Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Veiligheid en Justitie

> Retouradres Postbus 20011 2500 EA Den Haag

Aan de Voorzitter van de Tweede Kamer
Der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

Nationaal Coördinator Terrorismebestrijding en Veiligheid
Directie Cyber Security

Schedeldoekshaven 200
2511 EZ Den Haag
Postbus 20011
2500 EA Den Haag
www.nctv.nl

Ons kenmerk
370470

Bij beantwoording de datum en ons kenmerk vermelden. Wilt u slechts één zaak in uw brief behandelen.

Datum 3 april 2013
Onderwerp Onderzoek Pobelka botnet

In mijn brief d.d. 18 maart heb ik uw Kamer geïnformeerd over het handelen van de overheid en de ondernomen acties om botnets te bestrijden en dergelijke aanvallen eerder te detecteren. In deze brief heb ik tevens aangegeven dat vanuit de coördinerende rol van de NCTV partijen waaronder OM, Politie, AIVD, MIVD en het NFI bij elkaar zijn gebracht om op grond van de eigen taken en bevoegdheden onderzoek te doen naar het Pobelka-botnet. Doel van dit onderzoek is om de dataset in een bredere context te analyseren om de potentiële impact van de gegevens in de dataset op de nationale veiligheid in te schatten. Met deze brief informeer ik u over de uitkomsten en conclusies van dit onderzoek en de vervolgstappen die op basis hiervan zowel op de korte als de lange termijn zullen worden ondernomen.

Uitkomst van het onderzoek
In de onderzochte gegevens is geen informatie aangetroffen die een acuut risico vormt voor de continuïteit van getroffen organisaties of de nationale veiligheid. De aard van de informatie is echter wel dusdanig dat de gegevens een mogelijke springplank kunnen vormen voor toekomstige aanvallen of gericht handelen. De geïnfecteerde computers bevinden zich bij een grote diversiteit aan entiteiten, (waaronder veel particulieren, maar ook bedrijven) in diverse sectoren, ook in sectoren die door de overheid als 'vitaal' zijn aangemerkt en bij de overheid zelf.

Belangrijkste conclusies
Het NCSC komt tot deze inschatting op basis van de volgende onderzoeksconclusies uit het gezamenlijke onderzoek:
- Het Pobelkabotnet was actief tussen 2 februari 2012 en 19 september 2012 en bestond voornamelijk uit Nederlandse en Duitse computers.
- Het botnet was er, net als de meeste botnets, op gericht om financiële transacties tijdens het internetbankieren te manipuleren en er op die manier voor te zorgen dat het geld uiteindelijk bij criminelen terecht komt.
- Als bijvangst zijn er veel potentieel gevoelige gegevens van verschillende aard buitgemaakt. Het betreft gegevens die hoofdzakelijk via invoervelden in de webbrowsers verstuurd zijn.
- Op basis van de door het botnet verzamelde gegevens en de opdrachten die door de beheerder van het botnet zijn afgegeven is er op dit moment geen aanleiding om aan te nemen dat er gericht gezocht is naar bepaalde soorten informatie of bepaalde documenten.

Nationaal Coördinator Terrorismebestrijding en Veiligheid
Directie Cyber Security

Datum
3 april 2013

Ons kenmerk
370470

- De getroffen systemen en buitgemaakte gegevens zijn dermate divers dat geen reden is om aan te nemen dat het botnet gericht was op specifieke overheden, sectoren of organisaties.
- Uit een analyse van de AIVD is gebleken dat er geen aanwijzingen zijn voor spionageactiviteiten door statelijke actoren.
- Uit een analyse van de MIVD zijn vooralsnog geen activiteiten gebleken die duiden op (digitale) spionage jegens het ministerie van Defensie, de defensie-industrie of ten aanzien van onderwerpen met een militaire relevantie in het algemeen.
- De politie doet op dit moment op last van het Openbaar Ministerie onderzoek naar de verantwoordelijken voor het Pobelka-botnet. Dit onderzoek is nog niet afgerond.

Deze casus toont de kwetsbaarheid aan van de toenemende verwevenheid van het privé en zakelijk gebruik van informatietechnologie. Hierbij zijn bijvoorbeeld zakelijke gegevens terug te vinden op privé-computers van gebruikers. Naast bankgegevens bestaat de bijvangst van de buitgemaakte data uit allerlei persoonlijke informatie die privacygevoelig is. Tenslotte zijn bijvoorbeeld wachtwoorden van privé-accounts en niet-kwetsbare systemen door het botnet gekopieerd. Deze kunnen een springplank vormen voor het plannen van een gerichte aanval op kwetsbare systemen. Ondanks dat er in deze casus niet van een acuut risico voor de nationale veiligheid is gebleken, is de bredere botnetproblematiek aanleiding om zowel op de korte als op de lange termijn maatregelen te treffen, mede met het oog op de potentiële vervolgschade die door botnets kan worden aangericht.

Acties op korte termijn
Voor de analyse van de gegevens uit het Pobelka-botnet is samengewerkt door OM, Politie, AIVD, MIVD, NFI en het NCSC. De ervaringen hieruit onderstrepen het belang van de samenwerking bij het inschatten van risico's die uitgaan van botnets. Deze risico-inschattingen vormen de basis voor snel en adequaat optreden, ieder vanuit het eigen perspectief en op grond van respectievelijke taken en bevoegdheden. Het NCSC heeft daarbij een initiërende en coördinerende rol waarbij na formele verkrijging van de gegevens een eerste triage uitgevoerd wordt om te zorgen dat er door de voor dat geval meest geschikte partij gehandeld kan worden. In voorkomende toekomstige gevallen zal deze werkwijze opnieuw worden ingezet.

Op basis van organisatienamen, domeinnamen die gebruikt worden door organisaties en veel gebruikte trefwoorden die in de dataset gevonden zijn, zullen partijen binnen de doelgroep van Rijksoverheid en vitale sectoren actief geïnformeerd worden door het NCSC. Andere organisaties worden daar waar mogelijk bediend door partner- en schakelorganisaties. Het informeren van de eigenaren van mogelijk getroffen informatiesystemen vergt een aanzienlijke inspanning van het NCSC (in samenwerking met onder meer de internet service providers ISP's), en zal een periode van circa 6 weken vergen.

Acties met uitwerking op langere termijn
Het digitale domein wordt gekenmerkt door voortdurende technologische ontwikkeling en nieuwe uitdagingen in het veiligheidsdomein die een passend antwoord van publieke en private partijen vergt. In mijn brief van 18 maart jongstleden heb ik daarom de volgende vier acties aangekondigd: 1) het uitvoeren van een juridische verkenning over de vraag hoe het NCSC op een

zorgvuldige wijze kan omgaan met de informatie die hem vanuit de ICT-community bereikt, 2) het op- en uitbouwen van een nationaal detectie en responsenetwerk, 3) het i.s.m. de vitale sectoren onverminderd up-to-date houden van ip- ranges en 4) het actualiseren van de Nationale Cyber Security Strategie.

Daarnaast acht ik het van belang om nu en in de toekomst alle bij botnetbestrijding betrokken partijen, zowel nationaal als in internationale afstemming, in stelling te brengen om snel en adequaat te kunnen reageren op de dreiging die uitgaat van botnets. Dat is een gedeelde en gezamenlijke verantwoordelijkheid van publieke en private partijen.

Tot slot zal ik een overleg vormgeven met alle voor botnetbestrijding relevante publieke (het Ministerie van Economische Zaken, OM, Politie en NCSC) en private partijen (ISP's, elektronische dienstverleners en andere partijen met een directe vertrouwensrelatie met afnemers van een digitale dienst). Dit overleg moet bijdragen aan de effectiviteit van de aanpak van botnets in Nederland en de ontwikkelingen die daarin zijn te verwachten. Een voorbereidend overleg is inmiddels gepland.

De bredere botnetproblematiek blijft helaas onlosmakelijk verbonden met het gebruik van internet. Deze problematiek vraagt om een gepast antwoord van publieke en private partijen. De ingezette acties voorzien hierin en zullen in gezamenlijkheid worden uitgevoerd.

De Minister van Veiligheid en Justitie,

I.W. Opstelten

Nationaal Coördinator Terrorismebestrijding en Veiligheid
Directie Cyber Security

Datum
3 april 2013

Ons kenmerk
370470