



peer2peer

hur dyrt är gratis?



Filosofie kandidatuppsats inom Datavetenskap
Blekinge Tekniska Högskola, VT02

Författare: Björn Folbert
Magnus Persson
Henrik Svensson

Handledare: Bengt Carlsson

Ronneby, maj 2002

Sammanfattning

Detta arbete behandlar de tillägsprogram som, på senaste tid, börjat spridas med bland annat peer2peerverktyg. Dessa tillägsprogram, som brukar benämnas spyware alternativt adware, misstänks för att samla in personlig information, så som e-mailadresser och lösenord. Det föreligger en risk att informationen sedan säljs vidare eller används för att exempelvis rikta reklam.

Vi utförde tre olika tester, samt efterforskningar på Internet, för att svara på vad tillägsprogrammen gör, om och i så fall hur de kan stoppas, samt hur de påverkar de system de har installerats på. I vart och ett av testerna genomförde vi mätningar, bland annat av trafiken till och från våra datorer, resursanvändningen i smittade system samt förekomsten av riktad reklam. Efter varje test analyserade vi resultaten.

Dessa resultat visade på att information verkligen samlas in och används för att sprida reklam baserat på användarens surfvanor. Det har också visat sig att vissa tillägsprogram utnyttjar stora delar av systemresurserna.

Undersökningen ledde oss bland annat fram till slutsatsen att användare, som är måna om sin integritet, bör tänka på vad man installerar och försöka skydda sig. I testerna tar vi upp möjliga sätt att göra det sistnämnda.

Abstract

Most peer2peer-tools of today are shipped with some kind of third party software (add-on software), often referred to as spyware or adware. These pieces of software are accused of collecting personal information, like email-addresses and passwords. There is a risk that this information is later sold on or used in direct marketing.

We conducted three different tests and searched the Internet to find out what the add-on software do, if and how they can be stopped and what their impact on a system is. For each test, a number of different variables, net traffic and system resource usage among others, were measured and analyzed.

These tests made it clear that information really is collected and used for direct marketing based on the users Internet surf-habits. Besides that, some add-on software uses a lot of system resources.

The tests leads us to the conclusion that, as a user of peer2peer-software, one should pay close attention to what is installed and take measures to protect personal information. The tests give examples of ways to protect a system from add-on software.

Förord

Vi vill tacka vår handledare Bengt Carlsson, som har varit till stor hjälp under arbetets gång.

Omslagsbilden är delvis upphovsrättsskyddad av E.C. Publications (MAD).

Ronneby, Maj 2002

Björn Folbert, bjorn@folbert.com

Magnus Persson, magnus@student.nu

Henrik Svensson, svensson@ny.com

Innehållsförteckning

SAMMANFATTNING	2
ABSTRACT	1
FÖRORD	1
INNEHÅLLSFÖRTECKNING	1
1 INTRODUKTION TILL PROBLEMOMRÅDET	1
1.1 INLEDNING	1
1.2 VARFÖR BÖR ÄMNET UNDERSÖKAS	2
2 NÄRMARE BESKRIVNING AV PROBLEMOMRÅDET	3
2.1 PEER2PEER	3
2.2 TILLÄGGSPROGRAM	3
2.3 BRANDVÄGG	4
2.4 ANTISPYWARE	5
3 LITTERATURGENOMGÅNG	6
4 METODBESKRIVNING	8
4.1 TESTMILJÖ	FEL! BOKMÄRKET ÄR INTE DEFINIERAT.
4.1.1 Mjuk- och hårdvara	8
4.1.2 Testprogram	8
4.1.3 Motivering till val av testprogram	10
4.2 TEST ETT	11
4.2.1 Testplan	11
4.2.2 Resultatbeskrivning	11
4.2.3 Resultatanalys	12
4.3 TEST TVÅ	13
4.3.1 Testplan	13
4.3.2 Resultatbeskrivning	13
4.3.3 Resultatanalys	14
4.4 TEST TRE	15
4.4.1 Testplan	15
4.4.2 Resultatbeskrivning	16
4.4.3 Resultatanalys	19
5 DISKUSSION	22
5.1 IRRITATIONSMOMENT	22
5.2 KAPPRUSTNINGEN	22
5.3 POTENTIELL SÄKERHETSRIK	23
5.4 FRAMTIDEN FÖR PEER2PEER OCH TILLÄGGSPROGRAMMEN	24
6 SLUTSATS	26
7 REFERENSLISTA	27
BILAGOR	

1 Introduktion till problemområdet

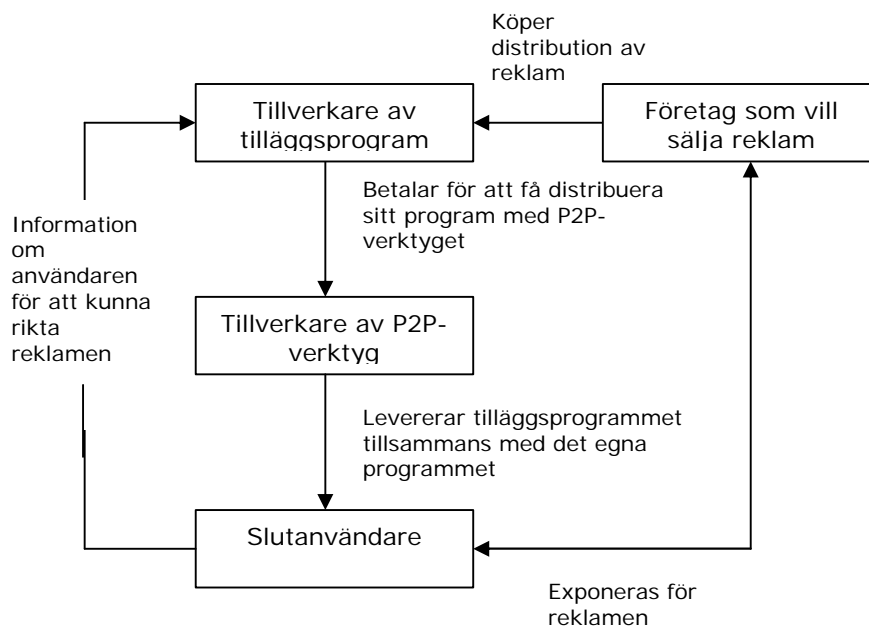
1.1 Inledning

Om vi skall vara helt ärliga så var det lite av en slump att vi kom in på vårt ämne lägligt till att vi skulle skriva kandidatarbetet i datavetenskap. Från början viste vi inte riktigt vad vi skulle inrikta oss på. Det kändes allmänt förvirrat, eftersom vi var tvungna att skriva ett utredande arbete. Vi var mer inställda på att arbeta i projektform för ett företag och på uppdrag av dem utveckla eller vara med och skapa datasystem. Då detta inte gick fick vi tänka om.

Efter mycket tankeverksamhet och lite ämnestips på kursens hemsida, blev vi intresserade av peer2peersystem. Vi var indirekt redan bra insatta i peer2peersystem genom vår flitiga användning av fildelningsprogrammen Napster¹, Morpheus², Kazaa³ och Audiogalaxy⁴, som alla representerar peer2peer.

I vår sökning efter möjliga infallsvinklar till peer2peer, fick vi upp ögonen för en annan del av området, nämligen de program som följer med de olika peer2peerprogrammen. Peer2peerprogrammen utnyttjas som värdprogram av dessa "extraprogram", som vi i fortsättningen kommer att referera till som tilläggsprogram. De mest intressanta varianterna av dessa är spyware, adware samt foistware.

Att företag använder sig av denna typ av tilläggsprogram för att få tag i uppgifter om användare, i syfte att kunna rikta reklam (fig. 1), verkade intressant och samtidigt skrämmande.



Figur 1: Schematisk bild över informationsflödet

¹ <http://www.napster.com>

² <http://www.morpheus-os.com/>

³ <http://www.kazaa.com>

⁴ <http://www.audiogalaxy.com>

Tittar vi på utvecklingen i peer2peervärlden de senaste månaderna (februari - maj 2002), kunde vi inte valt ett bättre tillfälle att undersöka ämnet. Vi tänker främst på Audiogalaxy, Kazaa och Morpheus, vilka alla nyligen avslöjats för att innehålla olika former av mer eller mindre suspekta tilläggsprogram, där ett av de mest omtalade hittills, Brilliant Digital¹, distribuerats med Kazaa.²

Precis som med en stor del av den nya tekniken är namnen helt på engelska alternativt försvenskade. I vissa fall ställer detta till problem då man vill använda de engelska namnen och ska skriva i exempelvis bestämd form pluralis. Spyware blir t.ex. "spywaret". Vi har därför valt att skriva "spywareprogrammet" alternativt "spywareapplikationen" trots att ordet ware kan översättas till program eller vara. I obestämd form använder vi dock ordet spyware. Värt att nämna är även att peer2peer, i vissa källor, hänvisas till som peer-to-peer, peer-2-peer eller P2P.

1.2 Varför bör ämnet undersökas

Om någon kan övervaka vilka sidor vi besöker på Internet, var vi klickar, komma åt personuppgifter vi lämnar i formulär, lösenord till e-mailkonton och andra inloggningsfunktioner, samt komma åt filer på våra datorer, känner vi användare oss plötsligt inte lika säkra i den digitala världen. Detta är idag, med hjälp av spyware, fullt möjligt att göra utan vår vetskap. Ha dessutom i åtanke att den insamlade informationen kan säljas vidare till diverse intressenter.

Det är förmodligen inte många användare som vet att ovanstående är vanligt förekommande idag. Detta antar vi eftersom vi anser oss själva vara vana datoranvändare och vi var inte medvetna om att detta föregick tills för ett par månader sedan. Saknas kännedom om att tilläggsprogram finns, samt kunskap om hur dessa fungerar, är det väldigt svårt att veta hur man skyddar sig.

Vi vill uppmärksamma vilka typer av tilläggsprogram som sprids med några av dagens populäraste peer2peerverktyg. Med hjälp av våra försök vill vi ta reda på vad dessa tilläggsprogram gör, om de går att stoppa samt hur de, tillsammans med sina värdprogram, påverkar de system de har installerats på.

¹ <http://www.brilliantdigital.com/>

² <http://nyheter.idg.se/display.asp?id=020402-pfa1>, 2002-05-17, 17:50

2 Närmare beskrivning av problemområdet

2.1 Peer2peer

Generellt definieras peer2peer som en kommunikationsmodell i vilken varje användare har samma möjligheter till kommunikation, det vill säga vem som helst av användarna kan starta en kommunikationssession med någon annan. I Internetsammanhang definieras peer2peer som en typ av obestående nätverk som låter en grupp av användare med samma nätverksprogram att koppla upp sig mot varandra och få direkt tillgång till filer på varandras hårddiskar.¹

Tekniken har främst fått genomslag via fildelningssystem som de redan tidigare nämnda Napster och Kazaa. I ett antal år nu, så har debatten rasat om dessa programs existensberättigande. Främst i motståndarledet står film- och musikbranschen, som vill förhindra att deras upphovsrättsskyddade material sprids gratis. Peer2peer är dock inte endast användbart för att sprida olagligt material. Företag har börjat titta på fördelarna med att använda peer2peer som ett sätt för de anställda att dela filer utan att behöva en centraliserad server.²

2.2 Tilläggsprogram

I det här arbetet kommer vi att diskutera spyware och adware som centrala begrepp, men vi kommer även att nämna foistware. Vad räknas som spyware, vad räknas som adware? Nedan förklarar vi begreppen, vad som är representativt för dem samt vad som skiljer dem åt.

Vi har valt att gruppera samtliga typer av tilläggsprogram under samlingsnamnet tilläggsprogram. Detta namn är ett centralt begrepp i vårt arbete, och vi vill således redogöra för vad vi räknar in under detta. Tilläggsprogrammen klassificeras utifrån vad de har för uppgift och definitionerna varierar från källa till källa. Vi har dock valt att utgå från definitionerna nedan.

Spyware: Generellt sett är spyware en teknologi som går ut på att samla information om en person eller organisation utan dennes kännedom. I Internetsammanhang definieras spyware som ett program som placeras i en dator för att i hemlighet samla information om användaren och sedan skicka den vidare "hem" (till intressent).³ Vi vill betona att arbetet inte handlar om den typ av spyware som räknas som övervakningsprogram av den egna datorn, exempelvis loggning av tangentbords-händelser.

För det mesta hittar man spyware inbäddade i diverse freewareapplikationer, det vill säga program som går att hämta hem gratis från Internet. För att finansiera freewareprogram och just kunna hålla dem gratis, går utvecklarna med på att bädda in spyware i deras originalprogram mot en viss summa pengar. Vissa freewareutvecklare väljer att skriva en liten, nästan osynlig, rad i det vanligtvis meterlånga licensavtalet där man redogör för att andra program medföljer, andra väljer att inte nämna det alls. Frågan är vad som är värst, att försöka få användarna att gå med på att låta spyware härja fritt på deras datorer genom att acceptera licensavtalet eller att försöka dölja kopplingar till dessa befintliga spyware.

När en användare installerar freewareprogrammet, installeras även spywareprogrammet i bakgrunden, oftast utan att användaren upptäcker det. Detta program är sedan aktivt

¹ http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci212769,00.html, 2002-05-19, 14:06

² http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci212769,00.html, 2002-05-19, 14:23

³ <http://whatis.techtarget.com/definitionsSearchResults/1,289878,sid9,00.html?query=spyware>, 2002-05-11, 17:52

vare sig värdprogrammet körs eller inte. Informationen som samlas kan vara allt från vilka sidor användaren besöker och vilka länkar denna klickar på, till lösenord och känsliga personuppgifter. Med jämna mellanrum kopplar sedan spywareprogrammet upp sig mot en server någonstans i världen och skickar "hem" den insamlade informationen.

Datainsamlingsprogram som installeras med användarens kännedom räknas inte definitionsmässigt som spyware, så länge användarna är införstådda med vilken data som samlas och till vem den skickas.¹ Värt att notera här än en gång är att vi inte kunde se exakt vad som samlas och skickas av spywareprogrammen. Detta bidrar till att vi i vårt arbete inte skiljer på dessa detaljer utan även rankar dessa program som spyware.

Alla spyware används emellertid inte till att samla känsliga personuppgifter. En del används "bara" till att övervaka en användares intressen för att sedan kunna rikta rätt typ av reklam. Det är dock nästan omöjligt att avgöra vilka spyware som gör vad eftersom det inte går att se exakt vad tilläggsprogrammen skickar.

Adware: Adware är applikationer som genererar reklam, i form av popups.² Popups är en instans av webbläsaren som, utan att användaren gör något, öppnas upp. Ofta innehåller popupfönstret reklam eller annan information. En annan variant är de så kallade popunderfönstren, som lägger sig under alla aktiva programfönster. Vi har i arbetet valt att referera till båda varianterna som popups.

Adware återfinns, liksom spyware, oftast inbäddade i freewareprogram. Även här handlar det också om att finansiera utvecklingskostnader. Den påstådda skillnaden gentemot spyware ligger i att adware "endast" samlar information om var användaren klickar och vilka sidor denna besöker på Internet. Syftet är att kunna rikta reklam. Det går dock inte att utesluta att adwareprogrammen är begränsade till denna informationssamling, eftersom det är svårt att identifiera all data som programmen samlar in. Detta bidrar till att det bara är en tunn linje mellan vad som är spyware och vad som är adware.

Foistware: Med foistware menas applikationer som i hemlighet lägger till och gömmer komponenter i ett system.³ Detta är ett relativt nytt begrepp som innefattar spyware som mer eller mindre uppför sig som virus. Dessa spywareprogram kan generera nya filer och ändra i befintliga filer hos användarna. Foistware kan från början vare en liten fil på datorn, men allt eftersom tiden går genererar den nya filer och snart har det installerats ett helt nytt program på datorn utan att användaren har märkt någonting.

2.3 Brandvägg

Brandväggen kan ses som en länk mellan datorn och ett nätverk, till exempel Internet, och bevakar och skyddar datorn mot angrepp utifrån. Med brandväggen kan man förutom stoppa trafik till datorn också blockera trafik ut från datorn, vilket vi använde oss av i våra försök. Brandväggen vi har använt är ZoneLabs ZoneAlarm Pro⁴ som är en mjukvarubrandvägg. Skillnaden på en sådan och en hårdvarubrandvägg är att mjukvaruvarianten skyddar en enskild dator via mjukvara och inte som en hårdvarukomponent som i regel skyddar ett lokalt nätverk. Mjukvarubrandväggar är i regel mindre säkra än hårdvarubrandväggar, men erbjuder tillräcklig funktionalitet för våra tester.

¹ <http://whatis.techtarget.com/definitionsSearchResults/1,289878,sid9,00.html?query=spyware>, 2002-05-11, 17:52

² <http://whatis.techtarget.com/definitionsSearchResults/1,289878,sid9,00.html?query=adware>, 2002-05-11, 17:52

³ <http://e-magazineonline.com/QUI/QUI013903.htm>, 2002-05-11, 20:31

⁴ <http://www.zonelabs.com/>

2.4 Antispyware

I takt med att medvetenheten om tilläggsprogram har börjat öka, främst genom Internet, har både privatpersoner och företag också sökt vägar att skydda sig och sin information. Antispyware fungerar genom att antingen ta bort oönskade komponenter eller blockera dem från att komma åt Internet. Genom att ta bort dessa oönskade komponenter upphör visserligen tilläggsprogrammen att existera, men i vissa fall upphör även värdprogrammen att fungera. Namnet till trots letar dessa program i de flesta fall även efter adware och andra tilläggsprogram.

I våra tester använde vi Ad-aware¹, ett antispyware som, genom att genomsöka datorns hårddiskar, minne och register, ger användaren en lista på komponenter från kända tilläggsprogram. Användaren kan sedan välja att ta bort dessa komponenter från systemet. För att hålla programmet uppdaterat kan användaren, med hjälp av ett litet extraprogram, enkelt ladda hem uppdaterade referensfiler från tillverkarens hemsida. Ad-aware finns både i en gratisversion och i en mer avancerad version som kostar en mindre summa pengar. Vi använde oss av gratisversionen då denna finns tillgänglig för alla och funktionaliteten var tillräcklig för våra tester.

¹ <http://www.lavasoft.nu>

3 Litteraturgenomgång

Eftersom området, vid tidpunkten för undersökningen, var relativt outforskat, var det svårt att hitta publicerad litteratur. De källor vi har använt är därför uteslutande verk publicerade på Internet samt webbsidor. Vi är medvetna om att material på Internet är mindre trovärdigt än publicerat material, detta borde dock inte påverka trovärdigheten på arbetet eftersom det, till största del, bygger på våra egna tester.

En stor del av informationen om tilläggsprogram återfinns dessutom på sidor av mer eller mindre suspekt natur. Vi anser att denna information är subjektiv, då det i de flesta fall endast är de negativa aspekterna som tas upp. Detta gäller även för mer respekterade sidor som [idg.se](http://www.idg.se)¹ och [cnn.com](http://www.cnn.com)².

Nedan följer en kort redogörelse för de sidor som vi har använt som informationskällor men inte beskrivit närmare i den löpande texten. Informationen kommer från respektive sida.

Idg.se tillhandahålls av International Datagroup, världens största utgivare av IT-relaterad information. Företaget publicerar bland annat tidningar som *Internetworld*, *PC För Alla* samt *Mikrodatorn*. Sidan, där dagsfräsch information publiceras, används som ett komplement till det tryckta materialet.

techtarget.com; denna domän innehåller subdomänerna *searchnetworking* och *whatis*. Den sistnämnda återfinns även under *whatis.com*, vilken vi har använt oss av för förklaringar av diverse begrepp. *Whatis.com* är en söktjänst för ord inom området informationsteknologi. Tjänsten startades 1996.

e-magazineonline.com är en elektronisk version av den filippinska tidningen *e*. Tidningens inriktning är mot teknologi.

Cnn.com fungerar som ett komplement till tv-kanalen Cable News Network (CNN). Företaget är en av världsledarna inom nyhetsförmedling.

Download.com tillhandahåller en stor mängd program för nedladdning. Vidare erbjuds användaren nyheter, information och statistik om programmen.

Newsbytes.com, som ägs av The Washington Post Company, fokuserar helt på nyheter inom informationsteknologivärlden. Sidan är den äldsta källan för fortlöpande nyheter inom området.

slashdot.org, som ägs av Open Source Development Network (OSDN), tillhandahåller nyheter för it-intresserade, eller som de själva uttrycker det "News for Nerds. Stuff that matters". Sidan startades 1997.

news.zdnet.co.uk och *news.com.com* har samma ägare och båda erbjuder teknikrelaterade uppgifter.

*aftonbladet.se*³, papperstidningens nätbilaga. Sidan är Sveriges mest besökta nyhetsportal.

¹ <http://www.idg.se>

² <http://www.cnn.com>

³ <http://www.aftonbladet.se>

Följande sidor kan anses vara subjektiva, men de har ändå bidragit med material till vårt arbete.

cexx.org är en privat sida där vi inte kunde hitta någon information om sidans syfte eller personerna bakom. Namnet står för Counter Exploitation (motexploatering) och sidan innehåller information om olika typer av tilläggsprogram, vilka program de sprids med samt vad de gör.

accs-net.com/smallfish/ drivs i privat regi. Ägaren samlar information från andra webbsidor och från inlägg i forum och nyhetsgrupper som behandlar säkerhet och integritet på Internet.

infoanarchy.org drivs av Erik Möller, redaktör på den tyska tidningen Der Humanist och frilansjournalist. Sidan bevakar nyheter om fildelningsprogram och därtill relaterade områden. Bland annat kan besökarna kommentera artiklar, vilket ofta leder till hetsiga och intressanta diskussioner.

oit.duke.edu/ats är en informationssida för studenter och lärare vid Duke University i Amerika.

För att utforma arbetet har vi använt oss av Patel & Davidson (1991).

4 Testmiljö

4.1 Mjuk- och hårdvara

Då vi inte hade tillgång till en ordentlig testmiljö med datorer specifikt dedikerade till våra försök fick vi använda våra egna maskiner. De tre datorerna som användes, en för varje författare, befann sig på samma nätverk, Ronneby StudentNätverk (RSN).

Vad det gällde hårdvara skiljde sig konfigurationen väsentligt åt då åldrarna på datorerna sträckte sig från 3½ år till ½ år. Då detta inte borde påverka tilläggsprogrammets möjligheter att infiltrera systemen ansåg vi inte detta vara ett problem.

Alla tre datorer kördes under engelsk Microsoft Windows XP Professional. Inför testet kördes Windows Update på samtliga testmaskiner för att ytterligare försäkra oss om att ge tilläggsprogrammen likvärdiga möjligheter. Windows Update kopplar upp mot Microsoft, hämtar och uppdaterar Microsoft Windows XP. De tre datorerna hade varit i drift ett tag före testerna inleddes och följaktligen fanns olika mjukvara installerad på de olika datorerna, inför test ett och två ansåg vi dock inte att detta skulle kunna påverka utfallet. Vi tyckte att det viktigaste var att operativsystemen och därmed den grundläggande miljön var likvärdig. Till test tre ville vi dock ha än mer likvärdiga testmiljöer, vilket ledde till att de tre datorerna formaterades.

4.2 Testprogram

För samtliga tre tester, vilka beskrivs närmare under de följande rubrikerna, användes tre program; Kazaa Media Desktop, BearShare och Audiogalaxy. Till test ett och två användes dessutom ett fjärde program, Yo Mama Osama.

För att visa på vilken stor spridning dessa program, och därmed även de program som användaren "får på köpet", har redogör vi för hur många nedladdningar dessa program genererat.

I beskrivningen av respektive program har vi tagit med antal nedladdningar för varje program. Dessa siffror gäller endast nedladdningar från download.com och bör dessutom endast ses som ett ungefärligt mått på spridningen då de kan påverkas av yttre omständigheter vilka vi tar upp i diskussionen.

4.2.1 Kazaa Media Desktop 1.5

Version för test ett: 1.5

Version för test två: 1.5

Version för test tre: 1.5

Antal nedladdningar: 58,444,735¹

Kazaa Media Desktop är en andra generationens peer2peer fildelningsservice med vilken man kan leta efter och ladda ner media filer från andra användare av Kazaa. Användaren kan även organisera och spela upp/se sina mediafiler genom en integrerad mediajukebox, publicera sina egna alster, nå en publik och kommunicera med andra Kazaa användare. Kazaa stöder ljud, video, mjukvara, spel, bilder och dokument.²

Installationen av Kazaa 1.5 sker genom att användaren laddar hem en exefil som, när den körs, kopplar upp sig mot en Kazaaserver och laddar hem filer som behövs. Med

¹ <http://www.download.com>, 2002-04-02, 21:21

² <http://www.download.com>, 2002-04-02, 21:34

detta i åtanke så kan det, trots att vi alla använde oss av samma exefil, vara så att vi har tre olika varianter av Kazaa.

4.2.2 BearShare 2.5

Version för test ett: 2.4.4

Version för test två: 2.5.0.17

Version för test två: 2.5.0.17

Antal nedladdningar: 13,777,198¹

BearShare låter användaren söka efter, ladda hem och dela filer med alla på det globala informationsnätverket Gnutella. Detta program fungerar med MP3 MPEG, AVI, ASF, MOV, JPEG, GIF, och alla andra filtyper.²

4.2.3 Audiogalaxy Satellite

Version för test ett: 0.608w

Version för test två: 0.609

Version för test tre: 0.609w

Antal nedladdningar: 30 026 789³

Audiogalaxy Satellite är ett realtids, transaktionsbaserat fildelningssystem för MP3 användare. Programmet använder ett webbaserat gränssnitt som låter användaren söka efter artister, låtar och album samt ladda hem dessa till sin dator. Klientprogrammet är litet, enkelt och designat för att använda ett minimum av processorkraft och minne. Satelliten väljer automatiskt ut den närmsta användaren med den specifika filen du vill åt, vilket reducerar resursanvändandet vad gäller bandbredd. Filer som för tillfället ligger offline kan läggas på kö för att laddas hem så snart en användare med filen går online. Om en nedladdning avbryts letar satelliten upp en annan användare med samma fil och fortsätter nedladdningen.⁴

4.2.4 Yo Mama Osama

Antal nedladdningar: över 100.000 de första 12 timmarna (färska siffror saknas).⁵

Detta program, som närmare bestämt är ett spel gjort i Macromedia Flash, släpptes 2001-10-03 i efterdyningarna av attacken på World Trade Center. Spelet är gjort av Lions Pride Enterprises och publicerat på TwistedHumor.com⁶. Idén med spelet är att skjuta Osama Bin Laden i luften med hjälp av diverse vapen. Spel, bilder och filmer med liknande budskap släpptes under denna tid i mängder och cirkulerade snabbt på nätet. För att ytterligare försäkra sig om att generera många nedladdningar gavs spelaren möjlighet att donera \$1 till The American Red Cross Disaster Relief Fund. Doneringen skedde om spelaren klickade på en länk i spelet, som endast kunde startas om användaren angav sitt namn, sin e-mailadress samt minst en e-mailadress till en vän.

Från licenstexten har vi översatt de två följande styckena:

Du tillåter att Lions Pride Enterprises, Inc. kan, som de finner godtyckligt och för vilket syfte som helst, tillhandahålla uppdateringar, automatiska eller andra, till Osama-mjukvaran (vilket inkluderar, men inte begränsas, till reklamjukvaran och tekniken

¹ <http://www.download.com>, 2002-04-02, 21:19

² <http://www.download.com>, 2002-04-02, 21:39

³ <http://www.download.com>, 2002-04-02, 21:18

⁴ <http://www.download.com>, 2002-04-02, 21:43

⁵ <http://www.newsbytes.com/news/01/171646.html>, 2002-04-02, 21:56

⁶ <http://www.twistedhumor.com/games/osama/mail/>, 2002-05-21, 10:39

som beskrivs i paragraf 4 nedan (nästa stycke, vår kommentar)); genom att använda Osama-mjukvaran visar du din vilja att erhålla dessa uppdateringar.

Genom att installera, ladda ner, kopiera, uppdatera eller på något annat sätt använda Osama-mjukvaran, går du med på att inkludera nämnda mjukvara och teknologi genom vilken Lions Pride Enterprises, Inc., dess dotterbolag, filialer, partners, avdelningar och klienter tillhandahåller reklammaterial på din dator. Du erkänner att du önskar erhålla reklammaterial, om något, från Lions Pride Enterprises, Inc., dess dotterbolag, filialer, partners, avdelningar och klienter.

2002-05-20 fanns spelet fortfarande att ladda hem på TwistedHumor.com. Vi rekommenderar, givetvis, ingen att ladda hem och köra programmet.

Detta program fanns inte med i planerna från början, men då det var smittat med ett av de, vid tidpunkten, mer intressanta tillägsprogrammen föll det sig självklart att ta med det i vår undersökning. Att en av testpersonerna, under perioden för test 1, var smittade upptäcktes mer eller mindre av en slump då snifferprogrammet fångade upp trafik som såg misstänkt ut.

4.3 Motivering till val av testprogram

Den primära anledningen till att vi valde att använda oss av fildelningsprogram för våra tester, var att vi från början tänkte skriva om peer2peer. Dessutom återfinns ofta denna typ av program högt på listor över mest nedladdade program.

Till beskrivningen för de tre först listade programmen hörde dessutom följande text från folket på download.com;

Editor's note: Denna nedladdning inkluderar applikationer som följer med mjukvarans installationsfil, varav vissa kan komma från andra parter än utvecklaren av installationsfilen. Dessa applikationer kan leverera annonser, samla information, överlagra innehåll eller grafik på webbsidor som du besöker eller modifiera dina systeminställningar. Som med alla nedladdningar rekommenderar CNet (ägaren av download.com) att du är lägger stor vikt vid de val som du kan göra under installationen.¹

Efter denna notis följer exempel på program som är inbakade i installationsfilen för respektive program. Vi anser det inte motiverat att ta upp vilka tillägsprogram som nämns, då dessa kan ändras, i princip från dag till dag.

¹ <http://www.download.com>, 2002-04-02, 22:05

5 Metodbeskrivning

5.1 Test ett

Detta test inleddes 2002-02-20 och var egentligen tänkt som en förberedelse inför ett kommande test, då vi ville se om vi överhuvudtaget kunde fånga upp och hänföra trafik till installerade program och dess tillägsprogram. Efter vi hade testat lite fram och tillbaka så fick vi reda på att det var totalförbjudet att avlyssna trafiken på RSN, dit vi alla tre var uppkopplade. Vi var således tvungna att avbryta försöket, i princip redan innan det hade börjat. Vi anser ändå att vi fick fram ett så pass intressant resultat att det finns ett värde i att beskriva testet och dess utfall i denna den slutliga rapporten.

5.1.1 Testplan

Vi hade, inför detta test, kommit överens om en grov testplan där det stod var och en fritt att experimentera för att på så sätt komma fram till en väl fungerande plan inför, vad vi trodde skulle bli, det giltiga testet. Vi började med att installera ett sniffer-program. Denna typ av program används för att lyssna av trafik på ett nätverk. Det fångar upp TCP-paket och ger oss möjlighet att analysera innehållet i dessa. Exempelvis kan man få fram vem som skickar paket, vart paketen ska samt innehållet i dessa. Det sistnämnda kan dock vara svårt att tyda. Vi använde vi oss av SnifferPro version 4.50.04 från Network Associates¹.

Med hjälp av en uppdaterad version av Ad-aware säkerställde vi sedan att systemet var tömt på komponenter från tillägsprogram. Därefter installerade vi de ovan beskrivna testprogrammen och körde dessa. Under tiden som programmen körde avlyssnade vi trafiken.

Vårt att nämna är att var och en till detta första test laddade hem testprogrammen vid varierande tidpunkter, spritt över en period av två dagar. Vi verifierade, i efterhand, att det var samma versioner av programmen som var installerade, men det kan ändå ha varit så att utvecklarna lagt till och tagit bort spyware i sina installationsfiler.

5.1.2 Resultatbeskrivning

Som vi redan nämnt fick detta test avbrytas i förtid, men vi fann det lilla vi fick fram så pass intressant och relevant att vi trots allt vill ta upp det.

Efter att ha experimenterat en del med SnifferPro så kunde vi, till viss del, avläsa och analysera trafiken. På en av testdatorerna fick vi fram trafik till och från Rankyou.com². Dessutom kunde vi se att en lokal fil på denna dator, wnad.dat, var involverad på eller annat sätt. Rankyou.com sysslar med marknadsföring på Internet, exempelvis håller de i kampanjer med banners. Företaget hävdar bland annat att de var först med popunderfönster.

Vid installation av Yo Mama Osama! installeras även följande filer på datorn: wnad.exe, wnad.dat samt wnad-update.exe. Dessutom läggs en rad till i datorns register så att wnad.exe exekveras varje gång datorn startas. wnad.exe kopplar upp mot www.rankyou.com:80 och andra sajter, uppenbarligen för att skicka personlig information.³

¹ <http://www.nai.com/>

² <http://www.rankyou.com>

³ <http://www.cexx.org/osama.htm>, 2002-04-16, 16:54

Vad vi har kunnat se så uppdateras wnad.dat på regelbunden, en gång varje till varannan dag, basis. Vi har inte kunnat se att någon personlig information verkligen har skickats. Nedan följer ett exempel på hur innehållet i wnad.dat filen kan se ut.

```
1.016
4
17-Apr-2002 11:22:43
CPT_831
www%2Eleadgreed%2Ecom%2Fads%2Fcpt%2Fxbox%2Findex%2Ephp
04-May-2002 19:10:04
CPT_1133
bestlodging%2Eworldres%2Ecom%2Fscript%2Fnode%2Easp%3Ffront%5Fend%5Fid%3D9970
06-May-2002 23:06:13
CPT_1136
www%2Ethemomi%2Eorg%2Fpreboarding%2Ehtml
12-Apr-2002 08:03:07
CPT_1087
www%2Echina%2Dguide%2Ecom
37354,4050739352
intro2.php
37334,8986415509
0
1
37355,4187511574
2
5
x1440
5
37195,5
```

Bild 1: Innehållet i wnad.dat 2002-04-09, 11:32

Den gråmarkerade raden översätts till följande adress:
<http://www.leadgreed.com/ads/cpt/xbox/index.php>, då exempelvis %2E representerar en punkt. Kopierar vi in denna adress till adressfältet i en webbläsare får vi fram en sida som visar reklam för ett TV-spel. Exakt denna sida, med samma adress, har visats ett antal gånger i den maskin som var smittad med wnad. Likaså har de andra sidorna, vars adresser återfinns i wnad.dat, visats.

5.1.3 Resultatanalys

Resultaten visar att en smittad dator tog emot och även skickade information. Detta gjorde oss än mer nyfikna på vad som egentligen händer i bakgrunden på våra datorer. Tyvärr kunde vi inte tyda vad som skickades, däremot kunde vi se vad som togs emot; text som lades in i wnad.dat. På grund av problemet med att analysera trafiken, samt att vi inte fick mäta mer, insåg vi att vi var i behov att, till viss del, ändra inriktning på arbetet. Detta ledde oss fram till test två.

5.2 Test två

Syftet med detta test var att övervaka tilläggsprogram med hjälp av en brandvägg och ett antispyswareprogram. Testet skulle utföras på tre datorer samtidigt, men på grund av hårdvarufel föll en av testdatorerna bort. För att åstadkomma så lika förutsättningar som möjligt behövde vi samma tilläggsprogram på de två datorerna. Vårdprogrammen skulle dessutom installeras samtidigt. Vi behövde även samma versioner av antispysware och brandvägg. Med undersökningen ville vi dokumentera skillnader mellan datorer smittade med spyware och en dator som inte var smittad samt att se vilka komponenter som försökte få tillgång till nätet. Vi ville också se hur tilläggsprogrammen fungerar med vårdprogrammen igång respektive avstängda; är tilläggsprogrammen aktiva även om vårdprogrammet i sig inte är det?

Testet delades upp i tre delmoment om vardera 10 timmar:

- Brandvägg igång, testprogrammen igång
- Brandvägg av, testprogram av
- Brandvägg av, testprogram på

Dessa test utfördes under en femdagars period. Vi beslutade att inte synkronisera tidpunkterna för testet utan var och en bestämde själv när han ville köra testet. Notera även att de tio timmar som varje testdel tog inte var sammanhängande.

5.2.1 Testplan

För att säkerställa att vi hade samma versioner av programvaran på samtliga datorer uppdaterades ZoneAlarm och Ad-aware. Därefter söktes datorerna igenom med Ad-aware för att ta bort alla spywarekomponenter som sedan tidigare fanns där. En av oss laddade hem installationsfilerna från download.com och distribuerade sedan dessa till de två övriga. Samtliga program laddades hem 2002-03-19 mellan klockan 14.31 och 15.07. Notera dock att installationsprogrammet till Kazaa plockar hem filer från nätet under installationens gång vilket kan ha orsakat att vi återigen kan ha installerat olika versioner.

Genom att med hjälp av brandväggen blockera tillgång till Internet för kända spywarekomponenter med kunde vi dokumentera vilka komponenter som aktivt skickade eller tog emot information efter installationen av testprogrammen. Vi gjorde också regelbundna sökningar med Ad-aware för att dokumentera de nya komponenter som dök upp under undersökningens gång.

5.2.2 Resultatbeskrivning

Återigen ser vi att wnad.exe är aktiv då denna fil söker tillgång till nätet. Något som fångas upp av brandväggen. Detta inträffade sammanlagt 9 gånger under de 60 (3 testperioder om 10 timmar på 2 datorer) timmar som testet utfördes. Även tilläggsprogrammen SaveNow och Gator Silent Installer bad om att släppas ut vid olika tillfällen. Vi har valt att lägga beskrivningen av de två sistnämnda i resultatbeskrivningen av test tre (3.4.2).

Efter det att vi tog bort brandväggen och körde testet utan att ha några av programmen aktiva, märkte vi direkt en skillnad. Tilläggsprogrammen hade nu fri tillgång till nätet. Det genererades popup-fönster med annonser både när vi använde Internet Explorer och ibland även när vi inte hade webbläsaren igång. Under testperioden noterade vi 9 popups av vilka 4 kan relateras direkt till tilläggsprogram.

Den tredje 10 timmarsperioden körde vi datorn utan brandvägg med alla freewareprogrammen igång. Skillnaden från den andra testen utan brandvägg var inte särskilt stor. Det genererades några fler popups, annars var det samma resultat som i det föregående testet. Av de 15 popups vi noterade kunde 7 relateras direkt till spyware.

5.2.3 Resultatanalys

Med en nyligen uppdaterad brandvägg kan vi om inte helt förhindra tillägsprogrammen att utföra sina uppgifter, åtminstone hålla tillbaka det. Vi fick inga popups som vi kunde relatera till tillägsprogram under de testtimmar vi körde med brandväggen igång. Vi märkte inte heller några andra händelser, som vi kunde relatera till tillägsprogrammen, under den tiden. Märk dock att tillägsprogrammen ofta försökte komma ut på Internet men att vi inte släppte ut dem genom brandväggen.

Är brandväggen däremot avstängd, genereras det oregelbundet popupannonser av tillägsprogrammen. Vi kunde dock inte se vad dessa processer gjorde. Av våra tester har det emellertid framkommit att det inte är någon nödvändighet för värdprogrammen att vara aktiva för att tillägsprogrammen skall kunna köra i bakgrunden och generera popupfönster. Värt att notera är också att vid en del tillfällen då vi fått popupannonser, har vi inte ens haft Internet Explorer (webbläsaren) igång.

Tillägsprogrammen verkar överlag väldigt oregelbundna i sina agerande. Ibland börjar de köra när man sätter igång datorn och ibland tar det någon timme. Tillägsprogrammen gör något, men vi kan fortfarande inte se vad. Skillnaden mellan det två testerna utan brandvägg är inte speciellt stor, det enda som skiljer är att det genereras lite mer popups när man har programmen igång.

5.3 Test tre

Efter att vi analyserat resultaten från test ett och test två, insåg vi med hjälp av vår handledare behovet av ett tredje test. En del intressanta saker framkom av de föregående testerna, men vi kände att vi inte fullt ut kunde sätta resultaten i relation till varandra. De utförda testerna var ofullständiga och saknade den rätta strukturen. Detta utan att minska sin vikt i sammanhanget. Test ett och två visade mer eller mindre vägen till det tredje testet. I detta test kvarstod konceptet från test två, syftet var fortfarande att övervaka och dokumentera olika tilläggsprogramms agerande i diverse miljöer, upplägget på testet ändrades dock och bättre struktur tillfördes.

5.3.1 Testplan

Vi delade upp testet i fem tio timmars perioder enligt följande (förkortningarna som vi redogör för här kommer att användas i resten av rapporten):

- BI/UP Brandvägg igång, utan testprogram installerade.
- BI/PA Brandvägg igång, testprogram av
- UB/PA Utan brandvägg installerad, testprogram av
- BI/PI Brandvägg igång, testprogram igång
- UB/PI Utan brandvägg installerad, testprogram igång

Testet utfördes på tre datorer under en sjudagars period. För att förutsättningarna skulle vara mer lika än i de föregående testerna, samt för att säkerställa att datorerna var helt fria från adware och spyware, formaterades hårddiskarna på varje testdator. Därefter installerades operativsystemet Microsoft (MS) Windows XP, samt basprogrammen MS Word, MS Excel, kommunikationsverktyget ICQ¹, e-mailklienten Eudora², mediaspelaren Winamp³, och Norton Antivirus. Basprogrammen var program som vi ansåg att de flesta användare har tillgång till. Därpå installerade vi ZoneAlarm och Ad-aware. Efter installationerna uppdaterades referensfilen för Ad-aware till senaste version.

Vi beslutade att, även för detta test, inte synkronisera tidpunkterna för testerna utan var och en bestämde själv när han ville köra testet. En testdel behövde inte heller vara sammanhängande, det vill säga att en tio timmars period inte behövde köras i sträck. Allt för att skapa en så normal användarmiljö som möjligt med ett för oss troligen normalt användarmönster.

För att vi skulle kunna urskilja skillnader mellan de utvalda testprogrammen och dess olika medföljande spyware, gjorde vi följande uppdelning:

	Kazaa	BearShare	Audiogalaxy
Dator 1 (BS/KA)	X	X	
Dator 2 (AG/KA)	X		X
Dator 3 (AG/BA)		X	X

Datorerna kommer i fortsättningen att hänvisas till som förkortningarna, inom parentes, i tabellen.

Som ett led i att säkerställa att respektive program var av samma version, användes samma installationsfil. Som redan nämnts installeras Kazaa genom att filer laddas hem

¹ <http://www.mirabilis.com>

² <http://www.eudora.com/>

³ <http://www.winamp.com>

från en server under installationstillfället. För att, i största möjliga mån, kringgå detta problem installerades Kazaa vid ungefär samma tidpunkt.

För att få mer struktur i själva loggandet av testet satte vi upp några allmänna regler. Varje period innefattade tio timmars mätning med minst fem omstarter. Efter varje omstart, skulle tio utvalda webbsidor besökas. Tio svenska webbsidor valdes ut, på fem av sidorna fanns det någon form av befintlig reklam, på de andra fem ingen reklam alls. Detta för att se huruvida tilläggsprogrammen byter ut befintliga banners mot sina egna eller lägger till reklam på de sidor som inte har det, ett fenomen vi läst om i diverse artiklar på Internet.¹ Vi förde även logg över varje testdators resurser. Resursmätningar gjordes två gånger i timmen där vi uppmärksammade CPUutnyttjande, utnyttjande av minne (RAM) samt det totala nätverksutnyttjandet. I samtliga delar i försöket noterades popups.

Genom att blockera access till Internet för kända spywarekomponenter via brandväggen kunde vi dokumentera vilka komponenter som var aktiva. För vår dokumentation av testet skapade vi loggböcker, där vi loggade alla händelser, som kunde relateras till tilläggsprogram.

Den första mätningen genomfördes med brandväggen igång och utan testprogrammen installerade. Denna delen gjordes för att få värden från "rena" datorer att jämföra med de senare delarna i försöket.

För mätning två installerades programmen och dessa fick köra under en timme, då också nedladdningar gjordes. Detta för att eventuellt väcka upp sovande tilläggsprogram. Under resten av den här delen kördes inte programmen. Därefter gjordes en sökning med Ad-aware för att notera förändringar. I loggfilen noterades de nya processer som körde efter installationen av programmen.

För mätning tre avinstallerades brandväggen för att släppa ut eventuella tilläggsprogram på Internet. Testprogrammen i sig kördes inte under den här delen. Samma mätningar gjordes i denna delen och resultaten noterades i loggfilen och som skärmdumpar.

För mätning fyra lät vi undersökningsprogrammen köra, men vi blockerade access till Internet med hjälp av brandväggen som installerades igen. Återigen mätte vi och noterade resultaten.

Inför mätning fem avinstallerades brandväggen återigen för att inte på något sätt begränsa tillgång till Internet för programmen. Programmen fick sedan köra fritt under tiden vi gjorde våra mätningar.

Testplanen återfinns, i originalform, i bilaga 1.

5.3.2 Resultatbeskrivning

Vi vill nämna att sökningarna med Ad-aware inte gav några intressanta uppgifter. Detta eftersom de filer som upptäcks kan, även om de tillhör tilläggsprogram, vara vilande och därför inte påverkar testet. Vi koncentrerade oss istället på de processer som vi kunde se i listan över aktiva processer. Genom denna kunde vi se att ett antal nya processer körde. Vi har här valt att beskriva de fyra som vi, efter sökning på Google, kunde hänföra till tilläggsprogram. Dessa fyra processer är msbb.exe, SaveNow.exe, CMESys.exe samt GMT.exe.

I samband med installationen av BearShare, får användaren chansen att välja att även installera ett program vid namn n-case. N-case samlar information om dig som

¹ <http://www.cexx.org/adware.htm>, 2002-05-20, 11:27

användare, i syfte att leverera riktad reklam. Informationen som samlas kan vara allt ifrån vilka Internetsidor du besöker till vilka program som finns på din dator. Företaget bakom detta program, 180Solutions, redogör i sin integritetspolicy för att de inte samlar någon personlig information som kan kopplas till någon enskild användare.¹

I vår processövervakning på den testdator där n-case installerades, hittade vi dock ingen process med direkt anknytning till programmet. Istället uppenbarade sig en annan process vid namn *msbb.exe*. Vid en första titt kopplade vi ihop processen med Microsoft, eftersom många av Microsofts programfiler börjar med bokstäverna *ms*, men efter att vi kommit fram till att den bara existerade på testdatorn med n-case, blev vi misstänksamma.

Efter att vi undersökt saken på Internet visade det sig att *msbb.exe* var ett spyware-program som utan vår kännedom installerats i bakgrunden under installationen av n-case. *Msbb* fungerar ungefär som n-case, det vill säga att den samlar information om användaren som den sedan vid oregelbundna tillfällen skickar till olika servrar för bearbetning. Detta görs i huvudsyfte för att kunna direktrikta reklam till användare i form av popups.

Företaget som tillverkat *msbb* kallar sig för web3000. Precis som företaget 180Solutions ovan, anger web3000 i sin policy att de "bara" samlar information om användarens surfvanor, övrig information som företaget sparar, erhålls endast genom att användaren själv skickar den till företaget. De gör även klart att information som samlas inte kan kopplas till någon enskild användare, samt att de inte skulle få för sig att sälja någon information vidare till tredje part.²

Det finns dock skillnader mellan de två nämnda programmen. Det sistnämnda programmet (*msbb*) har bland annat upptäckts ersätta systemfilen "*winsock32.dll*" i Windows med en egenproducerad fil³. Detta innebär att det inte är rekommenderat att ta bort *msbb* från datorn om användaren inte avinstallerar programmet det kom med först (n-case), eftersom systemfilerna i annat fall inte återställs rätt. Med andra ord, kan det uppstå problem om användaren vill fortsätta köra originalprogrammet, men avlägsna *msbb*.

*SaveNow*⁴ distribueras bland annat genom BearShare och Kazaa. Programmet ger användaren reklam och erbjudanden baserat på de webbplatser som denne besöker och/eller sökord som skrivs i sökmotorer. Reklamen och erbjudandena kommer från företag som samarbetar med WhenU.com och den visas i olika format, bland annat med popup-fönster. Gör användaren exempelvis en sökning med en sökmotor kommer *SaveNow* att jämföra sökningen med de reklam-erbjudanden som sedan tidigare har lagrats på användarens dator. Finns det någon passande reklam kommer den att visas i ett nytt fönster eller på annat vis. Programmet laddar automatiskt ner reklamen och erbjudandena till användarens dator.

WhenU är mycket noga med att påpeka att de inte samlar information om en användare som kan härledas till just den användaren. Men läser man deras integritetspolicy förstår man att de förutom kön, ålder och postadress även lagrar användarnas e-postadresser. Den information som samlas in om användaren kan enligt WhenU distribueras till andra intressenter.

¹ <http://www.180solutions.com/n-case/Privacy.htm>, 2002-05-03, 16:08

² <http://www.web3000.com/support/privacy/privacy-site.asp>, 2002-05-03, 16:47

³ <http://accs-net.com/smallfish/web3000.htm>, 2002-05-03, 16:52

⁴ <http://www.whenu.com>

Enligt "Children's Online Privacy Protection Act of 1998" är det förbjudet för aktörer på Internet att samla information om användare under 13 år. På grund av detta tillåter inte WhenU att användare under denna ålder använder programmet.

Slutligen uppges det att programmet uppdateras automatiskt när WhenU släpper en ny version av SaveNow och detta sker helt utan användarens medverkan.¹

CMESys.exe och GMT.exe kan hänföras till GAIN², Gator Advertising & Information Network. Enligt tillverkaren The Gator Corporation³ hjälper GAIN till att tillhandahålla gratis mjukvara i utbyte mot att de får leverera reklam, information och mjukvara baserat på de sidor som användaren besöker.⁴ Program som levereras med GAIN kallas av Gator för GAINware.

Gator tillverkar även eWallet, en programvara som hjälper användaren att fylla i formulär och komma ihåg lösenord.

Från The Gator Corporations f.a.q. (lista över vanliga frågor) har vi översatt följande: Vi vet inte vem du är och vi vet inget om dig personligen. Vi lagrar, eller använder, inte information som kan hänföras till dig personligen. Till exempel så känner vi inte till dina e-mail adresser, efternamn, gatuadress eller telefonnummer. Inte heller samlar vi in någon annan känslig eller personlig finansiell information, så som kreditkortsnummer, användarnamn, lösenord eller kontonummer. All sådan information som du skriver in i någon programvara som vi utvecklar, såsom Gator eWallet, stannar på din dator och skickas inte till våra servrar. Detta garanterar att vi inte vet vem du är och att din integritet är skyddad.⁵

Vidare skriver de: GAINware samlar och använder viss information. All insamlad information associeras med ett anonymt ID som slumpmässigt genereras av The Gator Corporation. Informationen som vi kan samla, använda och associera med ditt unika ID inkluderar:

- Vilka webbsidor din dator besöker och under hur lång tid dessa sidor besöks
- Ditt gensvar på reklamen som vi levererar
- Den information som vanligtvis lagras vid besök på hemsidor (Standard web log information) och systeminställningar
- Vilken mjukvara som finns på din dator
- Ditt förnamn, land, och ett femsiffrigt postnummer
- Användarstatistik och inställningar för ditt GAINware

Informationen som associeras med ditt anonyma ID används på några av följande sätt: För att erbjuda assistans (veta när du behöver hjälp att fylla i ett formulär eller ställa in systemklockan).

För att välja ut och leverera installationsfiler för valfria nya GAINware och/eller tredjeparts applikationer.

För att leverera reklam och information till dig för våra klienters räkning vilka ofta är konkurrenter till webbsidorna du besöker.

Ibland använder vi av oss tredjeparts tillverkare som kan ges tillgång till all information vi har så att de kan utföra uppgifter som annars skulle ha utförts av våra anställda.

¹ http://www.whenu.com/about_savenow.html, 2002-05-10, 12:48

² <http://www.cexx.org/gator.htm>, 2002-05-10, 14:06

³ <http://www.gator.com>

⁴ <http://www.gatoradvertisinginformationnetwork.com/help/gainfaq.html#1>, 2002-05-10, 16:18

⁵ http://www.gatoradvertisinginformationnetwork.com/help/app_privacy/#Privacy_Policy, 2002-05-10, 17:53

Dessa tillverkare har ingen rätt att använda informationen för några andra ändamål än de beskrivna och de är bundna till samma restriktioner som våra anställda.¹

Ytterligare ett resultat av denna del av undersökningen, är det faktum att vi, i vissa fall, kunde se ett klart samband mellan den reklam vi utsattes för och de sidor vi besökte. Det mest tydliga exemplet på detta var då vi flertalet tillfällen, på separata datorer, utsattes för reklam som vi direkt kunde knyta till de sökord vi använde oss av vid sökningar på google.com. Reklamen genererades av SaveNow och inte av den aktuella sidan.

5.3.3 Resultatanalys

Orsaken till skillnaderna på utfallen mellan de olika datorerna kan bero på hur datorn användes och vilka surfvanor respektive användare har. Exempelvis kan en användare besökt många sidor till vilka tilläggsprogrammen inte hittar någon matchande reklam. Ytterligare en förklaring kan vara att resursmätningarna endast är ögonblicksbilder av verkligheten vilket kan ha medfört att alla händelser inte dokumenterats.

5.3.3.1 Popups

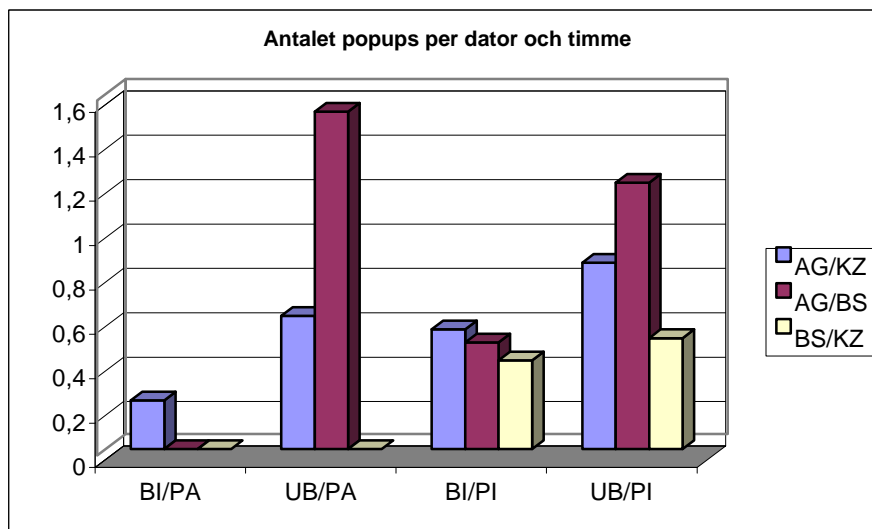


Diagram 1

Diagram 1 visar antalet uppmätta popups per dator och timme. Det framgår tydligt att när brandväggen inte är igång inträffar en markant ökning av antalet popups. Då det inte inträffade någonting under den första testperioden, har vi valt inte ta med denna i diagrammet.

Diagram 2, 3 och 4 visar förekomsten av popups per tillägsprogram på respektive dator under de fyra sista testperioderna.

¹ http://www.gatoradvertisinginformationnetwork.com/help/app_privacy/#Privacy_Policy, 2002-05-10, 17:53

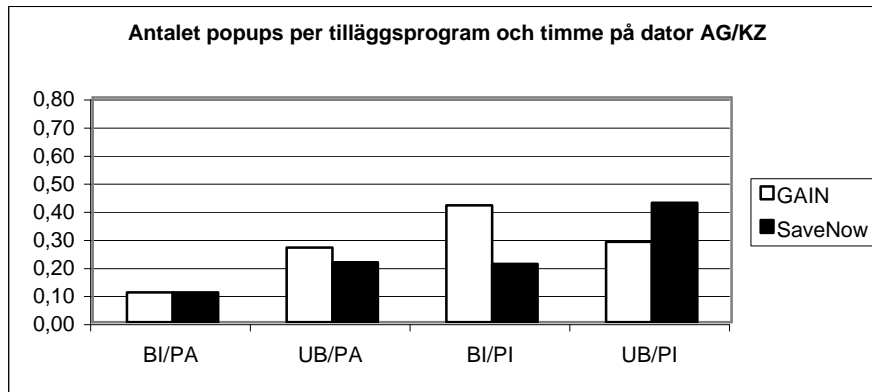


Diagram 2

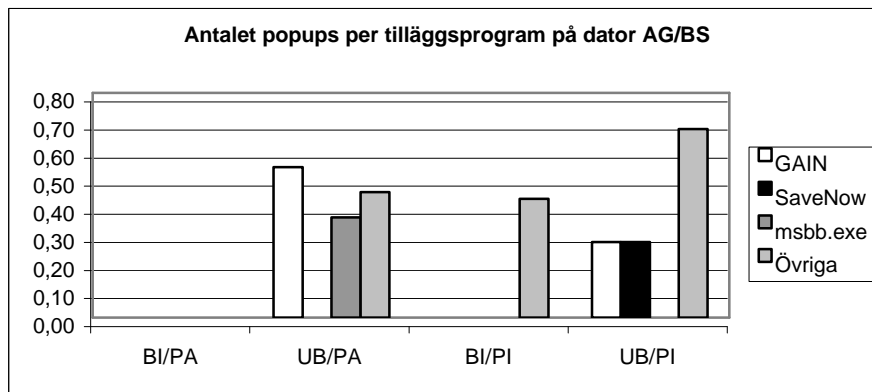


Diagram 3

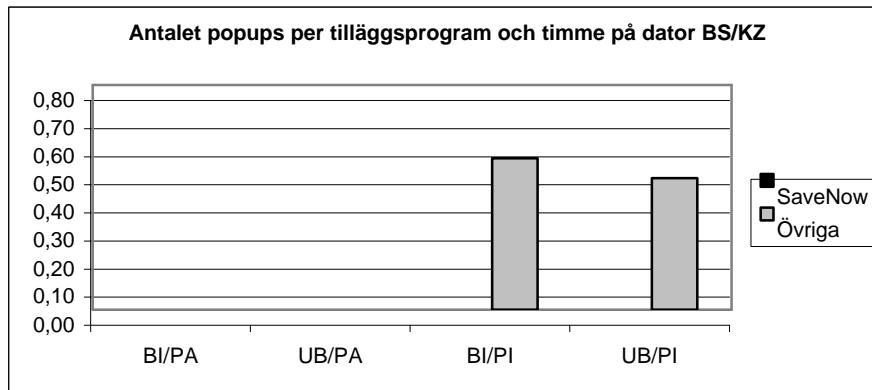


Diagram 4

Under perioden *UB/UP*, då systemen var helt fria från peer2peerverktyg och dess tilläggsprogram, inträffade det ingenting av intresse för undersökningen. Denna mätperiod fungerar därför endast som referens.

Under den efterföljande perioden, *UB/PA*, genererades sammanlagt två popupfönster, dock endast på en dator. Trots den låga siffran visar detta på att värdprogrammet inte behöver exekvera för att tilläggsprogrammen ska vara aktiva.

Perioden *UB/PA* visar på en markant frekvensökning av popups på två av datorerna. Under denna mätperiod var brandväggen avinstallerad, vilket med största sannolikhet förklarar ökningen. Vi vet inte vad som orsakade att frekvensen på den tredje datorn låg kvar på noll, men vi misstänker att det beror på användaren av denna dator, under denna period, använde Internet mindre flitigt.

Under perioden *BI/PI*, det vill säga med brandväggen och programmen igång, sjunker antalet popups på de två datorer som även tidigare genererade popups. På en av dessa datorer, AG/BS, sjunker antalet dessutom drastiskt, med nästan 70 %. Ökningen på datorn med BS/KZ kan förklaras med att testprogrammen är igång och att det är dessa som skapar popups. Denna förklaring grundar vi på att de popups som dyker upp inte kan hänföras direkt till SaveNow, vilket var det adware som nämnda dator var infekterad med. Samma sak gäller för datorn med AG/KZ, då det även på denna endast rörde sig om popups av typen övriga. På den sista datorn, AG/KZ, genererades flest popups av GAIN.

Den sista perioden, *UB/PI*, då brandväggen är avinstallerad men med testprogrammen igång visar en kraftig ökning av förekomsten av popups. Exempelvis ökar antalet på datorn med AG/BS med 150 %. Precis som i BA/PA torde utfallet bero på att brandväggen är avstängd.

5.3.3.2 Systemprestanda

Under testets gång kändes datorerna stundtals instabila. Vid en närmare kontroll av systemens resursförbrukning då detta inträffade noterade vi att SaveNow tog en stor del av datorns resurser i anspråk. Vid ett tillfälle använde SaveNow så mycket som 38 % av processorn, som på den aktuella testdatorn har en klockfrekvens av 1400 Mhz.

Vid två tillfällen kraschade systemet helt och omstart krävdes. Dessa två krascher, en då brandväggen och programmen kördes samt en utan brandvägg men med programmen igång, inträffade då popupfönster öppnades. Detta fick till följd att Internet Explorer kraschade, vilket i sin tur ledde till att hela Windows slutade fungera som det skulle. Sättet dessa krascher uppstod på och omständigheterna runt dem får oss att misstänka att testprogrammen, alternativt tillägsprogrammen, orsakar krascherna. Noterbart är att dessa krascher endast inträffade på datorn med AG/KZ. Vad krascherna beror på vet vi inte, men en tanke är att de båda programmen tillsammans gör systemet instabilt. Det låga antalet krascher gör dock att vi inte kan dra några slutsatser av resultatet.

Under testet inträffade även en ofrivillig omstart av datorn med BS/KZ. Vad denna omstart berodde på är oklart, men misstanken faller naturligtvis på något av testprogrammen eller de medföljande programmen. Detta eftersom det inte har inträffat på nämnda dator, varken före eller efter testperioden.

6 Diskussion

6.1 Irritationsmoment

Den minst kritiska aspekten av tillägsprogrammen är irritationsmomentet. Användaren utsätts då och då för oönskad reklam som dyker upp oavsett vad denne gör. Exempelvis kan reklamen presenteras när användaren sitter och jobbar med Microsoft Word. Förutom att arbetsrytmen störs, krävs det även en viss, om än kort, tid för att stänga ner reklamen. I vissa fall leder dessutom reklamfönstret till ett instabilt system, vilket kan få förödande konsekvenser i form av systemkrascher och förlorat arbete.

Både företag som har helt reklamfria sidor, så som IKEA¹ och Ericsson², och företag med reklam, exempelvis Aftonbladet³ och IDG⁴ drabbas när deras besökare utsätts för reklam från adware. Även om tillägsprogrammen försöker matcha reklamen med den sida som besöks kan det bli helt fel. Ett exempel på detta är när besökarna på den amerikanska sexupplysningssidan AllAboutSex⁵ (AAS) utsattes för reklam från porrsidor.⁶ Det blev inte bättre av att AAS riktar sig till ungdomar. Företaget bakom AAS fick skulden för reklamen som kom upp och arga föräldrar hörde av sig med klagomål. Efter att folket bakom AAS kontaktat WhenU visade det sig att det var SaveNow som genererade reklamen. Problemet är numera, enligt WhenU, åtgärdat.

Ytterligare ett problem med att reklamen matchas mot innehållet på sidorna som besöks, är att besökare på en sida kan utsättas för reklam från ett konkurrerande företag. Detta är naturligtvis inte önskvärt för företaget, vars sida du besöker. Pondera att du ska göra ett inköp hos en skivbutik på nätet, exempelvis cdnow.com, och du får reklam för exakt den skiva du för närvarande läser om. Problemet för cdnow.com är att reklamen kommer från konkurrenten amazon.com. För dig som kund kan detta givetvis vara bra, om priset hos amazon.com är lägre än det hos cdnow.com. Frågan är hur etiskt korrekt detta marknadsföringssätt är. Hur skulle det se ut om Sibylla gjorde reklam för sina hamburgare på McDonalds' restauranger?

6.2 Kapprustningen

I takt med att kunskapen om tillägsprogram som spyware och adware ökar, ökar även medvetenheten om riskerna och behovet att skydda sig. Nya program som hjälper användaren att hålla systemet fritt från spyware och adware dyker upp hela tiden och kan oftast hittas på dedikerade nedladdningssajter, exempelvis download.com⁷. I vårt arbete har vi, som tidigare nämnts, endast använt Ad-aware. Detta på grund av dess tillgänglighet och möjligheten att uppdatera programmet. Att fortlöpande uppdatera motmedlen är ett viktigt led i kampen mot tillägsprogrammen.

Med motmedel som uppdateras kontinuerligt kommer naturligtvis en motattack från de företag som utvecklar och tjänar pengar på tillägsprogrammen. För att utvecklarna av tillägsprogrammen ska kunna fortsätta erbjuda sina tjänster till sina kunder måste programvaran, för att undkomma motmedlen, hela tiden förbättras och skrivas om.

¹ <http://www.ikea.se>

² <http://www.ericsson.se>

³ <http://www.aftonbladet.se>

⁴ <http://www.idg.se>

⁵ <http://www.allaboutsex.org/>

⁶ http://www.allaboutsex.org/pop-up_ads.html

⁷ <http://www.download.com>

Vad leder då denna kapprustning till? Ett framtida scenario skulle kunna vara att tilläggsprogrammets komponenter gömmer sig genom att exempelvis byta namn på regelbunden basis. Dessutom kan det tänkas att tilläggsprogrammets komponenter allt oftare döps till namn som lätt kan tas för exempelvis komponenter som tillhör operativsystemet. Ett exempel på detta är msbb.exe (web3000) som vi, till en början, tog för en komponent från en Microsoftprodukt.

Det har redan nu bevisats att det går att avinstallera andra program, i detta fall Ad-aware, från en dator då ett annat program installeras. Tillverkaren av RadLight¹, ett program främst avsett för filmvisning, lade till följande rad i sitt användaravtal: "*Du får inte använda något tredjepartsprogram (Tex. Ad-aware) för att avinstallera program som medföljer RadLight. Sådana program kommer tas bort.*"². Mycket riktigt utfördes även en avinstallation av Ad-aware vid installation av RadLight.³ Detta diskuterades flitigt på bland annat slashdot.org⁴, vilket kan ha bidragit till att funktionen numera har tagits bort från RadLight. Det sägs att tillverkaren har gått ut med att funktionen skrevs i syfte att visa vad som går att göra, något som utvecklaren onekligen lyckades med.⁵

6.3 Potentiell säkerhetsrisk

Om tilläggsprogrammen kan samla in och skicka mindre känslig information, som vilka webbsidor användarna besöker, vad är det då som säger att de inte kan samla in känslig information, som lösenord, e-postadress och kontonummer?

Under augusti 2001 spreds information om att Audiogalaxy innehöll ett tilläggsprogram, vid namn vx2⁶, som samlade in personlig information.⁷ Bland det som samlades in ingick användarens fulla namn, e-mailadresser samt vilka program som fanns installerade i systemet. Vx2 fångade till och med upp innehåll i webbformulär, inte bara vanliga utan även så kallade säkra formulär som krypteras vid sändning. Företaget bakom vx2 hävdar dock i sin integritetspolicy⁸ att de inte samlar in lösenord och kreditkortsnummer. Sättet på vilket företaget förhindrar insamling av lösenord är genom att inte bry sig om information i fält med namn som innehåller 'pas', 'pwd', eller 'pin'. Kreditkortsnummer upptäcks genom en kontroll gentemot standardformatet på sådana.⁹ Det är tydligt att dessa säkerhetsåtgärder innehåller brister, lösenordsfält innehåller exempelvis inte alltid 'pas', 'pwd', eller 'pin', ett lösenordsfält på en svensk sajt skulle mycket väl kunna vara döpt till 'losenord'. Man kan även tänka sig att känslig information, så som lösenord, skickas med webbaserad e-post via formulär. Den informationen skulle därmed inte identifieras som lösenord och alltså fångas upp av vx2.

I mars 2002 utsattes användarna av fildelningsprogrammet Morpheus för en av de grövsta integritetskränkningarna vi har hört talas om. Morpheus, som alltid ansetts vara fritt från tilläggsprogram, slutade plötsligt att fungera. Efter att utvecklarna av mjukvaran, MusicCity, inte hade betalat licensavgiften till FastTrack, utvecklarna av tekniken bakom Morpheus, stängdes programmet av från nätverket som delades med Kazaa. Detta skedde, enligt uppgift, genom att en bakdörr i programvaran tillät ändringar i registret på användarnas datorer. Kazaa har anklagats för att ligga bakom

¹ <http://www.radlight.net/>

² <http://nyheter.idg.se/display.asp?id=020426-tst1>, 2002-05-16, 14:16

³ <http://www.newsbytes.com/cgi-bin/udt/im.display.printable?client.id=newsbytes&story.id=176075>, 2002-05-16, 14:25

⁴ <http://slashdot.org/article.pl?sid=02/04/24/1946204&mode=thread&tid=99>, 2002-05-16, 14:17

⁵ <http://www.infoanarchy.org/comments/2002/4/24/151850/224?pid=1#2>, 2002-05-18, 13:50

⁶ <http://www.vx2.cc>

⁷ <http://www.cexx.org/vx2.htm>, 2002-05-16, 15:56

⁸ <http://www.vx2.cc/privacy.htm>, 2002-05-16, 16:10

⁹ <http://www.cexx.org/vx2.htm#gather>, 2002-05-16, 16:50

detta, vilket de förnekar.¹ Oavsett vem som ligger bakom intrånget visar det hur sårbara vi, som användare, är och hur mycket skada som skulle kunna åsamkas oss.

Kazaa nämns även i samband med ett av de mest uppmärksammade fallen av tilläggsprogram, nämligen det med Brilliant Digital, som omnämndes i inledningen av arbetet. Brilliant Digital Entertainment (BDE) är ett amerikanskt företag som sysslar med tekniker för att sprida reklam.² De har, sedan hösten 2001, distribuerat sitt program, b3d Digital Projector, med Kazaa. Programmets syfte har varit att visa reklam i form av 3D-animeringar. Under april 2002 framkom det att BDE installerat än mer sofistikerad programvara på Kazaa-användarnas datorer. Denna extra programvara, som kan aktiveras på kommando av BDE, ser till att datorn blir en del av ytterligare ett nätverk, som kontrolleras av Brilliant Digital. Tanken är att datorer ska, med dess användares godkännande, användas för att lagra och sprida material såsom reklam och musik.³ BDE ska även kunna låna datorkraft för att utföra exempelvis matematiska beräkningar. Brilliant Digital motiverar idén med att användarna äger datorer med hög kapacitet, medan företag behöver mer kraft och plats för att tillfredsställa sina behov. BDE anser att om användarna ges möjlighet att låna ut datorkraft, plats och bandbredd till företagen så är det en "win-win for everyone"⁴ (alla tjänar på det). Detta påstående kan givetvis ifrågasättas då det inte nämns någonting om hur mycket resurser som faktiskt kommer att användas eller vad dessa resurser kommer att användas till. Är alla som installerar Kazaa beredda att låna ut sin datorkraft till okända företag?

6.4 Framtiden för peer2peer och tilläggsprogrammen

Dagens peer2peerprogram når en väldigt bred användargrupp bestående av allt från vana datoranvändare till totala nybörjare som endast är ute efter gratis musik. Troligtvis är det så att en stor del av användargruppen inte har kunskap, eller bryr sig, om vilka program de får på köpet när de installerar verktygen för att komma åt exempelvis gratismaterial. Ytterligare ett antagande från vår sida är att även om en del användare vet att de får vissa program "på köpet" är det inte säkert att de är medvetna om vad dessa program gör, eller kan göra.

I takt med att medvetenheten om problemen och riskerna med tilläggsprogram ökar bland användarna, kommer värdprogrammen antagligen att utsättas för hårdare granskning. Redan nu, maj 2002, finns det en hel del information om hur man skyddar sig och vilka program som agerar värdprogram, att hämta på Internet. Men för att informationen ska nå ut till så många som möjligt krävs att denna sprids genom fler kanaler. Så länge informationen bara finns tillgänglig på nischade sidor, såsom slashdot.org, infoanarchy.org⁵ och idg.se kommer denna endast att nå en liten del av användarna. På senare tid har dock sidor som aftonbladet.se⁶ och cnn.com⁷ tagit upp problemen vilket förhoppningsvis innebär att fler kommer att ta del av informationen.

Frågan är om inte många användare, trots kunskap om tilläggsprogrammen, är beredda att släppa lite på sin integritet för att få tillgång till fria nedladdningar genom peer2peerprogram. Skulle så vara fallet finns det ingen anledning för utvecklarna av peer2peerprogrammen att inte distribuera sina program med tilläggsprogram och på så sätt tjäna pengar. Ett tecken på användarens likgiltighet är det faktum att Kazaa, mellan

¹ <http://nyheter.idg.se/display.asp?id=020322-iw3>, 2002-05-19, 02:28

² <http://news.zdnet.co.uk/story/0,,t269-s2107584,00.html>

³ <http://news.com.com/2100-1023-873181.html>, 2002-05-19, 03:04

⁴ <http://www.brilliantdigital.com/content.asp?ID=779>

⁵ <http://www.infoanarchy.org/>

⁶ <http://www.aftonbladet.se/vss/it/story/0,2789,157403,00.html>, 2002-05-17, 11:06

⁷ <http://www.cnn.com/2002/TECH/ptech/05/16/disaster.ware.idg/index.html>, 2002-05-17, 11:19

den 9:e och 16:e maj 2002, laddades ned 4 252 962 gånger vilket placerade programmet högst på listan över mest nedladdade program på download.com under denna period. Under samma period laddades Morpheus ned 891,734 gånger vilket gav den en tredjeplats. Detta trots att CNet, på respektive programs nedladdningssida, varnar för att programmen innehåller tilläggsprogram.¹

Skulle det å andra sidan vara så att användarna slutar använda peer2peerverktyg för att slippa riskera att deras personliga uppgifter sprids, blir situationen en helt annan. Ett scenario är att utvecklarna av peer2peerverktygen börjar ta betalt för sina program för att kunna hålla dem rena från tilläggsprogram, vilket kan leda till att användarna börjar väga kostnaden för programmet mot kostnaden för att köpa det som de i vanliga fall laddar hem. I våra ögon är dock detta scenario mindre troligt.

Nedladdningssiffrorna vi nämner i detta arbete bör tas med en nypa salt, då samma användare med största sannolikhet laddar hem programmet vid flera tillfällen. Anledningen till att vi misstänker detta, är att nya versioner av programmen släpps med jämna mellanrum. En möjlig orsak till att programmen ofta släpps i nya versioner är att utvecklarna vill sprida uppdaterade versioner av tilläggsprogrammen, trots att värdprogrammen innehåller inga eller enbart mindre uppdateringar. Ytterligare en orsak till de höga nedladdningssiffrorna kan vara att utvecklarna själva laddar hem sina program i ett försök att få upp sina nedladdningssiffror för att på så sätt öka intresset från utvecklarna av tilläggsprogrammen.

Det har, som vi tidigare nämnt i avsnittet Resultatbeskrivning av test tre (3.4.2), även framkommit att vissa tilläggsprogram, så som web3000², kan ersätta systemfiler i Windows. I just web3000's fall gäller det åtminstone wsock32.dll. Att skriva över denna fil är samma taktik som vissa virusmakare använder sig av för att infiltrera ett system.³ Så när blir ett tilläggsprogram så pass aggressivt att det kan klassas som virus? Enligt en kort rapport⁴ från Symantec⁵, utvecklare av bl.a. Norton Antivirus och Norton Internet Security, kommer åtminstone inte de att räkna spyware som virus så länge som det, i licensavtalet eller på annat lättåtkomligt ställe, anges vad programmet gör. Författaren av rapporten betonar dock att licensavtalen ofta är långa och krångliga vilket gör att användaren inte bryr sig om att läsa dem.

¹ <http://www.download.com>, 2002-05-17, 14: 38

² <http://web3000.com>

³ <http://www.oit.duke.edu/ats/support/spyware/gozilla.html>, 2002-05-17, 10: 13

⁴ Post, A. *The Dangers of Spyware*, Leiden: Symantec Ltd.

<http://securityresponse.symantec.com/avcenter/reference/danger.of.spyware.pdf>, 2002-05-19, 17: 27

⁵ <http://www.symantec.com>

7 Slutsats

Vi har, under arbetets gång, blivit både förvånade över och intresserade av det som framkommit, dels genom våra egna tester men även genom den information vi läst. Av testerna kan vi se hur både värddprogrammen och tilläggsprogrammen påverkar våra datorer. Reaktionerna på den reklam som genereras är våra egna och har givetvis ingen vetenskaplig grund. Vi inser att en del användare kan se en nytta i att få reklam och erbjudanden som är riktad direkt till dem.

För de användare som, i likhet med oss, vill skydda sig och sin integritet, finns det, som vi redogör för i arbetet, möjlighet till detta. Vi vill dock påpeka att de metoder vi har beskrivit inte nödvändigtvis ger fullgott skydd. I likhet med exempelvis antivirusprogram gäller det att utvecklarna av skyddet, i detta fall Ad-aware och ZoneAlarm, ständigt förbättrar, utvecklar och uppdaterar sina produkter. Dessutom är det upp till användaren att verkligen uppdatera programmen. Det kommer förmodligen alltid vara så att utvecklarna av virus och tilläggsprogram ligger några steg före. Vare sig användarna känner till detta eller inte, är det lätt att invaggas i falsk säkerhet. Ett enkelt, men ofta felaktigt, sätt att mäta hur bra ett visst skydd är, är att se till antalet blockeringar av exempelvis virus och intrångsförsök. Det som programmen däremot släpper igenom, är svårt eller omöjligt att upptäcka i tid.

Tyvärr lyckades vi, genom våra tester, aldrig ta reda på exakt vad tilläggsprogrammen skickar till och från våra datorer. Det enda vi kunde se var att någonting skickades och togs emot, vilket borde vara nog för att väcka intresse och misstanke. Genom att söka information, kunde vi ändå få reda på, och redogöra för, vad som skickas av de olika tilläggsprogrammen. Vi har kunnat se att det är mer än bara surfvanorna som registreras och skickas. I ett fall (vx2) samlas exempelvis den information som ifylls i formulär in och skickas till företaget bakom programmet. Att dessutom det inbyggda skyddet för att undvika insamling av extremt känsliga uppgifter är så dåligt som det är, gör inte saken bättre och visar på hur dålig kontroll man har över sina personliga uppgifter.

Som förslag till framtida arbete vill vi föreslå en fördjupning av test tre, där längden på testperioden utökas. Ytterligare en intressant infallsvinkel är att undersöka om, och i så fall hur, tilläggskomponenterna ökar i antal utan yttre påverkan. Detta skulle exempelvis kunna genomföras i en totalt oskyddad testmiljö, där tilläggsprogrammen tillåts verka fritt. Genom att använda exempelvis Ad-aware kan förändringarna dokumenteras och därefter analyseras. Vi vill också föreslå en fortsättning av test ett, för att ta reda på vilken information som verkligen skickas av de olika tilläggsprogrammen.

7.1 Så här kan du skydda dig

Det bästa skyddet sig är att känna till riskerna och vidta åtgärder baserat på dessa. Förhoppningsvis har vi, genom detta arbete, lyckats uppmärksamma läsaren på de risker som kan föreligga vid användandet av gratisprogram, främst då peer2peerverktyg. Vi hoppas också att vi genom att beskriva Ad-aware och ZoneAlarm har visat läsaren vilka möjligheter som finns för att praktiskt skydda sina personliga uppgifter.

8 Referenslista

<http://nyheter.idg.se>
<http://seachnetworking.techtarget.com>
<http://whatis.techtarget.com>
<http://e-magazineonline.com>
<http://www.download.com>
<http://www.newsbytes.com>
<http://www.twistedhumor.com>
<http://www.cexx.org>
<http://www.180solutions.com>
<http://www.web3000.com>
<http://accs-net.com>
<http://www.whenu.com>
<http://www.gatoradvertisinginfomationnetwork.com>
<http://www.slashdot.org>
<http://www.infoanarchy.org>
<http://www.vx2.cc>
<http://www.news.zdnet.co.uk>
<http://www.new.com.com>
<http://www.aftonbladet.se>
<http://www.cnn.com>
<http://www.oit.duke.edu/ats>

Post, A. *The Dangers of Spyware*, Leiden: Symantec Ltd.
<http://securityresponse.symantec.com/avcenter/reference/danger.of.spyware.pdf>

Patel, R & Davidson B. (1991) *Forskningsmetodikens grunder*, Andra upplagan. Lund: Studentlitteratur.

Bilagor

Bilaga 1: Testplan för test tre

Försöksbeskrivning:

1. Formaterar hårddisken.
2. Installerar Microsoft Windows XP, Word, Excel, ICQ, Eudora, Winamp, ZoneAlarm, NortonAntivirus, AdAware.
3. Uppdatera Ad-Aware.
4. Kolla taskmanager, ta skärmdump när alla ovanstående program (utom Ad-Aware) kör.
5. Kolla taskmanager, networking, ta skärmdump.
6. Mätningar
 - a. BI/UP (utan p. installerade)
 - b. Scanna med Ad-Aware och ta bort eventuella komponenter
 - c. Installera våra två program.
 - d. Scanna med Ad-Aware, ta INTE bort komponenter, ta skärmdump.
 - e. Repetera punkt 4 och 5
 - f. Notera nya, spyware relaterade, processer och lägg in i Exceldiagrammet under "Nya processer".
 - g. Kör KZ, BS och AG i en timme (samma timme). Ladda hem ngt med varje program
 - h. Scanna med Ad-Aware, ta INTE bort komponenter, ta skärmdump.
 - i. BI/PA (p. installerade, ej igång)
 - j. Avinstallera ZoneAlarm
 - k. UB/PA (p. installerade, ej igång)
 - l. Installera ZoneAlarm
 - m. BI/PI (p. igång)
 - n. Avinstallera ZoneAlarm
 - o. UB/PI (p. igång)
7. Vid varje mätning
 - a. Notera popups
 - b. Resursmätning 2 ggr/ h.
 - i. CPU / spyware relaterad process
 - ii. MEM Usage / spyware relaterad process
 - iii. Nätutnyttjande

Allmänna regler

Varje scenario innefattar 10 timmars mätning.

Minst fem omstarter per 10-timmars period

Efter varje omstart; besök sidorna och ta en skärmdump på var och en av sidorna.

Sidorna som ska besökas är:

<http://www.aftonbladet.se>

<http://www.idg.se>

<http://www.dn.se>

<http://www.lunarstorm.se>

<http://www.torget.se>

<http://www.ikea.se>

<http://www.ericsson.se>

<http://www.telia.se>

<http://www.tele2.se>

<http://www.libero.se>

Programlista

	Kazaa	BearShare	AudioGalaxy
Dator 1 (h)	X	X	
Dator 2 (b)	X		X
Dator 3 (m)		X	X