gegevens te stelen en te manipuleren door de harddisk te lezen, toetsaanslagen door te geven, screenshots door te sturen en het internetverkeer van de computer te sturen. Malware beperkt zich niet alleen tot de klassieke PC, maar is ook gericht op bijvoorbeeld mobiele platformen en process control systemen. De verscheidenheid aan malware voor deze platforms is nog aanzienlijk kleiner dan voor de PC markt, maar de procentuele groei aanzienlijk hoger.

Figuur 3.3

Soorten malware aangetroffen op computers wereldwijd



Bron: Pandalabs 2011

3.3.1 Trojans

De term 'trojan' is voortgekomen uit de bekende Griekse mythe over het Paard van Troje. In dat verhaal werd Troje door de Grieken binnengedrongen doordat de soldaten zich in een gigantisch houten paard hadden verstopt, dat als cadeau de stadsmuren was binnengehaald. Een trojan werkt in digitale zin vergelijkbaar: het probeert, eenmaal binnen in het systeem, van binnenuit een poort te openen.

Een trojan is een programma dat ongemerkt meekomt als een computergebruiker een programma installeert of een bestand uit bijvoorbeeld een e-mail, USB-stick of website opent of downloadt. Het programma voert zelf geen aanvallen uit, maar is wel in staat om andere malware binnen te halen die schade kan aanrichten. Een verklaring voor het 'succes' van trojans[19] is dat

[19] Zie bijvoorbeeld tabel 2.2.

ze van binnenuit contact leggen met de buitenwereld, terwijl beveiligingsmechanismen zoals firewalls[20] voornamelijk gericht zijn op het verkeer dat van buitenaf de computer bereikt.

3.3.2 Virussen

Een voorname categorie malware wordt gevormd door de computervirussen. Een computervirus, meestal eenvoudigweg virus genoemd, is een programma dat in staat is om zich te nestelen in een bestand, bij voorkeur een bestand van het besturingssysteem van de computer. Als een dergelijk bestand wordt opgestart, kan het virus actief worden, zich verspreiden of zijn commando's uit gaan voeren. Vroeger werden computervirussen verspreid door geïnfecteerde programma's of bootsectors[21] op floppy disks. Bij het laden van het programma of het plaatsen van de floppy kon het virus zich naar het geheugen kopiëren om zich, zodra de mogelijkheid zich voordeed, op een ander programma of andere floppy te nestelen. Daarnaast hadden de meeste virussen een 'payload': een malafide set instructies in een deel van het virus dat de daadwerkelijke schade toebrengt aan de computer.

Het aantal virussen volgens de strikte definitie 'zelfreplicerend binnen een systeem na een actie van de gebruiker' is in de loop van de tijd niet echt gestegen. Dat neemt niet weg dat er naast oude ook moderne virussen actief zijn, die nog steeds volgens dit principe werken. Uiteraard zijn ze dan wel geavanceerder en hebben ze vaak een polymorf karakter.

Polymorfie

Polymorfie (of: polymorfisme) doelt op de eigenschap van malware om zichzelf te veranderen. Dit betekent dat hetzelfde stuk malware verschillende vormen kan aannemen, waarbij het de functionaliteit behoudt. Al in 1991 werd een virus aangetroffen met een polymorf karakter: 'Tequila'. Dit virus was moeilijk te detecteren omdat het daar door mutatie beter tegen bestand was.

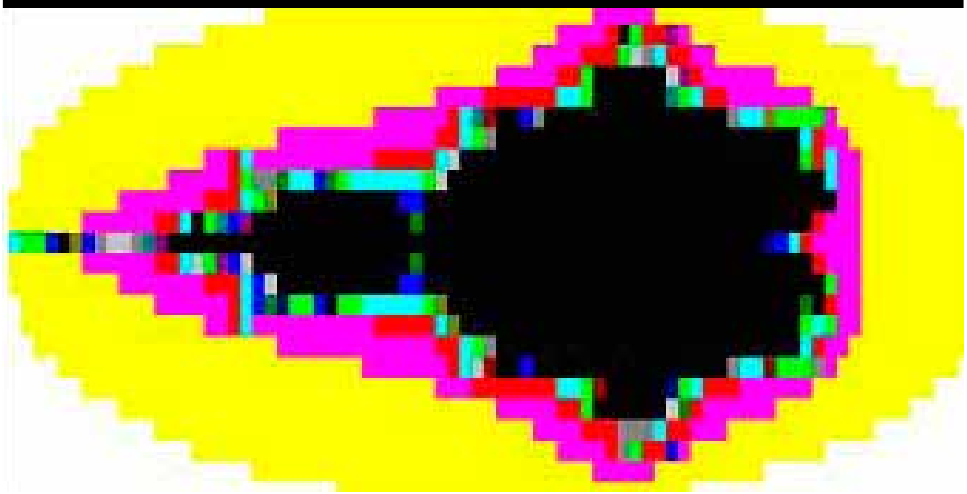
---

20 De verzameling van aanverwante computerprogramma's, gelegen op een netwerk-gateway (zoals router of PC), die de middelen van een privénetwerk beschermen tegen misbruik van buitenaf.

21 Het gebied op een harddisk of diskette waar alle gegevens staan die nodig zijn bij het opstarten van het besturingssysteem op dat medium.

Figuur 3.4

Een uitvergrote fractie van het Tequila virus



Bron: Hypponen.com

Klassieke antivirus software is vaak niet effectief in de bestrijding van polymorfe malware. In de klassieke aanpak wordt potentiële malware vergeleken met een lijst 'signatures' (beschrijvingen van het uiterlijk van de malware). Polymorfe malware kan echter in vele vormen voorkomen. In potentie is moderne malware in staat om bij elke besmetting een andere vorm aan te nemen. Signatures zijn hier niet meer voor te schrijven. De aard van de software die antivirusbedrijven maken verandert dan ook naar 'behavioral analysis'. Dat betekent dat de malware herkend wordt op grond van het gedrag.

3.3.3 Wormen

Wormen vormen een speciale categorie binnen de malware. In tegenstelling tot virussen hechten zij zich bijvoorbeeld niet aan andere programma's. Wormen zijn vaak een stuk code die niet of nauwelijks een gebruikersinteractie (bijv. het starten van een programma) vereisen om zichzelf te repliceren. In plaats daarvan maken ze vaak gebruik van beveiligingslekken in de programma's van netwerk-servers om zich vervolgens autonoom te verspreiden.

De eerste wormen vermenigvuldigden zich via Unix-systemen. Tegenwoordig worden wormen voornamelijk geschreven voor Windows-systemen, hoewel er wel degelijk een aantal bestaan voor Linux en Unix.

ILOVEYOU

De bekendste worm ooit is waarschijnlijk wel de ILOVEYOU e-mailworm, geschreven door de vierentwintigjarige Filippijn Onel de Guzman, en naar verluidt per ongeluk losgelaten op 4 mei 2000. Een dag later was 10 procent van alle op het internet aangesloten computers besmet. De worm bestond uit een simpel e-mailtje met de titel ILOVEYOU en bodytekst 'kindly check the attached LOVELETTER coming from me'. Het e-mailtje bevatte een attachment LOVE-LETTER-FOR-YOU.TXT.vbs, een Visual Basic script dat na het openen de computer besmette. Vervolgens verstuurde het zichzelf naar alle adressen in het Outlook adresboek. De geschatte schade was 5,5 miljard dollar, voornamelijk bestaand uit schoonmaakkosten. Instituten als het Pentagon en de CIA moesten offline om hun e-mail systemen te schonen.

3.4 Malware - aanvallen

Het besmetten van de computer van het slachtoffer is zelden het einddoel van de high tech crimineel. Na besmetting wordt vaak een achterdeurtje opengezet om meer malware op het systeem van het slachtoffer te kunnen plaatsen. Deze malware voert de handelingen uit waar het de crimineel werkelijk om te doen is. We zullen in deze paragraaf een aantal functionaliteiten van deze malware beschrijven. Het bereik van de aanvallen die hieronder de revue zullen passeren wordt nog veel groter als met malware geïnfecteerde machines aan elkaar verbonden worden in botnets, daarover leest u meer in de hieropvolgende paragraaf 3.5.

3.4.1 Resources van een systeem gebruiken

Als een crimineel binnen is gedrongen in een systeem kan hij software installeren die de resources van het systeem aanwendt ten behoeve van crimineel gebruik. Het kan gaan om gebruik van rekencapaciteit, opslagcapaciteit, IP-adres of bandbreedte.

Na de infectie (of hack) is het gebruik van middelen een volgende tussenstap in de criminele keten. Rekencapaciteit kan bijvoorbeeld gebruikt worden om wachtwoorden te kraken om zo de feitelijke doelwitten binnen te kunnen dringen. Opslagcapaciteit kan worden aangewend om illegale content (copyright materiaal, drop server) op te slaan zonder dat deze herleidbaar is tot de crimineel. Het IP-adres kan gebruikt worden om de eigen identiteit te verhullen. Ook bandbreedte kan voor verscheidene doelen gebruikt worden, bijvoorbeeld

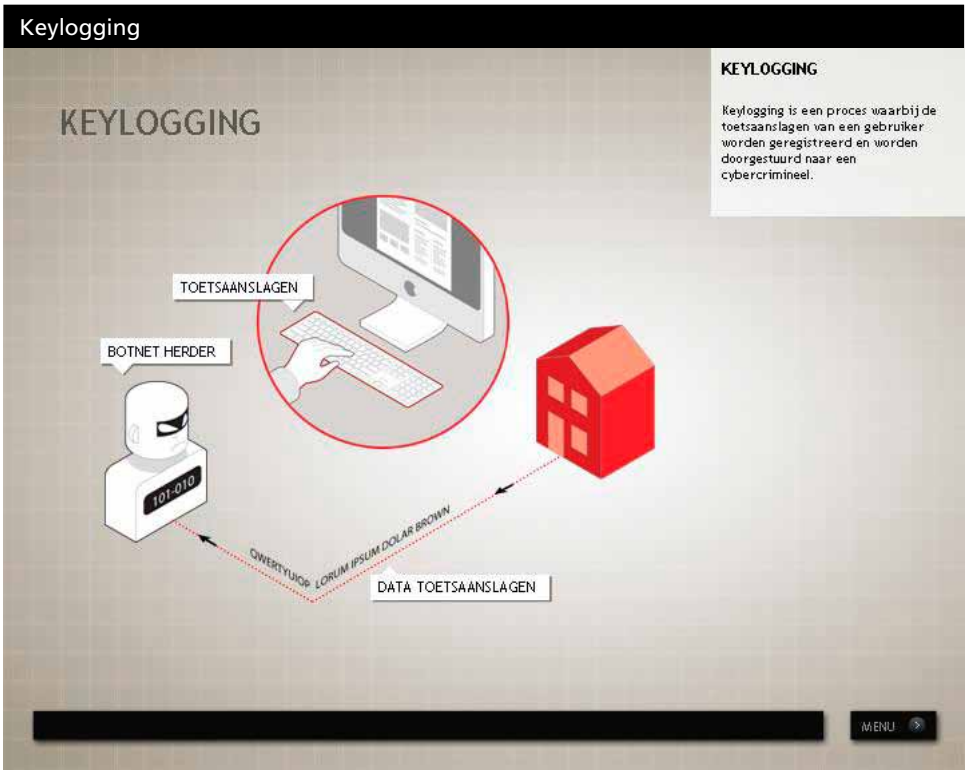
het uitvoeren van een Denial of Service (DoS)-aanval. De laatste twee voorbeelden zullen later in dit hoofdstuk uitgebreider aan bod komen.

3.4.2 Spyware

Spyware is software die meekijkt met alle toetsaanslagen van de gebruiker en deze opslaat (keylogging). Daarnaast is veel spyware in staat om ook afdrukken van het scherm te maken en deze op te slaan. De buitgemaakte informatie wordt, al dan niet gefilterd, gesorteerd of versleuteld, verstuurd naar een drop zone: één of meerdere computers die de informatie opslaan. De drop zone server is in veel gevallen een gecompromitteerde server. De opgeslagen gegevens kunnen door middel van data mining verder geanalyseerd worden om relevante gegevens te gebruiken of te verkopen. Bij ongerichte aanvallen gaat het hierbij vaak om login gegevens of persoonlijke financiële gegevens. Bij gerichte aanvallen moet eerder gedacht worden aan bedrijfsgevoelige informatie, bijvoorbeeld ter verbetering van de concurrentiepositie of voor afpersing.

Spyware verhoogt het dataverkeer van de slachtoffers enigszins, maar kan betrekkelijk eenvoudig verborgen gehouden worden.

Figuur 3.5



3.4.3 Ransomware

Ransomware is malware die een geautomatiseerd systeem of de gegevens daarop gijzelt, bijvoorbeeld door gebruikersdata te versleutelen.

Een voorbeeld hiervan is het 'politievirus' dat in 2011 veel Europese burgers heeft geraakt. De malware versleutelde feitelijk geen bestanden, maar zorgde ervoor dat Windows onbruikbaar werd en vertoonde een scherm waarop de federale politie van het desbetreffende land (vooral Duitsland en Engeland) zou aangeven kinderpornografisch materiaal aangetroffen te hebben op de computer. De computer kon weer bruikbaar worden gemaakt door een flinke 'boete' te betalen via een online banking systeem (bij deze systemen is de eigenaar van het rekeningnummer niet te achterhalen). In maart 2012 kreeg ook Nederland en het KLPD te maken met ransomware. Criminelen verspreidden de volgende boodschap middels spam-berichten: "Het KLPD heeft kinderporno op uw pc ontdekt en in verband daarmee uw pc vergrendeld. Indien u 100 euro

betaalt via de link in deze mail door gebruik te maken van U-kash of Pay-Safe zal het KLPD geen verdere actie ondernemen."

Ook private organisaties zijn interessante slachtoffers voor vergelijkbare afpersing.

Figuur 3.6

Een moderne variant van ransomware op de IPhone

3.4.4 Omleiden van het internetverkeer

Een cybercrimineel kan ervoor zorgen dat wanneer vanuit een geïnfecteerde PC een bepaald IP-adres behorende bij een website wordt opgevraagd, de PC in plaats daarvan doorverwezen wordt naar een malafide website. Hier zit vaak een van de volgende twee verdienmodellen achter:

- Fraude met internetbankieren: bijvoorbeeld door via een zogeheten man-in-the-middle-aanval financiële opdrachten af te vangen en aan te passen. Hierover leest u meer in het volgende hoofdstuk.
- Klik-fraude: hierbij worden inkomsten gegenereerd uit advertenties door er zoveel mogelijk internetgebruikers op te laten klikken.

DNS-spoofing

Met spoofing wordt gedoeld op de situatie dat iemand zichzelf voordoet als iemand anders. Het is een soort digitale identiteitsvervalsing en kan vele vormen aannemen. Elke techniek waarbij de bron of afzender niet op een betrouwbare manier geverifieerd wordt, is in principe kwetsbaar voor spoofing.

De afgelopen periode hebben we in opsporingsonderzoeken gezien dat ten behoeve van het omleiden van internetverkeer niet alleen PC's met malware geïnfecteerd werden, maar ook DNS-servers. Doordat er dan geen verandering is aangebracht op de PC's is dit moeilijker te detecteren door antivirus software.

Bij DNS-spoofing wordt een DNS-server die verantwoordelijk is voor bijvoorbeeld het domein van een aangevallen website, of een willekeurige name server op het internet, gemanipuleerd. De crimineel kan er vervalste informatie naartoe sturen en zo de database of de cache (tijdelijk geheugen waarin informatie wordt opgeslagen) van een DNS-server aanpassen. Zo kunnen gebruikers die een IP-adres behorende bij een aangevallen website opvragen worden omgeleid naar een malafide server.

DNS-spoofing kan op verschillende manieren plaatsvinden. Het kan bijvoorbeeld zo zijn dat een aanvaller een DNS-server misbruikt en daarin de verwijzing van de hostname naar het IP-adres aanpast. Een andere techniek is dat de aanvaller het antwoord vervalst dat van een (caching) nameserver afkomt, voordat het antwoord daadwerkelijk is teruggekomen. Voor systeembeheerders is een dergelijke actie moeilijk te detecteren, omdat zulke nameservers vaak door iemand anders worden beheerd.

3.5 Botnets

Door niet één maar honderdduizenden tot miljoenen geïnfecteerde computers aan elkaar te verbinden in botnets kunnen de hierboven genoemde aanvalsmogelijkheden en het bereik ervan vergroot worden. Bovendien stellen botnets criminelen in staat om hun identiteit af te schermen. Vanwege deze aantrekkelijke functionaliteiten zijn botnets populaire services in de cyber underground en worden ze ook wel beschouwd als het Zwitserse zakmes voor high tech crime.

3.5.1 Definities

Een botnet is een netwerk van aan het internet verbonden gecompromitteerde computers die op afstand kunnen worden aangestuurd, zonder medeweten of goedkeuring van de eigenaar. De gecompromitteerde computers worden ook wel bots of zombies genoemd. De term botnet is een verkorte samenvoeging van de woorden robot en netwerk. De eigenaar of beheerder van het botnet wordt botnet herder genoemd.

De bovenstaande definitie behoeft wat nuancering. Het hoeven niet noodzakelijkerwijs computers te zijn die onderdeel uitmaken van een botnet. Wederom is de meer techniekneutrale term 'geautomatiseerd werk' beter toepasbaar. Elk aan het internet verbonden geautomatiseerd werk kan in principe gecompromitteerd worden en onderdeel gaan uitmaken van een botnet. Smartphones en routers zijn reeds in botnets aangetroffen.

In 2010 begon de Anonymousbeweging gebruik te maken van het LOIC-tool. Sympathisanten installeerden dit vrijwillig op hun computer om onderdeel uit te gaan maken van een botnet en zo gezamenlijk aanvallen uit te kunnen voeren. Hier is echter geen sprake van een botnet in de klassieke zin: de computer wordt met medeweten en goedkeuring van de eigenaar aangestuurd en dit is alleen mogelijk op het moment dat de tool aanstaat. De eigenaar heeft dus de controle over zijn computer dus nog enigszins in eigen handen. Bij een botnet in de klassieke zin heeft de botnet herder volledige controle over de bot PC's.

Bredolab

In 2010 heeft THTC samen met verscheidene publieke en private partners project Taurus gestart, een proeftuin met als doel een gezamenlijke aanpak van botnets. Het project was gebouwd op drie pilaren: Intelligence (inlichtingen), Intervention (interventie) en Investigation (opsporing).
Een grote Nederlandse hosting provider, een van de partners in de samenwerking, werd in deze periode door een security expert op de hoogte gesteld van het feit dat er een C&C server in hun infrastructuur gedetecteerd was. Deze server bleek onderdeel van een Botnet, dat gebruikmaakte van Bredolabmalware.
Bredolab bleek uitzonderlijk goed in infecteren. Het gebruikte hiertoe tenminste drie technieken:

- Phishing e-mails;
- Harvesten (automatisch verzamelen) van FTP credentials op geïnfecteerde machines;
- Besmetting via advertenties op websites.

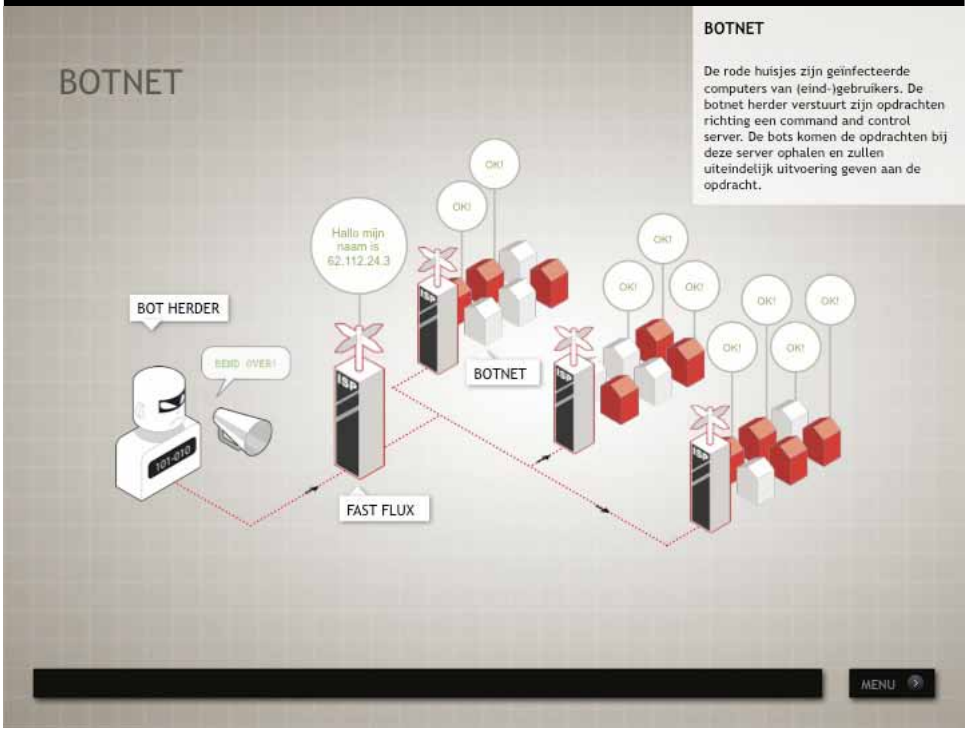
Bredolab had een webshop waar criminelen delen van het botnet konden huren of kopen, inclusief installatie van de gewenste malware op de zombie-PC's. Er hadden bijna 30 miljoen infecties in korte tijd plaatsgevonden via dit specifieke botnet. De als botnet herder verdachte Armeen Georgy A. stuurde daarnaast nog minstens één ander botnet aan vanuit een C&C server in Parijs. Het THTC en partners zijn in deze zaak in staat geweest het botnet in kaart te brengen en over te nemen, de verdachte te identificeren en de slachtoffers te waarschuwen. Inmiddels is Georgy A. in Armenië voor de rechter verschenen en is veroordeeld tot 4 jaar cel. In §7.5 worden de hierboven benoemde stappen nader toegelicht.

3.5.2 Aansturing van botnets

Er zijn verschillende manieren om een botnet aan te sturen. Allemaal komen ze wezenlijk neer op hetzelfde: de geïnfecteerde bot-computer legt via het internet contact met de botnet herder die hem vervolgens opdrachten geeft. De aansturing kan centraal plaatsvinden (via een command and control server) of decentraal (peer-to-peer). Gezien het belang van botnets voor high tech crime zullen we de verschillende aansturingsmogelijkheden hier iets verder toelichten.

Figuur 3.7

Botnet



Centraal aangestuurde botnets

De command and control (C&C) server, de centrale aansturing van een botnet, is de server die de commando's aan de verschillende bots geeft. De bots verbinden met de C&C server en wachten tot ze een taak krijgen. Zo'n taak kan bijvoorbeeld zijn het downloaden van nieuwe malware, het bijdragen aan een DDoS-aanval of het opsturen van de toetsaanslagen van de gebruiker naar een drop zone.

De C&C moet niet gezien worden als een statische server; het zijn vaak verschillende servers met verschillende IP-adressen en URL's die in veel gevallen rouleren (fast flux, verderop beschreven). De servers zijn doorgaans (eventueel via derden) gehuurd op basis van valse of gestolen (creditcard)gegevens of simpelweg gecompromitteerd.

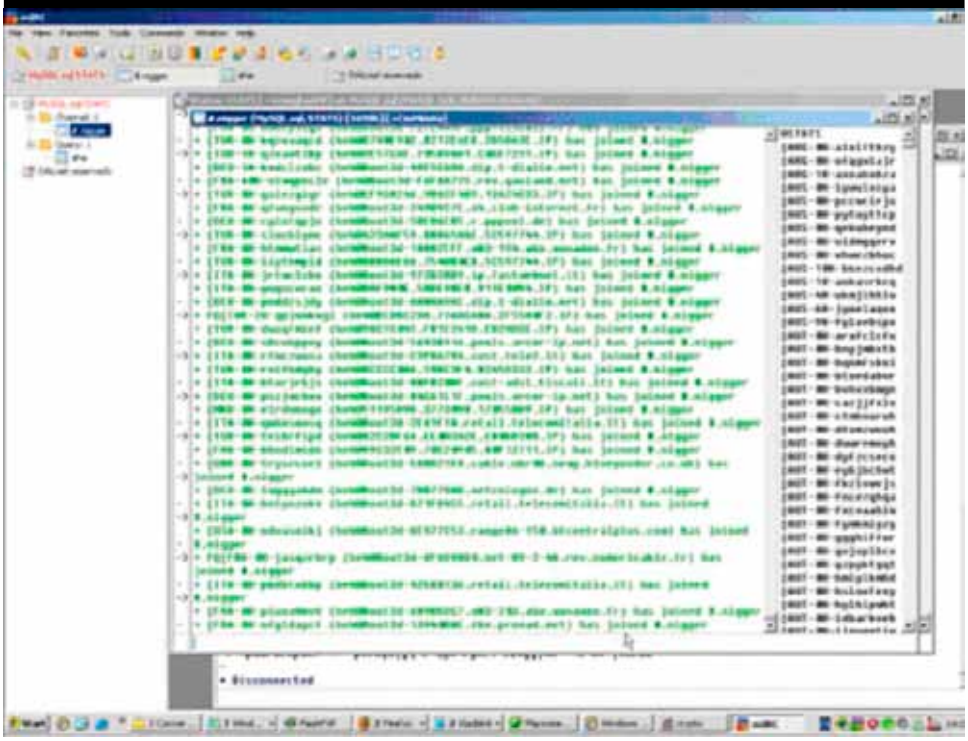
IRC botnets

Om communicatie op internet mogelijk te maken, bestaan verschillende talen waarmee mensen met behulp van computers in staat zijn bepaalde boodschappen over te brengen. Een voorbeeld hiervan is Internet Relay Chat (IRC). Dit systeem is bedacht om verschillende personen tegelijkertijd met elkaar te laten communiceren. Het is eigenlijk een oervorm van het hedendaagse chatten op internet. Bij IRC wordt gebruik gemaakt van een chat-kanaal, waarbij verschillende mensen zich op ieder moment kunnen aansluiten. Het kanaal wordt beheerd door een operator. Deze persoon is onder meer gemachtigd om mensen toe te laten of uit te sluiten van de chat. Omdat chat-kanalen gemaakt zijn om grote hoeveelheden mensen tegelijk te voorzien, zijn ze uitermate geschikt voor de aansturing van botnets.

De malware voor bots kan zo geprogrammeerd worden dat de bots, zonder dat gebruikers van de geïnfecteerde computers dat doorhebben, via het IRC-protocol inloggen op een specifiek IRC-kanaal op de C&C server. De botnet herder heeft dan al zijn bots bij elkaar en kan via dit medium makkelijk opdrachten geven. Dit kan hij bijvoorbeeld doen door een algemeen commando in het kanaal te plaatsen, waardoor het lijkt alsof er tegen de gehele groep gechat wordt. Ook zou hij individuele opdrachten aan de bots kunnen geven via een privé-bericht.

Figuur 3.8

Snapshot uit een door de verdachte gemaakt filmpje



Uit een onderzoek van het Team High Tech Crime. De verdachte stuurde het filmpje naar een medeverdachte als bewijs van het bestaan van zijn botnet. Op het filmpje is te zien hoe via het programma mIRC een kijkje wordt genomen in het IRC-kanaal waarmee het botnet werd aangestuurd. In het midden (groen) is zichtbaar hoe alle individuele bots zich in het kanaal aanmelden.

IRC-gestuurde botnets kunnen beschouwd worden als 'klassieke' botnets. IRC wordt namelijk al jaren misbruikt voor deze functionaliteit. Vanwege de relatief eenvoudige implementatie en de relatief geringe hoeveelheid dataverkeer, is een deel van de waargenomen botnets nog altijd IRC-gestuurd. Wel neemt de populariteit onder high tech criminelen af omdat dit type botnets vrij eenvoudig op te sporen en offline te halen is.

HTTP botnets

HTTP staat voor Hypertext Transfer Protocol: een communicatieprotocol dat vooral is ontworpen om webpagina's over het internet te sturen. Botnets kunnen ook via dit protocol worden aangestuurd. De botnet herder verstuurt zijn opdrachten aan de bots door ze bijvoorbeeld te publiceren op een webpagina, waar individuele bots de opdracht kunnen lezen. Deze webpagina kan daarvoor speciaal zijn aangemaakt, of er kan gebruik gemaakt worden van bestaande websites die voor dit doel gehackt zijn.

Ten opzichte van IRC-gestuurde botnets hebben HTTP-botnets een aantal voordelen voor botnet herders. Zo is er geen voortdurende verbinding met het internet nodig. In plaats daarvan kunnen de bots incidenteel checken of er nieuwe opdrachten klaarstaan. Daarnaast gebruikt het HTTP-protocol in veel gevallen poort 80 van de computer. Firewalls hebben deze poort per definitie openstaan, omdat al het reguliere webverkeer via deze poort verloopt. Dit in tegenstelling tot het IRC-protocol, dat in veel gevallen via poort 6665 tot 6669 communiceert en dus eenvoudiger is af te sluiten zonder dat veel eindgebruikers dat merken.

Vanuit de cybercrimineel bezien is een nadeel van de HTTP-botnets ten opzichte van IRC-botnets dat ze meer bandbreedte gebruiken. Daardoor kan een eventuele infectie eerder opgemerkt worden. Met de algemene groei in bandbreedte de afgelopen jaren begint dit bezwaar steeds minder zwaar te wegen.

Web 2.0 botnets

De groei van web 2.0 applicaties is de afgelopen jaren explosief geweest. Door een hoge mate van gebruikersinteractie en 'user generated content' zijn sites als Facebook, Twitter, YouTube en Wikipedia niet meer weg te denken uit de samenleving. Botnet herders kunnen web 2.0 misbruiken om botnets aan te sturen. Dat werkt relatief eenvoudig. Opdrachten voor de bots worden gepubliceerd via berichten op interactieve sites. Deze manier van aansturen levert diverse voordelen:

- Er hoeft niet eerst een systeem gehuurd of gehackt te worden om commando's te verspreiden. Interactieve mediakanalen zijn gratis aanwezig en er is een ruime keuze aan aanbieders.
- Bediening van de kanalen is zeer eenvoudig.

- Verschillende web 2.0-toepassingen bieden programmeurs Application Programming Interfaces (API's)[22] aan. Hiermee wordt het gemakkelijker om botnets te bouwen die voor deze web 2.0-applicaties ontwikkeld zijn.
- Het gaat om stabiele infrastructuren, die zijn ingericht op het afhandelen van een groot aantal verschillende bezoekers.
- De C&C server kan niet zonder meer geblokt of uit de lucht gehaald worden. Hij is namelijk onderdeel van een regulier gebruikte website.
- Communicatie vindt plaats via poort 80. Firewalls hebben deze poort per definitie openstaan.

Een nadeel van web 2.0 botnets gezien vanuit het oogpunt van botnet herders is de afhankelijkheid van een derde partij. Aanbieders van de web 2.0-diensten proberen botnetactiviteiten in hun netwerk zo snel mogelijk op te sporen en uit te bannen, en zijn daarin behoorlijk effectief. Het gebruik van Twitter, Facebook en dergelijke sociale netwerksites voor de aansturing van botnets heeft dan ook geen hoge vlucht genomen.

Fast flux botnets

Van fast flux (voortdurende verandering) wordt gesproken als netwerk- of IP-adressen, in dit geval van een C&C server, snel wijzigen om de dienst te beschermen tegen uitschakelen. Reguliere fast flux kan bijvoorbeeld door druk bezochte websites worden gebruikt om bezoekers te verdelen over verschillende webservers. Op die manier kan de druk verdeeld worden ('load balancing'). Botnet herders misbruiken de techniek echter door de DNS referentie naar het IP-adres van de C&C server constant te wijzigen. Daardoor is het voor de politie lastig om grip te krijgen op de C&C server. Een internettap is bijvoorbeeld minder succesvol omdat een IP-adres slechts tijdelijk gebruikt wordt. Ook het fysiek of virtueel ontoegankelijk maken van een C&C server is moeilijker, aangezien de connectie dan overspringt naar de volgende.

Een variant van fast flux is 'double (fast) flux'. Bij deze techniek wordt ervoor gezorgd dat de te gebruiken name server ook steeds wordt gewijzigd. Hierdoor is het louter regelmatig checken van de domeinnaam op een willekeurige domeinnaam server niet voldoende, omdat de informatie niet klopt. De juiste server moet daarvoor eerst bekend zijn. De politie, maar ook Internet Service Providers (ISP's), kunnen hierdoor moeilijk de locatie van de C&C server traceren.

---

[22] Een 'Application Programming Interface' (API) is een verzameling definities op basis waarvan een computerprogramma kan communiceren met een ander programma of onderdeel (meestal in de vorm van bibliotheken).

Peer-to-peer botnets
Een botnet dat peer-to-peer (P2P) wordt aangestuurd, kent geen hiërarchische verhoudingen. Bij HTTP- en IRC-gestuurde botnets zijn de bots wel via één of meerdere hiërarchische lagen verbonden met de botnet herder. Bij een P2P-gestuurd botnet zijn de bots, in dat geval 'peers', gelijkwaardig op elkaar aangesloten. Botnet herders die gebruik maken van een P2P-gestuurd botnet kunnen commando's aan een willekeurige bot uit het netwerk aanbieden. Deze verspreidt het commando aan alle peers met wie hij verbonden is. De commando's worden door deze peers vervolgens weer verder verspreid. De implementatie van het P2P-algoritme is lastiger dan bij HTTP- en IRC-gestuurde botnets. Er zijn echter verschillende open implementaties van P2P-protocollen die gebruikt kunnen worden als basis voor het inrichten van een dergelijk netwerk.

P2P-botnets bieden de botnet herders het voordeel van weerstand en veerkracht. Het botnet is namelijk bestand tegen het uitschakelen van verschillende nodes. Er is immers geen centraal punt. Elke bot is namelijk op zichzelf zowel 'client'[23] als (C&C) server. Voor de politie en ISP's is het lastig om te achterhalen waarvandaan het originele commando is verstuurd. Dit kan immers via verschillende bots gegaan zijn. Daarnaast is de lengte van de achterliggende keten niet bekend.

Moderne botnets
Moderne botnets maken gebruik van een combinatie van technieken zoals hierboven beschreven. De communicatie tussen bots onderling of tussen bots en de C&C server gebeurt in veel gevallen versleuteld. Die versleuteling maakt het opsporingsproces moeilijker en helpt voorkomen dat concurrenten het botnet overnemen. Naast versleuteling beschikken veel moderne botnets over aanvals- en verdedigingswapens. Daarmee wordt malware van concurrerende partijen uitgeschakeld. Ook wordt de antivirusindustrie tegengewerkt door het gedrag afhankelijk te maken van de omgeving waarin de bot opereert, of simpelweg door een DDoS-aanval op de onderzoekende partij te lanceren.

Er is een trend zichtbaar waarin botnets steeds toegankelijkere middelen worden en niet langer alleen voorbehouden zijn aan de topcriminelen. Hoewel gesloten botnets die slechts door één groepering gebruikt worden blijven bestaan zijn

[23] Een computersysteem dat een dienst vereist van een ander computersysteem. De client vraagt diensten van een andere computer of computerprogramma, de server. Een werkstation dat bijvoorbeeld de inhoud van een bestand opvraagt bij een file server is een client van de file server.

een aantal bekende botnets in verschillende varianten te koop. Het betreft dan vaak pakketten waar de volledige functionaliteit, bijvoorbeeld voor fraude met internetbankieren, al zit ingebouwd.

Tabel 3.1

Botnets worden een gebruiksgoed		
	2009	2011
SpyEye	Volledig: $4.000	Binary met set-up en injecties: $600
Zeus	Volledig: $10.000	Recompile: 2 voor $380
HTML injecties meegeleverd?	Nee	Op maat gemaakt voor $50 - $75
Anti-security software?	Nee	Eenmalige licence $250, upgrades $10

Bron: RSA 2012 cybercrime trends report

3.5.3 Gebruik van botnets

In paragraaf 3.4 zijn reeds een aantal functionaliteiten van malware genoemd. Bots kunnen dat gebruik schalen. Dat betekent dat de bots als middel ingezet kunnen worden als stap in de keten om het uiteindelijke doel van de high tech crimineel te bereiken. Bijvoorbeeld door gebruik te maken van de reken-capaciteit, opslagcapaciteit, IP-adres of bandbreedte van de bots[24].

Bots zijn vanwege de schaalgrootte ook aantrekkelijk als slachtoffer, zoals bij het genereren van criminele inkomsten door middel van spyware, ransomware en het omleiden van internetverkeer[25].

[24] Zie paragraaf 3.4.1.
[25] Zie paragraaf 3.4.2, 3.4.3 en 3.4.4.

FBI krijgt hulp van Team High Tech Crime bij oprollen botnet

10-11-2011 (uit Nederlandse en Amerikaanse persberichten)

De FBI heeft zeven Estse en Russische cybercriminelen aangehouden op verdenking van het infecteren van miljoenen computers wereldwijd met een DNS changer Trojan.

Deze malware verving de IP-adressen van 15.000 populaire sites (o.a. Netflix en iTunes) door een malafide IP-adres ten behoeve van klik-fraude. Zo werd ruim 10 miljoen euro aan inkomsten uit advertenties gegenereerd. Het onderzoek 'Ghost Click' duurde twee jaar en was voor de FBI 'het meest complexe cybercrime-onderzoek tot nu toe'.
Naast de aanhoudingen heeft de FBI verschillende DNS-servers van de bende uitgeschakeld en door legitieme servers vervangen. Tijdens het onderzoek en bij het oprollen van het netwerk heeft de FBI assistentie gekregen van het Nederlandse Team High Tech Crime, dat onder meer opdracht heeft gegeven voor de bevriezing van vier IP-blokken bij RIPE NCC.

Botnets bieden daarnaast een aantal unieke extra mogelijkheden aan de high tech crimineel. We geven daar hieronder nog twee voorbeelden van. In de praktijk worden deze mogelijkheden door elkaar heen gebruikt en worden continu nieuwe varianten bedacht.

3.5.4 Anonimiteit via SOCKS-proxy

Botnets kunnen van grote waarde zijn voor het afschermen van de identiteit. Er kan verbinding met het internet gemaakt worden via een keten van tussenstations: de bots. Deze tussenstations zijn zogeheten SOCKS-proxies. Hierdoor is alleen het IP-adres van de laatste bot in de keten zichtbaar in achtergebleven sporen, bijvoorbeeld in logbestanden van een bank. Daarnaast is al het verkeer tussen de bots die als proxy worden gebruikt versleuteld. Deze combinatie maakt het werk van opsporingsdiensten tijdrovender en ingewikkelder. Overigens zijn er ook legitieme diensten voor het verhullen van de identiteit voorhanden, bijvoorbeeld TOR[26].

[26] Zie paragraaf 3.8.3.

3.5.5 Distributed Denial of Service (DDoS)

Botnets kunnen ook ingezet worden om specifieke geautomatiseerde werken, zoals websites of mailservers, aan te vallen.

Middels Denial of Service (DoS)-aanvallen kunnen diensten moeilijk of zelfs geheel onbereikbaar gemaakt worden. Er worden massale verzoeken richting het doelwit gestuurd, waardoor het systeem overbelast raakt. Legitieme internetgebruikers hebben op deze manier geen toegang meer tot de service(s). DoS kan naast het zenden van massale verzoeken ook ontstaan door stelselmatig foutieve gegevens aan te bieden, waardoor de beveiligingsinstellingen van een systeem zelf ervoor zorgen dat het systeem (tijdelijk) wordt afgesloten.

Een Denial of Service-aanval kan in beginsel vanaf een enkel systeem worden uitgevoerd. Echter is het in de praktijk zo dat een dienst meestal door diverse systemen tegelijk met dataverkeer wordt bestookt. Men spreekt dan van een 'Distributed' Denial of Service (DDoS)-aanval. Botnet herders hebben met een botnet een ideale structuur om dergelijke aanvallen uit te voeren. Als een server bijvoorbeeld berekend is op een gelijktijdige connectie van 1.000 computers en de botnet herder geeft een botnetwerk van 10.000 computers de opdracht de server simultaan te bezoeken, is de server niet meer bereikbaar voor legitieme connecties. In veel gevallen loopt de server zelfs helemaal vast. Een DDoS-aanval laat zich goed vergelijken met de wegen naar het strand op een warme zomerse zaterdagochtend: door de grote hoeveelheid auto's is het strand niet of slechts zeer moeizaam bereikbaar.

DNS Amplification attack

Een speciale variant van een Denial of Service-aanval is de DNS amplification attack. Bij een dergelijke aanval worden 'recursive DNS name servers' misbruikt door 'spoofed' netwerkpakketten.

Recursive name servers zijn cruciaal voor het functioneren van het internet. Dergelijke servers accepteren namelijk verzoeken van andere systemen om IP-adressen op te zoeken[27]. Om een antwoord te versturen op het verzoek moet de DNS-server weten welke computer, en dus welk IP-adres, het verzoek heeft verstuurd. Het antwoord bevat, afhankelijk van de gestelde vraag, een IP-adres dat overeenkomt met de gevraagde domeinnaam of een foutmelding als geen koppeling gevonden kan worden.

---

[27] Zie voor DNS paragraaf 2.4.

Een verzoek aan een DNS-server is in de regel vrij klein van omvang, ongeveer 60 bytes. In de oorspronkelijke DNS specificatie kon een antwoord maximaal 512 bytes bevatten. Het antwoord van de DNS-server kan dus ongeveer 8,5 maal groter zijn dan de omvang van de vraag. De komst van nieuwe, aanvullende protocollen en technieken die bovenop of naast het bestaande DNS gebouwd zijn zoals IPv6 en DNSSEC maken het zelfs mogelijk voor een DNS-server om antwoorden te geven die een factor 60 (4.000 bytes) tot wel 73 (4.320 bytes) groter zijn dan de vraag.

Een DNS amplification attack kan uitgevoerd worden door bij het versturen van het verzoek aan de DNS-server niet het eigen IP-adres in te vullen maar het IP-adres van de computer waarop de aanval gericht is. De DNS-server ontvangt dan het verzoek van de aanvaller, maar stuurt het antwoord naar de computer van het slachtoffer. Deze ontvangt data van de DNS-server waar hij nooit om gevraagd heeft. De data kan dan een factor 73 groter dan de oorspronkelijk verstuurde data van de aanvaller zijn. Dit is het amplification (versterkings-) aspect van de aanval.

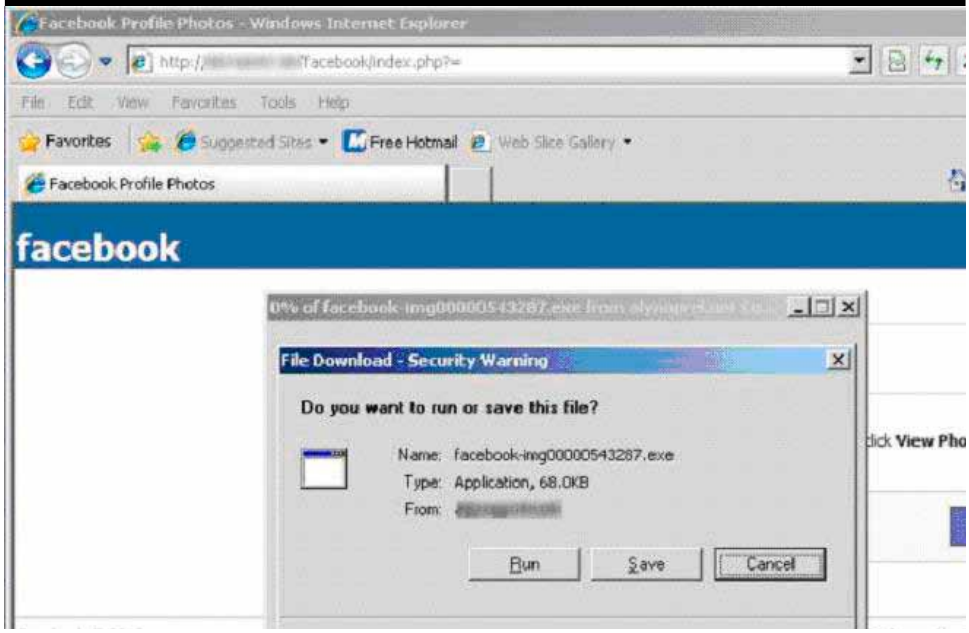
Het op deze manier uitvoeren van één verzoek veroorzaakt geen noemenswaardige hinder, noch voor de DNS-server, noch voor de computer waarop de aanval gericht is. Bij een DNS-aanval worden echter in korte tijd vele van deze korte vragen gesteld aan een of meerdere DNS-servers. Hoe meer vragen gesteld worden, hoe groter de datastroom die op gang komt tussen de DNS-servers en de computer waarop de aanval gericht is. Het slachtoffer ziet daarbij verkeer van de DNS-server afkomen en niet van de aanvaller. Het IP-adres van de aanvaller is voor het slachtoffer niet direct herleidbaar. Eerst moet gekeken worden naar de DNS-servers, waar mogelijk de identiteit van de aanvaller achterhaald kan worden.

3.6 Social engineering

Social engineering is een containerbegrip voor technieken die inspelen op het sociaal-psychologisch gedrag van computergebruikers. In aanvulling op gebruik van geavanceerde technieken word ook in high tech crime ketens misbruik gemaakt van de menselijke factor als zwakke schakel in beveiliging. De kwaadwillende kan zich voordoen als een vertrouwde partij en slachtoffers zo overhalen ergens op te klikken, iets te openen of vertrouwelijk informatie af te geven, met alle gevolgen van dien.

Figuur 3.9

Een screenshot van social engineering via Facebook

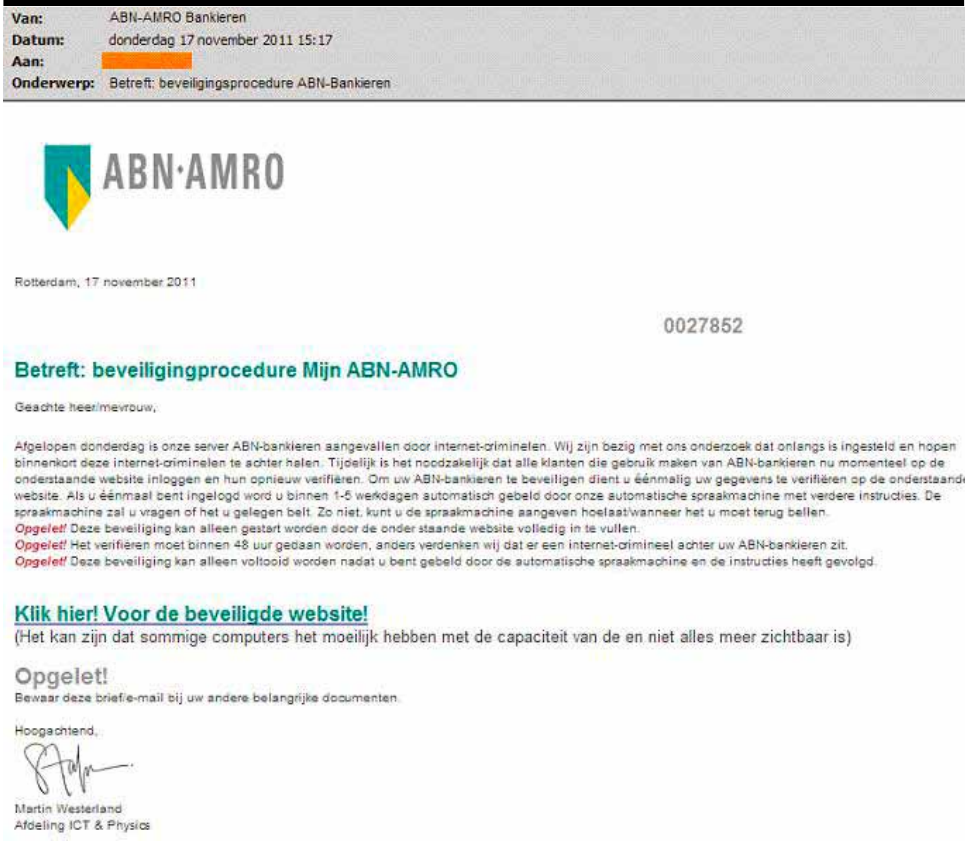


Phishing

Een bekend begrip binnen de context van social engineering is phishing. Deze term verwijst naar het hengelen naar persoonlijke gegevens. Het woord is afgeleid van de termen fishing en phreaking. Fishing staat voor een ouderwetse dieventruc in de fysieke wereld waarbij 'gehengeld' wordt in brievenbussen. Phreaking (dat weer afgeleid is van 'phone' en 'freaking') staat voor het hacken van een telefoonnet, bijvoorbeeld om gratis te kunnen bellen.

Figuur 3.10

Voorbeeld van phishing spam



Van: ABN-AMRO Bankieren
Datum: donderdag 17 november 2011 15:17
Aan: [redacted]
Onderwerp: Betreft: beveiligingsprocedure ABN-Bankieren

ABN·AMRO

Rotterdam, 17 november 2011

0027852

Betreft: beveiligingprocedure Mijn ABN-AMRO

Geachte heer/mevrouw,

Afgelopen donderdag is onze server ABN-bankieren aangevallen door internet-criminelen. Wij zijn bezig met ons onderzoek dat onlangs is ingesteld en hopen binnenkort deze internet-criminelen te achter halen. Tijdelijk is het noodzakelijk dat alle klanten die gebruik maken van ABN-bankieren nu momenteel op de onderstaande website inloggen en hun opnieuw verifiëren. Om uw ABN-bankieren te beveiligen dient u éénmalig uw gegevens te verifiëren op de onderstaande website. Als u éénmaal bent ingelogd word u binnen 1-5 werkdagen automatisch gebeld door onze automatische spraakmachine met verdere instructies. De spraakmachine zal u vragen of het u gelegen belt. Zo niet, kunt u de spraakmachine aangeven hoelaat/wanneer het u moet terug bellen.
Opgelet! Deze beveiliging kan alleen gestart worden door de onder staande website volledig in te vullen.
Opgelet! Het verifiëren moet binnen 48 uur gedaan worden, anders verdenken wij dat er een internet-crimineel achter uw ABN-bankieren zit.
Opgelet! Deze beveiliging kan alleen voltooid worden nadat u bent gebeld door de automatische spraakmachine en de instructies heeft gevolgd.

Klik hier! Voor de beveiligde website!
(Het kan zijn dat sommige computers het moeilijk hebben met de capaciteit van de en niet alles meer zichtbaar is)

Opgelet!
Bewaar deze briefje-mail bij uw andere belangrijke documenten.

Hoogachtend,

Martin Westerland
Afdeling ICT & Physics

Voorbeeld van phishing spam, in dit geval specifiek gericht op het ontfutselen van inloggegevens voor internetbankieren bij klanten van ABN-AMRO.

Alhoewel de meeste phishing spam nog altijd via e-mail verstuurd wordt bestaan er ook varianten waarbij gebruik gemaakt wordt van bijvoorbeeld SMS-berichten (SMiShing), Fax-berichten (phaxing) en berichten via sociale netwerken als Facebook en Twitter.

Een specifieke vorm van phishing is spear phishing. Hiermee wordt een gerichte aanval bedoeld, die gericht is op één persoon of een kleine groep, waarbij gebruik gemaakt wordt van de persoonlijke informatie die reeds bekend is. Standaard phishing is een vorm van een ongerichte aanval: er worden veel

pogingen gedaan met elk een kleine kans van slagen, maar door het volume is het succesvol. Spear phishing daarentegen is een vorm van een gerichte aanval: er worden één of enkele gerichte geavanceerde pogingen gedaan.

3.7 Communicatie

In de voorgaande paragrafen is beschreven welke technieken en middelen gebruikt worden voor de uitvoering van high tech crime. In deze paragraaf worden een aantal belangrijke middelen besproken die door high tech criminelen worden gebruikt om met elkaar te communiceren en te handelen.

3.7.1 Forums

Forums zijn een oude en populaire manier van samenkomen en samenwerken op het internet, zeker niet alleen bedoeld voor criminelen. Het biedt mogelijkheden voor centrale discussie, het aanbieden van producten of diensten en communicatie tussen leden via privé berichten. High tech criminelen, vooral uit Oost-Europese landen, hebben de afgelopen jaren veelvuldig gebruik gemaakt van besloten underground forums (voornamelijk in de Russische taal of in het Engels) om kennis uit te wisselen en met elkaar te handelen. Op dergelijke forums is sprake van een strakke hiërarchie, met beheerders aan de top, gevolgd door moderators die erop toezien of de regels worden nageleefd, verified members, gewone leden en nieuwelingen aan de voet. De status is bepalend voor het vertrouwen dat aan leden geschonken wordt.

Forums bedienen verschillende doelgroepen. De meest interessante binnen deze context zijn cardingforums zoals mazafaka.cc en verified.ru (gespecialiseerd in het verhandelen van creditcardgegevens) en de hackerforums (gespecialiseerd in het bespreken en verhandelen van technieken en middelen om te hacken) zoals unkn0wn.ws en hack-info.ru. Dit betekent niet dat dergelijke forums zich exclusief met deze vormen van criminaliteit bezighouden. De begrenzing van het werkgebied verschilt van forum tot forum. Criminelen combineren vaak het lidmaatschap van diverse forums, soms onder verschillende nicknames.

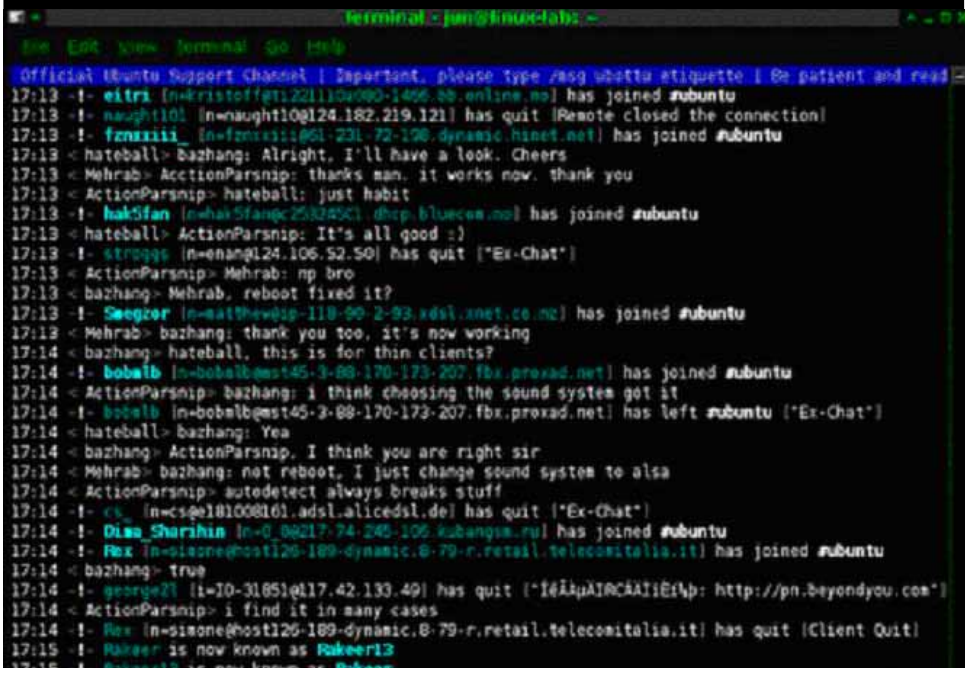
Waar cybercriminelen zich lang veilig hebben gewaand op besloten underground forums is dat sinds opsporingsdiensten actief op dergelijke ontmoetingsplaatsen interveniëren niet meer het geval. Daardoor worden forums tegenwoordig soms nog wel als eerste punt van contact gebruikt, maar vinden uitgebreidere besprekingen en handelsovereenkomsten versplinterd over uiteenlopende communicatiekanalen plaats.

3.7.2 IRC

IRC (Internet Relay Chat) is zoals eerder besproken de oervorm van het hedendaagse chatten op internet. Naast oneigenlijk gebruik van het IRC-protocol[28] voor de aansturing van botnets is IRC al lange tijd een populair communicatiemiddel onder cybercriminelen.

Figuur 3.11

Screenshot van een IRC chat.



3.7.3 Instant Messenging

Instant messenging systemen, zoals Jabber, ICQ, MSN, Torchat, AIM of Skype zijn een uitstekend communicatiemiddel voor criminelen die elkaar al kennen. De communicatie is in de meeste gevallen versleuteld waardoor de inhoud van de communicatie niet eenvoudig afgevangen kan worden.

---

[28] Zie paragraaf 3.5.2.

Een digitale identiteit is vaak erg belangrijk voor cybercriminelen. Instant messengers bieden een goede basis om die identiteit te creëren en te behouden. Bij ICQ is het bijvoorbeeld zo dat een persoon één of meerdere unieke ICQ-nummers (met bijbehorende nickname) heeft. Die crimineel maakt gebruik van zijn contacten lijst (buddy list) en verleent anderen het vertrouwen op basis van eerdere ervaringen met dit unieke contact.

3.8 Verhullen van de identiteit

In de voorgaande paragrafen zijn zowel aanval- als communicatietechnieken aan bod gekomen. Een aantal technieken en middelen voor het verhullen van de identiteit zijn ook al de revue gepasseerd, zoals versleuteling[29]. In deze paragraaf zullen tot slot nog een aantal mogelijkheden benoemd worden.

3.8.1 Proxy servers

Een van de belangrijkste technieken om de anonimiteit te garanderen is het verhullen van het eigen IP-adres. Via dit IP-adres kan immers de locatie van de gebruikte computer worden achterhaald. High tech criminelen hebben verschillende methodes tot hun beschikking om hun IP-adres te verhullen, die in combinatie met elkaar kunnen worden gebruikt. De eenvoudigste techniek is wellicht simpelweg niet vanaf het eigen IP-adres te werken, maar openstaande of gekraakte draadloze netwerken te gebruiken ('war driving').

Voor verdergaande beveiliging loont het om een of meer proxy servers te gebruiken. Proxy servers fungeren als tussenstation bij de communicatie tussen computer en internet. Door het opzetten van een proxy server kunnen high tech criminelen hun eigen IP-adres verborgen houden: al hun internetverkeer herleidt naar het IP-adres van de proxy server. Ze kiezen hierbij bij voorkeur een proxy server in een ander land, om opsporing te belemmeren. Het is mogelijk om een keten van proxy servers te bouwen. Ook bots zijn als proxy server in te zetten[30].

3.8.2 VPN

Een volgende stap is het zoveel mogelijk verhullen van de inhoud van de berichten die over het internet worden gestuurd. Een manier om dat te

---

[29] Zie bijvoorbeeld paragraaf 2.2 en 3.2.5.

[30] Zie paragraaf 3.5.4.

bewerkstelligen is door gebruik te maken van VPN. VPN staat voor Virtual Private Network. Het is een veilige manier om een verbinding te maken met een netwerk of om twee netwerken aan elkaar te koppelen over een publiek netwerk zoals het internet. De gegevens worden hierbij versleuteld over het internet verstuurd. Verkeer dat verzonden is via een zogenaamde VPN tunnel kan dus wel onderschept worden maar niet gelezen.

3.8.3 TOR

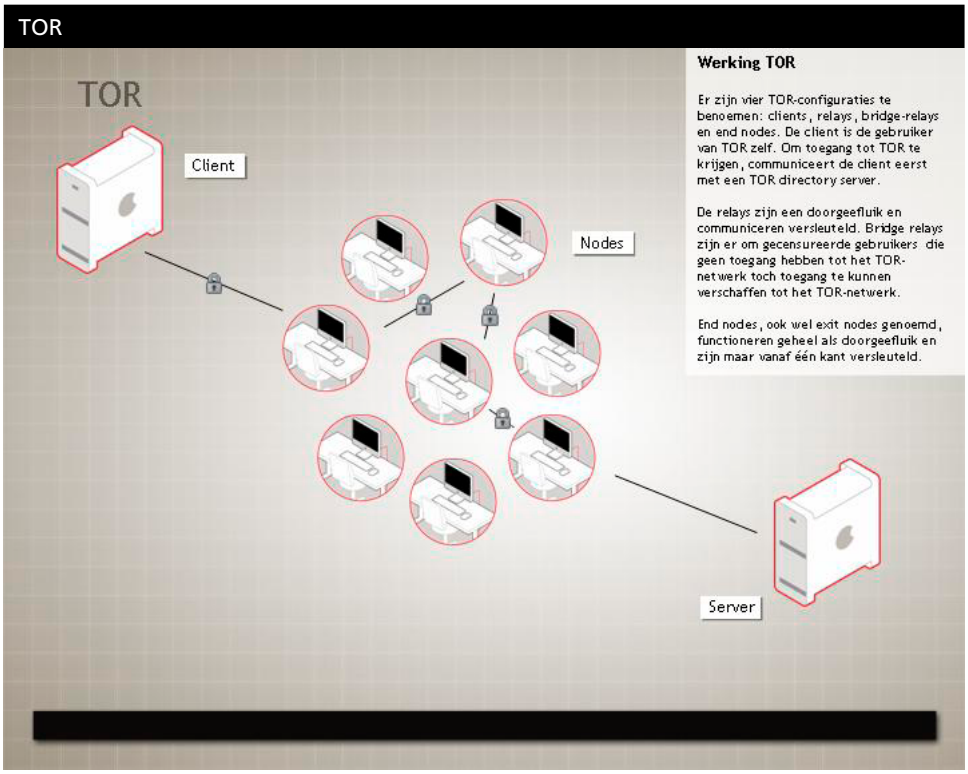
Er bestaan verschillende toepassingen waarbij zowel het IP-adres als de inhoud van het verkeer verborgen blijft. Een voorbeeld daarvan waar de afgelopen periode veel aandacht naar uit is gegaan is TOR (The Onion Router). TOR verschaft gebruikers online anonimiteit door de rechtstreekse verbinding tussen gebruikers en websites te vervangen door ketens van verschillende tussen-stations, de TOR nodes. Dit zijn vooral vrijwillig ter beschikking gestelde PC's. Bovendien is de verbinding binnen de verschillende TOR nodes versleuteld.

TOR biedt ook de mogelijkheid om een server binnen het TOR netwerk op te stellen. Deze server kan dan websites met een .onion extensie aanbieden die alleen via het TOR netwerk, dus anoniem, te bereiken zijn. Ook de locatie van de server zelf blijft zo verborgen. Dit worden daarom ook wel de 'hidden services' genoemd. Uit onderzoek door onder andere het THTC blijken deze vooral gebruikt te worden als ontmoetingsplaatsen voor criminelen. Een digitale TOR-marktplaats, SilkRoad, biedt criminelen bijvoorbeeld de mogelijkheid drugs te kopen, liquidaties te arrangeren of gestolen creditcards te kopen. Het THTC heeft zich in onderzoek Descartes vooral geconcentreerd op de gigantische hoeveelheden kinderpornografisch materiaal dat via TOR verspreid wordt[31].

Het TOR netwerk is opgezet ten behoeve van bescherming van privacy, denk bijvoorbeeld aan communicatie van dissidenten binnen een onderdrukkend regime, maar is hiermee ook onbedoeld facilitair aan criminelen. TOR is overigens niet de enige service van dit type, er zijn verscheidene alternatieven zoals bijvoorbeeld JAP eni2P.

[31] Zie paragraaf 4.6.

Figuur 3.12



3.8.4 Cryptocurrency

De criminelen die op fora zakendoen, zoals op het eerder genoemde SilkRoad, betalen doorgaans niet middels contant of giraal geld. De betaling op criminele ontmoetingsplaatsen verloopt vaak via virtueel geld dat met echte valuta wordt gekocht op online valutamarkten[32]. Dergelijke cryptocurrency, waar bitcoins een voorbeeld van zijn, zorgen ervoor dat de betaler en de ontvanger anoniem kunnen blijven. Bitcoins worden versleuteld van betaler naar ontvanger verzonden en de aanschaf ervan vindt anoniem plaats.

[32] Bijvoorbeeld mtgox.com en bitcoinmarket.com.

3.9 Conclusie

Criminelen in het aandachtsgebied maken vaak gebruik van technologische maar ook menselijke feilbaarheid om op digitale en fysieke manier hun criminele activiteiten te ontplooien. Ten aanzien van high tech crime geldt dat vooral malware en botnets als instrumenten worden ingezet. Botnets worden beschouwd als het 'Zwitsers zakmes' van de cybercrimineel en stonden de afgelopen periode hoog op de onderzoeks- en opsporingsagenda.

De technieken en middelen die high tech criminelen ter beschikking staan voor de uitvoering van hun activiteiten kenmerken zich door een grote mate aan variatie. Zowel qua complexiteit als beschikbaarheid. De wisselwerking tussen die twee kenmerken laat interessante trends zien. Zo zijn veel geavanceerde technieken steeds eenvoudiger en sneller toegankelijk geworden voor een groter publiek.

Een andere belangrijke trend, die high tech crime moeilijker te bestrijden maakt, is het feit dat criminelen steeds meer gebruik maken van anonimiserings-technieken en versleutelingstechnieken. De politie zal manieren moeten vinden om zich hier tegen te wapenen. Niet alleen op het gebied high tech crime. In de reguliere misdaad komt het namelijk ook steeds meer voor dat anonimisering plaatsvindt op manieren die tot voor kort enkel werden toegepast door high tech criminelen. TOR netwerken, VPN's en de betaling met bitcoins zijn hier enkele voorbeelden van.

4
Verschijningsvormen

4.1 Inleiding

In het vorige hoofdstuk zijn de belangrijkste middelen en technieken voor de uitvoering van high tech crime beschreven. Deze basiselementen kunnen op uiteenlopende manieren en ten behoeve van uiteenlopende doelen worden ingezet. In dit hoofdstuk zal daaromtrent meer context gegeven worden. Hiertoe worden een aantal high tech crime verschijningsvormen uitgelicht die als actuele dreigingen worden beschouwd. Daarbij worden voorbeelden aangehaald van aanvallen die zich de afgelopen periode hebben voorgedaan.

We zullen ons beperken tot de volgende verschijningsvormen:
- Aanvallen op de vitale infrastructuren;
- Aanvallen op het financiële stelsel;
- Hacktivisme;
- Bedrijfsspionage;
- Kinderporno.

De laatstgenoemde hoort feitelijk niet in het aandachtsgebied high tech crime thuis. Toch zullen we er aandacht aan schenken vanwege het gebruik van high tech technieken en middelen en daardoor de betrokkenheid van het Team High Tech Crime op dat gebied in recent gedraaide onderzoeken.

4.2 Aanvallen op vitale infrastructuren

De overheid heeft de elektriciteits- en drinkwatervoorziening, de banksector en nog dertig andere producten en diensten aangemerkt als vitaal voor de Nederlandse samenleving. Uitval of ernstige verstoring van deze sectoren kan grote schade tot gevolg hebben. Veel, zo niet alle, van deze sectoren zijn sterk afhankelijk van automatisering. High tech aanvallen kunnen de ICT infrastructuur van dergelijke sectoren onderuit halen, hetgeen kan leiden tot ernstige of kritieke situaties. Om deze reden heeft de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) een cybercomponent toegevoegd aan het Alerteringssyteem Terrorismebestrijding (ATb). Meer nog dan terroristen moeten high tech criminelen in staat worden geacht om vitale infrastructuren succesvol aan te vallen of lam te leggen. De afgelopen tijd hebben we verschillende

voorbeelden gezien van dergelijke aanvallen. De twee bekendste gevallen van de afgelopen jaren zijn de StuxNet-worm en de DigiNotar-hack. Deze voorbeelden zullen verderop in deze paragraaf dan ook apart behandeld worden.

4.2.1 SCADA-systemen

Binnen veel vitale sectoren wordt gebruik gemaakt van process control systemen, en dan met name SCADA-systemen[33]. Industriële systemen worden van oudsher afgeschreven in een periode van decennia, en dat geldt binnen deze omgeving meestal ook voor hardware en software die de aansturing van dergelijke systemen verzorgen. Aangezien het vaak zeer kritische processen betreft, verbieden veel bouwers van dergelijke systemen alle updates van het besturingssysteem van de computers en de installatie van antivirus software. Updates en installaties zouden het primaire proces namelijk voor lange tijd plat kunnen leggen en de bedrijfszekerheid wordt door de mensen in de bestuurskamers vaak als topprioriteit benoemd.

De toenemende automatisering zou niet al te problematisch hoeven zijn zolang de geautomatiseerde systemen niet van buitenaf te benaderen zijn. Vanwege kostenbesparing, maar ook vanwege gebrek aan voldoende geschoold personeel en/of outsourcing van bepaalde onderdelen en beheer, worden SCADA-systemen echter vaker van buitenaf toegankelijk gemaakt. High tech criminelen kunnen profiteren van de gebrekkige scheiding van PA (proces automatisering) en KA (kantoor automatisering) die bedrijven vaak maken. Bijvoorbeeld doordat modems met een rechtstreekse internetverbinding open staan, of simpelweg doordat een monteur een besmette USB-stick insteekt.

4.2.2 StuxNet

In de afgelopen periode zijn veel (potentiële) SCADA-aanvallen bekend geworden. StuxNet is het bekendste voorbeeld en zal in deze paragraaf uitgelicht worden.

StuxNet werd in juni 2010 ontdekt door het Wit-Russische antivirusbedrijf VirusBlokAda. Het bleek om malware ten behoeve van de meest geavanceerde cyberaanvallen ooit te gaan, gericht tegen specifieke SCADA-systemen.

---

[33] Zie paragraaf 2.10.

Analyse leerde dat StuxNet naast andere exploits maar liefst 4 Windows 0-day exploits bevatte, wat betekent dat elke Windows computer geïnfecteerd kon worden. De malware was geprogrammeerd om op de getroffen computer op zoek te gaan naar Siemens' WinCC/Step 7 process control systemen. De malware werd pas actief bij een heel specifieke configuratie. In alle andere gevallen wist de malware zich door toepassing van verschillende technieken goed verborgen te houden. Indien de juiste configuratie werd aangetroffen werden de PLC's[34] besmet en werden er besturingscommando's op uitgevoerd. Deze leidden ertoe dat de motoren van specifieke Siemens centrifuges zichzelf als gevolg van snel wisselende frequenties opbliezen. De meest getroffen installatie lijkt de nucleaire faciliteit te Natanz in Iran te zijn, waar volgens schattingen zo'n 1000 centrifuges het begeven hebben.

Harde bewijzen ontbreken, maar StuxNet wordt door veel experts beschouwd als een voorbeeld van een staatsgesteunde aanval. Om een dergelijke aanval uit te kunnen voeren is veel geld en kennis nodig, want:

- 0-days zijn duur en arbeidsintensief;
- De malware wist zich uitstekend verborgen te houden;
- De malware werd alleen actief in de juiste configuratie;
- Het aanpassen van besturingscommando's in een PLC vraagt specifieke kennis;
- De besmette systemen bevonden zich voornamelijk in Iran (59%) en India (18%)[35];
- StuxNet installeert zijn eigen gesigneerde driver met een vervalst certificaat.

Staatsgesteund of niet, malware ontwikkelaars hebben direct gebruik weten te maken van de bekend geworden exploits en delen van de code van StuxNet.

Duqu

Duqu werd ontdekt in 2011. Uit analyse bleek dat deze malware ontwikkeld moest zijn door dezelfde schrijvers als StuxNet, of door een team dat toegang had tot de broncode van StuxNet. Duqu lijkt zich niet te richten op het vernietigen van process control systemen maar eerder op het verzamelen van informatie. Het botnet zit wel zo in elkaar dat indien gewenst elke willekeurige malware op besmette systemen kan worden geladen.

---

[34] Programmable logic controllers zijn speciale computers die verantwoordelijk zijn voor het realtime aansturen van machines binnen een process control systeem.

[35] Volgens Symantec: Symantec, W32.Stuxnet, Stuxnet: www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99.

Volgens antivirusbedrijf Kaspersky zijn StuxNet en Duqu twee programma's uit een grotere familie van malware en zijn er nog minstens vier andere programma's in gebruik of in gebruik geweest. Daarnaast lijkt de code van deze malware alweer verscheidene jaren oud te zijn.

Het lijkt erop dat we met StuxNet en Duqu buiten het gebied high tech crime treden en meer in de richting van cyberwarfare gaan. Desalniettemin heeft het een golf van inzicht veroorzaakt, zowel voor de aanpak van het aandachtsgebied high tech crime als voor de ontwikkeling van high tech criminelen zelf. Na StuxNet is het aantal bekende kwetsbaarheden van alsmede daadwerkelijke aanvallen op SCADA-systemen sterk toegenomen.

Voorbeelden

In 2011 werd bekend dat in de periode 2007/2008 minstens twee satellieten[36] aangevallen zijn. Daarbij werd via een grondstation in Noorwegen contact gelegd met de satellieten. Alle stappen om de besturing van de satellieten over te nemen zijn daarbij succesvol uitgevoerd. De aanvallers hebben geen commando's naar de satellieten gestuurd.

In 2011 werd malware aangetoffen op het besturingssysteem van de Amerikaanse drones-vloot.[37]

Eind 2011 werd een 0-day bekend gemaakt voor process control software van Siemens. Dit maakte het mogelijk om systemen die deze software gebruikten wereldwijd aan te vallen. Dergelijke systemen waren eenvoudig via een zoekmachine te vinden. Een grootschalige aanval heeft niet plaatsgevonden. In Nederland bleek onder andere TNO deze software te gebruiken, maar daar heeft men de software gelijk gepatcht.

Eind 2011 ontdekten beveiligingsexperts ernstige kwetsbaarheden in de SCADA-systemen van Nederlandse sluizen, bruggen en gemalen.

In veel gevallen hebben de kwetsbaarheden nog niet geleid tot misbruik met ernstige gevolgen. Gezien de verhoogde activiteit lijkt dit slechts een kwestie van tijd.

---

36 Landsat 7 en TERRA EOS AM-1. Zie: U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION - 2011 Report to congress of the U.S.-China economic and security review commission (2011).

37 Op afstand bestuurbare, onbemande vliegtuigen.

Shell vreest cyberaanvallen op olie- en gasinstallaties

12-12-2011 (tweakers net)

Volgens Shell neemt het aantal cyberaanvallen op zijn bedrijfsnetwerken toe. Het Nederlands-Britse bedrijf vreest onder andere de gevolgen als aanvallers erin slagen om kleppen in olie- en gasinstallaties te openen of sluiten. Volgens het bedrijf is er in een dergelijk scenario grote kans dat er mensenlevens verloren gaan. Ook is er volgens Shell aanzienlijke kans op forse schade, vooral aan het milieu.

4.2.3 De DigiNotar-hack

Het belang van certificaten voor het vertrouwen in het internet en de rol van Certificate Authorities (CA's) werd eerder al aangegeven[38]. Het uitgeven van certificaten stelt hoge eisen aan CA's. In 2011 waren er veel (geruchten van) hacks op CA's, zoals Comodo, GlobalSign, VeriSign en natuurlijk de Nederlandse CA DigiNotar. Het vertrouwenssysteem waarop het beveiligde internet gebouwd is, kreeg hiermee een flinke klap en in het geval van DigiNotar waren er daadwerkelijk valse certificaten aangemaakt met alle gevolgen van dien. Het THTC heeft onderzoek in deze zaak verricht.

Op 18 augustus 2011 ontdekte een gebruiker in Iran een frauduleus google.com certificaat. Dit bleek uitgegeven te zijn door DigiNotar. Onderzoek toonde aan dat een hacker ingebroken had op de systemen van DigiNotar. Alle onderzochte computers bleken gecompromitteerd te zijn. Het was aanvankelijk onduidelijk hoeveel valse certificaten aangemaakt waren aangezien hiervan geen administratie was bijgehouden, maar het zou om minstens 500 certificaten gaan. De infrastructuur die zorg droeg voor de uitgifte van certificaten voor de Nederlandse overheid (vallend onder PKIoverheid[39]) bleek ook gecompromitteerd waardoor de validiteit van de certificaten niet langer te garanderen was.

Als gevolg hiervan heeft de Nederlandse overheid het vertrouwen in DigiNotar opgezegd. Browsers en besturingssystemen hebben vervolgens een patch

[38] Zie paragraaf 2.6.

[39] PKIoverheid is de 'Public Key Infrastructure' (PKI) van de Nederlandse overheid. Net als elke andere PKI is het een systeem waarmee uitgiften en beheer van digitale certificaten kan worden gerealiseerd.

uitgebracht waarin DigiNotar van de lijst met vertrouwde CA's af werd gehaald. Bestaande certificaten moesten in grote haast worden vervangen door certificaten van andere CA's, omdat anders de betreffende websites als onveilig zouden worden aangemerkt. Immers, als de uitgever van het certificaat niet meer vertrouwd kan worden, dan kunnen de door deze partij uitgegeven certificaten ook niet meer vertrouwd worden. DigiNotar is als gevolg van dit incident failliet gegaan.

De DigiNotar hack geeft aan dat het internet zelf ook als vitale infrastructuur voor het land moet worden gezien. Een incident op een vitaal knooppunt op het internet zoals een hack op een CA heeft grote gevolgen. Eén van de maatregelen die naar aanleiding van het DigiNotar incident zijn ondernomen door veel partijen is de aanvraag van backup-certificaten bij een tweede CA.

4.3 Aanvallen op het financiële stelsel

Het financiële stelsel is op zichzelf een vitale infrastructuur, maar wordt in deze CBA apart uitgelicht vanwege het feit dat het financiële stelsel tot op heden het meest aantrekkelijke doelwit is voor cybercriminelen. Gezien de focus van deze CBA is het overzicht betrekkelijk beperkt, namelijk tot verschijningsvormen die het THTC in de afgelopen periode op het gebied van high tech crime waargenomen heeft:

- Fraude met internetbankieren;
- Nieuwe vormen van skimmen;
- Hacks op banksystemen;
- Carding.

Voor andere verschijningsvormen van cybercrime gericht op het financiële stelsel verwijzen we naar de CBA Cybercrime Bancaire Sector[40] uitgebracht door de Electronic Crimes Task Force (ECTF).

[40] Electronic Crimes Task Force – Criminaliteitsbeeldanalyse Bancaire Sector (2011).

Electronic Crimes Task Force (ECTF)

De afgelopen jaren heeft het THTC een aantal grote opsporingsonderzoeken gedraaid waarbij banken het doelwit waren van aanvallen. In het kader daarvan zijn positieve ervaringen opgedaan met het laten participeren van vertegenwoordigers van de desbetreffende banken in lopende onderzoeken. Vanuit de banken bestond al langer de behoefte aan structurele samenwerking met de politie voor de aanpak van cybercrime. In april 2011 is een dergelijke samenwerking geïnstitutionaliseerd in de vorm van de Electronic Crimes Task Force (ECTF). Het doel van de ECTF is het voorkomen en bestrijden van (geavanceerde) cybercrime die het vertrouwen van de maatschappij in de integriteit van het financiële stelsel aantast. Deelnemers zijn de drie grootbanken (ING, ABN AMRO en Rabobank), NVB, CPNI.NL (Informatieknooppunt Cybercrime), OM en politie. Samen wordt er gewerkt aan het versterken van de informatiepositie, het ontwikkelen van interventiemaatregelen, en het bijdragen aan opsporing en vervolging. Vertegenwoordigers van de banken en politie werken daartoe nu dagelijks samen in het zogenaamde bankenteam dat fysiek ondergebracht is bij het THTC.

Specifiek op het gebied van skimmen worden dreigingen in kaart gebracht door het Skimmingpoint. Dit is een publiek-privaat samenwerkingsverband geïnitieerd binnen het Programma Aanpak Cybercrime (PAC) van de politie, waar onder andere Equens[41] als expert op dit gebied in deelneemt.

Overigens gaat het hier slechts om verschijningsvormen waarbij sprake is van directe financiële schade aan de kant van slachtoffers en financieel gewin aan de kant van daders. DDoS-aanvallen op financiële instellingen, waar in het algemeen ideologische beweegredenen aan ten grondslag liggen, worden in deze paragraaf buiten beschouwing gelaten en zullen later in dit hoofdstuk aan bod komen.

4.3.1 Fraude met internetbankieren

Aangezien de ICT infrastructuur van banken bovengemiddeld beveiligd is ligt het voor high tech criminelen voor de hand om de computers van (privé en zakelijke) klanten aan te vallen. De bedoeling daarbij is om via de machine van het slacht-

[41] Equens is een grote Europese 'full service payment processor'. Zij zorgen voor de verwerking van girale en cards-gerelateerde betalingen.

offer malafide betalingen te doen en het geld weg te sluizen voordat het slachtoffer of de bank actie kan ondernemen.

Er zijn verschillende mogelijkheden om dit voor elkaar te krijgen, die allemaal gebaseerd zijn op het 'man-in-the-middle' (MITM) principe.

Man-in-the-middle

De aanvaller vervangt als 'man-in-the-middle' de directe communicatie tussen klant en bank door een communicatie klant-aanvaller-bank. Voor de klant gedraagt de aanvaller zich als bank en voor de bank gedraagt de aanvaller zich als klant. Ze vertrouwen elkaar en er worden financiële transacties verricht, die door de aanvaller aangepast worden. Een dergelijke aanval kan op verschillende manieren worden opgezet. In de meeste gevallen is er sprake van het omleiden van internetverkeer[42].

Man in the browser: hierbij is de computer van het slachtoffer besmet. De malware zorgt ervoor dat de webpagina die de bank opstuurt en de webpagina die de klant te zien krijgt niet identiek zijn. De aanvaller gebruikt de gegevens die het slachtoffer invult om frauduleuze transacties uit te voeren. De aanvaller onderschept en manipuleert dus de browser-sessie.

Pharming[43]: deze term staat voor een verzameling methodes om zonder social engineering slachtoffers om te leiden naar een website die identiek is aan de officiële website van de bank. Vervolgens kan vanuit deze website dan een man-in-the-middle aanval worden opgezet. Bij pharming worden vooral technische middelen ingezet, zoals:

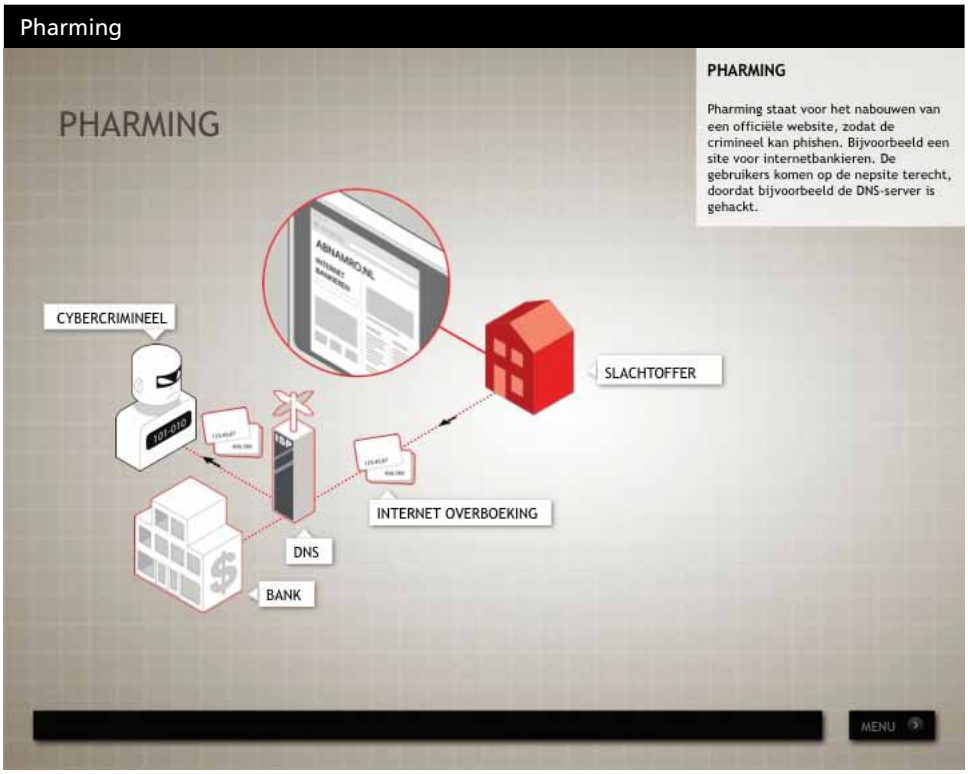
- Besmetting van het slachtoffer via een besmette website, waarna de omleiding op de computer van het slachtoffer zelf plaatsvindt;
- Binnendringen in een DNS server[44], waarna hele groepen slachtoffers omgeleid worden naar frauduleuze websites.

42 Zie paragraaf 3.4.4.

43 Pharming is een samentrekking van farming en phishing.

44 Zie paragraaf 3.4.4.

Figuur 4.1



Om bovengenoemde activiteiten schaalbaar te maken wordt relatief steeds meer gebruik gemaakt van specifiek voor fraude met internetbankieren ontwikkelde malware en botnets. Bekende voorbeelden hiervan zijn Zeus, Torpig, SpyEye en Carberp. Daarbinnen is bovendien een trend naar rendementsverhoging zichtbaar. In sommige gevallen zijn aanvallen specifiek ontwikkeld gericht op de meer vermogende klanten, bijvoorbeeld het JabberZeus botnet gericht op midden- en kleinbedrijven.

4.3.2 Nieuwe vormen van skimmen

Skimmen is het wederrechtelijk kopiëren van pinpas- en / of creditcardgegevens. Door het kopiëren van de magneetstrip en de pincode op het moment van de transactie, wordt het voor criminelen mogelijk een kopie te maken van de pas en met de afgevangen pincode geld op te nemen.

Shimmen is de moderne variant van skimmen. Hierbij wordt geen aanval gedaan op de magneetstrip maar in plaats daarvan wordt het dataverkeer tussen de EMV chip en terminal afgevangen en gemanipuleerd.

Bij betaalautomaten werkt shimmen door een zeer dunne flexibele circuit board (een shim) in de gleuf van de kaartlezer aan te brengen zodat deze tussen de chip van de kaart en de lezer van de betaalautomaat ingeklemd zit. De shim voert vervolgens een man-in-the-middle aanval uit bij transacties van klanten.

Een Nederlands shimgeval

In 2009 maakte Nederland kennis met een geval van shimmen. In het THTC onderzoek Aries bleek dat kaartlezers voor internetbankieren die klanten ter beschikking gesteld kregen voor gebruik in bankshops in Nederland gemanipuleerd werden door criminele samenwerkingsverbanden opererend vanuit Londen en Friesland. Zo wisten ze magneetstripinformatie en pincodes buit te maken.

Eind 2011 heeft de rechter de hoofdverdachte in deze zaak, de 34-jarige Engelsman Clive M., veroordeeld tot een gevangenisstraf van 3 jaar. De bank stelde een schade van meer dan 1,5 miljoen euro geleden te hebben door de shimpraktijken. Uiteindelijk moest Clive M. 168.567,87 euro daarvan aan schadevergoeding betalen van de rechter.

4.3.3 Hacks op banksystemen

Er zijn relatief weinig gevallen bekend van hacks direct op systemen van de bank zelf, waarschijnlijk vanwege de bovengemiddelde beveiliging van banken. Toch gaat er een reële dreiging vanuit. In 2008 heeft het THTC al bijgedragen aan een onderzoek van de FBI waarbij sprake was van gehackte banksystemen. Een internationale groep hackers had een gebruikersnaam en wachtwoord verkregen van een RBS WorldPay server. Van daaruit bleken ze in staat om de centrale versleutelde database te benaderen en gegevens van bankrekeningen te manipuleren. In een periode van 12 uur werd zo in 280 verschillende steden wereldwijd 9 miljoen dollar buitgemaakt. Inmiddels is Eugene A., een Russische hacker die van overwegende betekenis was voor deze aanval, veroordeeld tot 5 jaar cel.

In de afgelopen periode is het vooral bij dreigingen gebleven. Zo waren voornemens bekend van aanvallen op het SWIFT-systeem dat betalingsverkeer

tussen verschillende (internationale) banken faciliteert, maar hebben er voor zover bekend geen geslaagde hacks plaatsgevonden.

Klanten van de bank laten hun gegevens niet alleen achter bij de bank zelf, maar bij uiteenlopende online aanbieders van goederen en diensten. Deze zijn vaak niet goed beveiligd en in de afgelopen periode zijn zeer regelmatig databases met betaalgegevens gehackt.

Bij het hacken van banksystemen hoeft niet alleen gedacht te worden aan de centrale computers van de banken. Het is hackers in Rusland en Oekraïne al in 2009 gelukt het besturingssysteem van een ATM binnen te dringen. Dit is feitelijk een aanval op een process control system[45], maar zou ook beschouwd kunnen worden als een alternatief voor skimming.

4.3.4 Carding

Carding kan worden gedefinieerd als het geheel aan technieken waarmee persoonlijke financiële gegevens verworven, verhandeld en gebruikt worden door criminelen. Het gaat om vormen van identiteitsfraude: persoonlijke data (meestal creditcard- of bankgegevens) van slachtoffers worden onrechtmatig door criminelen gebruikt.

Diefstal
De hierboven beschreven verschijningsvormen zijn belangrijke manieren om dergelijke gegevens te verwerven. De opsomming is echter niet allesomvattend. Denk bijvoorbeeld ook aan de mogelijkheid om door middel van spyware[46] toetsaanslagen af te vangen of betaalgegevens van binnenuit te ontvreemden.

De buitgemaakte gegevens worden vaak niet direct door de daders zelf gebruikt. De data wordt verkocht of er worden diensten van andere partijen ingehuurd om te kunnen cashen.

Handel
Gegevens kunnen verhandeld worden in het levendige carding circuit van de underground economy. Forums[47] zijn nog altijd belangrijke handelsplaatsen voor

[45] Zie paragraaf 4.2.1.
[46] Zie paragraaf 3.4.2.
[47] Zie paragraaf 3.7.1.

carders. De grotere deals worden echter buiten de forums om gesloten, vaak door partijen die elkaar al jaren kennen en vertrouwen.

Gebruik

Het cashen en eventueel witwassen van (potentiële) fraudeopbrengst wordt meestal uitbesteed aan gespecialiseerde organisaties. Vaak is er sprake van money launderers die het proces coördineren en katvangers (drops) die het meeste risico lopen. Kenmerken van deze actoren komen in het volgende hoofdstuk aan bod.

De manier waarop de data omgezet kan worden in cash is afhankelijk van de gebruikte modus operandi en het type gegevens waar het om gaat.

Bij fraude met internetbankieren komt er al direct geld vrij. In dat geval worden bankrekeningen van katvangers, in dit geval geldezels ('money mules') genoemd, gebruikt als eerste ontvanger van frauduleuze transacties. Hierna volgt een vaak onnavolgbaar pad van cashen, overboekingen via money transferorganisaties, betalingen via bitcoins, gebruik van online betaalsystemen als Webmoney en normale overboekingen. Met de invoering van SEPA (Single European Payment Area) kunnen buitenlandoverboekingen naar bijvoorbeeld Eurolanden aan de grens van het SEPA gebied sneller dan voorheen plaatsvinden. Criminelen maken hier dankbaar gebruik van en tegen de tijd dat de fraude wordt ontdekt is het vaak niet meer terug te halen.

In andere gevallen, bijvoorbeeld bij skimmen, dienen gegevens eerst op white plastic gekopieerd te worden voor de productie van valse kaarten. Dit wordt ook wel card present fraude (CP) genoemd en is een intensief proces waar veel resources mee gemoeid zijn.

In het geval van creditcardgegevens vindt bijvoorbeeld niet in alle gevallen fysieke controle plaats en hoeft men voor fraude dus niet noodzakelijkerwijs fysiek over kaarten te beschikken. Dit heet card not present fraude (CNP). Er kunnen bijvoorbeeld online aankopen gedaan worden. Bij bezorging van fysieke goederen worden afleveradressen van katvangers gebruikt en is het proces verder vergelijkbaar met het gebruik van geldezels. Uiteindelijk vindt verkoop van de aangeschafte goederen plaats op sites als eBay. De crimineel is namelijk uit op geld. Goederen zoals fraaie plasmatelevisies zijn slechts een middel om daaraan te komen.

4.4 Hacktivisme

De term hacktivisme is een samenvoeging van hacken en activisme en verwijst naar het inzetten van computers en telecommunicatienetwerken om een ideologisch of politiek doel te bereiken. In de meeste gevallen is daarbij sprake van strafbare feiten (vaak computervredebreuk) en dus cybercrime. Deze beweging kan tot op heden voor wat betreft organisatievorm, werkwijze en vereiste aanpak niet beschouwd worden als high tech crime. In de afgelopen periode was er als gevolg van een aantal daden echter wel sprake van ondermijning en high impact. Bovendien ging het om een enorme toename aan activiteit op dit gebied waardoor het van belang werd geacht dat het THTC hier snel en effectief op in zou grijpen. Om die reden lijkt een korte beschrijving van deze verschijningsvorm, waar in de afgelopen periode zoveel aandacht naar uit is gegaan, wel op zijn plaats in deze CBA HTC.

Binnen het fenomeen is een voor high tech crime relatief nieuwe dadergroep vertegenwoordigd. De motieven voor deze groep liggen namelijk niet op het financiële vlak. In de meeste gevallen is er sprake van ideologische beweegredenen, hierover leest u in het volgende hoofdstuk meer.

Voorbeelden van bewegingen die actief zijn op het gebied van hacktivisme zijn Anonymous, LulzSec en AntiSec. Zij hebben in de afgelopen periode een aantal grootschalige aanvallen uitgevoerd die wereldwijd impact hebben gehad.

4.4.1 Anonymous

Het begrip Anonymous is rond 2003 voortgekomen uit het internetforum 4chan, waar bezoekers anoniem beeldmateriaal kunnen posten en becommentariëren. Op het forum is een protestbeweging ontstaan van een amorfe groep mensen die het gevoel hebben deel uit te maken van een internetsubcultuur. Ze hebben zich in de loop der jaren steeds meer toegelegd op hacktivisme in de vorm van defacements (inbraken op webservers om bestaande webpagina's te vervangen door andere), DDoS-aanvallen en hacks gevolgd door het publiceren van data.

De specifieke overtuiging die volgens hun eigen manifest ten grondslag ligt aan hun activiteiten is het realiseren van een vrije stroom van informatie, vrijheid van meningsuiting en vrijheid van internet. Wat dat precies inhoudt is vaag, aangezien Anonymous niet één samenhangende organisatie is. Binnen Anonymous bestaan verschillende subgroepen; er is geen centraal gezag voor de gehele organisatie. Daarnaast variëren de aanhangers afhankelijk van het doelwit.

Figuur 4.2

Het symbool voor Anonymous is het Guy Falkesmasker

Het aantal aanhangers van Anonymous is enorm toegenomen toen ze zich eind 2010 in 'Operation Payback' op vermeende tegenstanders van WikiLeaks zijn gaan richten. Dit resulteerde in een ongekende opleving van hacktivisme. Veel sympathisanten stelden hun computer en bandbreedte vrijwillig beschikbaar voor DDoS-aanvallen op onder andere Amazon, PayPal, Visa en MasterCard, nadat deze bedrijven besloten donaties aan WikiLeaks niet langer te ondersteunen. De betrokkenen werden vrijwillig onderdeel van een tijdelijk botnet. De aanval werd gecoördineerd met behulp van de LOIC-tool[48].

Eind 2010 heeft het THTC in het kader van onderzoek Talang een zestienjarige Nederlander aangehouden die ervan verdacht werd als kanaalbeheerder het commando gegeven te hebben voor de DDoS-aanval op de website van MasterCard. Toen dit in de pers kwam, werd als reactie een DDoS-aanval op de website van het Openbaar Ministerie (om.nl) uitgevoerd. Hierna is direct weer een Nederlander door het THTC aangehouden die ervan verdacht werd van overwegende betekenis te zijn geweest voor die aanval.

[48] Zie paragraaf 3.5.1.

Politie arresteert DDoS'er Justitie-sites

11-12-2010 (webwereld nl)

De politie heeft een 19-jarige Groningse jongen aangehouden in verband met het platleggen van de site van het Openbaar Ministerie. 'Awinee' zou ook anderen hebben aangezet tot cyberaanvallen.

De arrestatie werd zaterdag aan het eind van de middag verricht in het Groningse Hoogezand-Sappemeer. Volgens het Openbaar Ministerie (OM) is de jongen "vermoedelijk medeverantwoordelijk voor de gerichte cyberaanval" op de website van het Openbaar Ministerie. De Groninger werd in zijn kraag gevat door het Team High Tech Crime.

"Vanachter zijn computer bestookte de man met behulp van hackerssoftware de website van het OM met zoveel digitaal verkeer, dat deze vrijdagmorgen een paar uur moeilijk bereikbaar en korte tijd helemaal onbereikbaar was voor het publiek", bericht het OM. "Uit het onderzoek door de Nationale Recherche is gebleken dat de man, die actief is onder de internet-nickname Awinee, ook andere computergebruikers aanzette om deel te nemen aan de aanval."
Er is beslag gelegd op de computer van de jongen en op een replica van een Italiaans pistool. De politie vermoedt dat hij ook betrokken was bij een aanval op de site Moneybookers afgelopen vrijdag.

Makkelijk opgespoord
De jongen kon makkelijk worden opgespoord doordat de software die hij gebruikte bij het uitvoeren van een Distributed Denial of Service (DDoS)-aanval op de site ook zijn IP-adres meestuurde. "De aanvalssoftware die door sympathisanten van WikiLeaks wordt gebruikt stuurt overigens altijd het IP-adres van de afzenders mee. Meedoen aan dergelijke DDoS-aanvallen is strafbaar. Er staat een maximum gevangenisstraf op van zes jaar", waarschuwt de politie.

Anonymous niet anoniem
Uit gisteren gepubliceerd onderzoek van de universiteit Twente bleek al dat de LOIC-client, gebruikt voor de recente DDoS-aanvallen, het IP-adres van de vurende computer naar de server van de aangevallen site stuurt.

lees verder op de volgende pagina

Dat maakt dat heel veel 'hacktivisten' van de groep Anonymous ironisch genoeg allesbehalve anoniem zijn. De recherche hoeft slechts een blik te werpen in de logfiles en vervolgens de NAW-gegevens uit de CIOT-databank te trekken.

Het OM heeft wel aangegeven niet achter iedereen aan te gaan die de DDoS-tool heeft gebruikt. Het Team High Tech Crime heeft vooral degenen op de het oog die een organiserende rol spelen bij de aanvallen.

Tweede arrestatie
Dit is de tweede DDoS'er die op korte termijn in Nederland is gearresteerd. Afgelopen week hield de politie een 16-jarige jongen aan die sites van MasterCard en Visa aanviel. Dit deed hij omdat de betalingsverwerkers de banden met klokkenluiderssite Wikileaks hebben doorgesneden. Ook Moneybookers weigert nog betalingen aan Wikileaks te verwerken. De DDoS-actie tegen het OM werd opgezet als een reactie op de arrestatie en het nog twee weken in hechtenis houden van de 16-jarige "Jeroenz0r".

4.4.2 LulzSec en AntiSec-NL

LulzSec (ook wel Lulz Security) was een groep hackers die de verantwoordelijkheid claimde voor een aantal 'high profile' aanvallen. Een bekend voorbeeld is de Sony hack in mei/juni 2011 waarbij klantgegevens van een miljoen klanten gecompromitteerd werden. Als motivatie claimt de groep het voor de lol te doen. Lulz is afgeleid van LOL (Laughing Out Loud).

In juni 2011 maakte LulzSec bekend dat ze gingen samenwerken met Anonymous in 'Operation AntiSec': aanvallen op overheden en banken. Het resultaat hiervan was onder meer een DDoS-aanval op SOCA[49], het lekken van vertrouwelijke documenten van de Arizona Department of Public Safety en een hack op de Amerikaanse defensie contractor Booz Allen Hamilton. De persoonsgegevens, inclusief wachtwoorden, die bij de vele hacks werden buitgemaakt zijn in de meeste gevallen gepubliceerd. Opsporingsonderzoeken

[49] Landelijke politie-unit van het Verenigd Koninkrijk, die zich bezighoudt met zware en georganiseerde misdaad.

naar aanleiding van deze acties hebben in Groot-Brittannië en de Verenigde Staten tot een aantal aanhoudingen geleid.

Een groep genaamd AntiSec-NL liet zich inspireren door LulzSec en wist een aantal grote websites te hacken en de verkregen klantgegevens openbaar te maken. In reactie daarop heeft het THTC in het kader van onderzoek Eniac direct 4 Nederlandse verdachten aangehouden. Zij maakten gebruik van de nicknames Ziaolin, Calimero, DutchD3V1L en Time en communiceerden via een niet-openbaar chatkanaal. Bij de aanhouding werden in totaal vijftien computers, externe harde schijven en andere gegevensdragers in beslag genomen.

De belangrijkste constatering is dat het voor hackers relatief gemakkelijk is om systemen binnen te dringen. Default wachtwoorden, onversleutelde klant-gegevens en verouderde software zijn nog steeds de norm. Het is te eenvoudig voor hackers om daar misbruik van te maken. Zowel bedrijven als de overheid zouden zich daarom moeten afvragen of bezuiniging op beveiliging nog wel opweegt tegen de schade van cyberaanvallen. Ook zouden mogelijkheden voor betere richtlijnen voor vulnerability disclosure (bekendmaking van kwetsbaar-heden) verkend kunnen worden.

4.5 Bedrijfsspionage

Bij cyberspionage worden IT-middelen (in combinatie met social engineering) gebruikt om vertrouwelijke informatie van de computer of het netwerk van het slachtoffer buit te maken. Hier kunnen uiteenlopende technieken en middelen uit het in het vorige hoofdstuk beschreven arsenaal voor ingezet worden. Zoals in de introductie aangegeven wordt cyberspionage waarbij staten actoren of slachtoffer zijn in deze CBA buiten beschouwing gelaten. Bedrijfsspionage valt echter wil binnen het aandachtsgebied high tech crime. Er zijn veel signalen dat het aantal gevallen van bedrijfsspionage toeneemt. Vooral grote multinationals zijn aantrekkelijke doelwitten om bedrijfsgevoelige informatie van af te vangen, bijvoorbeeld door (of in opdracht van) concurrenten die daar hun voordeel mee kunnen doen. Het is bekend dat ook in Nederland gevestigde multinationals hier last van hebben. Tegelijkertijd is er weinig bekend over de daadwerkelijke omvang van deze verschijningsvorm. Slachtoffers houden aanvallen vaak onder de radar. Het THTC wil inzetten op een betere informatiepositie en effectief ingrijpen op het gebied van bedrijfsspionage, maar de ervaring leert dat bij bedrijven grote huiver bestaat om aangifte te doen.

4.5.1 APT

APT staat voor Advanced Persistent Threat, het modewoord van 2011 in de wereld van cyber security. Het verwijst naar specifieke vormen van cyber-spionage waarbij de actoren:

- Geavanceerde technologische kennis, technieken en middelen tot hun beschikking hebben (Advanced);
- de tijd nemen om het netwerk van het slachtoffer binnen te dringen (network intrusion) en te leren kennen, en langdurig toegang hebben tot het netwerk teneinde hun doelen te bereiken (Persistent);
- kwaadaardige intenties hebben (Threat).

Hoewel vooral van staten verwacht wordt dat ze zoveel resources in een aanval kunnen steken hoeft dat niet per definitie het geval te zijn. Goed georganiseerde high tech criminele organisaties moeten hier ook toe in staat worden geacht. Het eerder aangehaalde voorbeeld van de RBS WorldPay zaak[50] heeft jaren geleden al uitgewezen waartoe dergelijke dadergroepen in staat zijn.

4.6 Kinderporno

Kinderporno hoort feitelijk niet binnen het aandachtsgebied high tech crime thuis. Desondanks zijn er in de afgelopen periode twee onderzoeken geweest waarin het THTC betrokken was: het Holitna onderzoek naar het netwerk van Robert M. en het Descartes onderzoek naar het verspreiden van kinderpornografisch materiaal binnen het TOR netwerk. De reden voor de inzet van het THTC was het gebruik van technologisch bijzonder geavanceerde technieken en middelen om de materialen te verbergen en de eigen identiteit verborgen te houden. Hoewel kinderporno strikt genomen geen high tech crime is, bleek voor de opsporing wel een hoog niveau van recherche expertise in complexe digitale omgevingen gevraagd te zijn. Naar aanleiding van die inzichten is in 2012 binnen de Landelijke Recherche een het nieuwe team Bestrijding Kinderporno en Kindersekstoerisme opgericht. Dit team beschikt over vergelijkbare resources als het THTC en de teams werken nauw met elkaar samen om kennis en expertise op het gebied van opsporing in complexe digitale omgevingen uit te wisselen.

---

[50] Zie paragraaf 4.3.3.

4.6.1 Kinderpornografisch materiaal op TOR-netwerken

Eind 2010 werd na een tip uit de Verenigde Staten Robert M. aangehouden in wat bekend zou worden als de 'Amsterdamse zedenzaak'. Dit onderzoek wees onder andere uit dat Robert M. onderdeel was van een omvangrijk online netwerk. Dit leidde ertoe dat het KLPD het onderzoek Holitna opstartte met de doelstelling om dit netwerk inzichtelijk te maken en startinformatie te verzamelen voor verscheidene nieuwe opsporingsonderzoeken in binnen- en buitenland.

Tijdens onderzoek Holitna bleek dat makers en verspreiders van kinderpornografisch materiaal dit materiaal volledig anoniem delen op de zogenaamde hidden services op TOR netwerken[51]. Het bleek om enorme hoeveelheden te gaan. Ook werden er ongekend schokkende discussies gevoerd, onder meer over misbruik en het verminken van kinderen.

In onderzoek Descartes heeft het THTC de volgende acties ondernomen:

- Het verzamelen van de betreffende .onion websites (dit gebeurde met behulp van een speciaal geschreven 'crawler': een algoritme die het internet continu afzoekt op zoek naar nieuwe of vernieuwde webpagina`s).
- het, waar mogelijk, toegang verschaffen tot de bewuste sites (op basis van artikel 125i Wetboek van Strafvordering[52]);
- het veiligstellen van het materiaal;
- het, voor zover mogelijk, ontoegankelijk maken van het materiaal (op basis van artikel 125o Wetboek van Strafvordering);
- het kenbaar maken politieaanwezigheid.

Bij het onderzoek moest het THTC relatief vergaande opsporingsmiddelen inzetten en heeft het zorgvuldig met het OM afgewogen of er een wettelijke bevoegdheid voor bestond. Waar nodig is een machtiging van een rechter-commissaris verkregen. In sommige gevallen bleek het gebrek aan wettelijke grondslag een probleem om verder te rechercheren, bijvoorbeeld in de gevallen waarin de PC's van verdachten zich in het buitenland bevonden. Dit onderstreept de behoefte vanuit de politie om de huidige internationale wetgeving omtrent jurisdictie ter discussie te stellen[53].

Het Descartes onderzoek richtte zich noch op de infrastructuur van TOR, noch op de personen of organisaties die de TOR nodes beheren, noch op individuele

---

51 Zie paragraaf 3.8.3.

52 Zie paragraaf 7.4.

53 Zie voor juridische knelpunten paragraaf 7.5.

bezoekers die niet betrokken waren bij de verdachte hidden services. In twee gevallen heeft het onderzoek een directe link naar het IP-adres van een server opgeleverd. In deze gevallen is het bewijsmateriaal direct aan de betreffende bevoegde instanties overhandigd.

4.7 Conclusie

Aanvallen op vitale infrastructuren vormen een realistische en actuele bedreiging voor de maatschappij. Voorbeelden als StuxNet en de hack op DigiNotar hebben dat de afgelopen periode geïllustreerd. Dit heeft geresulteerd in een groeiend bewustzijn. Vooral voor de kwetsbaarheden in SCADA-systemen is veel aandacht geweest. Er zijn gevallen bekend geworden waarbij misbruik uitzonderlijk ernstige gevolgen had kunnen hebben. Vooral staten lijken motieven te hebben om tot dergelijke aanvallen over te gaan, maar ook de dreiging die van high tech criminelen uitgaat op dit gebied moet niet onderschat worden.

Tot op heden lijken zij zich vooral te richten op aanvallen gericht op het financiële stelsel. Deze dreiging heeft inmiddels zodanige vormen aangenomen dat de betrouwbaarheid van het elektronisch betaal- en bankverkeer op (inter)nationaal niveau in het geding komt. Alhoewel de daarbinnen te onderscheiden verschijningsvormen in de afgelopen periode niet wezenlijk veranderd zijn, worden de aanvallen technisch steeds geavanceerder en is er een trend richting rendementsverhoging zichtbaar.

Een verschijningsvorm die zich in de afgelopen periode voor het eerst zo prominent gemanifesteerd heeft is hacktivisme. Deze ontwikkeling illustreert de snelheid waarmee technieken en middelen uit de cyberunderground toegankelijk gemaakt worden voor een breed publiek en de dreiging die van de massa uitgaat wanneer daar redenen voor gevonden worden. Die redenen zijn enorm divers, de komende jaren zullen aanvallen daarom maatschappijbreed gevoeld worden. De politie, maar ook de burgers en het bedrijfsleven zullen hier alert op moeten blijven, fors moeten investeren op cyber security en intensief samen moeten blijven werken ten behoeve van de bestrijding.

5
Actoren

5.1 Inleiding

Criminele technieken en middelen en de verschijningsvormen waarin ze in de praktijk voorkomen zijn voor het THTC vooral relevant als ze gekoppeld kunnen worden aan actoren op wie een opsporingsonderzoek zich kan richten. In de context van deze CBA doelen we met actoren op alle personen of instanties die op enigerlei wijze verband houden met een high tech crime delict. Het kan zowel om daders, ondersteuners als slachtoffers gaan. De focus zal in deze CBA liggen op daders en in mindere mate op ondersteuners. De rol van de slachtoffers past meer in de bredere cyber security context, en zal om die reden nauwelijks aan bod komen.

In dit hoofdstuk wordt zo in de eerste plaats antwoord gegeven op onderzoeksvraag 3 voor het NDB: 'Hoe heeft de aard van het criminele verschijnsel zich ontwikkeld voor wat betreft de kenmerken van personen respectievelijk criminele samenwerkingsverbanden die van (betrokkenheid bij) het plegen daarvan worden verdacht?'.

5.2 Daders

Bij cyber-incidenten is het vaak niet eenvoudig om de dader te achterhalen. Een aanval opgezet door een staat, een private organisatie of een individuele hacker kan er aan de oppervlakte namelijk identiek uitzien. Pas na een significante onderzoeksinspanning kunnen dergelijke actoren onderscheiden worden. Staatsactoren vallen buiten de scope van deze CBA. Gezien het attributieprobleem is het echter waarschijnlijk en zelfs wenselijk dat ondermijnende cyberaanvallen althans in eerste instantie door high tech crime teams onderzocht worden.

Daarnaast is het niet onwaarschijnlijk dat staten of private organisaties voor de daadwerkelijke uitvoering van geavanceerde aanvallen gebruik maken van diensten van zogenaamde beroepscriminelen. Zo kunnen bedrijven, om middels cyberspionage vertrouwelijke informatie van concurrenten te bemachtigen, een professionele hacker uit de cyberunderground inhuren. In deze paragraaf ligt de

nadruk op de actoren die daadwerkelijk uitvoering geven aan de criminele activiteiten.

In het verleden hebben verschillende wetenschappers en specialisten daders geclassificeerd. Bekende voorbeelden hiervan zijn de taxonomie en het hacker circumplex van Rogers[54] en de indeling van Lovet[55]. Deze zijn inmiddels in veel opzichten ingehaald door de snelle ontwikkelingen op het aandachtsgebied. Er verschijnen regelmatig nieuwe classificaties. Deze leveren echter geen eenduidig beeld op en zijn vaak gebaseerd op aannames. Verder wetenschappelijk onderzoek op basis van empirische gegevens is dan ook onontbeerlijk. In aanvulling daarop zou het voor bestrijding interessant zijn beter inzicht te krijgen in socio-economische factoren die tot high tech crime leiden.

In de volgende subparagrafen zal getracht worden daders die de afgelopen periode nadrukkelijk in high tech crime onderzoeken naar voren kwamen te classificeren aan de hand van motieven en niveau van expertise en vaardigheden.

5.2.1 Motieven

De volgende motieven hebben we, in deze volgorde van dominantie, de afgelopen periode nadrukkelijk terug zien komen in high tech crime onderzoeken. Overigens speelt in de praktijk in veel gevallen een combinatie van motieven een rol.

Financieel gewin
Net als bij traditionele vormen van georganiseerde misdaad is financieel gewin een van de meest voorkomende motieven. Denk hierbij bijvoorbeeld aan de eerder beschreven high tech crime aanvallen op het financiële stelsel, zoals fraude met internetbankieren. Dergelijke verschijningsvormen zijn er primair en direct op gericht om geld te verdienen. Activiteiten waar dit motief aan ten grondslag ligt worden dan ook zoveel mogelijk onder de radar gehouden.

Hetzelfde motief speelt (indirect) een rol bij high tech crime gericht op het verbeteren van de concurrentiepositie van een bedrijf. Een voorbeeld hiervan is cyberbedrijfsspionage waarbij bedrijfsgevoelige informatie van een belangrijke concurrent afgevangen wordt om daar zelf voordeel mee te doen. Zoals in het

[54] M.K. Rogers - A two-dimensional circumplex approach to the development of a hacker taxonomy (2006).
[55] G. Lovet - Dirty Money on the Wires (2007).

vorige hoofdstuk al naar voren kwam hebben ook in Nederland gevestigde multinationals hier last van.

Uitdragen van gedachtegoed

Meer dan andere vormen van georganiseerde misdaad speelt bij high tech crime ook vaak het uitdragen van een ideologisch gedachtegoed een rol. Voorheen ging het dan vooral om nationalistisch of religieus gedachtegoed. De afgelopen periode heeft vooral anti-establishment een nieuwe dimensie gekregen. Denk bijvoorbeeld aan de in het vorige hoofdstuk beschreven verschijningsvorm hacktivisme. Bewegingen als Anonymous en de vele afsplitsingen daarvan geven aan te handelen ten behoeve van vrijheid van internet en vrije stroom van informatie (inclusief transparantie van overheden). In het kader daarvan zijn de afgelopen periode veelvuldig DDoS-aanvallen gepleegd op vermeende tegenstanders en werd data uit uiteenlopende gesloten bronnen gepubliceerd. In het belang van de boodschap worden de resultaten van het gebruik van technieken en middelen meestal juist goed zichtbaar gemaakt.

Voor de lol

Bij de verschijningsvormen, zoals hierboven en eerder benoemd, die onder de noemer hacktivisme geschaard worden blijken in de praktijk niet voor alle betrokkenen (dezelfde) ideologische beweegredenen van toepassing te zijn. Er zijn steeds meer betrokkenen, bijvoorbeeld binnen LulzSec[56], die aangeven 'voor de lol' mee te doen. Met dit motief lijkt de dreiging gereduceerd tot die van jonge vandalen zoals we ze ook uit de fysieke wereld kennen. Echter zijn door gebruik van technieken en middelen uit het high tech crime arsenaal de gevolgen van de handelingen die ze met dit motief verrichten vaak veel ernstiger.

Intellectuele uitdaging en/of roem

Van oudsher waren uitdaging en roem dominante motieven voor activiteiten in het aandachtsgebied high tech crime. Echter lijkt dit steeds meer naar de achtergrond te verdwijnen of in ieder geval niet meer het hoofdmotief te zijn van daders die tegenwoordig in high tech crime onderzoeken naar voren komen. Desalniettemin speelt de intellectuele uitdaging nog altijd een rol. Betrokkenen zijn nieuwsgierig en voelen zich gedreven beschermende maatregelen te doorgronden en kraken. Zucht naar roem en daarmee het verkrijgen van een hogere status in de gemeenschap ligt daar vaak mede aan ten grondslag. Ook zonder kwaadaardige intenties, of zelfs met het motief beveiliging te verbeteren,

[56] Zie paragraaf 4.4.2.

bestaat de kans dat een systeem gecorrumpeerd wordt en kan er feitelijk toch sprake zijn van criminaliteit.

Overigens zullen zogeheten white hat hackers die handelen met het motief cyber security te verbeteren en zich daarbij aan de wet houden, geheel buiten beschouwing gelaten worden. Het gaat daarbij immers niet om criminelen, maar om onderzoekers die legitieme werkzaamheden verrichten, zelfstandig of als pentester voor een bedrijf of als digitaal rechercheur bij de politie.

5.2.2 Niveau van expertise en vaardigheden

Het niveau van expertise en vaardigheden binnen dadergroepen loopt uiteen in een continuüm van specialisten naar zogeheten script kiddies. Hoewel we binnen het aandachtsgebied high tech crime voornamelijk specialisten verwachten kan het toch voorkomen dat de schade die veroorzaakt wordt door script kiddies een hoge impact heeft.

Specialisten
Het topsegment van daders achter high tech crime bestaat uit specialisten. Zij worden gekenmerkt door een hoge mate van professionaliteit en innovatie. Deze daders blijven continu vernieuwen door zelf nieuwe codes te schrijven en modi operandi uit te proberen. Denk daarbij aan:

- *Hackers* die door eigen kennis en creativiteit in staat zijn nieuwe manieren te bedenken om in te breken in complexe, relatief goed beveiligde systemen.
- *Ontwikkelaars (Coders)* die malwarepakketten of onderdelen daarvan ontwikkelen. Zij zijn in staat met de nieuwste inzichten op het gebied van software engineering programmatuur te ontwerpen en te bouwen.
- *Botnet herders* die nieuwe botnets creëren en beheren voor eigen gebruik of voor verhuur.

Aanpak van deze dadergroepen kan grote effecten sorteren. De keten wordt dan in een vroeg stadium verstoord doordat toegang tot belangrijke technieken en middelen wordt beperkt. Wel vraagt opsporing van dit type daders in het algemeen meer energie en een hoger niveau van expertise en vaardigheden van rechercheurs.

Script kiddies
Tegenover de groep specialisten staan de script kiddies. Daders binnen deze categorie hebben een relatief laag niveau van expertise en vaardigheden. Het gaat om wannabe-hackers, vaak tieners, die wel in staat zijn om gebruik te maken van verschillende tools maar niet om eigen codes te schrijven.

Ze kopiëren bestaande hacking-scripts zonder deze precies te begrijpen. Overigens hoeven ze vaak niet lang te zoeken naar programmatuur die ingezet kan worden voor hun doeleinden. Er is een groot gratis, open source aanbod te vinden op internet, onder andere bedoeld voor penetratietesten. Ondanks het relatief lage niveau van expertise en vaardigheden moet de dreiging die van deze dadergroep uitgaat niet onderschat worden. Bij een gebrek aan ethos, inzicht in gevolgen van het handelen en andere remmingen kunnen dergelijke daders relatief veel schade aanrichten. Wel zijn deze daders is in het algemeen gemakkelijk op te sporen.

Doorgaans zien we dat specialisten hun vaardigheden als beroepscriminelen inzetten, dat wil zeggen: ten behoeve van financieel gewin. Bij activiteiten waar het uitdragen van gedachtegoed of lol als motief aan ten grondslag hebben we de afgelopen periode overwegend script kiddies terug gezien. Het beeld is echter niet zwart-wit. Ook script kiddies proberen financieel de vruchten te plukken van de mogelijkheden die high tech crime biedt en ook specialisten laten zich weleens verleiden bij te dragen aan bepaalde ideologisch gemotiveerde aanvallen.

5.2.3 Criminele samenwerkingsverbanden

Markt voor beroepscriminelen
Er zijn een aantal opvallende verschillen aan te wijzen tussen samenwerkingsverbanden van zogenaamde beroepscriminelen in high tech crime en in 'reguliere' georganiseerde misdaad.

In de eerste plaats is er in de meestal gevallen geen fysiek, maar uitsluitend online contact. Partners in crime maken hooguit in de rechtbank uiteindelijk kennis met elkaars fysieke identiteit. Fysiek geweld is dan ook zelden aan de orde. Digitaal geweld is daarentegen een zeer gebruikelijke manier om conflicten op te lossen.

Een tweede verschil is dat de structuur veel minder hiërarchisch is. Er is binnen de meeste samenwerkingsverbanden tussen beroepscriminelen in dit aandachtsgebied geen centrale leider aan te wijzen die expliciet macht uitoefent en taken verspreidt over uitvoerders in de periferie van het netwerk. Een administrator van een forum[57] heeft weliswaar tot op zekere hoogte macht over centrale communicatiestromen, maar niet op de samenwerkingsverbanden die

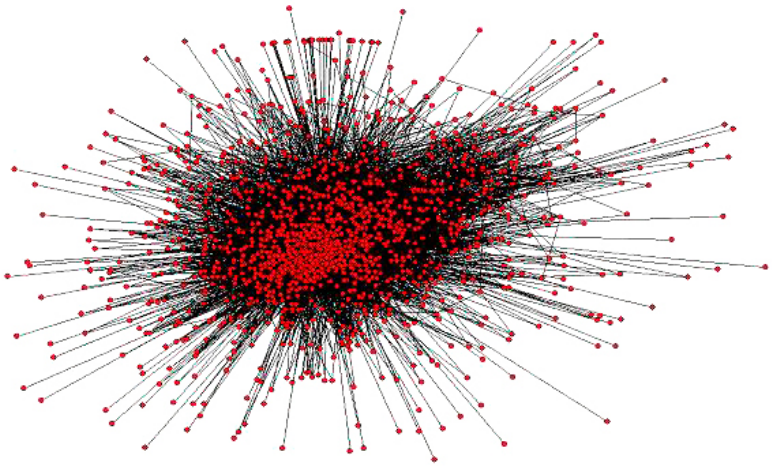
[57] Zie paragraaf 3.7.1.

leden uiteindelijk samen aangaan. De wereld van high tech crime wordt gekenmerkt door zelf-organiserende netwerken van specialisten die hun producten of diensten aanbieden op 'de markt'. Vanwege de complexiteit van het aandachtsgebied bestaan er vele wederzijdse afhankelijkheden en worden er in wisselde relaties kennis en middelen uitgewisseld. Door het aaneenknopen van verschillende resources ontstaat een modus operandi. Vaak heeft geen van de betrokken actoren daarbij overzicht op de totale keten. Een coder van malware heeft bijvoorbeeld in veel gevallen geen zicht op waar verkochte pakketten uiteindelijk voor gebruikt worden.

Dat er geen sprake is van een duidelijke kern-periferie structuur wil niet zeggen dat alle actoren even populair en even succesvol zijn in termen van financieel gewin. Aanbieders van de meest exclusieve en kritieke resources hebben de beste positie op de markt. Vertrouwen is daarbij wel een randvoorwaarde. Zeker sinds bekend (en ondervonden) is dat de politie actief in communicatiekanalen infiltreert valt het voor nieuwelingen niet mee om binnen te komen in de vertrouwensstructuur. Dit vereist een geschiedenis van deals, betalingen en kwaliteitsleveringen.

Figuur 5.1

Resultaat netwerk-analyse



Relatief grote kern en kleine periferie. Bron: forum data veiliggesteld door het THTC

Open ideologische netwerken
De hierboven beschreven kenmerken zijn in mindere mate van toepassing op bewegingen die zich relatief recent prominent in het speelveld gemeld hebben als (afsplitsingen van) Anonymous. Daarbij gaat het om fluïde netwerken vooral bestaande uit wisselende script kiddies. Deze criminele samenwerkingsverbanden staan vaak open voor bijdragen van iedereen. Beschikbare resources en vertrouwen zijn minder van belang. Aangezien het uitdragen van gedachtegoed en/of lol drijfveer voor hun activiteiten zijn speelt concurrentie ook nauwelijks een rol en worden kennis en middelen meer vrijelijk en onvoorwaardelijk gedeeld. Wel zijn er bepaalde sleutelfiguren in deze netwerken aan te wijzen die van overwegende betekenis zijn voor aanvallen. Bijvoorbeeld mensen die de leiding nemen in het initiëren van activiteiten, zoals beheerders van IRC-kanalen.

Gesloten professionele criminele samenwerkingsverbanden
Daar staat tegenover dat er in de afgelopen periode ook steeds meer aanwijzingen zijn voor het bestaan van totaal gesloten professionele criminele samenwerkingsverbanden die zich niet of nauwelijks mengen op de hierboven beschreven 'markt' dan wel 'open hacktivisme netwerken'. Zij lijken langdurig in kleine, besloten groepjes van specialisten specifieke gerichte aanvallen voor te bereiden. Deze criminele samenwerkingsverbanden hebben tot op heden het beste onder de radar van opsporingsdiensten weten te blijven.

5.2.4 Land van herkomst

Hoewel daders achter high tech crime over de hele wereld verspreid zijn komen een aantal herkomstlanden relatief vaak in onderzoeken terug. Daarbij kan een zekere mate van specialisatie waargenomen worden. Opkomende landen, zoals Brazilië en Mexico, zijn nog niet in dit overzicht opgenomen omdat ze in de afgelopen periode nog niet behoorden tot de top van herkomstlanden op het gebied van high tech crime die aan Nederland gelinkt kan worden.

Oost-Europese landen
Al zijn botnet herders tegenwoordig overal wel te vinden, veel van de nieuwste ontwikkelingen op het gebied van botnets komen uit voormalige Oostblok-landen. Daders uit deze landen lijken zich expliciet te hebben toegelegd op aanvallen op het financiële stelsel. Zo lijken Russische high tech criminelen specialisten in het omleiden van internetverkeer om fraude met internet-

bankieren te plegen. Oekraïners spelen een dominante rol in de handel in creditcardgegevens (carding).

Een voor de hand liggende verklaring voor de opvallende rol van deze landen op het gebied van high tech crime is dat het technisch opleidingsniveau relatief hoog is, maar de werkgelegenheid in relevante arbeidssectoren laag. Uit veiliggestelde data van Russischtalige ondergrondse forums blijkt ook dat ze de aanvallen op het financiële stelsel zelf verheerlijken met Robin Hood-verhalen over geld stelen van de rijken (het Westen) voor de armen (het Oosten). Naast deze socio-ecologische factoren die van invloed zijn kunnen zijn bestaat er in veel van deze landen een lage pakkans en mild strafklimaat voor veel high tech crime delicten. Wel lijken er op dat gebied in een aantal van deze landen positieve ontwikkelingen gaande. In het door THTC uitgevoerde botnet-onderzoek Tolling[58] was Armenië graag bereid de hoofdverdachte in eigen land te vervolgen op basis van hun nieuwe cybercrime wetgeving met relatief hoge strafmaten. Nu bijvoorbeeld Rusland zelf ook steeds vaker geraakt wordt door high tech crime, wordt er ook daar steeds meer in de aanpak ervan geïnvesteerd.

China

Malware wordt tegenwoordig door daders overal ter wereld ontwikkeld. Echter blijkt malware die zich in hardware bevindt, vaak uit China afkomstig te zijn. Een voor de hand liggende verklaring daarvoor is dat relatief veel hardware in China geproduceerd wordt. Daardoor is de benodigde kennis voorhanden en bestaat de mogelijkheid tot fysieke toegang voordat de hardware (en daarmee de malware) over de wereld verspreid wordt. Ook cyber(bedrijfs)spionage is een Chinese specialisatie die dit herkomstland in onderzoeken naar boven doet drijven.

West-Europa en de Verenigde Staten

West-Europa en de Verenigde Staten werden in het verleden vaak bestempeld als slachtoffer-landen. Dat is nog steeds het geval. Echter is een groot deel van de hacktivisten die we in de afgelopen periode op de radar hebben zien verschijnen afkomstig uit deze werelddelen.

Nederland

Ook specifiek Nederlanders zijn de afgelopen periode bijzonder actief geweest op het gebied van hacktivisme. In eerste instantie leek het vooral om jonge script kiddies te gaan. De laatste tijd springen echter ook steeds vaker specialisten uit

[58] Zie paragraaf 3.5.1.

de gevestigde Nederlandse hacker scene in het oog door op de een of andere manier bij dergelijke bewegingen aan te sluiten.

Nederland neemt echter een nog veel prominentere positie in waar het gaat om het faciliteren van de infrastructuur die nodig is voor de uitvoering van high tech crime. Hier zullen we in de volgende paragraaf meer aandacht aan besteden.

5.3 Ondersteuners

Een niet onbelangrijke groep actoren binnen het aandachtsgebied high tech crime zijn de ondersteuners, ook wel facilitators genoemd. Zij maken de criminele activiteiten mede mogelijk: ongewild of willens en wetens.

Men kan betogen dat vrijwel iedereen die zich bezighoudt met het doorontwikkelen van het in hoofdstuk 2 beschreven technologische landschap ongewild indirect mogelijkheden creëert voor high tech crime.

Inzoomend op specifiek de logistieke rol van Nederland in het aandachtsgebied hebben we in vorige CBA's HTC al moeten concluderen dat Nederland vanwege de goede infrastructuur aantrekkelijk is voor high tech criminelen. Specifiek de diensten van Nederlandse hosting providers zijn bijzonder populair in de cyberunderground. Deze partijen worden daarom uitgelicht als belangrijke ondersteuners voor high tech crime.

5.3.1 (Bulletproof) Hosting providers

Hosting providers kunnen bewust of minder bewust high tech crime faciliteren. Zonder de diensten van hosting providers zijn veel verschijningsvormen immers niet mogelijk. De meeste hosting providers hanteren een model van subcontracting (reselling), waardoor zij geen zicht hebben op de feitelijke gebruikers van hun infrastructuur. Het gebeurt dan ook dat een malafide subcontractor een heel rek doorverhuurt aan high tech criminelen. Een betere controle zou dit probleem wellicht kunnen verminderen. Voor veel hosting providers geldt dat ze meer verantwoordelijkheid zouden kunnen nemen ter voorkoming van misbruik van hun diensten. In sommige gevallen zou dat het afsluiten van de meest lucratieve klanten kunnen betekenen.

Er zijn hosting providers die een stap verder gaan, door bewust criminele activiteiten te faciliteren. Zij bieden bulletproof hosting (BPH) aan in de cyberunderground: een vorm van hosting waarbij volledige anonimiteit wordt

geboden aan de gebruiker in ruil voor goede financiële tegemoetkomingen. Dergelijke ondersteuners zorgen ervoor dat de identiteit van criminelen die gebruik maken van hun diensten verborgen blijft voor opsporingsdiensten. Deze groep ondersteuners kan direct als (mede)dader worden aangemerkt.

5.3.2 Financiële ondersteuners

Bij veel verschijningsvormen spelen ook financiële ondersteuners een rol. Zoals in het vorige hoofdstuk[59] reeds naar voren kwam zijn ook bij deze processen een aantal legitieme diensten onbedoeld facilitair, zoals de money transfer organisaties Western Union en MoneyGram en online betaalsystemen als Webmoney. Criminele dienstverleners die het proces van cashen en eventueel witwassen van fraudeopbrengsten verzorgen (zogeheten money launderers) maken misbruik van dergelijke diensten. Daarbij speelt het gebruik van katvangers (in de cyberunderground drops genoemd) een belangrijke rol. Drops stellen hun bankrekening beschikbaar en verzorgen transacties (in dat geval wordt meestal gesproken over geldezels) of stellen hun huisadres beschikbaar als afleveradres voor goederen die vervolgens verkocht kunnen worden. De namen geven al aan dat deze mensen geen hoge status hebben in de cyber-underground. In de meeste gevallen maken ze daar niet eens deel van uit en worden ze (onder valse voorwendselen) geworven en aangestuurd door money launderers, in enkele gevallen in de veronderstelling dat ze met een legitieme werkgever te maken hebben. Geldezels die ingezet worden om met valse kaarten geld uit betaalautomaten te halen maken daarentegen nadrukkelijker en bewuster deel uit van de keten.

De afgelopen periode lag de focus in de onderzoeken van het THTC en daarmee ook in deze CBA relatief meer op de technische aspecten dan op de financiële aspecten van high tech crime ketens. Daar gaat met de komst van financieel rechercheurs als onderdeel van de uitbreiding van het team verandering in komen. Daarbij zou het ook interessant zijn om te onderzoeken of en waar in deze delen van high tech crime ketens sprake is van overlap met andere vormen van georganiseerde misdaad en waar onder- en bovenwereld elkaar ontmoeten.

---

[59] Zie paragraaf 4.3.4.

5.4 Slachtoffers

De slachtoffers zijn de benadeelden van de criminaliteit. Het kan hier net als bij daders om staten, private organisaties en burgers gaan. Zij kunnen het doelwit van de aanval zijn, maar dit is niet noodzakelijk. Bij een geslaagde hack op een bedrijf is het bedrijf het primaire slachtoffer. Wanneer daarbij gegevens gestolen worden van klanten en/of klanten geen toegang meer hebben tot bepaalde diensten zijn burgers secundaire slachtoffers. Bij infectie van hun PC zijn burgers wel het primaire doelwit. Kenmerkend voor het overgrote deel van de aanvallen op burgers is dat zij geen specifiek doelwit zijn: de aanval is niet persoonlijk maar vindt slechts plaats omdat deze mogelijk is, bijvoorbeeld omdat het betreffende slachtoffer zijn computer niet met de laatste updates gepatcht heeft.

5.5 Conclusie

In dit hoofdstuk werd een voor de politie zeer relevant aspect van het aandachtsgebied beschreven: actoren. Daarbij is vooral aandacht uitgegaan naar dadergroepen, oftewel: de personen of criminele samenwerkingsverbanden achter de criminele technieken en verschijningsvormen.

Er kan geconcludeerd worden dat de motieven, het niveau van kennis en expertise en de vorming van criminele samenwerkingsverbanden in de kern van de high tech crime underground niet wezenlijk veranderd is in de afgelopen jaren. Financieel gewin blijft een dominant motief en het is nog steeds een betrekkelijk kleine groep specialisten die de motor van nieuwe ontwikkelingen op het gebied van high tech crime vormt. Daders uit Oost-Europese landen komen nog altijd vaak in onderzoeken terug, vooral bij fraude met internetbankieren en handel in creditcardgegevens, maar tegenwoordig zijn er wereldwijd specialisten die zich als beroepscriminelen toeleggen op high tech crime. In Nederland lijkt wat dat betreft vooral in de hoek van facilitators gezocht te moeten worden, specifiek naar bulletproof hosting providers.

De in het vorige hoofdstuk benoemde trend van het toenemende gebruikersgemak van technieken en middelen uit de wereld van high tech crime heeft er wel toe bijgedragen dat een relatief nieuwe dadergroep zich op het speelveld gemeld heeft. Het gaat voornamelijk om script kiddies uit de VS en West-Europa met ideologische beweegredenen. Veel meer dan beroepscriminelen staan zij open voor samenwerking met iedereen die enigszins hetzelfde doel voor ogen heeft. Beschikbare resources en vertrouwen lijken minder van belang.

Daartegenover staan totaal gesloten professionele criminele samenwerkingsverbanden die langdurig met elkaar samen lijken te werken om gerichte aanvallen voor te bereiden. Hier kunnen verschillende beweegredenen aan ten grondslag liggen en deze dadergroepen hebben tot op heden het beste onder de radar van opsporingsdiensten weten te blijven.

6
Omvang

6.1 Inleiding

In de voorgaande hoofdstukken stond een kwalitatieve beschrijving van het aandachtsgebied centraal. In dit hoofdstuk is er aandacht voor het kwantitatieve gedeelte. Getracht wordt een indruk te geven van hoe de omvang van het criminele verschijnsel zich ontwikkeld heeft in termen van hoeveelheid van activiteit. Daarmee wordt antwoord gegeven op de tweede onderzoeksvraag voor het NDB.

Accurate en vergelijkbare kwantitatieve data met betrekking tot het aandachtsgebied is tot op heden helaas nog bijzonder schaars. Daarom zullen we ons voornamelijk op trends richten die zich (eerder) wel in cijfers (lieten) uitdrukken. Op die manier kunnen er toch onderbouwde uitspraken over de ontwikkeling van het aandachtsgebied in termen van omvang worden gedaan.

6.2 Statistieken bij criminele technieken en middelen

In hoofdstuk 3 is geconstateerd dat vooral exploits, malware en botnets een belangrijke rol spelen in de uitvoering van high tech crime. Om een indruk te geven van de schaalgrootte van high tech crime is er daarom in deze paragraaf aandacht voor statistieken die op deze gebieden voorhanden zijn.

6.2.1 Exploits

In het Cybersecuritybeeld Nederland 2011 wordt beschreven dat het aantal nieuwe kwetsbaarheden dat in standaardsoftware werd gevonden de laatste jaren is gestabiliseerd. In 2010 was er zelfs voor het eerst sinds lange tijd sprake van een daling: van 5535 gemelde kwetsbaarheden in 2009 naar 4365 in 2010. Desalniettemin gaat het nog altijd om gemiddeld 12 meldingen van nieuwe kwetsbaarheden per dag[60]. Bovendien geeft deze trend niet per definitie aan dat er daadwerkelijk sprake is van verbeterde beveiliging. Het kan ook zo zijn dat

[60] GOVCERT.nl - Cybersecuritybeeld Nederland, december 2011, p. 40.

een bepaald aantal kwetsbaarheden wel bekend is in kleine kring, maar niet publiek wordt gemaakt.

Overigens is er voor wat betreft het aantal ontdekte kwetsbaarheden in de zogeheten SCADA software voor industriële systemen juist sprake van een flinke stijging. In 2010 werd er gemiddeld 1 nieuwe kwetsbaarheid per maand in de CVE-database[61] opgenomen. In 2011 werden daar gemiddeld 5 kwetsbaarheden per maand aan toegevoegd. Voor veel van deze kwetsbaarheden bestaan (proof of concept) exploits. Het totale aantal exploits is onbekend, maar dit is waarschijnlijk hoger. Het betreft immers een relatief nieuw aanvalsterrein, waardoor het aantal 0-days naar verwachting groot is. Er zijn gerichte pakketten in omloop die exploits voor SCADA-systemen bundelen, zoals het SCADA+ pack van het Russische GLEG. Eind 2011 waren 96 SCADA kwetsbaarheden publiek bekend[62].

6.2.2 Malware

Aantal malwarepaketten

De Shadowserver Foundation houdt het aantal verschillende malwarepaketten (samples/binaries) bij en gebruikt daarbij een methode om dubbeltelling door polymorfie[63] zoveel mogelijk te voorkomen. Figuur 6.1 toont een geleidelijke toename in 2011 van ongeveer 40% ten opzichte van 2010.

61 De CVE-database is een genummerde lijst van alle gemelde ICT-kwetsbaarheden wereldwijd.
62 Bron: www.scadahacker.com.
63 Zie paragraaf 3.3.2.

Figuur 6.1

Aantal malwarepakketten 2011

Bron: Shadowserver Foundation

Voorgaande jaren toonden de statistieken een sterkere groei. In de CBA 2009 werd nog naar een toename van 60% verwezen.

De afvlakking van de groei is hoopvol, maar hoeft op zichzelf nog niet veel te betekenen. Zo is er al jaren een trend naar meer gerichte aanvallen zichtbaar. De standaard manier om nieuwe malware te vangen is met behulp van zogenaamde honeypots: machines die zich moedwillig laten infecteren. Deze vangen echter alleen ongerichte malware op. Het is dus mogelijk dat er steeds meer (gerichte) malware wordt gemist in de telling. Omdat dit type malware poogt alleen de doelmachines te infecteren blijft het veel langer onder de radar.

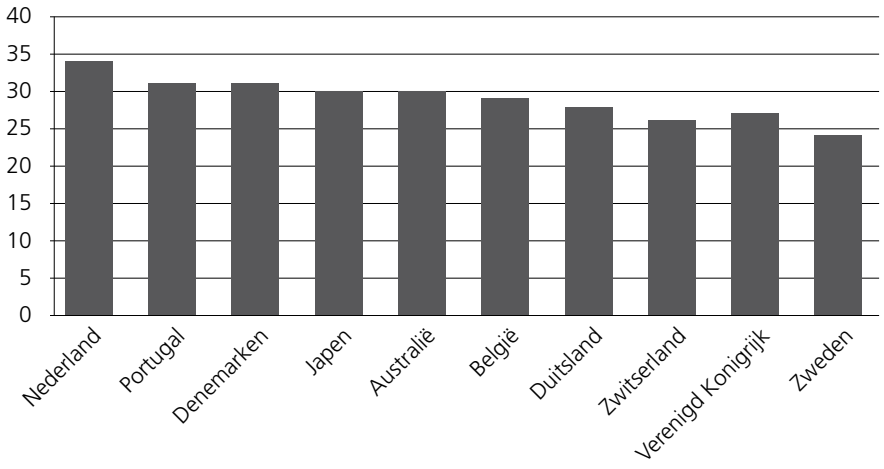
Aantal infecties in Nederland

Statistieken voor het aantal met malware geïnfecteerde computers in Nederland geven geen eenduidig beeld. Infecties zijn namelijk moeilijk meetbaar, het zijn momentopnames en partijen kunnen er belang bij hebben om cijfers op een bepaalde manier naar buiten te brengen. Antivirusbedrijven presenteren bijvoorbeeld vaak schokkendere cijfers dan software-ontwikkelaars. Zij verdienen immers geld aan die dreiging, terwijl software-ontwikkelaars erdoor op hun kwetsbaarheden gewezen worden.

Volgens onderzoek van antivirusbedrijf Pandalabs[64] was in 2011 ongeveer 34% van alle computers in Nederland besmet met malware. Daarmee behoort Nederland tot de top tien landen met de laagste infectiegraad ter wereld. Echter zou dit dus betekenen dat nog steeds ruim één op de drie computers op eniger wijze geïnfecteerd was met malware. Overigens heeft Pandalabs niet verantwoord hoe deze cijfers waren vergaard[65].

Tabel 6.1

Overzicht van met malware geïnfecteerde computers per land



Bron: Pandalabs 2011

Software-ontwikkelaar Microsoft laat een totaal ander beeld zien. Volgens diens Security Intelligence Report[66] werd in het eerste kwartaal van 2011 4,6% en in het tweede kwartaal 5,3% van de PC's in Nederland draaiend op Windows, verschoond van malware door hun Malicious Software Removal Tool.

64 Panda Labs - Annual Report 2011.

65 Zie: http://www.security.nl/artikel/40144/1/33%25_Nederlandse_pc%27s_besmet_met_malware.html.

66 Microsoft - Microsoft Security Intelligence Report, Volume 11 (2011), p. 126.

Uit wetenschappelijk onderzoek[67] blijkt dat in de periode van januari 2009 tot juni 2010 1,1 miljoen IP-adressen gerelateerd leken te zijn aan geïnfecteerde machines in Nederland. Dat zou wijzen op 5-10% van alle klanten van Nederlandse Internet Service Providers (ISP's). Aangezien deze aantallen uit een beperkte dataset komen zal het totale aantal in werkelijkheid hoger liggen.

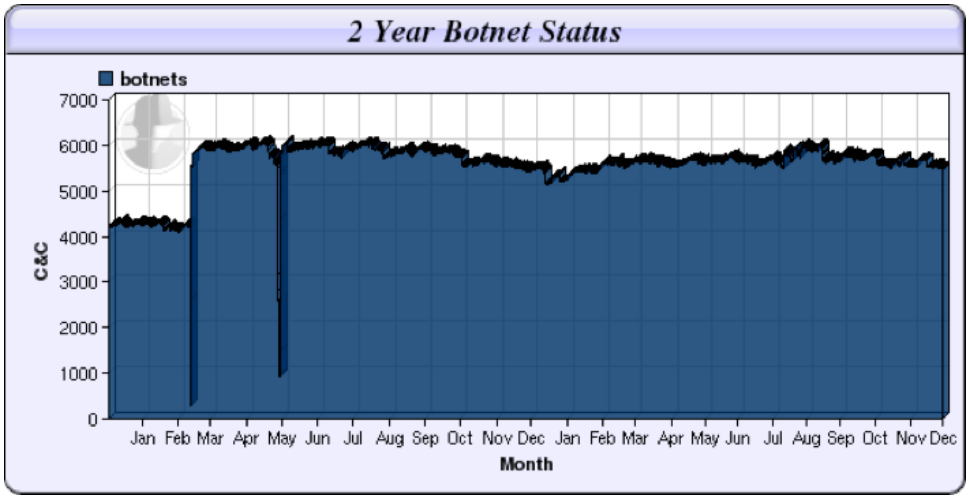
6.2.3 Bot(net)s

Totaal aantal botnets

Zoals eerder uitgelegd[68] vindt de aansturing van botnets van oudsher plaats met behulp van C&C servers. De Shadowserver Foundation[69] monitort het aantal actieve C&C's. In figuur 6.2 zijn de aantallen voor 2010 en 2011 weergegeven.

Figuur 6.2

Aantal C&C servers 2011



Bron: Shadowserver Foundation

[67] Van Eeten e.a. 2011, Internet service providers and botnet mitigation; A Fact-Finding Study on the Dutch Market(2011),p. 40.

[68] Zie paragraaf 3.5.

[69] De Shadowserver foundation bestaat uit vrijwilligers die werkzaam zijn in de cyber security industrie en houdt informatie bij over botnet- en malware-dreigingen.

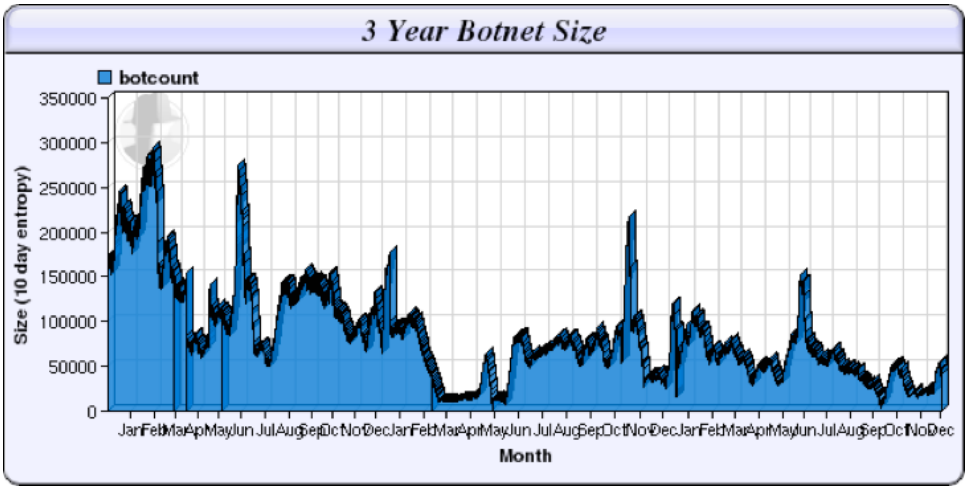
In tegenstelling tot de statistieken voor malware is er volgens de data van Shadowserver geen sprake van een toename in het aantal C&C's. Dit lijkt in tegenspraak met het algemene beeld dat de afgelopen jaren het aantal botnets is toegenomen. Een verklaring hiervoor kan zijn dat de afgelopen jaren een verschuiving heeft plaatsgevonden van C&C botnets naar peer-to-peer botnets.

Omvang van de botnets

Om een indicatie te geven van de omvang van botnets houdt de Shadowserver Foundation ook het totale aantal bots (geïnfecteerde computers) bij dat met de gemonitorde C&C's in verbinding staan bij. In figuur 6.3 zijn de cijfers voor 2011 weergegeven.

Figuur 6.3

Aantal actieve[70] bots 2011



Bron: Shadowserver Foundation

De onregelmatigheid in de aantallen heeft waarschijnlijk vooral te maken met het feit dat alle bots behorende bij inactieve C&C servers tijdelijk niet meegeteld worden tot het moment dat de C&C weer actief is. Dat betekent dat het ontmantelen van C&C servers vaak wel tijdelijk effect heeft, maar als ze later (op

[70] '10 day entropy' wil zeggen dat bots die 10 dagen niet actief zijn geweest niet meer worden meegeteld tot het moment dat ze weer actief zijn.

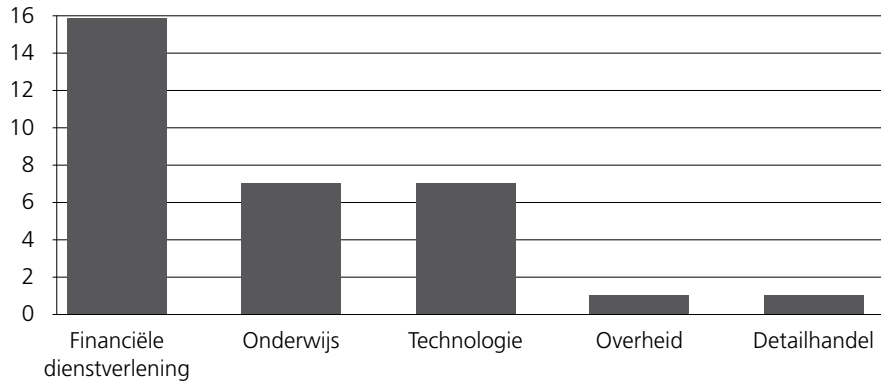
een andere locatie) weer actief kunnen worden is het effect alweer tenietgedaan.

6.2.4 Dossieranalyse THTC

De dominante rol die de eerder uitgelichte technieken en middelen in het aandachtsgebied spelen blijkt ook uit het dossieronderzoek op data van het THTC voor het 'Data Breach Investigations Report 2011' (Verizon). In het kader van dat onderzoek zijn alle dossiers (vanaf de oprichting van het team in 2007) waarbij op de een of andere manier sprake was van een (potentieel) datalek geanalyseerd. Daaruit bleek hacken (met name het gebruik van gestolen wachtwoorden en exploits) het meest voor te komen. In 24 (van de 32) gevallen bleek sprake te zijn van gebruik van malware/botnets.

Figuur 6.4

Meest gebruikte technieken (totaal aantal datalekken / totaal aantal records)



Bron: Dossiers THTC zoals naar verwezen in DBIR 2011

Het grote verschil tussen de bovenstaande cijfers en de cijfers die in de vorige paragrafen naar voren kwamen, is gelegen in de relevantie daarvan voor het aandachtsgebied. De cijfers uit de THTC dossiers hebben namelijk vooral betrekking op high tech crime zaken, maar slechts op een klein deel van het totaal. Op basis daarvan kunnen geen conclusies getrokken worden met betrekking tot de totale omvang. De Shadowserver statistieken geven wel een zo goed mogelijke indicatie van het totale arsenaal, maar deze malware-

pakketten en botnets worden in de praktijk niet uitsluitend ingezet voor high tech crime, maar ook voor andere vormen van cybercrime.

6.3 Statistieken bij verschijningsvormen

In deze paragraaf wordt een poging gedaan om vanuit een ander perspectief een indicatie te geven van ontwikkelingen in de omvang van high tech crime. Namelijk door verschijningsvormen die in hoofdstuk 4 reeds kwalitatief beschreven zijn nu in termen van frequentie, incidentie en prevalentie proberen te duiden. Helaas is dat slechts tot op zekere hoogte mogelijk. Hieronder zal toegelicht worden hoe dat komt en vervolgens zullen de statistieken die wel beschikbaar zijn aangedragen worden.

6.3.1 Gebrek aan accurate cijfers

Aangiftes bij politie

Op dit moment ontbreekt het de politie aan centraal inzicht in prevalentie van high tech crime in Nederland. Burgers zijn zich vaak niet bewust van het feit dat een incident waar ze bij betrokken waren wijst op high tech crime. Bovendien ontbreekt het de politie aan gespecialiseerde (digitale) intake om relevante incidenten toch boven water te krijgen en eventueel te kunnen bundelen en opschalen. Dat resulteert in weinig vertrouwen in opvolging en daarmee in een vicieuze cirkel.

Ook bedrijven doen zeer zelden aangifte en lijken weinig vertrouwen te hebben in opvolging. Voor internationaal opererende bedrijven komt daar nog de vraag bij in welk land aangifte gedaan moet worden. Bovendien zijn veel bedrijven bang voor imagoschade als de zaak in de openbaarheid komt. Een onderzoek dat KPMG in 2012 verrichtte onder ruim 170 bestuurders toonde aan dat bijna de helft van alle Nederlandse bedrijven in 2011 op enige manier slachtoffer was van cybercrime[71]. Zo werden er bijvoorbeeld servers gehackt, waarop persoonsgegevens konden worden buitgemaakt. 60 procent van aangevallen bedrijven geeft aan dat de schade zich jaarlijks beperkt tot een bedrag van 100.000 euro, bij ruim 10 procent gaat het om een schadebedrag boven de 1,5 miljoen euro.

De werkelijke schade blijft overigens gissen, vanwege de beperkingen van detectiemethodes en het eerder genoemde gebrek aan aangiftebereidheid. Dat

[71] KPMG – Nieuwe perspectieven vragen om actie, een genuanceerde visie op cybercrime (2012).

laatste geldt inmiddels niet meer voor de Nederlandse banken. Zij maken tegenwoordig juist omwille van hun reputatie incidenten steeds sneller kenbaar aan de politie. Daar zijn de afgelopen jaren steeds vaker high tech crime opsporingsonderzoeken uit voort gekomen.

Schadecijfers

Beschikbare cijfers bestaan in de meeste gevallen uit schattingen van schade gebaseerd op rapportages van de slachtoffers zelf. Dergelijke cijfers blijven hoe dan ook beperkt inzicht geven, omdat ze afhankelijk zijn van de waarneming (en perceptie) van de bevraagden. In veel gevallen ontgaat slachtoffers het zicht op aanvallen en de schade die het tot gevolg heeft. Er ontbreekt informatie, er bestaat onvoldoende overeenstemming over de grenzen van het fenomeen en de schade wordt op verschillende manieren gemeten. Het kan gaan om:

- Directe schade: het ontvreemde bedrag (de som van de gelden die niet teruggehaald konden worden). Bijvoorbeeld het geld dat door fraude met internetbankieren daadwerkelijk van rekeningen af is geschreven.
- Misgelopen inkomsten: een schatting van het bedrag dat het slachtoffer misloopt door het uitvallen van een kritieke dienst. Bijvoorbeeld de schade van Amazon, PayPal, Visa en Mastercard toen bepaalde diensten door DDoS-aanvallen vanuit Anonymous tijdelijk ontoegankelijk werden gemaakt.
- Opvolgschade: het bedrag dat gemoeid is met de afhandeling van het incident. Bijvoorbeeld kosten voor het terughalen van passen en verbeteren van de beveiliging.
- Potentiële schade: het theoretisch maximale bedrag dat ontvreemd had kunnen worden. Bijvoorbeeld door rekeningen volledig leeg te halen.
- Imagoschade: de inkomsten die het slachtoffer misloopt door een geschonden imago als gevolg van de criminaliteit. In het geval van DigiNotar heeft de imagoschade (door het verborgen houden van het incident) zelfs uiteindelijk geleid tot een faillissement.

6.3.2 Schadecijfers Nederlandse banken

Het is algemeen bekend dat zich regelmatig high tech crime aanvallen gericht tegen sectorale ordening of vitale knooppunten van virtuele en/of fysieke infrastructuren voordoen. Elektriciteits-, water-, telecommunicatie-, vervoers- en internetbedrijven treden echter niet graag naar buiten met statistieken. In het algemeen worden alleen als het bij een specifiek incident onoverkomelijk is schadecijfers bekend gemaakt. Een uitzondering hierop vormen de Nederlandse banken. Zij publiceren jaarlijks gezamenlijk schadebedragen die voortkomen uit de belangrijkste aanvallen op financiële systemen, namelijk skimmen en fraude met internetbankieren. Tabel 6.2 biedt een overzicht van deze cijfers.

Tabel 6.2

Schadebedragen als gevolg van skimmen en internetbankieren			
Jaar	Schade door skimmen		Schade door fraude internetbankieren
2005	€ 4	miljoen	geen cijfers
2006	€ 8	miljoen	geen cijfers
2007	€15	miljoen	geen cijfers
2008	€31	miljoen	geen cijfers
2009	€36	miljoen	€1,9 miljoen
2010	€19,7	miljoen	€9,8 miljoen
2011	€38,9	miljoen	€35 miljoen

Bron: NVB

Uit de tabel blijkt dat de schade door skimmen sterk daalt en in 2011 opeens weer stijgt. Met name aan het einde van dat jaar zijn er ineens weer veel nieuwe skimgevallen waargenomen. Een mogelijke verklaring daarvoor is dat de EMV chip op dat moment nog niet breed ingevoerd was en criminelen nog op het laatste moment wilden profiteren van de kwetsbaarheden van de magneetstrip[72]. Uit de tabel kan ook worden opgemaakt dat de schade door fraude met internetbankieren de afgelopen jaren explosief gestegen. Doordat het gebruik van malware langzamerhand de overhand neemt op social engineering gaat het om aanvallen op steeds grotere schaal en daarmee om meer schade.

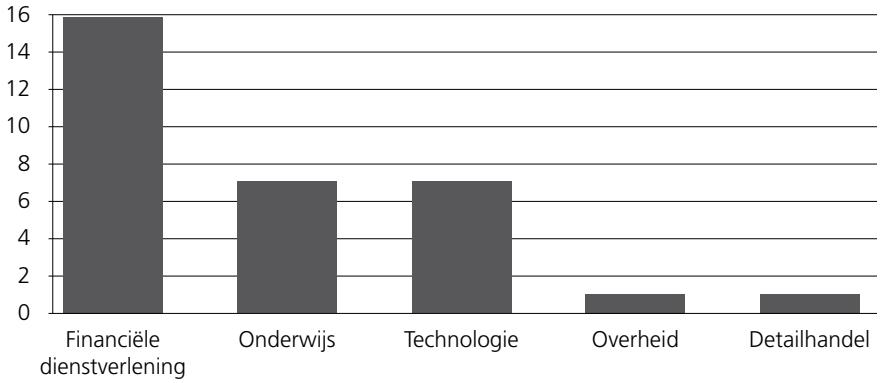
6.3.3 Dossieranalyse THTC

Uit de dossieranalyse in het kader van het DBIR 2011[73] blijkt dat de meeste (16 van de 32) door het THTC onderzochte datalekken bij financiële instellingen plaats hebben gevonden. Een belangrijke verklaring hiervoor is dat de Nederlandse banken het meest actief de samenwerking met de politie op hebben gezocht, specifiek voor de aanpak van bovengenoemde verschijningsvormen. Daarnaast komt ook het slachtofferschap van Universiteiten (Education) en IT-security bedrijven/bedrijven voor software-ontwikkeling (Tech Services) duidelijk naar voren in dossiers van het THTC.

[72] Zie ook paragraaf 8.2.5.
[73] Zie paragraaf 6.2.4.

Figuur 6.5

Aantal datalekken per sector



Bron: DBIR 2011

Uit tabel 6.3 blijkt dat het vooral om datalekken bij grotere organisaties gaat. Ook dat wordt mede verklaard door de intake van HTC onderzoeken en niet per definitie door daadwerkelijke verhoudingen in termen van hoeveelheid.

Tabel 6.3

Aantal datalekken per organisatiegrootte

Aantal werknemers	Aantal datalekken
1 tot 10	0
11 tot 100	1
101 tot 1000	4
1001 tot 10000	9
10001 tot 100000	14
Meer dan 100000	2
Onbekend	2

Om een indruk te geven van de ontwikkeling in omvang van het aandachtsgebied wordt hieronder een overzicht gegeven van het totale aantal door het THTC uitgevoerde opsporingsonderzoeken en rechtshulpverzoeken in de afgelopen jaren.

Tabel 6.4

Jaarcijfers afgesloten onderzoeken en rechtshulpverzoeken THTC					
	2007	2008	2009	2010	2011
Totaal afgesloten zelfstandige onderzoeken	2	6	4	5	8
Inkomende rechtshulpverzoeken politioneel	52	54	57	62	95
Inkomende rechtshulpverzoeken justitieel	2	4	12	15	14
Totaal uitgevoerde RHV's	54	58	69	77	109

De cijfers in tabel 6.4 geven slechts een indruk van de omvang van het aandachtsgebied zoals die zich in de zin van zaaksvoorraad bij het THTC heeft ontwikkeld. Alleen de afgesloten onderzoeken worden in een jaar geteld, daardoor zijn er geen cijfers omtrent het aantal gestarte onderzoeken in de tabel weergegeven. Onderzoeken kunnen namelijk over de jaargrens heen lopen.

In algemene zin geldt in binnen- en buitenland dat ontwikkelingen in het aantal uitgevoerde opsporingsonderzoeken en rechtshulpverzoeken geen gelijke tred meer houden met de toename in termen van hoeveelheid van activiteit (frequentie, incidentie, prevalentie). De schaalgrootte per onderzoek is de afgelopen jaren enorm toegenomen en in Nederland is in 2010 in ieder geval een punt van verzadiging bereikt. Dat wil zeggen dat er meer zaaksvoorraad was dan capaciteit om de toename bij te houden. Overigens dient dit beeld van een toename in omvang van specifiek high tech crime iets genuanceerd te worden. Het THTC voert nu nog regelmatig rechtshulpverzoeken met betrekking tot veelvoorkomende/high volume cybercrime uit die eigenlijk in de politieregio's uitgezet zouden moeten kunnen worden. Uit tabel 6.4 valt af te lezen dat er met name op dat gebied een behoorlijke stijging waarneembaar is: van 52 in 2007 naar 95 in 2011. Enkele redenen hiervoor zijn dat als een verzoek via het 24/7 netwerk met spoed bij het THTC binnenkomt alleen dit team de gewenste snelheid kan leveren en/of dat er in de regio's onvoldoende capaciteit en expertise beschikbaar is. De hoop is dat hier met de inrichting van de Nationale Politie verandering in gaat komen.

6.4 Conclusie

Op basis van dit hoofdstuk kunnen een aantal interessante conclusies getrokken worden. Ten eerste blijken statistieken ten aanzien van het gebruik van middelen, vooral malware, behoorlijk van elkaar te verschillen. De belangen die

partijen hebben bij het presenteren van cijfers staan accurate statistieken helaas in de weg. Toch kunnen een aantal concrete waarnemingen worden gedaan op basis van trends in die statistieken. Zoals die van de Shadowserver Foundation, die laten zien dat de groei van het totaal aantal malwarepakketten en de omvang van (C&C gestuurde) botnets voorzichtig afneemt. Dergelijke cijfers zijn echter pas goed te plaatsen als er context aan gegeven kan worden. Een afname betekent niet per se dat de impact daardoor ook minder wordt. Uit voorgaande hoofdstukken bleek immers dat ontwikkelingen in de aard van het verschijnsel aan lijken te tonen dat middelen tegenwoordig minder massaal en random ingezet worden, maar meer gericht. Op die manier wordt getracht met minder activiteit meer winst te behalen en zeggen de aangehaalde absolute cijfers dus niet zoveel over de totale impact.

Als het specifiek om high tech crime verschijningsvormen gaat, ontbreken accurate absolute cijfers vrijwel geheel. Enerzijds heeft dit te maken met het verborgen houden van incidenten door slachtoffers. Anderzijds blijkt de politie onvoldoende in staat het werkaanbod op dit aandachtsgebied inzichtelijk te maken. Desalniettemin konden ontwikkelingen in het aantal door het THTC uitgevoerde opsporingsonderzoeken en rechtshulpverzoeken geen gelijke tred meer houden met de toename in activiteit op het aandachtsgebied. Daarom moet er alvast een winstwaarschuwing worden afgegeven: ook een groter THTC zal deze achterstand in de komende jaren niet zomaar inlopen.

7
Knelpunten in het juridisch kader

7.1 Inleiding

De titel van een interessant artikel over de implementatie van relevante wetgeving op het gebied van cybercrime is: 'Wet computercriminaliteit II: de boeven zijn er - nu de wet weer'[74]. De kwinkslag die de auteurs in deze titel maken kan exemplarisch genoemd worden voor de positie die wetgeving inneemt ten aanzien van cybercrime en daarmee ook high tech crime. Wetgevingsprocessen nemen namelijk dermate veel tijd in beslag, dat de (technologische) ontwikkelingen in het aandachtsgebied de 'nieuwe' wetten meestal allang weer vooruit zijn gesneld. Desalniettemin trachten nationale en internationale instanties om de evolutie binnen het aandachtsgebied middels (nieuwe) wetgeving het hoofd te blijven bieden.

In dit hoofdstuk wordt eerst in het kort het huidige juridische kader voor het aandachtsgebied geschetst[75]. De focus ligt daarbij steeds op wat relevant is voor specifiek high tech crime. In wetgeving wordt dat onderscheid echter niet expliciet gemaakt, daarom zal er regelmatig naar cybercrime verwezen worden. Hierbij wordt voornamelijk gefocust op de voor de politie meest relevante juridische onderdelen: strafrechtelijke (inhoudelijke) en strafvorderlijke (procedurele) bepalingen. Dit hoofdstuk is echter niet bedoeld om een volledig overzicht te geven, maar om leemtes en knelpunten in het huidige kader aan te kunnen wijzen. Deze knelpuntenanalyse staat centraal in het tweede deel van dit hoofdstuk.

7.2 De Cybercrime Conventie

De strafbaarstellingen en opsporingsbevoegdheden zijn in Nederland voornamelijk vervat in het Wetboek van Strafrecht en het Wetboek van Strafvordering. Vanwege het specifieke internationale karakter van het aandachtsgebied hebben vooral internationale verdragen aanzienlijke invloed

---

74 Bijvoorbeeld via www.wetten.nl.

75 Bij de beschrijving wordt zoveel mogelijk aangesloten bij de uitgangspunten die in dit kader vanuit het NCSC zijn vastgesteld, onder meer in de 'Handreiking Cybercrime: Van Herkenning tot aangifte'.

gehad op relevante wetgeving. Enerzijds ter begrenzing op de wetgeving (grondrechten) en anderzijds ter implementatie of verandering van de wetgeving (inhoudelijke en procedurele bepalingen en/of de uitleg daarvan).

Ten aanzien van cybercrime zijn de belangrijkste internationale afspraken vervat in de Cybercrime Conventie (CCC) van de Raad van Europa, dat in 2001 door onder meer alle EU-lidstaten en de Verenigde Staten werd ondertekend en geratificeerd. De verdragspartijen hebben zich daarin bijvoorbeeld gecommitteerd om hun nationale materiële en formele strafrecht op het gebied van cybercrime gelijk te trekken. Daarnaast wordt met dit verdrag de internationale samenwerking bij de opsporing en vervolging van cybercrime bevorderd. In het vorige hoofdstuk zijn twee voorbeelden benoemd die een direct gevolg zijn van implementatie van het verdrag: direct bilateraal contact via de zogenaamde 24/7 contact points en de mogelijkheid tot het nemen van maatregelen (zoals het veiligstellen van data) zonder dat een formeel rechtshulpverzoek reeds is ingediend.

7.3 Strafrechtelijke bepalingen

7.3.1 Wet computercriminaliteit

Zoals meermaals al uit deze CBA bleek, vervult Nederland op het gebied van cybercrime een pioniersrol, ook op juridisch gebied. Lang voordat de CCC werd gesloten was er in Nederland bijvoorbeeld al wetgeving op het gebied van cybercrime: de Wet Computercriminaliteit I (WCCI). Met deze wet, die van kracht werd in 1993, werden het Wetboek van Strafrecht en het Wetboek van Strafvordering op vele punten gewijzigd. De bedoeling was om de Wet Computercriminaliteit techniekneutraal te formuleren. De gedachte hierachter was dat nieuwe ontwikkelingen anders niet onder bestaande wetgeving geschaard zouden kunnen worden. Er wordt in relevante wetgeving bijvoorbeeld gebruik gemaakt van de term 'geautomatiseerde werken'[76]. Een term die ook de politie bij het definiëren van cybercrime heeft aangehouden[77].

---

[76] In het Wetboek van Strafrecht is de term 'geautomatiseerde werken' als volgt omschreven in artikel 80sexies: een inrichting die bestemd is om langs elektronische weg gegevens op te slaan, te verwerken en over te dragen.De rechter zal per zaak bezien of er wordt voldaan aan deze definitie.

[77] Zie paragraaf 1.2.2.

De technologie en de misdaad bleven zich echter ontwikkelen en het bleek dat de WCCI toch al relatief snel weer aan vervanging toe was. Het heeft echter, mede door de internationale ontwikkelingen op het gebied van de CCC, nog een behoorlijke tijd geduurd voordat de opvolger er was. Deze kwam er uiteindelijk in 2006, onder de naam Wet Computercriminaliteit II.

In de Wet Computercriminaliteit II zijn de belangrijkste strafbaarstellingen op het gebied van cybercrime vervat. Deze bepalingen zijn voor het grootste gedeelte in het Wetboek van Strafrecht (Sr) opgenomen. In de volgende paragrafen wordt nader belicht om welke delicten het gaat.

7.3.2 Hacken

Hacken is onder 'computervredebreuk'[78] strafbaar gesteld in artikel 138ab Sr. Computervredebreuk is in dit artikel omschreven als elke vorm van opzettelijk en wederrechtelijk binnendringen in een geautomatiseerd werk of een deel daarvan.

In de delictsomschrijving van het artikel zijn de begrippen 'opzet' en 'wederrechtelijkheid' opgenomen. Opzet wordt in algemene zin uitgelegd als het 'willens en wetens' veroorzaken van een bepaald gevolg door een handelen of nalaten. Een dader wist dus wat het gevolg van zijn gedraging zou zijn en wilde dit gevolg ook doen intreden[79]. Het begrip wederrechtelijkheid doelt op de voorwaarde dat een strafbaar feit ook in strijd met het recht moet zijn gepleegd. Aan de voorwaarde van wederrechtelijkheid wordt bijvoorbeeld niet voldaan als er sprake is van noodweer of het uitvoering geven aan een wettelijk voorschrift.

Een belangrijke wijziging in artikel 138ab Sr die de Wet Computercriminaliteit II met zich meebracht, is dat niet meer vereist is dat er een beveiliging doorbroken wordt om van 'binnendringen' te kunnen spreken. Het is wel zo dat het doorbreken van een beveiliging sowieso 'binnendringen' oplevert. Net als een technische ingreep, het gebruik van valse signalen of een valse sleutel, of het aannemen van een valse hoedanigheid (lid 1). De lijst van lid 1 is niet-limitatief. Daarom is het mogelijk dat er ook nog andere technieken onder 'binnendringen' in de zin van dit artikel kunnen vallen.

---

78 Zie bijvoorbeeld paragraaf 3.2 en 4.3.3.

79 Opzet kan ook in voorwaardelijke zin aanwezig zijn. In dat geval is het zo dat de dader een aanmerkelijke kans aanvaard dat door zijn gedraging een bepaald gevolg intreedt.

7.3.3 DDoS-aanvallen

In artikel 138b Sr wordt onder meer de DDoS-aanval strafbaar gesteld: het belemmeren van de toegang tot een geautomatiseerd werk door het aanbieden of toezenden van gegevens. De wetgever heeft in dit artikel bewust gekozen voor een brede delictsomschrijving, zodat vergelijkbare aanvallen via een ander middel en/of met een ander doel of uitwerking er ook onder geschaard kunnen worden. Hierbij kan bijvoorbeeld gedacht worden aan e-mail bommen om een systeem vast te laten lopen of een DNS amplification attack[80].

7.3.4 Malware maken, verspreiden en gebruiken

In art. 139c Sr wordt het aftappen en/of opnemen van gegevens strafbaar gesteld die door een geautomatiseerd werk of telecommunicatienetwerk worden verwerkt of overgedragen en die voor een ander zijn bestemd. Ten aanzien van high tech crime is dit artikel voornamelijk van toepassing in de context van malware. Denk hierbij bijvoorbeeld aan spyware[81]. Ook kan het van toepassing zijn op sniffing indien er gegevens, die verzonden worden over een telecommunicatienetwerk, opzettelijk worden onderschept.

Er kan al sprake zijn van strafbaar handelen voordat het aftappen daadwerkelijk begonnen is. Indien er apparatuur is geplaatst om daarmee opzettelijk gegevens af te tappen, kan de daarvoor verantwoordelijke persoon vervolgd worden op basis van artikel 139d lid 1 Sr[82]. Hetzelfde geldt voor het produceren van of handelen in dergelijke aftapapparatuur (artikel 139d lid 2 sub a Sr).

Daarnaast wordt in artikel 139d lid 2 sub b en lid 3 Sr ook het bezitten of verspreiden van een wachtwoord of code waardoor toegang kan worden gekregen tot een geautomatiseerd werk strafbaar gesteld. Ook hier kan weer gedacht worden aan het verspreiden van malware.

7.3.5 Vernielingsdelicten

Voor de invoering van de Wet Computercriminaliteit II bestond eerdergenoemd artikel 138b Sr nog niet. Destijds waren er twee andere relevante artikelen: 161septies en 161sexties Sr. Deze bepalingen bestaan nog steeds en regelen de

---

80 Zie paragraaf 3.5.3.

81 Zie paragraaf 3.4.2.

82 Het zou bijvoorbeeld om een trojan kunnen gaan die op de achtergrond draait en alle communicatie stiekem naar een server stuurt.

veroorzaking van de stoornis in de gang of werking, vernieling, beschadiging of het onbruikbaar maken van geautomatiseerde werken. Dit worden vernielingsdelicten genoemd. Ook hier kan men aan (D)DoS-aanvallen denken.

Naast artikelen 161sexies en 161septies Sr zijn er nog andere vernielingsdelicten in de wet omschreven. Bijvoorbeeld in artikelen 350a en 350b Sr. Deze artikelen hebben betrekking op de gegevens die zich op geautomatiseerde werken bevinden en niet op de werken zelf.

In de praktijk zijn deze artikelen onder meer relevant indien er malware, zoals spyware, wordt geïnstalleerd.

7.3.6 Identiteitsfraude

Binnen high tech crime komt identiteitsfraude in allerlei vormen voor. Bijvoorbeeld als er sprake is van spoofing of indien het internetverkeer wordt omgeleid. In het Nederlandse strafrecht is, in tegenstelling tot bijvoorbeeld de Verenigde Staten, geen expliciet artikel over identiteitsfraude opgenomen. Het 'verkrijgen van gegevens omtrent de identiteit' is echter wel omschreven in verschillende afzonderlijke strafrechtelijke bepalingen. Misbruik van die gegevens kan bijvoorbeeld vallen onder diefstal of oplichting (art. 310, 326 Sr). Daarnaast zou het ook onder geschaard kunnen worden onder valsheid in geschrifte, onder opgave van onware gegevens, en onder schending van de verplichting gegevens te verstrekken (art. 225 t/m 232 Sr).

Het vervaardigen, ontvangen, aanschaffen, verkopen, overdragen of voorhanden hebben van stoffen, voorwerpen of gegevens bestemd tot het plegen van vormen van identiteitsfraude, kan ook strafbaar zijn. Artikel 234 Sr handelt hierover. Ook artikel 139e Sr kan relevant zijn, daarin is het voorhanden hebben van afgetapte gegevens (bijvoorbeeld via malware) strafbaar gesteld.

Vormen van identiteitsfraude waardoor een crimineel betalingen kan verrichten zijn overigens specifiek strafbaar gesteld in artikel 232 Sr. Het gaat dan bijvoorbeeld om het huren van een auto met een nagemaakte creditcard.

7.4 Strafvorderlijke bepalingen

In de vorige paragraaf kwam het materiële (inhoudelijke) deel van het strafrecht aan de orde. In deze paragraaf zal er aandacht zijn voor het formele (procedurele) deel van het strafrecht: strafvordering. In de strafvorderlijke

bepalingen, die voornamelijk opgenomen zijn in het Wetboek van Strafvordering, wordt onder meer het opsporingsonderzoek (politie), het vervolgingstraject (OM) en het onderzoek ter terechtzitting (rechter) omschreven. Voor de politie is vooral de fase van het opsporingsonderzoek relevant.

7.4.1 Jurisdictie

De politie heeft zich in het verleden ten aanzien van de georganiseerde misdaad vooral beziggehouden met criminele activiteiten die zich in de fysieke wereld afspeelden. Tegenwoordig is de focus, ook ten aanzien van klassieke misdaad, steeds meer verschoven richting cyber als vierde domein naast de klassieke domeinen land, lucht en water. De grenzeloosheid van dit domein heeft ervoor gezorgd dat opsporingsdiensten meer dan ooit tegen de grenzen van jurisdictie aanlopen als het gaat om de inzet van bevoegdheden. Zeker als het high tech crime betreft. De zaaksvoorbeelden in deze CBA laten zien hoe high tech criminelen daarentegen uitstekend gebruik weten te maken van de grenzeloosheid van het internet. Zo kon de Bredolab botnet herder met een klik vanuit Rusland via Frankrijk een DDoS-aanval uitvoeren op Nederlandse servers en had hij niet veel klikken verder zijn complete infrastructuur naar een ander land kunnen verplaatsen als er niet zo kordaat was opgetreden[83].

Jurisdictie in de context van opsporing betekent dat de politie slechts onderzoek op computernetwerken mag doen voor zover de Nederlandse rechtsmacht reikt. Rechercheurs mogen dus geen onderzoek doen wanneer de betrokken computers zich kennelijk buiten Nederland bevinden. De strafrechtelijke normering houdt op bij de fysieke landsgrenzen, terwijl het internet als zodanig juist een grensoverschrijdend karakter heeft.

Dit betekent niet dat er geen mogelijkheden zijn als het onderzoek zich naar het buitenland verplaatst: internationale samenwerking is noodzakelijk en vindt daarom ook veelvuldig plaats. In het vorige hoofdstuk is dit reeds besproken.

Ondanks de goede internationale samenwerking blijven er toch juridische knelpunten bestaan als het gaat om een efficiënte internationale opsporing. Aan deze knelpunten zal later in dit hoofdstuk meer aandacht worden besteed. Eerst is er aandacht voor een aantal relevante bevoegdheden die zijn opgenomen in het Wetboek van Strafvordering.

---

[83] Zie voor meer hierover: paragraaf 7.5.

7.4.2 Doorzoeking ter vastlegging en inbeslagneming van gegevens

Tijdens een opsporingsonderzoek is het voor de politie van belang om digitale gegevens veilig te (kunnen) stellen. Dergelijke gegevens kunnen zich bijvoorbeeld op gegevensdragers zoals USB-sticks en harde schijven bevinden. Op grond van artikel 94 Sv mogen die gegevensdragers in het kader van een doorzoeking in beslag worden genomen. Omdat het echter veeleer om de data gaat dan de drager waarop die data zich bevinden, is in artikel 125i Sv de bevoegdheid opgenomen om die gegevens ter gelegenheid van een doorzoeking ter plaatse veilig te stellen uit een geautomatiseerd werk.

Voor zover de toegang tot die gegevens kan worden verkregen via een netwerkverbinding die aanwezig is op het geautomatiseerde werk waar vanuit al gegevens worden veiliggesteld, mogen die gegevens op grond van artikel 125j Sv worden veiliggesteld. Deze bevoegdheid kent echter zijn beperking in de grenzen van de Nederlandse rechtsmacht. Als vooraf duidelijk is dat de gegevens zich bevinden op een geautomatiseerd werk in het buitenland, dan mag de bevoegdheid niet worden ingezet.

Het THTC treft bij een doorzoeking ook regelmatig versleutelde gegevens op computers, USB-sticks e.d. aan. In een dergelijk geval kan op basis van artikel 125k Sv een bevel tot ontsleuteling worden gegeven aan een persoon. Die persoon mag echter niet de verdachte zijn. Een verdachte hoeft namelijk niet mee te werken aan zijn eigen veroordeling. Dit uitgangspunt vloeit voort op het grondrecht op een eerlijk proces en wordt het 'nemo-tenetur-beginsel' genoemd.

7.4.3 Het ontoegankelijk maken van gegevens

Het is goed mogelijk dat gegevens die tijdens een doorzoeking worden aangetroffen, in het kader van een (potentieel) strafbaar feit gebruikt worden. In art. 125o Sv is een bevoegdheid opgenomen om gegevens in zulke gevallen ontoegankelijk te maken. Met het begrip 'ontoegankelijk maken' wordt gedoeld op het treffen van maatregelen waardoor de beheerder van het geautomatiseerd werk of derden niet meer gebruik kunnen maken van de gegevens of deze verder kunnen verspreiden. Ook is het mogelijk dat de bestanden in zijn geheel worden verwijderd uit het geautomatiseerde werk. In dat geval blijven de gegevens wel beschikbaar voor justitie ten behoeve van de strafvordering.

Er zijn allerlei andere mogelijkheden om gegevens ontoegankelijk te maken. Zo kunnen de gegevens versleuteld worden of kan de toegangspoort van het

systeem onbruikbaar worden gemaakt. Daarbij moet steeds beoordeeld worden welke actie het meest proportioneel is.

Het gaat in het geval van artikel 125o Sv overigens om een tijdelijke maatregel. Indien er geen strafvorderlijk belang meer bestaat, dienen de gegevens weer onder beheer van het geautomatiseerd werk te worden gebracht. Het kan echter zo zijn dat bij de raadkamer van de rechtbank verlof verkregen dient te worden om de toegankelijkmaking definitief te maken (vergelijkbaar met verlof om ten aanzien van in beslag genomen voorwerpen te handelen alsof zij verbeurd verklaard waren of waren onttrokken aan het verkeer).

7.4.4 Wet BOB

Op 1 februari 2000 is de Wet Bijzondere opsporingsbevoegdheden (Wet BOB) in werking getreden. Deze wet introduceerde in de titels IVA en V van Boek I van het Wetboek van Strafvordering een regeling voor nieuwe opsporingsbevoegdheden en daarmee samenhangende procedures.

De bevoegdheden die in deze bepalingen zijn omschreven maken een zwaardere inbreuk op de grondrechten van verdachten en mogen daarom uitsluitend voor de bestrijding van georganiseerde criminaliteit en de bestrijding van bepaalde ernstige misdrijven worden ingezet.

In de volgende paragrafen zal een aantal van de bijzondere opsporingsbevoegdheden beschreven worden, dat relevant is voor de opsporing van high tech crime.

7.4.5 Vordering tot verstrekking van gegevens

Een aantal bijzondere opsporingsbevoegdheden dat relevant is voor opsporingswerk van high tech crime zijn omschreven in artikelen 126n tot en met 126ng Sv. In deze bepalingen zijn bevoegdheden opgenomen die de politie in het opsporingsonderzoek heeft als het gaat om het vorderen van gegevens. Ieder artikel heeft betrekking op een andere situatie, waarbij met name het onderscheid op basis van de gegevens waarop het artikel betrekking heeft van belang is. Dit onderscheid betreft grofweg:

- Het soort gegevens;
- De hoedanigheid van degene aan wie de vordering wordt gedaan, en:
- De vraag of de betreffende gegevens reeds zijn verwerkt ten tijde van de vordering, of dat die verwerking nog moet plaatsvinden.

Ten aanzien van de mate van privacyschending is verder nog relevant de plaats waar de gegevens waarop de vordering betrekking heeft, zich bevinden.

Het soort gegevens is vooral van belang voor de zwaarte van de inbreuk die mag worden gemaakt op de (grond)rechten van de verdachte. Het door de wetgever gemaakte onderscheid heeft vooral betrekking op identificerende gegevens, verkeers- en overige gegevens of gegevens met betrekking tot de inhoud van communicatie.

Met betrekking tot de hoedanigheid van degene aan wie de vordering wordt gedaan, geldt dat een 'aanbieder' (zoals omschreven in artikel 126la Sv) een grotere mate van rechtsbescherming geniet dan 'eenieder, niet zijnde een aanbieder'. Voor vorderingen gedaan aan 'aanbieders' gelden zwaardere eisen (vervat in diverse artikelen). De politie zal bij het vorderen van gegevens daarom altijd goed moeten afbakenen welk artikel van toepassing is op de situatie.

7.4.6 Vordering tot het veiligstellen van gegevens (bevriezingsbevel)

Naast de bevoegdheid tot het vorderen van gegevens, heeft de politie ook de bevoegdheid om het veiligstellen van gegevens te vorderen. Dit 'bevriezings-bevel' is opgenomen in artikel 126ni Sv en houdt een verbod in om bepaalde bestaande gegevens gedurende maximaal 90 dagen te bewerken. Het bevriezingsbevel mag alleen gegeven worden indien er aanwijzingen bestaan dat de te bewaren gegevens bijzonder kwetsbaar zijn voor verlies of wijziging.

In de fase van de bevriezing kunnen er dan maatregelen worden genomen om de gegevens op de gewenste manier te verkrijgen, bijvoorbeeld nadat een officieel rechtshulpverzoek tot 'uitlevering' van de gegevens is binnengekomen. Hiermee kan worden voorkomen dat potentieel bewijsmateriaal verdwijnt.

7.4.7 Tapbevoegdheden: het opnemen van openbare en vertrouwelijke communicatie

De tapbevoegdheid van de politie spreekt veel mensen tot de verbeelding. Vaak denkt men daarbij aan een politieman die met een grote hoofdtelefoon mee-luistert bij telefoongesprekken. In high tech crime opsporingsonderzoeken is dat beeld vaak anders. Het zal bijvoorbeeld eerder gaan om het tappen van e-mail-verkeer dan om het tappen van telefoonverkeer. In artikelen 126m en 126l Sv zijn belangrijke tapbevoegdheden vervat.

Artikel 126m Sv geeft aan elke opsporingsambtenaar de bevoegdheid om communicatie op te nemen die wordt gevoerd via een communicatiedienst of –netwerk. Daarbij mag een technisch hulpmiddel worden ingezet.

Indien het onderzoek dit dringend vordert bestaat op grond van artikel 126l Sv de mogelijkheid om vertrouwelijke communicatie, die niet verloopt via een communicatiedienst of –netwerk op te nemen. Ook hiertoe mag een technisch hulpmiddel worden aangebracht, bijvoorbeeld om toetsaanslagen en muisklikken te registreren, voor zover die aan te merken zijn als communicatie.

Voorbeelden
De politie heeft een verdachte hacker op het oog. De opsporingsambtenaren plaatsen een e-mailtap om te bezien of deze persoon zich in die communicatie uitlaat over de activiteiten die hij verricht zou hebben. Deze bevoegdheid komt iedere opsporingsambtenaar toe ex artikel 126m Sv. Er moet wel een bevel toe gegeven zijn door de officier van justitie en een machtiging zijn van een rechter-commissaris.

Stel dat de e-mailtap onbruikbaar blijkt te zijn omdat alle berichten van de verdachte versleuteld worden verzonden. De opsporingsambtenaren kunnen dan besluiten een bug te plaatsen op het toetsenbord van de verdachte om zo de informatie op te vangen die de verdachte intypt bij het opstellen van zijn e-mails. Dus nog in de fase voordat die berichten versleuteld verzonden worden. Deze bevoegdheid komt slechts aan bepaalde opsporingsambtenaren toe ex artikel 126l Sv. Ook hier dient er een bevel van een officier van justitie en een machtiging van een rechter-commissaris te zijn verkregen. Een minder ingrijpende bevoegdheid (zoals artikel 126m) moet worden ingezet als die ook soelaas biedt.

7.4.8 Handhaven van de rechtsorde

In deze paragraaf wordt er een kort uitstapje gemaakt naar de Politiewet 1993. Deze wet regelt het beheer, taak en organisatie van de politie en het gezag waaraan zij is onderworpen. In artikel 2 van die wet is de taakstelling van de politie omschreven als het handhaven van de rechtsorde en het verlenen van hulp aan hen die het behoeven. Deze taak dient ondergeschikt aan het bevoegde gezag en in overeenstemming met de geldende rechtsregels te worden uitgevoerd.

De Hoge Raad heeft in het Zwolsman-arrest[84] bepaald dat bevoegdheden op basis van dit artikel slechts beperkte inbreuk mogen maken op de grondrechten van de verdachte. Indien het gaat om zwaardere inbreuken dan moet daarvoor een expliciete basis in het Wetboek van Strafvordering of bijzondere wetgeving zijn.

Voor het THTC is artikel 2 Politiewet zeer relevant. Voornamelijk als het gaat om handelingen die een inbreuk maken op de privacy. Later zullen we hier nog op terugkomen[85].

7.5 Knelpuntenanalyse

De snelle veranderingen in het aandachtsgebied nopen tot een fundamentele discussie of de bestaande wetgeving nog (volledig) geschikt is om high tech crime effectief te kunnen bestrijden. De opsporingspraktijk laat namelijk zien dat er belangrijke knelpunten zijn op juridisch gebied. Een aantal van deze knelpunten komen in deze paragraaf aan bod. Om enige praktische context aan die knelpunten te geven, wordt eerst het botnet-onderzoek Tolling[86] vanuit juridisch perspectief belicht.

Juridische componenten in de praktijk: de Bredolab ontmanteling

Uit het publiek-private samenwerkingsproject Taurus ontving het THTC informatie van een Nederlandse hosting provider dat er servers bij hun werden gehuurd die mogelijk werden misbruikt voor een omvangrijk botnet.

Op basis hiervan heeft het THTC onderzoek Tolling opgestart. Een van de eerste acties uit het opsporingsonderzoek was de inbeslagname van 143 (voor het botnet cruciale) servers die bij een Nederlandse hosting provider gehuurd waren.

Vervolgens kon er telecommunicatie worden getapt die plaatsvond tussen de in beslag genomen servers en servers die zich op andere plekken bevonden.

---

84 HR 19 december 1995, NJ1996 ,249, m.nt.Sch. (Zwolsman).
85 Zie paragraaf 7.5.3.
86 Zie ook paragraaf 3.5.1.

Uit de getapte informatie kon onder meer de identiteit van de verdachte achterhaald worden. Het bleek te gaan om een in Rusland wonende Armeniër. Ook kon worden achterhaald dat er C&C servers van andere botnets bij een hosting provider in Frankrijk stonden. Op basis van die informatie werd besloten om de Franse autoriteiten om rechtshulp te verzoeken, zodat zij bij de uiteindelijke ontmanteling van het botnet konden assisteren.

Uit onderzoeksgegevens was inmiddels gebleken dat de verdachte Armeniër naar een dancefeest in Amsterdam zou komen. Het THTC zag zijn kans schoon en wilde hem bij aankomst in Nederland aanhouden. Echter kreeg de verdachte geen visum waardoor zijn feesttrip niet door kon gaan. Daarop werd er een internationaal aanhoudingsbevel uitgevaardigd.

Ondertussen werd in Nederland de ontmanteling van het botnet voorbereid. De uiteindelijke uitvoering daarvan was speciaal: de servers werden namelijk niet gewoon uitgeschakeld, maar er werd van binnenuit controle verkregen over het botnet zelf. De verdachte had vrij snel door dat er iets aan de hand was en reageerde door een DDoS-aanval uit te voeren op de Nederlandse servers. Dit deed hij via het vanuit Frankrijk aangestuurde botnet. Dit mislukte echter, mede dankzij de kundige reactie van de private partners en de Franse autoriteiten op dat moment.

De verdachte verloor de slag, raakte zijn botnet kwijt en keerde daarna terug naar zijn thuisland Armenië. Op het vliegveld van Yerevan werd hij echter ingerekend door de politie. De Nederlandse autoriteiten hebben het dossier in het Armeens laten vertalen en overgedragen aan de autoriteiten van dat land. Zij hebben namelijk aangegeven de verdachte zelf te willen berechten.

Politie en justitie in Nederland hebben de slachtoffers van het botnet op bijzondere wijze geïnformeerd. Namelijk via de nog bestaande infrastructuur van het botnet. Deze bevoegdheid werd gestoeld op artikel 2 Politiewet. Er werd een bestandje klaargezet op de nog werkende C&C servers, die door de geïnfecteerde PC's sowieso automatisch zouden worden bezocht. Het bestandje zorgde ervoor dat er een pop-up op de PC's van de slachtoffers verscheen met daarin een waarschuwingsbericht met achtergrondinformatie en tips ten aanzien van hun besmetting.

7.5.1 Jurisdictie

De plaats delict van high tech crime is meestal het internet. In tegenstelling tot de klassieke domeinen is cyber een minder tastbaar gebied waarin er nauwelijks over grenzen gesproken kan worden. Het is wereldwijd, gedeterritorialiseerd , flexibel en snel ontwikkelend, waardoor het een internationale informatie-economie kan faciliteren die voornamelijk om gegevens in plaats van goederen draait. Misdadigers kunnen hierdoor op innovatieve wijze op afstand, geautomatiseerd en tegen grote groepen potentiële slachtoffers hun criminele activiteiten ontplooien zonder daarbij al te veel last te hebben van fysieke, meer 'tastbare' landsgrenzen[87].

Echter heeft de politie ten aanzien van haar opsporingsbevoegdheden wel te maken met die grenzen. Vanwege de soevereiniteit van staten kunnen opsporingsbevoegdheden niet zomaar zelfstandig worden toegepast en zal er om rechtshulp moeten worden verzocht indien een onderzoek een internationale dimensie krijgt. Mede vanwege de vluchtigheid van het relevante materiaal is dit schadelijk, vooral omdat een rechtshulpverzoek tijdsverlies impliceert.

Vanuit de politie is er daarom behoefte aan betere internationale (verdragsrechtelijke) afspraken omtrent internationale samenwerking. Op dit moment biedt artikel 32 van de CCC al een mogelijkheid voor de ene staat om toegang te verkrijgen tot gegevens op een computer op het grondgebied van een andere lidstaat. Dit kan slechts indien het gaat om openbaar benaderbare systemen of indien de beheerder van de computer toestemming geeft tot het inzien van de gegevens op de computer die zich in het andere land bevindt. In een dergelijk geval behoeft de verzoekende staat de andere staat niet op de hoogte te stellen van het feit dat er opsporingshandelingen hebben plaatsgevonden met betrekking tot een computer op haar grondgebied.

De praktijk leert dat de bovenstaande mogelijkheden niet toereikend zijn. Een kindermisbruiker uit China die zijn kinderporno via servers in Thailand verspreidt om klanten in Nederland te bedienen zal uiteraard niet via openbare systemen te werk gaan. Een hacker vanuit het Midden-Oosten die een Engelse CA aanvalt en diens certificaten vervalst evenmin.

---

[87] Zie voor deze redenering ook: Koops- De dynamiek van cybercrime-wetgeving in Nederland, in: Justitiële Verkenningen 1/12 (WODC, maart 2012).

Vanwege de fundamentele disbalans tussen jurisdictie enerzijds en het specifieke karakter van high tech crime anderzijds is de discussie over jurisdictie momenteel groter dan ooit[88].

De discussie is niet eenvoudig omdat de soevereiniteit van staten ermee gemoeid is. Vergaande afspraken (zoals in onderstaand kader) lijken daarom voorlopig nog een utopie.

Expert wil 'cyber-tribunaal' in Den Haag

16-06-2011 (security nl)

Cybercriminelen moeten voor een apart tribunaal in Den Haag worden berecht, zo pleit cybercrime-expert Stein Schjolberg. Volgens het hoofd van de Cybercrime Legal Working Group van het EastWest Institute (EWI) moet het tribunaal in actie komen als nationale rechtbanken zeer ernstige cybermisdrijven niet aanpakken.

Het tribunaal in Den Haag zou onder het Internationaal Strafhof moeten vallen en verdachten van cybercrime vervolgen, zo laat Schjolberg in zijn pleidooi weten. Mede omdat er in Den Haag al zoveel internationale gerechtshoven zijn. Mocht Den Haag afvallen, dan zou Singapore een mogelijk alternatief zijn, aangezien het Interpol Global Complex daar wordt gebouwd.

7.5.2 Binnendringen als opsporingsbevoegdheid

In de media en de politiek is er naar aanleiding van het botnet-onderzoek Tolling en het kinderporno-onderzoek Descartes een discussie ontstaan over de bevoegdheden van de politie om in het kader van opsporingsonderzoek te mogen 'hacken'. In juridische zin gaat deze discussie er eigenlijk over of het 'binnendringen' in een geautomatiseerd werk in het kader van opsporings-

[88] Zie hieromtrent bijvoorbeeld http://krant.volkskrant.nl/ipaper-online/print/article/8002/10673/NL/837952 of http://webwereld.nl/opinie/109837/digitale-irt-affaire-of-nieuwe-opsporing---opinie.html.

onderzoek 'wederrechtelijk' is. Wederrechtelijk binnendringen is namelijk vereist om van computervredebreuk (art. 138ab Sr) te kunnen spreken.

In het Wetboek van Strafvordering is geen expliciete bevoegdheid voor opsporingsambtenaren opgenomen met betrekking tot 'hacken'. Impliciet is het wel zo dat bepaalde feitelijke handelingen ter uitvoering van een wettelijke bevoegdheid een 'binnendringen' in geautomatiseerde werken veronderstelt. Zo zal een doorzoeking op grond van artikel 125i Sv betekenen dat de opsporingsambtenaren zichzelf toegang tot een geautomatiseerd werk verschaffen zonder toestemming van de rechthebbende. Hiermee wordt een handeling verricht zoals die in artikel 138ab Sr strafbaar is gesteld. Echter gebeurt dit op basis van een wettelijk voorschrift. Een vergelijking kan worden gemaakt met de aanhouding van een verdachte, die door de politie wordt meegenomen naar het bureau om te worden verhoord. In dat geval spreekt men ook niet over 'ontvoeren'[89].

Op basis van de redenering van hierboven zou men kunnen concluderen dat er vanuit de politie geen behoefte is aan expliciete bevoegdheden om binnen te dringen, omdat feitelijke handelingen ten aanzien van binnendringen inherent voortvloeien uit bestaande bevoegdheden[90]. Desalniettemin zijn er situaties die zich in de praktijk voordoen die geen directe of indirecte basis in expliciete wetgeving hebben. Voor die gevallen bestaat de behoefte vanuit de politie aan duidelijke regelgeving wel. De volgende casus betreft een praktisch voorbeeld hieromtrent:

Stel dat een rechercheur op basis van artikel 126l communicatie gaat afvangen middels een keylogger op de PC van een verdachte. Het kan dan gebeuren dat hij op basis van alarmerende berichten die hij uit die communicatie heeft opgevangen, gegevens wil vergaren die zich op dat moment op de PC van de verdachte bevinden. Bijvoorbeeld terroristisch materiaal. Dat zou momenteel juridisch onmogelijk zijn omdat er voor opsporingsambtenaren (nog) geen bevoegdheid in het Wetboek van Strafvordering is opgenomen om gegevens, niet zijnde communicatie, te vergaren ten tijde van het opslaan, bewerken of overdragen daarvan. Dergelijke gegevens kunnen slechts gevorderd worden. Het

---

89 Zie voor een toelichting bij deze redenering de speech die diensthoofd Wilbert Paulissen gaf bij de uitreiking van de Big Brother Award aan het KLPD in maart 2012. Deze is te bekijken via www.bigbrotherawards.nl/kijk-online.

90 Dit neemt overigens niet weg dat in de juridische wereld een dergelijke discussie inmiddels wel hoog op de agenda staat. Fundamentele juridische principes als rechtszekerheid en wetssystematiek nopen daartoe.

nadeel van vorderen is vooral dat het risico dan zeer groot is dat de verdachte zijn gegevens zal versleutelen of vernietigen.

Verdergaand op dit voorbeeld: stel dat dezelfde rechercheur een keylogger wil installeren zonder daarbij fysiek het huis van de verdachte te betreden/ doorzoeken (op basis van art. 125i Sv). Hij kan namelijk veel sneller en effectiever gegevens vergaren door binnen te dringen in de computer van de verdachte en daarop software te installeren die de toetsaanslagen vastlegt. De rechercheur zou dan juridisch gezien niet alleen de PC, maar als het ware ook het huis van de verdachte (want daar stond de PC) betreden. Een bevoegdheid om dit te doen is er echter (thans) nog niet. Het als het ware virtueel op afstand betreden van een fysieke plaats is dus vooralsnog onmogelijk.

De bovenstaande casus is een vereenvoudigde weergave van de high tech crime opsporingspraktijk. In werkelijkheid gaat het vaak om veel ingewikkeldere gevallen, waarbij meestal ook nog diverse internationale componenten kunnen worden toegevoegd. Echter geeft de casus wel goed aan waar de schoen momenteel wringt ten aanzien van de opsporingsbevoegdheid om geautomatiseerde systemen binnen te kunnen dringen. De politie zou er bij gebaat zijn als de wetgever deze leemte zou kunnen ondervangen.

7.5.3 Privacy afwegingen

De wetgever heeft strenge eisen gesteld aan de inzet van (strafvordelijke) bevoegdheden ten aanzien van het recht op privacy van de burger[91]. Een bevel tot het opnemen van vertrouwelijke communicatie (art. 126l Sv) mag bijvoorbeeld alleen door een officier van justitie worden afgegeven, met machtiging van een rechter-commissaris.

In algemene zin zal de politie bij de uitvoering van alle (opsporings)handelingen altijd een afweging moeten maken tussen een effectieve taakuitvoering enerzijds en een proportionele privacy-inbreuk anderzijds. In de praktijk ontstaat hier wel eens discussie over. In het geval van de Bredolab ontmanteling bijvoorbeeld, waar de slachtoffers geïnformeerd werden middels een pop-up waarmee een waarschuwingsbericht op de PC van de slachtoffers werd getoond. Sommigen zijn van mening dat hiermee de privacy van de slachtoffers onrechtmatig werd geschonden.

[91] Meestal de verdachte in het geval van opsporingshandelingen.

Bij het voorbereiden was er echter nadrukkelijk nagedacht over de effectiviteit, proportionaliteit en subsidiariteit van de te ondernemen acties. Zo werd er gekozen om op basis van een enkele lijst met IP nummers, zonder geolocatie-gegevens, gebruik te maken van de functionaliteit van het botnet om een simpele executable file te laten ophalen door de bot clients[92]. Iedere andere actie, zoals een vordering tot het verstrekken van identificerende gegevens of het verstrekken van informatie aan derden, zou meebrengen dat er meer informatie over de IP-nummers vergaard zou moeten worden. Daarmee zouden de slachtoffers steeds minder anoniem worden en zou dus sprake zijn van een grotere inbreuk op de privacy van de slachtoffers.

Het oordeel of de afweging ten aanzien van de privacy zorgvuldig is gemaakt, komt uiteindelijk aan de rechter toe. Vanwege de complexiteit van en de vernieuwing binnen high tech crime zaken is een precedent echter niet altijd even makkelijk geschapen. Vanuit de politie is er daarom ook op dit vlak behoefte aan duidelijke(re) wetgeving. Zo kunnen situaties vooraf mogelijk nog scherper afgewogen worden.

7.5.4 Ontsleutelingsplicht voor verdachten

In veel high tech crime onderzoeken wordt data in versleutelde vorm aangetroffen. Eerder werd in deze CBA beschreven dat versleuteling tegenwoordig laagdrempelig en beschikbaar is, maar tegelijkertijd zo sterk geworden is dat de politie het achteraf moeizaam of niet kan ontsleutelen. Hierdoor dreigt bewijsvoering in bepaalde zaken onmogelijk te worden, en daarmee de verdachten onaantastbaar.

De enige wettelijke mogelijkheid die de politie momenteel tot zijn beschikking heeft, is het ontsleutelingsbevel van artikel 125k lid 2 Sv. Echter mag dat bevel alleen in het kader van de doorzoeking worden gegeven en dient het zich te richten tot eenieder, behalve de verdachte (die hoeft immers niet mee te werken aan zijn eigen veroordeling). In de praktijk is 'eenieder' vrijwel nooit op de hoogte van de versleuteling(stechnieken) van een verdachte. De criminelen zijn slim genoeg om hier voorzichtig mee om te gaan.

Op dit moment is er een discussie gaande over het wettelijk opnemen van een ontsleutelingsbevel aan de verdachte, binnen de grenzen van het nemo tenetur-

[92] De code voor deze exe-file is daarna actief gedeeld om zoveel mogelijk openheid te geven over de inhoud ervan.

beginsel. Verdachten worden in andere situaties, zoals bijvoorbeeld de vordering van een ademanalyse of bloedproef bij verkeerscontroles, of bij een vordering tot uitlevering van een vuurwapen, op een vergelijkbare manier benaderd. Dergelijke vorderingen worden niet beschouwd in strijd te zijn met het nemo tenetur-beginsel.

In Engeland kan een ontsleutelingsbevel wel tot een verdachte worden gericht. In Nederland lijkt de wetgever deze drempel nog niet te willen nemen. Er zijn namelijk nog meer obstakels, ook in praktische zin. Een verdachte kan zijn wachtwoord bijvoorbeeld vergeten zijn. Ook zou een ontsleutelingsbevel een negatieve invloed kunnen hebben op het algemeen gebruik van versleuteling, terwijl het in het kader van cyber security juist als waardevol wordt beschouwd.

7.5.5 Beslag en ontneming

In high tech crime onderzoeken komt het voor dat de behoefte ontstaat om zaken in beslag te nemen waarvan niet duidelijk is of dit wettelijk mogelijk is. Het gaat dan onder meer om IP-adressen, domeinnamen en digitale identiteiten.

IP-adressen en domeinnamen kunnen worden misbruikt voor het hosten van phishing websites, of voor de aansturing van botnets. Het neerhalen van dergelijke structuren kan dan zinvol zijn. In bepaalde gevallen is echter een vorm van beslag gewenst, bijvoorbeeld voor sporenonderzoek of om een botnet af te pakken. De huidige wetgeving is onduidelijk over de legaliteit hiervan.

In het eerder in deze CBA beschreven rechtshulpverzoek[93] uit de Verenigde Staten in verband met een DNS changer trojan, heeft het THTC vier IP-blokken door RIPE NCC (de RIR voor Europa en het Midden-Oosten[94]) laten bevriezen op grond van het eerder aangehaalde artikel 2 Politiewet. Zij hebben dit bevel aanvankelijk opgevolgd, maar hebben dit later weer opgeheven omdat zij van mening zijn dat artikel 2 Politiewet onvoldoende wettelijke grondslag biedt voor het doen geven van het bevel.

Tot slot het beslag en de ontneming van digitale entiteiten. Ook op dat gebied is er behoefte aan juridische kadering. In een onderzoek van het THTC bleek dat een high tech crimineel die 2 jaar had vastgezeten in Scandinavië direct na zijn invrijheidsstelling zijn daden weer oppakte met behulp van zijn eerder gebruikte

---

93 Zie paragraaf 3.5.2.

94 Zie hierover onder meer paragraaf 6.3.2.

ICQ-nummer. Hij stond op die manier gelijk weer wederzijds in contact met de rest van zijn criminele contacten en adverteert inmiddels weer openlijk met zijn oude (vertrouwde) ICQ-nummer. Beslag of ontneming van een dergelijke digitale identiteit zou zeer effectief kunnen zijn voor het voorkomen van verder misbruik ervan.

7.6 Conclusie

Met dit hoofdstuk werd een blik geworpen op een gedeelte van het juridisch kader dat betrekking heeft op high tech crime. Een opvallende constatering is dat Nederland, lang voordat er internationale afspraken werden vastgelegd in de Cybercrime Conventie, al wetgeving op het gebied van cybercrime kende.

Anno 2012 zijn de voor het aandachtsgebied relevante strafrechtelijke bepalingen zoveel mogelijk techniekneutraal geformuleerd. In de onderzoeken die het THTC heeft uitgevoerd blijken deze bepalingen echter niet altijd gelijke tred te kunnen houden met ontwikkelingen in het aandachtsgebied. Ten aanzien van high tech crime gaat het daarnaast vaak om dermate complexe materie dat de grenzen van de juridische kaders opgezocht en waar nodig opnieuw overwogen moeten worden om deze vorm van misdaad te kunnen bestrijden. Voornamelijk als het gaat om wetgeving op strafvordelijk gebied. De bevoegdheden die er nu zijn bieden niet altijd voldoende helderheid.

Vooralsnog worden het KLPD en het Openbaar Ministerie gedwongen om 'out of the (legal) box' te blijven denken. Snelle en effectieve bestrijding wordt gehinderd doordat nationale wetgeving niet internationaal toegepast mag worden. De rechtshulp die dan gezocht moeten worden, verloopt over het algemeen goed, maar het kan wel tot ernstige vertraging leiden. Dat is ongewenst in een aandachtsgebied waarin gegevens een vluchtig karakter hebben. Betere internationale afspraken over rechtshulp en andere vormen van samenwerking zijn daarom nodig.

8
Toekomst

8.1 Inleiding

Gefundeerde verwachtingen voor de toekomst staan aan de basis van een goed beleid op het gebied van high tech crime. Niemand heeft echter een kristallen bol en voorspellingen moeten daarom gezien worden voor wat ze zijn: verwachtingen, die in de loop van de tijd bijgesteld zullen moeten worden. Daar komt bij dat de ontwikkelingen op het gebied van high tech crime dermate snel gaan dat verder dan pakweg twee jaar in de toekomst kijken zinloos is.

Wat we kunnen en zullen doen is lijnen doortrekken. Ontwikkelingen die nu al plaatsvinden extrapoleren naar de nabije toekomst. Dat betekent dat we plotseling opkomende fenomenen kunnen missen. In de voorgaande CBA high tech crime (2009) hebben we met het doortrekken van de destijds actuele ontwikkelingen voorspellingen gedaan voor de periode 2010-2011, die in de meeste gevallen accuraat zijn gebleken. Echter is de plotselinge sterke opkomst van het hacktivisme daarin gemist. We zullen op deze ontwikkelingen terugblikken in paragraaf 8.2. Vervolgens zullen we de voorspellingen voor de komende jaren beschrijven in paragraaf 8.3 Hiermee is ook onderzoeksvraag 7 van het NDB beantwoord.

8.2 Terugblik

In deze terugblik zullen we de belangrijkste voorspellingen uit het CBA high tech crime 2009 op een rijtje zetten en evalueren.

8.2.1 Ontwikkelingen in omvang

We voorspelden dat het aantal groeperingen dat zich bezig houdt met enige vorm van high tech crime zou toenemen. De markt is nog niet verzadigd, en naarmate meer landen aansluiten op breedband internet komen er potentiële nieuwe slachtoffers en daders bij. Inderdaad hebben THTC en andere high tech crime units een toename gezien in het zaaksaanbod, waarbij niet alleen het aantal zaken maar ook de diversiteit van de zaken is toegenomen. Diversiteit is een indicator voor aantallen criminele samenwerkingsverbanden. Daarnaast

bleek de opkomst van nieuwe fenomenen zoals hacktivisme de groei in de hand te werken.

CSV's
Verwacht werd dat de omvang en structuur van criminele samenwerkingsverbanden op het gebied van high tech crime niet zou veranderen. Wel werd een toename verwacht in de hoeveelheid 'voetvolk' dat ingeschakeld zou worden. Het aantal groeperingen dat zich bezighoudt met high tech crime zou naar verwachting ook toenemen. Het blijkt niet eenvoudig om deze voorspellingen te staven, omdat er weinig gedegen en voldoende breed onderzoeksmateriaal van de afgelopen twee jaar voorhanden is. Uit opsporingsonderzoeken van het THTC en vergelijkbare buitenlandse opsporingsonderzoeken blijkt dat de omvang en organisatie van carrière-criminele groepen niet wezenlijk is veranderd. Money mule netwerken hebben zich uitgebreid met het werven van scholieren op het schoolplein.

8.2.2 Ontwikkelingen in aard

Een interessante ontwikkeling in de aard van het criminele verschijnsel is de verschuiving van motieven. In paragraaf 4.4.2 kwam reeds naar voren dat de factoren 'ideologie' en 'lol' een steeds belangrijkere rol in dat kader zijn gaan spelen. Dit kwam vooral tot uiting in de opmars van het hacktivisme.

Hacktivisme
De opmars van het hacktivisme, zoals die zich in de afgelopen jaren heeft voorgedaan, is een niet voorspelde ontwikkeling. Hoewel deze vorm van cybercrime al langer bestond is hacktivisme anno 2012 volstrekt verschillend van aard en omvang dan anno 2009. Anonymous was bijvoorbeeld al in 2006 actief, maar de omvang en impact van aanvallen van deze en dergelijke groepen werd pas goed duidelijk na de WikiLeaks affaire, eind 2010.

De meeste ontwikkelingen in de aard van het verschijnsel worden specifiek door technologische ontwikkelingen gedreven. In de volgende paragraaf zullen we de voorspellingen die in het vorige CBA op dat gebied gedaan zijn beschrijven.

8.2.3 Technologische ontwikkelingen

Verjaren van cryptografie
Net als in deze CBA werd in de vorige CBA aandacht besteed aan het verjaren van bepaalde cryptografiealgoritmes. Voorspeld werd dat dit zou leiden tot het

breken van algemeen gebruikte versleutelingen. Het breken van de GSM versleuteling en het MD5-algoritme zijn hier voorbeelden van.

Cloud

We verwachtten dat de beveiliging van cloud diensten onvoldoende zou blijven om er vertrouwelijke documenten aan toe te vertrouwen. Inderdaad zijn er nieuwe aanvalstechnieken ontstaan die zich specifiek op de cloud richten. Medio 2011 berichtte Google dat er honderden Gmail accounts waren gehackt. Ook verwachtten we dat het toenemend gebruik van cloud diensten opsporingsonderzoek zouden bemoeilijken. Dit is onverminderd van kracht, hoewel we er in de afgelopen jaren betrekkelijk weinig last van hebben gehad.

Malware voor mobiele telefoons

Er werd voorspeld dat malware voor mobiele telefoons sterk zou stijgen. Inderdaad is sprake geweest van een explosieve stijging, de hoeveelheid malware is echter nog een stuk kleiner dan die voor de PC platforms. Mobiele telefoons zijn ook zoals voorspeld succesvol in botnets opgenomen.

Web 2.0

Web 2.0 maakte een sterke groei mee, die nog steeds voortduurt. We verwachtten dat het zwaartepunt van de risico's zou verschuiven van het besturingssysteem naar de browsers en web-applicaties. Bij ongerichte aanvallen heeft deze verschuiving inderdaad plaatsgevonden. Daarnaast verwachtten we dat Web 2.0 datamining voor criminelen eenvoudiger zou maken, aangezien alles met alles verbonden is en mensen de neiging hebben teveel details van zichzelf (en anderen) online te zetten. Datamining en uitbuiting van Web 2.0 sites als Facebook en LinkedIn zijn ondertussen gemeengoed geworden. Daarnaast werd voorspeld dat Web 2.0 in toenemende mate zou worden gebruikt voor de aansturing van botnets. Dit is in de praktijk echter niet gebeurd.

Radiografische aanvallen

Er werd een toename voorspeld van draadloze radiografische aanvallen op apparatuur. Als voorbeeld werd genoemd de mogelijkheid tot het beïnvloeden van iemands pacemaker (en andere medische implantaten zoals insuline-pompen) op afstand. Hoewel er tot op heden geen aanvallen van dit type zijn waargenomen is er serieus aan deze dreiging gewerkt. In 2011 presenteerden wetenschappers een persoonlijke stoorzender die aanvallen op implantaten

moet voorkomen.[95] Hoe serieus dit type dreiging moet worden genomen bleek uit de bekendmaking van vermeende hacks op de Amerikaanse Landsat-7 en Terra AM-1 satellieten in 2007 en 2008.[96]

8.2.4 Aanvallen op vitale infrastructuren

Process control systemen
In de voorgaande CBA's werd gewaarschuwd voor het gemak waarmee industriële systemen gepenetreerd kunnen worden door kwetsbaarheden in SCADA software, en de risico's die dat met zich meebrengt. In de afgelopen periode hebben we hier verschillende voorbeelden van gezien. StuxNet heeft de ogen geopend van zowel IT security als van high tech criminelen.

Gebruik van DigID
In de vorige CBA werd belicht dat de beveiliging van het gebruik van DigID voor serieuze toepassingen diepgaande aandacht zou behoeven. De aan DigID gekoppelde gegevens zijn vanuit crimineel oogpunt namelijk zeer aantrekkelijk. In augustus 2011 kon de betrouwbaarheid van DigID certificaten niet langer gegarandeerd worden nadat de uitgever van deze certificaten, DigiNotar, gehackt bleek te zijn. In oktober 2011 kwam aan het licht dat bij 50 gemeenten de website een kwetsbaarheid bevatte waardoor de DigID sessie door aanvallers kon worden overgenomen.

8.2.5 Aanvallen op het financiële stelsel

Voorspeld werd dat de aanvallen op het betalingsverkeer, ondanks verscheidene verbeteringen in de beveiliging, door zouden gaan en zich aan zouden passen aan de nieuwe beveiliging. Inderdaad gaan de aanvallen op het betalingsverkeer onverminderd door.[97]

Invoering EMV chip
Er werd voorspeld dat de invoering van de EMV chip voor een tijdelijke daling van de schade als gevolg van skimmen zou leiden, tot de criminele wereld zich had aangepast. De exponentiële stijging van de schade is inderdaad een halt toegeroepen. De schade is in 2010 zelfs sterk gedaald. Vanaf het derde kwartaal

---

95 Dit werd gedemonstreerd op de SIGCOMM Communications Conference door een team van MIT en University of Massachussets in Amherst, in augustus 2011, in Toronto.

96 Dit is voor het eerst beschreven in: 2011 Report to congress of the U.S.-China economic and security review commission (2011).

97 Zie paragraaf 6.3.2.

2011 is echter weer een stijging waar te nemen. Waarschijnlijk hebben de criminelen hun laatste kans benut om misbruik te maken van de kwetsbaarheden van de magneetstrip voordat de EMV chip verplicht moest zijn ingevoerd per 1 januari 2012. Ondertussen hebben criminelen door de verschuiving van skimmen naar shimmen een nieuw wapen gevonden om de EMV chip aan te vallen.

Invoering SEPA
De invoering van SEPA (Single European Payment Area) is een grote stap vooruit in het Europese betalingsverkeer. In de vorige CBA werd echter voorzien dat criminelen misbruik zouden gaan maken van de snelheid van buitenlandoverboekingen naar bijvoorbeeld Eurolanden aan de grens van het SEPA gebied. De financiële wereld heeft deze dreiging in de afgelopen jaren serieus genomen en methodes geïmplementeerd om dergelijke overboekingen strenger te monitoren.

Social engineering en spear phishing
Voorspeld werd dat social engineering een belangrijk wapen zou blijven, en spear phishing zou toenemen. Die voorspelling is uitgekomen. ING en Rabobank hebben in 2010 last gehad van een tussenvariant, waarin mensen gebeld werden door iemand die zich voordeed als medewerker van de bank.

8.3 Vooruitblik

In de voorgaande hoofdstukken is de verwachte ontwikkeling per onderwerp reeds aangegeven. Onderzoeksvraag 7 ten behoeve van het NDB (verwachtingen voor de komende jaren) is hiermee al grotendeels beantwoord. In deze paragraaf zetten we onze toekomstverwachtingen nog eens op een rij.

8.3.1 Ontwikkelingen in omvang

De omvang van het fenomeen high tech crime is in het afgelopen decennium explosief gestegen. Mede daardoor is men zich bewuster geworden van de aanwezigheid en impact van het fenomeen en zijn er maatregelen genomen. Dit heeft een duidelijk dempende werking op de schade. Echter blijkt keer op keer dat de getroffen maatregelen slechts een tijdelijk effect hebben. Al snel weten de eerste aanvallers de maatregelen weer te omzeilen en moet nagedacht worden over weer nieuwe maatregelen. Daarnaast zorgt het voortdurend op de markt brengen van nieuwe technologie (technology push) zonder de tijd te kunnen nemen om de beveiliging goed op orde te brengen, steeds voor nieuwe

aanvalsvectoren. De protocollen waarop het internet gebaseerd is en die decennia lang hebben stand gehouden blijken nu allemaal toch gevoelig voor aanvallen. Al met al is er de komende jaren nog voldoende ruimte voor groei van cybercrime. De exponentiële groei van het afgelopen decennium lijkt wel af te vlakken. De verwachting is dat met de toenemende ICT-afhankelijkheid van de maatschappij aan de ene kant en de steeds laagdrempeligere toegang tot het aandachtsgebied (bijvoorbeeld middels het LOIC-tool) aan de andere kant de criminaliteit zeker niet tot stilstand zal komen.

8.3.2 Ontwikkelingen in aard

Hacktivisme
We verwachten de komende jaren meer voorbeelden te zien van hacktivistische aanvallen.

Dit als gevolg van een combinatie van factoren, zoals:
- De ronduit slechte beveiliging van veel websites en servers (gelegenheid);
- De beschikbaarheid van standaard hacking-toolsets (middel);
- Trendvolgers (proof of concept);
- Toenemende overheidsbemoeienis met het internet (motief).

Toenemende overheidsbemoeienis is gezien de cruciale rol die het internet in de huidige samenleving vertegenwoordigt onontkoombaar. Tegelijkertijd betekent het dat de vrijheid van het web, van oudsher het hoogste goed, beknot kan gaan worden. Dit zal ook in de komende jaren leiden tot rebellie in de vorm die het beste past bij het internet: hacktivisme. Daarbij moet rekening worden gehouden met het feit dat steeds minder mensen en minder kennis nodig zijn om maatschappelijk ontwrichtende aanvallen uit te voeren, en het feit dat de overheid, en daarmee de politie, doelwit zal zijn van dergelijke aanvallen.

Cyberspionage en cyberwarfare
Hoewel de schade als gevolg van cybercrime nog steeds een stijgende lijn laat zien is daarnaast ook waar te nemen dat andere partijen, in het bijzonder staten, zich in toenemende mate bedienen van dezelfde technieken ten behoeve van cyberspionage en (voorbereiding op) cyberwarfare[98]. Dergelijke aanvallen zullen in de regel groter opgezet, technologisch geavanceerder, en meer gericht zijn dan high tech crime. Deze nieuwe, geavanceerde aanvallen zorgen daardoor onbedoeld voor enorme evolutionaire sprongen in 'reguliere' high tech crime.

[98] Volgens de AIVD: AIVD - Jaarverslag 2010 (2011).

Tevens valt niet uit te sluiten dat expertise (mankracht, 0-days) ten behoeve van cyberspionage en cyberwarfare wordt ingekocht via de underground economy. Daarnaast is er geen duidelijke scheidslijn tussen de gebieden aan te geven. Dit grijze gebied, gecombineerd met het feit dat aan de voorkant niet duidelijk is wie de aanvaller is en wat zijn doelstellingen zijn, betekent dat de politie de komende tijd meer betrokken zal raken in zaken die onder de noemer cyberspionage/cyberwarfare vallen. Een goede afstemming met de AIVD en defensie zal dan ook op dit gebied in de toekomst nog harder nodig zijn dan het nu al is.

Nieuwe herkomstlanden
Binnen high tech crime geldt nog onverminderd dat landen als Rusland, Oekraïne en Roemenië de grootste herkomstlanden zijn voor op Nederland gerichte (financiële) criminaliteit. Er is geen reden om aan te nemen dat dit in de nabije toekomst verandert. Er is echter wel een stijging te zien van CSV's uit andere landen waar Nederland vroeg of laat slachtoffer van kan worden. Naast reeds genoemde landen als China en Brazilië kunnen ook andere landen zich als kandidaten aandienen. Voorwaarde lijkt te zijn een combinatie van een hoog opleidingsniveau met beperkte mogelijkheden voor het vinden van een passende baan. Dat laatste zal in sterke mate afhankelijk zijn van het economische klimaat.

Wederom is de verwachting dat de meeste ontwikkelingen in de aard van het verschijnsel gedreven zullen blijven worden door technologische ontwikkelingen. In de volgende paragraaf worden een aantal voorspellingen op dat gebied gedaan.

8.3.3 Technologische ontwikkelingen

Verjaren van cryptografie
Wat in het voorgaande CBA over versleuteling werd gezegd is nog steeds van kracht. Encryptietechnieken verouderen snel en worden tegelijkertijd zo breed ingezet dat vervanging langzaam en duur is. Dat betekent dat meer en meer breed ingezette technieken zoals GSM onveilig zijn geworden en de high tech crimineel meer middelen voor zowel ongerichte als gerichte aanvallen tot zijn beschikking heeft.

Van IPv4 naar IPv4 én IPv6
De adresruimte binnen het IPv4 protocol is op en IPv6 wordt momenteel uitgerold. Het zal waarschijnlijk echter nog decennia duren voordat IPv4 volkomen is verdwenen. In de tussentijd zullen de twee protocollen naast elkaar moeten bestaan. Hier is een aantal risico's aan verbonden. De overstap naar IPv6

kost providers geld. Enkele providers zullen naar creatieve oplossingen zoeken om de overstap zo lang mogelijk uit te stellen. Eén van de mogelijkheden is om verschillende klanten hetzelfde IPv4 adres te geven, waarbij de gegevens-pakketjes via Network Address Translation (NAT) naar de goede klant worden gestuurd. Een dergelijke oplossing maakt het voor de politie onmogelijk om op grond van een IP-adres eensluidend een fysiek adres vast te stellen, wat de opsporingsmogelijkheden ernstig beperkt. Daarnaast bestaat de situatie dat de besturingssystemen IPv6-ready zijn maar de netwerkbeveiliging nog niet, waardoor kwaadwillenden via IPv6 bij systemen binnen kunnen komen die niet bereikbaar zouden mogen zijn. Ook de implementatie van IPv6 bevat nog zwakke plekken die in de komende jaren ongetwijfeld aan het licht zullen komen, uitgebuit zullen worden, om vervolgens weer gerepareerd te worden.

Malware voor mobiele telefoons

Het gebruik van PC platforms wordt ingehaald door het gebruik van mobiele platforms op smartphones en tablets. Dit betekent een verschuiving in besturings-systeem en in de daarop ontwikkelde software. Momenteel is Windows XP 'marktleider' ten aanzien van de aantallen malwarepakketten. Daarbij moet overigens worden opgemerkt dat de browsers en de Adobe en Java platforms voor de meeste beveiligingsgaten zorgen. Hoewel de hoeveelheid malware voor het Windows platform vele malen groter is dan voor mobiele platforms is er reden om aan te nemen dat deze situatie in de komende jaren zal veranderen.

Naarmate het marktaandeel van de mobiele platforms toeneemt zal de hoeveelheid beschikbare malware voor deze systemen volgen. Android is marktleider bij de mobiele besturingssystemen en de prognoses zijn dat deze positie nog verder verstevigd zal worden. Daaruit volgt dat het Android besturingssysteem de meeste aanvallen te verduren zal krijgen. Van Android bestaan vele varianten, vaak aangeboden door telefoonfabrikanten of providers. Door deze extra laag sijpelen beveiligingsupdates langzaam door: niet alleen Android moet worden aangepast, maar voor elke nieuwe Android versie moet ook de software die er op gebouwd is aangepast worden. De aanbieders van op Android gebouwde besturingssystemen missen echter de prikkel om hun systeem snel aan te passen: hun marktmodel ligt in de verkoop van de telefoon, niet in de verkoop van het besturingssysteem. Mede daardoor is de gevoeligheid van handheld devices voor malware mogelijk nog groter dan voor Windows XP.

In 2014 wil Microsoft stoppen met de ondersteuning voor Windows XP. Dat betekent in eerste instantie dat een deel van de gebruikers zal overstappen op Windows 7 of Windows 8, maar ook dat een aanzienlijk deel van de gebruikers gebruik zal blijven maken van een besturingssysteem dat niet langer gepatcht

wordt. Gedurende een periode van enkele jaren zal XP daardoor een makkelijk doelwit zijn voor cybercriminelen.

Tegelijkertijd valt te verwachten dat de top van de high tech crime wereld zich zal gaan richten op de mobiele besturingssystemen. Aanvallen worden immers gericht op besturingssysteem met de relatief zwakste beveiliging en tegelijkertijd het grootste marktaandeel. De aanvallen op het Android OS zullen dan ook mede door het niet langer ondersteunen van XP sterk toenemen. Bovendien leveren aanvallen op smartphones een aantal nieuwe aanvalsvectoren op dat bij aanvallen op PC's niet bestaat, zoals het door de geïnfecteerde telefoon ongemerkt laten bellen naar dure betaalnummers.

De roboticarevolutie

Eerder in deze CBA werd reeds aangestipt dat er in 2011 malware is aangetroffen op de besturingssystemen van de onbemande vliegtuigen die het Amerikaanse leger in gebruik heeft (drones). Hiermee is een voorbeeld van de kwetsbaarheid van robots gegeven. De verwachting is dat de roboticarevolutie de komende jaren wereldwijd steeds grotere vormen zal aannemen. Robots zullen meer en meer ingezet worden voor gevaarlijk politie- en defensiewerk en zullen werkzaamheden (gaan) verrichten die mensen als vies, intensief of gevaarlijk beschouwen. Het Rathenau instituut[99] waarschuwt voor de kloven die er zijn tussen techniekontwikkelaars, beleidsmakers, politici, gebruikers en investeerders als het gaat om de inzet van robots. Het THTC neemt deze waarschuwing serieus en beseft dat de roboticarevolutie ook aan high tech criminelen nieuwe aanvalsvectoren biedt.

Verschuiving van doelwitten

Verwacht wordt dat er een verschuiving zal gaan plaatsvinden van aanvallen op grotere instellingen naar aanvallen op kleinere instellingen. De afgelopen periode viel al te zien dat het aantal gestolen records per inbraak is afgenomen terwijl het aantal inbraken is toegenomen[100]. Dit duidt op een verschuiving van grotere naar kleinere instellingen. Deze trend zal zich naar verwachting doorzetten.

Daarnaast valt een verdere stijging te verwachten van gerichte aanvallen: gerichte hacks, spear phishing, insiders en social engineering. De oorzaken

---

99 Het Rathenau Instituut bestudeert het wetenschapssysteem en de maatschappelijke gevolgen van nieuwe technologie en ondersteunt het maatschappelijk debat en de politieke oordeelsvorming hierover.

100 Verizon, 2011 Data Breach Investigations Report (2011), p. 24.

hiervan zijn de opkomst van (bedrijfs)cyberspionage en hacktivisme. Dit alles betekent overigens niet dat de huidige slachtoffers de komende jaren minder risico zullen lopen. Er is slechts sprake van een (lichte) verschuiving van het zwaartepunt.

8.3.4 Aanvallen op vitale infrastructuren

Process control systemen
Experts waarschuwden jaren geleden al dat SCADA software aanvalsgevoelig is, op verouderde en ongepatchte besturingssystemen draait en dat veel van dergelijke systemen op een onveilige manier op het internet zijn aangesloten. Desondanks is het jarenlang betrekkelijk rustig gebleven op dit gebied. Daar is in de afgelopen periode verandering in gekomen.

Wij denken dat we aan het begin staan van een periode van SCADA-aanvallen. Ten eerste omdat sinds StuxNet de bekendheid van dit soort systemen in de high tech crime wereld is toegenomen. StuxNet en andere aanvallen hebben laten zien dat aanvallen op process control systemen mogelijk en zelfs betrekkelijk eenvoudig kunnen zijn. Ten tweede omdat er momenteel meer dan voorheen motieven zijn om SCADA-systemen aan te vallen. Er zijn nieuwe spelers bijgekomen. SCADA-aanvallen kunnen goed ingezet worden voor het uitdragen van gedachtegoed door hacktivistische groeperingen of voor het aanvallen van concurrenten (cyberconflict of zelfs cyberwarfare).

Het internet
De DigiNotar hack heeft pijnlijk duidelijk gemaakt dat het internet zelf ook een vitale infrastructuur is, met verschillende vitale elementen die we mogelijk niet goed in zicht hebben. Het internet is gebouwd op protocollen die dateren uit de jaren ’80 van de vorige eeuw die niet ontworpen zijn voor het huidige gebruik. Deze protocollen hebben lang stand gehouden maar blijken nu toch een voor een gebreken te vertonen. Dit maakt nieuwe typen aanvallen mogelijk die gebruik maken van fouten in de onderliggende structuur van het web, of de manier waarop vertrouwen op het internet geregeld is. De stabiliteit van het internet zelf kan in gevaar komen. We hebben een dergelijke zwakheid al eerder gezien, toen Pakistan YouTube in 2008 wereldwijd onbereikbaar maakte. Dergelijke scenario’s kunnen zich in de toekomst herhalen.

8.3.5 Aanvallen op het financiële stelsel

Geld blijft de voornaamste drijfveer van high tech criminelen, en daarmee blijft het betalingsverkeer hun voornaamste doelwit. Zoals altijd kunnen we daarbij verwachten dat de criminelen de weg van de minste weerstand kiezen: als grote

banken hun beveiligingsniveau verbeteren verschuift de aandacht naar de kleinere banken; als met de invoering van de EMV chip een drempel wordt opgeworpen voor skimmen verschuift het zwaartepunt naar aanvallen op internetbankieren.

Verschuiving van skimmen naar shimmen

Met de invoering van de nieuwe EMV chip valt te verwachten dat de klassieke vormen van skimmen sterk af zullen nemen. De specificaties voor de implementatie van 'chip and pin' zijn echter tamelijk uitgebreid. Er zijn dan ook verschillende implementaties met ernstige fouten bekend, waardoor het bijvoorbeeld mogelijk wordt om bij een betaalterminal te betalen zonder pincode. Shimmen, waarbij de communicatie tussen chip en terminal wordt gemanipuleerd, lijkt dan ook een waardige opvolger van skimmen te kunnen worden.

9
Samenvatting en conclusies

In dit hoofdstuk worden de ontwikkelingen in het aandachtsgebied high tech crime voor bestrijding samengevat.

9.1 Criminaliteitsbeeld

Maatschappelijke en economische processen zijn in sterke mate afhankelijk van ICT. Er wordt voortdurend nieuwe technologie op de markt gebracht zonder dat er voldoende aandacht wordt besteed aan de beveiliging ervan. Ontwikkelingen in de techniek worden dan ook onmiddellijk gevolgd door hierop gebaseerde ontwikkelingen in high tech crime.

Kwetsbaarheden in beveiliging worden misbruikt om binnen te dringen in computersystemen- en netwerken en eventueel besmetting met malware te realiseren. Met malware besmette werken worden vaak onderdeel gemaakt van botnets om de aanvalsmogelijkheden en het aanvalsbereik te vergroten. Botnets kunnen ingezet worden voor uiteenlopende doeleinden en worden dan ook beschouwd als het Zwitsers zakmes voor de uitvoering van high tech crime. In aanvulling op het technisch arsenaal is social engineering, gericht op kwetsbaarheden in menselijk gedrag, nog altijd een belangrijk element in high tech crime ketens.

Massale aanvallen op random slachtoffers lijken iets af te nemen, terwijl het aantal gerichte aanvallen toeneemt. Criminelen laten hierdoor minder sporen achter. De motor van nieuwe ontwikkelingen op het gebied van high tech crime lijkt nog altijd een relatief kleine groep specialisten binnen de totale subjectenpool. Een uitzonderlijk hoog niveau van kennis en expertise stelt hen in staat geavanceerde aanvallen te ontwikkelen.

Dit maakt dat aanvallen op vitale infrastructuren geen theorie meer zijn, maar een actuele dreiging. Voorbeelden als StuxNet en in Nederland de hack op DigiNotar hebben dat in de afgelopen periode geïllustreerd. Vooral staten lijken motieven te hebben om (mogelijk met betrokkenheid van specialisten uit de cyber underground) tot dergelijke aanvallen over te gaan, maar ook de dreiging die van high tech criminelen zelf uitgaat op dit gebied moet niet onderschat worden. Tot op heden lijken de beroepscriminelen zich echter vooral te richten op aanvallen gericht op het financiële stelsel en in toenemende mate op andere

sectoren in het bedrijfsleven. De Nederlandse banken zagen de schade door fraude met internetbankieren in de afgelopen periode zeer sterk stijgen.

Technieken worden niet alleen steeds geavanceerder, maar zijn ook steeds meer beschikbaar voor een breder publiek. Compleet ingerichte kits worden (te koop) aangeboden op het internet. Dit stelt ook script kiddies in staat om als beroepscriminelen het financiële stelsel aan te vallen.

Het toenemende gebruikersgemak heeft er bovendien toe bijgedragen dat het hacktivisme in de afgelopen periode een hoge vlucht heeft genomen. Het lijkt tot op heden te gaan om verschillende amorfe groeperingen, voornamelijk (maar niet uitsluitend) bestaande uit script kiddies. Het blijkt dat zonder al te veel kennis een grote dreiging kan ontstaan voor vitale infrastructuren.

Dankzij de goede ICT infrastructuur fungeert Nederland ook binnen dit aandachtsgebied als doorvoerland. Facilitators zoals bulletproof hosting providers spelen daarbij een belangrijke rol door de cyberunderground in staat te stellen hun activiteiten uit het zicht van de politie te houden.

9.2 Bestrijding

De maatschappelijke aandacht voor cyber security is bij het uitbrengen van deze CBA groot. Grote incidenten en zichtbare dreigingen zorgen ervoor dat mensen steeds beter begrijpen welke risico's het gebruik van internet met zich meebrengt. Binnen cyber security is cybercrime een belangrijk thema. Het Team High Tech Crime is belast met de bestrijding van de meest zware, innovatieve, en georganiseerde vormen daarvan: high tech crime. Naast het neutraliseren van accute dreigingen door opsporing van daders wordt zoveel mogelijk gekozen voor een fenomeengerichte aanpak. Om maximaal effect te genereren in het aandachtsgebied ligt de focus op fenomenen die ten grondslag liggen aan verschillende criminaliteitsketens tegelijkertijd.

De fenomeengerichte aanpak is vooral uit de verf gekomen voor wat betreft de aanpak van botnets. Aangezien dit fenomeen nog steeds beschouwd kan worden als het Zwitsers zakmes voor high tech crime lijkt er geen reden om die focus te verschuiven. Daarnaast kan meer aandacht voor belangrijke Nederlandse facilitators, specifiek bulletproof hosting providers, effectief zijn. Bulletproof hosting providers zijn met name interessant omdat zij criminelen anonimiteit kunnen garanderen. Die anonimiteit wordt ook middels betere versleutelingstechnieken, het gebruik van TOR-netwerken en anonieme

betalingen, bijvoorbeeld middels bitcoins, gefaciliteerd. Overigens niet alleen als het gaat om high tech crime, maar ook bij fysieke misdaad. TOR faciliteert bijvoorbeeld ook kinderporno, wapenhandel en drugshandel. Om deze reden dient het THTC meer samenwerking te zoeken met units die zich met de bestrijding van dergelijke criminaliteit bezighouden. Uiteraard in de vorm van een wisselwerking om tot een optimale benutting van de wederzijdse expertise te komen. Financiële expertise is hier een goed voorbeeld van.

Het doel is om op basis van zo goed mogelijk inzicht in de criminele processen met de best passende middelen in te grijpen op die plekken in de keten waar het meest effect gesorteerd kan worden. Dit begint met een goede informatiepositie. Daar zal het THTC in de komende periode fors op investeren. Op basis daarvan kunnen gerichte interventies gekozen worden: zowel door middel van opsporen als tegenhouden. Bij iedere actie die in zulke gevallen wordt ondernomen wordt er een belangenafweging gemaakt tussen het opsporingsbelang enerzijds en grondrechten van de verdachten en derden anderzijds. Met name als het gaat om een inbreuk op het recht op privacy. Een passende aanpak betekent voorts dat waar relevant en mogelijk de aandacht niet alleen uitgaat naar het opsporen van daders, maar ook naar het ontmantelen van criminele infrastructuren en het waarschuwen van slachtoffers. Een dergelijke aanpak heeft in de afgelopen periode onder andere in het botnet-onderzoek Tolling gestalte gekregen. Om die in het verleden behaalde kwaliteit standaard te maken staat het beleid van het THTC de komende periode in het teken van groeien en consolideren.

Vanwege het grensoverschrijdende karakter van high tech crime vraagt effectieve bestrijding om centraal inzicht. Dit kan gelegen zijn in informatievoorziening, strategiebepaling en coördinatie op (minimaal) nationaal niveau. Op basis van dit inzicht kunnen er adequate maatregelen worden getroffen. De in 2011 geformuleerde Nationale Cyber Security Strategie (NCSS) heeft daartoe richtlijnen gegeven. Een direct resultaat hiervan is de uitbreiding van de capaciteit van het THTC van 30 naar 119 medewerkers in 2014 om het aantal grote HTC opsporingsonderzoeken per jaar te op te voeren naar 20. Ook zal de politie moeten investeren in regionale opsporingscapaciteit ten behoeve van de aanpak van cybercrime. In de NCSS is ook een belangrijke rol weggelegd voor het Programma Aanpak Cybercrime (PAC), dat een centrale rol gaat spelen in onder meer het opzetten van een kenniscentrum binnen de politie, de versterking van de politieorganisatie en het effectief verschuiven binnen de bestaande capaciteiten. Onder andere hiermee lijkt de NCSS een katalysator te worden om te voorzien in de behoefte aan een sluitende structuur voor de aanpak van cybercrime binnen de politie.

Een ander belangrijk resultaat van de NCSS is de inrichting van het Nationaal Cyber Security Centrum (NCSC). Daarbinnen brengen uiteenlopende publieke en private partijen, op basis van hun eigen taken en binnen de wettelijke mogelijkheden, informatie, kennis en expertise bij elkaar. Zo kan inzicht verkregen worden in ontwikkelingen, dreigingen en trends en kan ondersteuning worden geboden bij incidentafhandeling en crisisbesluitvorming. De politie, specifiek het THTC, is hierin vertegenwoordigd. Dit helpt afstemming met andere publieke partijen zoals de AIVD en defensie te verbeteren. Aangezien het THTC steeds vaker betrokken dreigt te raken bij zaken die onder de noemer cyberspionage of cyberwarfare geschaard worden is dat hard nodig. Ook publiek-private samenwerking op het gebied van cyber security wordt met dit centrum geïnstitutionaliseerd. Desalniettemin dient het THTC ook daarbuiten vanwege de unieke taakstelling zelfstandig te blijven investeren in publiek-private samenwerkingsverbanden ten behoeve van de bestrijding van high tech crime, zoals bijvoorbeeld de ECTF.

Samenwerking met internationale politiepartners is onontbeerlijk voor het THTC. Daartoe zijn in de afgelopen periode relaties met zowel herkomstlanden als landen waar relatief veel prioriteit gegeven wordt aan de aanpak van high tech crime wederom geïntensiveerd. Dit netwerk is cruciaal en verdient blijvend de aandacht. High tech crime houdt immers niet op bij landsgrenzen. In tegenstelling tot de klassieke domeinen land, lucht, water wordt de politie geconfronteerd met een domein dat veel grenzelozer en moeilijker bespeelbaar is. Vooral in juridische zin, omdat zelfstandig opsporingsonderzoek vanwege de soevereiniteit van staten nauwelijks mogelijk is. De huidige internationale regelgeving faciliteert alleen rechtshulp en samenwerking met partnerdiensten die elk hun eigen agenda en prioriteiten hebben. Dit veroorzaakt afhankelijkheid en vertraging in een onderzoek waardoor informatie verloren kan gaan of onnodig schade kan worden aangericht.

De dynamiek van het aandachtsgebied noopt ook op nationaal niveau tot een fundamentele discussie over de knelpunten in het huidige juridische kader. Enerzijds als het gaat om effectieve wetgeving die al dan niet specifiek geformuleerd zal moeten worden, anderzijds als het gaat om de kennis en kunde die politie-breed aanwezig zou moeten zijn om aan de bestaande juridische bevoegdheden uitvoering te kunnen geven.

De ontwikkelingen in het aandachtsgebied en de bestrijding ervan vertonen een toenemende mate van professionalisering en innovatie. Om hen enigszins bij te kunnen benen zal ook in de aanpak van high tech crime out of the box denken en innovatief rechercheren centraal moeten blijven staan.

Bronnenlijst

7Safe – UK Security Breach Investigations Report 2010 (2010)

AIVD – Jaarverslag 2009 (2010)

AIVD – Jaarverslag 2010 (2011)

Akamai – The state of the internet Q1 2011 (2011)

Akamai – The state of the internet Q2 2011 (2011)

Calce – Mafiaboy: Portrait of the hacker as a young man, Lyons Press (2011)

CBS – ICT, kennis en economie 2011 (2011)

Cisco Systems – 2011 Annual Report (2011)

Damballa – First half 2011 advanced threat report (2011)

Electronic Crimes Task Force – Criminaliteitsbeeldanalyse Bancaire Sector (2011)

Enisa – Country Reports 2009 (2010)

Enisa – Country Reports 2010 (2011)

Ernst & Young – ICT barometer over cybercrime (2011)

GOVCERT.nl – Factsheet FS2009-05 (2009)

GOVCERT.nl – Cloudcomputing & Security, whitepaper, versie 1.0 (2011)

GOVCERT.nl – Cybersecuritybeeld Nederland, december 2011 (2011)

GOVCERT.nl – IP versie 6, whitepaper, versie 1.2 (2010)

GOVCERT.nl – Nationaal Trendrapport Cybercrime en Digitale Veiligheid 2010 (2010)

Internet Crime Complaint Center – 2010 Internet Crime Report (2011)

Kaspersky – Kaspersky Security Bulletin, Malware Evolution 2010 (2011)

Koops – De dynamiek van cybercrime-wetgeving in Nederland, in: Justitiële Verkenningen 1/12 (WODC, maart 2012)

KLPD, Dienst IPOL – Georganiseerde criminaliteit in politieregio's (2010)

KLPD, Dienst Nationale Recherche, Team High Tech Crime – Kennisdocument Taurus: Ervaringen uit een proeftuin (2011)

KLPD, Dienst Nationale Recherche, Team High Tech Crime – CBA High Tech Crime 2009 (2010)

KPMG – Nieuwe perspectieven vragen om actie, een genuanceerde visie op cybercrime (2012)

Lovet – Dirty money on the wires (2007)

M86 Security – Security Labs Report, January - June 2011 recap (2011)

McAfee – McAfee Threats Report: First Quarter 2011 (2011)

McAfee – McAfee Threats Report: Second Quarter 2011 (2011)

McAfee – McAfee Threats Report: Third Quarter 2011 (2011)

Messagelab – May 2011 Intelligence Report, MessageLab Intelligence (2011)

Microsoft – Microsoft Security Intelligence Report, Volume 11 (2011)

Murdoch, Drimer, Anderson en Bond – Chip and PIN is Broken (IEEE Symposium on Security and Privacy, 2010)

Nederlandse Vereniging van Banken – Jaarverslag 2010 (2011)

Ohigashi en Morii – A Pratical Message Falsification Attack on WPA- Hiroshima University en Kobe University (2009)

Oswald en Paar – Breaking Mifare DESFire MF3ICD40: Power analysis and templates in the real world- Chair for embedded Security Ruhr-University Bochum (2011)

OPTA – Marktcijfers tweede kwartaal 2011

Panda Labs – Annual Report 2011

Rogers – A two-dimensional circumplex approach to the development of a hacker taxonomy (2006)

Rathenau Instituut- Het Bericht Overal Robots: 'Robotrevolutie vraagt om aandacht' (Bericht no. 5-2012: www.rathenau.nl).RSA – RSA 2012 Cybercrime trends report

Sophos – Security Threat Report: 2011 (2011)

Security Labs Report, January-June 2011 recap, Orange, CA: M86 Security (2011)

Shaked en Wool – Cracking the bluetooth pin- School of Electrical Engineering Systems (in co. with Intel) (2005)

Symantec – Norton cybercrime report - The human impact (2010)

Symantec.cloud MessageLab Intelligence – May 2011 Intelligence Report (2011)

Symantec, W32.Stuxnet, Stuxnet*:* www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99

Thuiswinkel marktmonitor (TMM) 2011, De Nederlandse thuiswinkelmarkt 2005-2011, Thuiswinkel.org (2011)

Trend Micro – The future of threats and threat technologies (2009)

U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION – 2011 Report to congress of the U.S.-China economic and security review commission (2011)

Van Eeten et al. – Internet service providers and botnet mitigation; A Fact-Finding Study on the Dutch Market (2011)

Verizon, 2010 Data Breach Investigations Report (2010)

Verizon, 2011 Data Breach Investigations Report (2011)

Begrippenlijst

0 – 9

0-day:
Een zero-day-aanval misbruikt een nog onbekende of niet gemelde zwakke plek in een computerprogramma. Ze zijn nog niet bekend bij de softwareontwikkelaar of er is nog geen oplossing (patch) beschikbaar om het gat te dichten. Zero-day exploits worden gebruikt of gedeeld door hackers voordat de softwareontwikkelaar weet heeft van de kwetsbaarheid.

A

Achterdeur:
Een achterdeur (of: backdoor) kan op verschillende manieren gebruikt worden. Oorspronkelijk was een backdoor een achterdeur in een computerprogramma, die met opzet door de programmeur was gemaakt. Door zo'n achterdeur kan een programmeur altijd in de door hem ontwikkelde programmatuur komen, ook als deze op andere computers geïnstalleerd is. De term backdoor wordt nu ook gebruikt voor een programma dat buiten medeweten van een computergebruiker op zijn of haar computer geïnstalleerd wordt, waarna aanvallers van buitenaf later toegang hebben tot de computer.

Admin/Administrator:
Een administrator van een server is over het algemeen de eigenaar of betalende voor een server. Het kan ook iemand zijn die door de eigenaar de rechten toegewezen heeft gekregen om deze te kunnen beheren. De rechten die de administrator op een server heeft worden ook wel admin rechten genoemd.

Adware:
Adware is de naam voor kleine programma's die, soms zonder dat deze worden opgemerkt, op een computer worden geïnstalleerd. Adware zit vaak bij gratis software. Adware wordt gebruikt voor pop-ups van advertenties maar wordt ook gebruikt om na te gaan waar de gebruiker zoal in is geïnteresseerd op het internet. Deze informatie wordt dan periodiek gestuurd naar een leverancier die deze informatie vervolgens weer gebruikt om gerichte reclame te sturen. Adware is een vorm van spyware.

Advance Persistent Threat:
Advanced Persistent Threat (APT) verwijst naar specifieke vormen van cyberspionage waarbij de actoren geavanceerde technologische kennis, technieken en middelen tot hun beschikking hebben (Advanced).

De actoren nemen de tijd om het netwerk van het slachtoffer binnen te dringen en te leren kennen. Daarnaast hebben ze langdurig toegang tot het netwerk (Persistent) teneinde hun kwaardaardige intenties (Threat) te verwezenlijken.

Antivirusprogramma:
Een antivirusprogramma controleert of een computer besmet is met (een) virus(sen). Daarnaast controleert een antivirusprogramma ook of een virus is verborgen in een bestand dat is gedownload of in een ontvangen e-mailbericht. Het antivirusprogramma kan op losse gegevensdragers en harde schijven zoeken naar virussen, maar ook herstellend optreden door het virus te verwijderen.

Application Programming Interface (API):
Een 'API is een verzameling definities op basis waarvan een computer-programma kan communiceren met een ander programma of onderdeel (meestal in de vorm van bibliotheken).

Assembly:
Basale programmeertaal waarin elke instructie één op één overeenkomt met een instructie in machinetaal.

ATM:
ATM staat voor Automated Teller Machine:

geld- of bankautomaat. Het is een apparaat waarmee met behulp van een betaalpas geld kan worden opgenomen.

Attachment:
bijlage van een e-mail. Het e-mailprotocol stelt in principe geen eisen aan vorm en formaat van attachments. Besmettingen via e-mail vinden plaats doordat een slachtoffer een besmet attachment opent.

B

Bandbreedte:
De hoeveelheid data die in een bepaalde tijd verzonden en ontvangen kan worden door een computer. De bandbreedte is afhankelijk van de snelheid van de verbinding en het aantal (andere) verbindingen. Een ouderwetse

telefoonmodem had een bandbreedte van 14,4kbit/s (14,4 kilobit per seconde), een drukbezochte website heeft eerder een bandbreedte van 1.000 Mbit/s (1000 megabit per seconde).

Bestand:
De logische eenheid voor gegevensopslag voor computergebruikers. Ieder bestand binnen een bestandssysteem heeft een uniek pad, bijvoorbeeld c:\windows\user.dat.

Bestandssyteem:
Een softwaresysteem dat zorg draagt voor de toegang van bestanden op een opslagmedium, vaak een harde schijf. De meeste bestandssystemen maken het mogelijk om bestanden hiërarchisch te organiseren in mappen. De wijze waarop bestanden worden opgeslagen is specifiek voor een bestandssysteem. Om de inhoud van een harde schijf goed te kunnen interpreteren is het noodzakelijk om te weten met welk bestandssysteem de bestanden naar de harde schijf zijn geschreven. Veel voorkomende bestandssystemen zijn FAT (in verschillende varianten, van Microsoft), NTFS (Microsoft), Ext2 (Linux) en Netware (Novell).

Besturingssysteem:
Het besturingssysteem maakt het de gebruiker mogelijk programma's te draaien op een computer. Het besturingssysteem verzorgt onder andere de communicatie met toetsenbord, muis, modem, webcam en netwerk. Voorbeelden van besturingssystemen zijn MS-DOS, Microsoft Windows 95/98/Me/NT/2000/XP/Vista, Unix, Linux, BSD en Apple MacOS.

Big data:
Big data staat voor gegevenssets die zo groot zijn dat ze met behulp van de standaardprogramma's niet meer beheerd of binnen redelijke tijd verwerkt kunnen worden.

Bluetooth:
Een techniek waarmee apparaten zoals mobiele telefoons, draadloos kunnen communiceren met andere apparaten. Met behulp van bluetooth is het op dit moment slechts mogelijk om over een beperkte afstand draadloos te communiceren.

Bootsector:
Diskettes en harde schijven bevatten een bootsector. Dit gedeelte van de schijf wordt als eerste ingelezen door de computer wanneer deze start. In dit gedeelte

van de schijf zorgen speciale programma's ervoor dat een besturingssysteem kan opstarten.

Bot:
Een bot is een geïnfecteerde computer die op afstand (met kwade bedoelingen) bestuurd wordt. Het woord 'bot' komt van robot. Een bot voert via een programma zelfstandig 'geautomatiseerd werk' uit. Een bot kan onschuldig zijn: zoekmachines gebruiken bots om websites in kaart te brengen. Maar bots worden ook ingezet om kwaadaardige handelingen uit te voeren op computers. Zo kan een bot volledige toegang krijgen tot informatie op een computer of deze als onderdeel van een botnet gebruiken bij criminele acties tegen anderen (zie ook: zombie).

Botnaam:
Indien een IRC server gebruikt wordt als command and control server melden de bots zich aan in een IRC kanaal. Bij het aanmelden op IRC dient een unieke naam opgegeven te worden. Bots die met een command and control server verbinden gebruiken daarom meestal een naam waarin bijvoorbeeld hun IP-adres, of ander uniek gegeven van de besmette computer, verwerkt is. Vaak is deze informatie versleuteld in de naam weergegeven. Ook kan in de naam, al dan niet versleuteld, locatie, internetsnelheid of up-time staan.

Botnet:
Een botnet is een netwerk van aan het internet verbonden gecompromitteerde computers die op afstand kunnen worden aangestuurd, zonder medeweten of goedkeuring van de eigenaar. De gecompromitteerde computers worden wel bots of zombies genoemd. De term botnet is een verkorting van de woorden robot en netwerk. De eigenaar of aanstuurder van het botnet wordt botnet herder genoemd.

Botnet herder:
De persoon die het beheer heeft over het botnet.

Broncode:
De broncode van een computerprogramma is de code die door de programmeur in een formele programmeertaal is geschreven. Dit staat tegenover de uitvoerbare code of machinetaal voor de processor zoals die door een compiler of interpreter vanuit de broncode gegenereerd wordt.

Browser:
Een browser is een programma waarmee pagina's (websites) op internet bekeken kunnen worden. De browser zet HTML-pagina's om in leesbare tekst. Er zijn verschillende browsers zoals Mozilla Firefox, Opera, Safari en Microsoft Internet Explorer.

Bruteforce:
Bruteforce houdt in dat binnen een opgegeven range elk mogelijk wachtwoord wordt gegenereerd en vergeleken met het gecrypte wachtwoord.

Bulletproof hosting:
Het aanbieden van hosting service (de mogelijkheid om websites te plaatsen) waarbij de mogelijkheid wordt geboden om illegale activiteiten te ontplooien en waarbij zorg wordt gedragen dat de identiteitsgegevens van de gebruikers van de service worden afgeschermd. Voorbeelden: RBN (Russian Business Network), McColo, 3FN.

Byte:
Een byte is gedefinieerd als 8 bits. Een byte heeft 256 verschillende mogelijke waarden.

C

Card not present:
Transacties waarbij de creditcard niet aanwezig is, alleen de gegevens op de kaart zijn voldoende. Dit is meestal het geval bij internettransacties. Het gevolg is dat hierbij vaak gevraagd wordt om extra gegevens op de kaart zoals de card security code.

Chatprogramma:
Chatprogramma is een populaire benaming voor een programma waarmee direct met andere computergebruikers gecommuniceerd kan worden. Bekende voorbeelden zijn: MSN Messenger, ICQ en IRC.

Certificaat:
Een digitaal certificaat wordt gebruikt om te kunnen aantonen dat een website de site is die hij beweert te zijn. Beveiligde verbindingen maken gebruik van certificaten. Een voorbeeld hiervan zijn de https:// webpagina's (deze zijn ook te herkennen aan het slotje onderin de browser). Certificaten worden uitgegeven door een certificate authority.

Certificate Authority:
Een Certificate Authority (CA) (ook wel certificaatautoriteit of Certification Authority) is in de cryptografie een entiteit die digitale certificaten verleent aan andere partijen. De bedoeling is dat het digitale certificaat bewijst dat de eigenaar daadwerkelijk degene is die hij beweert te zijn. Een certificaatautoriteit is een voorbeeld van een 'trusted third party'. CA's zijn kenmerkend voor veel schema's met een 'Public Key Infrastructure' (PKI).

Chip & Pin:
Creditcard met chip en pincode, ter vervanging van het gebruik van de magneetstrip.

Client:
Een computersysteem dat een dienst vereist van een ander computersysteem. De client vraagt diensten van een andere computer of computerprogramma, de server. Een werkstation dat bijvoorbeeld de inhoud van een bestand opvraagt bij een file server is een client van de file server.

Client server:
Client server is de benaming voor een structuur achter een computernetwerk waarbij diverse clients communiceren met één of enkele servers. Een typisch voorbeeld van een dergelijke structuur is te vinden bij het controleren van e-mail. Een computer die controleert of er nieuwe e-mail is, legt verbinding met een (centrale) server waar deze staat opgeslagen.

Cloud:
Met de term cloud wordt in eerste instantie het internet bedoeld. Meer specifiek wordt bedoeld het opslaan en verwerken van gegevens via het internet. In het cloud model zijn data en rekencapaciteit online beschikbaar zonder dat bekend is waar de data is opgeslagen en welke computers het rekenwerk uitvoeren. De fysieke locatie van opslag en rekencapaciteit wisselt en doet binnen het cloud model niet ter zake. Het model kan gemak en kostenbesparing opleveren, de beveiliging van het cloud model staat echter nog in de kinderschoenen. Ook voor opsporingsdiensten levert de cloud de nodige uitdagingen op, bijvoorbeeld omdat in beslag te nemen data verspreid kan zijn over verschillende opslagmedia.

CNP:
Zie card not present.

Command and control server:
Dit begrip refereert naar een server, die vaak centraal geplaatst is, waar individuele computers zich aanmelden in afwachting van opdrachten. Deze worden verstrekt door een botnet herder.

Configuratie:
Een verzameling van instellingen van een programma of hardware.

Cookie:
Een cookie is een bestandje dat door een website op de harde schijf van een bezoeker wordt geplaatst. Dit bestandje kan op een later moment door dezelfde website ook weer uitgelezen worden. Cookies worden vaak gebruikt voor identificatie van bezoekers van websites. Ze bevatten informatie als datum en tijd van bezoek en namen van bezochte pagina's.

Crash:
Het vastlopen van een computer of een computerprogramma noemt men een crash. Dikwijls kan het vastgelopen computerprogramma niet meer worden afgesloten en moet de computer worden uit- en aangezet. Vaak is het een combinatie van software, hardware en gebruiker die de computer laat vastlopen.

Crawler:
Een algoritme die het internet continu afzoekt op zoek naar nieuwe of vernieuwde webpagina`s.

Crimeware:
Zie malware.

Cross site scripting:
Een aanvalstaktiek waarbij het adres van een hiervoor kwetsbare website wordt misbruikt om extra informatie te tonen of programma's uit te voeren. Er zijn diverse vormen van cross site scripting waarbij complexe aanvallen mogelijk zijn.

Cryptografie:
Cryptografie of geheimschrift houdt zich bezig met technieken voor het zodanig versleutelen van te verzenden informatie, dat het voor een cryptoanalist, een persoon die toegang heeft tot het kanaal tussen zender en ontvanger, en dus als het ware 'mee kan luisteren', onmogelijk is om tegen aanvaardbare inspanning uit de getransporteerde data af te leiden welke informatie er door de zender was verzonden. Enkel de zender en ontvanger beschikken over de juiste sleutel (key) om de gegevens terug om te zetten in hun originele vorm.

CSV:
Crimineel samenwerkingsverband (CSV) is een term waarmee de Nederandse politie al jarenlang werkt. Sinds enkele jaren wordt het denken over de betrokkenen bij georganiseerde misdaad voor een deel gedomineerd door de gedachte dat er allerlei groepen zijn die in wisselende samenstelling (winstgevende) misdaden plegen: dit zijn de CSV's.

CVE-database:
De CVE-database is een genummerde lijst van alle gemelde ICT-kwetsbaarheden wereldwijd.

Cybercrime:
Cybercrime omvat elke strafbare gedraging voor de uitvoering waarvan het gebruik van geautomatiseerde werken bij de verwerking en overdracht van gegevens van overwegende betekenis is.

Cyber security:
Cyber security is het overkoepelende begrip voor beveiliging van informatie, systemen en netwerken. De dreigingen op dat gebied worden in het algemeen onder een van de volgende deelgebieden geschaard: cybercrime, cyberactivisme, cyberspionage, cyberterrorisme en cyberconflict/-warfare.

D

Database:
Een database is de naam voor een bestand of verzameling bestanden waarin gegevens gestructureerd zijn vastgelegd. Door de structuur is het eenvoudig om gegevens te vinden of statistieken en overzichten te maken.

Datalek (data breach):
Het onopzettelijk naar buiten komen van vertrouwelijke gegevens.

Decryptie:
Bestandsgegevens terugzetten die door middel van een speciale code beveiligd zijn, zodat die gegevens gelezen kunnen worden. Zie encryptie.

Defacement:
Het onbevoegd en vaak met kwaadaardige intentie vervangen of beschadigen van de inhoud van een bestaande webpagina. Vaak gebeurt dit door aanvallers die zichzelf op onrechtmatige wijze toegang hebben weten te verschaffen tot een webserver.

(Distributed) Denial of Service (DoS)-aanval:
Een actie waarbij wordt geprobeerd een computer, een systeem of telecommunicatienetwerk zo te belasten of te manipuleren, dat deze wordt uitgeschakeld en niet meer beschikbaar is voor (bevoegde) gebruikers. DoS houdt in dat een computer continu 'aangevallen' wordt door bijvoorbeeld e-mail of ander netwerkverkeer. Bij een Distributed Denial of Service-aanval (DDoS) wordt door een groot aantal computers tegelijk een gecoördineerde aanval uitgevoerd.

DNS:
DNS (Domain Name System) is een techniek om de onpraktische IP-adressen te koppelen aan leesbare en begrijpelijke domeinnamen. Een DNS-server vertaalt niet, omdat er geen enkele logica zit in de domeinnamen en IP-adressen. DNS wordt gebruikt op het internet maar ook in bedrijfsnetwerken.

Drop:
Tussenpersoon die wordt gebruikt om geld en goederen door te sluizen. De tussenpersonen krijgen een percentage en versluieren het pad naar de crimineel. Zie ook money mule, katvanger. Drop is een generieke term. Money mules sluizen alleen geld door, drops kunnen ook goederen doorgeven.

Dropzone:
Computersysteem waar gestolen gegevens (tijdelijk) worden opgeslagen.

Downloaden:
Het binnenhalen van een bestand van een andere computer naar een eigen computer noemt men downloaden. Het bestand kan een computerprogramma, tekst, beeld, video of geluid zijn.

E

EMV chip:
Chip in betaalkaarten, volgens de standaard opgesteld door Europay, Mastercard en Visa. De chip maakt de combinatie chip & pin mogelijk ter vervanging van bestaande creditcardtransacties en magneetstrip-pintransacties. De EMV chip is een belangrijk wapen in de strijd tegen fraude en skimming.

Encryptie:
Door informatie te versleutelen (encryptie), kan voorkomen worden dat die informatie door onbevoegden gebruikt wordt. Dit is belangrijk bij gevoelige informatie zoals gebruikersnamen en wachtwoorden, maar kan ook bij e-mails

essentieel zijn. In de praktijk wordt bij versleuteling vooral gebruik gemaakt van de public key encryption methode.

Exploit:
Een kwaadaardig programma of computercode waarmee misbruik kan worden gemaakt van een kwetsbaarheid in programma's of een besturingssysteem om zo niet-normaal gedrag te creëren op een computersysteem. Exploits voor bekende kwetsbaarheden zijn soms makkelijk te vinden op het internet.

F

Facebook:
Een sociale netwerksite waar mensen online contact onderhouden met hun vrienden. De meeste mensen schrijven zich in onder hun eigen naam en voeren ook persoonlijke gegevens zoals hun geboortedatum in. Bij de verkeerde veiligheidssettings kan dit criminelen de gelegenheid bieden om deze persoonlijke gegevens te gebruiken om bijvoorbeeld gestolen creditcardgegevens te verrijken. Daarnaast worden facebook-accounts gebruikt om te spammen.

Fast flux:
Als de netwerk- of IP-adressen van een domeinnaam van bijvoorbeeld een phishingsite of command and control server snel wijzigen om de dienst te beschermen tegen uitschakelen, wordt gesproken van de fast-flux- DNS-techniek.

File transfer:
Kopiëren van bestanden via het netwerk.

Firewall:
Een apparaat of programma dat, mits van voldoende kwaliteit en goed geconfigureerd, bescherming biedt tegen een aantal gevaren op internet. Een firewall zal netwerkverkeer bekijken en op basis van vooraf ingestelde regels bepalen of het verkeer toegestaan is of niet.

Firewire:
Een standaard voor gegevensoverdracht die een zeer snelle verbinding tussen computer en randapparatuur mogelijk maakt. Hiertoe moet de randapparatuur via een firewire-kabel op de computer aangesloten te zijn. Een alternatieve technologie is USB.

Forum:
Een forum bestaat uit digitale discussiepagina's op het internet. Op ingedeelde onderwerpen kan vrijwel iedereen reageren via een formulier. Op sommige internetforums is het nodig om je als bezoeker te registreren onder een bijnaam (nickname) voordat gereageerd kan worden op berichten. De virtuele persoonlijkheid van een forumbezoeker kan naast het gebruik van bijnamen ook tot uiting komen in het gebruik van persoonlijke plaatjes en zogeheten handtekeningen.

Fraude:
Fraude is een opzettelijke handeling waarbij door het geven van een onjuiste voorstelling van zaken een gepretendeerde rechtvaardiging voor de handeling ontstaat, waarmee onrechtmatig voordeel wordt verkregen.

FTP:
File Transfer Protocol (FTP) is een protocol dat uitwisseling van bestanden tussen computersystemen vereenvoudigt. Een internetgebruiker heeft vaak een programma op zijn of haar PC geïnstalleerd dat verbinding kan maken met zogenaamde FTP-servers. Met behulp van zo'n FTP-programma kunnen bestanden worden geplaatst of gelezen van een FTP-server.

G

Geautomatiseerd werk:
Een geautomatiseerd werk is een inrichting die bestemd is om langs elektronische weg gegevens op te slaan, te verwerken en over te dragen. Hieronder vallen computer- en netwerkapparatuur of -systemen, elektronische gegevensdragers of telecommunicatienetwerken, telefoon en fax. Onder geautomatiseerde werken vallen dus 'de middelen van informatie- en communicatietechniek'.

Gedeelde map:
Een gedeelde map is een map met bestanden die niet alleen op een bepaalde computer, maar ook via een netwerk te bekijken is. In bedrijven worden op servers vaak mappen gedeeld waarop gezamenlijke bestanden staan.

Gegevens:
Iedere weergave van feiten, begrippen of instructies, op een overeengekomen wijze, geschikt voor overdracht, interpretatie of verwerking door personen of geautomatiseerde werken. Hieronder vallen dus alle op een elektronische gegevensdrager, computer of ander geautomatiseerd werk verwerkte of opgeslagen informatie. Het begrip 'gegevens' omvat niet alleen gegevens die

zijn opgeslagen in geautomatiseerde werken, maar ook de programmagegevens voor besturing van de computer.

H

Hacker:
In positieve zin is een hacker een persoon die zwakke plekken op computersystemen of software aantoont, zonder er verder misbruik van te maken. In de volksmond zijn hackers mensen die op systemen proberen in te breken. Dit zijn eigenlijk 'crackers'.

Hacktivisme:
Het inzetten van computers en telecommunicatienetwerken om een ideologisch of politiek doel te bereiken. Aanvallen richten zich bijvoorbeeld op het beschadigen of onbereikbaar maken van websites en internetvoorzieningen van tegenstanders.

Hardware:
Alle tastbare onderdelen van de computer, bijvoorbeeld: toetsenbord, kabels, harde schijf, maar ook alle andere ICT-gerelateerde apparaten zoals routers en hubs.

Hashwaarde:
Een hashwaarde is het resultaat van een cryptografische hashfunctie. Deze zet de waarde van een invoer om in een (meestal) kleiner bereik van karaktertekens. De uitkomst is een onbegrijpelijke reeks van tekens met zeer weinig kans dat twee verschillende invoerwaarden dezelfde uitvoer geven. Bovendien is het zeer moeilijk om de oorspronkelijke invoerwaarde af te leiden. Een typische toepassing is het versleutelen van wachtwoorden of het berekenen van controlewaarden (checksums).

Honeypot:
Een computersysteem dat bewust kwetsbaar is gemaakt voor verschillende types aanvallen. Het doel is om de honeypot te laten besmetten met malware, waarna deze geanalyseerd kan worden.

Hotspot:
Een publieke locatie (hotel, tankstation) waar, al dan niet tegen betaling, draadloos toegang tot het internet verkregen kan worden.

HTML:
HTML staat voor Hypertext Markup Language: een verzameling codes die gebruikt wordt om de opmaak van een tekst te beschrijven. HTML wordt

voornamelijk gebruikt voor de opmaak van webpagina's, waarbij het de browser (bijvoorbeeld Netscape of Opera) is die de opmaakcodes omzet in de uiteindelijke opmaak, zoals dikgedrukte of schuingedrukte tekst.

I

ICANN:
Internet Corporation for Assigned Names and Numbers. Onder meer beheerder van de Internet Protocol Address Space, IPv4 en IPv6.

ICQ:
Zie Instant Message.

IFrame-injectie:
Malafide en onzichtbare toevoeging aan een gehackte site waardoor bezoekers van deze site blootstaan aan een poging tot infectie.

Image:
Een digitale kopie van een datadrager zoals een harddisk of een USB-stick.

Instant Message (IM):
Een algemene term voor een vorm van realtime communicatie over een netwerk zoals het internetverkeer tussen twee of meer mensen, gebaseerd op tekst. Veelgebruikte IM netwerken/protocollen zijn onder andere AIM (AOL Instant Messenger), ICQ, Yahoo IM, MSN Messenger en Google Talk. IRC (zie aldaar) wordt door sommigen ook als IM gezien, maar gedraagt zich net anders.

Integriteit:
Een kwaliteitskenmerk voor gegevens, een object of dienst in het kader van de (informatie)beveiliging. Het is een synoniem voor betrouwbaarheid. Een betrouwbaar gegeven is juist (rechtmatigheid), volledig (niet te veel en niet te weinig), tijdig (op tijd) en geautoriseerd (gemuteerd door een persoon die gerechtigd is de mutatie aan te brengen).

Intrusion Detection System (IDS):
Dit is software die alarm slaat als het pogingen detecteert van ongeoorloofde toegang tot een netwerk.

IP-adres:
Een adres waarmee een apparaat aangesloten op een computernetwerk eenduidig (logisch) kan worden geadresseerd binnen het TCP/IP-model. Het Internet Protocol-adres verbindt elke computer met een telecommunicatie-

netwerk of het internet via een uniek IP-adres, dat gebruikt wordt voor het bepalen van bestemming en herkomst van netwerkverkeer.

IPv4:
Internet protocol versie 4. Het protocol dat gebruikt wordt om IP-adressen weer te geven. Een IP-adres volgens dit protocol ziet er bijvoorbeeld als volgt uit: 192.168.0.1.

Dit protocol maakt het mogelijk om 232 adressen uit de delen, oftewel ongeveer 4 miljard. Op topniveau zijn alle blokken met IPv4 adressen uitgegeven. Daarmee zijn de adressen op. De voorgestelde oplossing is een overstap op IPv6.

IPv6:
Internet protocol versie 6, de opvolger van IPv4 (er is geen IPv5). Dit nieuwe internet protocol maakt het mogelijk om veel meer IP-adressen uit te geven en lost daarnaast nog een aantal onvolkomenheden van het IPv4 protocol op. Het aantal IPv6 adressen is 2128. Als we ons de IPv4 adresruimte voorstellen als ongeveer een tennisbal, dan is de IPv6 adresruimte ongeveer zo groot als de aarde. Adressen volgens dit protocol zien er bijvoorbeeld zo uit: 2001:0db8:85a 3:0000:0000:8a2e:0370:7334 (afgekort als 2001:db8:85a3::8a2e:370:7334).

Internet Relay Chat (IRC):
IRC is een elektronische babbelbox van het internet. Door in te loggen op een IRC-server kan met meerdere mensen tegelijk, of met één netgebruiker apart, worden gecommuniceerd door getypte boodschappen uit te wisselen. IRC bestaat uit zogenoemde kanalen die ieder hun eigen onderwerp hebben, zodat gerichte discussies kunnen plaatsvinden.

IRC-Bot:
Een IRC-bot is een programma geschreven om een PC automatisch te verbinden met een IRC-server. Zo'n programma kan na verbinding met een IRC-server worden aangestuurd door de IRC-server voor het uitvoeren van bepaalde handelingen. IRC-bots zijn goed bedoeld maar tegenwoordig wordt IRC-bot software vaak geïnstalleerd als onderdeel van een worm om zo een aanvaller volledige toegang te geven tot een besmet systeem via een IRC-netwerk.

Internet Service Provider:
Leverancier van internetdiensten, vaak simpelweg aangeduid als 'provider'. De geleverde diensten kunnen zowel betrekking hebben op de internetverbinding zelf als op de diensten die men op het internet kan gebruiken.

K

Katvanger:
Zie money mule.

Keylogger:
Een keylogger is een programma dat bijhoudt welke toetsen een gebruiker aanslaat. Deze gegevens kunnen vervolgens via het internet of per e-mail onopgemerkt verstuurd worden naar een kwaadwillende. Keyloggers zijn een van de verschijningsvormen van spyware

Klik-fraude:
Een frauduleuze manier van omgaan met de op internet gebruikelijke manier van betalen voor reclame, de pay per click. De adverteerder betaalt voor elke keer dat er op zijn reclame-uiting wordt geklikt. Door bijvoorbeeld met een botnet artificiële clicks te genereren kan frauduleus geld verdiend worden.

Kwetsbaarheid (vulnerability):
Een kwetsbaarheid is een zwakke plek in een proces, object, software of hardware dat kan worden misbruikt door één of meerdere dreigingen. Kwetsbaarheden kunnen worden gekwalificeerd als *enorm* (E), *groot* (G), *behoorlijk* (B), *minimum* (M) of *verwaarloosbaar* (V), afhankelijk van de vatbaarheid voor de betreffende zwakte en de gevolgen daarvan.

L

LinkedIn:
LinkedIn is een virtueel sociaal netwerk dat zicht richt op personen in het beroepsleven.

M

Malware:
Samentrekking van malicious (kwaadaardig) en software. Verzamelnaam voor software met kwaadaardige bedoelingen zoals virussen, wormen, trojans, keyloggers, spyware, adware en bots.

Man-in-the-middle-aanval:
Een aanval waarbij de aanvaller zich tussen een klant (client) en een dienst (service) bevindt. Hierbij doet hij zich richting de klant voor als de dienst en andersom. Als tussenpersoon kan de aanvaller nu uitgewisselde gegevens afluisteren en/ of manipuleren.

Money mule:
Een money mule is iemand die frauduleus verkregen geld (en soms ook goederen) doorsluist naar criminelen. De money mule fungeert als tussenstation en helpt de identiteit van de crimineel te versluieren. Money mules worden ook wel drops of katvangers genoemd. De money mule zelf is vaak een naïef (of misleid) persoon die zijn bankrekening beschikbaar stelt voor transacties. De aansturing van money mules is een professionele business.

MSN:
Windows Live Messenger (WLM) is de huidige naam van de Instant Messaging dienst van het Microsoft Windows Live platform. Deze heette voorheen MSN Messenger (vóór versie 8), de naam waaronder het programma het meest bekend is. Met dit programma kunnen gebruikers met een Windows Live ID elkaar digitale berichten sturen. Daarnaast biedt Windows Live Messenger ondersteuning voor audio en video. Ook is het mogelijk om spelletjes te spelen, winks te versturen (kleine Flash -filmpjes die automatisch worden afgespeeld), dynamische schermafbeeldingen te gebruiken, enzovoorts.

N
Nickname:
Bijnaam. Alter ego van een persoon op het internet. Ook: handle.

O
Online:
Wanneer een gebruiker verbinding heeft met een andere computer of met het internet is hij online. Door middel van een telefoonlijn met modem of een ADSL-modem kan via een internet service provider (zie provider) verbinding worden gemaakt met het internet.

Operating System (OS):
Besturingssysteem van een computer. De basissoftware waarop alle programma's draaien. Voorbeelden: Windows XP, Windows 7, Linux, Unix, OpenSolaris.

Overnemen:
Het kopiëren van bestaande opgeslagen gegevens van een geautomatiseerd werk.

P

Password:
Wachtwoord om toegang te krijgen tot een bepaalde computer, netwerk of website.

Patch:
Een patch (letterlijk 'pleister') kan bestaan uit reparatiesoftware of kan wijzigingen bevatten die direct in een programma worden doorgevoerd om dat programma te repareren of te verbeteren.

Paypal:
Winkels kunnen zich bij paypal aansluiten. Klanten kunnen vervolgens met Paypal betalingen doen. De betalingen worden van de creditcard van de klant afgeschreven zonder dat de persoons- en creditcardgegevens aan de winkelier bekend worden.

Peer-to-peer:
Een computernetwerk waarin de aangesloten computers gelijkwaardig zijn. Een peer-to-peer-netwerk kent geen vaste werkstations en servers, maar heeft een aantal gelijkwaardige aansluitingen die tegelijkertijd functioneren als server en als werkstation voor de andere aansluitingen in het netwerk. Bestanden die via P2P-netwerken worden uitgewisseld, worden in delen binnengehaald en tegelijkertijd weer gedeeld.

Pharming:
Poging om via digitale middelen, vaak in combinatie met hacking, identiteits-gegevens te ontfutselen.

Phishing:
Phishing is een verzamelnaam voor digitale activiteiten die ten doel hebben persoonlijke informatie aan mensen te ontfutselen. Een vorm van phishing is mensen lokken naar een valse website, die een kopie is van de echte website en ze daar (nietsvermoedend) zich laten aanmelden. De fraudeur krijgt hierdoor de beschikking over de inloggegevens van het slachtoffer met alle gevolgen van dien. De slachtoffers worden vaak via e-mail naar de valse website gelokt. De persoonlijke informatie kan direct worden misbruikt voor het doen van bijvoorbeeld grote uitgaven (in het geval van creditcardnummers) of voor wat in het Engels 'identity theft' wordt genoemd, het stelen van een identiteit. Dan zijn gegevens als burgerservicenummers (BSN), adressen en geboortedata nodig.

PKI:
De Public Key Infrastructure (PKI) is een systeem waarmee uitgiften en beheer van digitale certificaten kan wordt gerealiseerd.

Platform:
Verzamelnaam voor een besturingssysteem en bijbehorende apparatuur. Bijvoorbeeld Windows-platform, UNIX-platform en Linux-platform.

Polymorfe malware:
Malware die verschillende vormen aanneemt, afhankelijk van de gebruikte software (webbrowser of besturingssysteem) van het slachtoffer.

Poort:
Een poort (port) is een gedefinieerd communicatiekanaal op een computer. Op het moment dat communicatie tussen twee computers plaatsvindt, zal aan beide kanten een programma aanstaan dat ingesteld is om een bepaalde poort te gebruiken. Elke toepassing op een computer gebruikt een specifiek communicatiekanaal om met een andere computer gegevens te kunnen uitwisselen die nodig zijn voor dat programma. Aan beide zijden van het communicatiekanaal luistert de computer op deze poorten of er iets is voor de toepassing. Standaard luistert uw computer naar alle poorten.

Port scan:
Een scan van de poorten van een computer om snel een indruk te krijgen van welke diensten een computer allemaal gebruik maakt. Op basis daarvan kan een aanvaller bepalen welk soort kwetsbaarheden hij/zij kan gebruiken voor een aanval.

Private key:
Een private key, ook wel een geheime sleutel, is één van de twee sleutels die gebruikt wordt voor een asymmetrische cryptografie zoals RSA, waarbij één sleutel wordt gebruikt om de informatie te vercijferen en de tweede sleutel om de informatie weer te ontcijferen. De private key moet de gebruiker strikt geheim houden en mag hij nooit uit handen geven. De andere sleutel, de publieke sleutel, is bedoeld om uit te wisselen met degene met wie men wil communiceren.

Process control system:
Een process control system (PCS) is een automatiseringssysteem dat speciaal is toegerust voor het besturen van industriële processen in de procestechniek. Vroeger stonden dergelijke systemen ook wel bekend onder de naam distributed

control system (DCS) omdat de componenten van een dergelijk systeem veelal verschillende functies hebben en door één of ander communicatienetwerk met elkaar verbonden zijn.

Programmable logic controller:
Programmable logic controllers (PLC's) zijn speciale computers die verantwoordelijk zijn voor het realtime aansturen van machines binnen een process control systeem.

Protocol:
Een protocol is een afspraak over de eigenschappen van informatie die tussen computers worden uitgewisseld. Zo maken alle internettoepassingen gebruik van de protocollen TCP en IP.

Proxyserver:
Een proxyserver is een server die zich bevindt tussen de computer van de gebruiker en de computer die de gebruiker wil benaderen. De proxy is een 'tussenpersoon' die de opdrachten namens de gebruiker uitvoert. Proxyservers worden veel gebruikt om computers van een (lokaal) bedrijfsnetwerk gecontroleerd toegang te geven tot het internet. Een open proxy staat verbindingen van willekeurige gebruikers (IP-adressen) toe.

Public key encryptie methode:
Bij public key encryptie (versleuteling) wordt gebruik gemaakt van een key pair (sleutelpaar). Een key pair bestaat uit een public key en een private key. De public key mag iedereen hebben en wordt gebruikt om een tekst te versleutelen. De private key is geheim en alleen in het bezit van de eigenaar van het key pair. Een tekst die versleuteld is met een public key kan alleen met de bijbehorende private key weer leesbaar gemaakt worden.

R

Rainbow table:
Een tabel met mogelijke wachtwoorden en de hashwaarden van deze wachtwoorden. Ze worden gebruikt om wachtwoorden te testen op veiligheid of om deze te kraken. De techniek is vele malen sneller dan een brute force-techniek, waarbij de hashwaarden van de wachtwoorden nog moeten worden berekend.

Ransomware:
Een vorm van malware waarbij computerbestanden worden versleuteld en pas na betaling weer vrijgegeven. Slachtoffers worden naar websites gelokt waarna

er door een lek in de browser een programma geïnstalleerd wordt buiten medeweten van de gebruiker. Deze software versleutelt vervolgens bekende bestandstypes. Het slachtoffer krijgt een bericht met e-mailadres om de sleutel aan te vragen tegen betaling van een niet onaanzienlijk geldbedrag.

Reverse engineering:
Reverse engineering is het onderzoeken van een product om daaruit af te leiden wat de eisen zijn waaraan het product probeert te voldoen, of om de precieze interne werking ervan te achterhalen. Dit doet men meestal met het doel een concurrerend product te ontwerpen.

Router:
Een schakelapparaat op de knooppunten in een netwerk zoals het internet. Een router zorgt voor de verzending van gegevens naar de juiste bestemming.

S

SCADA:
SCADA staat voor Supervisory Control And Data Acquisition. Het zijn industriële (proces control) systemen. Ze worden veelvuldig gebruikt om industriële systemen van uiteenlopende grootte te besturen. Ze sturen de verschillende machines aan, en verzamelen en verwerken gegevens van meet- en regelsensoren om het proces stabiel te houden. De systemen worden onder meer gebruikt door elektriciteitscentrales, boorplatforms, gemalen, kerncentrales en drinkwaterbedrijven.

Scene:
Een geheel van personen en zaken die een bepaalde subcultuur of trend vertegenwoordigen.

Script kiddies:
Dit zijn hackers/crackers die met een minimum aan kennis in staat zijn veel schade aan te richten door het gebruik van programma's (scripts) waarmee andere computers kunnen worden bekeken en waarmee kwetsbaarheden kunnen worden misbruikt om toegang te krijgen op een computer.

Script:
Een script is een verzameling opdrachten voor een programma. Scripts zijn geschreven in programmeertalen die over het algemeen relatief makkelijk te lezen zijn. Met behulp van scripts is het mogelijk om snel en eenvoudig simpele programma's in elkaar te zetten of simpele acties uit te voeren. Scripts worden ook vaak in webpagina's gebruikt.

Sector:
De (kleinste) eenheid van opslag op harde schijven. Alle sectoren op een harde schijf zijn van gelijke grootte. Bij de meeste harde schijven is een sector 512 bytes groot. Iedere sector op een harde schijf heeft een eigen, uniek sectoradres. Sector kan in meer algemene zin ook betrekking hebben op een deel van het economische leven en een onderdeel van een bedrijf.

Secure Sockets Layer:
Secure Sockets Layer (SSL) is een methode om via internet gegevens veilig uit te wisselen tussen een website en een browser. De gegevens, bijvoorbeeld creditcardgegevens, worden, via een public key encryptiemethode versleuteld en gecodeerd, zodat niemand anders op internet ze kan zien of volgen.

SEPA:
Single European Payments Area. Project met als doel binnen heel Europa alle financiële transacties te laten plaatsvinden alsof het nationale transacties zijn. Dit betekent onder andere dat transacties direct worden uitgevoerd. SEPA wordt in 2010 de belangrijkste vorm van elektronische betalingen.

Server:
Een computer die informatie levert (serveert). Wordt in relatie tot internet vaak gebruikt als omschrijving van een computer waarop websites staan (gehost worden). De term server wordt echter ook als afkorting van webserver gebruikt: een computerprogramma.

Shimmen:
Een aanvalsmethode op chipkaarten, waarbij de communicatie tussen terminal en chipkaart wordt afgeluisterd en eventueel gemanipuleerd.

SIDN:
Stichting Internetdomein Registratie Nederland. Deze registry beheert sinds 1996 de domeinnamen voor het top level domein nl (zie: top level domain).

SOCA:
Landelijke politie-unit van het Verenigd Koninkrijk, die zich bezighoudt met zware en georganiseerde misdaad.

Social engineering:
Het manipuleren van mensen om ze zover te krijgen dat ze informatie geven of een actie uitvoeren, zoals het klikken op een link of het installeren van malware.

Sociale netwerken:
Online Sociale Netwerksites (OSN) zijn hulpmiddelen waar- mee mensen hun (privé en/of zakelijke) sociale netwerk op internet kunnen onderhouden. Voorbeelden zijn Hyves, Facebook, Twitter en LinkedIn.

Software:
Alle programma's die op een computer werken zoals de webbrowser, tekstverwerker en spelletjes zijn software, maar ook het besturingssysteem van een computer valt onder de software.

Spear phishing:
Vorm van phishing die specifiek gericht is op een bepaalde gebruiker of groepen van gebruikers, bijvoorbeeld medewerkers van een bepaalde organisatie.

Spam:
Spam is grootschalige ongewenste berichtgeving via e-mail, mobiele telefonie (sms of mms) of via een ander elektronisch kanaal zoals sociale netwerken, fax of bellen via een automatisch oproepsysteem, of via de telefoon. De inhoud van het bericht is verschillend en loopt uiteen van reclame tot het verzoek voor een financiële bijdrage. Spam betreft het grote volume van e-mailberichten dat verzonden wordt, niet de inhoud van het bericht.

Spoofing:
Je voordoen als een ander. Iemand kan bijvoorbeeld het e-mailadres van een ander gebruiken als afzendadres zodat de geadresseerde in verwarring raakt. Deze methode kan handig zijn voor de verspreiding van virussen, omdat de ontvanger zou kunnen denken dat de afzender betrouwbaar is. Spoofing gebeurt ook op netwerkniveau, vaak met als doel internetverkeer in de war te schoppen.

Spyware:
Een programma dat informatie over een gebruiker verzamelt en deze zonder dat de gebruiker daarvan op de hoogte is doorstuurt naar een derde partij.

SQL:
SQL betekent Structured Query Language: een computertaal waarmee een gebruiker met een database kan communiceren. Door voor deze database onbekende SQL statements naar de database te versturen, kan een onverwachte uitkomst ertoe leiden dat kwaadwillenden extra informatie van de database ontvangen zoals gebruikersnamen en wachtwoorden.

SQL-injectie:
SQL-injecties zijn een zeer gebruikelijke manier om te hacken. Bij een SQL-injectie geeft de crimineel een SQL-opdracht aan de database via zijn browser. Op die manier kunnen bijvoorbeeld databases uitgelezen, aangepast of verwijderd worden.

T

Technology push:
Het voortdurend op de markt brengen van nieuwe technologie.

Top-level domain:
Domeinaanduiding van het hoogste niveau. Het gedeelte achter de laatste punt van een domeinnaam is het top-level domain. De top-level domains zijn wereldwijd geografisch en naar organisatie ingedeeld. Bijvoorbeeld: .com staat voor commerciële bedrijven, .gov voor overheidsinstellingen en .edu voor scholen en universiteiten. Over het algemeen volgen niet-Amerikaanse organisaties de geografische indeling, zoals .nl voor alle Nederlandse domeinen, ongeacht de aard van de organisatie.

TOR (-netwerk):
Het TOR-netwerk, kort voor The Onion Router network, is een open netwerk voor anonieme communicatie gebaseerd op een techniek genaamd Onion Routing. Onion routing is een technologie ontwikkeld in 1995 door het US Naval Research Laboratory. Het TOR-netwerk is bedoeld om te voorkomen dat anderen door analyse van het berichtenverkeer kunnen achterhalen wat de herkomst en bestemming van berichten is. Criminelen maken hier misbruik van.

Transmission Control Protocol/Internet Protocol:
Verzamelnaam voor een aantal netwerkprotocollen waarop internetdiensten gebaseerd zijn. IP is het fundamentele protocol, waarvan TCP en ook UDP (User Datagram Protocol) gebruik maken. TCP/IP wordt beschreven door open standaarden en is onafhankelijk van specifieke hardware.

Trojan:
Een Trojan, Trojaans paard of Trojan horse is een programma dat vermomd is als een legaal, onschuldig programma, maar daarnaast ongewenste functies uitvoert. Die functies zijn bedoeld om bijvoorbeeld de maker of verspreider van het programma ongemerkt toegang te geven of om schade toe te brengen.

Twitter:
Micro-blogging dienst. Gebruikers van twitter kunnen korte boodschappen (maximaal 140 karakters) de wereld insturen. Ze kunnen zich ook abonneren op andere gebruikers (deze gebruikers volgen). Op deze manier kunnen ze bijhouden wat vrienden, bekenden en andere doen en razendsnel op de hoogte zijn van relevant nieuws.

U

Update:
Een aanpassing van een bestaand programma. Updates verschijnen regelmatig om fouten in een programma op te lossen.

Uploaden:
Het verzenden van een bestand van een computer naar andere computer. Het bestand kan een computerprogramma, tekst, beeld, video of geluid zijn. Uploaden is het tegenovergestelde van downloaden.

URL:
Uniform Resource Locator (URL) is een eenduidige plaatsaanduiding van een bestand, webpagina, programma, dienst of iets willekeurig anders op het internet, waarin naast de locatie ook het protocol vermeld is waarmee het bestand, de webpagina, het programma, de dienst of dat 'willekeurige anders' aangesproken kan worden. Vaak wordt de benaming URL gebruikt om het webadres aan te geven, bijvoorbeeld http://www.waarschuwingsdienst.nl/.

V

Variant:
De term variant wordt gebruikt om een kleine afwijking in een virus aan te geven. Als een virus een variant is van een ander virus, dan zijn de twee virussen ín grote lijnen gelijk. De verschillen beperken zich meestal tot verschillen in teksten van e-mails.

Veerkracht:
Veerkracht (of 'resilience') is de mate waarin een object, proces of systeem (de gevolgen van) dreigingen (dynamisch) kan opvangen zonder dat hierbij direct (significante) schade ontstaat waardoor de continuering of integriteit en betrouwbaarheid van de kritische functies in gevaar worden gebracht.

Virtual Private Network:
Virtual Private Network (VPN) is een veilige manier om een verbinding te maken met een netwerk of om twee netwerken aan elkaar te koppelen over een publiek netwerk zoals het internet.

Virus:
Een virus is een klein programma bedoeld om al dan niet stiekem dingen te doen met een systeem waar de eigenaar niet om gevraagd heeft. Soms blijft het bij onschuldige pop-up schermen, maar virussen kunnen ook erg gevaarlijk zijn. Ze kunnen de instellingen van een computer ruïneren, of de computer misbruiken om bijvoorbeeld e-mail te sturen aan duizenden mensen of om privébestanden klakkeloos te verspreiden. Virussen zijn er in vele soorten en maten. De meest voorkomende virussen op dit moment, richten zich op Windows-computers, maar er zijn ook virussen die andere systemen kunnen infecteren en beschadigen.

Vitale infrastructuur:
Producten, diensten en de onderliggende processen die, als zij uitvallen of worden verstoord, maatschappelijke ontwrichting kunnen veroorzaken. Dat kan zijn omdat er sprake is van veel slachtoffers en/of grote economische schade, dan wel omdat de uitval van lange duur is en er geen reële alternatieven voorhanden zijn, terwijl de betreffende producten en diensten maatschappelijk niet kunnen worden gemist. De vitale infrastructuur is kritisch om de territoriale, fysieke, economische en ecologische veiligheid en de sociale en politieke stabiliteit van Nederland te garanderen.

Vitale sector:
Een publiek en/of private groep organisaties en bedrijven die producten, goederen of diensten leveren en/of beheren, die als kritisch zijn benoemd voor de handhaving van de vitale belangen of vitale infrastructuur van Nederland. De vitale sectoren zijn: Energie, Drinkwatervoorziening, Telecommunicatie / ICT, Voedsel, Gezondheid, Keren en beheren oppervlaktewater, Financieel, Transport, Chemische en nucleaire industrie, Openbare Orde en Veiligheid, Rechtsorde en Openbaar Bestuur.

W

Wardriving:
Het rondrijden met een voertuig, voorzien van een notebook (laptop) met draadloze netwerkkaart, om plaatsen (hotspots) te vinden waar gebruik gemaakt kan worden van een draadloos computernetwerk (WiFi).

Web 2.0:
Verzamelnaam voor technieken en mogelijkheden die het internet socialer en interactiever maken. Binnen het web 2.0 concept bepalen de gebruikers zelf de inhoud van de pagina. Web 2.0 wordt ook als term gebruikt voor websites die gebruik maken van deze technieken en mogelijkheden.

Webserver:
De webserver is een computerprogramma dat op verzoek van een bezoeker van een website de bijbehorende internetpagina's doorgeeft.

Website:
Verzameling internetpagina's van een persoon, bedrijf of organisatie met een eigen thuispagina (homepage).

White plastic:
Kale creditcard of bankpas. Hierop kan de magneetstrip van een bestaande creditcard of bankpas worden gekopieerd, waarna de pas kan worden gebruikt om te betalen. Deze kaarten hoeven overigens niet wit te zijn, het kunnen volledig getrouwe kopieën zijn, inclusief reliëf en hologram.

WiFi:
Wireless Fidelity, een populaire vorm van een draadloos netwerk. WiFi kent een groot bereik, namelijk tussen de 30 (binnen) en de 300 (buiten) meter. Een andere vorm van draadloos netwerk is Bluetooth.

World Wide Web:
Benaming voor de verzameling van alle websites (www), en alle hypertekst-verbindingen tussen die websites op het internet. Met een browserprogramma op een computer surft iedereen over het world wide web. Het web is in gebruik sinds 1991 en bedacht door Tim-Berners Lee.

Worm:
Een programma speciaal gemaakt om zichzelf te verspreiden naar zoveel mogelijk computers. Een worm verschilt van een virus. Een virus heeft een bestand nodig om zichzelf te verspreiden, een worm niet. Een worm heeft niet altijd schadelijke gevolgen voor een computer, maar kan de verbinding wel langzaam maken.

Z

Zombie(-computer):
Als een computer geïnfecteerd is met een bot, dan wordt gesproken over een zombiecomputer. De geïnfecteerde computer vormt onderdeel van een botnet en staat als een zombie ter beschikking van een kwaadwillende.

Index