

CERT-FI

ÅRSÖVERSIKT 2009

20.1.2010

CERT-FI årsöversikt 2009

Inledning

Conficker fick stor spridning

Det skadliga programmet Conficker spred sig till miljoner datorer under 2009. Conficker, som också i Finland spridit sig till tusentals datorer via nätet eller minnesmedier som flyttas mellan datorer, är gåtfullt, eftersom man fortfarande inte har kunnat konstatera att det egentligen gör något annat än sprider sig från en dator till en annan.

Med hjälp av skadliga program är det möjligt att olovligt fjärradministrera användarens dator eller fiska fram användarens uppgifter. Också i Finland kom sådana fall till kännedom där någon med hjälp av ett skadligt program har blandat sig i innehållet i en nätbankssession och utfört olovliga kontoöverföringar utan att användaren är medveten om dem.

Intensivt internationellt samarbete

De internationella informationssäkerhetsgemenskapen och -myndigheterna har effektiviserat sitt samarbete under året. Förutom bekämpning av skadeprogrammet Conficker har företag som tillhandahåller skadligt innehåll utslutits från nätet. Vidare har man förhindrat användning av domännamn som skadliga program anlitar.

Jämförande undersökning av europeiska CERT-aktörer

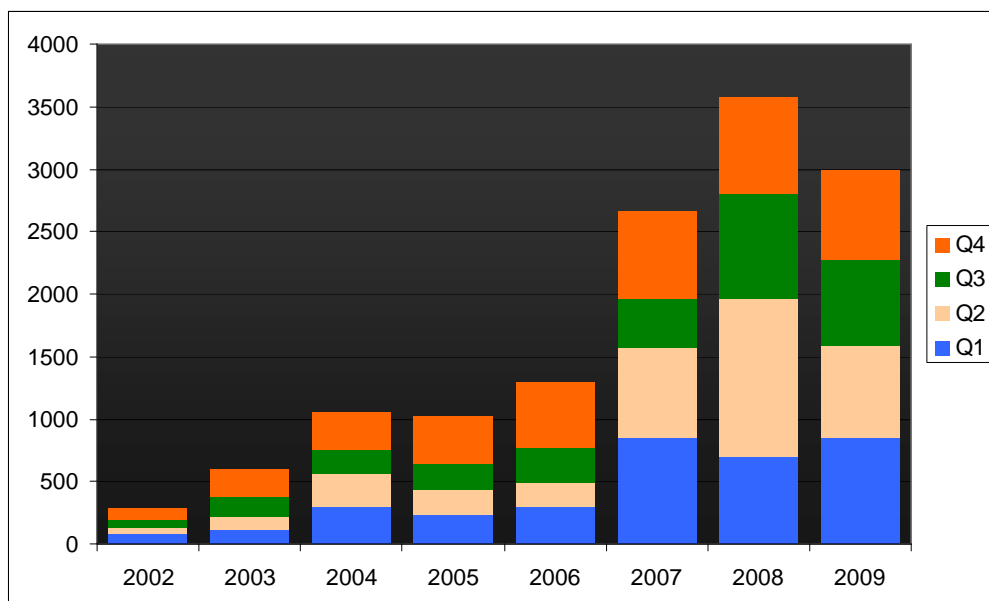
CERT-FI färdigställde en undersökning av europeiska CERT-aktörer under 2009. I undersökningen jämfördes elva CERT-enheters verksamhet. Undersökningen var den första av sitt slag i Europa och dess resultat har väckt internationellt intresse.

Lagen om dataskydd vid elektronisk kommunikation förnyades

Ändringen av lagen om dataskydd vid elektronisk kommunikation trädde i kraft i juni. Efter att lagen trädde i kraft har Kommunikationsverket redan en gång uppmanat teleföretagen att vidta de åtgärder som föreskrivs i den nya lagen i syfte att skydda dem som använder de finländska nätbankerna.

Sveriges spaningsverksamhet kan inverka även på finländarnas telekommunikationsförbindelser

En ny lag om signalspanning trädde i kraft i Sverige den 1 december 2009. Enligt Kommunikationsverkets bestämmelse är teleföretagen skyldiga att informera sina kunder om hot mot informationssäkerheten som riktar sig mot sådana tjänster som produceras i utlandet och som erbjuds finländska kunder.



Antalet fall som CERT-FI behandlar årligen verkar jämnas ut sig.

Skadeprogrammet Conficker har den största spridningen

Den aggressiva spridningen av det skadliga programmet Conficker ledde till att miljoner datorer smittades. Enligt en uppskattning i slutet av 2009 hade omkring sju miljoner datorer runtom i världen infekterats av Conficker. Också i Finland har tusentals datorer infekterats av detta skadliga program.

CERT-FI:s system Autoreporter skickade nästan 100 000 meddelanden i anslutning till nätmasken Conficker under 2009. Siffran anger inte direkt antalet infekterade datorer eftersom meddelandena innehåller många IP-adresser som upprepas. En närmare granskning visar att man i de finländska näten upptäckte drygt 25 000 datorer som infekterats av nätmasken under året.

Conficker sprider sig effektivt bland annat på grund av dess förmåga att sprida sig via portabla lagringsmedia, t.ex. USB-minnespinnar. Dessutom sprider sig programmet också via nätförbindelsen, vilket är typiskt för maskar.

Conficker är ett gåtfullt skadligt program eftersom man fortfarande inte känner till dess egentliga syfte. Det är dock känt att en variant av Conficker också har spridit skadeprogrammet Waledac samt skadeprogrammet Spyware Guard, som är känt som ett falskt säkerhetsprogram (scareware). Waledac har tidigare utnyttjats för att skicka skräppost och för att stjäla koderna för olika nättjänster.

Skräppostkampanjer som sprider skadliga program hittade sin väg också till Finland

Skräppostkampanjer som försöker svindla mottagarna har huvudsakligen riktat sig mot utländska bankers och olika amerikanska aktörers, exempelvis USA:s skatteverks IRS webbplatser.

Inte heller i Finland har man lyckats undgå skräppost med skadligt innehåll. CERT-FI mottog flera rapporter om skräppost till finländska adresser som innehållit länkar till skadliga program.

Länkarna i skräppostmeddelandena innehåller ofta en variant av den skadliga programfamiljen Zeus. Programmet är också känt under namnet Zbot och WSNPOEM. I Zeus-skräppostkampanjen, som drabbade även Finland, fick e-postmottagaren ett meddelande som innehöll en länk via vilken det skulle vara möjligt att ladda ned ett hjälpprogram som fastställer inställningarna i e-postprogrammet Outlook. Länken ledde dock i verkligheten till ett skadligt program.

Man vet att det skadliga programmet Zbot har använts bland annat för att stjäla koderna för nättjänster och kreditkortsinformation. Vissa varianter av den skadliga programfamiljen har även försetts med mekanismer som identifierar olika nätbanker. Tills vidare har man inte stött på en version av det skadliga programmet som skulle ha skräddarsytt för en attack mot de finländska nätbankerna.

Datorer som har infekterats av Conficker eller Zbot utgör ett exempel på hur användarnas datorer olovligt övertas och används för många typer av skadlig verksamhet. Stora fjärradministerade botnät kan bestå av upp till hundratusentals kapade datorer.

Skadliga program spreds via knäckta www-sidor

CERT-Fi får hela tiden meddelanden om finska webbplatser som har knäckts eller är sårbara. Innehållet på webbplatserna har bearbetats genom att lägga till JavaScript-kod som gjorts oläslig, eller en dold iframe-ram. När användaren besöker den knäckta webbsidan laddar webbläsaren ner sidan som innehåller det skadliga programmet.

Det ovan beskrivna sättet att sprida skadliga program kallas på engelska för en drive by download-attack. Användaren märker nödvändigtvis inte alls att datorn har blivit smittad och datorn kan smittas också då man besöker en webbplats som anses vara pålitlig.

Det är möjligt att lägga till skadligt innehåll på webbplatsen antingen med hjälp av webbläsarens sårbarheter eller stulna uppdateringskoder.

Gumblar stjälar FTP-koder

Skadliga program som stjälar uppdateringskoder för webbplatser, exempelvis Gumblar, gör det möjligt att olovligt manipulera innehållet på webbplatsen. Programmet söker FTP-koder för uppdatering på den infekterade datorn och lösenord i anknäring till dem genom att undersöka lösenordsregistren i de program som används för uppdatering av webbplatsen, t.ex. Filezilla eller Dreamweaver.

Vidare kan Gumblar övervaka nättrafiken mellan datorn och FTP-servern och från den övriga trafiken separera koder och lösenord som sänds i klartext. Det skadliga programmet utnyttjar koderna för att sprida sig vidare genom att manipulera webbsidor med hjälp av de stulna koderna. Den använder koderna för att lägga till en dold iframe-ram som innehåller länkar till skadliga webbplatser.

Användare lockas till skadliga webbplatser med hjälp av sökmaskiner

Manipulering av de resultat som sökmaskiner på internet visar används också för att sprida skadliga program. En webbplats med skadligt innehåll lyfts fram högre i sökmaskinens resultat än rena webbplatser. En del sökmaskiner tar emot rapporter om skadliga webbplatser och filtrerar bort dem från sökresultatet.

Aktuella händelser, t.ex. naturkatastrofer och skandaler kring kända personer är populära sökmål. Det är möjligt att påverka sökmaskinernas resultat genom att inkludera lämpliga sökord och med hjälp av SQL-injektioner och skadliga program länka många sidor att dirigera till det önskade målet. Efter årsskiftet har jordbävningen på Haiti också varit svindlarnas favoritämne.

Namntjänsten ofta utsatt för försök till missbruk

Namntjänsten är en så väsentlig del av internetanvändningen att den lockar till försök till missbruk. Skadliga program kan omdirigera namntjänstförfrågningar till en namnserver som administreras av den som utför attacken, varvid användaren kan luras till en förfalskad webbplats.

Det finns en verifieringsmekanism, DNSSEC, för verifiering av svaren från namntjänsten, men den används tills vidare inte i särskilt stor omfattning.

Sårbarheter i applikationsprogramvaror kan utnyttjas längre

De skadliga programmen utnyttjar sårbarheter i operativsystemet eller programvarorna. Operativsystemet eller webbservern uppdateras ofta automatiskt varvid sårbarheter i dem åtgärdas relativt snabbt.

Därför riktar sig de skadliga programmen oftast till övriga programvaror eller tilläggskomponenter som installeras i webbläsare. Senast har man påträffat skadliga program som försöker utnyttja sårbarheter i t.ex. PDF-läsare, Flash-spelare eller Javamiljö.

Användaren kan lockas till att installera ett skadligt program

Knäckta webbplatser kan också locka användaren att själv installera ett skadligt program i datorn vilket gör det lättare att passera operativsystemets säkerhetssystem.

Då man besöker webbplatsen öppnas ett poppuffönster som varnar för att datorn har smittats av ett skadligt program. Genom att installera och utföra programmet som rekommenderas i fönstret, undersöker programmet om datorn är smittad med skadliga program och avlägsnar eventuella skadliga program. Programmet som installeras är i verkligheten ett skadligt program.

Falska säkerhetsprogram kan se mycket trovärdiga ut och det är omöjligt att direkt se att de inte är riktiga informationssäkerhetsprogram. Vidare kan programmen i samband med installationen fråga efter kreditkortsnummer för licensavgiften och installera ett program som sparar användarens tangenttryckningar eller andra spionprogram.

Man har påträffat falska program som ser ut som informationssäkerhetsprogram redan i flera års tid och deras antal beräknas fortsätta att växa.

Riktade attacker med stor spridning

Skadliga program kan spridas genom omfattande distribution och på det sättet försöka påverka så många datorer och användare som möjligt. Målet kan vara att utöka ett botnät som administreras av den som leder attacken eller olovlig anskaffning av information.

CERT-FI mottog också meddelanden om riktade attacker mot vissa organisationer. Avsändarinformationen är förfalskad, och meddelandenas ämnen är trovärdiga och har koppling till organisationens normala verksamhet. Meddelandet kan vara t.ex. en kallelse till ett möte eller en konferens och det distribueras till nyckelpersonerna i organisationen. Tillsammans med meddelandet distribueras en ny version av ett skadligt program som informationssäkerhetsprogrammet inte känner till från tidigare.

Ghostnet

I mars 2009 publicerades i Canada en rapport som redogjorde för en omfattande serie av dataintrång som gjorts med hjälp av riktad distribution av skadliga program. Förbindelser för administration på distans som skapats med hjälp av det skadliga programmet Ghost användes för att spionera på data från datorer i olika organisationer.

Enligt den information som CERT-FI har finns det inga finländska aktörer bland dem som distribuerat de skadliga programmen. CERT-FI fick kännedom om två datorer tillhörande en främmande stat som påträffats i ett finländskt nät.

Obefogade varningar om skadliga program förekom

CERT-FI mottog upprepade meddelanden under 2009 om ett e-postutskick som varnade för ett skadligt program som distribueras som e-postbilaga och som påstods förstöra alla filer på hårddisken. Engelsk- och svenskspråkiga versioner av meddelandet har tidigare spridits på nätet. En person som tillhör de anställda på central-kriminalpolisen hade förfalskats som avsändare av meddelandet i december 2009.

Enligt den information som CERT-FI har innehöll de kopior av meddelandet som personer skickade till varandra i varnings-syfte inget skadligt program eller länkar till webbplatser som innehåller skadliga program. Förutom detta utskick har det också förekommit andra cirkulär som utlovar antingen mobiltelefoner eller pengar. Traditionellt utlovar cirkulären antingen lycka eller olycka beroende på till hur många personer som mottagaren skickar dem vidare.

Traditionella försök till svindel som skickas som e-post förekommer hela tiden. De handlar ofta om arv, lotterivinster eller erbjuder arbete som penningförmedlare.

Säkerhetsbrister och skadliga program även i mobiltelefoner

I början av 2009 upptäcktes informations-säkerhetsproblem som gäller inställnings-meddelanden och WAP push-meddelanden av datormobiler.

Experterna har redan under en lång tid varit medvetna om bristerna i hanteringen av de inställningsmeddelanden som är avsedda för nätinställningarna i mobiltelefoner. Alla mobiltelefoner erbjuder nämligen inte användaren möjlighet att försäkra sig om inställningstextmeddelandenas verkliga avsändare. I en del fall är det dessutom möjligt att telefonen godkänner inställningarna utan att meddela användaren eller låter bli att visa de inställningar som ändras.

Ett WAP push-meddelande sänds till telefonen och det innehåller länkens WAP-adress. Det har förekommit problem med hanteringen av WAP push-meddelanden i en del äldre telefonmodeller som är sällsynta i Finland. Då en mobiltelefon som har funktionsproblem tar emot ett WAP push-meddelande är det möjligt att den laddar ner och till och med installerar WAP-innehållet i meddelandet utan att användaren känner till detta.

En mask spred sig i iPhone-mobiltelefoner

I slutet av året påträffades en nätmask i Apples iPhone-mobiltelefoner, vilken gick under namnet Ikee.B och som spred sig mellan telefonerna med hjälp av sshd-tjänsten och standardlösenord som inte hade bytts ut. Masken spred sig endast till telefoner från vilka man avlägsnat spärrningen så att det går att använda också andra programvaror än sådana som är officiellt godkända av Apple. Det är inte möjligt att installera sshd-programvaran utan att avlägsna spärrningen.

Datormobiler är ett lockande mål

Datormobilernas egenskaper börjar så småningom vara av samma klass som de av persondatorer. De har ofta nästan oavbruten internetförbindelse och det är möjligt att ta kontakt med dem via internet. Tillämpningarna som används är delvis samma eller påminner till sina egenskaper om de programvaror som används i egentliga datorer.

Informationssäkerheten i datormobilernas operativsystem och programvaror är i många hänseenden sämre än i vanliga datorer. Normalt innehåller datormobilerna inte informationssäkerhetsprogram och de tillämpar sig inte för centraliserad administration eller automatiska programuppdateringar. Vidare förekommer datormobiler och de stjäls oftare. Spridningen av maskar främjas av att datormobilerna rör sig mellan olika datanät.

Skadliga program har påträffats också i andra apparater

I början av året påträffades i Finland ADSL-terminalutrustning som hade infekterats av ett skadligt botnät-program. 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.

Internationellt samarbete för att förebygga missbruk

De aktörer som gör och sprider skadliga program och som är botnätoperatörer har bildat nätverk och deras verksamhet är uppbyggd enligt en modell som är bekant från programvaru- och ICT-tjänstindustrin.

Serverar som används för spridning av skadliga program och som kommandoserverar för botnät hyrs ofta av stora tjänsteleverantörer som kan ha ett stort antal underleverantörsförhållanden från någon som hyr en fysisk serveranordning till någon som hyr slutlig webbtjänstkapacitet. Den som hyr ut lokaliteter för utrustningen vet inte nödvändigtvis något om den brottsliga slutkunden. Den andra ytterligheten utgörs av aktörer som uppenbarligen helt och hållet har koncentrerat sig på brottslig verksamhet och som utåt upprätthåller kulisserna för en till synes saklig leverantör av hostingtjänster.

Inga tecken på en långsammare tillväxt av antalet fall av missbruk kunde ses 2009

Utredningen av botnäten som baserar sig på kraftigt decentraliserad verksamhet kräver i sin tur omfattande internationellt samarbete mellan flera branscher. CERT-aktörer, webbtjänstleverantörernas informationssäkerhetsenheter, informationssäkerhetsforskare vid universiteten och branschföretagen samt polismyndigheterna håller på att bilda allt tätare samarbetsnätverk. Nätverkens verksamhet blev tydligt aktivare och intensivare under 2009.

Informationssäkerhetsgemenskapens internationella samarbete har visat sig fungera

Ett exempel på fungerande samarbete mellan informationssäkerhetsaktörer är utredningen av en blockeringsattack som till en del också riktade sig mot ett finländskt företag hösten 2009.

Tack vare det internationella samarbetet hittade CERT-FI kommandoservern för det botnät som använts för attacken ungefär inom en timme efter att ha mottagit meddelandet om dataintrång. Effektiva åtgärder för att begränsa attacken kunde inle-

das snabbt. Vidare varnade CERT-FI ett flertal utländska aktörer som var föremål för en attack av samma botnät. Kommandoservrar städades bort i flera länder på olika håll i världen.

Operatörer som erbjuder skadligt innehåll avstängdes från nätet

Enligt en utredning av informationssäkerhetsgemenskapen förlorade flera operatörer som koncentrerat sig på skadlig verksamhet sin nätförbindelse under 2009. Det synligaste fallet var kanske den amerikanska tjänsteleverantören 3FN. Flera kommandoservrar för nätverk för spridning av skräppost underhölls i operatörens nät.

CERT-FI bistod sina isländska kolleger i utredningen av ett fall med ett skadligt program som stal koder till nätbankssystem. I samband med fallet identifierades en tjänsteleverantör i Lettland som koncentrerat sig på skadlig verksamhet. Lettland är det EU-land som ligger närmast Norden i vilket man kunde konstatera ett tydligt ökat utbud av tjänster som utgör en risk för informationssäkerheten.

Bekämpningen av Conficker förenade informationssäkerhetsaktörer

En av den internationella informationssäkerhetsgemenskapens mest omfattande gemensamma aktioner riktades mot den skadliga programfamiljen Conficker. En särskild arbetsgrupp, "Conficker Working Group", utvecklade bekämpningsåtgärder mot det skadliga programmet. ICANN, som administrerar domännamn på internet, deltog för första gången eftersom bekämpningsåtgärderna krävde att registreringen av en stor mängd domännamn förhindras i samarbete med de organisationer som registrerar domännamn.

CERT-FI genomförde en jämförande undersökning av europeiska CERT-aktörer

CERT-FI färdigställde en undersökning av europeiska CERT-FI-aktörer under 2009. Syftet med undersökningen var att jämföra elva CERT-enheters verksamhet och identifiera bra verksamhetsmodeller som tillämpas och som kunde utnyttjas i CERT-FI:s och Kommunikationsverkets verk-

samhet. Undersökningen var den första av sitt slag i Europa och dess resultat har väckt internationellt intresse.

Som väntat fann man såväl likheter som skillnader mellan de CERT-aktörer som deltog i undersökningen. På basis av resultaten kan man konstatera att alla enheterna som deltog i jämförelsen är unika. Var och en har utformat sin verksamhet till en helhet som uppfyller placeringsstatens och kundkretsens krav.

Det fanns dock också en stor mängd likheter i verksamheten. Alla enheter som deltog i jämförelsen agerar som nationell kontaktpunkt i sitt eget land gällande hanteringen av brott mot informationssäkerheten. Kontaktpunkten måste ha fungerande och omfattande inhemska och utländska kontaktnätverk vilkas betydelse betonas av samtliga aktörer.

Dessutom erbjuder alla enheter en mängd bastjänster till sin kundkrets. Dessa omfattar analys och koordinering av dataintrång som gäller deras egen stat, uppföljning av informationssäkerhetsläget och skapandet av en lägesbild över informationssäkerheten.

I undersökningen framgick det vidare att det råder stora skillnader i förutsättningarna för framgångsrik CERT-verksamhet mellan staterna i Europa. Europeiska kommissionen har också fäst uppmärksamhet vid detta.

Kommunikationsverket deltar i utvecklingen av CERT-funktioner i länderna i Afrika

Kommunikationsverket har under 2009 bistått med internationell experthjälp vid inledningen av nationell CERT-verksamhet. Projektet som finansieras av utrikesministeriet har bistått Sydafrika med att utveckla förutsättningar för etablering och ibruktagning av CERT-funktioner.

Projektarbetaren som anställdes vid CERT-FI har haft i uppdrag att stöda partnerorganisationen i Sydafrika i planeringen av CERT-verksamheten som ska etableras. Vidare ansvarar projektarbetaren för inledning och koordinering av det internationella samarbetet samt för anordnande av evenemang och kurser.

Kommunikationsmyndigheterna i Kenya och Tanzania har också fått ta del av åsikter och råd för planering och inledning av CERT-verksamheten.

Autoreporter fick pris

Tjänsten Autoreporter, som producerats av CERT-FI, fick pris i en tävling som ordnades av FIRST (Forum of Incident Response and Security Teams) och CERT/CC (CERT Coordination Center)¹. Tävlingen sökte efter bästa förfaranden för att upptäcka och förhindra dataintrång.

Tjänsten Autoreporter, som produceras av CERT-FI, samlar automatiskt in observationer om skadliga program och dataintrång som gäller finländska nät. Under 2009 sände systemet drygt 215 000 anmälningar till dem som uppdaterar finländska nätverksområden. Antalet anmälningar har ökat med över 250 procent jämfört med året innan. Ökningen kan till en del förklaras med det stora antalet anmälningar gällande nätverksmasken Conficker.

CERT-FI publicerar mer exakt statistik om observationer av skadliga program år 2009 i sin följande informationssäkerhetsöversikt i april 2010.

1 <http://www.cert.fi/tietoturvanyt/2009/06/ttn200906301435.html>

Flera programsårbarheter med omfattande inverkan publicerades

CERT-FI publicerade under 2009 resultatet av två omfattande sårbarhetskoordineringsprojekt. De gällde sårbarheter i bibliotek avsedda för implementeringen av TCP-protokollet och hantering av XML-filer. Dessutom offentliggjordes sårbarheter i anslutning till Microsofts ATL-utvecklingsbibliotek och protokollet SSP.

Sårbarheten hos protokollet TCP

Fel i anslutning till implementeringen av protokollet TCP möjliggjorde blockeringsattacker med mycket små trafikmängder. Sexton olika tillverkare har under slutet av året lämnat ett utlåtande om sårbarhetsmeddelandet som offentliggjordes i september. CPNI², JP-CERT³ och US-CERT⁴ som deltog i koordineringen har publicerat egna meddelanden.

Sårbarheten i hanteringen av XML-filer

I början av året överlät det finländska Codenomic Oy testresultaten gällande program för hantering av XML-filer för att koordineras av CERT-FI. Sårbarheter påträffades i sammanlagt tre programbibliotek som hanterar XML-filer.

Tolv tillverkare har offentliggjort korrigeringar i programvarorna under årets lopp. En del av sårbarheterna hade korrigerats i ett av bibliotekens kodutdelning, men korrigeringen hade inte nått fram till alla produkter som använder biblioteket. Detta bevisar att korrigeringen av sårbarheter inte begränsar sig till att orsaken till problemet avlägsnas. Det är viktigt att förmedla budskapet om korrigeringsbehovet och detaljer i anslutning till korrigeringen också till de aktörer vilkas produkter påverkas av sårbarheten.

2 <https://www.cpni.gov.uk/Products/technicalnotes/Feb-09-security-assessment-TCP.aspx>

3 <http://www.jpCERT.or.jp/english/at/2009/at090019.txt>

4 <http://www.kb.cert.org/vuls/id/723308>

Fel i bibliotek som utnyttjats för Microsofts programutveckling

I utvecklingsversionen av programbiblioteket ATL, som producerats av Microsoft, upptäcktes en sårbarhet som gjorde det möjligt för dem som utför attacker att utföra sin programkod i målsystemet. Även om bibliotekets källkod aldrig egentligen har offentliggjorts som en produkt för användarna har den ändå tillämpats i många programvaror. Microsoft har offentliggjort en korrigerig av sårbarheten och spärrlistor som spärrar de sårbara komponenternas funktion har utdelats i samband med de månatliga uppdateringarna.

Eftersom sårbarheten förutom Microsofts programvaror även gäller för en stor grupp tredje parters produkter, meddelade Microsoft att bolaget har inlett samarbete också med övriga tillverkare i syfte att korrigera felet.

Sårbarheten i protokollet SSL/TLS

En sårbarhet i anslutning till protokollet SSL/TLS som offentliggjordes i november gör det i vissa fall möjligt att mata in eget innehåll i början av en skyddad förbindelse. Även om sårbarheten inte gör det möjligt för konfidentiell information att läcka ut, anses den vara allvarlig eftersom SSL-skyddet är en viktig del t.ex. av säkerheten vid elektronisk handel.

Sårbarheten är ovanlig eftersom den beror på ett fel i planeringen av protokollet och påverkar därför i praktiken alla SSL/TLS-tillämpningar. Ju tidigare i förverkligandet av systemet felet som leder till sårbarheten har uppstått, desto större blir sårbarhetens verkningsområde och desto svårare blir det att korrigera sårbarheten.

Sårbarheten korrigeras genom att i protokollet TLS definiera en expansion som gör det möjligt att täppa till hålet.

Ändringarna i lagen om dataskydd vid elektronisk kommunikation trädde i kraft

Ändringen av lagen om dataskydd vid elektronisk kommunikation trädde i kraft i juni. Förutom rättigheter att behandla identifieringsuppgifter gällde ändringen också 20 § om dataskyddsåtgärder. Bestämmelsen ändrades för att bättre motsvara teleföretagens, mervärdestjänsteleverantörernas och sammanslutningsabonnenternas behov.

Vid beredningen av dataskyddsbestämmelsen tog man i beaktande det nära beroendet mellan samhällets livsviktiga funktioner och kommunikationsnät, kommunikationstjänster och datasystem. I syfte att skydda den kritiska infrastrukturen är det väsentligt att säkerställa de elektroniska data- och kommunikationssystemens funktion. Det är nödvändigt att minimera de skadliga effekterna av hoten mot dataskyddet genom åtgärder som utförs i Finland, eftersom det är möjligt att påverka utländska aktörer och system endast i begränsad utsträckning.

Enligt lagen har ett teleföretag, den som tillhandahåller mervärdestjänster eller en sammanslutningsabonnent samt de som verkar för dessas räkning rätt att vidta i lagen fastställda åtgärder för att säkra dataskyddet.

Åtgärder kan i första hand vidtas för att upptäcka, förhindra och utreda störningar som kan inverka menligt på dataskyddet i kommunikationsnäten eller för de tjänster som anslutits till dem och för att göra störningarna föremål för förundersökning. En annan situation som möjliggör åtgärder är säkerställandet av kommunikationsmöjligheterna för avsändaren eller mottagaren av ett meddelande. En tredje situation som berättigar till datasäkerhetsåtgärder är förhindrande av förberedelser av betalningsmedelsvindel som förverkligas i omfattande skala via kommunikationstjänster.

De möjligheter som den nya lagen erbjuder utnyttjades för att skydda användarna av nätbanker

Efter att lagen trädde i kraft har Kommunikationsverket en gång uppmanat teleföretagen att vidta de åtgärder som föreskrivs i den nya lagen om dataskydd vid elektronisk kommunikation i syfte att skydda dem som använder de finländska nätbankerna. I situationen i fråga hade en amerikansk nätoperatör upprepade gånger varit delaktig i phishing- och svindelfall.

Teleföretagen behöver inte en rekommendation av Kommunikationsverket för att filtrera trafiken. Filtreringsåtgärder kan inledas alltid när teleföretagen anser att förutsättningarna för filtrering uppfylls.

Sveriges spaningsverksamhet kan sträcka sig även till finländarnas telekommunikations-förbindelser

En ny lag om signalspaning trädde i kraft i Sverige den 1 december 2009. Genom lagen fick Försvarets Radioanstalt rätt att i försvarssyfte utföra signalspaning också i de fasta näten gällande elektronisk kommunikation som överskrider Sveriges gränser. Detta betyder att även finländska aktörers telekommunikation till Sverige eller som förmedlas via Sverige kommer att omfattas av spaningsverksamheten.

Spaningsverksamheten gällande telekommunikation via Sverige har tagits i beaktande i Kommunikationsverkets förnyade föreskrift som gäller teleföretagens skyldighet att informera sina kunder och Kommunikationsverket om hot mot informationssäkerheten som riktar sig mot deras tjänster. Bestämmelsen trädde i kraft från inledningen av 2010. Bestämmelsen betonar särskilt teleföretagens skyldighet att informera sina kunder om hot mot informationssäkerheten som riktar sig mot sådana tjänster som genomförs i utlandet och erbjuds finländska kunder. Informationskyldigheten grundar sig på lagen om dataskydd vid elektronisk kommunikation.

Kommunikationsverket har påmint teleföretagen om denna informationskyldighet ända sedan 2007. Samtidigt har man bland annat påpekat att teleföretagen ska

genomföra sina tjänster på ett informationssäkert sätt. Om ett teleföretag inte förmår genomföra en tjänst utan hot mot informationssäkerheten, måste teleföretaget informera sina kunder och Kommunikationsverket om hoten. Meddelandena ger kunderna en möjlighet att bedöma om tjänsten motsvarar deras informationssäkerhetsbehov. Kommunikationsverket har också publicerat information om hur man skyddar kommunikationen.⁵

Framtidsutsikter

CERT-FI anser att skadliga program fortfarande sprids i syfte att få ekonomisk vinning. Kreditkortsnummer och användar-ID:n är de mest intressanta målen, eftersom de är lätta att marknadsföra.

Webbaserade gemenskapstjänster är lämpliga mål för svindelförsök. En del av tjänsterna har avgiftsbelagt innehåll som kan säljas vidare inom tjänsten, men även olika försök till phishing av användar-ID:n och betalkortsuppgifter förekommer allmänt.

Förutom undersökning av sårbarheter i programvaran i datormobiler kan man också förvänta sig att intresset gentemot undersökning av protokoll som används i mobilnätet och nätets funktion ökar. År 2009 offentliggjordes programvaror med vilka det är möjligt att simulera funktionen hos delar i mobilnätverket med hjälp av ett program

⁵ <http://www.ficora.fi/viestinsuojaus/>

Största delen av de kontakter som CERT-FI behandlade gällde skadliga program och hot mot informations säkerheten förorsakade av dem.

CERT-FI kontakter per kategori	2009	2008	Förändring
Intervju	97	88	+10 %
Sårbarhet eller hot	148	375	-61 %
Skadligt program	1828	2156	-15 %
Rådgivning	387	359	+8%
Beredning av attack	48	87	-45 %
Dataintrång	120	187	-36 %
Blockeringsattack	89	96	-7 %
Övriga informationssäkerhetsproblem	118	43	+174%
Social Engineering	164	189	-13 %
Sammanlagt	2999	3580	-16 %