door **Vincent Ossewaarde**

Indringers verklikken

Hoe herkent u misbruik en welke maatregelen kunt u nemen?

Als u programma's gebruikt om het verkeer op uw internetverbinding in de gaten te houden, dan stuit u misschien op pogingen tot misbruik. Ook op andere manieren kunt u ontdekken dat er iets mis is. Gelukkig staat u er niet alleen voor: providers helpen doorgaans graag om hackers, spammers of verspreiders van virussen op te sporen en aan te pakken. Maar hoe benadert u ze? Wie moet u hebben? En waar moet u op letten bij het indienen van een klacht?

Misbruik van een internetverbinding kent vele verschijningen. U kunt het slachtoffer worden van een hacker, maar u kunt ook getroffen worden door een virus of een spambom, of andere manieren van misbruik tegenkomen. Het opsporen van degene die achter een hackpoging of spamrun zit, is vaak een ingewikkeld traject. Providers helpen daar graag bij, maar het startpunt van zo'n zoektocht ligt bij u. Door providers op een juiste manier aan te spreken, kunt u helpen om zo snel mogelijk maatregelen te nemen tegen degene die u lastig valt.

HOE MERKT U HET?

Misbruik van een internetverbinding of computer is lastig op te merken. Als kwaadwillenden misbruik proberen te maken van een internetverbinding, zullen ze proberen om dit zo onopgemerkt mogelijk te doen. Gelukkig slaagt slechts een klein percentage erin om écht verborgen te blijven. U kunt dan ook vaak zien dat er is geprobeerd in te breken op uw computer of op uw netwerk. Zo kunt u in de logbestanden van Windows controleren of onbekenden hebben geprobeerd in te loggen met (on)bekende gebruikersnamen en wachtwoorden. Ook het doorspitten van logbestanden van aanwezige ftp- of webservers levert vaak aanwijzingen op dat iemand misbruik heeft proberen te maken. Ten slotte zijn ook eventuele logmogelijkheden van internetrouters en -modems belangrijk: sommige typen en merken kunnen redelijk nauwkeurig vaststellen of iemand probeert in te breken.

WIE BENADERT U?

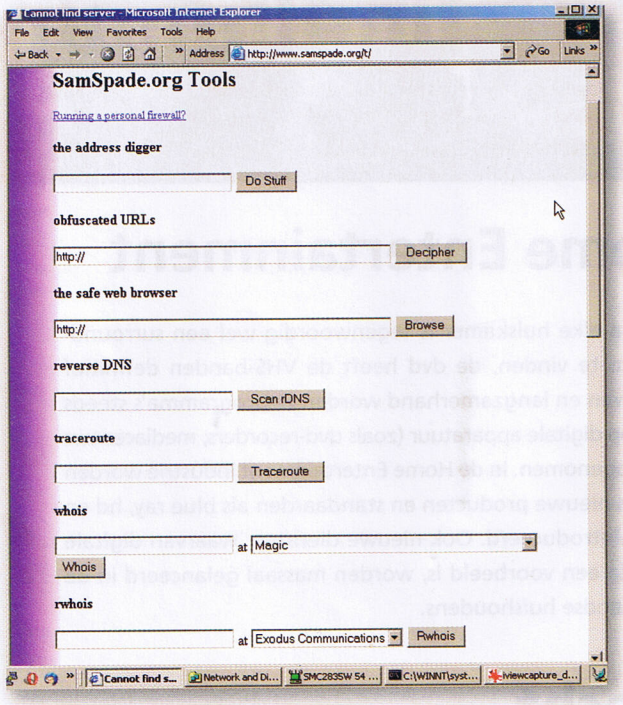
Vrijwel alle providers werken serieus mee aan de bestrijding van kwaadwillende computergebruikers die virussen en spam verspreiden of proberen in te breken op uw computer. Elke provider hanteert zijn eigen procedure voor het melden en de verdere afhandeling. Let erop dat het melden van misbruik bij uw provider niet gelijk staat met het doen van aangifte bij de politie. Providers kunnen uw aangifte soms ondersteunen door het verschaffen van ondersteunende gegevens, maar voor een strafrechtelijk onderzoek moet u beginnen met een aangifte bij de politie.

WAT MOET U MELDEN?

Providers zijn vrij om maatregelen te nemen tegen hun klanten indien ze misbruik plegen, dus een melding bij een provider is doorgaans de eerste stap die u kunt zetten om misbruik te laten stoppen. Het is daarbij van belang om de juiste informatie op te sporen en door te geven aan de instantie of provider waar u uw probleem meldt. Vrijwel altijd wordt gevraagd vanaf welk IP-adres misbruik heeft plaatsgevonden en hoe u dit hebt ontdekt. Het is daarnaast belangrijk om de logbestanden waaruit het misbruik blijkt, mee te sturen naar de instantie die uw klacht onderzoekt. Daarom adviseren we u om logbestanden langere tijd te bewaren, zodat u altijd kunt terugzoeken of er misschien eerdere pogingen zijn gedaan om in te breken. Doorgaans is het raadzaam om logbestanden minimaal zes maanden te bewaren. Overigens zijn de meeste logbestanden simpele tekstbestanden, die u eenvoudig kunt comprimeren.

WELKE PROVIDER MOET U HEBBEN?

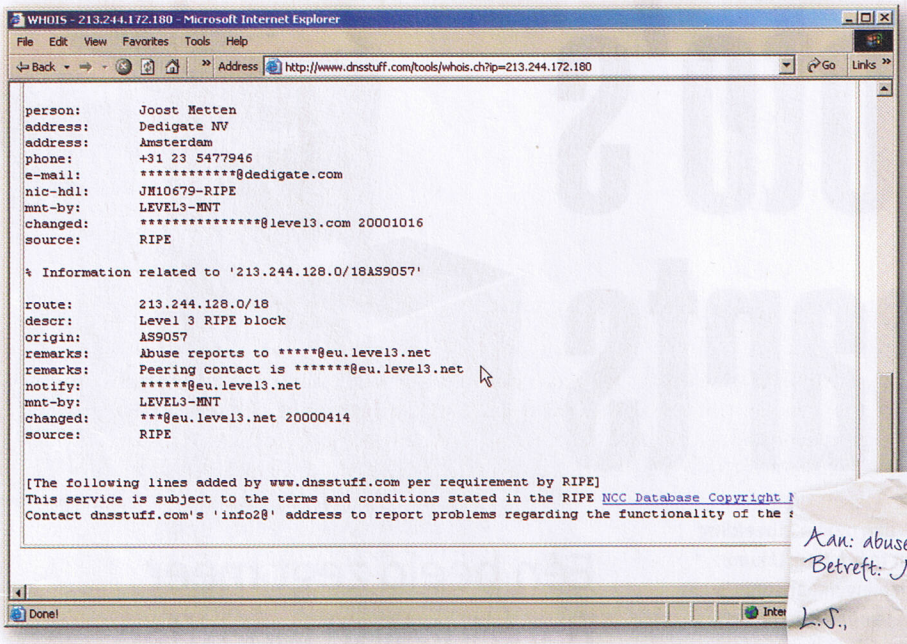
In de logbestanden staat vrijwel altijd vanaf welk IP-adres de pogingen tot misbruik zijn ondernomen. U kunt eenvoudig opzoeken welke provider verantwoordelijk is voor een willekeurig IP-adres door de zogenoemde Whois-database te raadplegen. In deze database staan alle IP-adressen die op internet in gebruik zijn, inclusief de gegevens van de provider die ze heeft uitgegeven. Providers zijn verplicht om deze gegevens



▲ *SamSpade.org biedt allerlei hulpprogramma's voor het nazoeken van eigenaars van domeinnamen en IP-adressen.*

IS HET IP-ADRES WEL JUIST?

Het IP-adres dat in uw logbestanden gevonden is, hoeft niet het adres te zijn van een kwaadwillende computergebruiker. Het komt namelijk veel voor dat hackers zich voordoen als een andere internetgebruiker om betrekkelijk anoniem in te breken op andere computersystemen. Dit zogenoemde 'spoofen' van IP-adressen is voor veel experts een fluitje van een cent en zorgt ervoor dat alle sporen naar een nietsvermoedende computergebruiker leiden. Spoofing komt ook voor door het 'overnemen' van een computer. In zo'n geval wordt speciale software geïnstalleerd die de controle van een computer ongemerkt overneemt.



▲ *De programma's die via DNS-Stuff worden aangeboden, stellen u in staat om veel gegevens terug te vinden. Hier ziet u bijvoorbeeld de Whois-gegevens (waarbij de e-mailadressen onherkenbaar zijn gemaakt) van de websites van Computer!Totaal.*

up-to-date te houden, zodat u ervan uit mag gaan dat vermelde telefoonnummers en e-mailadressen correct zijn. Om de database te raadplegen kunt u gebruikmaken van een aantal online hulpmiddelen, zoals de Whois-mogelijkheid op de site van RIPE of op de website van SamSpade. Op deze twee sites vindt u bovendien nog veel meer handige hulpmiddelen voor het tegengaan van misbruik.

ONMISBAAR: WHOIS

In de resultaten van een Whois-query zijn vaak de gegevens van meerdere providers opgenomen. Providers zijn namelijk zelf weer klant bij andere providers, die op hun beurt ook weer klant zijn van nog andere providers. IP-adressen zijn bijvoorbeeld uitgegeven aan een grote provider, die bepaalde delen weer uitgeeft aan zijn klanten. Onder die klanten kunnen weer andere providers zijn, die de IP-adressen zelf ook weer uitgeven. De Whois-database geeft alle stappen in deze structuur weer, waardoor u goed moet kijken welke provider uw aanspreekpunt is. Meestal is de laatste provider in de resultaten van de Whois-query de provider die u moet aanspreken voor uw klacht. In de Whois-database vindt u meestal een telefoonnummer en een aantal e-mailadressen. Tussen de e-mailadressen moet u op zoek gaan naar een adres dat gebruikt wordt voor zogenoemde 'abusemail'. Meestal begint dit e-mailadres met abuse@. Het melden van uw klacht doet u meestal bij de provider die verantwoordelijk is voor het IP-adres én bij uw eigen provider. Deze zal meestal niets kunnen ondernemen om het misbruik te laten stoppen, maar kan wel zelf contact opnemen met andere providers om in overleg bepaalde maatregelen te nemen.

WANNEER BENT U GETROFFEN?

Naast het IP-adres, dat u in uw logbestanden vindt, is het belangrijk om een juiste tijd door te geven. Alle providers zullen hierom vragen, zodat ze kunnen nazoeken welke gebruikers op dat tijdstip ingelogd waren. Hou er rekening mee dat de klok in uw computer mogelijk niet gelijk loopt met andere klokken. Daarom is het handig om de tijd in uw logbestanden terug te rekenen naar de standaard tijdzone, UTC. Zo kan elke internetprovider zelf berekenen op welke tijdskenmerken gezocht dient te worden.

CONCLUSIE

Het is moeilijk om precies aan te geven wanneer u uw provider moet waarschuwen en wanneer slechts sprake is van onschuldige logmeldingen. Op internet circuleren diverse programma's die de beveiliging van een computer automatisch testen op zwakke plekken. In logbestanden zijn dergelijke programma's eenvoudig terug te vinden, aangezien ze veel meldingen veroorzaken en alle alarmbellen laten rinkelen. Providers zullen in het algemeen niet zo heel erg veel doen met dit soort meldingen, omdat het opsporen en nazoeken meer tijd zal kosten dan de schade die het heeft opgeleverd. Als u echter daadwerkelijk braaksporen, inbraakpogingen of andere vormen van misbruik ziet, is het zeker raadzaam om contact op te nemen met uw internetprovider.

VOORBEELDBERICHT

Hier ziet u een voorbeeld van een mailbericht dat u kunt zenden aan uw provider wanneer u misbruik wilt melden. In dit mailbericht wordt een inbraakpoging via een ftp-server gemeld.

Aan: abuse@een-provider.nl
Betreft: Melding misbruik internetverbinding

L.S.,

Via dit mailbericht wil ik u op de hoogte brengen van misbruik dat ik heb geconstateerd via mijn internetverbinding. Op [datum] trof ik in mijn logbestanden van mijn ftp-server [software, fabrikant en versie vermelden] de volgende regels aan:

[regels uit logbestand]

De IP-adressen die u in deze regels aantreft, behoren volgens de RIPE-database toe aan u. Ik heb de gebruikers van deze IP-adressen geen toestemming gegeven om mijn ftp-server te gebruiken, noch om via mijn internetverbinding enig andere netwerkdienst te raadplegen. De klok van mijn server is gesynchroniseerd via NTP (Network Time Protocol) en geeft dus de juiste tijd in mijn tijdzone. Ik heb een kopie van de volledige logbestanden meegestuurd. Indien nodig ben ik graag bereid meer informatie te verschaffen.

Ik verzoek u maatregelen te nemen tegen de gebruiker met de IP-adressen zoals deze in de logbestanden zijn weergegeven en mij op de hoogte te stellen van de maatregelen die u hebt genomen. Tevens verzoek ik u om medewerking bij het doen van aangifte, zodat mijn aangifte volledige en juiste gegevens bevat.

Vriendelijke groet,

[uw naam]

WEBSITES

http://ct.link.idg.nl/abuse_mail: bovenstaande voorbeeldbrief in het Nederlands en Engels.
www.samspade.org/t: hulpprogramma's (website niet altijd bereikbaar).
www.dnsstuff.com: diverse hulpprogramma's voor het zoeken van IP-adressen en contactgegevens.
www.ripe.net: RIPE, organisatie die IP-adressen uitgeeft binnen Europa.
www.abuse.net: hulpprogramma om op te zoeken wie verantwoordelijk is voor een bepaalde domeinnaam.