Fakulteten för ekonomi, kommunikation och IT
Informatik

Tommy Andersson

Framtidens skadliga kod

Examensarbete, D-uppsats, 15 högskolepoäng
Juni 2008

Sammanfattning

Fenomenet skadlig kod är ett problem som blir allt större i vårt moderna samhälle. Detta beror på att användandet av datorer och andra enheter som använder sig av operativsystem ökar hela tiden, samtidigt som skaparna av den skadliga koden i allt högre utsträckning kan slå mynt av den. Det är de ekonomiska drivkrafterna som för utvecklingen av den skadliga koden framåt och utsätter användare av datorer och andra enheter som använder sig av operativsystem för säkerhetsrisker.

Syftet med denna uppsats är att undersöka hur den skadliga kodens värld kan tänkas se ut ur ett antal olika synvinklar år 2013, dvs. fem år framåt i tiden efter att denna uppsats färdigställts. De viktigaste synvinklarna är de tänkbara skillnader som finns mellan dagens och framtidens skadliga kod samt de tänkbara trender och nyheter som förväntas dyka upp.

Dessa prognoser grundar sig på intervjuer av fyra i Sverige boende experter samt på litteratur.

De viktigaste slutsatserna som dras i denna uppsats är:

- Skadlig kod kommer att utgöra ett mycket större hot i framtiden än idag
- Skadlig kod kommer att bli mycket mer förekommande
- Kostnaden av dess skadeverkningar kommer att öka
- Ekonomisk vinning blir en ännu starkare drivkraft för skapandet av skadlig kod
- Skadlig kod kommer drabba andra enheter än datorer i högre utsträckning än idag
- Trojaner och Rootkits utgör framtidens största hot
- Den skadliga koden kommer att fortsätta att ligga steget före antivirustillverkarna

Innehållsförteckning

1 Inledning

I detta kapitel förklaras varför denna uppsats handlar om fenomenet skadlig kod, som i dagligt tal ofta lite slarvigt kallas för datavirus. Vidare beskrivs här problemformuleringen, uppsatsens syfte och avgränsning, vilken målgrupp den vänder sig till samt vald metod. Till grund för uppsatsen ligger problemformuleringen, samt den avgränsning av ämnet som valts. Till detta kommer syfte och metod som talar om *vad* uppsatsen ska uppnå samt *hur* detta kom att realiseras.

Vårt moderna samhälle förankras mer och mer i informationssamhället för varje dag som går, och i detta samhälle är datoranvändandet oundvikligt. Internets betydelse och omfattning ökar i raskt takt och fler och fler datorer är ute på Internet och kopplas samman i allt större nät. Trots att det finns många fördelar med bredband, Internet och ett enkelt utbyte av information finns det även många risker med denna utveckling. Dessa inkluderar bland annat säkerhetsproblem som virus, trojaner, maskar, DDoS-attacker, bakdörrar samt phishing (”Post och Telestyrelsen: Alltid på! Bredbandsmarknaden ur ett konsumentperspektiv”, 2003). Fenomenet skadlig kod ligger verkligen i tiden, vilket exempelvis märks genom att de kända formerna av skadlig kod fördubblats under år 2007 (”Aftonbladet: Osynliga viruset snor dina pengar”, 2007). Dessa faktorer fick mig att välja fenomenet skadlig kod som uppsatsämne.

1.1 Problem

Följande frågor saknar hittills lättillgängliga och välstrukturerade svar:

- Kommer skadlig kod bli mer eller mindre förekommande i framtiden?
- Kommer nya typer av skadlig kod att tillkomma?
- Vilka typer av skadlig kod kommer vara de dominerade?
- Vilka trender inom den skadliga koden man kan förvänta sig i framtiden?

Kommer framtidens skadliga kod att skilja sig från dagens i avseende på:

- Vad och vilka den kan drabba?
- Spridningssätt?
- Hur den kan undgå upptäckt?
- Vilken skada den kan göra?
- Hur mycket ekonomiskt lidande den orsakar?

1.2 Syfte

Syftet med uppsatsen är att förutse hur fenomenet skadlig kod kommer att se ut i framtiden, och syftet uppfylls genom att de frågor som formulerats i 1.1 besvaras. Med framtiden avses i denna uppsats en tidsperiod på fem år vilket är en lång tidsrymd i datorvärlden. Då uppsatsen färdigställdes i början av år 2008 ger den en bild av hur den skadliga kodens värld kan komma att se ut år 2013.

1.3 Avgränsning

Uppsatsen behandlar den skadliga kod som kan drabba ett system oavsett operativsystem samt oavsett enhet. Dock ligger uppsatsens tyngdpunkt på den skadliga kod som kan smitta datorer som använder sig av operativsystemet Windows, då dessa är de absolut vanligaste. Microsoft Windows hade i oktober 2007 en marknadsandel på 92 % av operativsystemen (”Market share: Operating system market share for november 2007”, 2007).
Denna avgränsning valdes för att inte begränsa uppsatsen till några speciella enheter eller operativsystem då det är svårt att sia om vilka enheter och operativsystem som kommer vara de vanligaste i framtiden. Uppsatsens horisont sträcker sig fem år framåt i tiden från början av 2008, vilket i uppsatsen benämns som framtiden.

1.4 Målgrupp

Uppsatsen riktar sig till läsare som redan har grundläggande kunskaper om skadlig kod. Läsaren ska inte behöva vara expert, och därför är uppsatsen utformad så att den inledningsvis går igenom den skadliga kodens grunder.

1.5 Metod

I detta avsnitt beskrivs den metod som använts vid skrivandet av uppsatsen, och det motiveras också varför denna metod valts.

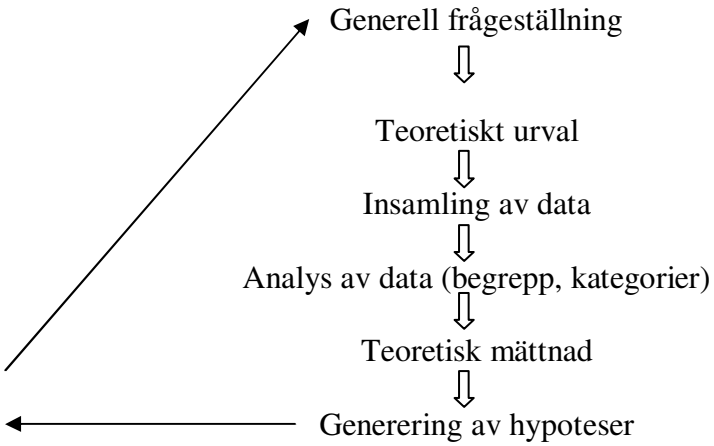
De två huvudsynsätten som används vid skrivandet av en uppsats som denna är det kvantitativa eller det kvalitativa synsättet.

Det kvantitativa synsättet har på sätt och vis med mängd att göra, och den kvantitativa analysen har därför avsikten att studera mängder av ett eller flera specifika fenomen. Målsättningen med en kvantitativ analys är enligt Starrin & Svensson (1994,s.21-22) att undersöka hur på förhand definierade företeelser, egenskaper och innebörder fördelar sig mellan olika grupper i en population eller fördelar sig med avseende på olika händelser och situationer. Samt att undersöka om det föreligger samband mellan två eller flera företeelser, egenskaper eller innebörder och vilka slutsatser detta i så fall kan ge.
Enligt Starrin & Svensson (ibid.) är därmed den kvantitativa analysen att betrakta som en företeelse-, egenskaps- och innebördsstyrd analys (FEI-styrd analys).

Det kvalitativa synsättet, å andra sidan, används ofta när man ska karaktärisera något eller gestalta något. Målsättningen med en kvalitativ analys är att identifiera ännu okända eller otillfredsställande kända företeelser, egenskaper och innebörder med avseende på variationer, strukturer och processer (ibid.).
Med andra ord är analysen att betrakta som en företeelse-, egenskaps- och innebördssökande analys (FEI-sökande analys) enligt Starrin & Svensson (1994, s.21).
Därmed står det klart att dessa två synsätt inte bara skiljer sig i tillvägagångssätt, utan att de även skiljer sig i målsättning. Vidare skriver Starrin & Svensson (Ibid.) att kvalitet är den väsentliga karaktären eller egenskapen hos något; medan kvantitet är mängden av denna karaktär eller egenskap.

Uppsatsen strävar efter att beskriva hur fenomenet skadlig kod kan se ut i framtiden, och därför passar det kvalitativa synsättet bäst då det är det mest lämpade synsättet vid identifiering av okända företeelser(ibid.).
Uppsatsen formulerar ett teoretiskt bidrag utefter studiet av litteratur samt intervjusvar, och därmed använder den sig av ett induktivt arbetssätt då den skapar teorier om framtiden utefter verkligheten, som den ser ut idag (Rienecker & Stray Jørgensen, 2002).

Inom det kvalitativa synsättet finns en metod som kallas för grounded theory, och denna ligger till grund för arbetet med uppsatsen då den bedöms vara den mest lämpade för att besvara forskningsfrågorna. Detta på grund av att metoden ger utrymme för både induktion, där hypoteser kan formuleras utifrån specifika data, och deduktion, där specifika slutsatser kan dras utifrån hypoteser. Enligt skaparna, Glaser & Strauss (”The Discovery of Grounded Theory: Strategies for quality research”, 1967), innebär grounded theory en formulering av en teori utifrån systematiskt insamlad och analyserad data under forskningsprocessens gång. Uppsatsens teoretiska bidrag bygger således på de empiriska data som samlats in och analyserats. Arbetssättet för grounded theory, vilken uppsatsen använder sig av, sammanfattas i **figur 1**:



Figur 1. Arbetssättet för grounded theory (Bryman & Bell, 2005, s. 350).

För att ge uppsatsen så hög validitet som möjligt är målsättningen att intervjua framstående experter inom detta område. Intervjuformen som valdes benämns av Krag Jakobsen (1993, s.19) som den styrda eller strukturerade forskningsintervjun. Den kallas också ibland för den kvalitativa intervjun, då den är ett utmärkt verktyg för att samla in information, som det är svårt att få tag i på annat sätt enligt Jakobsen (ibid.). Enligt Jakobsen har denna metod många fördelar. Bland annat nämner han att tillvägagångssättet ger en viss säkerhet, då intervjuerna blir så pass strukturerade att de kan bearbetas och jämföras med varandra.
Då uppsatsen är skriven ur det kvalitativa synsättet är det naturligt att ställa mestadels öppna frågor, där respondenten inte kan svara ja eller nej. Vidare ger användandet av öppna frågor möjligheten att ställa följdfrågor, vilket är användbart. Krag Jakobsen (ibid.) anser nämligen att den kanske största behållningen med öppna frågor är att de möjliggör för nya och oförutsedda aspekter att dyka upp under intervjuns gång. Inte sällan alstras dessa aspekter av följdfrågor som användandet av öppna frågor möjliggör. Enligt Jakobsen (1993, s. 191) inleds intervjun när man för första gången kontaktar motparten, och allt som sker kommer påverka det fortsatta intervjuarbetet. Jakobsen (1993, s.192) rekommenderar också att intervjuobjektet ska förberedas på syftet för uppsatsen, i vilket sammanhang den ska publiceras, hur och när intervjun ska genomföras, hur lång tid intervjun tar samt när den ska publiceras.

2 En introduktion till skadlig kod

I detta kapitel ges en bild av hur den skadliga kodens värld ser ut idag. De olika sorter av skadlig kod som existerar idag beskrivs samtidigt som centrala begrepp förklaras och definieras. Den skadliga kodens historik samt den kostnad som den gett upphov till under årens lopp belyses också. Detta är nödvändigt för att läsaren av uppsatsen ska få den förförståelse som krävs för att kunna tillgodogöra sig de slutsatser och de resonemang som förs senare i uppsatsen.

2.1 Vad är skadlig kod?

Uttrycket skadlig kod är ett samlingsnamn som alla typer av skadlig kod faller under. Tidigare användes samlingsnamnet datavirus istället, men då det efterhand tillkom många ”gränsfall” för vad som egentligen var datavirus eller något annat används nu istället den mer moderna termen skadlig kod.

En bra definition av begreppet skadlig kod ges av Mcgraw & Morrisett (2000):

“*Malicious code is any code added, changed, or removed from a software system in order to intentionally cause harm or subvert the intended function of the system. Traditional examples of malicious code include viruses, worms, Trojan Horses, and attack scripts, while more modern examples include Java attack applets and dangerous ActiveX controls*.”

2.1.1 Den skadliga kodens livscykel

Enligt professor Eric Filiol (2007) genomgår den skadliga koden normalt sett nedanstående fem stadier:

- Design och testning av den skadliga koden
- Spridning och infektionsfas då den skadliga koden tar sig till målet
- Inkubationsfas då den skadliga koden sprider sig inom målet
- Attackfas då den eventuella skadan tillfogas målet
- Eventuellt upptäcks den skadliga koden och den tas då eventuellt bort

2.2 Vad kan skadlig kod skada?

Den skadliga koden kan infektera och skada betydligt fler föremål än vad man kanske tror. Det är absolut inte enbart datorer, handburna enheter och mobiltelefoner som är utsatta för skadlig kod. En bra definition för vad den skadliga koden kan skada ses nedan (”Informit: Program security”, 2003):

”..all devices containing computer code, including automobiles, airplanes, microwave ovens, radios, televisions, and radiation therapy machines have the potential for being infected by a virus.”

2.3 Traditionella typer av skadlig kod

För att läsaren bättre ska förstå de skillnader som eventuellt kommer att framkomma i en jämförelse mellan dagens skadliga kod samt framtidens beskrivs de traditionella formerna av skadlig kod under denna rubrik. Detta avsnitt är viktigt för att en läsare med eventuellt begränsad förkunskap om ämnet ska kunna tillgodogöra sig uppsatsen.

2.3.1 Datavirus

Datavirus var tidigare samlingsnamnet för det som idag mer korrekt betecknas som skadlig kod. Datavirus är egentligen den ursprungliga formen av skadlig kod. Termen datavirus myntades av den Amerikanske studenten Fred Cohen (”Experiments with Computer Viruses", 1984). Anledningen till att termen myntades är att experter tenderar att likna datavirus med de virus som kan smitta levande varelser.

En förklaring av vad ett datavirus är har min respondent Viiveke Fåk gett i sin bok Datavirus:

”*Ett datavirus är en självständig del av ett program som gömmer sig i ett annat program och som vid exekvering kopierar sig självt till andra program i den aktuella miljön*.” *Namnet ”virus” kommer självfallet av att det ”smittar”. Dessutom behöver datavirus precis som biologiska virus en värdcell för sin fortplantning. De har inget ”liv” på egen hand. Själva förutsättningen för ett virus är att det finns en samlad uppsättning data, som kommer att läsas av datorn och tolkas som instruktioner”* (Fåk, 1990).

Med andra ord är ett datavirus ett program som har förmågan att infektera filer på en dator där de sedan kan sprida sig vidare i nästa fas. Vilken skada virusen sen kan ställa till med är högst individuellt, och beror på hur viruset är konstruerat. Med andra ord kan man säga att ett datavirus består av två delar; en som sörjer för att viruset smittar och en som gör någon typ av skada (Beckman, 1993).

Majoriteten av dagens datavirus är skrivna för Microsoft Windows, vilket främst beror på den ledande marknadsposition operativsystemet har. Det finns också virus till DOS och Mac OS, men det finns ytterst få traditionella UNIX-virus. De virus som finns till UNIX är ofta skadliga script och inte traditionella e-postvirus eller datavirus som utnyttjar säkerhetshål. (”Wikipedia: datorvirus”, 2005)

De farligaste exemplaren av virus är de som är selektiva när de infekterar andra program, vilket förbättrar oddsen för att de ska överleva. Om viruset sprids för ofta och okontrollerat på datorn så upptäcks det snabbare, vilket också medför att de är lättare att ta död på. De mest illasinnade virusprogrammerarna tillverkar därför sina virus så att de inte sprider sig för fort på datorn, samt att virusen ska vänta med att göra skada tills omständigheterna för viruset är optimala. Själva skadedelen är egentligen ofta det enda som den som råkar ut för ett virus märker av. Vad som virus kan ställa till med är det egentligen bara viruskonstruktörens fantasi och kunskaper som begränsar. (Fåk, 1990, s.45)

På senare tid har trenderna inom den skadliga koden varit sån att dessa traditionella datavirus inte är lika vanliga som förr, samt att de som tidigare tillverkade dessa datavirus nu tillverkar andra former av skadlig kod (”Symantec: Datavirus allt svårare att hitta”, 2004).

2.3.1.1 Filvirus

Ett filvirus fäster sig självt vid en körbar programfil genom att lägga in sin egen kod i filen. Virusets kod ändras för det mesta på ett sådant sätt att ingreppet är svårupptäckt. När den smittade filen öppnas kan viruset fästa sig vid andra programfiler (”IDG: Datavirusens A till O”, 2003). Denna form av virus kallas också för parasiterande virus och smittar främst filer med ändelserna *.COM, *.EXE, *.DRV, *.DLL, *.BIN, *.OVL, *.SYS (”Trend Micro: Virus Primer”, 2005).

2.3.1.2 Bootsektorvirus

Detta avsnitt grundar sig på information från F-Secure (”Bootsektorvirus”, 2003). Ett bootsektorvirus lägger sig i datorns systemsektorer, vilka är speciella områden på en hårddisk eller en diskett som innehåller program som körs när datorn startas upp. Sektorerna är osynliga för vanliga program men är livsnödvändiga för datorns funktion. Bootsektorvirus ändrar den körbara koden i boot- eller partitionssektorn. Eftersom det inte finns mycket plats här (bara 512 byte) så måste virusen gömma koden någon annanstans på disken. Detta orsakar ibland problem när detta "annanstans" redan innehåller data som då skrivs över. Alla bootsektorvirus är minnesresidenta, vilket innebär att de lägger sig i datorns RAM-minne. När en smittad dator startas laddas bootvirusets kod in i minnet. Viruset skriver sen in sin kod till bootsektorn på det media som används på den infekterade datorn. Bootvirus förekommer relativt sällan nu för tiden och en orsak till det är att moderna datorers moderkort har inbyggt skydd mot dem samt att användandet av bootdisketter i det närmaste upphört.

2.3.1.3 Multidelsvirus

Är enligt Bishop (”Computer Security – Art and Science”, 2003) ett virus som är tvådelat och består av både ett filvirus och ett bootsektorvirus och därmed har det bägge virustypernas karaktäristiska drag och egenskaper.

2.3.1.4 Polymorfa virus

Detta avsnitt grundar sig på information från Forskning & framsteg (”olika typer av farlig kod”, 2003). Ett polymorft virus (som även kan vara ett så kallat blandat hot, om det blandas med exempelvis en trojan eller en mask) ändrar sig själv till att få många olika utseenden. Polymorfa virus förändrar sitt utseende varje gång det startas eller kopieras. På så sätt blir inget virus det andra likt och därmed är de svåra att hitta. Förändringen sker på olika sätt, men framför allt med hjälp av krypteringsteknik. Ofta förändras både krypterings- och dekrypteringskoden, vilket gör dem mycket svåra att finna då antivirusprogram bland annat arbetar utefter tekniken att jämföra kod med signaturer (redan kända exempel på skadlig kod). Detta går att jämföra med polisens register över fingeravtryck över kända brottslingar, om då en signatur (fingeravtryck) dyker upp som känns igen är detta ett virus eller någon annan form av skadlig kod. Men om den skadliga koden hela tiden till stor del ändrar utseende kan det naturligtvis vara svårt för antivirusprogrammen att känna igen den när det ser den.

2.3.1.5 Metamorfa virus

Detta avsnitt grundar sig på information från Securityfocus (”Detecting Complex Viruses”, 2004). Ett metamorft virus (som även kan vara ett så kallat blandat hot, om det blandas med exempelvis en trojan eller en mask) påminner i många avseenden om ett polymorft, men det

finns skillnader. För varje gång det startas och kopieras får det ett nytt utseende, och är på så vis mycket svårt att hitta för antivirusprogram. Dock bygger inte dess förändring på krypteringsteknik, utan den kommer från förändringar av den egna kroppen. En metod som viruset använder sig av för att ändra sitt utseende är att lägga till ”skräptecken” i den egna koden, exempelvis för att göra sig större eller mindre. Denna kod har ingenting med dess funktion att göra, utan tar bara plats. Att lägga till skräpkod i den egna koden gör också att den verkliga koden är svårare att finna och analysera. Dock finns det typer av metamorfa virus som verkligen byter ut sin egen kod till annan kod, och som trots detta får samma funktionalitet. En liknelse är att om du ska skriva 3X, så kan du antingen skriva det så eller X+X+X, summan är den samma trots att utseendet är olika. Orsaken till att viruset gör så här är, precis som för det polymorfa viruset, att göra det svårare för antivirusprogrammen att hitta det.

2.3.1.6 Stealthvirus

Detta avsnitt grundar sig på information från Forskning och framsteg (”Olika typer av farlig kod”, 2003). Själva termen stealth kommer av den teknik som används av några av den amerikanska militärens topphemliga flygplan, vilka är tillverkade för att inte synas på radar. Ett stealthvirus kan till exempel ta bort sig själv från filerna när ett antivirusprogram startas för att sedan infektera dem igen när programmet avslutas. Det finns även virus som ändrar så att de infekterade filerna verkar lika stora som innan de blev infekterade. För att undvika upptäckt undersöker ett stealthvirus om det aktuella datorsystemet har ett antivirusprogram igång och om viruset hittar ett sådant sänder det ut falska bilder av sig själv för att lura det. Ett stealthvirus är ett virus, som när det är "aktivt", gömmer de ändringar det gjort i filer och bootsektorer.

2.3.1.7 Makrovirus

Detta avsnitt grundar sig på information från Forskning och framsteg (”Olika typer av farlig kod”, 2003). Ett av de mer moderna exemplen på datavirus är makroviruset, som först dök upp i Microsofts Word och senare i Excel och andra makrobaserade program under den senare halvan av 90-talet. Dokumenten i Word är inte rena textdokument, utan de innehåller även en hel del körbar kod som talar om hur Word skall handskas med dem. Detta är tvunget, då virus inte kan spridas genom rena textdokument. Denna körbara kod kan, liksom all annan körbar kod, ersättas av skadlig kod. Makrokommandon skrivs i särskilda makrospråk och dessa kan med lätthet användas för att skapa farlig kod. Makrospråken i Word, Excel och andra Windows-program kan användas för att programmera om delar av operativsystemet. En stor del av alla virus är just makrovirus, vilket inte är så konstigt med tanke på hur populära Microsofts produkter är. Ett av de mest kända virusen, Melissa, är ett exempel på ett makrovirus som kom 1999.

2.3.1.8 Logisk bomb

Detta avsnitt grundar sig på information från Search Security (”What is a logic bomb?”, 2007). En logisk bomb är en form av skadlig kod som är skapad för att orsaka skada på en specifik dator eller ett nätverk. Själva namnet kommer av att den skadliga koden aktiveras, eller ”exploderar”, när vissa fördefinierade villkor uppfylls. Vanligen är detta villkor ett visst klockslag eller datum, men fantasin sätter gränserna. De kan också tillverkas så att de utlöses när ett visst villkor inte uppfylls. Det har exempelvis hänt att systemansvariga har lagt in en logisk bomb i systemet, som utlösts om han inte loggat in i systemet på en viss tid. I händelse

av att den systemansvarige skulle få sparken så skulle han därmed få sin hämnd på sin tidigare arbetsgivare. Logiska bomber utgörs ofta av virus eller trojaner, men de kan också vara andra former av skadlig kod.

2.4 Övriga exempel på skadlig kod

Under denna rubrik nämns de vanligaste typerna av skadlig kod som inte klassificeras som datavirus.

2.4.1 Mask

En mask är det allra första exemplet av skadlig kod, och de första maskarna skapades så tidigt som på 1970-talet, med andra ord långt innan de första datavirusen såg dagens ljus. Maskar har förmågan att sprida sig vidare utan mänsklig inverkan, till skillnad från virusen, som kräver en mänsklig aktivitet för att de ska spridas (Sörensen, 2004, s.71).
Ofta sprider sig maskarna vidare automatiskt genom att de utnyttjar säkerhetsluckor i datorernas operativsystem. Även diverse chatprogram och fildelningsprogram hjälper också till att sprida maskarna runt om i världen (”Symantec: datavirusen allt svårare att hitta”, 2004). Maskar strävar i högre grad efter att sprida sig vidare till andra datorer än vad datavirus gör. Därför är maskarna mycket farligare än datavirus i dagens moderna samhälle, då allt fler datorer är uppkopplade mot Internet samt sammankopplade i nätverk. En av de viktigaste skillnaderna mellan virus och maskar är spridningshastigheten, där maskarna är mycket snabbare och på så vis även farligare. Maskar är en mycket vanlig form av skadlig kod, vilket förklaras av att den är väldigt duktig på att sprida sig själv vidare. Maskar kombineras ofta med andra sorters skadlig kod, vanligen trojaner, för att skapa så kallade blandade hot (”Microsoft: Mask-Hoten-säkerhet”, 2005).

Enligt professor Eric Filiol (”Concepts and future threats in computer virology”, 2007) finns det i huvudsak tre olika sorter av maskar:

- I-maskar, eller enkla maskar, som sprider sig genom att utnyttja säkerhetshål i mjukvara. Exempel på sådana maskar är Sasser och Slammer.
- Macromaskar, som spelar på människors blåögdhet för att sprida sig vidare, något som kallas för ”social engineering”. Själva masken utgörs av ett bifogat dokument som skickas via e-mail. Ett exempel på denna form av mask är Melissa.
- Email-maskar, vilka också använder sig av ”social engineering” och som också sprids via e-mail, fast med den skillnaden att den bifogade filen är en körbar fil (.exe-fil i Windows-miljö). Exempel på denna form av maskar är Bagle och Netsky.

2.4.2 Trojansk häst

Precis som namnet antyder är detta något som utger sig för att vara en sak, men i själva verket är något annat, precis som den trojanska hästen i den klassiska grekiska historieskrivningen. Trojanska hästar har för det mesta namn som gör att de ser ut att vara spel, skärmsläckare eller andra ”bra” datorprogram. När de sedan används kan de ställa till med stor skada för användaren, till exempel radera filer, ändra på data, kopiera allt du skriver på datorn, stjäla lösenord eller andra känsliga uppgifter (”F & F: Olika typer av farlig kod”, 2003).
Trojaner finns i en mängd varianter, gemensamt för dem alla är att de installeras på din dator utan din vetskap. Det kan ske genom ett virus som kommer med e-posten eller när du besöker en webbsida innehållande ett elakt script. Men det allra vanligaste är att du själv luras att

installera den trojanska hästen genom att ladda ner ett annat program som har en eller flera trojaner inbäddade. Trojaner kan nämligen inte sprida sig på egen hand (”Göteborgsposten: Trojansk häst”, 2004).
En speciell form av trojanska hästar kallas för remote access trojans (RAT), eller backdoors, vilket innebär att de kan styras på avstånd av dess skapare eller öppna en bakdörr in i systemet. Skillnaden dessa två trojaner emellan är att bakdörren endast öppnar en port medan en remote access trojan skapar en server på systemet som skaparen av koden kan logga in på. Dessa Rats och backdoors är också närbesläktade med bots, och de definieras ofta som bots istället för trojaner (”Symantec: Internet Security Threat Report Volume XII”, 2007).
Så kallade ”keyloggers” eller ”passwordstealers” är också något som ofta anses vara trojaner. Dessa kan logga vad som skrivs på din dator eller stjäla dina lösenord, och är en farlig form av trojan. Andra former av trojaner är de som kallas för ”modular malicious code” eller ”downloaders” och som har den finurliga egenskapen att de kan ladda ner ytterligare kod från exempelvis Internet så att de får ökad funktionalitet. Dessa laddar ofta ner exakt den funktionalitet som de behöver för att genomföra ett specifikt uppdrag. Denna form av trojaner ökar just nu lavinartat (ibid.). Trojanska hästar är ofta ansedda att vara den allra farligaste formen av skadlig kod, och tillsammans med maskar utgör de ett så kallat blandat hot, vilket gör dem ännu farligare (”Symantec: Det nya hotet: blandade hot”, 2003). Många exempel på skadlig kod som egentligen är blandade hot klassificeras som trojaner, vilket kan vara intressant att notera vid den fortsatta läsningen av uppsatsen.

2.4.3 Spyware

Är en sorts skadlig kod som ofta ligger inbäddade i Trojaner och som har till uppgift att spionera på den som installerat dem, Spyware kallas ibland också för Adware som står för advertising supported software (”Webgate: Spyware”, 2003). Skillnaden dessa två emellan är att användaren känner till vad adware-programmen gör eftersom tillverkaren av programmet berättar exakt vad som görs medan spywaren är okänd och dess funktion och existens inte är uttalad från tillverkaren av programmet (ibid.). Spyware är vanligt förekommande i fildelningsprogram som exempelvis Kazaa, Grokster eller Limewire som på så vis utgör trojaner (”Geek news: KaZaA distributes trojan-ware”, 2002). Spyware är mycket vanligt, och finns i de allra flesta datorer som har använts för fildelning i någon form eller i de datorer där gratis programvara, freeware, installerats. För även om programmen är gratis för dig kostar de ändå oftast att tillverka, något som mindre nogräknade programtillverkare finansierar genom att ge programmen gratis till användaren men istället ta betalt av reklambyråerna som får informationen som spywaren samlar in om de som använder den (”Webgate: Spyware”, 2003).

En form av spyware, som ofta kallas för crimeware (men som ofta klassificeras under som trojaner), är det som kallas keyloggers eller passwordstealers. Dessa former av crimeware kan logga det som skrivs på den infekterade datorns tangentbord. Detta blir mer och mer vanligt, och kan naturligtvis vara mycket farligt, speciellt med avseende på lösenord samt information som handlar om kreditkort och så vidare (”Websense: Security Trends report 2004, 2005). Spyware upptäcks inte alltid av antivirusprogrammen, vilket kanske inte så konstigt, då det inte utgör ett fysiskt hot mot datorn.

En cookie är ett välkänt fenomen för de flesta som är ute på Internet ofta. Cookien laddas ner från en aktuell sida på Internet och lägger sig fysiskt på datorn där den samlar information om datorn och systemet. Dessa cookies skulle, om de skrevs annorlunda, fungera som Spyware

och samla in information om användaren och systemet som man inte kan räkna med (”Spychecker: What is Spyware”, 2005).

Fler och fler börjar idag radera sina cookies, eller så avaktiverar de cookies i sina webbläsare, detta innebär att företagen i allt högre utsträckning måste få in sin information på andra vis, vilket medför en ökning av Spyware (Fjordvang, 2002, s.106).

2.4.4 Rootkits

Är ett relativt modernt exempel på skadlig kod, och som sådant är det också intelligent och är svårt att upptäcka. Det har funnits ganska länge till Unix och Linux-system, men det är först relativt nyligen som rootkits började dyka upp till operativsystemet Windows. Ett rootkit är ett litet program, som förs in i datorn med hjälp av annan skadlig kod. Det kan inte transportera sig självt och inte heller kopiera sig självt. Det sinnrika med rootkits är att det ”lägger” sig mellan Windows källkod (kernel), och de övriga programmen. (”Symantec: Var kan ett rootkit gömma sig?”, 2006).
Det finns två generella former av rootkits: resistenta och de som lägger sig i datorns internminne eller i det virtuella minnet. De resistenta försvinner inte när systemet startar om, vilket däremot de som lägger sig i datorns internminne och i det virtuella minnet gör. De resistenta ligger därmed på någon annan form av media, exempelvis en hårddisk eller någon annan form av lagringsenhet. Ofta är de rootkits som ligger i internminnet de farligaste. Detta förklaras med att de är ännu svårare att hitta med antivirusprogram. Vidare startar många system inte om speciellt ofta, exempelvis servers (”SecurityFocus: Windows rootkits of 2005 part two”, 2005) . När ett antivirusprogram körs för att undersöka om skadlig kod finns på datorns hårddisk eller i datorns internminne, uppfattar rootkitet denna förfrågan och ger därefter programmet ett svar tillbaka vilket indikerar att ingen oönskad aktivitet förekommer på datorn (”Symantec: Var kan ett rootkit gömma sig?”, 2006). Med andra ord kan man säga att rootkitet öppnar upp ett system för att annan skadlig kod ska kunna husera omkring fritt i det.

2.4.5 Attackskript

Är program som ofta är skrivna av experter och som är speciellt utformade för att utnyttja säkerhetshål i operativsystem, exempelvis Windows. Angriparen använder sig av antingen Internet eller ett nätverk för att koppla upp sig mot sitt offer (Mcgraw & Morrisett, 2000). De som använder sig av attackskript är ofta amatörer som använder sig av ett redan skrivet verktyg som de använder sig av för att skapa oreda. Exempelvis kan ett skript användas för att slumpvis genomsöka Internet efter användare som har en viss svaghet som är speciellt intressant. När dessa användare väl är identifierade kan angriparen, ofta kallad script-kiddie, använda ett annat skript för att utnyttja svagheterna för att på så vis sprida skadlig kod på datorn som utgör målet för attacken (”Smart Computing: The Dark Side Of Scripts”, 2002).

2.4.6 Javaskript

Är en form av kod som är skriven i programmeringsspråket Java och som ligger inbäddade i hemsidor på Internet, och när sidan öppnas genom en javakompatibel webbläsare överförs koden till den egna datorn. Denna kod kan utgöras av skadlig kod, om hemsidan är utformad på det sättet. När koden sedan exekveras i webbläsarens ”Java virtual machine” körs den skadliga koden på datorn (”Sun Developer Network: Applets”, 2007). Detta kan alltså ske utan att man som användare behöver trycka på något eller ladda hem någon fil som man sedan

kör, vilket oftast är tvunget när det handlar om de traditionella typerna av skadlig kod. Då dessa program är skrivna i programmeringsspråket Java, vilket är plattformsoberoende, kan alla datorer oavsett operativsystem drabbas. Den skadliga koden kan exempelvis läggas in i en bild som visas på den aktuella sidan, eller så kan den läggas in i något så enkelt som en gästbok. Den skadliga koden läggs sällan upp på sidan av dess egentliga skapare, utan av hackers som kapar sidan för sina egna syften (”Sun Developer Network: Applets”, 2007).

2.4.7 ActiveX-kontroller innehållandes skadlig kod

Dessa är en form av skadlig kod som liknar Javaskript, men med vissa skillnader. Koden kan skrivas i flera olika programmeringsspråk, och kan egentligen påstås vara en uppsättning regler för hur tillämpningsprogram ska dela på information (”Paginas IT-ordbok: ActiveX-kontroller”, 2007). ActiveX-kontrollen ligger inbäddad i hemsidor på Internet, och laddas där ner automatiskt. Dessa kontroller kan då innehålla skadlig kod som kan köras på den egna datorn. Oftast är det inte hemsidans skapare som lagt dit denna skadliga kod, utan en hackare som kapat sidan. ActiveX-kontrollerna har full tillgång till operationssystemet Windows, vilket inte Javaskript har. Detta beror på att ActiveX ursprungligen är tillverkat av Microsoft. Trots att ActiveX-kontroller inte är plattformsoberoende såsom Javaskripten används trots allt Windows som operativsystem på drygt 90 % av alla datorer idag, vilket gör dessa smittade ActiveX-kontroller farliga (”Market Share: Operating system share for april 2007, 2007).

2.4.8 Bots

En bot är ett program som arbetar automatiskt som en agent för en användare eller ett annat program. Själva termen bots är en förkortning av robot. En Hacker kan förmedla dessa bots till sina mål på en rad olika sätt, och väl där infekterar programmet systemet. Ofta sker detta med hjälp av en trojansk häst (”Symantec: Crimeware: Bots”, 2007). Sedan väntar programmet på vidare instruktioner från hackern som på avstånd kan fjärrstyra programmet och på så vis manipulera själva boten samt det infekterade systemet. Den infekterade datorn kallas ofta för ”Zombie” och kan själv användas för att sprida smittan vidare till andra system. Den infekterade datorns ägare vet oftast inte om att hans dator är infekterat. Ett stort bot-nätverk kan vara uppbyggt av miljoner datorer runt om i världen (ibid.). Ofta är dessa på något sätt sammankopplade med nätverket IRC, vilket står för Internet Relay Chat. En av de mer vanligt förekommande skadorna som dessa bots kan göra är så kallade DDoS-attacker (distributed denial of service), vilket innebär att det har genomförts en överbelastningsattack mot en speciell IP-adress, vilket exempelvis kan vara ett företags server. Om attacken är framgångsrik och resulterar i att servern inte klarar av den utan slutar att fungera kan detta orsaka störningar som kan få stora ekonomiska konsekvenser (ibid.). Dessa bots används också ofta för att skicka ut spam, vilket är den elektroniska varianten av skräppost. Oftast är denna skräppost reklam för något som mottagaren inte har något intresse av eller så kan det användas för att sprida skadlig kod (”Symantec: How They Attack: Spam, 2007). Fram till runt år 2002 var det vanligast att spammeddelandena utgjorde reklam för mindre nogräknade företag och dess produkter, men efter det har spammeddelanden i allt högre utsträckning handlat om att det blivit ett lönsamt sätt för kriminella att ägna sig åt bedrägeri med eller utan hjälp av skadlig kod. Ett annat vanligt användningsområde för bots är att skicka iväg e-mail av phishing-typ. Phishing är en term vilken avser en olaglig metod för att försöka lura system och användare att lämna ut elektronisk information såsom kreditkortsnummer, lösenord eller annan användbar information. Själva termen kommer från ”password harvesting fishing” (”Wikipedia: Phishing”, 2007). Ett närliggande fenomen är så kallad Pharming, vilket innebär att någon använder skadlig kod för att utföra Phishing. Pharming går också under namnet

DNS poisoning och fungerar som så att det är ett Phishingbedrägeri som genomförs med hjälp av skadlig kod som pekar om datorn till en annan ipadress/webbadress utan att detta upptäcks av användaren. När så användaren skriver in exempelvis www.swedbank.se och ska betala sina räkningar, kanske användaren befinner sig på en helt annan, och mycket mer oärlig sida (”Wikipedia: Pharming”, 2008).

2.4.9 Blandade hot

Är en sorts kombination där flera olika virus eller varianter av skadlig kod blandas ihop till en mix som ger dem en kombination av de olika typernas egenskaper. Genom denna blandning av tekniker kan den skadliga koden konstrueras för att få vissa önskvärda egenskaper (”Forskning och framsteg: Olika typer av farlig kod”, 2003).

De blandade hoten kan exempelvis ofta automatiskt söka efter sårbarheter som kan användas för att ta sig in i ett system och för att sedan sprida sig vidare. Till motsats från virus som i hög grad förlitar sig på att människor ska sprida dem vidare, sköter ofta dessa blandade hot den saken själva genom att automatiskt skicka sig vidare via det angripna systemets adressbok. Genom att dessa blandade hot kan attackera flera punkter än de klassiska typerna av skadlig kod blir återställningen efter en attack extra svår. Två exempel på dessa blandade hot är Nimda samt CodeRed, vilka orsakat stora skador och kostnader runt om i världen (”Symantec: Det nya hotet: blandade hot”, 2003).

Just hur farliga dessa blandade hot anses vara märks bland annat i detta citat (ibid.):

”De tider då det var möjligt att skydda företagets nätverk mot maskar och virus med endast antivirusprogram är förbi. Idag är tyvärr traditionella antivirusskydd inte längre tillräckliga mot den nya sorts hot som Symantec kallar ”blandade hot”. Den snabba och omfattande skada som orsakas av dessa sofistikerade attacker kan dra upp kostnaden för affärsförlust, produktivitet, uppstädning och återskapning till miljonbelopp, till och med miljardbelopp världen över…Det befaras att blandade hot kommer bli allt vanligare, och att de kommer bli allt mer komplexa i framtiden”.

2.5 Tidigare forskning

När en uppsats som denna skrivs är det viktigt att undersöka vilken tidigare forskning som bedrivits inom det valda uppsatsområdet. Detta är bland annat viktigt då uppsatsen strävar efter att alstra ny och unik kunskap. Efter omfattande efterforskningar stod det mer och mer klart att det inte skrivits mycket om det valda ämnet tidigare. Det finns ett antal uppsatser på kandidat- och magisternivå i Sverige som handlar om skadlig kod, fast inte med fokus på framtidens skadliga kod. Bara en i Sverige funnen uppsats påminde i viss mån om denna. Den aktuella uppsatsen är en d-uppsats som heter ”Computer viruses: The threat today and the expected future”, och är skriven på Linköpings universitet (Li, 2003). Det är intressant att notera att handledaren till den uppsatsen var Viiveke Fåk, en av denna uppsats fyra respondenter.
Om man letar efter forskning på högre nivåer internationellt sett finns det inte mycket skrivet där heller att finna, vilket professor Eric Filiol (”Concepts and future threats in computer virology”, 2007) också anser. Han menar att det är tillverkarna av antivirusprogrammen som har det största ansvaret för att det forskas om framtidens skadliga kod, då skyddet mot den samma annars riskerar att halka efter, med katastrofala konsekvenser.

Tillverkarna av antivirusprogrammen är trots denna kritik några av de få som brukar sticka ut hakan och göra prognoser inför framtiden, men då handlar det oftast ”bara” om nästkommande år. Det påträffades dock ett antal artiklar och annan information där prognoser ställdes längre fram i framtiden
Med andra ord anser jag att denna uppsats bör har ett relativt högt värde genom sin originalitet och torde vara av intresse inom området.

2.6 Historik och trender

Då uppsatsens mål är att förutse hur skadlig kod kommer att fungera och verka i framtiden är dennas historik av stort intresse då den visar de trender som förekommit under åren.

År 1984 myntade Fred Cohen begreppet datavirus, som kom att bli den förhärskande termen för all skadlig kod för lång tid framöver (”Experiments with Computer Viruses", 1984).
Det första moderna exemplet på skadlig kod av betydelse var det så kallade Brain-viruset, som dök upp 1986. Det var ett Bootsektorvirus som infekterade disketter och gjorde dem oanvändbara. Det var också det första exemplet på ett stealthvirus, då det kunde göra sig självt osynligt. Skadlig kod hade förekommit tidigare, även till andra operativsystem, men dessa var av mindre betydelse (”Exn: The history of computer viruses – a timeline”, 2007). I början av den skadliga kodens historia skrevs den för att orsaka förstörelse samt för att göra dess skapare känd. På senare år har den skadliga koden snarare skrivits för att dess skapare ska dra ekonomiska eller andra fördelar av den.

År 1986 kom PC-write, som troligen var den första trojanska hästen. Hästen utgav sig för att vara en ny version av det mycket populära shareware-programmet med samma namn som användes som ordbehandlare. När den trojanska hästen kördes formaterades hårddisken (“Smart Computing: Tales of Trojan horses”, 2003). Alla dessa tidiga former av skadlig kod spred sig via disketter, och det var först under 1990-talet som Internet kom att ta över som det främsta spridningssättet för den skadliga koden.

1987 kom de första exemplen på skadlig kod som kunde infektera annat än bootsektorn. Bland annat upptäcktes Lehigh-viruset som var det första exemplet på skadlig kod som var minnesresident, vilket innebar att det kunde lägga sig i datorns RAM-minne och därifrån göra skada. Samma år dök Jerusalem-viruset upp, och liksom Lehigh-viruset var det minnesresident (”Exn: The history of computer viruses – a timeline”, 2007).

1987/88 skrevs det första antivirusprogrammet, vilket kunde ta bort Brain-viruset och även göra disketterna immuna mot framtida angrepp från viruset. 1988 dök Cascade-viruset upp, vilket var det första viruset som var krypterat och på så vis kunde det dölja sig mer effektivt. Detta virus var ett av de vanligaste förekommande från sin tillkomst till några år in på 1990-talet (”F-Secure Virus Descriptions: Cascade”, 2000). Lehigh-viruset, Jerusalem-viruset samt Cascade-viruset var alla exempel på filvirus. Ett ännu större steg togs i slutet av 1988 då den så kallade ”Morris-masken” dök upp och terroriserade datorer genom spridning över Internet. Masken drabbade Unix-system och var det första exemplet på hur effektivt Internet kan sprida skadlig kod så att många användare drabbas. Masken drabbade sex tusen datorer, vilket uppskattningsvis utgjorde 10 % av alla datorer som vid den tidpunkten befann sig på Internet. Kostnaden för de skador masken gjorde uppskattades vara någonstans mellan 10-100 miljoner dollar (”Wikipedia: Morris Worm”, 2007).

1989 startade de första antivirusföretagen sin verksamhet (”Viruslist: History of Malware”, 2004). De första antivirusprogrammen var skrivna för att lägga märke till program eller filer som betedde sig misstänkt och då varna användaren och fråga den om vilken åtgärd som skulle vidtas. Denna metod används fortfarande i dagens antivirusprogram. Successivt växte sedan användandet av signaturer fram (vilket ju förutsätter att det finns signaturer i databasen att arbeta mot) och användandet av heuristik, vilket innebär att antivirusprogrammet undersöker och i vissa fall provkör koden innan den körs på riktigt. Heuristik är alltså en metod som antivirusprogrammen använder sig av för att hitta hittills okänd skadlig kod (”Viruslist: History of Malware”, 2004).
Samma år dök viruset ”Dark Avenger” upp, som var det första exemplet på skadlig kod som var designat så att det infekterade ett system långsamt. Anledningen till detta var att det skulle undgå upptäckt, och om filer säkerhetskopierades skulle dessa filer förhoppningsvis också vara smittade (“Exn: The history of computer viruses – A timeline).

1990 började flera olika antivirusprogram säljas och det började dyka upp skadlig kod som kombinerade flera olika traditionella egenskaper, exempelvis multidelsvirus kombinerade med polymorfa virus (ibid.). Samma år skapades EICAR (European Institute for Computer Antivirus Research) som än idag är ansett som en av de mest respektabla antivirusorganisationerna (”Viruslist: History of Malware”, 2004). Detta år dök Windows 3.0 upp, vilket därefter successivt tog över som det vanligaste operativsystemet för PC-baserade datorer och därmed efter hand blev den nya plattformen för skaparna av skadlig kod att smitta. Innan Windows 3.0 infördes användes främst operativsystemen MS-dos samt de tidigare formerna av Windows, version 2.x (”Wikipedia: Windows 3.0”, 2007).

1991 dök ”Tequila-viruset” upp, vilket var ett Stealthvirus, ett polymorft virus samt ett multidelsvirus i ett (”Exn: The history of computer viruses – A timeline”, 2007). Tequila-viruset var med andra ord det första verkliga exemplet på ett blandat hot. Antalet exempel på skadlig kod ökade så saktliga, och 1991 fanns det över tre hundra kända former av skadlig kod (”Viruslist: History of Malware”, 2004).

1992 släpptes program som kunde användas av i stort sett vem som helst för att skapa egen skadlig kod. Detta medförde att tillväxten av fientlig kod accelererade betydligt snabbare än tidigare. Dessa program, som kallas toolkits, blir idag allt vanligare (”Viruslist: History of Malware”, 2004.).

1993 dök skadlig kod upp som använde sig av ny teknik för att penetrera system, infektera filer, förstöra data samt undgå upptäckt från antivirusprogrammen (”Viruslist: History of Malware”, 2004)

1994 började cd-spelare i datorerna bli vanligt förekommande, vilket gav den skadliga koden ännu ett flyttbart medium att spridas på: cd-skivan. Fram till att Windows 95 lanserades var Bootsektorvirus som kunde drabba MS-dos den vanligaste formen av skadlig kod. Detta ändrades 1995.

1995 förändrades datoranvändandet i grunden i och med att Windows 95 gav den stora massan möjlighet att ge sig ut och surfa på Internet samt att på ett relativt enkelt sätt koppla samman flera datorer i nätverk. Denna förändring gav den skadliga koden mycket större möjligheter då den nu fick många fler sammanhängande mål. Eftersom Microsoft Office blev så otroligt populärt blev detta ett tacksamt mål för den skadliga koden. 1995 blev därmed året då den första skadliga koden skrevs för Windows 95, och då dök även de första Macrovirusen

upp (”Exn: The history of computer viruses – A timeline”, 2007). I mitten av 1990-talet började Microsoft Windows ta allt större marknadsandelar som operativsystem, och de flesta exemplen på skadlig kod började skrivas uteslutande för att drabba den plattformen (”Viruslist: History of Malware”, 2004).

1996 var Macroviruset Concept den vanligaste formen av skadlig kod. Viruset angrep Microsoft Word dokument, och kan anses vara det första virus som kunde fungera i flera olika miljöer då det fungerade i Microsoft Word 6 och 7, samt för Word for Macintosh 6 samt både på Windows 95 och Windows NT (”F-Secure Virus Descriptions: Concept”, 2003). Med andra ord var den mest förekommande skadliga koden inte längre ett Bootsektorvirus som spreds via disketter, utan ett Macrovirus som spreds via Internet samt disketter. Samma år skrevs det första viruset till Windows 95, Boza. Detta år drabbades Microsofts tidigare version av Windows, 3.xx, av sin första virusepidemi. Nu släpptes flera verktyg för tillverkning av makrovirus, som nästan vem som helst kunde använda. 1996 kan man säga blev året då tillverkarna av skadlig kod angrep den nya plattformen Windows 95 samt Microsoft Office, som nu var nästan var mans egendom (”Viruslist: History of Malware”, 2004).

1997 kom det första makroviruset ut som kunde sprida sig vidare via e-mail, Sharefun. Detta virus blev det första att använda sig av detta sätt för spridning. Samma år dök det första exemplet på en mask som spred sig via FTP upp (ibid.).

1998 var året då Microsoft Windows 98 lanserades och efterträdde Windows 95. Successivt blev Windows 98 allt vanligare, och till sist tog det över som det dominerande operativsystemet. I takt med detta bytte sedan skaparna av skadlig kod mål till Windows 98 istället. Detta år dök flera trojanska hästar upp som kunde stjäla lösenord. Samma år dök det upp skadlig kod som utnyttjade säkerhetshål för att ge hackaren tillgång till det attackerade systemet. Samma år dök också de första exemplen på Javavirus och Scriptvirus upp. (”Viruslist: History of Malware”, 2004)

1999 kom ett exempel på hur datorutvecklingen gett den skadliga koden nya möjligheter då masken Melissa, som även är ett Macrovirus, dök upp. Bara några timmar efter att det först upptäckts hade det spritt sig över hela jordklotet, snabbare än någon tidigare känd form av skadlig kod. Det blev därmed det första exemplet på skadlig kod som spred sig globalt. Viruset spred sig genom att automatiskt skicka sig vidare via e-mail till andra system (”F-Secure Virus Descriptions: Melissa”, 2003). Viruset var skrivet för Microsoft Word och krävde att systemet även hade Microsoft Outlook som e-mailprogram för att det skulle sprida sig vidare. Denna programkonfiguration användes av många system, och därför fick viruset stor och snabb spridning. Melissa var ett bra exempel på att tillverkarna av skadlig kod nu inte längre var ute efter att göra stor skada på få system, utan att de numera satsade på mycket snabb spridning samt att drabba så många system som möjligt. Den nya tekniken gav dessa möjligheter. Genom att Melissa dök upp blev även den ekonomiska aspekten på den skadliga kodens verkningar en stor fråga. Melissa beräknas ha orsakat skador för ungefär 1 miljard dollar, vilket då var ett nytt rekord (”Reuters: The cost of Code Red”, 2001).

Det var efter Melissa som många datoranvändare skaffade sig antivirusprogram, och detta gällde i ännu högre utsträckning för myndigheter och företag som efter incidenten med Melissa tog riskerna på betydligt större allvar än tidigare. Efter Melissa kom flera liknande typer av skadlig kod, exempelvis Love letter och Anna Kornikova som bar namn som uppmuntrade användare att öppna e-post utan försiktighet. När väl e-posten hade öppnats

aktiverades den skadliga koden och skickade sig vidare automatiskt till andra system som fanns i e-mailprogrammets adresslista (”Antivirus World: History of computer viruses”, 2006). 1999 kom ännu en nyhet då maskarna Bubbleboy och Kakeworm dök upp. Dessa maskar kunde spridas via e-post utan att det behövde finnas någon attacherad fil i e-posten. Samma år tog den skadliga koden ännu ett steg framåt i och med den Babyloniska masken som hela tiden undersökte om det fanns en nyare version av sig själv utlagd på Internet. Om det gjorde det laddade masken ner uppdateringen och fortsatte sitt liv i sin modernare och möjligen mer destruktiva form (”Antivirus World: History of computer viruses”, 2006). Denna metod har senare kommit att användas av flera olika exempel på skadlig kod som ofta kallas för ”modular malicious code” eller ”downloaders” och som ofta utgörs av trojaner. Dessa har specialegenskapen att de själva kan uppdatera sig själva genom att ladda ner annan skadlig kod, eller moduler, från Internet eller från nätverk. Denna nedladdning kan då ge den skadliga koden ny funktionalitet (”Computer Crime Research Center: Hackers shift targets in 2006”, 2006).

År 2000 lanserades Microsoft Windows 2000 samt Microsoft Windows ME, och dessa blev efter hand allt mer använda operativsystem. Även om ME aldrig fick så stor marknadsandel, så tog Windows 2000 desto större, och det gick efter något år förbi Windows 98 i marknadsandel och var därefter det näst vanligaste operativsystemet efter Windows XP tills Microsoft Windows Vista tog över andraplatsen år 2007 (”Market share: Operating system market share for 2004-2007”, 2007). Då åtminstone Windows 2000 kom att bli ett vanligt förekommande operativsystem skrevs därmed större andel skadlig kod till det.
Detta var för övrigt ett år då den skadliga koden tog flera steg framåt i utvecklingen. Först kom det enormt skadliga Loveletter-viruset, som också är känt under namnet LoveBug eller ILoveYou. Detta var ett Scriptvirus som skickar sig vidare till användare i adressboken, samt smittar filer på den aktuella datorn. Senare försöker viruset ladda ner en fil från Internet som innehåller ett program som är utformat för att stjäla lösenord från den aktuella datorn. Efter att lösenorden är stulna skickas de vidare via e-mail till virus-skaparen (”Viruzlist: Loveletter, 2000). Loveletter var den mest förekommande typen av skadlig kod detta år, och därmed tog Scriptvirusen över förstaplatsen från Makrovirusen, som innehaft ledningen sedan 1996 (”Viruslist: History of Malware”, 2004). Loveletter-viruset slog detta år Melissas rekord vad gäller kostnader som specifik skadlig kod orsakat. Skadorna som Loveletter-viruset orsakade uppskattas vara någonstans mellan 9 Miljarder dollar till 15 Miljarder dollar (”Reuters: The cost of Code Red”, 2001).

Samma år kom ännu en nyhet då masken Jer var upplagd på flera hemsidor på Internet. Efter att hemsidan öppnades drog Script-program igång och för första gången kunde skadlig kod smittas bara genom att en användare öppnade en sida på Internet. Jer visade en ny trend inom skadlig kod, nämligen att en mask placerades på en hemsida och sedan lockas mängder med användare dit. Tillverkaren av den skadliga koden räknar med att om tillräckligt många människor besöker sidan så kommer ett stort antal göra bort sig och bli smittade (ibid.). Samma år dök skadlig kod upp som kunde smitta andra former av enheter. Trojanen Liberty kunde smitta Palm Pilotes och dess operativsystem PalmOS. Samma år dök även ett klassiskt virus upp som också kunde drabba PalmOS. Samma år kom även det första exemplet på skadlig kod som kunde drabba mobiltelefoner, Timofonica. Samma år visades det med all önskvärd tydlighet att e-post var det medium som var bäst lämpat för att sprida skadlig kod. Uppskattningsvis 85 % av alla registrerade infektioner detta år spreds via e-post (Ibid.). Samma år dök också flera olika former av skadlig kod upp till operativsystemet Linux, och antalet kända virus till det operativsystemet sjudubblades detta år.

2001 lanserade Microsoft sitt Windows XP, som år 2007, fortfarande är det vanligaste av alla operativsystemen för PC-datorer (”Market share: Operating system market share for november 2007”, 2007). Det dröjde bara något år innan XP blev det mest använda operativsystemet. I takt med att det snabbt blev det mest populära operativsystemet skrevs det därmed mer och mer skadlig kod specifikt för det operativsystemet. Windows XP var det första operativsystemet från Microsoft som kom med en inbyggd brandvägg, som hjälper till att övervaka och kontrollera trafik in och ut ur datorn och på så vis tillåta trafiken att äga rum, eller att förbjuda den samma. Dock var denna brandvägg inte riktigt färdigutvecklad 2001, utan det dröjde till Microsoft släppte sin uppdatering, servicepack 2, år 2004 innan den blev till någon större hjälp för gemene man (”Wikipedia: Windows XP”, 2008). En brandvägg är ett relativt effektivt verktyg för att motarbeta skaparna av den skadliga koden att ta sig in i datorn samt att öppna ”backdoors” in i systemet. Det fanns brandväggar även tidigare, men dessa var då inte inbyggda i operativsystemet, utan användarna var tvungna att köpa dessa program från något annat företag.
Detta år blev den fientliga koden bättre på att utnyttja säkerhetshål. De nya maskarna CodeRed, Nimda i kombination med nya varianter på de äldre maskarna Love letter samt SirCam var de vanligaste formerna av skadlig kod detta år. Code Red orsakade skador runt om i världen för uppskattningsvis 2.6 Miljarder dollar och drabbade över en miljon system (Out-law: Code red costs $2.6 billion worldwide”, 2001).
Många av de moderna maskarna spred sig nu helt utan mänsklig påverkan, och siktade in sig på säkerhetshål i nätverk, system och program. Innan år 2001 var användarna tvungna att åtminstone göra någonting för att drabbas, något som nu inte längre behövdes.
Uppskattningsvis 55 % av all upptäckt skadlig kod detta år utnyttjade säkerhetshål av någon form (”Viruslist: History of Malware”, 2004). Masken SirCam stod själv för nästan 60 % av de totala förekomsterna av skadlig kod detta år (”Virus Bulletin: Virus Prevalence”, 2007).
Samma år dök de första exemplen på skadlig kod upp som kunde spridas via direktmeddelanden genom exempelvis chatt-programmen ICQ och MSN Messenger (”Viruslist: History of Malware”, 2004).
Fortfarande var trenden att skaparna av skadlig kod tillverkade sin kod för att drabba allt och alla, med liten urskiljning. Dock var denna trend nu på upphällningen, och framöver blev den skadliga koden mer utstuderad och inriktade sig mer på att drabba specifika mål såsom någon speciell organisation. Den skadliga koden började också i högre utsträckning fokusera på bedrägerier, stöld av data och kriminalitet (“Symantec Internet Security Report: Trends for January to June 2006”, 2006).

2002 visade sig bli ett relativt lugnt år då förekomsterna av fientlig kod blev färre och mindre kostsamma än på flera år. Dock märktes en förändring i det avseendet att betydligt fler attacker än tidigare gjordes med avsikten att lura till sig pengar. Den skadliga koden blev mer fokuserad på att stjäla användares lösenord, hemligstämplad information, företagshemligheter med mera (”Viruslist: History of Malware”, 2004).
En annan nyhet var att maskar som spred sig med e-mail numera kunde skicka sig själva vidare via de SMTP-servrar som de smittade systemen använde sig av. På detta vis behövde inte maskarna använda sig av de e-mailprogram som var inbyggda i måldatorerna och som antivirusprogrammen började bli bättre på att övervaka. Trenden att i högre grad utnyttja säkerhetshål, vilken inleddes 2001, fortsatte dock i ännu högre utsträckning 2002 (ibid.).
Det mest kända exemplet på skadlig kod detta år var masken Klez, som nästan stod för hälften av förekomsterna av skadlig kod detta år (”Virus Bulletin: Virus Prevalence”, 2007). En trend som dök upp detta år var att det inte längre var ett fåtal exempel på skadlig kod som orsakade nästan all skada runt om i världen. Nu hade det istället blivit betydligt flera exempel på

skadlig kod som delade på att leverera den totala skadan (”Viruslist: History of Malware”, 2004).

Detta år skedde en enorm bot-attack mot de tretton rootservrar som används för att styra DNS-trafiken på Internet. Denna attack fick följden att sju av servrarna tillfälligt slutade fungera tillfredställande. Detta fick dock ingen stor effekt för Internet i stort, då trafiken tillfälligt dirigerades om (”Enterprise Networking Planet: DNSSEC: Security for Essential Network Services”, 2003).

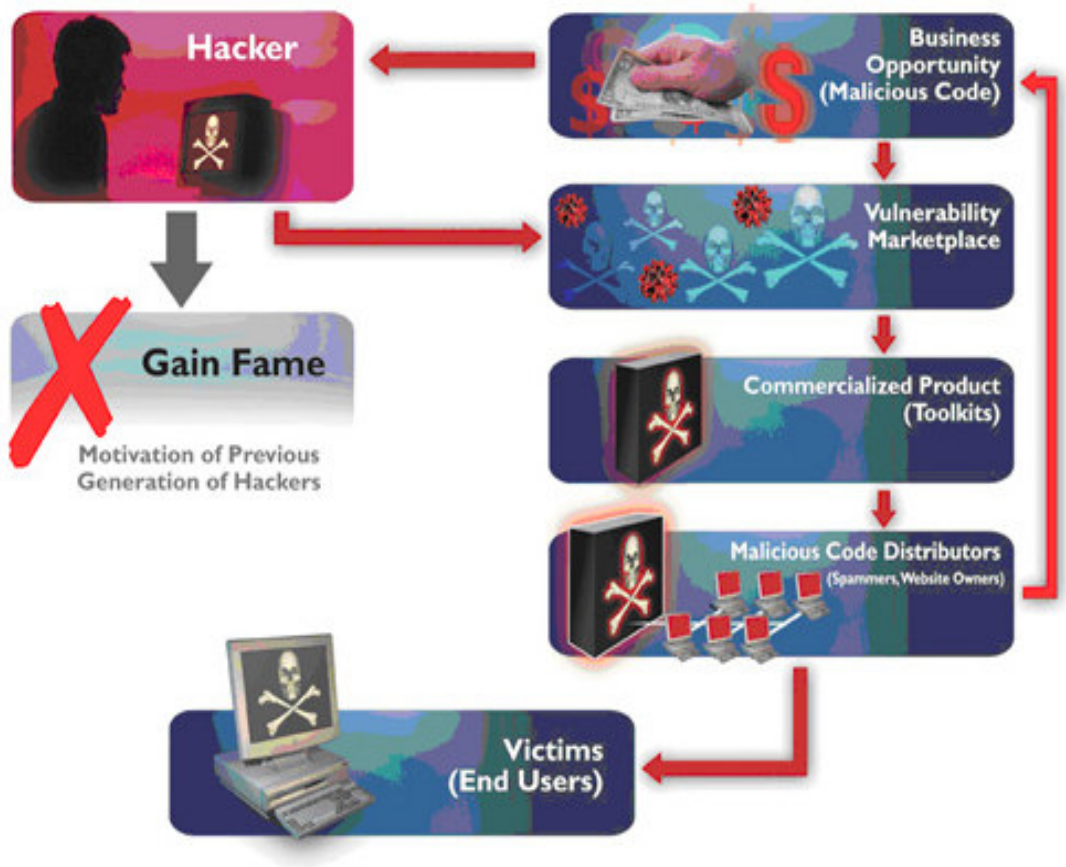
2003 skedde två större epidemier då de självförökande maskarna Slammer och Lovesan spreds över världen. Maskarna använde sig av säkerhetshål i Microsoft Windows för att kunna föröka sig. Detta år var också ett viktigt år vad gäller omfattande epidemier för maskar som spreds med e-post, vilka Ganda och Avron var två exempel på.
Det största utbrottet gjorde sig e-mail masken Sobig skyldig till då den dök upp i vart tjugonde skickat e-mail när den stod på sin topp (”Viruslist: History of Malware”, 2004).
En ny trend skedde detta år då Trojaner tillverkades med avsikten att skicka mängder med spam. Trojanerna tog det attackerade systemet i besittning och sedan skickades mängder med spam ut från systemet utan att dess ägare märkte det. Detta var också det år då Trojaner tog över som den näst mest vanliga formen av skadlig kod efter maskarna. Tidigare hade de klassiska formerna av virus varit näst vanligast, men nu tog alltså Trojanerna över.

2004 släppte Microsoft service pack 2 till sitt Windows XP, vilket innebar att operativsystemet därmed fick en betydligt bättre brandvägg än tidigare (”Wikipedia: Windows XP”, 2008).

Detta år blev phishing mycket vanligare, vilket innebar att fler användare och flera system drabbades av olagliga metoder som avsåg att få tag i elektronisk information såsom kreditkortsnummer, lösenord eller annan användbar information (”Wikipedia: Phishing”, 2007). En Phishing-metod är att skadlig kod, exempelvis en Trojan, installeras på målsystemet. Trojanen kan då exempelvis logga det som skrivs på systemets tangentbord, och senare skicka informationen vidare till dem som har intresse av det (”Websense: Security trends report 2004”, 2005). Andra metoder kan vara att exempelvis använda säkerhetshål som kan finnas i exempelvis Internet Explorer (”Wikipedia: Phishing”, 2007).
Detta år blev det även vanligare att skadlig kod smittade via att användare gick in på smittade hemsidor på Internet.
Trojanerna var vanligt förekommande detta år, och ofta fungerade de i kombination med maskar, vilket gjorde dem till blandade hot. Trojanerna användes ofta för att maskarna skulle ta sig in i systemen och sedan infektera det och sprida sig vidare. Detta år använde sig skaparna av den skadliga koden sig av peer-to-peer nätverken (exempelvis DC++ eller Kazaa) samt av direktmeddelanden i högre grad än tidigare för att sprida den skadliga koden vidare. Framförallt skedde den skadliga kodens framsteg detta år inom hur den spred sig och infekterade system (”Websense: Security trends report 2004”, 2005). Maskarna dominerade även detta år topplistorna över den mest förekommande skadliga koden totalt sett. Viruset Netsky dominerade listan totalt, genom att uppskattningsvis stå för 73 % av all skada som skadlig kod gjorde detta år (”Virus Bulletin: Virus Prevalence”, 2004).

2005 karaktäriserades av det faktum att skaparna av skadlig kod i ännu högre grad än tidigare inriktade sig på att tjäna pengar på sin kod. De brottslingar som gjorde på detta vis var duktiga på att finna nya sätt att sprida sin kod och utnyttja gamla säkerhetshål eller finna/skapa nya. Brottslingarna blev snabbare, och hann ofta utnyttja säkerhetshålen innan de hann åtgärdas.

Framförallt var detta tydligt när det gällde säkerhetshål i operativsystem samt webbläsare. Det medförde att den skadliga koden som inte hade dessa avsikter minskade i omfattning (“Symantec Internet Security Report: Trends for January to June 2005”, 2005). Dessutom var antalet säkerhetshål det största uppmätta sedan 1998 .(“Symantec Internet Security Report: Trends for July to december 2005”, 2006). Detta år blev det mycket vanligare att smittas bara genom att gå in på en hemsida som var infekterad med skadlig kod (”Websense: Security trends report 2005”, 2006). Phishing-försöken ökade med 44 % detta år, vilket var en ganska kraftig höjning (“Symantec Internet Security Report: Trends for July to december 2005”, 2006). Detta år var masken Sober det mest skadliga exemplet på skadlig kod. Den stod ensam för uppskattningsvis 92 % av alla infektioner (”Virus Bulletin: Virus Prevalence”, 2007).
Nu skapades majoriteten av den skadliga koden med avsikten att ge sin skapare ekonomisk vinning, vilket inte varit fallet tidigare då ära och rykte samt självhävdelsebehov varit de största drivkrafterna, Skillnaden från hur hackare arbetade förr och nu visas nedan i **figur 2**:



Figur 2. Figuren visar hur hackarnas drivkrafter förändrats över tiden (”IP communications: Malicious code for sale”, 2006).

Detta år ökade antalet nya virus och maskar som kunde infektera Windows-plattformen dramatiskt då Symantec fann närmare 22000 nya varianter av dessa. Detta innebär att antalet kända exempel på skadlig kod till Windows-plattformen mer än fördubblades detta år (“Symantec Internet Security Report: Trends for july to december 2005”, 2006). Vidare dök det detta år upp flera exempel på skadlig kod som var utformad för att drabba mobila enheter såsom exempelvis mobiltelefoner och dess vanligaste operativsystem, Sybian (“Symantec Internet Security Report: Trends for January to June 2005”, 2005). Den skadliga koden

fortsatte drabba plattformar som tidigare inte varit utsatta för den. Ett exempel på detta är spelkonsollen Playstation (“Symantec Internet Security Report: Trends for July to december 2005”, 2006).

En stor sak som hände detta år var att Sony BMG Music Entertainment satte ett kopieringsskydd på de musikskivor som såldes med avsikten att öka skivförsäljningen. Dock motsvarade den programvara som installerades av kopieringsskyddet ett Rootkit. Det orsakade inga direkta skador, men det var omöjligt att upptäcka på de datorer som det installerats på. Att sedan många datorer runt om i världen var infekterade med detta rootkit utnyttjades av skadlig kod som skapats för att dra nytta av de effekter som rootkitet hade på systemen. Opinionen kritiserade Sony starkt, och till sist återkallades alla skivor som sålts med kopieringsskyddet och Sony släppte flera program som skulle radera rootkitet från de drabbade systemen, något som till att börja med inte fungerade tillfredställande (”Wikipedia: 2005 Sony BMG CD copy prevention scandal”, 2007).

2006 lanserade Microsoft sitt Windows Vista, som togs emot ganska ljumt av datoranvändarna. De allra flesta bytte inte bort sitt Windows XP och Vista fick därmed en ganska blygsam procentuell andel av operativsystemmarknaden detta introduktionsår.

Detta år blev skaparna av skadlig kod mer organiserade och ännu mer sofistikerade. Aldrig tidigare hade det skickats så mycket e-mail med skräpinnehåll, spam. Enligt beräkningar gjorda i oktober 2006 var så mycket som 60 % av all e-mail som skickades spam (“Symantec Internet Security Report: Trends for July to december 2006”, 2007). En säker indikator på vilken nivå den illegala verksamheten på Internet befinner sig är mängden spam, och den ses därmed ofta som en sorts barometer som säger en hel del om hur säkerhetsnivån på Internet är. Samtidigt ansågs det att det, vid varje given tidpunkt, fanns mellan tre och fyra miljoner bots aktiva på Internet som enbart ägnade sig åt att skicka ut spam (ibid.). Sedan fanns det uppskattningsvis ett antal miljoner andra bots som kunde användas för distributed denial-of-service attacker. Vidare började skaparna av den skadliga koden att skapa den som yrke. Det upptäcktes nämligen att den största delen av brottsligheten skedde under den vanliga arbetsveckan, för att avta drastiskt under helgen. I slutet av 2006 slogs det rekord i funna antal webbplatser som ägnade sig åt phishing. Drygt 37000 sådana webbplatser hittades av den så kallade “anti-phishing Working Group” som är en koalition av företag som strävar att motarbeta bedrägerierna online. Detta var en ökning med 12000 webbplatser från augusti, eller nio gånger så mycket som året innan vid samma tidpunkt (”Washington post: Cybercrime hits the big time in 2006, 2006).

Samma år fortsatte antalet funna säkerhetshål att öka till en ny rekordnivå. Sju av tio säkerhetshål upptäcktes i applikationer som hade anknytning till Internet. Detta hänger samman med den omfattande ökningen av de kallade Zero-day attackerna som skedde detta år (“Symantec Internet Security Report: Trends for July to december 2006”, 2007).
En Zero-day attack innebär att skaparen av den skadliga koden skriver den för att utnyttja ett säkerhetshål som ingen officiellt känner till. Dessa säkerhetshål kallas för ”Zero-day vulnerabilities”. Detta innebär att tillverkaren av programvaran inte har släppt någon uppdatering till densamma som täpper igen det aktuella säkerhetshålet. En tillverkare av skadlig kod som kan hitta ett sådant här säkerhetshål kan därmed husera omkring fritt på ett stort antal system runt om i världen med hjälp av sin skadliga kod innan tillverkaren av programvaran släpper sin uppdatering som åtgärdar säkerhetshålet (”About.com: Zero Day Exploits- Holy Grail Of The Malicious Hacker”, 2007). Detta innebär att tillverkarna av den skadliga koden blivit bättre på att själva finna och utnyttja säkerhetshål än tidigare. Detta

fenomen är farligt då antivirusprogrammen kan ha mycket svårt att finna dessa intrång då den skadliga koden som används möjligen är helt ny, och därmed är inte antivirusprogrammen uppdaterade med de definitioner som krävs för att upptäcka dem (”About.com: Zero Day Exploits- Holy Grail Of The Malicious Hacker”, 2007). Ofta kallas detta också enbart för exploits när skadlig kod används för att utnyttja säkerhetshål i programvara. Denna tid som en programvara varit utsatt för risk, kallas för ”window of exposure” och mäts av exempelvis Symantec, vilket inkluderar denna i sin Internet security threat report.

Detta år blev det betydligt vanligare att den skadliga koden var inriktad på att stjäla specifik information från specifika företag och att denna information användes för ekonomisk vinning. Inte sällan var det då Zero-day vulnerabilities som angreps (“Search Security: Data thieves thrive on zero-day flaws”, 2007).
38 av de 50 vanligast förekommande exemplen av skadlig kod detta år var maskar, vilket utgör 75 % (”Virus Bulletin: Virus Prevalence”, 2007).

Faktorer som har styrt den skadliga kodens utveckling under åren är bland annat teknikutvecklingen som gett den nya möjligheter. En annan faktor är att programmeringsspråken har blivit mer och mer utvecklade och därmed gett skaparna av den skadliga koden ökade möjligheter. Från början drevs skaparna av den skadliga koden av personliga drivkrafter som exempelvis rykte och ära, men successivt har detta övergått till att i högre och högre grad utgöras av ekonomiska drivkrafter. Idag är det främst dessa ekonomiska drivkrafter som gör att den skadliga koden hela tiden utvecklas till nya nivåer.

2.6.1 Förekomsten av skadlig kod genom åren

Eftersom en av forskningsfrågorna är att undersöka om det är troligt att skadlig kod kommer att bli mer eller mindre förekommande i framtiden är det viktigt att se hur det sett ut historiskt sett.

Att fastslå hur många incidenter av skadlig kod som inträffar under ett specifikt år är mycket svårt, då det är sannolikt att långt från alla incidenter rapporteras och bekräftas. Vidare kanske inrapporteringen fungerar bättre nu för tiden än vilket var fallet tidigare. Dock anser jag att siffrorna nedan ändå ger en fingervisning om den ungefärliga verkligheten. Jag har valt att använda mig av perioden 1995-2006 i min redovisning av de historiska siffrorna. Denna medvetna avgränsning beror på att det i stort sett inte förekom någon skadlig kod alls innan år 1995 samt att siffrorna för år 2007 istället är placerade under kapitel 2.6.

I **diagram 1** på nästa sida syns den statistik som Virus Bulletin (”Virus Prevalence”, 2007) kommit fram till och som bygger på inrapporterade och bekräftade fall av förekomster. Eftersom diagrammet kan vara svårt att överblicka då återfinns källdatan till diagrammet i bilaga 2.

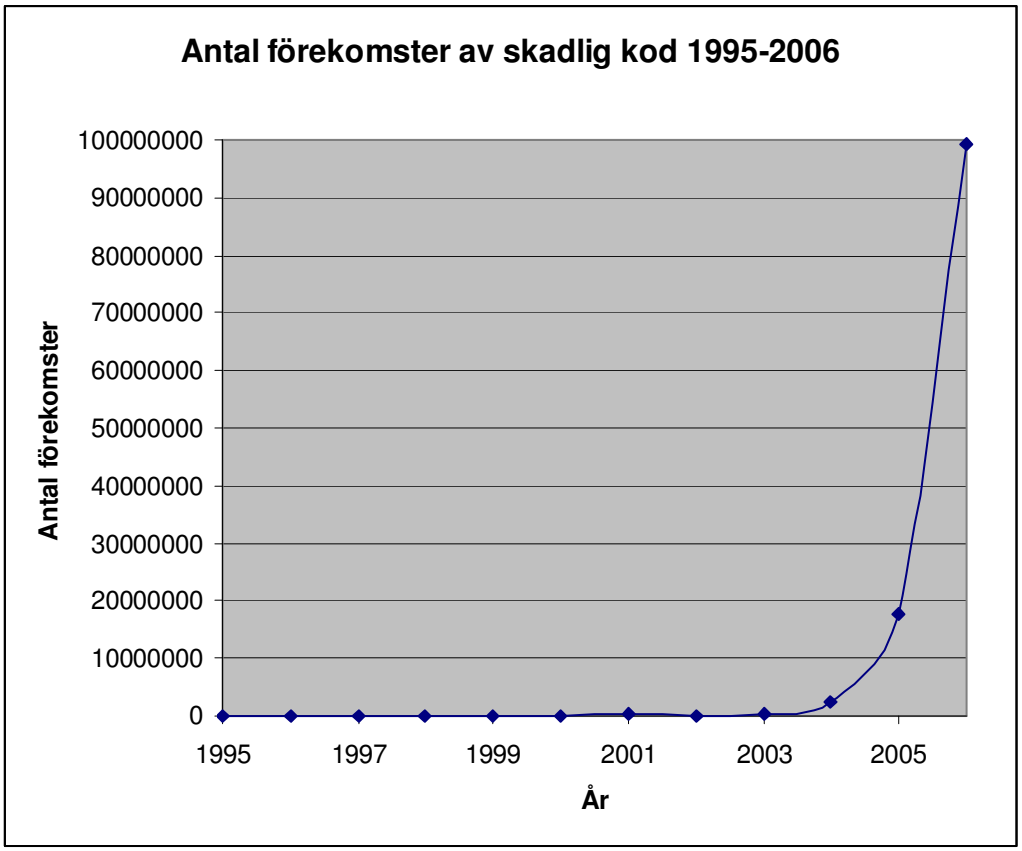


Diagram 1. Antal inrapporterade och bekräftade incidenter skapade av skadlig kod mellan 1995-2006 (”Virus Prevalence”, 2007).

2.6.2 Antal kända exempel av skadlig kod

Det är inte bara antalet bekräftade förekomster historiskt sett som är av intresse för uppsatsen, utan även hur många olika exempel av skadlig kod det har funnits över åren. Dessa siffror är även de lite osäkra, då de varierar från källa till källa. Dock är variationerna inte gigantiska och de visar därför åtminstone utvecklingen i stora drag.

I **diagram 2** på nästa sida visas hur de kända typerna av skadlig kod har ökat över åren från 1995-2006. Som underlag till diagrammet har flera olika källor använts, då det inte varit möjligt att finna en källa som angett samtliga års uppgifter. Underlaget till **diagram 2** kommer från Computer Knowledge (”Number of viruses”, 2005) för åren 1995-2000 och från Security Statistics (”Virus related statistics”, 2004) för år 2002 och från USA Today (**”**Worms and viruses and phishers, oh my!, 2005”) för år 2004 samt från Aftonbladet (”Osynliga viruset snor dina pengar”, 2007) för år 2006. Källdatan till nedanstående diagram återfinns i bilaga 3.

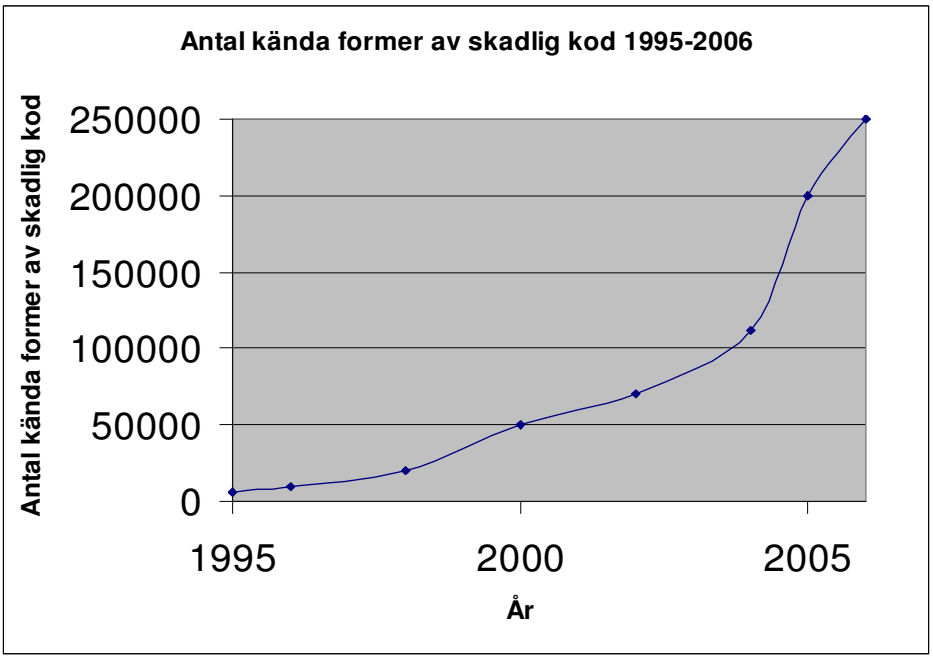


Diagram 2. Visar de uppskattade kända exemplen på skadlig kod från 1995-2006 (”Computer Knowledge: Number of viruses”, 2005), (”Security Statistics: Virus related statistics”, 2004), (”USA Today: Worms and viruses and phishers, oh my!, 2005), (”Aftonbladet: Osynliga viruset snor dina pengar”, 2007).

2.6.3 Kostnader för den skadliga koden genom åren

Eftersom en av de frågor som ställs till respondenterna är om de tror att kostnaden som den skadliga koden orsakar kommer att öka i framtiden, är det nödvändigt att visa hur mycket ekonomiskt lidande den skadliga koden har orsakat genom åren. Detta är mycket svårt att beräkna, då långt ifrån alla som drabbas av den rapporterar dess skadeverkningar så att det förs statistik på den. Med andra ord är nedanstående siffror uppskattningar, precis som i fallet ovan med antal förekomster av skadlig kod. Men även här anser jag att siffrorna åtminstone ger en fingervisning om den ungefärliga verkligheten.

I **diagram 3** på nästa sida visas den uppskattade totala direkta kostnaden som den skadliga koden uppskattas ha orsakat. Detta diagram belyser de direkta kostnaderna i samband med ett angrepp av fientlig kod och avser arbetskostnaden för att analysera, reparera och rengöra smittade system, förluster i produktiviteten, förluster av intäkt på grund av sämre fungerande system samt andra direkta kostnader orsakade av den skadliga koden.

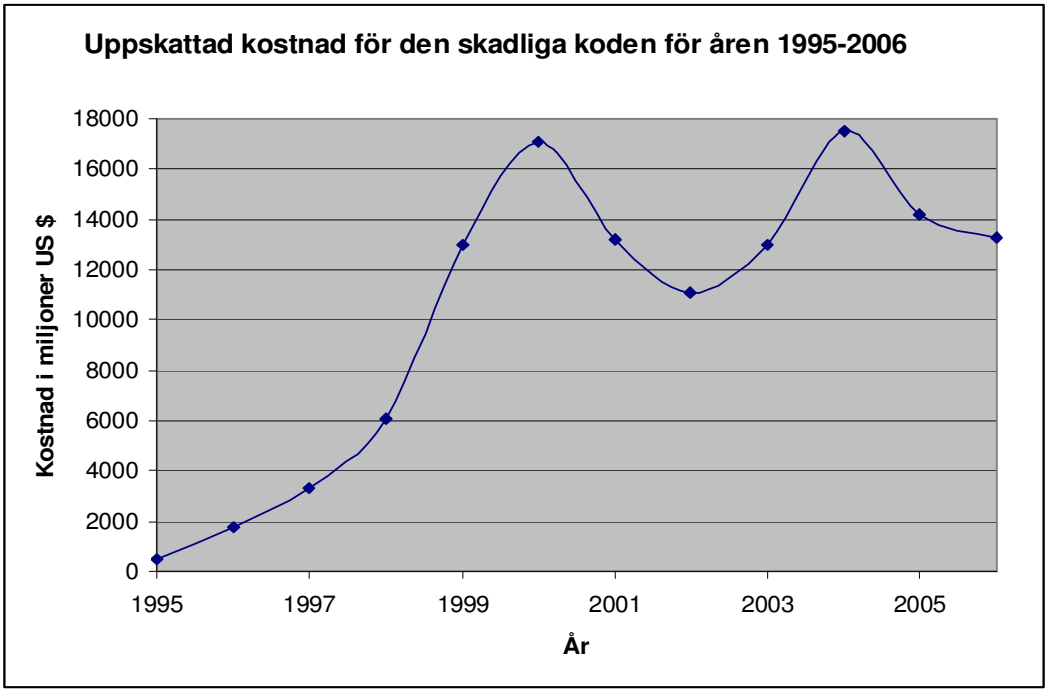


Diagram 3. Visar den uppskattade direkta kostnaden för skadlig kod från 1995-2006 (”Computer Economics: 2005 Malware Report: The impact of Malicious Code Attacks”, 2006), (”Computer Economics: Annual Worldwide Economic Damages from Malware Exceed $13 Billion”, 2007).

Anledningen till att kostnaden för den skadliga kodens verkningar minskat på senare år anses vara att datorerna numera är bättre skyddade mot den än tidigare samt att tillverkare av antivirusprogram numera reagerar snabbare och därmed undviks de verkligt globala smittorna. Vidare angrips specifika mål i mycket högre utsträckning än tidigare, istället för att angripa ett stort antal mål där kanske väldigt få är av intresse. Tidigare skrevs den skadliga koden för att orsaka maximal skada, vilket var mer kostsamt i direkta kostnader mätt, idag skrivs den för att skapa intäkter för dess skapare (”Computer Economics: Annual Worldwide Economic Damages from Malware Exceed $13 Billion”, 2007). Dock finns det mycket som tyder på att de sekundära kostnaderna ökat rejält de senaste åren. Dessa sekundära kostnader innefattar kostnader såsom för antivirusprogram, hård- eller mjukvara som är avsedda att skydda verksamheten från skadlig kod, löpande kostnader för IT-specialister som arbetar för att skydda verksamheten från skadlig kod, framtida kostnader orsakade av en attack av skadlig kod, försäkringskostnader, samt den kostnaden som den skadliga koden eventuellt tillfogar företaget i avseende på förlorat värde på företagsnamnet eller förlust av marknadsvärde (ibid.). Så trots att de direkta kostnaderna gått nedåt de senaste åren, har de indirekta kostnaderna troligen ökat rejält, vilket antyder att den totala kostnaden sannolikt ökar hela tiden trots allt (ibid.).

2.7 Nuläge

För att uppsatsen ska vara så aktuell som den bara kan vara är det viktigt att ta med även de allra senaste trenderna inom skadlig kod.

Eftersom Microsoft släppte sitt Windows Vista år 2006 och allt fler användare kommer att gå över till det operativsystemet kommer naturligtvis också den skadliga koden att göras om för att i allt högre grad rikta in sig på det. Dock har Windows XP fortfarande hela 81 % av operativsystemmarknaden i november 2007 (”Market share: Operating system market share for november 2007”, 2007). Med andra ord skrivs den mesta koden idag för att kunna smitta Windows XP. Microsoft Windows sammanlagda marknadsandel av operativsystemen för datorer var hela 92 % i november 2007 (ibid.).
Den organiserade brottsligheten som ofta ligger bakom skapandet av skadlig kod har blivit ännu mer organiserad. Bland annat säljs nu färdiga ”verktygslådor” av skadlig kod i mycket högre utsträckning än tidigare, där köparen kan få vad han vill i paketet. Exempelvis har färdiga verktygslådor som kan användas till att utnyttja säkerhetshål i webbläsare sålts, och även programvara som kan användas för phishing. Det finns även färdiga verktygslådor innehållande Rootkits ute på marknaden (”Finjan viral security: Web security trends report Q32007”, 2007). Vidare har ”ekonomiska föreningar” skapats på Internet av kriminella krafter som där säljer information om företag eller privatpersoner. Informationen kan utgöras av exempelvis kontokortsinformation eller e-mailadresser.
Nedan i **tabell 1** visas en sammanställning av tillgänglig information och ”verktygslådor” som finns till försäljning på Internet idag (**”**Symantec: Internet Security Threat Report Volume XII”, 2007).

Rank	Item	Percentage	Range of Prices
1	Credit Cards	22%	$0.50 - $5
2	Bank Accounts	21%	$30 - $400
3	Email passwords	8%	$1 - $350
4	Mailers	8%	$8 - $10
5	Email Addresses	6%	$2/MB - $4/MB
6	Proxies	6%	$0.50 - $3
7	Full Identity	6%	$10 - $150
8	Scams	6%	$10/week
9	Social Security Numbers	3%	$5 - $7
10	Compromised Unix Shells	2%	$2 - $10

Numera är den skadliga koden i högre utsträckning än tidigare skapad att angripa vissa regioner, exempelvis Tyskland eller Sverige, från att tidigare varit global i högre utsträckning. Detta medför exempelvis att maskar är relativt ovanliga i Nordamerika för närvarande, medan trojaner är vanliga, vilket kan bero på att Internetleverantörerna där är duktiga att bekämpa maskarna och sämre på trojaner. Alternativt kan det bero på att de trojaner som cirkulerar för närvarande är i högre grad riktade mot Nordamerika än de motsvarande maskarna (ibid.).

Den skadliga koden har börjat angripa onlinespelen, vilket innebär att exempelvis Kina och dess grannländer blir mer utsatta, då dessa länders innevånare spelar onlinespel i ovanligt hög utsträckning. Dessa spel är intressanta, bland annat för att det ofta finns möjligheter att betala eventuella avgifter via dessa (ibid.). Onlinespel, ”virtuella världar”, sociala nätverk, Internet-handel, möjligheten att göra bankärenden online samt mycket mera brukar placeras under samlingsnamnet ”Web 2.0” eller alternativt ”Web 2” och betecknar det moderna Internet som en fristående plattform med otroligt många möjligheter, skiljt från hur Internet såg ut tidigare (”Wikipedia: Web 2.0”, 2007). Dessa många möjligheter ger också skaparna av skadlig kod många möjligheter att använda sin skadliga kod på, idag mer än någonsin.

De allra flesta attacker som genomförs nu avser att ge den kriminelle ekonomisk vinning eller information. Förr spreds den skadliga koden snabbt och utan urskillnad, i fruktansvärda attacker med masspostande maskar via e-mail samt genom enorma mängder bots som genomförde denial of service attacker. Detta har i allt högre utsträckning blivit ineffektivt då det inte ger skaparna av den skadliga koden vad de vill ha: pengar eller information (som sedan kan bytas mot pengar). Så länge som denna metod att arbeta i mindre skala lönar sig för skaparna av koden så kommer den att fortsätta (”Symantec: Internet Security Threat Report Volume XII”, 2007).

Det har också skett en förändring i hur själva attackerna med hjälp av den skadliga koden går till. Förr skedde attackerna ofta i ett steg, för att nu ofta ske i flera steg. Attacktekniken har med andra ord blivit mer sofistikerad. Den skadliga koden gör numera inget väsen av sig, utan tar sig in obemärkt och sedan sker den fortsatta attacken i det fördolda. För att undvika att upptäckas används nu allt mer olika stealth-tekniker (ibid.).
Idag är det vanligt att den skadliga koden är en trojan, som när den väl infekterat ett system, laddar ner ytterligare programvara (moduler) från Internet för att få en, för dess skapare, önskad funktionalitet. Denna form av skadlig kod kallas ibland för ”modular malicious code” eller ”downloaders” och är i skrivande stund den vanligaste av all ny skadlig kod. Enligt Microsoft ökade den formen av skadlig kod, där en trojan laddar ner ytterligare programvara, med 500 % jämfört med perioden innan (”Microsoft Research Reveals New Trends in Cybercrime, 2007).

Ett modernt exempel på hur det kan gå till är att en trojan tar sig in obemärkt i ett system, där den sedan ligger dold och startar först när den känner av att systemet går in på exempelvis en banks hemsida. Då loggar exempelvis trojanen det som skrivs, eller så kan den exempelvis ändra i de transaktioner som görs, vart pengar ska gå, hur mycket det rör sig om, och så vidare. Dessa trojaner kan ofta fjärrstyras med nya konfigurationer och uppgifter att arbeta med från någon avlägsen server. Trojanen får ofta dessa nya konfigurationer och uppgifter i krypterad form, enligt det så kallade SSL-protokollet. Detta protokoll använder sig också ofta själva trojanen av när den i sin tur skickar iväg information. Användandet av kryptering medför att det är mycket svårt att upptäcka trojanen, och även att se vart informationen går samtidigt som det är svårt att se vad för information som verkligen skickas i de bägge riktningarna (ibid.).

Rootkit-egenskaper är också något som trojaner och andra former av skadlig kod får i allt högre utsträckning, då detta medför att koden kan dölja sig för de infekterade systemen på ett mycket effektivt sätt (”Finjan viral security: Web security trends report Q32007”, 2007).

En annan metod, som vuxit fram på sistone, är att istället för att angripa enskilda datorer angripa exempelvis en webbsida som ägnar sig åt försäljning via Internet och som sådan

besöks av många datoranvändare. På så sätt kan man nå många datorer genom att ”bara” bryta sig in i ett enda system. Genom att på detta sätt använda sig av det aktuella företagets trovärdighet gentemot sina kunder, tror folk att det är säkert och traskar in i eventuella fällor med öppna armar. Inte sällan kan angriparna på detta sätt få tag i information om kundernas kreditkort, e-mailadresser, användarnamn och lösenord med mera. Detta kan även gälla andra organisationer, såsom exempelvis e-mailleverantörer och sociala nätverk (”Symantec: Internet Security Threat Report Volume XII”, 2007).

En trend är också att skapare av fientlig kod som verkar inom olika genrer såsom spam, phishing, exploits med mera i högre grad än tidigare samarbetar med varandra, för ökad vinning. Det är mycket svårt att skydda sig mot en angripare som behärskar många olika angreppsmetoder. För att kunna bekämpa detta måste även de som gör skydd för datorer samarbeta i högre utsträckning, och göra heltäckande lösningar istället för att som tidigare exempelvis ha ett antivirusprogram, ett program för att finna adware och spyware samt kanske ett program som fungerade som mjukvarubaserad brandvägg och så vidare (ibid.).

Mängden spam ökade något under den första hälften av 2007, medan Phishing-försöken ökade med hela 150 % jämfört med den föregående perioden enligt Microsoft (”Microsoft Research Reveals New Trends in Cybercrime, 2007).

Trojanerna var på uppgång detta år, vilket märks då Symantec rapporterade att 40 % av all nyskapad skadlig kod utgörs av trojaner. Trojanerna har blivit mycket vanligare än tidigare, vilket visar att de är väl lämpade för att samla in pengar eller information åt dess skapare (”Symantec: Internet Security Threat Report Volume XII”, 2007).

Det farligaste hotet under 2007 ansågs vara den så kallade Storm-worm, som dök upp i ungefär 50.000 varianter under året. Masken spred sig genom att blogga, dölja sig inuti spam-meddelanden, gratulationskort med mera (”The Sydney morning herald: Microsoft wants to worm its way into your PC”, 2008).

Antalet förekomster av skadlig kod ökade under 2007 jämfört med året innan, dock finns det i skrivande stund inga siffror på hur mycket. Dock slogs fjolårets motsvarande siffra efter att nio av årets tolv månader passerat (”Virus Bulletin: Virus Prevalence”, 2007).

I utgången av år 2007 fanns det ungefär 500 000 kända exempel av skadlig kod, vilket är en fördubbling från år 2006 då det ”bara” fanns ungefär 250 000 kända exempel (”Aftonbladet: Osynliga viruset snor dina pengar”, 2007).

2.8 Teorier om framtiden

I detta kapitel återges de teorier om framtidens skadliga kod som har återfunnits på Internet och i annan litteratur. Det visade sig vara problematiskt att hitta källor till detta kapitel. Det är sannolikt så att ganska få vågar sticka ut hakan och spekulera om vad som kommer att hända i framtiden då den skadliga kodens värld ändrar sig så snabbt. Detta blir ännu mera tydligt om man bara ser till böcker, då de prognoser som ställs de dem i stort sett är föråldrade redan då boken kommit ut. Därför är det lättare för experter inom ämnet att ta med framtidsperspektivet i artiklar som publiceras på Internet i stort sett omedelbart efter att de formulerats. Det är också så att de flesta rapporter som publiceras på Internet rörande den skadliga kodens framtid, till stor del bygger på källor som också ligger ute på Internet. Detta

pekar på att författarna, i likhet med mig, anser att färska artiklar från Internet väger tyngre än föråldrade böcker i detta sammanhang.

Eftersom Microsoft Windows Vista i dagsläget är det operativsystem som det satsas på och som kommer att bli vanligare och vanligare till dess att Microsoft släpper sin nya version av Windows är det rimligt att anta att allt mera skadlig kod kommer att skrivas för det operativsystemet. Det är beräknat att Vista kommer stå för drygt 10 % av operativsystemmarknaden år 2008 (”IDG: Fler attacker mot Vista 2008”, 2007). Att Vista kommer att bli ett hett byte för den skadliga koden i framtiden är något som också som antivirusprogramtillverkaren Kaspersky Labs anser (”PC Pro Focus: Vista determines malware evolution”, 2007).
Microsoft Vistas efterföljare, som idag kallas för Windows 7, men som säkerligen kommer att få ett nytt namn till sin lansering, är beräknat att släppas under år 2010 (”Windows 7 news”, 2007). Eftersom Microsoft genom denna lansering återgår till att lansera ett nytt operativsystem ungefär vart tredje år igen, vilket inte blev fallet med Microsoft Vista, då det tog närmare sex år innan det efterträdde Windows XP, är det troligt att XP kommer att vara det vanligaste operativsystemet vid tidpunkten för lanseringen av Windows 7. Vissa källor tror att XP kommer att vara det vanligaste operativsystemet ända fram till år 2011 (”Neil Mcdonald: The future of malicious code”, 2007).
Kaspersky Labs tror att det kommer att skrivas mer skadlig kod till andra operativsystem i framtiden, såsom till Apples OS X samt till Unix (”PC Pro Focus: Vista determines malware evolution”, 2007).

McAfee, som är en av de största tillverkarna av antivirusprogram, har listat tio punkter som de anser kommer att infalla år 2008 eller senare, och dessa är intressanta teorier för framtiden (”IDG: De tio värsta IT-hoten som gör 2008 till en mardröm”, 2007).
Bland annat anser företaget att en trend för skaparna av skadlig kod kommer att vara att i högre grad än tidigare skriva sin kod för att drabba så kallade sociala nätsajter, såsom exempelvis Facebook eller Myspace eller andra former av det så kallade ”Web 2.0”. Då dessa sidor har miljoner användare är de mycket intressanta för attacker (ibid.). Detta gäller även för onlinespelen och ”virtuella världar”, enligt en rapport från Symantec (”Symantec: Internet Security Threat Report Volume XII”, 2007), men även exempelvis GTISC (”Georgia Tech Information Security Center: Emerging Cyber Threats Report for 2008”, 2007) instämmer i detta och menar att många attacker nu för tiden inte görs direkt mot måldatorerna, utan att vägen in i dem går via Web 2.0 istället. Exempelvis onlinespel är intressanta för hackarna då det ofta överförs pengar via dessa program och spel, samt genom att information går att stjäla via dem. Vidare skulle skadlig kod kunna utge sig för att vara en uppdatering till spelen/världarna för att ge dem ökad funktionalitet, och därmed gladeligen laddas ner av dess användare.
McAfee förutspår att det kommer skapas ett stort antal trojaner som är ute för att stjäla lösenord och användaruppgifter samt de pengar som överförs mellan spelaren och företaget som driver spelet online (”IDG: De tio värsta IT-hoten som gör 2008 till en mardröm”, 2007).
En annan prognos som både McAfee och GTISC ställer är att antalet Bots kommer att öka och därmed infektera ett högre antal datorer.
Vidare anser företagen att chatt-programmen kommer att drabbas av skadlig kod i högre utsträckning än vad som tidigare varit fallet. Ett annat område, som ännu är lite i sin linda, är IP-telefonin som ännu inte har blomstrat ut fullt ut. McAfee anser att det kommer att bli vanligare med attacker på IP-telefonin på olika sätt. Företaget spår att antalet attacker mot IP-telefonin kommer att öka med hela 50 % år 2008 (ibid.).

En trend som råder för närvarande, och som har hållit i sig de senaste åren, är att antalet kända former av skadlig kod fördubblas ungefär var tolfte månad (”Authentium: Virus outbreaks doubles every month”, 2005). Eftersom det idag, 2008, finns ungefär 500 000 kända olika exempel på skadlig kod, kommer det att finnas ungefär 16 miljoner kända exempel på skadlig kod år 2013 om den utvecklingen håller i sig. Vidare framgår det tidigare i uppsatsen att antalet förekomster av skadlig kod ökat explosionsartat de senaste åren, och att även år 2007 blev ett nytt rekordår sett till antalet förekomster av skadlig kod. Eftersom tillgängligheten till Internet kommer att fortsätta att öka, såväl i avseende av bandbredd och antal uppkopplade datorer kommer fler och fler system att göras sårbara för skadlig kod och dess verkningar i framtiden. Vidare kommer fler och fler datorer att sättas i nätverk, vilket också gör dem mer sårbara för skadlig kod. Andelen trådlösa nätverk kommer att öka jämfört med idag, vilket kommer att göra dem mer utsatta för skadlig kod (“Search Security: Mike Rothman: Top 5 next-generation messaging attacks that antivirus can't catch”, 2007). Enligt Mikko Hyppönen, som är chef för forskningsavdelningen på antivirusföretaget F-secure, kommer det ökande användandet av bärbara datorer med sina trådlösa uppkopplingar att medföra att det kommer att skapas skadlig kod som sprider sig automatiskt från en bärbar dator till en annan om de kommer tillräckligt nära varandra (”Search Security: Future - Information Security Magazine”, 2008).

Hyppönen (ibid.) anser också att kommer det att skapas mycket mera skadlig kod till mobiltelefoner och andra enheter inom några år. Han pekar speciellt ut de telefoner som använder sig av det vanligaste operativsystemet för mobiltelefoner, Sybian. Det finns skadlig kod till dessa enheter idag, men de har i stort sett inte varit skrivna för ekonomisk vinning för dess skapare. Något som Hyppönen tror kommer att förändras i framtiden. Den skadliga koden kan sprida sig via så kallad Bluetooth, vilket är ett trådlöst sätt för telefonerna att kommunicera med andra enheter, men även via e-mail och andra sätt. Han anser att det bara är en tidsfråga innan hackarna skapar mer intelligent skadlig kod för dessa enheter som i högre grad strävar efter att ge sin skapare ekonomisk vinning eller tillgång till information. En annan teori som han lägger fram är att mobiltelefoner skulle kunna användas till att skapa så kallade botnets, liknande dem som hackare skapar med hjälp av datorer idag. Detta möjliggörs av att mobiltelefonerna får allt mer inbyggd processorkraft samtidigt som telefonnätet som telefonerna kommunicerar via får större och större bandbredd (ibid.). Dessa botnets skulle då kunna användas till att skicka email-spam eller spam i form av textmeddelanden till andra telefoner (”Search Security: Apple iPhone to provoke complex mobile attacks, expert warns”, 2007). Att just mobiltelefoner är ett område som den skadliga koden kommer att angripa i framtiden är något som även antivirusföretaget McAfee tror då de i en rapport (”Search Security: Future mobile attacks inevitable”, 2007) varnar för just detta. Speciellt tror företaget att angreppen kommer att riktas mot så kallade ”smartphones”, exempelvis Apples iPhone, som gör det lättare för användarna att surfa på Internet med telefonen samt att handla via Internet. Vidare finns det redan idag teknik som kan förvandla en ”smartphone” till en komplett övervakningsenhet, som kan användas för att spela in samtal eller spara textmeddelanden eller ta kort med telefonens kamera för att senare skicka denna information vidare. Det spås att den skadliga koden till mobiltelefoner och handhållna enheter kommer att explodera den dag som man kan genomföra bankärenden via dessa enheter (”Lead Agency Publication: Future threats in malicious code – 2006 report”, 2006). Denna utveckling kommer att äga rum då skaparna av den skadliga koden kommer att hitta möjligheter att tjäna pengar på att angripa mobiltelefonerna. Ett exempel på hur man kan tjäna pengar på att skriva skadlig kod till mobiltelefoner är exempelvis genom ”smishing”, vilket är phishing som sker via sms. Eller ”vishing”, vilket är phishing som sker via ljud (i telefonen) . Många risker och

hot som tidigare har visat sig för datorerna kommer helt enkelt att återupprepas och införas även på mobiltelefonerna (”Search Security: Future mobile attacks inevitable”, 2007).

Handhållna enheter är också något som kommer drabbas av en större mängd skadlig kod i framtiden. Detta gäller även flyttbara media, såsom USB-minnen, musikspelare, externa hårddiskar, eller andra enheter som kan lagra information och som är flyttbara (”Lead Agency Publication: Future threats in malicious code – 2006 report”, 2006). Även andra enheter, som spelkonsoller med förmågan att koppla upp sig mot Internet samt att kommunicera med andra enheter är tänkbara framtida mål för skadlig kod (”PC Pro Focus: Vista determines malware evolution”, 2007).

Experten och professorn Eric Filiol hävdar att skaparna av skadlig kod i framtiden kommer att utnyttja att antivirusprogram är en kommersiell produkt och att den skadliga koden inte har samma begränsningar. Han menar att nya, komplexa och komplicerade former av skadlig kod kommer att sätta antivirusprogrammen på hårda prövningar. Bland annat varnar han för komplicerade rootkits som kan komma att bli vanligare i framtiden. Dessa rootkits kan vara så sinnrikt konstruerade att de är omöjliga att upptäcka inifrån det egna systemet, och därför måste upptäckas från utsidan av systemet (”Eric Filiol: Concepts and future threats in computer virology”, 2007). Denna fruktan för rootkits delas också av experten Mike Rothman som menar att rootkits är ”den mest allvarliga och påtagliga metoden den skadliga koden kan använda för att undvika att upptäckas av antivirusprogrammen” (“Search Security: Mike Rothman: Top 5 next-generation messaging attacks that antivirus can't catch”, 2007). Vidare talar Filiol om att polymorfism och metamorfism kommer att utvecklas till den grad att antivirusprogrammen, åtminstone inte initialt, kommer att kunna rå på dem (”Eric Filiol: Concepts and future threats in computer virology”, 2007). Denna syn har även experterna Ed Skoudis (”Search Security: Ed Skoudis: Polymorphic viruses call for new antimalware defenses”, 2007) och Noah Schiffman (”Search Security: Noah Schiffman: Metamorphic malware sets new standard in antivirus evasion”, 2007). Filiol har en ganska mörk framtidssyn där han tror att antivirusprogram är oumbärliga, men att de kommer att hitta allt mindre av den skadliga koden i framtiden och att antivirusprogrammen i allt högre utsträckning bara kommer att rå på redan kända hot (”Eric Filiol: Concepts and future threats in computer virology”, 2007).

Skaparna av den skadliga koden kommer sannolikt att fortsätta att ligga steget före tillverkarna av programvaran i det avseendet att de kommer att hinna utnyttja säkerhetshål i applikationer innan tillverkaren av den hinner åtgärda säkerhetshålen (”Lead Agency Publication: Future threats in malicious code – 2006 report”, 2006).

Direktmeddelanden, eller ”instant messaging” är något som spås kunna växa som spridningssätt för den skadliga koden i framtiden. Den skadliga koden kan själv ”chatta” med personer och sprida sig vidare genom personers kontaktlistor. Exempel på tänkbara program här är MSN, ICQ, Yahoo Messenger med flera. Något som talar för att detta kan komma att bli framgångsrikt för hackarna är att man oftast har stor tilltro till de personer som man har på sin kontaktlista för dessa program, och inte ofta ifrågasätter vad dessa gör eller skickar för filer. DDOS-attacker spås också kunna vara ett fenomen som åter blommar upp igen, efter att ha legat lite lågt de senaste åren(”PC Pro Focus: Vista determines malware evolution”, 2007). Så kallad ”ransomware” eller ”cryptoware”, vilket avser skadlig kod som kan användas för att kryptera filer för exempelvis företag och sedan användas i utpressningssyften är också något som kan bli mer vanligt i framtiden (ibid.).

Att den skadliga koden skapas främst för att ge sin skapare ekonomisk vinning är det normala redan idag, men detta kommer sannolikt bli ännu mera tydligt i framtiden. Neil Mcdonald, vice VD för säkerhetsföretaget Gartner, anser att 70 % av alla genomförda attacker år 2010 kommer att ha ekonomisk vinning som drivkraft (”Neil Mcdonald: The future of malicious code”, 2007)

De senaste åren har vi sett att den skadliga koden blivit mer och mer inriktad på specifika mål. Något som kommer att hjälpa till att göra detta ännu mera möjligt i framtiden är att det blir allt lättare att få reda på var specifika IP-adresser finns geografiskt på vår jord . Detta möjliggör att skaparna av den skadliga koden lättare kommer att kunna skicka sina skapelser till rätt mottagare. Exempelvis skulle detta kunna användas för att skicka ut e-post innehållande skadlig kod till personer som bor i ett visst land där en viss händelse inträffat som berör människorna mycket, vilket skulle kunna utnyttjas med exempelvis en träffande text i e-posten som får dem att öppna den i högre utsträckning. Dessa nya möjligheter gör också att hackarna lättare kan skicka sin skadliga kod till specifika företag. (”Lead Agency Publication: Future threats in malicious code – 2006 report”, 2006).

Något som sannolikt kommer att bli vanligare i framtiden är de verktygslådor för skapande av skadlig kod som finns till försäljning, de så kallade toolkitsen. Detta innebär att fler och fler människor kommer att kunna skapa och använda skadlig kod. Information om personers kontokort, användaruppgifter eller annan information, e-mailadresser med mera kommer i allt högre grad gå att köpa (ibid.).

Något som är nära sammanflätat med dessa toolkits är de trojaner som kan ladda ner ytterligare funktionalitet, så kallade ”modular malicious code” eller ”downloaders”. Dessa kommer sannolikt att bli ännu vanligare de kommande åren och troligen kommer de att bli den dominerande formen av skadlig kod (”Symantec: Internet Security Threat Report Volume XII”, 2007). Dessa trojaner kan användas till otroligt många olika saker, men ett tänkbart exempel som de kommer att rikta in sig mera på i framtiden är Internetbanker och när datoranvändarna interagerar med dessa. Påståendet att denna form av skadlig kod kommer att vara den dominerande de kommande åren rättfärdigas av att denna form av skadlig kod ökade med cirka 500 % under år 2007. Dessa trojaner utgör helt enkelt det bästa verktyget för hackare just nu för att ge sin skapare ekonomisk vinning eller information och det är sannolikt att detta kommer att fortsätta vara fallet under den närmaste framtiden (ibid.).

3 Intervjuer

Detta kapitel visar hur intervjuerna genomförs, vilka som intervjuas samt varför just dessa respondenter väljs. I slutet av kapitlet redovisas svaren som respondenterna lämnar på frågorna.

3.1 Genomförande

För att ge uppsatsen bästa tänkbara validitet är det viktigt att intervjua verkliga experter inom ämnet. Valet föll på fyra i Sverige boende och verkande experter. Dessa personer återfanns under inläsningen av ämnet, då de återkommit vid ett flertal tillfällen i den funna litteraturen. Dessa fyra experter valdes då de är högt ansedda och dagligen arbetar inom området. De valda personerna är alla mycket framstående inom ämnet vilket ger uppsatsens empiriska del

den nödvändiga validiteten. Dessa fyra personer tillhör utan tvivel de mest kunniga personerna inom detta område i Sverige. En tänkbar förbättring av uppsatsen hade varit att intervjua ännu mera erkända experter globalt sett.

Intervjuerna genomfördes via telefon, dels av bekvämlighetsskäl, men även av den anledningen att det inte ansågs vara någon fördel att genomföra intervjuerna öga mot öga. Dock är det tänkbart att det trots allt hade varit bättre. Intervjuerna spelades inte in då detta möjligen kunde stört respondenterna. Inledningsvis ringdes den tilltänkta respondenten upp och bads om hjälp. Samtidigt berättades det om vad uppsatsen handlade om, hur respondenten kunde hjälpa till och att intervjun skulle ta ungefär en timme. Hela tiden lades fokus på att vara korrekt och på att hålla en så artig och trevlig attityd som möjligt. Efter att respondenten tackat ja, vilket alla tillfrågade gjorde, enades vi om ett lämpligt datum och klockslag. Efter detta tillskickades respondenten en e-mail där det förklarades situationen återigen för att undvika oklarheter. Intervjufrågorna bifogades i e-mailen, så att respondenten kunde förbereda om denne så ville.

Intervjufrågorna är konstruerade på ett sådant sätt att samma svar eventuellt kan ges på flera olika frågor. Detta gjordes medvetet för att få så heltäckande svar som möjligt. Nackdelen med detta tillvägagångssätt är att det kan uppkomma upprepningar i svaren. Det ställdes även frågor som inte besvarade någon av forskningsfrågorna, men som trots detta ansågs kunna ge ytterligare information om vad respondenterna tyckte och trodde om den skadliga kodens framtid. Intervjufrågorna som ställdes var övervägande öppna frågor. Dessa frågor, som är motsatsen till slutna frågor, innebär att respondenten inte kan besvara intervjufrågorna med ja eller nej.

För att inte gå miste om något av det som framkom under intervjun, skrevs respondentens svar på frågorna ner samtidigt som de svarade. De fasta frågor som ställdes under intervjuerna återfinns i bilaga 1 och de följdfrågor som eventuellt ställdes under intervjuerna återfinns inte i uppsatsen.

3.2 Respondenter

I detta avsnitt belyses respondenternas bakgrund och kunskap inom ämnet. Detta ligger också till grund för varför de valdes ut.

3.2.1 Viiveke Fåk

Viiveke Fåk är professor i datasäkerhet vid Linköpings Universitet och hon har varit verksam inom området alltsedan hon blev utnämnd till professor 1978. Hon har utbildat, föreläst, arbetat som konsult samt forskat inom området under lång tid. Hon är mycket framstående inom kryptografi, där hon 1978 var med och startade företaget Sectra som är specialiserat på säker digital kommunikation. Vidare har hon mycket stor kunskap om skadlig kod, då hon skrivit böcker i ämnet. Hon föreläser och examinerar också personer inom ämnet regelbundet på Linköpings Universitet.

3.2.2 Johan Jarl

Johan Jarl är säkerhetsexpert på det finska antivirusföretaget F-secures svenska avdelning i Stockholm. Han är en ofta anlitad föreläsare och skriver nästan dagligen rapporter för F-

secures räkning. Hans namn är ofta synligt i svensk press då dagstidningar samt vetenskapliga publikationer regelbundet intervjuar honom angående skadlig kod.

3.2.3 Per Hellqvist

Per Hellqvist är säkerhetsspecialist på Symantecs svenska avdelning i Stockholm. Han har tidigare arbetat för det finska antivirusföretaget F-Secure med liknande arbetsuppgifter. Han är en flitigt anlitad konsult samt förekommer ofta i media i frågor som berör skadlig kod. Möjligen är han den expert som oftast intervjuas av svensk media i frågor om IT-säkerhet. Vidare är han är en av nordens mest anlitade föreläsare kring IT-säkerhet. Han startade år 2001 upp den svenska viruslistan som han drev och uppdaterade i flertalet år. År 2004 tilldelades han SigSecuritys säkerhetsstipendie och år 2005 tilldelades han Säkerhetsdelegationens säkerhetsstipendie. Nyligen skrev han en bok (”Handbok för föräldrar – Lär dig vad ditt barn gör på Internet”, 2007), vilken beskriver de risker som finns för barn när de befinner sig på Internet. Han har också blivit kallad som expertvittne till den rättegång som behandlade den svensk som påstås ha skapat Gandaviruset. Vidare driver han Sveriges enda blogg om IT-säkerhet, vilken han startade 2004.

3.2.4 Joakim Von Braun

Joakim Von Braun är en av de främsta experterna i Sverige inom skadlig kod. Han har arbetat som konsult samt rådgivare åt den svenska säkerhetspolisen, SÄPO, i tjugofem år. Vidare har han arbetat åt den svenska militära underrättelsetjänsten IB i drygt femton år. Han kontaktas regelbundet av Rikskriminalens IT-brottsrotel där han har anlitats som sakkunnig samt som specialist vid såväl brottsmål som civilrättsliga processer. Från slutet av 1980-talet har han varit konsult, föredragshållare samt journalist inom IT-säkerhetsområdet. Han drev också eget företag i branschen i tio år. I Början av 2000-talet började han arbeta på företaget Symantecs svenska avdelning i Stockholm där han främst arbetade som säkerhetsrådgivare åt större företag och organisationer. År 2001 fick han TelecomCity Prize för sin kunskap och sitt engagemang inom datasäkerheten. Efter att ha arbetat på Symantec i några år slutade han där och satsade istället på sitt eget företag, Von Braun Security Consultants. Von Braun är en av de svenska experter som syns mest i svensk dagspress samt i vetenskapliga publikationer.

3.3 Respondenternas svar

I detta avsnitt återges respondenternas svar på de ställda intervjufrågorna. För att det lätt ska gå att härleda respektive respondents svar på intervjufrågorna redovisas svaren från varje respektive respondent.

3.3.1 Vilken är enligt din mening den farligaste sortens skadliga kod som finns idag?

Viiveke Fåk: Antingen de former av skadlig kod som drabbar många hemanvändare, men som samtidigt inte gör så enormt stor skada, eller alternativt den skadliga kod som kan användas till att angripa ett specifikt stort mål, såsom exempelvis USA:s försvar. Ska en specifik form av skadlig kod nämnas är det kanske rootkits.

Johan Jarl: De nya rootkits som har dykt upp och som är svåra att upptäcka då de är så duktiga på att undgå upptäckt.

Per Hellqvist: Det beror på för vem man menar. För hemanvändare är den skadliga kod som förstör data för dem den farligaste, då de sällan har gjort backup på den data de har på sina datorer. För företag är den farligaste formen av skadlig kod den som stjäl information av dem. Nu för tiden är det trojanerna som utgör det största hotet. De utrustas med de funktioner som de behöver för ett specifikt ändamål och gör det de är byggda för.

Joakim Von Braun: En korsning mellan en trojansk häst och en mask (blandat hot), vilket möjliggör att trojanen kan sprida sig själv vidare. Det finns ganska många av dessa idag. Om trojanen är konstruerad att anfalla endast ett fåtal datorer får skaparna av antivirusprogrammen få chanser att få tag i den skadliga koden och därmed har de mycket svårare att lära sig bekämpa den. Något annat som är mycket farligt är rootkit-teknologin.

3.3.2 Kommer skadlig kod bli mer eller mindre förekommande om fem års tid?

Viiveke Fåk: Det är troligt att den kommer att bli mer förekommande.

Johan Jarl: Den kommer sannolikt att bli mer förekommande.

Per Hellqvist: Idag utgörs en stor del av den nyskapade skadliga koden av ett litet antal trojaner som ändras marginellt hela tiden och därmed får otroligt många varianter. Detta görs för att de ska undgå att upptäckas av antivirusprogrammen. Ofta räcker det att kompilera om den skadliga koden för att den ska få ett lite annorlunda utseende, vilket ofta räcker för att lura antivirusprogrammen. Vissa av dessa trojaner uppdateras automatiskt exempelvis var femtonde minut, för att få ett annat utseende och därmed undgå upptäckt. Med andra ord kan man säga att det år 2007 har skapats ett ganska litet antal trojaner som ändrats och då fått otroligt många olika skepnader. Dessa defineras sen som nya, okända, typer av skadlig kod. Detta fenomen har bidragit till att de kända formerna av skadlig kod fördubblats år 2007. På grund av denna explosionsartade ökning på kort tid är det svårt att sia om framtiden då man inte vet om detta är en tillfällig topp eller en utveckling som kommer att fortsätta. Dock kommer vi i allt högre grad använda datorer och andra enheter som använder operativsystem i framtiden och därför är det rimligt att anta att den naturliga utvecklingen är att det kommer att den kommer att bli mer förekommande i framtiden.

Joakim Von Braun: Den kommer att bli mer förekommande, då den fungerar och är lönande för dem som skapar den idag. Det krävs ingen fantasisk förmåga för att kunna skriva den och det lär inte komma någon teknologi som tar hand om problemen på ett enkelt sätt.

3.3.3 Hur kommer framtidens skadliga kod att skilja sig från dagens i avseende på spridningssätt?

Viiveke Fåk: Nya tekniska lösningar inom exempelvis operativsystem och hårdvara eller användandet av nya metoder ger skaparna av skadlig kod nya möjligheter att sprida den. Det kommer fortfarande vara mycket vanligt att skadlig kod skickas och sprids via e-mail. En risk är de automatiska uppdateringar som sker av programvara av olika slag. Om inte dessa uppdateringar är säkrade kan skaparna av skadlig kod skicka kod som innehåller exempelvis ett virus istället för den efterlängtade uppdateringen.

Johan Jarl: Sannolikt är att mer skadlig kod kommer att spridas via fildelningsprogram och chattprogram. IP-telefoni är någonting som med stor säkerhet kommer att drabbas av skadlig kod. Även i framtiden kommer en stor mängd skadlig kod spridas via e-post. Skadlig kod till mobiltelefoner och andra enheter kan spridas via Bluetooth eller SMS eller MMS.

Per Hellqvist: Den kommer nog att använda de sätt som finns idag, de är tillräckligt hemska och de fungerar.

Joakim Von Braun: Den största skillnaden kommer troligen vara att det kommer att bli lättare att bli smittad när man är ute och surfar på Internet. Det finns stora möjligheter att gömma scripts lite varstans på Internet som sedan kan ladda ner en fil och installera den per automatik.

3.3.4 Hur skiljer sig framtidens skadliga kod från dagens i avseende på hur den kan undgå upptäckt?

Viiveke Fåk: Helst ska den skadliga koden konstrueras så att den inte upptäcks alls innan den går till attack. Detta är en taktik som använts förr, men denna kommer vara framgångsrik även i framtiden. Datorerna själva måste bli mer utvecklade så att de kan ha koll på vad som görs inuti dem. Datorn eller användaren måste själv ligga till grund för vad som görs. En bilaga i en e-mail ska inte själv få skicka e-mail. Datorerna idag är inte byggda för att analysera varifrån ett kommando kommer. Rootkits är en farlig företeelse idag som kan bli ännu farligare i framtiden.

Johan Jarl: Rootkits är troligen det farligaste hotet i den närmaste framtiden.

Per Hellqvist: Det beror på hur tillverkarna av operativsystemen kommer att konstruera dem framöver. Så länge som ett operativsystem tillåter att ett främmande program kör sin egen kod under operativsystemet finns alla chanser att bli drabbad av skadlig kod. Operativsystemen är den svaga punkten. Rootkits är också något som kommer bli riktigt farligt framöver.

Joakim Von Braun: Sannolikt kommer denna att använda sig av rootkit-teknologin i högre utsträckning än idag. Den kommer att dölja sig väldigt effektivt från antivirusprogrammen. Möjligen kommer den att använda sig av så kallad tunnling av trafik för att undgå upptäckt på nätverk och Internet. Detta innebär att den skadliga koden gör så att den egna ip-trafiken döljs och skapas inuti annan ip-trafik vilket innebär att det inte uppdagas av systemet eller användaren. Ett sätt att exempelvis styra en trojan skulle kunna vara att styra den genom tunnling av trafik, eller att utnyttja det tomrum som finns i headern (vilket avser det första avsnitt i början av en datafil, vilken ger information om hur resten av filens innehåll ska tolkas av operativsystem eller applikationsprogram) för att där lägga in styrkoder till en trojan.

3.3.5 Hur kommer framtidens skadliga kod att skilja sig från dagens i avseende på den skada de gör?

Viiveke Fåk: Den kommer inte att skilja sig så mycket, förutom att den blir mer riktad mot specifika mål.

Johan Jarl: Koden kommer att göra mindre och mindre skada, helst så ska den göra så lite skada som möjligt, för att i möjligaste mån undvika upptäckt.

Per Hellqvist: Sannolikt är att hackarna redan idag har skapat tillräckligt många sätt att orsaka skada på, så i stora drag räcker det med dagens metodologi. En möjlig risk är så kallade ”datadiddlers”, vilket är skadlig kod som ändrar slumpvisa siffror eller tecken i databaser eller dokument. Ofta upptäcks inte denna förändring, och då kan företagen ta en backup på de skadade filerna. Eventuellt kan då hackern sälja en kopia av den oförstörda filen eller databasen till företaget och på så vis ägna sig åt utpressning.

Joakim Von Braun: Ett tänkbart scenario vore att en trojan skrivs för att angripa en viss sorts bankkunder som gör sina bankärenden på Internet. Trojanen skulle kunna kopiera det som användaren gör på systemet innan ordern till banken har skickats iväg. Det är viktigt att trojanen tar hand om informationen innan den skickas iväg på Internet, då den krypteras. Detta innebär att morgondagens trojaner kommer att förses med verktyg som kan användas för ”man in the middle attacker”. Detta kallas också ibland för ”man in the browser”, vilket innebär att trojanerna fungerar som en mellanhand mellan avsändare och mottagare. Sannolikt är att den skadliga koden kommer bli bättre på att kopiera digitala certifikat som används vid bankaffärer. Det kommer att ske ännu flera riktade attacker i framtiden än idag. Antivirusprogrammen kan inte se och bekämpa en ny och okänd trojan. Det kommer krävas nya verktyg än antivirusprogram för att bekämpa den skadliga koden i framtiden.

3.3.6 Vilken typ av skadlig kod kommer vara dominerade i framtiden?

Viiveke Fåk: Skadlig kod som sprids via e-post, fast den kommer att vara mycket mer riktad än vad den är idag. Om man skapar skadlig kod som inte är fruktansvärt farlig och destruktiv och konstruerar den så att den sprider sig långsamt dröjer det länge innan antivirustillverkarna skapar något motmedel.

Johan Jarl: Den skadliga kod som är bäst lämpad för riktade attacker mot specifika mål kommer vara den dominerande. De globala attackerna eller den globala spridningen av skadlig kod kommer att minska i framtiden. Däremot kommer den att riktas mer mot antingen specifika privatpersoner eller specifika företag. Allting görs med ekonomisk vinning i åtanke. Koden kommer att göra mindre och mindre skada, men mer vara ute efter att ge dess skapare eller dess användare någon form av vinning.

Per Hellqvist: Trojanerna kommer sannolikt att dominera även om fem år, då de fungerar så bra för sina tillverkare idag. Man ändrar inte på ett vinnande koncept.

Joakim Von Braun: Trojaner med nytillkomna möjligheter.

3.3.7 Kommer nya typer av skadlig kod att tillkomma?

Viiveke Fåk: Trojaner som har specifika mål som de är riktade mot kommer troligen i ännu högre utsträckning än idag skapas och utvecklas ytterligare. Dessa kan senare användas till att exempelvis bryta sig in användares datorer och stjäla koder eller annan hemlig information. Det kommer troligen inte att tillkomma några nya huvudtyper av skadlig kod, då de typer som finns idag är så generella och heltäckande. Däremot kommer det säkerligen att tillkomma nya undertyper av skadlig kod.

Johan Jarl: Det kommer det absolut att göra. På bland annat mobilsidan och handdator-fronten kommer det att hända mycket. Från att skadlig kod i stort sett bara existerat på PC-datorer som använt Microsoft Windows tidigare har det idag utvecklats till att även kunna smitta många andra former av enheter. Denna utveckling kommer att fortsätta. Tv-spel såsom Sony Playstation och andra enheter kan också komma att bli utsatta för skadlig kod i större utsträckning.

Per Hellqvist: De kommer att påminna om de som redan finns, men om det tillkommer någon ny filtyp för datoranvändare så kommer det möjligen att även tillkomma någon ny form av skadlig kod för att angripa dem.

Joakim Von Braun: Det är sannolikt, men det är svårt att sia om vad som kommer att komma. Sannolikt är att den kommer att drabba telefoner och andra enheter i högre utsträckning än idag. Utvecklingen på Internet styr detta, hur man betalar och vart brottslingarna kan tjäna pengar. Brottslingarna väger inkomsterna från att ägna sig åt detta mot vad de kan tjäna pengar på andra områden. Pengarna styr.

3.3.8 Vilka trender kommer vi att få se inom den skadliga koden i framtiden?

Viiveke Fåk: Sannolikt kommer de så kallade toolkitsen att bli ännu vanligare än vad de är idag. Den skadliga koden kommer att bli mer komplex än tidigare. Skadlig kod kommer i ännu högre grad skrivas på av ekonomiska skäl.

Johan Jarl: Den skadliga koden kommer i högre utsträckning angripa andra enheter än just datorer. Mobiltelefoner och handhållna enheter är två tänkbara mål. Själva koden kommer att bli mer intelligent och de som skapar den kommer att bli mer organiserade.

Per Hellqvist: Ungefär samma som idag, men möjligen kommer vi att få se mera av skadlig kod som genomför IT-krigsföring och politiska attacker. Troligen får vi se ännu mera av industrispionage. Troligen kommer sociala nätverk som Myspace och Facebook att bli mer utsatta. Detta gäller även onlinespel och liknande företeelser. Men egentligen är detta mest varianter på gamla företeelser och inte så mycket nytt.

Joakim Von Braun: Den skadliga koden kommer att användas mera i utpressningssyfte. Ett exempel på detta skulle kunna vara att en hackare krypterar ett företags kunddatabas, och sedan kräva betalning för att företaget skulle få tillbaka den okrypterad. Allt kommer att handla om pengar och information, det gäller bara att utveckla brottskoncepten.

3.3.9 Kommer kostnaden för den skadliga kodens skadeverkningar att öka eller minska i framtiden?

Viiveke Fåk: Det är svårt att säga, men den kommer troligen att öka.

Johan Jarl: Den kommer sannolikt att öka.

Per Hellqvist: Det är troligt att banker och försäkringsbolag inte kommer vara lika snälla som de hittills varit med att betala ut ersättning om någon har länsat en persons Internetbank eller liknande. Detta innebär att banker och även försäkringsbolag kommer flytta en del av sina kostnader till kunderna, vilket innebär att kunderna sannolikt kommer bli försiktigare i framtiden. Sannolikt är att de direkta kostnaderna kommer att minska och att de indirekta kostnaderna kommer att öka. Den totala kostnaden kommer sannolikt att öka.

Joakim Von Braun: Den kommer att öka avsevärt, dels för att den skadliga koden används oftare och oftare samt i större och större sammanhang. Det kommer att kunna löna sig mer för tillverkarna av den skadliga koden i framtiden. Det kommer att uppkomma situationer där drabbade företag eller organisationer måste betala utpressarnas krävda summor. Vad gör man annars när de kriminella går under jorden och de drabbade kanske står där med den ovan nämnda krypterade kunddatabasen utan möjlighet att få hjälp? Alternativet att skicka polisen på de kriminella kan ju innebära att de går under jord. En annan möjlighet är att information stjäls av skaparna av fientlig kod, och att de hotar med att publicera den om inte de får betalt. Detta skulle medföra att företagen skulle se till att betala i högre utsträckning framöver när det handlar om utpressning. Även DDOS-attacker är något som de kriminella skulle kunna använda sig av i utpressningssyfte.

3.3.10 Ge ett tänkbart exempel på ett framtidsscenario som kan hända i ett ”skadligkodsammanhang”

Viiveke Fåk: En person sitter uppkopplad mot Internet och någon har med en trojans hjälp lyckats skapa en bakdörr i datorn som möjliggörs av hur bristfälligt operativsystemet skapades för ett antal år sedan. Denna person placerar sin skadliga kod i datorn. Användaren av datorn märker att det förekommer trafik in och ut i datorn via Internet, trots att den inte arbetar mot Internet för närvarande. Detta väcker användarens uppmärksamhet. Den skadliga koden försöker sprida sig vidare och genom lite tur och skicklighet lyckas användaren, som tycks vara duktigare än genomsnittet, lokalisera det system som smittade ner det egna systemet. Dock visar det sig att detta inte var skaparen av den skadliga koden, utan denna dator var också smittad i sin tur. Användaren varnar omgivningen om förekomsten av den skadliga koden, och den reagerar inte utan bara gäspar och säger ”inte en sån till”.

Johan Jarl: En person för ett viktigt samtal med en högt uppsatt person. Skadlig kod har tagit sig in i mobiltelefonen och när man har lagt på och avslutat samtalet har den skadliga koden spelat in det och gjort en ljudfil av det, vilken sen sänds vidare av telefonen.
Ett annat scenario är att skadlig kod tar sig in i din mobiltelefon som du har med dig på ett viktigt möte och att den då automatiskt tar bilder eller spelar in det som sägs på mötet. Den kan även koppla upp sig mot andra telefoner eller mot annan utrustning i sin omgivning och sprida smittan vidare eller stjäla konfidentiell information av olika slag.

Per Hellqvist: Det kommer nog inte att föreligga någon direkt skillnad från idag, hackern lurar användaren eller skickar en e-post och tar ett starkt grepp om hemdatorn som kan användas

som ett verktyg att angripa andra med eller så stjäl hackern information ur datorn. Bara man kan lura användaren äger hackern datorn, och då kan han göra vad han vill.

Joakim Von Braun: Identitetsstölder med hjälp av Internet och skadlig kod skulle kunna vara ett tänkbart scenario. Exempelvis skulle ett företag kunna sättas i konkurs av någon som utger sig vara dess ägare. Hus och fordon skulle kunna skrivas över så att andra äger dem. För att kunna bestrida detta måste den verklige ägaren måste kunna bevisa sig själv oskyldig, annars är tillvägagångssättet lagligt.

4 Analys och diskussion

I detta kapitel analyseras, diskuteras, kommenteras och jämförs de svar som framkommit i intervjuerna med de som framkommit vid studiet av litteraturen.

4.1 Kommer skadlig kod att bli mer eller mindre förekommande i framtiden?

Samtliga respondenter tror att den skadliga koden kommer bli mer förekommande i framtiden än vad den är idag. En av respondenterna anser det vara osäkert hur utvecklingen av den skadliga koden kommer att te sig inom den närmaste framtiden då det skett en så explosionsartad ökning under år 2007. Han menar att den explosionsartade ökningen av kända former av skadlig kod under år 2007 kanske bara är en tillfällighet, eller så är det inte det, utan början på en ny trend. Samma respondent menar att det verkligen är sannolikt att det kommer ske en framtida ökning av den skadliga koden då mänskligheten kommer att använda datorer och andra enheter som har operativsystem i högre utsträckning i framtiden än vad som är fallet idag.
En stor anledning till att den skadliga koden exploderat så under år 2007 beror på att det är främst trojaner som tillverkas för tillfället. Det rör sig om ett ganska litet antal trojaner, som ändras minimalt från tillfälle till tillfälle och där varje enskild ny trojan utgör en ny form av skadlig kod. Eftersom trojanerna spås vara den dominerande formen av skadlig kod i framtiden kan man tolka det som att denna utveckling kommer att fortsätta och att vi kommer att få se en fortsatt ökning i framtiden.
Två av respondenterna säger att eftersom den skadliga koden är lönsam för dem som skapar den idag, samt att den är enkel att tillverka, finns det ingen anledning att tro att den inte kommer att öka ytterligare.

Litteraturen håller med respondenterna då den också tror att den skadliga koden kommer att bli mer förekommande i framtiden. Detta beror på en rad olika anledningar. En anledning är att allt fler datorer kopplar upp sig mot Internet samtidigt som de får större och större bandbredd. Vidare kommer Internet i sig kommer att fortsätta att förändras till att ännu mer uppfylla det som kallas ”Web 2.0” och på så vis ge skaparna av den skadliga koden ännu fler angreppsmål. Genom att se på de trender som rått de senaste tolv åren kan man tydligt se att både antalet kända former av skadlig kod och antalet förekomster av dem ökat över tiden. Dessutom har det skett en explosionsartad ökning i bägge avseendena år 2007, vilket tyder på en fortsatt ökning. Litteraturen förespår även en ökning av skadlig kod till andra enheter än datorer, vilket ytterligare styrker trovärdigheten i detta påstående.

Sammanfattningsvis anser både respondenter och litteratur att det ser ut som att vi kommer gå mot en framtid där skadlig kod är mer förekommande såväl i antalet kända former såsom i antalet förekomster.

4.2 Kommer nya typer av skadlig kod att tillkomma i framtiden?

Alla respondenter är överens om att det kommer att tillkomma nya typer av skadlig kod under de närmaste åren. Två av respondenterna anser att det med säkerhet skulle tillkomma nya typer av skadlig kod till exempelvis mobiltelefoner och till handhållna enheter. En av dessa respondenter tror att det kommer tillkomma nya typer av skadlig kod som angriper spelkonsoller. En av respondenterna anser att det är osannolikt att någon ny huvudtyp av skadlig kod kommer att tillkomma, utan denne tror snarare att det i så fall tillkommer nya undertyper. En tredje respondent anser att det kommer att tillkomma nya typer av skadlig kod i takt med att nya filtyper tillkommer, oavsett vad det är för sorts enhet de körs på. Han menar också att det i stort sett är operativsystemen som sätter gränserna för vad som kommer att ske med den skadliga koden i framtiden.

Litteraturen stöder det som respondenterna anser då även den tror att det kommer att tillkomma nya typer av skadlig kod i framtiden. Speciellt troligt anses det vara att det kommer att tillkomma nya former av skadlig kod till mobiltelefoner och andra enheter, som exempelvis spelkonsoller och handburna enheter. Skadlig kod kommer troligen att vara speciellt riktade mot så kallade ”smart phones”, som är i stark tillväxt idag, och som det möjligen kan behövas nya former av skadlig kod för att komma åt. En ganska stor del av den kommande skadliga koden kommer troligen att inrikta sig på Windows Vista, eller dess efterföljare, som i skrivande stund går under namnet Windows 7. Det är möjligt att detta kan ge upphov till nya typer av skadlig kod. Vidare nämns det i litteraturen att det kommer att skapas flera exempel på skadlig kod till andra operativsystem, såsom Apples X OS och Unix, och även här är det tänkbart att detta kan ge upphov till nya typer av skadlig kod.

Sammanfattningsvis anser både respondenter och litteratur att det kommer att tillkomma nya typer av skadlig kod, men att det är svårt att sia om vilka dessa kommer att vara.

4.3 Vilka typer av skadlig kod kommer att vara de dominerade i framtiden?

Tre av de fyra respondenterna ansåg att trojanerna kommer att vara den dominerande formen av skadlig kod i framtiden. Detta förklarades med att trojaner idag är den form av skadlig kod som är mest lämpad för att ge ekonomisk vinning åt sin skapare, och att det är osannolikt att detta kommer att ändra sig i den närmaste framtiden. En av dessa tre ansåg att det är sannolikt att toolkits som kan användas för att skapa skadlig kod, företrädesvis trojaner, kommer att bli vanligare i framtiden, vilket stöder påståendet att trojaner kommer att vara den dominerande formen av skadlig kod i framtiden. Eftersom det tycks stå helt klart att Microsofts produkter kommer att vara de dominerande även om fem års tid, kan man utveckla svaret till att den dominerande formen av skadlig kod i framtiden kommer att vara de trojaner som kan drabba den just då mest populära och mest använda typen av Microsoft Windows.

Den fjärde respondenten trodde att skadlig kod som sprids via e-post fortfarande kommer vara den dominerande i framtiden, med den skillnaden att den kommer att vara mera riktad mot specifika mål än vad den är idag. Samma respondent nämnde också att denna kod sannolikt kommer att följa den gamla principen om att sprida sig långsamt och försöka undvika att upptäckas samtidigt som den inte gör mycket skada.

Litteraturen håller även i detta avseende med majoriteten av de intervjuade respondenterna då den anser att trojaner som inriktar sig på Microsoft Windows kommer att vara den dominerande formen av skadlig kod i framtiden. Detta hänger delvis samman med att eftersom trojaner ofta skapas med hjälp av toolkits, som anses bli vanligare i framtiden, är det rimligt att anta att även trojanerna bör fortsätta vara dominerande i framtiden. Dessa toolkits ger även måttligt kunniga personer chansen att skapa egna trojaner eller att fjärrstyra redan skapade trojaner med enkla medel. Så kallad ”modular malicious code” och ”downloaders”, som oftast utgörs av trojaner, anses kunna bli vanligare i framtiden. Orsaken till detta är att de för närvarande är de mest inkomstbringande typerna av skadlig kod. Det är sannolikt att detta kommer att fortsätta vara fallet under ytterligare några år. Detta beror på att dessa trojaner har ett otroligt brett användningsområde och att de är relativt enkla att skapa samt att fjärrstyra och ge ytterligare funktionalitet när koden väl infekterat målet. Om det skulle behövas kan de också ofta anpassas till ändrade förhållanden. De är helt enkelt de mest mångsidiga verktygen som hackarna har till sitt förfogande idag. Ett indicium på att trojanerna kommer vara dominerande i framtiden är att de ökade med hela 500 % under 2007, vilket är en stor ökning.

Sammanfattningsvis kan man säga att respondenterna och litteraturen även här är överens om att det troligen är trojanerna som kommer att dominera den skadliga kodens värld inom den närmaste framtiden.

4.4 Hur skiljer sig framtidens skadliga kod från dagens i avseende på vad och vilka den kan drabba?

Tre av respondenterna anser att en stor skillnad i framtiden är att mobiltelefoner och handhållna enheter samt spelkonsoller såsom Sony Playstation och liknande kommer att drabbas i högre utsträckning.
Två av respondenterna pekar på att det är sannolikt att den skadliga koden i högre utsträckning än idag kan komma att användas i politiska syften eller till IT-krigsföring och industrispionage.
Två av respondenterna pekar på att när det skapas nya enheter, eller nya operativsystem, så kanske det även skapas nya former av filer. Dessa nya filtyper kommer naturligtvis också att utsättas för skadlig kod, om detta ger hackarna möjligheten att tjäna pengar eller att stjäla information.
En av respondenterna menar att ”virtuella världar”, onlinespel, sociala nätverk som Myspace och Facebook och liknande sidor som utgör exempel på ”Web 2.0” kommer att bli mer utsatta i framtiden.
En annan av respondenterna tror att hackare kan komma att angripa företag i högre utsträckning än idag och exempelvis stjäla och kryptera företagets kunddatabaser för att sedan utpressa företaget. Samma respondent pekade också på att det är troligt att användare som genomför bankärenden online kommer att vara mer utsatta för risk. Sannolikt kommer den skadliga koden då att använda sig av det som kallas för ”man in the middle” attacker eller ”man in the browser” attacker, vilket innebär att hackarna fungerar som en mellanhand mellan användaren och Internetbanken. Vidare menade samma respondent att hackarna skulle kunna

hota ett eventuellt företag med att genomföra DDOS-attacker om företaget inte betalade den avtalade summan pengar. Samma person anser också att det är troligt att hackare i framtiden kommer bli bättre på att kopiera de så kallade elektroniska certifikat som används idag vid exempelvis bankaffärer.
En av respondenterna ansåg att det kommer att bli vanligare med attacker mot IP-telefoni i framtiden.

Litteraturen håller med respondenterna om att troligen kommer att bli betydligt vanligare med skadlig kod som drabbar mobiltelefoner och handhållna enheter samt flyttbara medier såsom USB-minnen eller externa hårddiskar. Även musikspelare riskerar att drabbas i högre utsträckning. Litteraturen håller med respondenterna om att det kommer bli vanligare med skadlig kod som riktar sig till mobiltelefoner och andra enheter i framtiden. Det spås att den dag det blir vanligt förekommande att användarna använder mobiltelefoner eller andra enheter för att genomföra bankärenden på så kommer skapandet av skadlig kod till dessa enheter att formligen explodera. Det spås att den utveckling som skett för den skadliga koden inom datorernas värld i viss utsträckning kommer att återupplevas för mobiltelefonerna.

Även spelkonsoller och liknande som kan koppla upp sig mot Internet riskerar att drabbas av skadlig kod i högre utsträckning i framtiden. Något som också nämns är att det är tänkbart att skadlig kod kan sprida sig från en bärbar dator till en annan via trådlöst nätverk i framtiden. Detta innebär att datorer som är tillräckligt nära varandra fysiskt skulle kunna smitta varandra.
Litteraturen håller med om att det som populärt kallas ”Web 2.0” anser kommer att bli ett hett eftertraktat mål i framtiden, med allt som det innebär. Exempel på detta är sociala nätverk, virtuella världar och onlinespel.
Vidare anser litteraturen, precis som en av respondenterna, att IP-telefonin riskerar att attackeras mera i framtiden, något som nästan inte alls sker idag. Det spås att IP-telefonin kommer att attackeras i 50 % högre utsträckning under 2008 än vad som blev fallet 2007.
Enligt litteraturen kommer det att skrivas betydligt mer skadlig kod till Windows Vista under de kommande åren. Detta då det är det operativsystem som Microsoft just nu prioriterar fram till det att Windows 7 släpps, vilket är planerat att ske år 2010. Litteraturen anser också att det är sannolikt att skadlig kod i högre utsträckning kommer att skrivas till andra operativsystem, såsom Apples X OS och Unix.
Så kallad ”Instant messaging” spås vara ett framtida attackmål för den skadliga koden, och ett exempel på ett program som använder sig av det idag är exempelvis MSN.
Litteraturen tror att den skadliga koden kommer att fortsätta att ligga steget före tillverkarna av programvara, och därmed fortsätta att utnyttja säkerhetshål i applikationer innan de täpps igen.
Att det kommer att bli lättare för hackarna att se vem och vad som har en specifik IP-adress i framtiden, kommer att möjliggöra att de på ett enklare och effektivare sätt kommer att kunna angripa specifika mål i högre utsträckning.

Sammanfattningsvis anser både respondenterna och litteraturen att mobiltelefoner och andra enheter i högre grad kan drabbas av skadlig kod i framtiden. Vidare nämns IP-telefoni och virtuella världar, onlinespel, bankärenden via Internet samt sociala nätverk som Facebook och Myspace, eller andra former av det som kallas för Web 2.0. Chattprogram som använder sig av så kallad ”instant messaging” anses också kunna vara ett angreppsmål. Det är även mycket sannolikt att Windows Vista och dess efterföljare, Windows 7, kommer att utsättas för angrepp med hjälp av skadlig kod.

4.5 Hur skiljer sig framtidens skadliga kod från dagens i avseende på spridningssätt?

En respondent menar att nya tekniska lösningar inom operativsystem och hårdvara eller användandet av nya metoder kommer att ge skaparna av skadlig kod nya möjligheter att sprida den. En tänkbar metod för att sprida den skadliga koden är att på något sätt använda sig av någon av alla dessa automatiska uppdateringar av programvara som numera ofta dimper ner i datorerna. Respondenten menade dock att det vanligaste sättet för skadlig kod att sprida sig även i framtiden kommer att vara via e-posten.
En annan respondent menar att det kommer att spridas ännu mer skadlig kod via fildelningsprogram och chattprogram i framtiden än vad det gör idag. Samma person tror att skadlig kod sannolikt skulle spridas i högre utsträckning via Bluetooth, MMS eller SMS på mobiltelefoner i framtiden. Denna person tror också att de ”gamla” maskarna, som sprider sig självt vidare eller hjälper andra former av skadlig kod att sprida sig vidare via e-post inte kommer att försvinna i framtiden.
En tredje respondent menar att det sannolikt finns tillräckligt med sätt att sprida den skadliga koden på redan idag, och att hackarna knappast behöver skapa ytterligare metoder för att göra det på. Han menade dock att sociala nätverk såsom Facebook och Myspace kommer att vara mål för hackarna i framtiden, och som sådant även en potentiell källa för spridning av den skadliga koden. Detta gäller även för andra exempel av ”Web 2.0”.
En fjärde respondent tror att det troligen kommer att bli lättare att smittas av skadlig kod bara genom att befinna sig ute på Internet och besöka en smittad hemsida. Han menar att det finns stora möjligheter att gömma ett script på en hemsida som då kunde konstrueras så att det skulle ladda ner en fil och installera den per automatik.

Litteraturen anser, precis som en av respondenterna, att de sociala nätverken, samt andra former av ”Web 2.0” kommer att drabbas mera av skadlig kod i framtiden. Detta innefattar även onlinespelen och virtuella världar. Den skadliga koden kommer därför troligen ta sig in i system via omvägen ”Web 2.0” i framtiden istället för att angripa det aktuella systemet direkt.
Ett tänkbart spridningssätt som litteraturen nämner, som påminner om vad en av respondenterna trodde, är att den skadliga koden kan utge sig för att vara en uppdatering till exempelvis ett av onlinespelen och som en sådan utlova ökad funktionalitet.
I likhet med en av respondenterna anser litteraturen att chatt-programmen i högre grad än idag kommer drabbas av skadlig kod och även användas i högre utsträckning för att sprida den vidare.
Litteraturen nämner också att skadlig kod till mobiltelefonerna kommer att spridas i högre grad via Bluetooth, e-post och andra sätt, vilket även en respondent trodde.
Vidare nämner litteraturen att det sannolikt kommer att skapas fler Bots i framtiden, vilket i sin tur kommer att hjälpa till att sprida den skadliga koden vidare. Det spås till och med att det eventuellt kommer att skapas Botnets som går på mobiltelefoner istället för datorer. Detta möjliggörs av att mobiltelefonerna kommer att få större processorkraft i framtiden, och dessutom gå på ett telefonnät med större bandbredd än idag.
Dessutom kommer det finnas fler datorer och andra system att smitta i framtiden, vilket i sig föder möjligheter att sprida den skadliga koden vidare på ett enklare sätt. Vidare kommer uppkopplingarna mot Internet bli fler och snabbare, vilket ytterligare ökar möjligheterna. En annan möjlig smittoväg för skadlig kod anser litteraturen vara det ökande antalet trådlösa nätverk som inte alltid är väl skyddade. Skadlig kod som utnyttjar det trådlösa nätverket skulle kunna skapas för att hoppa från en bärbar dator till en annan, och på så vis sprida sig vidare.

Sammanfattningsvis rådde det här lite olika åsikter om vilka skillnader som kan uppstå i framtiden jämfört med idag angående den skadliga kodens spridningssätt.
Dock nämndes att nya tekniska lösningar skulle kunna alstra nya möjligheter för den skadliga koden att sprida sig på. Ett tänkbart framtida spridningssätt som skaparna av den skadliga koden skulle kunna använda sig av för att sprida den på ansågs kunna vara att använda sig av alla de automatiska uppdateringarna av program som idag flitigt används. Sociala nätverk, chatprogram, onlinespel och virtuella världar nämndes som tänkbara framtida sätt att sprida den skadliga koden på, samt även via andra former av det så kallade "Web 2.0". Skadlig kod kommer troligen i högre grad än idag själv sprida sig vidare genom att blogga eller chatta. Det varnades också för möjligheten att det skulle bli lättare för skadlig kod att sprida sig via "vanliga" hemsidor. Att fler och fler datorer och enheter kopplar upp sig emot Internet samtidigt som bandbredden på uppkopplingarna mot Internet ökar hela tiden ger också den skadliga koden större möjligheter till att sprida sig vidare. Till mobiltelefoner och andra enheter ansågs det att Bluetooth, MMS eller SMS eller e-mail i högre grad än i dag kommer att användas för spridning av den skadliga koden. Mobiltelefoner kommer att få starkare processorer och kommer att gå på telefonnät med allt större bandbredd, detta möjliggör nya spridningssätt för den skadliga koden. Det är också tänkbart att skadlig kod kan komma att spridas mellan bärbara datorer via dessas trådlösa nät.

4.6 Hur skiljer sig framtidens skadliga kod från dagens i avseende på hur den kan undgå upptäckt?

Alla fyra respondenterna anser att en ökad användning av rootkits är det mest sannolika framtidsscenariot och troligen det mest effektiva sättet för skaparna av den skadliga koden att dölja den.
Två respondenter tror att framtidens skadliga kod kommer att försöka att undgå upptäckt genom att vara föränderlig. Exempelvis nämner dessa respondenter de nya trojaner som finns redan idag, som i många fall uppdaterar sig automatiskt med jämna mellanrum. På så vis får de ett annat utseende, och kan därmed undgå upptäckt då de inte motsvarar några signaturer som finns i antivirusprogrammen. För att signaturer till antivirusprogrammen av antivirusföretagen måste dessa exempel av skadlig kod dyka upp ett antal gånger först. Gör de inte det utvecklas inte några signaturer heller. Detta visar på den inbyggda svaghet som finns i dagens antivirusprogram och det faktum att de är mer reaktiva än proaktiva.
En av dessa två respondenter anser att framtidens trojaner inte kan upptäckas av antivirusprogram och att det krävs nya verktyg än dessa för att bekämpa den skadliga koden i framtiden.
En respondent anser att framtidens skadliga kod kan komma att använda sig av så kallad tunnling av trafik för att undgå upptäckt på nätverk och på Internet. Detta innebär att den skadliga koden döljer den egna ip-trafiken genom att den skapar den inuti annan, befintlig ip-trafik. Detta upptäcks då inte av användaren eller det egna systemet. Samme respondent anser att ett sätt att fjärrstyra exempelvis en trojan utan att detta upptäcks kan göras genom att använda sig av ovanstående tunnling. Enligt respondenten kan detta även göras genom att lägga in styrkoder i det tomrum som finns i den så kallade header som finns i datafiler och som talar om hur resten av filens innehåll ska tolkas av operativsystem och applikationsprogram.
En respondent tror att den skadliga koden kommer att konstrueras så att den helst inte upptäcks alls innan den går till attack. Denna taktik har används förr, men den kommer sannolikt vara framgångsrik även i framtiden.

En annan respondent anser att den skadliga koden bör försöka göra så lite skada som möjligt för att på så vis inte dra till sig onödigt mycket uppmärksamhet och därmed också kanske undvika att hamna i antivirusprogrammens signaturlistor.

Även litteraturen varnar för rootkit-teknologin som troligen kommer att vara den effektivaste metoden för att försvåra den skadliga kodens upptäckt i framtiden.
Vidare nämner litteraturen att polymorfism samt metamorfism också är tänkbara metoder. Det är tänkbart att dessa former av skadlig kod kan komma att utvecklas så mycket att antivirusprogrammen inte kommer att hitta dem. Framtidssynen är mörk, och vissa experter tror att antivirusprogrammen överhuvudtaget kommer att få det mycket svårare att klara av sitt jobb i framtiden. Då den skadliga koden troligen kommer att bli mer riktad än idag tror även litteraturen att den inte kommer att göra lika stort väsen av sig i framtiden. Den kommer då upptäckas relativt få gånger och därmed kanske även mera sällan ge upphov till att antivirustillverkarna skapar en signatur för den.
Litteraturen tror, precis som respondenterna, att trojaner kommer att vara den vanligaste formen av skadlig kod i framtiden. Om detta stämmer kommer vi få se många exempel på så kallade ”modular malicious code” och ”downloaders”, som oftast utgör exempel av trojaner. Eftersom dessa trojaner har förmågan att ladda ner ytterligare filer utifrån, kan dessa trojaner förändra sitt utseende över tiden och på så vis försvåra för antivirusprogrammen.

Sammanfattningsvis anses det att rootkit-teknologin troligen kommer att vara den mest effektiva metoden att använda sig av för skadlig kod som vill undvika att upptäckas i framtiden. Andra liknande metoder som nämns var de trojaner som finns redan idag och som kan uppdatera sig automatiskt och på så vis ändra sitt utseende och därmed undgå upptäckt. Polymorfism och metamorfism anses vara tänkbara tillvägagångssätt. Den skadliga koden kan också komma att gömma sig mer effektivt i annan IP-trafik för att undgå upptäckt. Vidare anses det att den gamla metoden att göra så lite väsen som möjligt kan vara ett vinnande koncept även i framtiden, vilket sannolikt kommer att vara en naturlig utveckling då framtidens skadliga kod troligen kommer vara mer riktad mot specifika mål än idag.

4.7 Hur skiljer sig framtidens skadliga kod från dagens i avseende på vilken skada den kan göra?

Samtliga respondenter tror att de ekonomiska drivkrafterna bakom att skapa skadlig kod kommer att öka i framtiden, och därmed kommer framtidens skadliga kod också sannolikt att orsaka större ekonomisk skada än idag.
Tre av respondenterna tror att framtidens attacker kommer att bli ännu mera riktade än vad de är idag. På så vis kommer framtidens skadliga kod troligen att göra mer avsiktlig och planerad skada än vad som tidigare varit fallet.
En av respondenterna anser att det är troligt att hackarna redan idag skapat tillräckligt många sätt att orsaka skada på. Dock tror samma respondent att det är tänkbart att hackare i framtiden mera kommer att använda sig av vad som kallas för ”datadiddlers”, vilket innebär skadlig kod som ändrar på slumpvisa siffror eller tecken i databaser eller dokument. Om en hacker kopierar ett företags databas och sedan ändrar på den befintliga som företaget har på sin server och det görs en backup på denna, så har företaget därefter bara en skadad databas, och då kan en hackare idka utpressning i utbyte mot den korrekta databasen.
Även en annan av respondenterna menar att det är möjligt att det kommer att skapas mer skadlig kod som kommer att användas i utpressningssyfte i framtiden. Detta gäller även möjligheten att utpressa företag i utbyte mot att inte genomföra DDOS-attacker.

Två av respondenterna anser att framtidens skadliga kod kan användas till spionage. Exempelvis kan en mobiltelefon styras av skadlig kod så att den spelar in samtal som förs på telefonen, spelar in ljud från omgivningen, eller tar bilder med telefonens kamera. Denna information kan sedan skickas vidare av telefonen i form av MMS eller på andra sätt. En av dessa personer anser också att den skadliga koden kan användas i terrorist-syften samt till IT-krigsföring.

En av respondenterna anser att det är troligt att exempelvis trojaner kommer att skrivas för att angripa en viss sorts bankkunder som gör sina bankärenden på Internet. Dessa kan då skrivas för att ta hand om information eller ändra i det som användaren ska skicka iväg till Internetbanken innan informationen krypteras för att skickas över Internet. Han menar med andra ord att morgondagens skadliga kod kommer att förses med verktyg som kan användas för ”man in the middle attacker” eller ”man in the browser attacker”. Samma respondent menar att det är tänkbart att skadlig kod i högre utsträckning än idag kan komma att användas för att stjäla identiteter av olika slag. Vidare kan skadlig kod användas till att exempelvis sätta ett företag i konkurs av någon som utger sig vara dess ägare. Dessutom skulle skadlig kod kunna användas till att skriva över ägodelar så att de får en ny ägare.

Litteraturen tror, precis som samtliga respondenter, att de ekonomiska drivkrafterna bakom skapandet av den skadliga koden kommer att bli viktigare i framtiden. Därför anses det troligt att den skadliga koden kommer att orsaka mer ekonomisk skada. Exempelvis kommer troligen bankaffärer eller andra transaktioner av pengar som sker online att attackeras hårdare av den skadliga koden i framtiden.
Litteraturen håller med vissa respondenter om att så kallad ”ransomware” och ”cryptoware” kommer bli vanligare i framtiden.
Vidare antar även litteraturen att framtidens attacker kommer att bli ännu mera riktade än vad de är idag. Detta medför att de skador som den skadliga koden gör är mer planerade än tidigare.
Litteraturen tror också, precis som vissa av respondenterna, att mobiltelefoner kan komma att styras av skadlig kod för att spela in samtal, ta bilder med mera för att sedan skicka denna information vidare. Andra nya möjligheter som mobiltelefoner skulle kunna ge hackarna är enligt litteraturen så kallad ”smishing”, vilket är phishing som sker via SMS, eller ”vishing”, vilket är phishing som sker via ljud i telefonen.
Litteraturen tror att det i framtiden kan komma rootkits som är så skadliga att de inte går att få bort utan att formatera hårddiskarna och installera om allting på nytt. Dessa kan vara så sinnrikt konstruerade att de inte kan upptäckas inifrån det egna systemet.

Sammanfattningsvis anses det att ekonomisk vinning kommer att vara en ännu starkare drivkraft för skaparna av den skadliga koden i framtiden. Därför är det rimligt att anta att den kommer att göra mer ekonomisk skada än vad som är fallet idag. Det är sannolikt att framtidens skadliga kod kommer att vara mer riktad mot specifika mål än vad som är fallet idag. På så vis kommer skadan att bli mer avsiktlig och planerad än tidigare. Det anses vara sannolikt att framtidens skadliga kod i högre grad kommer att användas i utpressningssyfte. Eventuellt kan bankaffärer via Internet bli mer utsatta i framtiden. Mobiltelefoner kan komma att styras av skadlig kod som förvandlar dem till spionageverktyg. Det är också möjligt att mobiltelefoner kan komma att användas till smishing och vishing.

4.8 Vilka trender förväntas inom den skadliga koden i framtiden?

Denna fråga är svår att besvara på ett kort och enkelt sätt, då många av de svar som getts på de föregående forskningsfrågorna också hör hemma under denna. På grund av detta återges här bara de trender som bedömts viktigast. För tydlighetens skull återges dessa i punktform.

Respondenterna anser att nedanstående trender sannolikt kommer vara de viktigaste inom framtidens skadliga kod:

- Den kommer bli mer förekommande i framtiden.
- Den kommer vara mer riktad mot specifika mål.
- Den kommer i ännu högre grad att skapas för ekonomisk vinnings skull.
- Den kommer att användas mera i utpressningssyfte.
- Den kommer att användas i högre utsträckning än idag för spionage och krigsföring.
- Den kommer att drabba andra typer av enheter.
- Mobiltelefoner i allmänhet och ”smartphones” i synnerhet kommer att drabbas.
- Den kommer drabba ”Web 2.0” i högre utsträckning och även sprida sig vidare via det. Sociala nätverk, virtuella världar, onlinespel samt IP-telefoni kommer i högre utsträckning bli måltavlor för den skadliga koden.
- Bankaffärer via Internet kommer att bli ett vanligt mål för skadlig kod.
- Den kommer spridas via chattprogram och fildelningsprogram i högre utsträckning.
- Rootkits anses vara den form av skadlig kod som bäst kan undvika att upptäckas av antivirusprogram i framtiden.
- Så kallade toolkits kommer att bli vanligare i framtiden.
- Trojaner kommer sannolikt vara den dominerande formen av skadlig kod i framtiden.
- Den totala kostnaden som den skadliga koden orsakar kommer sannolikt att öka.
- Det är oklart om den direkta kostnaden som den skadliga koden orsakar kommer att öka, men det är sannolikt att den indirekta kostnaden kommer göra det.

Litteraturen anser att nedanstående trender kommer att vara de viktigaste i framtiden:

- Litteraturen håller med respondenterna om att den skadliga koden kommer bli mer förekommande i framtiden.
- Litteraturen håller med respondenterna om att den skadliga koden kommer bli mer riktad mot specifika mål för maximal ekonomisk vinning i framtiden.
- Litteraturen håller med respondenterna om att den skadliga koden i ännu högre utsträckning kommer skapas för ekonomisk vinnings skull i framtiden.
- Litteraturen håller med respondenterna om att den skadliga koden i ännu högre utsträckning kommer att användas i utpressningssyfte i framtiden.
- Litteraturen håller med respondenterna om att den skadliga koden i ännu högre utsträckning kommer att skapas för att angripa andra enheter i allmänhet och mobiltelefoner (”smartphones”) i synnerhet.
- Litteraturen håller med respondenterna om att den skadliga koden i ännu högre utsträckning kommer att drabba det som populärt kallas ”Web 2.0” och även sprida sig vidare via det.
- Litteraturen håller med respondenterna om att den skadliga koden i ännu högre utsträckning kommer att drabba de som gör bankaffärer via Internet i framtiden.

- Litteraturen håller med respondenterna om att den skadliga koden i ännu högre utsträckning kommer att drabba sociala nätverk och virtuella världar och onlinespel samt IP-telefoni i högre utsträckning i framtiden.
- Litteraturen håller med respondenterna om att den skadliga koden i ännu högre utsträckning kommer att spridas via chattprogram i framtiden.
- Litteraturen håller med respondenterna om att rootkits kommer att vara den dominerande metoden för skadlig kod som vill undgå upptäckt i framtiden.
- Litteraturen håller med respondenterna om att så kallade toolkits kommer bli ännu vanligare i framtiden.
- Litteraturen håller med respondenterna om att trojaner sannolikt kommer att vara den dominerande formen av skadlig kod i framtiden. Detta gäller speciellt så kallade ”modular malicious code” eller ”downloaders”.
- Litteraturen håller med en av respondenterna om att säkerhetshål i mjukvara kommer att fortsätta vara en viktig inkörsport in i systemen för den skadliga koden även i framtiden.

Vidare anser litteraturen nedanstående, vilket inte överensstämmer med de prognoser som gjorts av respondenterna:

- Bärbara datorer kommer sannolikt att drabbas av skadlig kod som sprider sig via det trådlösa nätverket.
- Kommande versioner av Microsoft Windows kommer utsättas för skadlig kod.
- Andra operativsystem kommer också drabbas i högre utsträckning.
- Det anses sannolikt att antalet bots kommer att öka i framtiden.
- Polymorfism och metamorfism kommer att sätta antivirusprogrammen på hårda prov.

Sammanfattningsvis kommer den skadliga koden bli mer förekommande i framtiden. Vidare kommer den vara mer riktad och kommer att skapas mer för ekonomisk vinning i framtiden än vad som är fallet idag. Den totala kostnaden som den skadliga koden orsakar kommer sannolikt att öka i framtiden. Den skadliga koden kommer att angripa andra enheter än datorer i högre utsträckning. Web 2.0 , mobiltelefoner, IP-telefoni samt chattprogram kommer att angripas mer än vad som är fallet idag. Toolkits kommer sannolikt att bli vanligare i framtiden. Trojaner kommer sannolikt att vara den vanligaste formen av skadlig kod även i framtiden. Rootkits anses bli den dominerande metoden för skadlig kod som vill undgå upptäckt i framtiden.

4.9 Hur skiljer sig framtidens skadliga kod från dagens i avseende på den kostnad som den orsakar?

Samtliga respondenter anser det troligt att den totala kostnaden för den skadliga koden kommer att öka i framtiden. Eftersom samtliga respondenter ansåg att den skadliga koden troligen kommer att bli mer förekommande i framtiden verkar detta rimligt.
En respondent menar att den skadliga koden kommer att användas mer och mer i större och större sammanhang, vilket han ansåg kommer att medföra avsevärt höjda kostnader i framtiden.
En respondent anser att den direkta kostnaden, vilken avser arbetskostnaden för att analysera, reparera och rengöra smittade system, förluster i produktiviteten, förluster av intäkt på grund av sämre fungerande system samt andra direkta kostnader orsakade av den skadliga koden, sannolikt kommer att minska. Dock menade respondenten att de indirekta kostnaderna

kommer att öka, vilket enligt denne därmed skulle leda till att den totala kostnaden trots allt skulle öka.

Det är svårt att hitta övriga källor som törs sia om hur den skadliga kodens ekonomiska skadeverkningar kommer att se ut i framtiden. Dock nämner exempelvis Computer Economics att trots att de direkta kostnaderna har minskat de senaste två åren, så har de indirekta kostnaderna ökat. Detta menar företaget innebär att den totala kostnaden därmed har ökat trots allt (”Annual Worldwide Economic Damages from Malware Exceed $13 Billion”, 2007). Eftersom att de flesta experter verkar tro att den skadliga koden kommer att bli mer förekommande i framtiden, vara mer riktade mot specifika mål, och dessutom verkar kunna orsaka mera skada och i högre utsträckning ha ekonomisk vinning som drivkraft verkar det sannolikt att kostnaden för dess skadeverkningar också kommer att öka i framtiden. En tänkbar utveckling är att de direkta kostnaderna för den skadliga koden kommer att vara relativt oförändrad, medan de indirekta kostnaderna kommer att öka, vilket innebär att den totala kostnaden kommer att öka.

Sammanfattningsvis ansågs det sannolikt att den totala kostnaden som den skadliga koden orsakar kommer att öka i framtiden. Källorna är oeniga om huruvida den direkta kostnaden kommer att öka i framtiden, men att de indirekta kostnaderna kommer att göra det anses sannolikt. Att den totala kostnaden som den skadliga koden orsakat i framtiden skulle öka motiverades med att det är sannolikt att den kommer att bli mer förekommande i framtiden och att drivkrafterna för dess skapare i ännu högre utsträckning än idag kommer att vara ekonomisk vinning. Dessutom anses det sannolikt att den skadliga koden kommer att bli mera riktad i framtiden vilket även det torde höja totalkostnaden.

5 Slutsatser

Huvudsyftet med denna uppsats är att förutspå, så gott det är möjligt, hur den skadliga kodens värld kommer att se ut fem år framåt i tiden från idag. Dessa prognoser om framtiden grundar sig på intervjuer av fyra svenska experter inom ämnet samt på funnen litteratur.

I detta kapitel redovisas de slutsatser som framkommit vid studiet av intervjuerna samt litteraturen. Diskussion förs om huruvida de funna slutsatserna är troliga eller mindre troliga. I slutet av kapitlet besvaras uppsatsens forskningsfrågor.

Nedan återfinns de slutsatser som dragits efter studiet av intervjuerna samt litteraturen:

- *Den skadliga koden kommer sannolikt att bli mycket mer förekommande i framtiden än vad som är fallet idag*. Detta är inte förvånande med tanke på hur **diagram 1** ser ut i avsnitt 2.7.1, där grafen stiger spikrakt uppåt efter år 2005. Antalet förekomster har ökat explosionsartat under senare år, vilket sannolikt kommer att hänga i sig ett tag till. Att denna ökning kommer att fortsätta beror på att det lönar sig för kriminella personer att skapa skadlig kod. Fler och fler datorer kopplas upp mot Internet varje dag, och tekniken ger hela tiden dessa kriminella personer större och större möjligheter att tjäna pengar. Dock är det ändå svårt att vara helt säker på detta. Kanske kan ny teknik och nya metoder förhindra denna utveckling. Exempelvis skulle nya effektiva antivirusprogram och högeffektiva brandväggar kunna förhindra att detta blir verklighet, något som betvivlas av experterna.

- *Det är sannolikt att det kommer att ske en explosionsartad ökning av kända former av skadlig kod*. Gjorda uppskattningar tyder på att det kommer att finnas ungefär 16 miljoner kända exempel på skadlig kod år 2013, att jämföra med dagens ungefärliga siffra på 500 000. Detta påstående kommer att bli sant om dagens utveckling hänger i sig, vilket innebär att antalet kända former av skadlig kod fördubblas var tolfte månad. Eftersom detta har varit fallet de senaste åren känns det rimligt att det kan komma att fortsätta att göra det. Dock går det inte att vara säker. Ny teknik och nya metoder kan möjligen förhindra denna utveckling. Exempelvis skulle nya effektiva antivirusprogram och högeffektiva brandväggar kunna förhindra att detta blir verklighet, men detta är tveksamt.

- *Den skadliga koden blir mer riktad mot specifika mål för maximal ekonomisk vinning*. Detta medför att den skadliga koden får lättare att undgå upptäckt då den exponeras för färre människor som kan upptäcka den och rapportera den till tillverkarna av antivirusprogrammen. Detta möjliggörs delvis av att det kommer att bli allt enklare att se var en specifik IP-adress befinner sig geografiskt på jordklotet. Sannolikt kommer detta också att medföra att de globala epidemierna orsakade av skadlig kod kommer att minska i framtiden. Att skaparna av den skadliga koden också anses bli mer organiserade i framtiden talar också för att detta kommer att ske. Möjligen skulle detta kanske inte bli fallet om situationen ändrade sig i framtiden och att det återigen skulle bli lönsamt att angripa alla datorer och system utan urskillnad. Exempelvis skulle detta kunna bli fallet om en stor del av alla datorer eller system på något sätt utgjorde ett lönsamt mål.

- *Den skadliga koden kommer i ännu högre grad än idag skapas för ekonomisk vinnings skull*. En källa anger att 70 % av alla attacker där skadlig kod används kommer att ha ekonomiska drivkrafter år 2010. De senaste åren har de ekonomiska drivkrafterna bakom den skadliga koden blivit allt vanligare, en utveckling som troligen kommer fortsätta. Det tycks osannolikt att skaparna av den skadliga koden helt plötsligt skulle börja drivas av idealistiska skäl igen och skapa koden för att ge sig själv ära och berömmelse, speciellt när de gör något brottsligt som är straffbart. Om lagarna skulle göras om och därmed avkriminalisera denna typ av verksamhet kanske andelen idealister inom branschen återigen skulle öka. En annan tänkbar anledning till att detta skulle ske kan vara om det inte längre går att tjäna pengar på den skadliga koden, något som känns avlägset idag.

- *Den skadliga koden kommer i högre grad att användas för utpressningssyften i framtiden än idag*. Detta påstående är sannolikt då attackerna troligen kommer att bli mer riktade, samt att skaparna och användarna av den skadliga koden sannolikt kommer att bli mer och mer organiserade och mer drivna av ekonomiska drivkrafter. Det finns redan idag skadlig kod som kallas för ”ransomware” eller ”cryptoware”, och dessa används i utpressningssyften. Denna utveckling skulle bara vara en fortsättning på den trend som rått under ganska lång tid. Att detta inte skulle bli fallet tycks osannolikt, då det, som tidigare skrivits, inte är troligt att skaparna av den skadliga koden återigen skulle bli idealister.

- *Den skadliga koden kommer att användas i högre utsträckning för spionage och krigsföring i framtiden än vad som är fallet idag*. Detta påstående motiveras av att det i allt högre grad är kriminella personer som skriver den skadliga koden för sin egen eller andra personers vinnings skull. Man kan även tänka sig att dessa kriminella

personer med den skadliga kodens hjälp kan få tag i information som sedan kan säljas vidare till andra för pengar. Att skadlig kod skulle kunna komma att användas i terrorist-syften i framtiden tycks vara en trolig utveckling. Visst är det enklare att orsaka skada med hjälp av skadlig kod än att kapa ett par flygplan och flyga in dem i två skyskrapor? Faktum är att den skadliga koden kan skapa större problem och förstörelse dessutom. Ett exempel skulle kunna vara skadlig kod som angriper Pentagon eller något kärnkraftverk. Möjligheterna till spionage och terrorism med hjälp av skadlig kod är i det närmaste outtömliga. Det enda som kan motverka detta är sannolikt att tekniken kan utvecklas till att upptäcka och stoppa alla former av skadlig kod, vilket är en väldigt avlägsen tanke.

- *Den skadliga koden kommer att drabba även andra typer av enheter än idag*. Alla system som använder sig av ett operativsystem kan drabbas av skadlig kod, vilket sannolikt kommer att ske i högre utsträckning i framtiden än idag. Detta förklaras av att den nya tekniken ger skaparna av den skadliga koden nya möjligheter att tjäna pengar på att angripa andra enheter än de traditionella datorerna. Detta anser jag vara en mycket sannolik utveckling, som vi redan sett början på idag.

- *Mobiltelefoner och framförallt ”smartphones” är sannolikt de enheter som bortsett datorerna ligger mest i riskzonen att drabbas av skadlig kod i framtiden.* Det fruktas att den skadliga koden ska kunna göra mobiltelefoner till ett spionverktyg. Det antas även att den skadliga koden kommer att skrivas i ännu högre utsträckning mot dessa ”smartphones” den dag då det blir vanligt att människor genomför sina bankaffärer via Internet över dem. Även här anser jag att det är frågan om en naturlig utveckling, som ligger i linje med vad som vi redan har sett idag. Det finns ju redan idag skadlig kod som är skriven till dessa mobiltelefoner, speciellt till dem som använder sig av operativsystemet Sybian.

- *Sociala nätverk och virtuella världar och onlinespel samt IP-telefoni kommer i högre utsträckning bli måltavlor för den skadliga koden i framtiden*. Den kommer att drabba det som populärt kallas ”Web 2.0” i högre utsträckning och även sprida sig vidare via det. Att IP-telefoni kommer att bli ett större mål i framtiden skvallrar möjligen det faktum att attackerna mot IP-telefonin beräknas öka med 50 % under år 2008. Även detta anser jag vara mycket sannolikt, då även detta skulle vara en naturlig fortsättning av den utveckling som redan påbörjats idag. Fler och fler människor ägnar sig åt dessa företeelser, vilket också ger skaparna av den skadliga koden fler tänkbara måltavlor, och därmed fler möjligheter till ekonomisk vinning.

- *Bankaffärer som genomförs via Internet är något som kommer att bli ett vanligare mål för skadlig kod i framtiden*. Detta anser jag vara högst sannolikt då bankaffärer via Internet är något handgripligt, där skaparna av skadlig kod kan få tag i pengar omedelbart. Det spelar ingen roll hur mycket bankerna krypterar trafiken över Internet ifall om skaparna av den skadliga koden kan arbeta som ”man in the middle” eller som det också kallas ibland, ”man in the browser”. Detta innebär att skaparna av den skadliga koden genomför ändringar i det som görs gentemot Internetbanken innan det sänds iväg och innan den krypterats. Vidare medför också tekniska landvinningar, som exempelvis snabbare processorer, att det blir allt lättare att knäcka krypteringar.

- *Den skadliga koden kommer att sprida sig mer via chattprogram och fildelningsprogram*. Detta är också något som verkar sannolikt då det trots allt är ett

utmärkt sätt att sprida skadlig kod på. Dock är det rimligtvis svårt att rikta den mot specifika mål vid spridning via dessa program, vilket på sätt och vis talar emot det.

Rootkits anses vara den metod som är mest lämpad att användas av skadlig kod som vill undgå upptäckt i framtiden, och därmed är det rimligt att det kommer skapas mer skadlig kod som använder sig av denna metod i framtiden. Då de allra flesta experter är eniga om detta verkar det högst sannolikt att så kommer att bli fallet. *Vissa källor nämner dock att polymorfism och metamorfism också kommer att bli en vanlig metod för skadlig kod att använda sig av när den vill undvika upptäckt i framtiden*.

- *Så kallade toolkits kommer att bli ännu vanligare i framtiden än vad de är idag*. Detta är sannolikt då det finns en stor marknad för dessa verktyg. Genom att skapa toolkits kan skaparna av den skadliga koden undvika att själva göra några brott, utan ”bara” skapa själva verktyget och sälja det. Detta är en programmeringsindustri som ofta lönar sig bättre för programmerarna i fattigare länder än att ägna sig åt ett mer lagligt och ordinärt arbete där lönerna är låga.

- *Trojaner kommer sannolikt vara den dominerande formen av skadlig kod i framtiden*. Detta är troligt, speciellt med tanke på att trojanerna har ökat så starkt på sistone, speciellt dessa trojaner som utgör så kallade ”downloaders” eller ”malicious modular code”. Anledningen till att det är sannolikt att trojanerna kommer att fortsätta att vara dominerande i framtiden är att de är mest dynamiska och därmed enklast kan anpassas till specifika omständigheter och därmed bli den mest lönsamma formen av skadlig kod. Eftersom pengar sannolikt kommer att bli en allt starkare drivkraft bakom den skadliga koden kommer den kod som skapar mest ekonomisk vinning vara den som tillverkas mest.

- *Den totala kostnaden som den skadliga koden orsakar kommer sannolikt att öka*, dock är det osäkert om den direkta kostnaden kommer att göra det. Respondenterna var dock överens om att den indirekta kostnaden kommer att öka. Denna prognos är lite osäker då det har varit svårt att finna andra källor i litteraturen som behandlat detta område. Dock verkar det sannolikt att det kommer att bli på detta sätt då den skadliga koden troligen kommer att få en explosionsartad tillväxt längre fram, vilket kommer att dra med sig ökade kostnader. Naturligtvis kan denna prognos komma på skam om inte den beräknade ökningen av skadlig kod kommer att infrias.

- *Kommande versioner av Microsoft Windows kommer sannolikt i hög grad utsättas för skadlig kod*. Att inte de kommande versionerna av Windows, som utgör den mest populära plattformen, skulle utsättas för skadlig kod i mängder tycks minst sagt osannolikt. Dock kommer sannolikt en relativt stor andel av användarna att hänga kvar vid Windows XP ända fram till år 2013, vilket kan medföra att det inte kommer att skrivas lika mycket till de nya versionerna som annars varit fallet. Dock kommer säkerligen Windows Vista att få en hel del skadlig kod skriven för sig. Något som talar emot att det kommer att skrivas mycket skadlig kod till de nya versionerna är att Microsoft i högre utsträckning än tidigare kommer att satsa på säkerheten i dem.

- *Säkerhetshål i mjukvara kommer att fortsätta vara en viktig inkörsport in i systemen för den skadliga koden även i framtiden*. Detta är ett påstående som tycks verkligt sannolikt, då det är osannolikt att framtida mjukvara är felfri och säker när den aldrig lyckats vara det tidigare i historien.

- *Bärbara datorer kommer sannolikt att bli ett mål för skadlig kod i framtiden med avseende på att den kan komma att sprida sig emellan dessa via det trådlösa nätverket.* Detta kan liknas med de teorier som finns om mobiltelefoner som kanske kan komma att smitta andra mobiltelefoner i sin närhet via exempelvis Bluetooth i framtiden. Denna prognos fanns enbart i den funna litteraturen, och ingen av respondenterna nämnde detta, vilket enligt min mening gör det lite mindre sannolikt.

- *Andra operativsystem drabbas i högre utsträckning i framtiden, exempelvis Apples OS X samt Unix*. Eftersom dessa plattformar traditionellt sett inte drabbats av många exempel av skadlig kod är försvaret mot den också relativt låg då det är troligt att användarna i lägre utsträckning har antivirusprogram och andra försvarsmekanismer. Varför det i framtiden skulle bli vanligare att angripa dessa plattformar än vad som varit fallet tidigare under historien tycks lite märkligt och ologiskt. Denna prognos nämns bara i litteraturen, vilket enligt min mening gör det lite mindre sannolikt.

- *Det anses sannolikt att antalet bots ökar i framtiden*. En möjlig förklaring till detta är att trojaner anses kunna bli den dominerande formen av skadlig kod i framtiden, och bots och trojaner hänger ofta ihop. Vidare används bots ofta till phishing, vilket har ökat rejält de senaste åren. Det anses till och med tänkbart att det kommer att skapas botnets som körs över telefonnätet framöver. Denna prognos hittades enbart i den funna litteraturen, och nämndes inte av någon av respondenterna, vilket enligt min mening gör det lite mindre sannolikt.

Slutligen besvaras de forskningsfrågor som återfinns i problemformuleringen (1.1).

Kommer skadlig kod bli mer eller mindre förekommande i framtiden?
Den skadliga koden blir *mer förekommande i framtiden*, såväl i antal förekomster såsom i antalet kända former av skadlig kod. Det är rimligt att anta att den skadliga koden kommer att vara betydligt vanligare om fem års tid. Detta beror på en mängd olika faktorer.

Kommer nya typer av skadlig kod att tillkomma?
Det kommer att tillkomma nya former av skadlig kod. Det är främst teknikutvecklingen och vilka sorters operativsystem som finns som styr denna utveckling.

Vilka typer av skadlig kod kommer vara de dominerade?
De former av skadlig kod som alstrar mest ekonomisk vinning åt sina skapare är de som kommer att vara de dominerande i framtiden. I dag är det *trojaner som är vanligast, vilket också sannolikt kommer att vara fallet om fem års tid*.

Vilka trender inom den skadliga koden man kan förvänta sig i framtiden?
Troligen kommer den *bli mer förekommande än idag*, samtidigt kommer den troligen att bli *mer riktad mot specifika mål. Ekonomisk vinning kommer troligen att bli en ännu klarare drivkraft* för dess skapare i framtiden. Därmed kommer den skadliga koden troligen användas i *utpressningssyfte* i högre utsträckning än idag. Dessutom kommer den troligen att användas mer för *spionage och krigsföring*. Den kommer troligen att *drabba andra former av enheter* än vad som skett tidigare. Det som kallas för *"Web 2.0"*, *sociala nätverk* och *virtuella världar* samt *IP-telefoni* kommer att drabbas i högre utsträckning än idag. Vidare kommer den skadliga koden sannolikt *sprida sig mer via chattprogram och fildelningsprogram i framtiden*. *Bankaffärer via Internet* kommer sannolikt angripas av den skadliga koden i högre

utsträckning än idag. *Rootkits* anses vara den *bästa metoden* för skadlig kod att använda sig av för att undvika att upptäckas i framtiden. P*olymorfism och metamorfism är två alternativa metoder* som möjligen kan konkurrera med rootkit-metoden. Det anses sannolikt att *toolkits kommer att bli mer vanliga. Trojaner anses bli den form av skadlig kod som kommer vara den dominerande i framtiden*. Sannolikt kommer *den totala kostnaden som den skadliga koden orsakar att öka i framtiden*, även om det är osäkert om den direkta kostnaden kommer att göra det. Däremot verkar det sannolikt att den indirekta kostnaden kommer att öka.

Sedan anses det i litteraturen vara tänkbart att:

- Bärbara datorer kommer att drabbas av skadlig kod som sprider sig via det trådlösa nätverket om två eller flera datorer står tillräckligt nära varandra fysiskt.
- Kommande versioner av Microsoft Windows kommer utsättas för skadlig kod.
- Andra operativsystem kommer också drabbas i högre utsträckning.
- Antalet bots kommer att öka i framtiden.

Hur skiljer sig framtidens skadliga kod från dagens i avseende på vad och vilka den kan komma att drabba?

Det är sannolikt att framtidens skadliga kod i högre grad *kommer att angripa andra enheter än just datorer*. Främst gäller detta *mobiltelefoner i allmänhet och så kallade "smartphones" i synnerhet*. Det är sannolikt att den skadliga koden kommer att vara *mer riktad mot specifika mål i framtiden.* Det anses också tänkbart att *bärbara datorer kan komma att utsättas för skadlig kod som sprids över det trådlösa nätverket. Sociala nätverk, virtuella världar, onlinespel och IP-telefoni eller andra exempel av det som kallas "Web 2.0" är sannolika mål för framtidens skadliga kod. Detta gäller även chattprogram av "instant messaging"-typ som MSN, Yahoo Messenger med flera. Bankaffärer via Internet kommer sannolikt att bli ett större mål* i framtiden än vad det är idag. *Framtida versioner av Microsoft Windows* kommer sannolikt att drabbas av en stor mängd skadlig kod. Det är tänkbart att andra operativsystem kommer att drabbas av den skadliga koden i högre utsträckning i framtiden. Om det tillkommer nya filtyper kommer det skrivas skadlig kod även till dessa om det kan ge skaparna av den ekonomisk vinning.

Hur skiljer sig framtidens skadliga kod från dagens i avseende på spridningssätt?

Det är sannolikt att framtidens skadliga kod kan komma att utge sig för att vara en uppdatering till en programvara och på så vis laddas ner. *Vidare anses det sannolikt att skadlig kod kommer att spridas mera via Bluetooth, MMS och SMS och e-post via mobiltelefoner i framtiden.* Det är sannolikt att skadlig kod kommer att sprida sig via *chattprogram, fildelningsprogram, IP-telefoni, eller andra former av "Web 2.0".* Det är tänkbart att skadlig kod kan komma att *sprida sig från en bärbar dator till en annan med hjälp av trådlösa nätverk.* Det är också tänkbart att det kommer att bli mer förekommande att man kan *bli smittad av skadlig kod bara genom att gå in på en smittad hemsida.*

Hur skiljer sig framtidens skadliga kod från dagens i avseende på hur den kan undgå upptäckt?

Rootkit-teknologin kommer troligen vara den bästa metoden. Andra tänkbara metoder, om än inte lika sannolika enligt denna uppsats, *är polymorfism och metamorfism. Detta gäller också de moderna trojaner ("modular malicious code" eller "downloaders") som kan uppdatera sig själva och på så vis ändra sitt utseende och funktionalitet och därmed kringgå signaturerna.* Det är tänkbart att den klassiska metoden att göra så lite skada som möjligt för att på så vis undgå upptäckt också i framtiden kommer att vara en fungerande metod för den

skadliga koden. En annan tänkbar metod i framtiden är att dölja den skadliga koden i annan, redan existerande IP-trafik.

Hur skiljer sig framtidens skadliga kod från dagens i avseende på vilken skada den kan göra?
Det är sannolikt att framtidens skadliga kod kommer att orsaka mera ekonomiskt lidande för sina offer. Vidare kommer den vara mer riktad mot specifika mål. Det kommer sannolikt att användas mera i utpressningssyfte. Vidare är det sannolikt att det kommer skapas skadlig kod till *mobiltelefoner och andra enheter* så att de kan komma att användas som *spionutrustning*. Vidare är det sannolikt så att den skadliga koden kan användas till *IT-krigsföring och för politiska ändamål*. *Bankärenden som genomförs över Internet* kommer sannolikt att bli ett mer vanligt mål i framtiden än idag. Så kallad *”smishing” och ”vishing”* via mobiltelefoner är två tänkbara framtida metoder. Så kallade *”datadiddlers”* kan också komma att bli vanligare i framtiden. Vidare anses det tänkbart att den skadliga koden i högre utsträckning kan användas till *identitetsstölder.*

Hur skiljer sig framtidens skadliga kod från dagens i avseende på hur mycket ekonomiskt lidande den orsakar?
Sannolikt kommer den totala kostnaden som den skadliga koden orsakar att öka i framtiden. Det anses osäkert om den direkta kostnaden kommer att öka, men däremot anses det troligt att den indirekta kostnaden kommer att göra det.

6 Trovärdighet

I detta kapitel diskuteras hur trovärdiga de slutsatser som framkommit i uppsatsen egentligen är.

Slutsatserna är behäftade med osäkerhet, och det finns inte några garantier för att de kommer att infrias i framtiden. Detta beror bland annat på den snabba tekniska utveckling som hela tiden sker inom detta område. Fem års tid inom detta område är mycket lång tid. Dock påstår bland annat säkerhetsexperten Bruce Schneier (”Search Security: Bruce Schneier reflects on a decade of security trends”, 2008) att det som fascinerar honom mest vid en tillbakablick på de senaste tio årens trender är hur lite tekniken förändrat sig. Han menar att vi på det stora hela försvarar oss på samma sätt som tidigare samtidigt som vi angrips på samma sätt. Om han har rätt känns det rimligt att påstå att det är möjligt att dra slutsatser om framtiden trots att det valda uppsatsämnet ständigt förändras. Dock är det fullt tänkbart att tekniska förändringar, som idag inte går att förutse, kommer att göra dessa slutsatser felaktiga.
Eftersom det är pengarna som styr den skadliga kodens värld idag, och troligen även i framtiden, är det hur pengarna bäst kan tjänas i framtiden som styr dess framtida utveckling. Hur pengarna bäst kan tjänas för skaparna av den skadliga koden i framtiden råder det av naturliga skäl osäkerhet om, även om det troligen kommer att vara på liknande sätt som idag. Många av de slutsatser som dragits är logiska fortsättningar av trender som tidigare inletts. För den skull finns det ingen garanti för att de kommer att infrias. En inneboende svaghet i denna uppsats är att många av slutsatserna, som i sig utgörs av antaganden, bygger på andra antaganden som i sin tur är osäkra. Naturligtvis medför detta att osäkerhetsfaktorn är relativt stor.
Trovärdigheten hos de fyra intervjuade respondenterna anser jag vara relativt hög, då dessa är fyra erkända experter. Sannolikt hade dock ledande internationella experterna haft större trovärdighet än de svenska.

Målsättningen har varit att, så långt det är möjligt, välja förstahandskällor. En annan målsättning är att välja så moderna källor som möjligt där det anses behövas. Vidare har det varit en målsättning att välja så bra källor som möjligt för att öka trovärdigheten. Att hitta material från opartiska källor har också varit en målsättning. Det kan anses vara en nackdel att det ligger så många källor till grund för uppsatsen, vilket kan sänka trovärdigheten. Vidare kan det anses att trovärdigheten sänks av att så många av källorna utgörs av information som är hämtad från Internet och inte från tryckt material. Det myckna användandet av källor från Internet har dock upplevts som ett krav för att uppsatsen skulle kunna slutföras. Det viktigaste vid valet av många källor har varit hur moderna de varit, då uppsatsen handlar om framtiden . En modernare källa har större möjligheter att bättre ge trovärdiga prognoser om framtiden. Mycket av den information som hämtats från Internet kommer från ledande tillverkare av antivirusprogram eller från andra företag. Denna information kan naturligtvis skrivas och framställas på ett vinklat sätt. Bland annat har tillverkarna av antivirusprogram ofta kritiserats för att överdriva farorna inför framtiden inför framtiden då detta kan ha en positiv inverkan på försäljningen av sin programvara. Detta är en tänkbar brist i uppsatsen, då den faktiskt till en ganska stor del grundar sig på sådan information.

Trots all denna osäkerhet är det min övertygelse att de flesta av de slutsatser som dragits i uppsatsen kommer att visa sig vara riktiga år 2013. Inte minst för att många av dessa bygger på en fortsatt utveckling av trender som redan pågått i många år.

7 Framtida forskning

I detta kapitel diskuteras vilken framtida forskning som kan och bör komma ifråga inom ämnet.

Eftersom det inte forskats mycket på det valda ämnet, är det lätt att rekommendera att det bör ske mer framtida forskning om det valda ämnet i framtiden. Ett stort säkerhetsproblem är att antivirusprogrammen idag är mer reaktiva än proaktiva. Det är sannolikt att forskning som drar korrekta slutsatser skulle kunna hjälpa tillverkarna av antivirusprogram och annat som har med datasäkerhet att göra att ändra sina produkter till att vara mer proaktiva. Detta tycks vara extra viktigt då det verkar som att framtidens skadliga kod kommer ha ett antal otrevliga överraskningar med sig i bagaget. Rimligtvis är det i de flestas intresse att förebygga dessa överraskningar så långt det bara är möjligt. En ökad kunskap inom ämnet kan också medföra att skaparna av programvara kan utforma den på ett säkrare sätt.
Skadlig kod behöver inte heller enbart vara av ondo. Ett tänkbart område för framtida forskning är att ta vara på de idéer och uppfinningar som skaparna av den skadliga koden bidragit med och sedan fundera ut mer positiva användningsområden för dem. Det är sannolikt så att det finns en hel del positiva saker att finna i allt det negativa. Ett exempel på detta kom ett forskarteam på företaget Microsoft nyligen med då det föreslog att företaget borde försöka använda sig av maskar för att sprida uppdateringar till sin programvara på ett snabbare och effektivare sätt. Resultatet av denna forskning publiceras i april, 2008 (”The Sydney morning herald: Microsoft wants to worm its way into your PC”, 2008).
Med dessa, i viss mån positiva, avslutningsord känns det som ett bra tillfälle att sätta punkt för arbetet med denna uppsats.

Referenser

”About.com: Zero Day Exploits- Holy Grail Of The Malicious Hacker”,
http://netsecurity.about.com/od/newsandeditorial1/a/aazeroday_2.htm , about.com,
Insatt 2007, Avläst 2007-05-31

”Aftonbladet: Osynliga viruset snor dina pengar”,
http://www.aftonbladet.se/nyheter/article1311238.ab, Aftonbladet.se,
Insatt 2007, Avläst 2007-12-02

”Antivirus World: History of computer viruses”,
http://www.antivirusworld.com/articles/history.php , Antivirusworld.com,
Insatt 2006, Avläst 2007-05-12

”Authentium: Computer Virus Outbreaks Doubling Every Twelve Months”,
http://www.emediawire.com/releases/2005/8/emw276981.htm, Emediawire.com,
Insatt 2005, Avläst 2007-12-14

Bishop, Matt, *Computer Security – Art and Science,* Addison-Wesley, Boston, 2003, s. 619

Bryman, Alan & Bell, Emma, *Företagsekonomiska forskningsmetoder*, Liber, Malmö, 2005, s. 350

Cohen, Fred, *Experiments with Computer Viruses*,
http://www.all.net/books/virus/part5.html, All.net,
Avläst 2007-05-16

“Computer Crime Research Center: Hackers shift targets in 2006”,
http://www.crime-research.org/analytics/1862/ , Crime-research.org,
Insatt 2006, Avläst 2007-05-31

“Computer Economics: Annual Worldwide Economic Damages from Malware Exceed $13 Billion”,
http://www.computereconomics.com/article.cfm?id=1225 , Computereconomics.com,
Insatt 2007, Avläst 2007-11-23

“Computer Economics: 2005 Malware Report: The Impact of Malicious Code Attacks”,
http://www.computereconomics.com/article.cfm?id=1090, Computereconomics.com,
Insatt 2006, Avläst 2007-11-15

“Computer knowledge: Number of viruses”,
http://www.cknow.com/vtutor/NumberofViruses.html , Cknow.com,
Insatt 2005, Avläst 2007-12-02

“Enterprise Networking Planet: DNSSEC – Security for Essential Network Services”,
http://www.enterprisenetworkingplanet.com/netsecur/article.php/10952_2204801 ,
Enterprisenetworkingplanet.com,
Insatt 2003, Avläst 2007-05-31

"Exn: The history of computer viruses – A timeline",
http://www.exn.ca/nerds/20000504-55.cfm , Exn.ca,
Insatt 2007, Avläst 2007-05-13

"Finjan viral security: web security trends report Q32007",
http://www.finjan.com/GetObject.aspx?ObjId=506 , Finjan.com,
Insatt 2007, Avläst 2007-11-27

Filiol, Eric, *concepts and future trends in computer virology*,
http://www.waset.org/lectures/eric_barcelona07.pdf, Waset.org,
Insatt 2007, Avläst 2007-12-14

Fjordvang, Peder, *Säkerhet på pc och Internet*, Pagina förlag AB, Sundbyberg, 2002, s.71

"F-Secure: Bootsektorvirus",
http://www.f-secure.se/virus/virusinfo.asp?Namn=BOO_infector , F-secure.se,
Insatt 2003, Avläst 2006-11-26

"F-Secure Virus Descriptions : Cascade",
http://www.f-secure.com/v-descs/cascade.shtml , F-secure.com,
Insatt 2000, Avläst 2007-05-13

"F-Secure Virus Descriptions : Concept",
http://www.f-secure.com/v-descs/concept.shtml , F-secure.com,
Insatt 2003, Avläst 2007-15-18

"F-Secure Virus Descriptions : Melissa",
http://www.f-secure.com/v-descs/melissa.shtml , F-secure.com,
Insatt 2003, Avläst 2007-15-18

Fåk, Viiveke, *Datavirus,* Studentlitteratur, Lund, 1990, ss. 8-13, 45-52

"Geek news: Kazaa distributes trojan-ware",
http://www.geek.com/news/geeknews/2002apr/gee20020402011013.htm , Geek.com,
Insatt 2002, Avläst 2007-05-15

"Georgia Tech Information Security Center: Emerging Cyber Threats Report for 2008",
http://www.gtisc.gatech.edu/pdf/GTISC%20Cyber%20Threats%20Report.pdf,
Gtisc.gatech.edu,
Insatt 2007, Avläst 2007-12-15

Glaser, Barney G & Strauss, Anselm L, *The Discovery of Grounded Theory: Strategies for quality research*, Aldine, Chicago, USA, 1967

"Göteborgsposten: Trojansk häst",
http://www.gp.se/gp/jsp/Crosslink.jsp?d=281&a=192074 , Gp.se,
Insatt 2004, Avläst 2006-11-27

Hellqvist, Per, *Handbok för föräldrar – Lär dig vad ditt barn gör på Internet*,
Annonsmakaren, Stockholm, 2007

”IDG.se – Datavirus från A till O”,
http://www.idg.se/ArticlePages/200306/11/20030611172720_IDG.se291/20030611172720_IDG.se291.dbp.asp, IDG.se,
Insatt 2003, Avläst 2006-11-26

”IDG.se – De tio värsta it-hoten som gör 2008 till en mardröm”,
http://www.idg.se/2.1085/1.132346, IDG.se,
Insatt 2007, Avläst 2007-12-14

”IDG.se – Fler attacker mot Vista 2008”,
http://computersweden.idg.se/2.2683/1.133334, IDG.se,
Insatt 2007, Avläst 2007-12-14

”Informit: Program security”,
http://www.informit.com/articles/article.aspx?p=31782&seqNum=3&rl=1, Informit.com,
Insatt 2003, Avläst 2007-11-23

”IP Communications: Malicious Code for sale”,
http://ipcommunications.tmcnet.com/hot-topics/Security/articles/1942-malicious-code-sale.htm, Ipcommunications.tmcnet.com,
Insatt 2006, Avläst 2007-12-15

Jacobsen, K.J., *Intervju – konsten att lyssna och fråga*, Studentlitteratur, Lund, 1993, ss. 19-20, 189, 191-192

”Lead Agency Publication: Future trends in malicious code – 2006 report”,
http://www.rcmp-grc.gc.ca/tsb/pubs/it_sec/r2-002_e.pdf , Rcmp-grc.gc.ca,
Insatt 2006, Avläst 2007-12-15

Lin, Xi, *Computer viruses: The threat today and the expected future,* Linköpings Universitet, 2003.

“Market Share: Operating system market share for april 2007”,
http://marketshare.hitslink.com/report.aspx?qprid=2, Marketshare.hitslink.com,
Insatt 2007, Avläst 2007-05-12

”Market share: Operating system market share for november 2007”,
http://marketshare.hitslink.com/report.aspx?qprid=10&qpmr=15&qpdt=1&qpct=3&qpcal=1&qptimeframe=Y&qpsp=2007, Marketshare.hitslink.com,
Insatt 2007, Avläst 2007-12-14

Mcdonald, Neil, *the future of malicious code,*
http://www.midsizeenterprise.com/northamerica/mese_07_presentations/mese7_103_macdonald_os.pdf , Midziseenterprise.com,
Insatt 2007, Avläst 2007-12-20

McGraw, Gary & Morrisett, Greg, *Attacking Malicious Code:*
A report to the Infosec Research Council,
http://www.cs.cornell.edu/home/jgm/cs711sp02/maliciouscode.pdf , Cs.cornell.edu,
Insatt 2000, Avläst 2007-05-12

”Microsoft: Mask- Hoten – Säkerhet”,
http://www.microsoft.com/sverige/security/threats/worm.mspx , Microsoft.se,
Insatt 2005, Avläst 2006-11-28

”Microsoft: Microsoft Research Reveals New Trends in Cybercrime”,
http://www.microsoft.com/presspass/press/2007/oct07/10-23IAPPRSAPR.mspx,
Microsoft.com,
Insatt 2007, Avläst 2007-11-27

”Out-Law: Code Red cost $2.6 billion worldwide”,
http://www.out-law.com/page-1953 , Out-law.com,
Insatt 2001, Avläst 2007-05-20

”Paginas IT-ordbok: ActiveX-kontroller”,
http://www.pagina.se/itord/default.asp?Id=5438 , Pagina.se,
Insatt 2007, Avläst 2007-05-12

”PC Pro Focus: Vista determines malware evolution” ,
http://www.pcpro.co.uk/security/news/106408/vista-determines-malware-evolution-report.html,
Insatt 2007, Avläst 2007-12-16

”Post- och Telestyrelsen: Alltid på! Bredbandsmarknaden ur ett konsumentperspektiv”,
http://www.pts.se/Archive/Documents/SE/Alltid_pa.pdf, Pts.se,
Insatt 2003, Avläst 2007-05-17

“Reuterts: The cost of Code Red”,
http://www.usatoday.com/tech/news/2001-08-01-code-red-costs.htm , Usatoday.com,
Insatt 2001, Avläst 2007-05-20

Rienecker,Lotte & Stray Jørgensen, Peter, *Att skriva en bra uppsats*, Liber,
Malmö, 2002

“Search Security: Apple Iphone to provoke complex mobile attacks, expert warns”
http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1267620,00.html ,
Searchsecurity.techtarget.com,
Insatt 2007, Avläst 2007-12-14

“Search Security: Bruce Schneier reflects on a decade of security trends”,
http://searchsecurity.techtarget.com/qna/0,289202,sid14_gci1283751,00.html ,
Searchsecuroty.techtarget.com,
Insatt 2008, Avläst 2008-01-22

“Search Security: Data thieves thrive on zero-day flaws”,
http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1247976,00.html ,
Searchsecurity.techtarget.com,
Insatt 2007, Avläst 2007-05-31

“Search Security: Ed Skoudis: Polymorphic viruses call for new antimalware defenses”, http://searchsecurity.techtarget.com/generic/0,295582,sid14_gci1146071,00.html, Searchsecurity.techtarget.com,
Insatt 2007, Avläst 2007-12-16

”Search Security: Future - Information Security Magazine”, http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1288739_idx2,00.html , Searchsecurity.techtarget.com,
Insatt 2008, Avläst 2008-01-21

”Search Security: Future mobile attacks inevitable”, http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1271668,00.html, Searchsecurity.techtarget.com,
Insatt 2007, Avläst 2007-12-15

“Search Security: Mike Rothman: Top 5 next-generation messaging attacks that antivirus can't catch” http://searchsecurity.bitpipe.com/data/mp3Player.do?res_id=1174826935_539, Searchsecurity.bitpipe.com,
Insatt 2007, Avläst 2007-12-16

“Search Security: Noah Schiffman: Metamorphic malware sets new standard in antivirus evasion”, http://searchsecurity.techtarget.com/generic/0,295582,sid14_gci1146071,00.html, Searchsecurity.techtarget.com,
Insatt 2007, Avläst 2007-12-16

“Search Security: What is a logic bomb?”, http://searchsecurity.techtarget.com/expert/KnowledgebaseAnswer/0,289625,sid14_gci1259222,00.html, Searchsecurity.techtarget.com,
Insatt 2007, Avläst 2007-11-29

“Securityfocus: Detecting complex viruses”, http://www.securityfocus.com/infocus/1813, Securityfocus.com,
Insatt 2004, Avläst 2007-11-30

“Securityfocus: Windows rootkits of 2005 part two”, http://www.securityfocus.com/infocus/1851, Securityfocus.com,
Insatt 2005, Avläst 2007-11-27

“Security Statistics: Virusrelated statistics”, http://www.securitystats.com/virusstats.html , Securitystats.com,
Insatt 2004, Avläst 2007-12-02

“Smart Computing: Tales of Trojan horses”, http://www.smartcomputing.com/editorial/article.asp?article=articles/archive/l0902/03l02/03l02.asp , Smartcomputing.com,
Insatt 2003, Avläst 2007-05-13

"Smart Computing: The dark side of scripts",
http://www.smartcomputing.com/editorial/article.asp?article=articles/archive/r0606/41r06/41r06.asp&guid= , Smartcomputing.com,
Insatt 2002, Avläst 2007-05-15

"Spychecker: What is spyware?",
http://www.spychecker.com/spyware.html , Spychecker.com,
Insatt 2005, Avläst 2007-05-15

Starrin, B & Svensson, P-G, *Kvalitativ metod och vetenskapsteori,* Studentlitteratur, Lund, 1994, s. 21

"Sun Developer Network: Applets",
http://java.sun.com/applets/ , Java.sun.com,
Insatt 2007, Avläst 2007-05-12

"Symantec: Datavirus allt svårare att hitta",
http://www.symantec.se/region/se/press/n040316_se.html, Symantec.se,
Insatt 2004, Avläst 2007-05-15

"Symantec: Det nya hotet: Blandade hot",
http://www.symantec.com/region/se/corporate/blended_threats.html, Symantec.se,
Insatt 2003, Avläst 2007-05-17

"Symantec: Crimeware: Bots",
http://www.symantec.com/avcenter/cybercrime/bots_page1.html#, Symantec.com,
Insatt 2007, Avläst 2007-05-31

"Symantec: How They Attack: Spam",
http://www.symantec.com/home_homeoffice/security_response/spam.jsp, Symantec.com,
Insatt 2007, Avläst 2007-05-31

"Symantec Internet Security Report: Trends for January to June 2005",
http://www.symantec.se/region/se/sepress/download/symantec_istr_8.pdf, Symantec.se,
Insatt 2005, Avläst 2007-05-16

"Symantec Internet Security Report: Trends for January to June 2006", 2006
http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_symantec_internet_security_threat_report_x_09_2006.en-us.pdf , Symantec.com,
Insatt 2006, Avläst 2007-05-23

"Symantec Internet Security Report: Trends for January to June 2007", 2007
http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_09_2007.en-us.pdf, Symantec.com,
Insatt 2007, Avläst 2007-11-23

"Symantec Internet Security Report: Trends for July to December 2005",
http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_symantec_internet_security_threat_report_ix.pdf, Symantec.com,
Insatt 2006, Avläst 2007-05-23

“Symantec Internet Security Report: Trends for July to December 2006”,
http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_symantec_internet_security_threat_report_ix.pdf, Symantec.com,
Insatt 2007, Avläst 2007-05-23

”Symantec: Var kan ett Rootkit gömma sig?”,
http://www.symantec.com/sv/se/home_homeoffice/library/article.jsp?aid=article2_02_06,
Symantec.se,
Insatt 2006, Avläst 2007-05-11

Sörensen, Torben.B, *Beskydda din PC*, Pagina förlag AB, Sundbyberg, 2004, s.71

”The Sydney morning herald: Microsoft wants to worm its way into your PC”,
http://www.smh.com.au/news/security/microsoft-wants-to-worm-its-way-into-your-pc/2008/02/15/1202760555255.html, smh.com.au,
Insatt 2008, Avläst 2008-02-27

”Trend Micro: Virus Primer”,
http://se.trendmicro-europe.com/enterprise/security_info/overview.php , Trendmicro.se,
Insatt 2005, Avläst 2007-05-17

“Usa Today: Worms and viruses and phishers, oh my!”,
http://www.usatoday.com/tech/columnist/ericjsinrod/2005-02-16-sinrod_x.htm ,
Usatoday.com,
Insatt 2005, Avläst 2007-12-02

”Virus Bulletin: Virus Prevalence”,
http://www.virusbtn.com/resources/malwareDirectory/prevalence/index, Virusbtn.com,
Insatt 2007, Avläst 2007-05-18

”Viruslist: History of Malware”,
http://www.viruslist.com/en/viruses/encyclopedia?chapter=153311164 , Viruslist.com,
Insatt 2004, Avläst 2007-05-18

”Viruzlist: Loveletter”,
http://www.viruzlist.tonyaustin.com/loveletter.html, Viruzlist.tonyaustin.com,
Insatt 2000, Avläst 2007-05-18

“Washington post: Cybercrime hits the big time in 2006”,
http://www.crime-research.org/articles/Cybercrime-hits-the-big-time-in-2006,
Crime-research.org,
Insatt 2006, Avläst 2007-11-23

”Websense: Security Trends Report 2004”,
http://www.websense.com/securitylabs/resource/WebsenseSecurityLabs20042H_Report.pdf
Websense.com,
Insatt 2005, Avläst 2007-05-20

”Websense: Security Trends Report 2005”,
http://www.websense.com/securitylabs/docs/WebsenseSecurityLabs20052H_Report.pdf
Websense.com,
Insatt 2006, Avläst 2007-05-21

“Webgate: Spyware”,
http://www.wgate.nu/spyware.htm , Wgate.nu,
Insatt 2003, Avläst 2007-05-17

”Wikipedia: 2005 Sony BMG CD copy prevention scandal”
http://en.wikipedia.org/wiki/2005_Sony_BMG_CD_copy_prevention_scandal,
En.wikipedia.org,
Insatt 2007, Avläst 2007-11-23

“Wikipedia: Datorvirus”,
http://sv.wikipedia.org/wiki/Datavirus, Sv.wikipedia.org,
Insatt 2005, Avläst 2007-05-17

”Wikipedia: Morris Worm”,
http://en.wikipedia.org/wiki/Morris_worm, En.wikipedia.org,
Insatt 2007, Avläst 2007-05-17

”Wikipedia: Pharming”,
http://en.wikipedia.org/wiki/Pharming, En.wikipedia.org,
Insatt 2008, Avläst 2008-02-27

”Wikipedia: Phishing”,
http://en.wikipedia.org/wiki/Phishing, En.wikipedia.org,
Insatt 2007, Avläst 2007-05-21

“Wikipedia: Web 2.0”,
http://en.wikipedia.org/wiki/Web_2, En.wikipedia.org,
Insatt 2007, Avläst 2007-12-15

”Wikipedia: Windows XP”,
http://en.wikipedia.org/wiki/Windows_XP, En.wikipedia.org,
Insatt 2008, Avläst 2008-02-27

Bilaga 1 – Intervjufrågor

1. Vilken är enligt din mening den farligaste sortens skadliga kod som finns idag?

2. Kommer skadlig kod bli mer eller mindre förekommande i framtiden (5 år)?

3. Hur kommer framtidens skadliga kod att skilja sig från dagens i avseende på spridningssätt?

4. Hur kommer framtidens skadliga kod att skilja sig från dagens i avseende på hur de kan undgå upptäckt?

5. Hur kommer framtidens skadliga kod att skilja sig från dagens i avseende på den skada de gör?

6. Vilken typ av skadlig kod tror du kommer vara dominerade i framtiden?

7. Kommer nya typer av skadlig kod tillkomma?

8. Vilka trender tror du vi kommer få se inom den skadliga koden i framtiden?

9. Kommer kostnaden för den skadliga kodens skadeverkningar att öka eller minska i framtiden?

10. Kan du ge ett tänkbart exempel på ett framtidsscenario som kan hända en vanlig människa i ett ”skadligkodsammanhang” om fem år?

Bilaga 2 – Antalet kända förekomster av skadlig kod under åren 1995-2006

År	Antal
1995	2400
1996	4900
1997	4800
1998	5700
1999	34500
2000	24450
2001	207500
2002	110000
2003	312000
2004	2462500
2005	17651000
2006	99185000

Bilaga 3 – Antalet kända former av skadlig kod under åren 1995-2006

År	Antal
1995	4500
1996	10000
1998	20000
2000	50000
2002	70000
2005	200000
2006	250000

Bilaga 4 – Direkt kostnad orsakad av skadlig kod under åren 1995-2006

År	Kostnad (M$)
1995	500
1996	1800
1997	3300
1998	6100
1999	13000
2000	17100
2001	13200
2002	11100
2003	13000
2004	17500
2005	14200
2006	13300