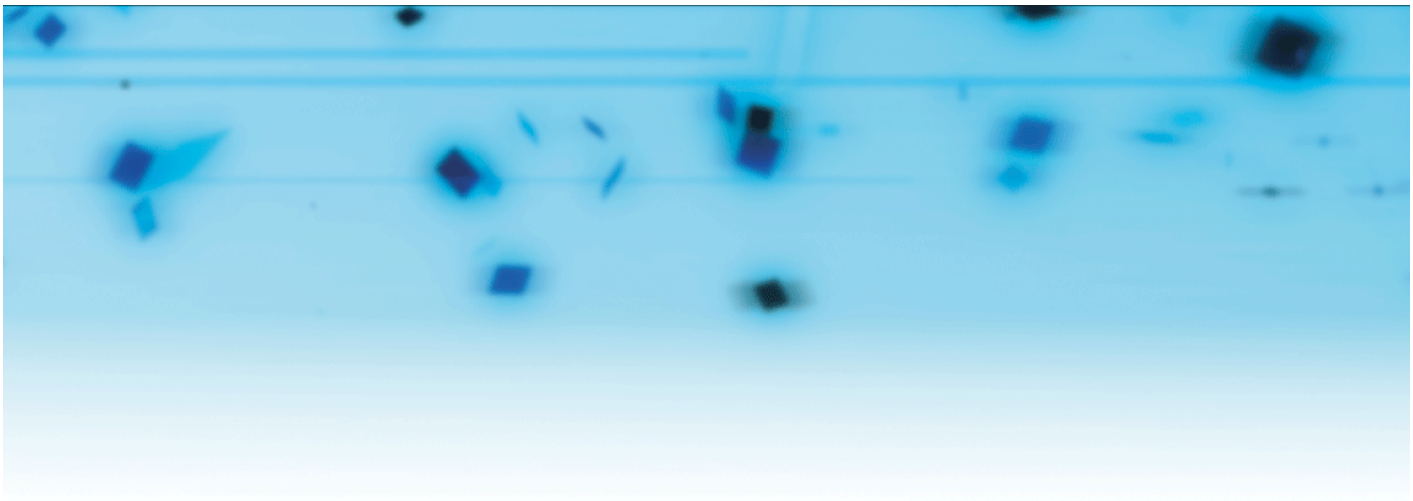


INFORMATIONSSÄKERHETS-ÖVERSIKT 1/2009

3.4.2009

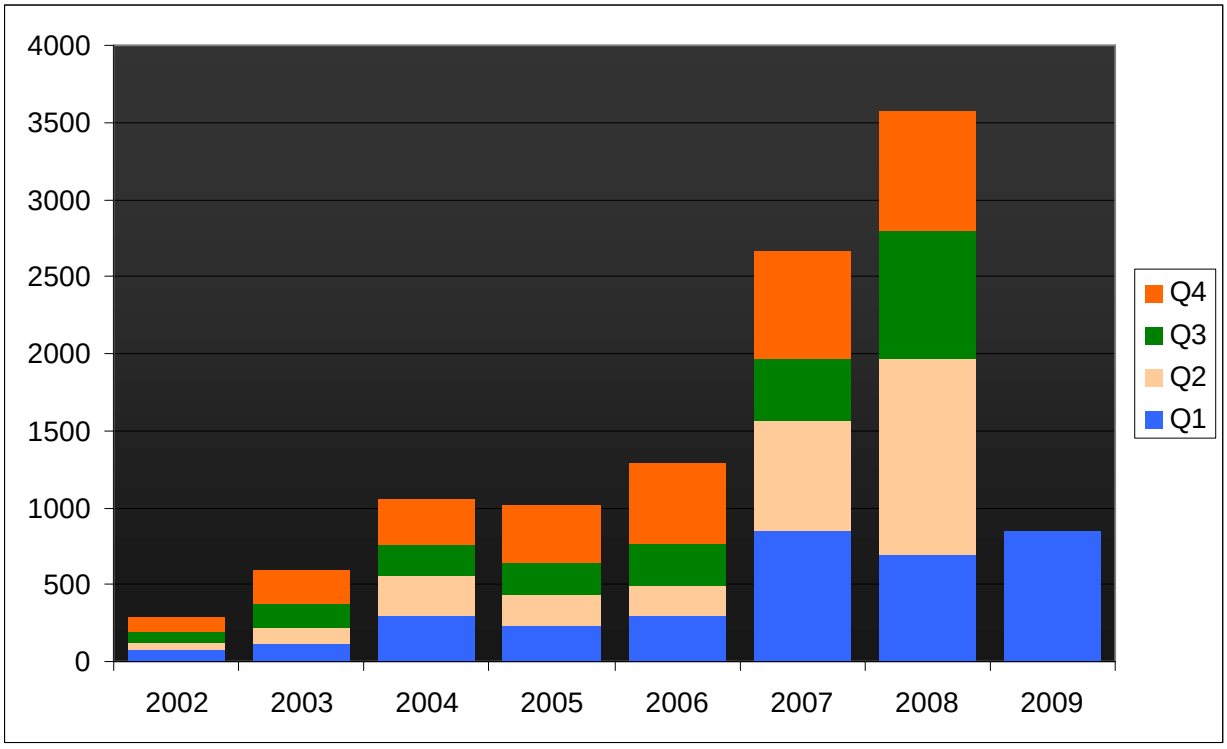
CERT-FI informations-säkerhetsöversikt 1/2009

Inledning

Efter årsskiftet har nyheterna om informationssäkerhet dominerats av ett skadligt program vid namn Conficker eller Downadup. Conficker har spridit sig till miljoner datorer i hela världen på tre olika sätt. Masken sprids via en redan åtgärdad säkerhetslucka i operativsystemet Windows eller genom att kopiera sig på nätverksdiskar som har svaga lösenord. Masken kopierar sig också på USB-minnesstickor som används i datorerna. Via minnespinnen angriper masken den nya datorn med hjälp av Windows-operativsystemets AutoRun-funktion. I Finland har man observerat relativt få fall av Conficker-infektion.

Skadliga program kan också infektera andra utrustningar. I Finland har man påträffat ADSL-terminalutrustning som infekterats av ett skadligt botnetprogram. Det kan vara svårt att upptäcka en infektion i nätets aktiva utrustning och det kan också vara svårare att skydda utrustningen och uppdatera programvarorna än att sköta om att arbetsstationen har de senaste programuppdateringarna.

Riktad distribution av skadliga program används för att skaffa information om en organisation på olagligt sätt. Skadliga program som stjäl information kan vara fjärrstyrda eller fungera självständigt och man försöker åstadkomma infektion genom att distribuera dem via e-post som bilagor eller länkar till en omsorgsfullt utvald grupp av mottagare. Avsändarinformationen är förfalskad och meddelandenas ämnen är trovärdiga och har koppling till organisationens normala verksamhet. En typisk bilaga som innehåller ett skadligt program kan vara exempelvis en inbjudan till ett möte eller en konferens.



Antalet incidenter som CERT-FI behandlade i början av året låg ungefär på samma nivå som under de två föregående åren.

En nätverksmask med stor spridning en påminnelse om grundläggande fakta om informationssäkerhet

Ett skadligt program som efter årsskiftet har infekterat flera miljoner datorer världen över har fått namnen *Conficker* och *Downadup.* Masken påminner om grundläggande fakta då det gäller att skydda sig mot skadliga program. Bra skyddsåtgärder är att uppdatera sårbara program, iaktta goda lösenordsförfaranden och vara försiktig med minnesmedier som flyttas mellan datorer (t.ex. USB-minnespinnar).

Det finns egentligen inget nytt i Conficker-programmet och dess sätt att spridas, men de egenskaper som kombinerats i programmet har visat sig vara en effektiv kombination med tanke på maskens spridning. Metoden att använda minnespinnar för spridning påminner om de virus som spreds via disketter redan på 1980-talet.

Nätverksmasken sprids på många sätt

Conficker-programmets första versioner använder flera spridningssätt. I omlopp finns flera versioner som avviker något från varandra.

Nätverksmasken använder sig av en säkerhetslucka i anslutning till delning av filer och skrivare i operativsystemet Microsoft Windows. En programuppdatering som åtgärdade luckan publicerades i oktober 2008. Det skadliga programmet kan emellertid sprida sig till datorer vilkas operativsystem inte är uppdaterade och vilkas sårbara tjänster kan kontaktas över nätet.

Efter att masken har infekterat en dator försöker den kopiera sig till flyttbara lagringsmedia, exempelvis på USB-minnespinnar. När en minnespinne som infekterats av Conficker överförs till en annan dator, startar det skadliga programmet med hjälp av Windows AutoRun-funktion, vilket gör att den andra datorn infekteras.

Conficker försöker även kopiera sig på nätdiskar i lokalnätet. För att kunna göra detta försöker programmet knäcka lösenord som behövs för användning av nätdiskarna och som lagrats på domänens kommandoserver. Om svaga lösenord används, kan programmet lyckas i sitt försök. Försöken att knäcka lösenord belastar kommandoservern och misslyckade försök kan orsaka att användarkonton blir låsta, vilket kan avslöja infektionen i lokalnätet.

Från programversionen Conficker C, som observerades i slutet av mars, har spridningsmekanismerna helt avlägsnats. Det skadliga programmet försöker alltså inte sprida sig till nya datorer utan försöker endast uppdatera sig till en ny programversion.

Maskens uppdateringsmekanism bygger på domännamn och P2P-förbindelser

Efter att ha infekterat en dator försöker Conficker uppdatera sig genom att kontakta ett domännamn som programmet beräknat utifrån datum och klockslag för att ladda ned en ny skadlig programfil.

Informationssäkerhetsforskare har lyckats utreda på vilket sätt det skadliga programmet bildar de domännamn det använder. Genom att på förhand registrera domännamn som används för uppdatering har man kunnat störa uppdateringen av masken.

Senare Conficker-versioner behöver nödvändigtvis inte en bestämd nätadress från vilken de försöker ladda ned en uppdatering, utan de använder P2P-teknik för att hitta och ladda ned uppdateringsfilen.

Sedan början av april använder en version av det skadliga programmet betydligt fler domännamn än tidigare i sina uppdateringsförsök, vilket gör det svårare att förebygga uppdateringarna.

Syftet med Conficker en gåta

Efter att Conficker har infekterat en dator försöker programmet dölja sig, vilket är typiskt för skadliga program, så att det är så svårt som möjligt att observera eller avlägsna programmet. Ett redskap för att avlägsna programmet från infekterade datorer har publicerats, men ofta är det säkrast att ominstallera operativsystemet i sin helhet på datorn.

Tills vidare har man inte upptäckt något egentligt syfte med spridningen av Conficker. De versioner som påträffats har inte konstaterats göra annat än att sprida sig mellan datorer och försöka uppdatera sig till en nyare version.

Om uppdateringen av det skadliga programmet lyckas, kan den nya programfilen innehålla nya egenskaper och skadliga funktioner.

Masken har bekämpats i Finland med rätt goda resultat

Eftersom man lyckats utreda Conficker-programmets sätt att uppdatera sig har man kunnat bedöma omfattningen av programmets spridning relativt pålitligt. Utifrån de uppdateringsanrop som det skadliga programmet skickat har man uppskattat att masken spridit sig till över femton miljoner datorer världen över.

Antalet infektioner i Finland har uppskattats till några tusen, vilket kan betraktas som ett relativt litet antal. Maskens spridning i Finland har bromsats upp på grund av att de portar, som används av den sårbara tjänst i Windows-operativsystemet som masken utnyttjar, är stängda i internetabonnemang för konsumenter. De brandväggar som skyddar företagsnäten spärrar även den internettrafik som orsakar infektionen. I lokalnät kan masken emellertid ofta spridas över nätet från en dator till en annan.

Trots allt har nätverksmasken lyckats spridas i några relativt stora organisationers nätverk. Den mest sannolika förklaringen är att masken kommit in i lokalnätet via portabla USB-minnespinnar.

Skadliga program kan också infektera andra utrustningar än persondatorer

CERT-FI har fått kännedom om fall där användarens bredbandsmodem har knäckts och kopplats till ett botnet-nätverk. Utrustningar med operativsystemet Linux och programmet BusyBox har infekteras med ett skadligt program vid namn PsyBot.

I detta fall har man inte utnyttjat en egentlig säkerhetslucka i programmet för att tränga in i utrustningen. Det skadliga programmet har installerats på utrustningar i vilkas gränssnitt för administration på distans man använt en fabriksinställd administratorkod och ett svagt lösenord som inte har gjorts säkrare när utrustningen togs i användning.

I anordningar som levereras av operatörer har användar-ID:n och lösenorden vanligen bytts ut mot tryggare, men ADSL-terminalutrustningar och WLAN-basstationer som kommer direkt från butikshyllan har standardkoder och standardlösenord, om användaren inte ändrar dem.

Då säkerhetsluckor i nätutrustningar och virusattacker mot luckorna blir vanligare, kan attackerna utvecklas till stora utmaningar. Ett skadligt program som infekterat en aktiv nätanordning kan lättare undgå upptäckt än ett skadligt program i en arbetsstation. I anordningarna används inte antivirusprogram och det finns ingen separat brandvägg som filtrerar förbindelserna mellan dem och internet. Anordningarna är i allmänhet påslagna hela tiden och därför behöver programkoden för det skadliga programmet nödvändigtvis inte lagras permanent i anordningen.

Regelbunden uppdatering av arbetsstationer och installation av tillverkarens informations-säkerhetsuppdateringar i operativsystem och program har blivit rutin. För programuppdatering av nätutrustning finns inte likadana metoder och förfaranden och därför tar det ofta längre

att åtgärda sårbarheter i dem än i arbetsstationer.

Riktade virusattacker mot olika organisationer

I slutet av mars publicerades i Kanada en rapport som redogjorde för en omfattande serie av dataintrång som gjorts med hjälp av riktad distribution av skadliga program. Enligt rapporten användes en förbindelse för administration på distans som skapats med hjälp av det skadliga programmet Gh0st för att stjäla data från datorer i olika organisationer.

CERTR-FI har redan tidigare rapporterat om skadliga program som stjäl information och som man också försökt sprida till organisationer till Finland. De skadliga programmen har distribuerats som bilagor till e-postmeddelanden till en begränsad och omsorgsfullt utvald grupp av mottagare. Som avsändare har man angett en känd aktör och meddelandenas ämnen har varit trovärdiga och haft koppling till organisationens normala verksamhet. En typisk bilaga som innehåller ett skadligt program kan vara exempelvis en inbjudan till ett möte eller en konferens.

De skadliga program som använts i de riktade attackerna har i allmänhet varit versioner som antivirusprogrammen vid tidpunkten för attacken ännu inte identifierat. Avsikten med programmen har varit att administrera användarens dator på distans, vilket gör det möjligt att skaffa information om organisationens verksamhet.

Statistiken om skadliga program visar ännu ingen tillväxt år 2008

CERT-FI har publicerat statistik om observationer av skadliga program år 2008. Statistiken visar att antalet observationer av skadliga program i finländska nät är så gott som oförändrad sedan sommaren 2007.

Antalet observationer av skadliga program per bredbandskund har minskat under de senaste åren trots att antalet bredbandsabonnemang fortsätter att öka. I slutet av år 2008 överskred antalet bredbandsabonnemang i Finland tvåmiljonersstrecket. Tillväxten från året innan var nästan 20 procent.

Nätverksmasken Conficker kommer att synas i statistiken åtminstone för första halvåret 2009. CERT-FI har under det första kvartalet skickat över 11 000 rapporter enbart i anslutning till denna nätverksmask. I finländska nätverk har man konstaterat datorer som infekteras av nätverksmasken på över 3 000 olika IP-adresser.

Även finländska aktörers information har av misstag lagts ut på webben

CERT-FI har fått kännedom om några fall, där skyddad information från en finländsk organisation, exempelvis användar-ID:n och lösenord av misstag lagts ut på webbsidor. Detta har inte orsakat de drabbade aktörerna stora skador, men i vissa fall har det funnits förutsättningar även för mer omfattande skador.

Nyheter som publicerats om liknande fall pekar på att det verkar vara relativt vanligt runt om i världen att skyddad information av misstag eller försumlighet blir offentligt tillgänglig.

Nya inslag i blockerings-attacker som utnyttjar namn-tjänster

CERT-FI har under de senaste åren berättat om flera fall, där öppna rekursiva namnservrar utnyttjats för blockeringsattacker.

Under den senaste tiden har man observerat allt fler attacker som använder namnservrar som svarar på förfrågningar gällande data som finns i namnserverns cache eller filsystem. Förfrågningarna kan gälla till exempel rotnamnservrarnas adresser, som finns på varje namnserver.

CERT-FI undersökte i augusti 2008 och februari 2009 namnservrar för domännamn som slutar på fi. Då konstaterades att det finns många servrar

som på olika sätt kan utnyttjas för blockeringsattacker. Utifrån dessa undersökningar har man konstaterat att det finns fler namnservrar som svarar på förfrågningar som gäller data i namnserverns cache än öppna rekursiva servrar i nätet.

Framtidsutsikter

I den närmaste framtiden är det av särskilt intresse att följa upp vad som sker med datorer som infekterats med Conficker-program. Masken har tills vidare endast spritt sig och försökt uppdatera sig med en nyare version.

På längre sikt kan man vänta sig att utvecklingen av skadliga program även inriktar sig på andra miljöer än egentliga datorer. Allt fler elektroniska anläggningar i hemmen kopplas till internet och sårbarheterna i de programvaror som används i dem har inte på långt när undersökts i samma utsträckning som datorernas operativsystem och programvaror.

CERT-FI kontakter per kategori	1-3/2009	1-3/2008	Förändring
Intervju	**35**	17	+106%
Sårbarhet eller hot	**20**	39	–49%
Skadligt program	**577**	460	+25%
Rådgivning	**93**	64	+45%
Beredning av attack	**10**	32	–69%
Dataintrång	**28**	14	+100%
Blockeringsattack	**23**	15	+53%
Övriga informationssäkerhetsproblem	**23**	10	+130%
Social Engineering	**33**	47	–30%
Sammanlagt	**842**	**698**	**+21%**

Anmälningar om skadliga program utgjorde största delen av de informationssäkerhetsincidenter som CERT-FI behandlade under början av år 2009.