DM71

Spyware

Jacob Christiansen, 130282

Institut for Matematik og Datalogi
Syddansk Universitet
http://www.imada.sdu.dk

15. maj 2006

1 Introduktion

Spyware er i løbet af få år gået fra at være en mindre online plage, til at være en at de største trusler mod internettet i dag. Brugere kæmper for at opretholde kontrollen med deres computer og befinder sig ofte i cykliske kampe med software som installerer sig selv uden advarsel, åbner nye sikkerhedshuller og installerer sig selv igen, efter de er blevet afinstalleret.
De værste af disse programmer, tillader kriminelle at stjæle personlige informationer. Men selv de mest uskyldige programmer kan tvinge en computer i knæ med unødvendige "services". Disse programmer kommer ikke kun ind på en computer via lovlige kanaler så som, ekstra software sammen med andet shareware fra nettet, men ofte benytter udviklerne af spyware sig af sikkerhedshuller i browsere, samt andre mere eller mindre smarte metoder til at liste software ind på en computer uden brugers accept.

Jeg har valgt i denne rapport at lægge vægt på den brede betagnelse af spyware. Dvs. at under termen spyware, gemmer der sig ord som adware, malware, stealware osv., som inbefatter alt lige fra simple pop-up vinduer til keyloggers. Da alle disse programmer normalt falder under den samme katagori i anti-spyware software, var dette en naturlig følge.

2 Hvad er spyware?

Definitionen på spyware har ændret sig flere gange. Fra at betagne keyloggers og andre spionprogrammer til at betegne en meget større gruppe af software, som alle har det til fældes at de i mere eller mindre grad er uønsket på en computer. Definitionen dækker i dag alt lige fra simple reklameprogrammer og cookies til dialers, keyloggers og rootkits.

2.1 Definition

Hvis man søger på nettet efter definitionen på hvad spyware er, finder man ud af at der er ca. lige sa mange definitioner som der er mennesker i verden. Ved en simpel Google på ”define:Spyware“ får man dog nogle af de mest dækkende. Jeg personlig, synes dog at Microsofts definition er mest dækkende.

> Spyware is a general term used for software that performs certain behaviors such as advertising, collecting personal information, or changing the configuration of your computer, generally without appropriately obtaining your consent.[1]

2.2 Virkemåde

Den type software som vi, via vores definition, beskæftiger os med i dette skrift, har alle nogle fælles karektaristika.

- Spyware virker generalt ikke som virus. Forstået på den måde, at de normalt ikke replikerer sig selv og bruger værtscomputeren til at distribuere sig selv videre.[2] Dog er der i flere tilfælde tale om at spyware bruger sikekrhedshuller i den allerede installerede software på værtscomputeren, til at trænge ind.
- Spyware trænger normalt ind i et system via en af følgende to metoder:
  - spyware kan udnytte, at eksisterende software har sikkerheds huller, som gør det muligt at installere spyware på en værtscomputer, uden at ejeren har kendskab til dette.
  - spyware kommer i forbindelse med gratis-programmer, som distribueres gratis via internettet. Spyware bliver installeret sammen med et program, som måske har anvendelse, som f.eks. et p2p fildelingsprogram eller en screensaver. Denne installation sker oftest med brugerens samtykke, da brugeren accepterer EULA.
- Som oftest vil tilstædeværelse af spyware skabe en del ekstra CPU aktivitet, disk forbrug og netværks trafik.
- Spyware lever sjælendt alene. I gennemsnit har en inficeret computer 27 forskelligt stykker spyware installeret pr 2005.[3] En undersøgelse fra 2004[4] angiver dog at der igennesnit er 93 stykker spyware på computere. Jeg vil dog udngå at kommentere på, om dette er en tendens eller ej.
- Desværre eller heldigvis, er problemerne med spyware pt. kun et Windows problem og især et Internet Explorer problem. Dette skyldes i høj grad det faktum at en Windows-bruger kører som admistrator. Det er ikke lykkes mig at finde et eksempel på spyware i Linux, men problemet vil helt sikkert migrere til Linux platformen, i takt med at flere og flere begynder at bruge Linux. Hvoraf mange af de nye brugere ikke han samme kendskab til systemet, som de superbrugere vi oftes ser i dag.

2.3 Eksempel

Jeg vil ikke gå i dybden med de enkelte stykker spyware man kan finde på nettet, men jeg vil dog nævne et par stykker, som illustration på de forskellige funktionaliteter som spyware kan have.

CoolWebSearch er en gruppe af små programmer som installerer sig selv på en computer vha. et sikkerhedshul i Internet Explorer. Programmerne laver pop-ups når man surfer på internettet, ændrer søgestrenge på søgemaskiner og ændrer host filen på computeren, DNS opslag diagerer brugeren hen til en reklameside.[8]
Internet Optimizer videresender Internet Explorer fejlsider til reklame sider. Så når man følger et *broken* link, kommer man til en side med reklame i stedet for en fejlside.[9] Dette har dog den yderlige konsekvens at man heller ikke kan logge ind på sider der bruger HTTP Basic authentication, da dette bruger de samme mekanismer som HTTP fejl.[10][1]
Aureate/Radiate er the grand old man inden for spyware, i det det var det første stykke spyware der blev opdaget. Aureate ligger i den snævreste kategori af spyware, i det den indsamler information om brugeres adfærd og transmiterer informationerne tilbage til bagmændene. Aureate er et klassisk eksempel på et stykke spyware der kommer ind i computeren med brugers accept.

> By using this software, you agree that you understand that this software will connect to the Internet UBIQUITOUSLY to download advertisement and/or to provide software updates.[11]

[1] Databasen er taget af nettet i øjeblikket.

3 Historie

Ordet *spyware* har ikke altid været brugt, som vi bruger det i dag. Første gang ordet er brugt online er slet ikke i forbindelse med ”spyware“, men i forbindelse med en humoristisk nedgøring af Microsofts business model på usenet 16. oktober 1995.[6]

Den næste reference til spyware som man støder på er i den press release som Zone Labs udsendte i forbindelse med udgivelsen ZoneAlarm 2.0 26. januar 2000. [5] Det er dog ikke nærmere specifiseret hvad spyware er og det refererer til såkaldte ”rogue applications“.

Den første kendte rapport om spyware, Aureate, sker tidligt i 2000[2]. Hvor Steve Gibson fra Gibson Research[2] finder ud af at der er blevet installeret reklamesoftware på hans computer, som han mistænker for at indsamle personlige oplysninger. Dette fører til det første stykke Anti-Spyware software, kaldet OptOut [3], som hovedsageligt fokuserer på at fjerne Aureate, nu kaldet Rediate.[7]

Siden fundet af det første stykke spyware og tilblivelsen af det første stykke anti-spyware, er udviklingen gået stærkt. Både mængden af spyware og mængden af anti-spyware er vokset eksponentielt og i 2005 var der over 300.000 websider[3] der distribuerede spyware og der er ingen grund til at dette ikke skulle fortsætte.

[2] http://www.grc.com/
[3] http://grc.com/optout.htm

4 Anti-spyware

Siden opdagelsen af de første stykke spyware, er der dukket mindst lige så mange stykke anti-spyware software op. Iblandt dem ikke kun godartede, men også software, som under påskud af at ville hjælpe brugerne med at komme af med spyware, installerer spyware. Men som med alt andet, så er et stykke anti-spyware software ikke nok.

4.1 God praksis på nettet[12]

Som med al anden sikkerhed, er det den sunde fornuft der er første led i forsvaret. Ved at følge følgende råd, er man allerede et godt stykke på vej, til at udgå spyware.

- FØRST skift browser. Selv om spyware er et problem i alle brovsere, så er Internet Explorer det absolut mest udsatte.
- Brug anti-spyware software reglmæssigt. Scan jævnligt og husk at holde softwaren opdateret.
- Hold software opdateret. Sikekrhedshuller i specielt browsere, er en yndet vej ind for spyware.
- Download kun fra velrenommerede sider og sider du har stor tillid til.
- Download aldrig eksekverbare filer, med mindre du er 110% sikker på hvad det er. Download ALDRIG eksekverbare filer fra p2p tjenester, du ved ikke hvor de kommer fra, uanset hvad du ser, hører og læser.
- Pas på cookies. Selv om de ikke er den farligste form for spyware, kan de i kombination med andet spyware, være med at at danne en detaljeret profil af dig og dine vaner, som kan udnyttes til at genere dig med pop-up vinduer og meget andet.
- Brug ikke emails i HTML format, men plain tekst. HTML i emails kan det samme som HTML på en hjemmeside. Dette er en generel fejl hos mange, da man beskytter sin browser, men ikke sin emailklient.

- Læs EULA. En stor del af den spyware der findes kommer bundlet sammen med andet software. Tilstædeværelsen af spyware kan oftest opdages ved at læse licensbetingelserne.
- Undgå drive-by download. En stor del af spyware problemet kan tilskrives forkerte sikkerhedsindstillinger i brovseren. Vælg et højt sikkerhedsniveau og lad vær med at downloade ActivX-componenter, som du ikke ved hvad skal bruges til eller ikke har tiltro til. Heller safe than sorry. Informationerne på nette bliver ikke dårligere af at animationen med bilen i toppe ikke kan ses.

4.2 Anti-spyware software

Listen med anti-spyware software er lang og uigennemskuelig. Nedenfor er en liste med et lille udvalg af nogle af de produkter, som findes på markedet:

- Spy Sweeper
- Ad-Aware
- Windows Defender
- Spyware Eliminator
- Spy Deleter
- Counter Spy

Ovenstående liste er kun et meget lille udpluk af det der findes. Men en på listen, Spy Deleter, er slet ikke et rigtigt stykke anti-spyware software. Som med alt andet, er der også folk som fremstiller software, som udgiver sig for at være anti-spyware, men som i virkeligheden installerer spyware som computaren.[13] En liste med de 10 mest farlige stykker “anti-spyware” kan findes på http://blogs.zdnet.com/Spyware/?p=727.

4.2.1 Ad-Aware

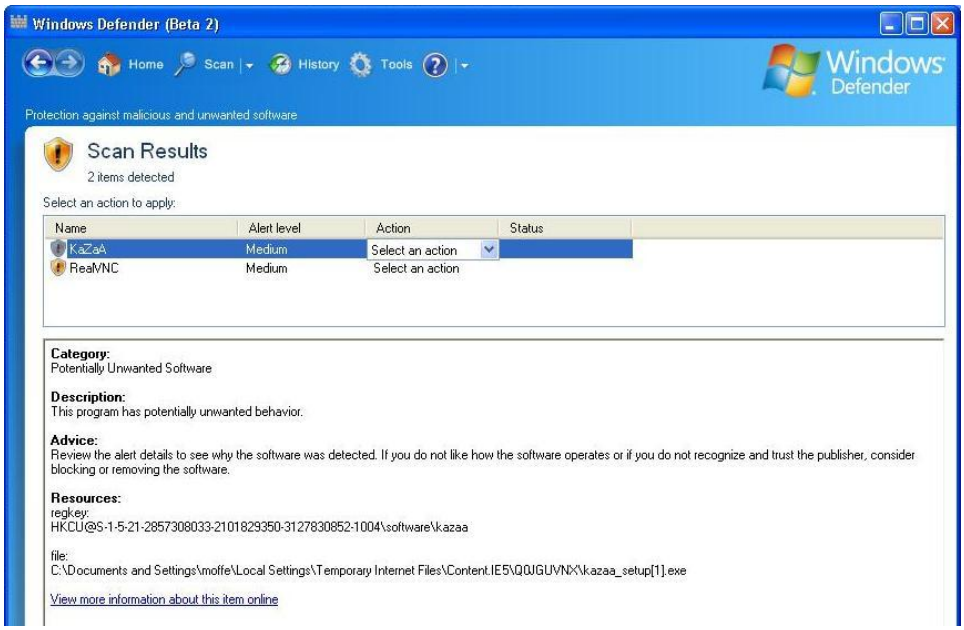
En af de mest populære anti-spyware løsninger på nettet pt., er Ad-Aware. Ad-Aware tilbyder private brugere gratis scanning af deres computer, for både kendte og ukendte spyware. Ad-Aware bruger en såkaldt Code Sequence Identification, CSI. Men hvad det dækker over, melder deres hjemmeside intet om, så man kan kun gætte på hvad der ligger bag denne teknologi.[14] Ud over en gratis version, tilbyder Lavasoft, firmaet bag, også betalings versioner til både private og firmaer, som ud over scannings-muligheden også tilbyder en real time beskyttelse. Ad-Aware understøtter alle Windows versioner fra Windows 98 op til og med Windows XP 64-bit.

4.2.2 Windows Defender

Som på så mange andre områder er Microsoft også kommet ind på markedet for anti-spyware. Da Microsofts produkter ofte bliver defacto standarder til Windows styresystemet, er deres nye anti-spyware værd at kigge nærmere på, selv om den stadig er i en beta fase.
Microsoft anti-spyware løsning udkom først gang i starten af 2005 under navnet Microsoft AntiSpyware Beta 1. Men under hjælmen gemte der sig GIANT AntiSpyware, som Microsoft havde købt i december 2004. AntiSpyware Beta 1 var implementeret i Visual Basic og kørte som en process. Dette medførte at man ikke havde beskyttelse når man ikke lige var logget på sin computer. Dette rettede Microsoft i næste release af deres løsning, denne gang under navnet Windows Defender Beta 2. Denne gang reimplementeret i C++ og kørende som en service, så alle brugere af den samme computer er beskyttet.[15]

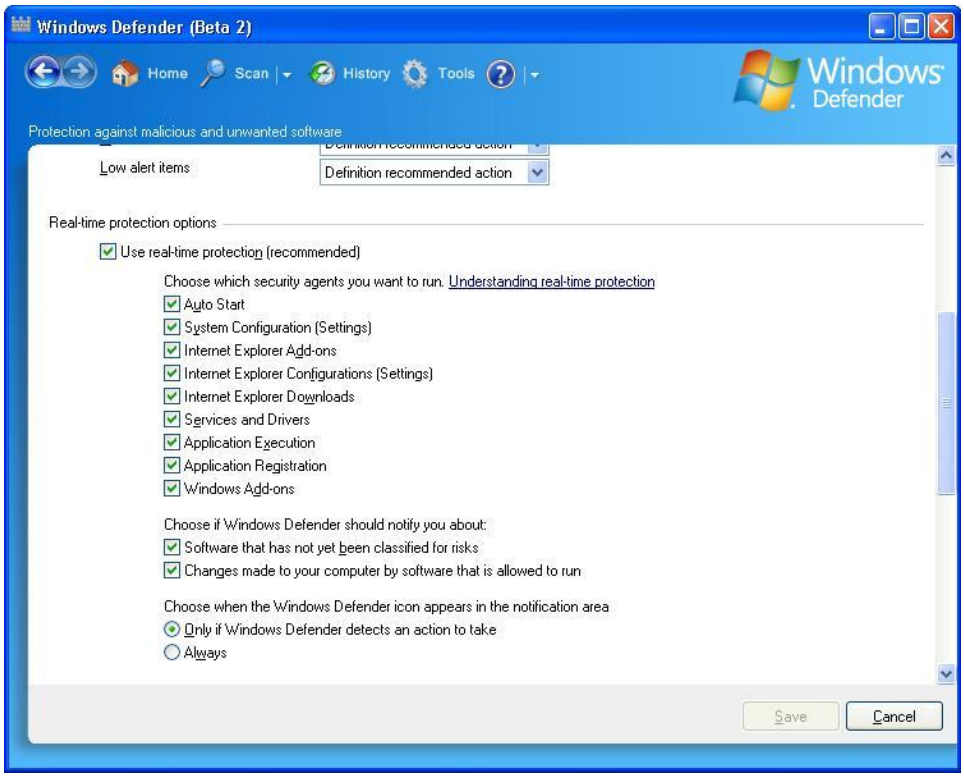
Windows Defender indeholder som alle andre anti-spyware løsninger en mulighed for at scanne en computer for spyware, men også real time beskyttelse, når man er på nettet. Desuden indeholder Windows Defender et SpyNet community.

Scanningen med Windows Defender går smertefrit omend noget langsomt i forhold til andre anti-spyware løsninger. Scanningen er dog så effektiv som man kan forvente af et anti-spyware produkt som kun er i beta.



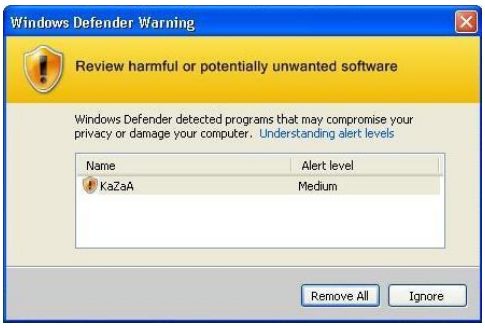
Figur 1: Scan resultat fra Windows Defender

Real time beskyttelse er en stor del af Windows Defender og man har mulighed for at vælge 9 forskellige ting der skal beskyttes, dog mangler der en nogle options, så man har mulighed for at konfigurer processen lidt mere.



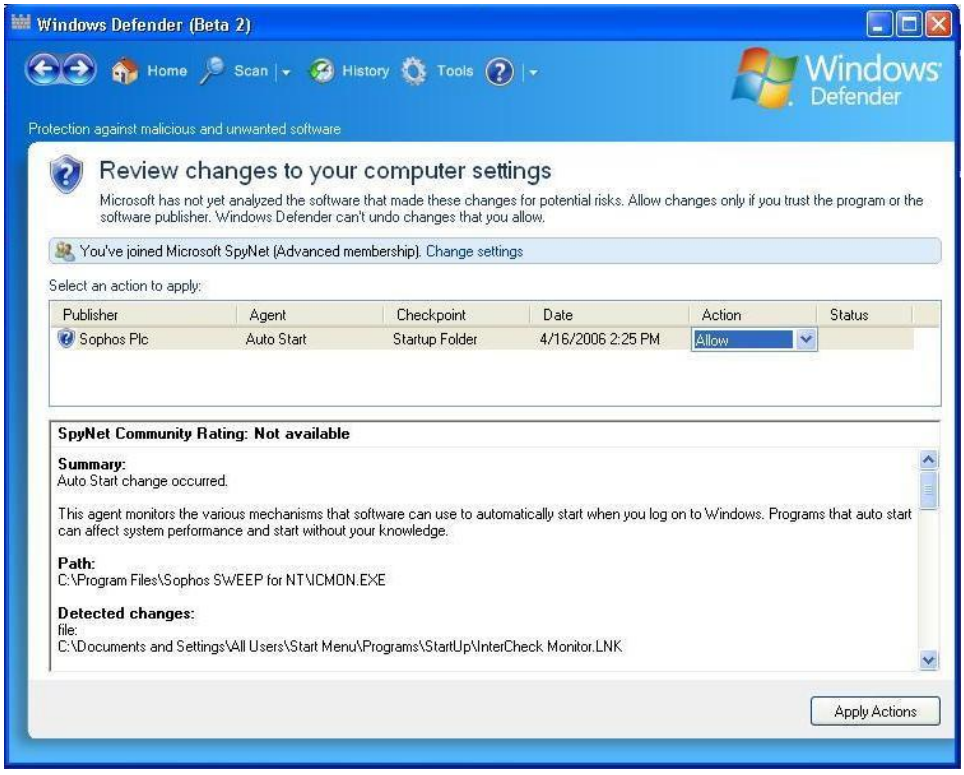
Figur 2: Real-time beskyttelse options i Windows Defender

Når real time beskyttelse er slået til, beskytter Windows Defender bl.a. mod ændringer af systemet, her under installation af ActivX componenter og ændringer i browserens konfiguration.[16] Hvis ændringer sker eller man prøver at downloade noget som er klassificeret som spyware vil Windows Defender spørge om ændringer er okay.



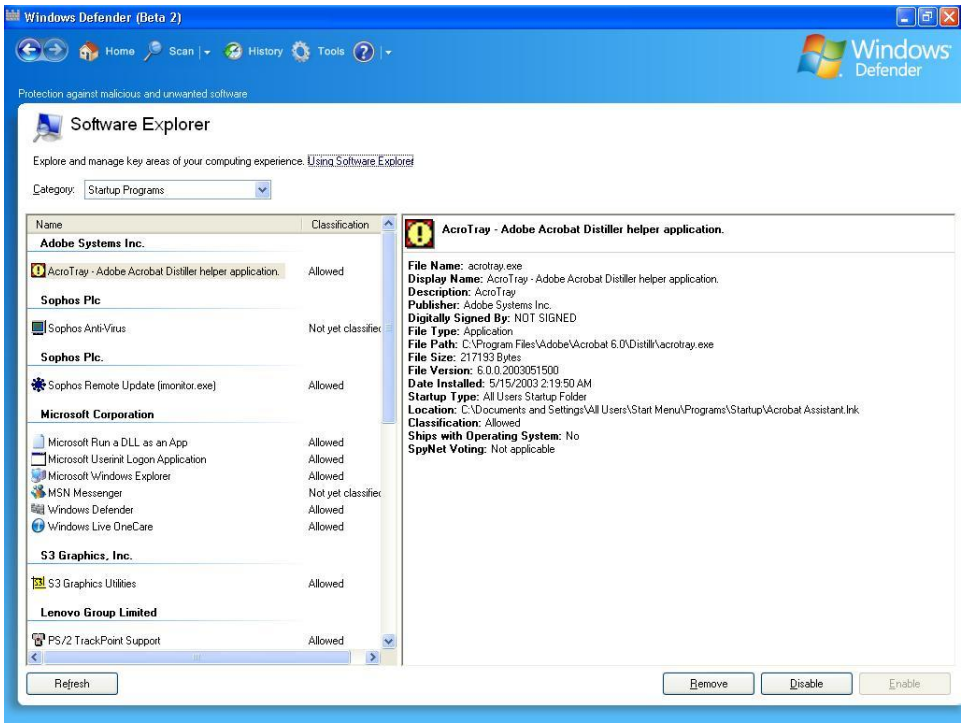
Figur 3: Pop-up i Windows Defender

Windows Defender indeholder, som tidligere nævnt et SpyNet community. Dette går ud på at når Windows Defender fanger en ny proces, som den ikke kender til, så vil den bede brugeren om at tage stillige til om processen har lov til at køre og om den skal betegnes som spyware. Denne stemme sendes til SpyNet, som samler alle stemmer fra alle brugere. Disse stemmer bruges af Windowes Defender til at foretage valg, når den støder på processer som den ikke kende. Dette ingår både i real-time beskyttelsen og ved scanning. Windows Defender bruger stemmerne i forbindelse heuristikker når den køre.[16] Hvad disse heuristikker præcist gør melder historien dog intet om.



Figur 4: SpyNet stemme i Windows Defender

Som en sidste ting vil jeg lige nævne Software Explorer, som er en anden feature i Windows Defender. Software Explorer er i bund og grund en udvidet Task Maneger. Dette synes jeg personligt er rart, da det ofte er umuligt at finde rundt i hvad alle de processer der kører på en computer egentlig laver.



Figur 5: Software Explorer i Windows Defender

5 Afrunding

Om Windows Defender og Ad-Aware er gode produkter, vil jeg lade være op den som bruger dem. For som med så meget andet software, så er det ofte et spørgsmål smag. Min opfattelse er at de to produkter generalt opfylder det som man kan forvente af anti-spyware software, dog kan ingen af de to fjerne alt spyware. Men dette var forventeligt, da spyware programmører lige som virus programmører, næsten altid er et skridt eller to foran.

En ting er dog sikker. Spyware vil ikke forsvinde lige forløbig og vil højestsandsynligvis blive en endnu større irritation for brugere af computare koblet til internettet.

Litteratur

[1] http://www.microsoft.com/athome/security/spyware/spywarewhat.mspx

[2] http://en.wikipedia.org/wiki/Spyware

[3] https://www.cert.dk/nyheder/nyheder.shtml?05-08-23-11-57-11

[4] http://www.staysafeonline.info/pdf/safety_study_v04.pdf

[5] http://www.zonelabs.com/store/content/company/aboutUs/pressroom/pressReleases/2000/za2.jsp

[6] http://news.com.com/2010-1032-5307831.html

[7] http://grc.com/faq-optout.htm

[8] http://en.wikipedia.org/wiki/CoolWebSearch

[9] http://en.wikipedia.org/wiki/Internet_Optimizer

[10] http://www.doxdesk.com/parasite/database.html

[11] http://accs-net.com/smallfish/radiate.htm

[12] http://www.pcmag.com/article2/0,4149,1522568,00.asp

[13] http://www.spywarewarrior.com/rogue_anti-spyware.htm

[14] http://www.lavasoft.com/software/adaware/

[15] http://www.winsupersite.com/reviews/windefender_beta2.asp

[16] http://www.winsupersite.com/reviews/ms_antispyware_preview.asp