



Eindrapportage pilot Quarantine-net voor SurfSnel ADSL

Van:	InterNLnet
Datum:	20 mei 2005
Gestuurd naar:	SURFnet

1. Inleiding

In november 2004 is een overeenkomst gesloten tussen Quarantainenet VOF en InterNLnet voor een pilot op de SurfSnel ADSL infrastructuur. Doel van deze pilot is het opdoen van ervaring met Quarantainenet (hierna Qnet) en te beoordelen of dit gebruikt kan worden om het aantal besmette pc's binnen de SurfSnel ADSL-populatie terug te dringen.

Om meerdere redenen is de start van de pilot (bedoeld voor 1 december 2004) vertraagd en is de pilot medio januari 2005 pas echt van start gegaan. Daarvoor is al wel de infrastructuur ingericht. Gedurende de periode medio januari – medio april heeft InterNLnet de Qnet oplossingen gebruikt als onderdeel van haar pakket aan maatregelen om de overlast van virussen en spam terug te dringen binnen de SurfSnelADSL-populatie.

Via deze rapportage wordt beschreven wat onze bevindingen zijn geweest tijdens de pilot en in hoeverre Qnet aan het doel heeft voldaan. Ook wordt bekeken of Qnet voor een Internet Service provider als InterNLnet een geschikt middel is voor verder gebruik.

2. Technische opzet van de pilot

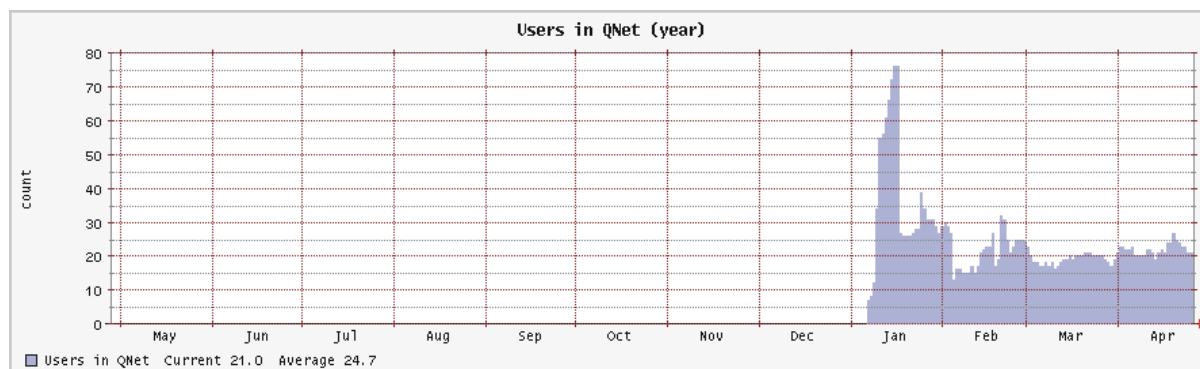
De configuratie voor Qnet bij InterNLnet bestaat uit twee servers: een 'honeypot' (vangmechanisme) en een beheer machine die ook zorgt voor de logging. Beide machines zijn voorzien van een Linux Operating System (Trustix) en voorzien van een single processor, 1 Gb geheugen en 72 Gb schrijfruimte. Op de beheer machine is Perl geïnstalleerd.

De SurfSnel-ADSL klanten maken gebruik van een modem (met een vast publiek IP adres) of een router (met een aaneengesloten reeks van vaste publieke IP-adressen).

3. Kwantitatieve resultaten

In de pilotperiode van Qnet van drie maanden zijn in totaal 325 IP adressen geblokkeerd. Er zijn klanten met meerdere IP adressen die meerdere keren 'gevangen' zijn. Hiernaar hebben wij (nog) geen onderzoek gedaan. InterNLnet merkt op dat overwogen zou kunnen worden Quarantainenet kennis te laten bevatten van het subnet van klanten: IP adressen zijn zo herkenbaar als horend bij één en dezelfde klant. De klant krijgt standaard één kans om zichzelf, na het ondernemen van een opschoonactie, af te melden (de zogeheten '1 strike' optie). In sommige gevallen slaagde de klant er niet in om in één actie de pc virus vrij te maken, zodat na gebruik van de 1 strik optie de pc al snel weer in quarantaine is geplaatst.

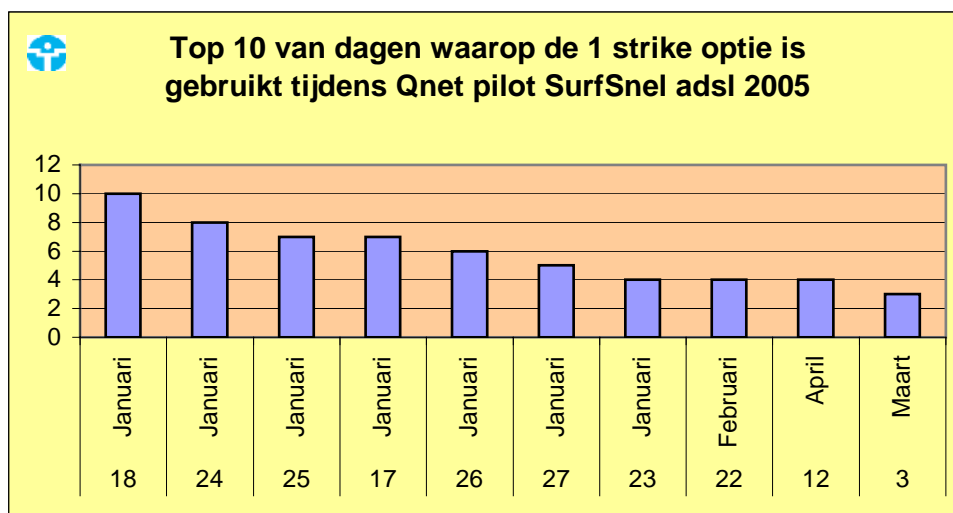
Het antwoord op de vraag in hoeverre het aantal besmette pc's gedaald zou zijn gedurende de pilotperiode is niet met zekerheid te geven. Dit valt niet goed te meten omdat we in deze periode ook nog andere maatregelen hebben genomen tegen vormen van abuse (spam / virussen), terwijl ook de N (de populatie klanten en IP adressen) niet statisch is geweest.



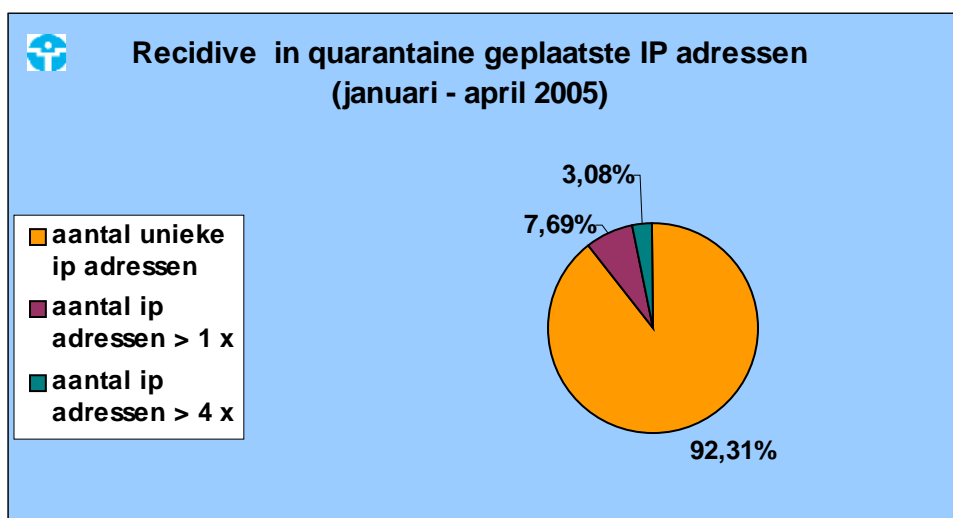
Het aantal klachten van SURFnet-CERT met betrekking tot SurfSnelADSL'ers is na het inzetten van Qnet duidelijk afgenomen. Duidelijk is ook dat de meeste 'vangsten' bij het begin van de pilot in januari plaats hebben gevonden. Daarna heeft zich dit aantal min of meer gestabiliseerd op ca. 20 IP-adressen die gelijktijdig in quarantaine staan. Wij hebben overigens de indruk dat het aantal



'vangsten' per maand vooral afhankelijk is van de ontwikkelingen op virus gebied: uitbraken van nieuwe agressieve virussen kunnen leiden tot een forse toename van klachten en problemen.

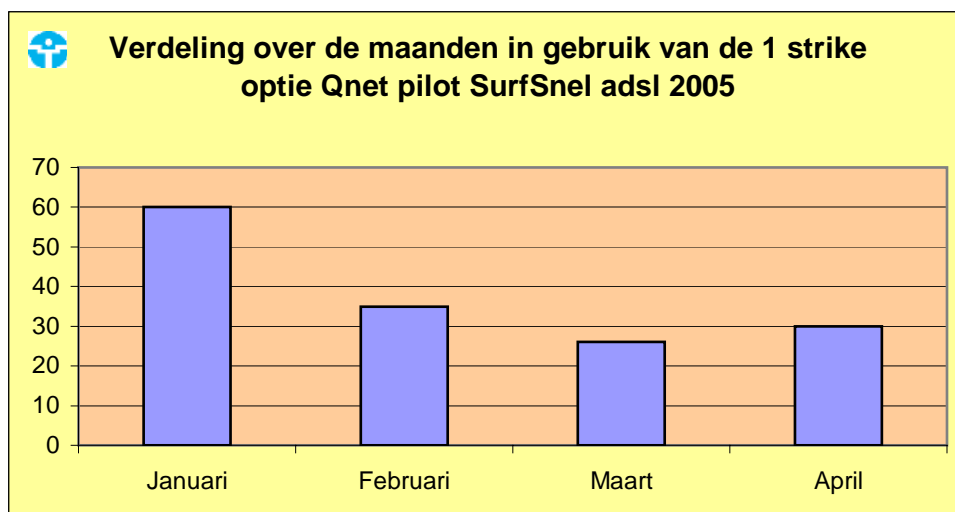


Meer dan 90 % van de gevallen is in de pilot periode (drie maanden) slechts één maal 'gevangen' door de honeypot. Een enkeling zat meer dan vier keer 'vast'. Er is geen onderzoek gedaan naar hoe lang een IP-adres in quarantaine gevangen zat (gemiddelden en uitschieters); indruk is wel dat in de meeste gevallen sprake was van een kortdurend verblijf in Qnet (veelal minder dan 24 uur), maar er waren ook gevallen bij van IP-adressen die langer dan 1 week 'vast' zaten.

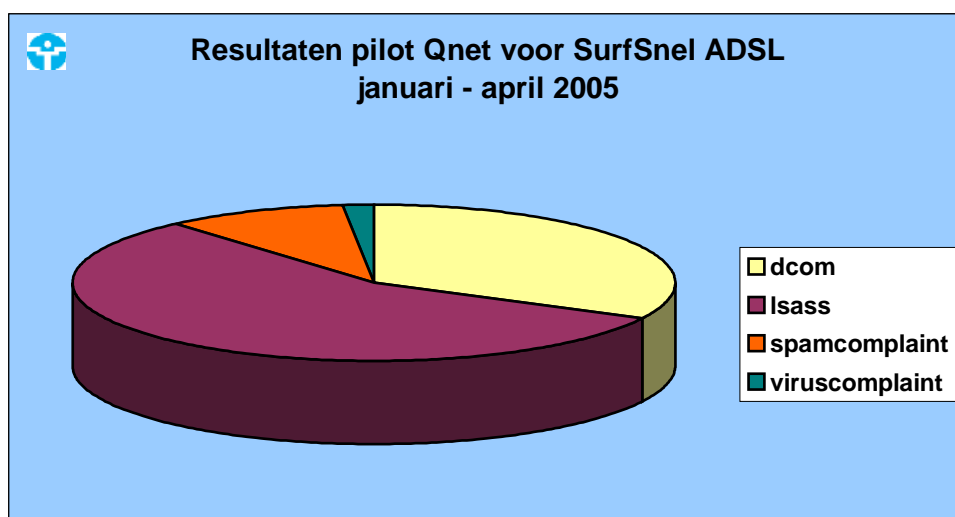


Begin februari heeft InterNLnet een kleine 'amnestieregeling' afgekondigd: in totaal werden 13 IP-nummers 'bevrijd', waarvan er slechts één kort daarna weer gevangen is door de honeypot. Mogelijke verklaringen hiervoor zijn:

- een 'passant' sluit een besmette laptop aan op de DSL verbinding van een SurfSnel'er; het IP-adres gaat in quarantaine maar wordt na vertrek van de passant niet (snel) meer gebruikt
- het betreft een 'verlaten' IP-adres: mensen hebben hun computer een ander adres uit hun eigen range gegeven. Het lijkt erop alsof 'naburige' IP-adressen regelmatig ook in quarantaine geplaatst worden.



Van de in Qnet geplaatste gevallen, werd de grootste groep gevormd door pc's die besmet waren met wormen die gebruik maken van het Isass exploit of een dcom exploit.



De categorieën spamcomplaint en viruscomplaint zijn categorieën die door InterNLnet zelf zijn gebruikt om mensen 'handmatig' in Qnet te plaatsen indien wij klachten over dit IP-adres hadden binnen gekregen van derden (via de abusemail).

4. Kwalitatieve resultaten

De installatie van de infrastructuur voor Qnet is redelijk soepel verlopen. Qua infrastructuur hebben wij gedurende de resterende pilotperiode geen bijzondere problemen ondervonden; er kan dus gesproken worden van een stabiele situatie.

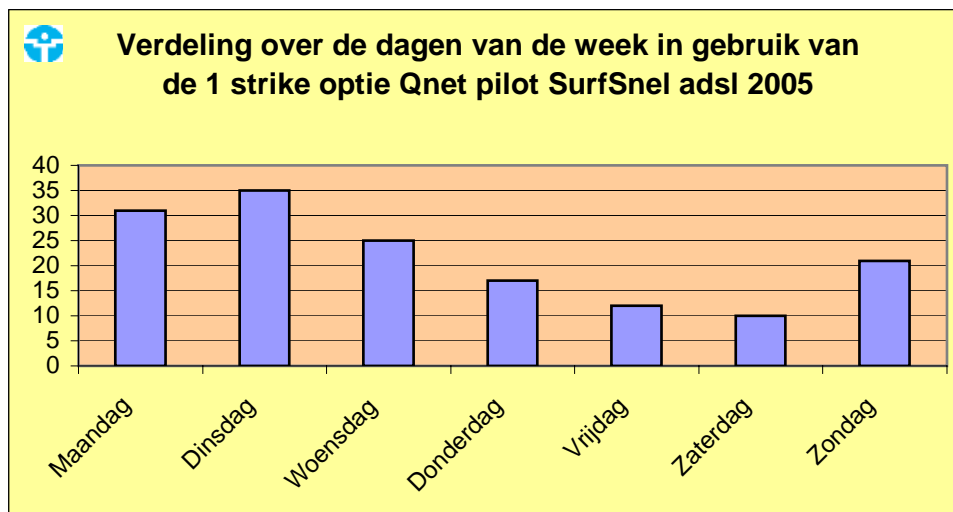
InterNLnet heeft bij de start relatief veel tijd moeten besteden aan het 'vertalen' van de teksten voor onze klanten. Deze waren te technisch van aard en niet duidelijk genoeg. Inmiddels hebben wij een set 'begrijpelijke' en klantvriendelijke teksten voor Qnet ontwikkeld. Klanten die in Qnet komen, wordt via deze teksten uitgelegd hoe een en ander werkt. Wij hebben er hierbij voor gekozen om er van uit te gaan dat de klant hulp nodig heeft bij een probleem (support karakter) en niet gestraft dient te worden voor iets waarvan de klant zich veelal zelf niet bewust is (besmette pc). Het aandeel 'bewuste' overlast veroorzakers rechtvaardigt in onze ogen deze houding.

Het klantvriendelijke, support achtige karakter van de teksten (met bijbehorende instructies voor onze support afdeling) is er in onze ogen ook mede voor verantwoordelijk geweest dat de 'ontvangst' van Qnet maatregelen overwegend positief was bij onze klanten. Onbekend is of dit op langere termijn zo zal blijven (een klant die binnen enkele maanden meerdere keren gevangen wordt, kan het 'beu' worden om steeds weer actie te moeten ondernemen).

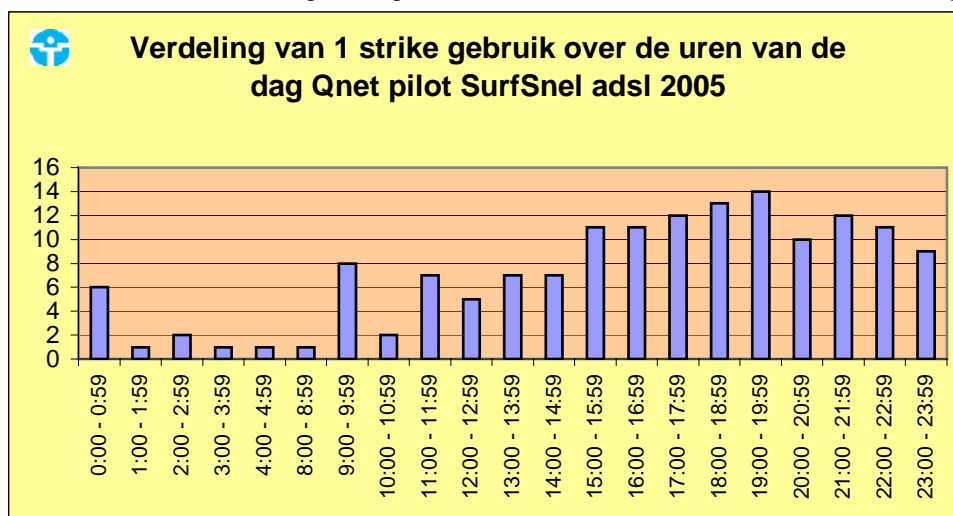
Een enkele klant reageerde wel negatief, voornamelijk omdat de consequentie was/is dat er geen mail verstuurd kan worden, hetgeen voor sommige klanten zeker op bepaalde momenten heel slecht kan



uitkomen. Deze vorm van overlast wordt vooral als hinderlijk ervaren indien de klant zich niet (meer) zelf uit Qnet kan halen na uitvoeren van een opschoon actie. Indien de dan benodigde assistentie van een medewerker van InterNLnet niet (direct) verkregen kan worden (bijvoorbeeld 's avonds of in het weekend), kan bij de klant de irritatie toenemen.



De klant krijg standaard één kans om zichzelf, na het ondernemen van een opschoonactie, af te melden (de zogeheten '1 strike' optie). In de huidige opstelling is deze optie niet aan tijd gebonden. Met andere woorden: een klant die in januari tegen een bepaald virus aanloopt, dat opruimt en in april een andere, nieuwe besmetting oploopt, kan zich in april niet meer 'zelf' uit Qnet halen. Na 'gebruik' van die ene optie om zichzelf af te melden, moet de klant nu altijd aankloppen bij InterNLnet en deze kan het verzoek handmatig inwilligen. Voor klant en InterNLnet is dit te bewerkelijk en omslachtig.



Mede om deze reden zal InterNLnet aan Quarantainenet VOF een voorstel doen om de applicatie aan te passen waarbij:

- er een expiratedatum komt voor de 1 strike optie (b.v. 24 uur)
- en/of de klant meerdere strikes krijgt (kan ook een soort 'test' zijn om te zien of er voldoende goed is opgeruimd)
- de klant een 'test' mogelijkheid krijgt die uitgevoerd kan worden alvorens de 1 strike optie te gebruiken.

Dit zal onderwerp van gesprek zijn tijdens een eerdaags te organiseren overleg tussen beide partijen.

Voor de mensen die de abuse mail afhandelen (bij InterNLnet de system operators) is Qnet een welkome aanvulling gebleken voor de tools om de overlast van virussen en spam terug te dringen. Het is voor hen een arbeidsextensieve en efficiënte tool. Voor de support afdeling levert Qnet wel het nodige werk op; zowel eenmalig (goede teksten en handleiding schrijven) als periodiek (klanten die hulp nodig hebben omdat ze 'vast' zitten). De support afdeling zal zelf een interface krijgen waarmee ze klanten 'direct' uit Qnet kunnen halen. Voor de netwerkbeheerders geldt dat zij zich met name in de beginperiode hebben moeten inzetten maar nu meer achterover kunnen leunen als het gaat om Qnet.



Qnet is door InterNLnet alleen getest voor diensten waarbij gewerkt wordt met vaste IP-adressen. Onbekend is of de oplossing ook geschikt gemaakt kan worden voor diverse andere (access) diensten van InterNLnet zoals dial en glasvezeldiensten, waarbij gebruik wordt gemaakt van dynamische toekenning van IP-adressen. Dit zal nog met Quarantainenet VOF besproken worden.

5. Kosten – baten analyse

InterNLnet ambieert om van Qnet gebruik te gaan maken op basis van een service model, waarbij Quarantainenet VOF een vaste periodieke vergoeding krijgt voor het actueel houden van het systeem. Gezien de huidige ontwikkelingen op het gebied van virussen en spam, is het nemen van aanvullende maatregelen ter bescherming van eigen klanten en andere gebruikers van het Internet een logische stap waarvoor ook onder klanten het nodige draagvlak lijkt te bestaan. Qnet past goed in een dergelijk pakket aan aanvullende maatregelen maar is niet zaligmakend. Of het op langere termijn ook succesvol blijft en breed binnen InterNLnet ingezet kan worden is op dit moment een vraagteken en is mede afhankelijk van het antwoord op de vraag of het systeem ook succesvol gebruikt kan gaan worden voor diensten die werken met het dynamisch toekennen van IP-adressen.

6. Conclusie

De pilot met Qnet heeft zeker voldaan aan één van de twee doelen van de pilot: InterNLnet heeft kennis en ervaring met Qnet opgedaan. Circa 300 klanten zijn in de pilotperiode 'gevangen' en hebben vervolgens hulp gekregen bij het opschonen van hun pc. Of dit ertoe heeft geleid dat er sprake is van een afname in het aantal besmette pc's op de totale populatie is niet ondubbelzinnig vast te stellen.

InterNLnet heeft in het algemeen een positief beeld gekregen van de mogelijkheden die Qnet biedt en ziet dan ook mogelijkheden om de applicatie en software 'blijvend' in te gaan zetten voor bepaalde productlijnen en klantgroepen. Hiertoe volgende deze maand nog onderhandelingen met Quarantainenet VOF. In overleg met hen zal ook bekeken worden of de huidige test opstelling wordt afgebroken dan wel gecontinueerd.

Met Quarantainenet VOF zal ook de mogelijkheid worden besproken om de applicatie zo aan te passen dat de klant meer mogelijkheden krijgt om zichzelf af te melden, indien deze na een geconstateerde besmetting de gewenste opruimactie heeft ondernomen. Dit kan zorgen voor een nog betere balans tussen een goed (netwerk)beheer enerzijds en klantvriendelijkheid anderzijds. Met deze rapportage beëindigd InterNLnet de medio januari 2005 gestarte pilot.