POLITIE

- Korps landelijke politiediensten
- Dienst Recherche Onderzoeken

Onderzoek : 2001 630

Nummer : 0000 021212 0815

Betreft : Algemeen dossier

P R O C E S – V E R B A A L

Hierbij verklaren wij,

Verbalisanten: **Robert van de Gaar** en **Lambert Smat**,

respectievelijk inspecteur van politie – tactisch coördinator en brigadier van politie rechercheur – dossiervormer bij de Dienst Recherche Onderzoeken van het Korps Landelijke Politiediensten, naar aanleiding van de binnen het onderzoek 2001-630 ingekomen en opgemaakte stukken, het navolgende:

AANLEIDING ONDERZOEK

Op 21 mei 2001 is op het Landelijk Parket Openbaar Ministerie een verzoek overname van strafvervolging binnengekomen van de Minister van justitie te Hamburg van 3 mei 2001, no. 9352 E-N1-55.4 inhoudende een verzoek tot overname van strafvervolging tegen Mike van der W.n. Op grond van dit verzoek is door de afdeling project voorbereiding van de Dienst Recherche Onderzoeken een onderzoek ingesteld.

Uit het onderzoek van de afdeling project voorbereiding (PV200148) is gebleken dat er in Nederland een groep hackers actief is onder de naam Xtreme-Power (of kortweg “XP”). Deze groep houdt zich bezig met het op grote schaal hacken van computers op het Internet.
Veelal wordt er op gehackte computer systemen software geïnstalleerd welke het netwerk verkeer onderschept en op deze wijze inlognamen en wachtwoorden van reguliere gebruikers op die systemen vastlegt.
Deze gehackte computers kunnen worden gebruikt voor zogenaamd Distributed Denial of Service (DDoS) aanvallen op het Internet. Hierbij worden de gehackte computers onderling gekoppeld en sturen zij op een gegeven commando een grote

hoeveelheid data pakketten in de richting van een uitgekozen computersysteem. Deze hoeveelheid is zo groot dat deze niet verwerkt kan worden met als gevolg dat de internet verbinding van de computer van het slachtoffer “verstopt” raakt en dus ook niet meer voor anderen (bijv. klanten) benaderbaar is.

Voor een effectieve DDoS aanval zijn een groot aantal computers nodig die door de hacker in een netwerk zijn geschakeld. Een vast onderdeel van de Modus Operandi is het plaatsen van het programma Stacheldraht dat gebruikt wordt voor het uitvoeren van DDoS aanvallen.
Deze computers worden aangestuurd door een centrale server. In de praktijk is gebleken dat men voor dit DDoS netwerk gehackte computers gebruikt. Tijdens de project voorbereiding is gebleken dat de hackers een voorkeur hebben voor computers met een snelle toegang tot Internet (breedband). Door de combinatie van het grote aantal computers en hun snelle Internetverbinding is het mogelijk om een grote datastroom te creëren. Deze kan een zodanige omvang aannemen dat ook Internet providers hier hinder van ondervinden. Het gevolg kan zijn dat voor de overige reguliere gebruikers bij een provider de snelheid terugloopt dan wel dat de gehele verbinding wegvalt.

Na de project voorbereiding periode werden de volgende gegevens bij proces – verbaal aangeleverd (PV 1038 011005 1200):

- Rechtshulpverzoek

Naar aanleiding van het hacken begin februari 2001 van een computer in Duitsland is er aangifte gedaan door het bedrijf Computer & Competence (hierna te noemen C&C) te Hamburg (Dld) en is na onderzoek in Duitsland een verzoek om overname van de vervolging van de Nederlandse verdachte(n) gedaan aan de Nederlandse autoriteiten.

Deze gehackte computer maakte deel uit van een netwerk dat door de hackers was ingericht voor DDoS aanvallen. Middels onderschepte communicatie tussen deze computers onderling werden nog andere computers in Duitsland achterhaald welke ook gehackt bleken te zijn. Aannemelijk is dat ook de andere computers in dit netwerk gehackt zijn (waaronder de Nederlandse computers pc-160.studver.uu.nl en boerhave.med.vu.nl) . Door de systeembeheerder van C&C is zelf een onderzoek ingesteld. Hieruit is gebleken dat een groep genaamd “Xtreme-Power” verantwoordelijk was voor het hacken van de computer en het opzetten van het DDoS netwerk. Ook kwamen uit het onderzoek verricht door deze systeembeheerder de namen Van der W. (Mike), Kruimel en Beast naar voren als mogelijke daders. Tevens is vastgesteld welke computers door deze groep als uitvalsbasis op Internet gebruikt worden. Het betreft hier de computers CAVEMEN.Nl en HIDALGO.RAPTORNET-IS.Nl welke gehost zijn op Nederlands grondgebied.

- Geen aangifte i.v.m. angst voor negatieve publiciteit

Uit het Duitse onderzoek naar aanleiding van de hacking bij C&C bleek dat de gehackte computer samen met zeker 14 andere computers deel uitmaakte van een DDoS netwerk. Een van deze computers bleek van de faculteit geneeskunde van de

Vrije Universiteit te Amsterdam zijn (boerhave.med.vu.nl). Deze computer bleek ook begin februari 2001 gehackt te zijn. Kenmerken op deze computer kwamen overeen met die van de Duitse zaak. Verder is er vanaf deze computer gezocht naar andere computers op Internet, welke kwetsbaar voor hacken waren. Daar deze faculteit door een reorganisatie wordt ondergebracht bij het ziekenhuis van de Vrije Universiteit is men uit vrees voor slechte publiciteit niet bereid aangifte te doen. Dit ondanks uit het feit deze computer geen informatie over patiënten dan wel andere privacy gevoelige informatie bevatte . Zie proces-verbaal nr 1038 010518 1200

- IRC discussie

Naar aanleiding van de aanhouding van Karim B. (nick name Mace) in het VU/Sonera onderzoek ontstond er op de Internetsite www.security.nl een discussie. In deze discussie werd Van der W. met naam, adres en telefoonnummer genoemd als iemand die zich op grote schaal met DDoS aanvallen bezig houdt en ook maar eens aangepakt moet worden. Door Van der W. werd hierop gereageerd: “Als jullie nou ook eens in irl (in real life) ook mans waren dan was het DDoSsen niet nodig en beukte ik gewoon jullie kankerkopjes in elkaar.”
Zie proces-verbaal nr. 1038 010801 1600

- Internet site “lamermike”

Op de Internetsite http://www.escd.dds.nl/lamermike is door onbekenden informatie geplaatst over Van der W. Hier werd aangegeven dat Van der W. leiding geeft aan Extreme-Power, zich bezig houdt van DDoS aanvallen en het hacken van computers. Tevens staat er een lijst met ongeveer 250 computers welke door Van der W. gehackt zouden zijn.
Hierop is met een aantal Nederlandse systeembeheerders van deze gehackte computers contact opgenomen. Hierbij bleek dat deze computers inderdaad gehackt waren. Zie proces-verbaal nr 1038 010807 1600

- Geen aangifte Tri-LAB te Den Haag i.v.m. bedreiging na een DDoS aanval.

Op 6 mei 2001 vond er op IRC een discussie plaats met Mike van der W. en een later slachtoffer (een bedrijf). Deze discussie ging over de website “lamermike”, waarvan Van der W. wilde dat deze werd verwijderd. Deze discussie eindigde met het feit dat Van der W. zei dat het ging regenen en dat het slachtoffer zijn paraplu maar moest pakken en dat hij wel via een andere host weer terug zou komen in het kanaal. Hierop werd de Internet verbinding van het slachtoffer met een DDoS aanval afgesneden. Tevens vond er een telefoongesprek tussen het slachtoffer en Van der W. plaats waarbij deze dreigde de Internetverbinding gedurende een aantal weken onmogelijk te maken. Van der W. uitte bedreigingen ten aanzien van de medewerkers van het bedrijf indien zij contact op zouden nemen met de politie.Hierdoor zag men inderdaad van aangifte af. De bedreigingen bestonden uit het dreigen met nieuwe DDoS aanvallen en het in brand steken van de woning van het slachtoffer (directeur Tri-Lab) Zie proces-verbaal nr 1038 010611 1200

- Aangifte Netco

In april 2001 wordt er door het bedrijf NETCO, te Haarlem aangifte gedaan van hacking (2x gepleegd). Hierbij werd vastgesteld dat de hacker gebruik maakte van de door hem aangemaakte inlognamen mike en mike2. Vanaf de gehackte computer werden er door de hacker meerdere verbindingen met andere computers op het internet opgezet. Een van deze verbindingen was opgezet met het IP adres 213.046.019.169. Aan dit adres is de DNS naam (computernaam) d19169.upc-d.chello.nl gekoppeld.

Op securtity.nl werd in relatie tot van der W. het internetadres d19169.dtk.chello.nl genoemd. Deze DNS naam bestaat niet meer. Gezien de namen betreft het hier vermoedelijk hetzelfde adres, maar is de naam gewijzigd van d19169.dtk.chello.nl in d19169.upc-d.chello.nl.

- Melding voorzitter NLIP

Van de voorzitter van het NLIP (overkoepelend orgaan van internet providers) is een email ontvangen met klachten van Internet Providers over DDoS aanvallen op internet. Hierbij wordt Mike van der W. als dader genoemd en wordt er tussen hem en de computernaam d19169.dtk.chello.nl een relatie gelegd. (1038 001013 1321)

Eerst ingesteld onderzoek

Naar aanleiding van bovenstaande werd door een team van de Dienst Recherche Onderzoeken van het Korps Landelijke Politiediensten, werkend onder het zaaksnummer 2001 – 630, vanaf november 2001 een nader onderzoek ingesteld. Alle opsporingshandelingen zijn verantwoord in het onderzoeksdossier.

Onder meer uit het ingestelde onderzoek is een beeld ontstaan van de onderzoeksmaterie. Van dit beeld wordt vervolgens een algemeen beeld van de zaak geschetst:

Internet:

Het onderzoek heeft zich gericht op activiteiten door hackers gepleegd via het internet.

De diensten welke op internet aangeboden worden zijn in een aantal onderwerpen te verdelen:

1 - : “surfen” een populaire naam voor het raadplegen van het World Wide Web

2 - : “e-mail” electronische post voor het uitwisselen van berichten, een tegenhanger voor fax en brief.

3 - : “chatten” een vorm van interactieve online communicatie welke het mogelijk maakt om direct met elkaar te converseren via ingetypte teksten. Wanneer je deelneemt aan een chat discussie worden jouw boodschappen direct doorgegeven

naar de andere leden in de 'chat room' terwijl de boodschappen van andere leden direct naar jou worden doorgegeven.

Er zijn verschillende vormen van chatten zoals bijv. MSN waarbij één op één berichtenverkeer gewisseld wordt of via de IRC (Internet Relay Chat) servers. Door diverse internet providers wordt deze IRC dienst aangeboden middels één of meerdere IRC servers. Deze servers zijn over het algemeen voor een ieder vrij toegankelijk. Door de providers zijn IRC operators aangesteld om de servers te beheren en het chatverkeer enigszins te monitoren en beheren. Door deze operators kunnen aan bepaalde personen de toegang tot het door hen beheerde netwerk ontzegd worden . (K-line)

Om deel te nemen aan een chat sessie is het niet noodzakelijk, zelfs ongebruikelijk, om dit met een echte naam te doen. Er wordt gebruik gemaakt van een verzonnen naam (nickname). Deze nickname geeft een beperkte anonimiteit. De deelnemers hebben elkaar feitelijk meestal nooit ontmoet. Men kent elkaars ware namen, woon of verblijfplaats meestal niet eens tenzij dit onderling wordt uitgewisseld. Identiteit is niet alleen persoons verbonden. De computer heeft ook een herkenning waardoor het mogelijk wordt om systemen gegevens met elkaar te laten uitwisselen. Door de computer van de gebruiker wordt een verbinding opgebouwd met een IRC server waarbij adressen worden uitgewisseld waarop de beide machines werken en te bereiken zijn. (IP adressen). Middels deze IP adressen is de gebruiker in veel gevallen alsnog te achterhalen. In een aantal gevallen worden deze IP adressen vervangen door verzonnen adressen zodat de anonimiteit meer gewaarborgd blijft. (spoofen) Om het eigen IP adres af te schermen wordt ook van de mogelijkheid gebruik gemaakt om via een of meerdere (gehackte) servers het internet op te gaan.

Door de gebruiker kan via een gebruikers programma contact gezocht worden met de IRC server. Door de gebruiker kan een kanaal geopend worden of hij kan deelnemen aan een bestaand kanaal waar meerdere gebruikers aanwezig zijn en met elkaar communiceren.

Er zijn vele duizenden chat kanalen waar gecommuniceerd wordt. In het chat kanaal wordt aangegeven wat het onderwerp (topic) is waar op dat moment over gesproken wordt.

In het chat kanaal zijn er gebruikers die operator rechten hebben. Deze gebruikers kunnen andere gebruikers de toegang tot dat kanaal weigeren (bannen) of gebruikers uit een kanaal verwijderen (kicken). Degene die het kanaal start heeft automatisch operator rechten. Deze gebruiker kan ook aan andere gebruikers operator rechten verlenen.

In principe zijn de kanalen voor een ieder toegankelijk. Er kunnen echter ook besloten kanalen zijn of gemaakt worden. Groepen gebruikers met een gelijke interesse zullen elkaar regelmatig in hetzelfde kanaal treffen. Als de laatste gebruiker in een bepaald kanaal uitlogt houdt het kanaal op te bestaan. Een andere gebruiker kan dan opnieuw een kanaal openen met die naam en heeft dan automatisch operator rechten en kan dan op dat kanaal bepalen wie wel of geen toegang heeft.

Een groep gebruikers die er aan hecht om een bepaald kanaal voor zich te behouden zal er alles aan doen om ingelogd te blijven op dat kanaal. Groepen die zich bezighouden om kanaaltjes op IRC te beheersen en behouden worden in een aantal gevallen IRC crews genoemd. Dergelijke IRC crews hebben veelal gezamenlijke interesse op het gebied van computers en daaraan gerelateerde activiteiten als bijvoorbeeld hacking. Een van deze IRC crews is de groep XP of voluit Xtreme Power. De groep heeft de naam om o.a. middels bedreigingen met zowel fysiek geweld als met het inzetten van Ddos aanvallen een gedeelte van het IRC verkeer te willen beheren en beheersen. (Voorbeelden hiervan zijn de zaaksdossiers 3019 en 3020)

Tijdens het onderzoek is gebleken dat de activiteiten binnen de groep XP afnamen. In december 2001 is er sprake dat een aantal (voormalige) leden van XP verder zouden gaan onder de naam “Down Under” (DU) crew. Uit het ingestelde onderzoek is niet vastgesteld dat XP of later Down Under crew (DU) een criminele organisatie is met een gestructureerd samenwerkingsverband van enige duurzaamheid. Veeleer was er sprake van een groep personen met een wisselende samenstelling maar wel met een gelijk interesse gebied die op enkele momenten samenwerkten in het plegen van strafbare feiten.

Vanuit de projectvoorbereiding is een pagina aangeleverd met de leden van XP zoals dit in maart 2001 op de homepage www.xtreme-power.com werd aangetroffen. Op de pagina staan nicknames vermeld met daarbij een taak verdeling. Gedurende het onderzoek zijn een aantal van deze nick names naar voren gekomen en is er een identiteit aan gekoppeld. Een aantal nick names zijn gedurende het onderzoek niet (meer) naar voren gekomen.

Op de home page is de volgende onderverdeling gemaakt:

Leader

Mike

Lords

Stamp Sargeant Kruimel

V|XX

Members

FTC PARA Uuutie

|Akra| Sargeant Macros

Leentje Brrrrrrrr Nossie

Double-X R|G|AN Orangehaw

Met betrekking tot de namen voorkomend op het hiervoor aangehaalde schema kan het navolgende worden opgemerkt:

Leader:

|Mike|
Betreft : Mike van der W. uit Almere
Verwerkt in: persoonsdossier **2001**

Lords:

Stamp
Betreft : Tommy Hafez A. uit Haarlem
Verwerkt in: persoonsdossier **2009**

Sargeant
Betreft : Patrick R. uit Terneuzen
Verwerkt in: persoonsdossier **2002**

Kruimel
Betreft : Michel K. uit Veenendaal
Verwerkt in: persoonsdossier **2007**

Advisors:

Beast|3
Betreft : Patrick van K. uit Helmond
Verwerkt in: persoonsdossier **2010**

Junk|e	(niet in onderzoek)
Dog|e	(niet in onderzoek)
V|xx	(niet in onderzoek)

Members:

FTC	(niet in onderzoek)
|Akra|	(niet in onderzoek)
Leentje	(niet in onderzoek)
Double-X	(niet in onderzoek)
`Para'	(niet in onderzoek)
Sargeant	(zie Lords)
Brrrrrrr	(niet in onderzoek)
R|G|AN	(niet in onderzoek)
UUUTIE	(niet in onderzoek)
MACROS	(niet in onderzoek)
NOSSIE	(niet in onderzoek)

ORANGEHAW
Betreft : Piet H. uit Culemborg
Verwerkt in: persoonsdossier **2003**

Tijdens het onderzoek zijn de volgende nick names naar voren gekomen die op enig moment activiteiten hebben verricht / deel hebben uitgemaakt voor de groep XP:

Mace
Betreft : Karim B.j uit Den Haag
Verwerkt in: persoonsdossier **2006**

Dr0kz
Betreft : Frank G. uit Naaldwijk
Verwerkt in: persoonsdossier **2008**

Skylimit
Betreft : Mark W. uit Leeuwarden
Verwerkt in: persoonsdossier **2005**

Xinoy
Betreft : Michael W. uit Goor
Verwerkt in: persoonsdossier **2004**

Hacken:

In verschillende publicaties wordt getracht om een definitie te geven wie of wat een hacker is. In de Hackers Guide (1999 Uitg. Pearson education ISBN 90-430-0160-0) staat hierover onder meer aangegeven:

Een hacker is een persoon die erg geïnteresseerd is in de geheimzinnige en obscure werking van om het even welk besturingssysteem. Hackers zijn meestal programmeurs. Hackers hebben dus een goede kennis van besturingssystemen en programmeertalen. Zij ontdekken soms tekortkomingen in computersystemen en kennen er ook de oorzaak van. Hackers proberen hun kennis voortdurend uit te breiden, delen hun kennis met andere gebruikers en beschadigen gegevens nooit opzettelijk.

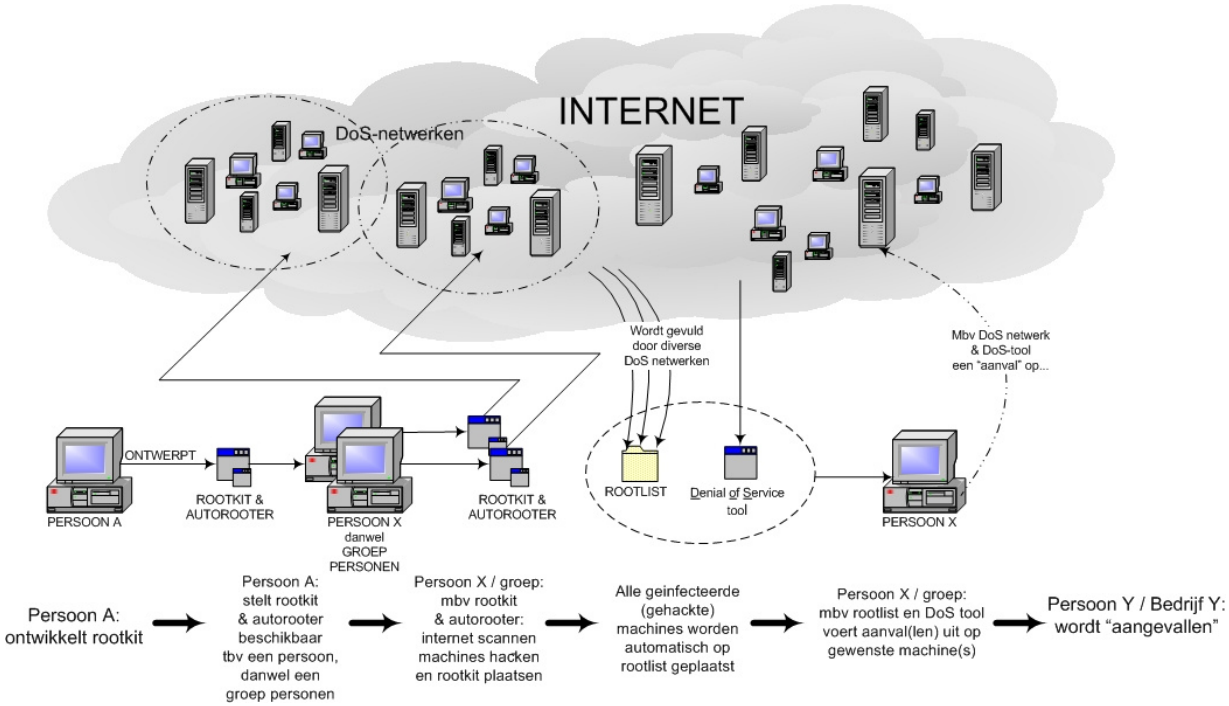
Naast deze beschrijving van een hacker wordt komt in deze publicatie ook de term cracker naar voren:

Een cracker is iemand die inbreekt op een systeem of externe computer of die het systeem op een andere manier opzettelijk beschadigt. Crackers vernielen belangrijke gegevens zodra ze op deze manier ongeoorloofd toegang hebben gekregen tot een systeem. Ze zorgen ervoor dat de computer niet langer normaal is te gebruiken of veroorzaken problemen om er zelf voordeel uit te halen. Crackers zijn makkelijk te identificeren aangezien hun bedoelingen kwaadaardig zijn.

In het spraakgebruik wordt er geen verschil gemaakt tussen hackers en crackers. De verdachten uit dit onderzoek zullen veelal in de laatste categorie gevonden worden. De term crackers komt verder in de zaak niet voor, de term scriptkiddies

wordt meer gehanteerd. Deze term wordt wel gebruikt als overkoepeling voor een IRC crew.

Door de IRC crew wordt door ieder voor zich of voor de gehele crew diverse (criminele) activiteiten op het internet verricht. Schematisch zou hierbij de volgende voorstelling gemaakt kunnen worden:



Hierbij zijn een aantal termen van belang:

<u>root kit</u>

Een rootkit is een verzameling van computer bestanden (programma's / scripts) die geïnstalleerd worden op een computer met de bedoeling het systeem ongezien te kunnen beheren. Door een rootkit te installeren op een systeem is het mogelijk voor een hacker om het systeem te bedienen met alle rechten behorende bij de root-account, dus zonder restricties. De sporen van de hacker zijn niet zichtbaar voor de beheerder van het computer systeem.

<u>fysieke toegang</u>

Wanneer een hacker de fysieke toegang heeft tot een systeem met de rechten behorende bij de root-account kan hij zonder meer een rootkit installeren. Dit geschiedt op dezelfde manier als met de installatie van elk ander programma.

Exploiten

Wanneer er op een systeem software actief is die een veiligheidsfout bevat kan de hacker deze fout uitbuiten (exploiten) over het Internet en zo toegang verkrijgen tot het systeem. Wanneer hij de root-rechten heeft (bemachtigd), installeert hij de rootkit zoals bij fysieke toegang. (o.a. zaakdossiers 3001, 3007)

auto-rooten / bulk-hacking

Het exploiten van een systeem kan ook geautomatiseerd worden. Op deze manier kan een zelf geschreven script hele delen van het Internet af scannen, en indien er een vatbaar systeem aangetroffen wordt deze direct infecteren met een rootkit.

Dit is een populaire manier onder hackers om een zo groot mogelijk aantal slachtoffers te kunnen maken zonder daar veel werk aan te hebben. Het script wordt immers geactiveerd en stopt pas wanneer de hacker daar opdracht toe geeft. De getroffen systemen verschijnen zo geheel geautomatiseerd in een lijst bij de hacker. (o.a. zaakdossiers 3011, 3014, 3016, 3017)

rootlist

In deze rootlist staan alle door de root kit gehackte computers. Afhankelijk van de rootkit zijn in deze lijst gegevens te vinden op welk IP adres het systeem zit, de inlog wachtwoorden en een naam van de server. (6314 020704 1300)

DDoS aanval

Op het Internet is een aantal programma's beschikbaar die een DDoS-aanval in kunnen zetten. Het is bekend dat deze programma's sinds 1990 verspreid worden over Internet. De meest toegepaste programma's hiervoor zijn Trinoo, Tribe Flood Network, Tribe Flood Network 2k, Stacheldraht, Shaft en Mstream.

Door de netwerkcapaciteit van verschillende gehackte computers te bundelen is de hacker in staat om een stroom data naar een slachtoffer over het Internet te sturen. Het gevolg is dat het slachtoffer voor de duur van de aanval via internet onbereikbaar wordt. Het slachtoffer kan een individueel systeem zijn, een verbinding of een netwerk. Ook kan het voorkomen dat de systemen of netwerkonderdelen waar een aanval op uitgevoerd wordt volledig vastlopen en zonder tussenkomst van een beheerder diensten zullen blijven weigeren.
De hacker gebruikt de gehackte systemen op deze manier dus als wapen. Een enkele (gehackte) machine een aanval uit laten voeren wordt ook wel een *Denial Of Service* aanval genoemd. Het inzetten van meerdere machines voor een dergelijke aanval wordt ook wel *Distributed Denial Of Service* aanval genoemd. (o.a. zaakdossiers 3002, 3006, 3008, 3009, 3013, 3019, 3020)

Sniffer:

Betreft een software programma wat netwerkpakketten onderschept. Er bestaan vele verschillende soorten sniffers en worden in deze zaak bijvoorbeeld gebruikt voor het onderscheppen van inlog codes, wachtwoorden en/of creditcard gegevens.

(zaakdossier 3003). Het gebruik van de creditcard is “beperkt” tot die handelingen waarbij geen verbinding wordt gelegd naar een natuurlijk persoon. Het bestellen en laten afleveren van goederen is tijdens het onderzoek niet gebleken.
Met de creditcard gegevens kunnen rechten verkregen worden tot toegang tot bepaalde sites of bijvoorbeeld domeinnamen geregistreerd worden. Dergelijke activiteiten zijn wel waargenomen.

Waaruit bestaat het nadeel van de omschreven activiteiten?

Uit het onderzoek is gebleken dat door de diverse verdachte wereldwijd zeer vele (duizenden) strafbare feiten zijn gepleegd. Daar waar sprake is van het gebruik van auto- of bulk rooters loopt het aantal strafbare feiten snel op. Door het plegen van elk strafbare feit ontstaat nadeel. De grootte van dit nadeel is moeilijk in te schatten. Het opnieuw installeren van computersystemen is afhankelijk van het soort systeem en het doel waarvoor het systeem is opgezet. Het onderzoek heeft zich beperkt tot een klein aantal zaken waarbij aangiften waren gedaan door de benadeelden. Deze zaken met het door de benadeelde aangegeven nadeel staat hierbij als volgt weergegeven:

Zaak 1 (RHV)	- installatie en confriguratie van het systeem kostte 3 mandagen - online shop 8 uur niet bereikbaar - bericht aan alle klanten - immateriële schade door vertrouwensverlies. Enkele klanten hebben aangekondigd te vertrekken (online shop)
Zaak 2 (Netnation)	- 10 uur downtime (voor bedrijf maar ook de klanten ze hosten 500 websites) - schade 125.000 euro
Zaak 3 (Chello)	- geen schadebedrag bekend. Er is geen schade aan systemen wel zijn ze weken niet inzetbaar geweest
Zaak 4	Niet ingezonden
Zaak 5	Niet ingezonden
Zaak 6 (KPN)	- niet meetbare imago schade - daarnaast totale directe schade 16.660 euro
Zaak 7 (Fom)	- schade 5000 euro
Zaak 8 (Obit)	- schade ongeveer fl. 3000,-- - dit los van de klanten wiens systeem niet bruikbaar was en de nodige manuren om het bedrijfsnetwerk na te kijken,
Zaak 9 (Maximedia)	- schade ongeveer 300 a 400 euro
Zaak 10 (Connexxion)	- schade ongeveer 1385 euro
Zaak 11 (Feka)	- schade ongeveer 880 euro
Zaak 12 (Milos Gispen – bedreiging)	- Geen schade bekend ??
Zaak 13 (De Haan – bedreiging DDOS)	- Geen schade bekend ?? wel gaan bij een DDoS aanval ook 100 computers van andere mensen down.
Zaak 14 (Angenent)	- Geen schade bekend.
Zaak 15	Niet ingezonden
Zaak 16 (VDL)	- Schade bedrag niet exact aan te geven

Zaak 17 (Hyundia)	- Schade bedrag kan niet exact worden aangegeven. - het heeft ongeveer een week geduurd voor systeem weer volledig operationeel was. Extra kosten voor post, telefoon en fax.
Zaak 18 (WWM)	Geen schade bedrag bekend
Zaak 19 (XS4ALL)	- Over schade kan niets gezegd worden, Servers zijn een tijd niet toegankelijk geweest, waarvoor onze klanten minimaal 5000 euro betalen.
Zaak 20 (Hage – studio12.com)	- Schade ongeveer € 1170,27

Naast bovenstaande schade geven een aantal bedrijven ook min of meer aan dat er een soort imagoschade en/of vertrouwenschade is.

De schade welke door niemand expliciet aangegeven wordt doch wel bestaat is de lijn capaciteit welke middels DDoS aanvallen gebruikt wordt.

Creditcard fraude:

Van een aantal door de verdachten gehackte systemen is het mogelijk om voor de verdachte interessante gegevens af te halen voor o.a. eigen gebruik. Een dergelijke zaak is beschreven in zaak 3 (Chello). Dit betrof het binnen dringen van een proxy server in het Chello netwerk van de regio Rotterdam. Door het afvangen van het verkeer wat over deze server liep (sniffer) was het onder meer mogelijk om creditcard gegevens en wachtwoorden te onderscheppen.

Met deze creditcard gegevens werd door de verdachten onder meer gebruik gemaakt om bepaalde diensten op het internet te kunnen krijgen alsmede voor het betalen van bedragen voor het vastleggen van o.a. domein namen. Voor de registratie van deze namen werden verzonnen persoonsgegevens gebruikt. De bedragen voor deze diensten weden natuurlijk wel afgeschreven van de houder van de creditcard.

Opbouw dossier:

Alle ambtshandelingen welke tijdens het onderzoek zijn verricht zijn bij proces – verbaal vastgelegd en in het onderzoeksdossier verwerkt. Hierbij is de volgende indeling gehanteerd:

1000 : bronnen en getuigen

Hierin staan alle ambtshandelingen verantwoord welke betrekking hebben op het raadplegen van bronnen dan wel het verhoren van getuigen.

2000 : verdachten

Hierin staan alle ambtshandelingen verantwoord welke betrekking hebben op de verdachten. Hieruit zijn o.a. alle dwangmiddelen welke op de verdachte zijn uitgeoefend alsmede alle verhoren verantwoord welke vervolgens tot een persoonsdossier zijn gevormd.

3000 : aangiften

Hierin staan alle ambtshandelingen verantwoord welke betrekking hebben op het opnemen van aangiften.

4000 : rechtspersonen

Niet gebruikt

5000 : doorzoekingen

Hierin staan alle ambtshandelingen verantwoord welke betrekking hebben op het doorzoeken van panden.

6000 : bijzondere opsporingsmethodieken

Hierin staan alle ambtshandelingen verantwoord welke betrekking hebben op het toepassen van bijzondere opsporingsmethodieken.

7000 : rechtshulp

Hierin staan alle ambtshandelingen verantwoord welke betrekking hebben op aanvragen / afhandelen van rechtshulp verzoeken.

8000 : beslag

Hierin staan alle ambtshandelingen verantwoord welke betrekking hebben op het afhandelen van inbeslaggenomen goederen.

Van dit onderzoeksdossier is van alle ingebrachte documenten een index bijgehouden. Deze index wordt in zijn geheel als bijlage bij dit proces – verbaal gevoegd. Tevens worden de processen-verbaal in zijn geheel op cd-rom aangeleverd. Bij deze cd-rom wordt een handleiding geleverd voor het zoeken op deze cd-rom.

Vanuit het onderzoeksdossier zijn zaaks- en persoonsdossiers samengesteld. In de zaaksdossiers staan de zaak en de strafbare feiten beschreven. Voorts zijn in kopie in het zaakdossier opgenomen de door de verdachte(n) in de betreffende zaak afgelegde verklaringen. In het persoonsdossier zijn opgenomen de dwangmiddelen welke tegen de verdachte zijn ingezet. Ook zijn in het persoonsdossier opgenomen alle door de verdachte afgelegde verklaringen met betrekking tot de strafbare feiten (zaken) waar hij verdachte in is. Aan de zaaksdossiers worden persoons dossiers gekoppeld van een of meer verdachten welke verantwoordelijk zijn voor de strafbare feiten in deze zaak.

Het gehele onderzoeksdossier blijft beschikbaar tot de zaak geheel is afgerond.

Gebruik kopieën

Door ons, verbalisanten, wordt opgemerkt dat de kopieën die zijn opgenomen in de samengestelde persoonsdossiers en zakendossiers **kopieën conform het origineel** zijn. Daar waar een kopie is gebruikt bevindt zich origineel in ieder geval in het complete onderzoeksdossier.
Als voorbeeld kan worden gegeven dat de origineel afgelegde verklaringen door de verdachten zich in de respectievelijke persoonsdossiers bevinden. In de zakendossiers zijn dus kopieën opgenomen van deze afgelegde verklaringen met hun bijlagen.

Bijlagen:

Als bijlagen worden bij dit algemeen dossier gevoegd:

- Leeswijzer
- Index
- Kruistabel
- Verklarende woordenlijst (waarin opgenomen de meeste van de in de zaaks- en persoonsdossiers opgenomen technische termen en afkortingen)

Sluiting

Waarvan door ons, verbalisanten, op respectievelijk ambtseed c.q. ambtsbelofte is opgemaakt dit proces-verbaal gesloten en getekend te Driebergen op 12 december 2002.

De verbalisanten,

R. van de Gaam en **L.A. Smat**.