

Spyware verwijderen en voorkomen

Mei 2006

Henk Jongedijk, maandag 23 oktober 2006 - 00:00:00

Veelal ongemerkt is spyware voor veel gebruikers een groot probleem. De PC wordt traag, ongewenste reclames en pop-ups en nog andere ellende zijn voor slachtoffers bekende verschijnselen die laten zien dat er spyware op hun computer aanwezig is. Maar niet iedereen is zo deskundig om alle symptomen als zodanig te herkennen. Uit sommige onderzoeken zou zelfs blijken dat een derde van alle Internetgebruikers is besmet met spyware. Eerdere columns op Web-start hebben het onderwerp spyware al meerdere malen beschreven, inclusief hoe het werkt en hoe het verwijderd kan worden. Aangezien de ontwikkelingen omtrent spyware continue doorgaan en ik het belangrijk vindt om gebruikers in te lichten over de gevaren van spyware heb ik de nieuwste feiten op een rij gezet.

De makers van spyware zitten natuurlijk niet stil en de ontwikkelingen volgen elkaar in snel tempo op. Graag wil ik dit artikel samen met lezers regelmatig van updates voorzien. Ik zie uw reacties, ervaringen, tips en ideeën om spyware slachtoffers te helpen en besmetting te voorkomen graag tegemoet in de reactie mogelijkheid onderaan dit artikel.

Wat is spyware?

De definitie van spyware is volgens het onderzoek "Spyware: de pest van de 21e eeuw" van de [Safe Internet Foundation](#) als volgt: Spyware is "downloadbare software, ook vaak bij andere software ingesloten, waarvan de gebruiker het effect op zijn computer redelijkerwijs niet heeft kunnen inschatten of niet op de hoogte was of kon zijn van het feit dat die software geïnstalleerd werd. De software wordt gebruikt om ongewenste reclames te versturen, nadere software te installeren of gegevens over de gebruiker te verzamelen, zoals zijn surfgedrag, mailadres of zelfs creditcardgegevens." Met mijn eigen woorden: stiekem geïnstalleerde software die informatie van de computer gebruiker misbruikt. Dergelijke software wordt ook wel malware genoemd.

Hoe werkt spyware?

Spyware kwam oorspronkelijk vooral binnen via zogenaamde ActiveX plugins. ActiveX is een technologie van Microsoft waarbij je in verschillende omgevingen een programma af kan draaien. Het is vergelijkbaar met de Java-technologie van Sun. ActiveX is software die je dus ook af kunt draaien in een webpagina. Om de software binnen de webomgeving af te spelen moet er wel eerst een programmaatje geïnstalleerd worden.

Malafide en kwaadwillende Internet ondernemers (oftewel de spyware makers) maken misbruik van de mogelijkheden die ActiveX biedt. ActiveX is platform onafhankelijk en het functioneert net zo makkelijk in Internet Explorer als in de Windows desktopomgeving. In Internet Explorer kun je zelfs aangeven dat ActiveX componenten automatisch worden gedownload. De computer houdt rekening met de verschillende zones van waaruit ActiveX-applicaties worden gedraaid. Het Internet wordt door de computer beschouwd als een restricted zone waar niet zomaar alles mag draaien. Je eigen computer is een zone waar veel meer mag. Hierin schuilt het venijn; met behulp van codes kunnen ActiveX-applicaties verstuurd worden van de onveilige Internet zone naar de veilige computeromgeving, waar ze zonder restricties uitgevoerd worden.

Om Internet Explorer gebruikers iets meer bescherming te bieden, heeft Microsoft de manier aangepast waarop ActiveX binnen de browser wordt aangeroepen. Gebruikers moeten eerst via een gele balk boven in het scherm toestemming geven om de applicatie te starten of installeren. Spyware verspreiders speelden hier al snel op in, door (onwetende) gebruikers screenshots te tonen wat ze moesten doen om die mooie 'screensaver' (die ook spyware bevat) te installeren.

Meer geavanceerd is de spyware zich dankzij lekken (ook wel exploits genaamd) in Internet Explorer weet te installeren. Spyware schrijvers maken gebruik van allerlei gaten in Microsoft's browser om dit te doen. In voorjaar 2006 werd het [WMF lek in Windows](#) nog massaal misbruikt. Een bewijs dat het belangrijk is om het besturingssysteem up-to-date te houden. Aangezien veel web gebruikers dit nog altijd niet doen, heeft spyware die gebruik maakt van 'oude' lekken nog steeds voldoende potentiële slachtoffers.

Hoe loop je spyware op?

1. Via websites

Doordat Internet Explorer goed overweg kan met ActiveX is dit de belangrijkste infectiebron. Bovendien zijn er exploits die in Internet Explorer malware kunnen installeren zonder dat er een installatiescherm aan te pas komt.

2. Via 'gratis' programma's

Een berucht programma is bijvoorbeeld KaZaa, het populaire peer-to-peer bestandsuitwisselprogramma, dat een bron van spyware is bij installatie. Inmiddels vragen recente versies van KaZaa uitvoerig om akkoord te gaan met allerlei advertentiesoftware voordat je het programma kunt gebruiken. Wees altijd op uw hoede; programma's die nu nog gratis en spywarevrij worden aangeboden kunnen in de toekomst te gelde gemaakt worden door toevoeging van adware. Een andere infectiebron zijn de zogeheten 'cracks en serialgenerators'. Deze programma's worden gebruikt om kopieerbeveiligingen op software te omzeilen. In de kraakprogramma's kan malware verstopt zijn.

Gebruik daarom altijd door uzelf aangeschafte software of betrouwbare open-source software.

3. volg de Gouden Regels niet

Een derde van de computergebruikers scant zijn computer nooit op virussen, maar vertrouwt volledig op zijn antivirusscanner. Nog eens 34 procent scant de computer [minder dan 1 keer per kwartaal](#). Lees hieronder de Gouden Regels om spyware te voorkomen.

Hoe verwijder je spyware?

Om spyware te verwijderen zijn allerlei programma's beschikbaar. Een kleine greep in alfabetische volgorde:

- » [Ad-Aware](#)
- » [HijackThis 1.99.1](#) ([Handleiding HijackThis](#))
- » [Hitman Pro](#)
- » [Spybot - Search & Destroy 1.4](#)
- » [Windows Defender](#)

Hoe voorkom je spyware?

1. Gebruik een andere browser

Er zijn meerder browsers voorhanden, bijvoorbeeld [Opera](#), [Konqueror](#) of [FireFox](#). Voor Apple gebruikers is er [Safari](#). [FireFox](#) is een populair open source alternatief voor de Microsoft Internet Explorer. Er wordt beweerd dat FireFox ook veiliger is. Het is standaard inderdaad niet gevoelig voor ActiveX-plugins. FireFox beschermt je overigens niet tegen malware die je via 'gratis' programma's zoals KaZaa binnenkrijgt. Een handige uitbreiding voor Firefox is de [NoScript plugin](#). Naarmate de populariteit van FireFox stijgt, worden er steeds meer omwegen gevonden om bijvoorbeeld toch pop-ups in FireFox te laten verschijnen.

2. Gebruik een Spyware verwijderprogramma

Aangezien spyware vooral een probleem is dat Windows gebruikers treft heeft Microsoft besloten om met haar eigen anti-spyware oplossing te komen. De softwaregigant heeft hiervoor geen eigen programma ontwikkeld, maar het programma van Giant AntiSpyware overgenomen. Microsoft of Windows Antispyware gaat inmiddels als Windows Defender door het leven en kan gratis gedownload worden (zie 'Hoe verwijder je spyware?')

3. Bewust gebruik

Er is geen betere bescherming tegen een spyware infectie dan veilig Internetgedrag. Gewoon blindelings overal op akkoord of ja

klikken kan je snel in de problemen brengen. Bewust nadenken, updates op software toepassen en voorwaarden lezen als gebruiker en daar je klikgedrag op aanpassen is de beste bescherming tegen spyware. Virusscanners, firewalls en updates zijn nooit zo goed in staat als de gebruiker om nieuwe gevaren te erkennen en de juiste acties daarop te ondernemen. De malware producenten kunnen heel snel hun software aanpassen, zodat ze niet worden ontdekt door detectie- en verwijder-software.

4. Pas de Gouden Regels toe

Om Spyware op je pc te voorkomen stel ik voor de volgende Gouden Regels altijd op te volgen:

- » Installeer Microsoft security patches
- » Gebruik geen onbekende freeware
- » Schakel downloads via ActiveX in Internet Explorer uit
- » Gebruik regelmatig een spyware verwijderprogramma
- » Installeer een anti-virus programma en update deze regelmatig

Top 10 gevaarlijkste spyware

Om gebruikers over de gevaren van spyware te informeren besloot anti-spyware aanbieder Webroot (maker van Spysweeper) een top tien samen te stellen. De lijst is gebaseerd op hoe vaak de spyware voorkomt en op complexiteit ervan. Sommige spyware is bij de meeste gebruikers wel bekend, maar het zijn vaak de onbekende programma's die voor veel ellende kunnen zorgen.

De Top 10 spyware (mei 2006):

1. [AbetterInternet](#)
2. CoolWebSearch
3. [EliteBar](#)
4. [IST Istbar](#)
5. [Look2Me](#)
6. [ShopAtHomeSelect](#)
7. [SurfSideKick](#)
8. [Virtumonde](#)
9. [WebSearch Toolbar](#)
10. [180search Assistant/Zango](#)

Spyware gefilmd

In onderstaande online filmpjes wordt getoond hoe spyware zich via Internet Explorer en Windows kan infecteren, verspreiden en vermenigvuldigen:

- » [CreateTextRange exploit](#)
- » [WMF exploit](#)
- » Nog een [WMF exploit](#)

Conclusie

Spyware infecties zijn met een portie gezond verstand en de juiste tools en programma's redelijk te voorkomen, hoewel het altijd lastig blijft om spyware websites te herkennen. Dat neemt niet weg dat het updaten van browsers, applicaties en besturingssysteem een hoop ellende voorkomt.

Relevante links

[Spyware: de pest van de 21e eeuw. \(pdf\)](#)

[Hoe verwijder je spyware?](#)

[CWS CoolWebSeach verwijderen](#)