Frank Brokken f.b.brokken@rc.rug.nl

De Blaster.Worm en het Sobig.F-virus

Helpdesk is een vaste rubriek waarin vragen en problemen met betrekking tot computergebruik worden behandeld.

Security manager van het RC Frank Brokken gaat in op de laatste virussen die veel problemen veroorzaken: de W32.Blaster.Worm en het Sobig.F-virus.

Dat Windows-systemen eenvoudig het slachtoffer kunnen worden van virussen en andere kwaadaardige software is algemeen bekend.
Het is belangrijk om een aantal voorzorgsmaatregelen te nemen om uw pc te beveiligen.

1. installeer een virusscanner die een recente virus-database hanteert;
2. houd uw computer up-to-date door zogenaamde 'security patches' te installeren (Microsoft publiceert talrijke adviezen over hoe dat in z'n werk gaat [1])
3. wees (uiteraard) voorzichtig met het openen van attachments, extra bestanden die door de afzender van e-mail aan het verstuurde bericht worden toegevoegd.

Recent is veel ophef ontstaan over de W32.Blaster.Worm en het Sobig.F-virus. Zo wijdde De Volkskrant van 25 augustus j.l. een voorpagina artikel aan de effecten van het Sobig.F-virus. Hoewel we kunnen verwachten dat de storm rondom het Sobig.F-virus bij het verschijnen van dit artikel enigszins zal zijn geluwd, is het toch nuttig om een en ander op een rijtje te zetten.
We kunnen in de toekomst meer van dergelijke malafide software in het internet verwachten, en het is belangrijk te weten wat zo'n virus zoal doet, onder het motto 'een gewaarschuwd mens telt voor twee'.

Sobig.F-virus

Het Sobig.F-virus is een zogenaamde worm die zich via e-mail verspreidt over computers die zich waar ook ter wereld kunnen bevinden. Het maakt gebruik van zogenaamde 'gespoofde' (valse) afzenderadressen. De adressen worden door het virus uit het adressenbestand van een besmette computer gelicht.
Het virus wordt tot 10 september verspreid; geïnfecteerde systemen zullen na deze datum blijven proberen nieuwe updates te downloaden waardoor het virus zich vernieuwt.

Systemen

De volgende systemen kunnen door de worm worden geïnfecteerd: Windows 2000, Windows 95, Windows 98, Windows ME, Windows NT, Windows XP. Daarentegen zijn Linux, Macintosh, OS/2, UNIX, en Windows 3.x systemen niet ontvankelijk voor de worm.
Symantec (de leverancier van de Norton antivirus-software) geeft een overzicht [2] van de activiteiten van de worm.

Eigenschappen e-mail

De worm is mogelijk aanwezig in e-mail waarin het volgende onderwerp (Subject) wordt gehanteerd:

- Re: Details
- Re: Approved
- Re: Re: My details
- Re: Thank you!
- Re: That movie
- Re: Wicked screensaver
- Re: Your application
- Thank you!
- Your details

Persoonlijk heb ik de afgelopen dagen zeker zo'n 400 van dergelijke e-mails ontvangen (overigens zonder risico, want ze werden al door mijn spamfilter herkend, en bovendien gebruik ik geen systeem dat vatbaar is voor het Sobig.F-virus). Ik veronderstel dat ook anderen gelijksoortige e-mail zullen hebben ontvangen.

Maatregelen voor thuisgebruikers

Symantec beschrijft niet alleen dat het virus bestaat, maar ook wat er tegen kan worden gedaan. Samengevat komt het neer op het volgende:

1. Installeer de Symantec virusdefinities van 19 augustus of later (het regelmatig (eens per week) verversen van de virusdefinities is zonder meer een goede zaak: doen!). De verversing kan automatisch plaatsvinden, maar het meest recente bestand kan ook worden gedownload van 3
2. Download gereedschap om de worm te verwijderen van 4 en volg de instructies die op deze webpagina zijn gegeven.

Maatregelen voor netwerkbeheerders

Netwerkbeheerders kunnen overwegen om de volgende 'poorten' af te sluiten:

- inbound op poorten 99x/udp
- outbound op poort 8998/udp

Bovendien worden NTP requests op poort 123/udp gegenereerd door geïnfecteerde computers.

W32.Blaster.Worm

Voorafgaand aan het Sobig.F-virus, was de W32.Blaster.worm al actief. Dit is een virus dat gebruikmaakt van een lek in een aantal recente versies van Windows. Voorzover nu bekend is het virus vooral hinderlijk en brengt het geen schade toe aan gegevens op de pc. Het virus gebruikt veel geheugencapaciteit van de computer waardoor deze trager kan worden. Daarnaast kan de pc door het virus uit zichzelf herhaaldelijk herstarten.

Systemen

De Blaster-worm kan onbeschermde pc's infecteren die gebruikmaken van Windows XP, Windows 2000, Windows Server 2003, Windows NT 4.0 of Windows NT 4.0 Terminal Services Edition. Microsoft heeft op 16 juli 2003 een security patch (MS03-026) beschikbaar gesteld waarmee u uw computer en systemen kunt beschermen. Indien u deze patch al geïnstalleerd heeft, bent u beschermd tegen de Blaster-worm. Heeft u een oudere Windows-versie, zoals Windows 95, Windows 98, of Windows ME, dan hoeft u géén maatregelen te treffen tegen de Blaster-worm.

Herkenning van besmetting

Aanwezigheid van het bestand 'MSBLAST.exe' in de standaard Windows-System32 directory. (C:\Windows\System32). Ook in de registry kunnen zich aanwijzingen bevinden die er op wijzen dat de pc is geïnfecteerd. Het is aan te raden om aanpassingen in de registry van Windows alleen te laten uitvoeren door Windows-specialisten.

Maatregelen

1. Installeer de security patch 'MS03-026' wanneer u gebruikmaakt van een van de boven genoemde kwetsbare systemen en dit nog niet heeft gedaan van 5
2. Wanneer uw pc besmet is met de blaster-worm, kunt u gereedschap downloaden om de worm te verwijderen van 6

Samenvattend

1. De beste beveiliging bent u zelf: open geen attachments en installeer geen onbekende software, tenzij u 100 % zeker bent van de integriteit van de software. Beschouw attachments en nieuwe software als het elektronisch equivalent van een mogelijke briefbom;
2. Zorg voor recente Windows-security patches;
3. Zorg voor een goede virusscanner en ververs regelmatig, liefst wekelijks, de bijbehorende virusdefinities.

Neem desgewenst contact op met de helpdesk van uw provider wanneer u moeite heeft met het installeren van de geadviseerde software.

Links

- De Nederlandse website van Micorsoft: **www.microsoft.nl**
- De Nederlandse website van Synantec: **www.symantec.nl**
- Uitgebreide en actuele informatie over computervirussen vindt u ook op **www.virusalert.nl**

1 Informatiepagina van Microsoft over beveiliging: **www.microsoft.com/security/**

2 Een overzicht van de activiteiten van het Sobig.F-virus: **securityresponse.symantec.com/avcenter/venc/data/w32.sobig.f@mm.html**

3 De Symantec virusdefinities kunt u downloaden van **securityresponse.symantec.com/avcenter/download/pages/US-N95.html**

4 Instructies en gereedschap voor het verwijderen van het Sobig.F-virus is te vinden op **securityresponse.symantec.com/avcenter/venc/data/w32.sobig.f@mm.removal.tool.html**

5 De security patch MS03-026 waarmee u de pc tegen de Blaster.worm kunt beschermen, kunt u downloaden van **windowsupdate.microsoft.com**

6 Instructies en gereedschap voor het verwijderen van de Blaster.Worm is te vinden op **securityresponse.symantec.com/avcenter/venc/data/w32.blaster.worm.removal.tool.html**