

cert-fi

**INFORMATIONSSÄKERHETSÖVERSIKT
3/2009**

21.10.2009

CERT-FI

Informationssäkerhetsöversikt 3/2009

Inledning

CERT-FI har sedan början av 2008 fram till slutet av augusti innevarande år slutbehandlat cirka 1 800 sådana ärenden där ett skadligt program som stjälar information har förmedlat användarens uppgifter till utomstående. Även finländska användare har utsatts för skadliga program som stjälar information.

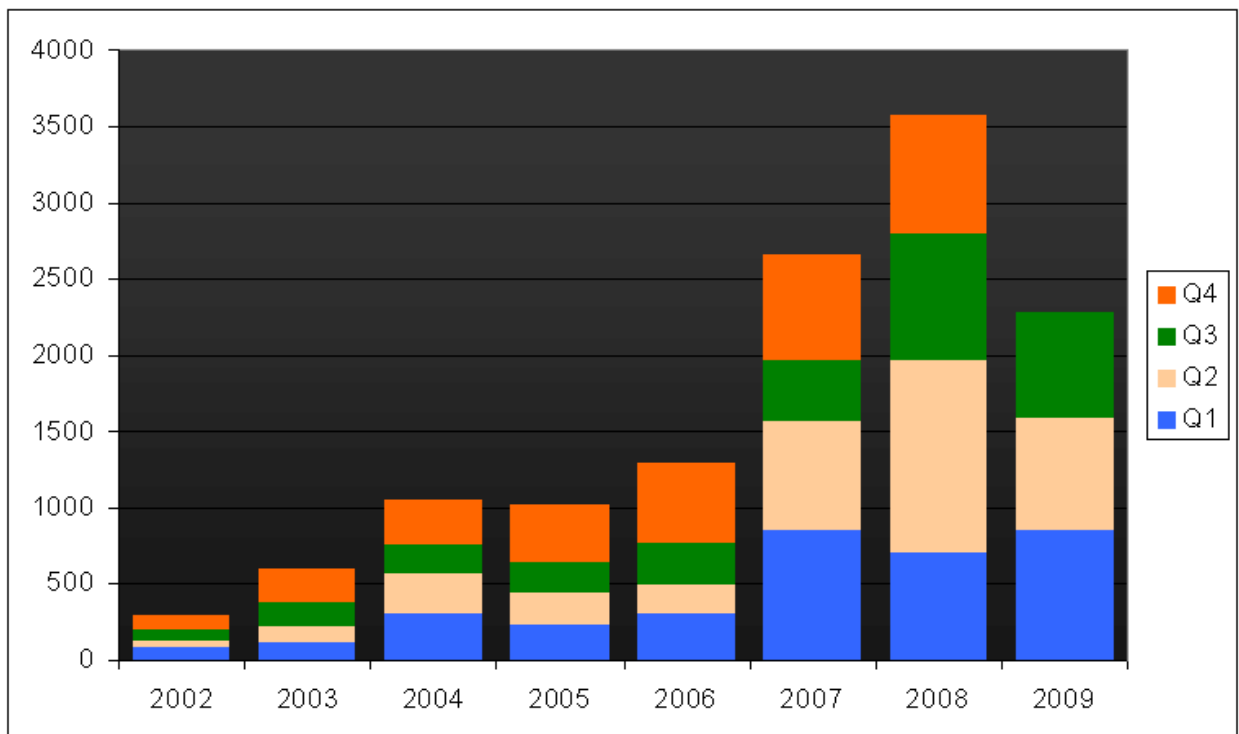
Resultaten av två sårbarhetssamordningsprojekt, som var mer omfattande än normalt, har publicerats. I augusti offentliggjordes ett samordningsprojekt i anslutning till XML-bibliotek. XML-bibliotek används för hantering av information och dokument i många slags datasystem.

I september offentliggjordes resultaten av ett långvarigt sårbarhetssamordningsprojekt i anslutning till servertillämpningar av protokollet TCP. TCP är ett förbindelseförfarande för nätet som används för dataöverföring i de flesta webbtillämpningar,

och därför omfattade detta fall flera programtillverkare.

Målet med sårbarhetssamordningen är att få tillverkarna att testa sina produkter och åtgärda eventuella sårbarheter i dem. Tack vare det goda samarbetet mellan programtillverkarna och CERT-FI lyckades samordningsprojekten väl.

Förutom flera utländska tjänster har även en finländsk webbplats varit föremål för blockeringsattacker. CERT-FI har samordnat utredningen av fallet. Med hjälp av internationellt samarbete har utredningsarbetet framskridit väl.



Antalet fall som CERT-FI har behandlat har sjunkit från fjolåret.

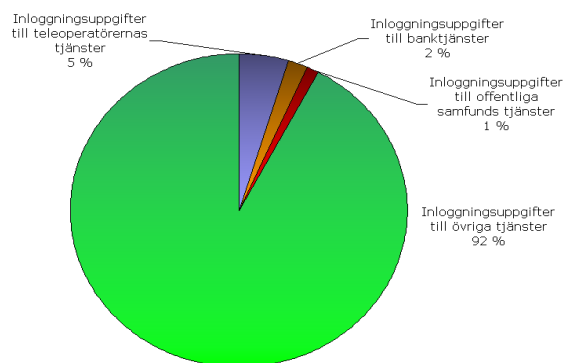
Skadliga program stjälar användar-ID:n även av finländare

CERT-FI får sporadiskt anmälningar om fall där finländska användare av elektroniska ärendehanteringstjänster har blivit offer för skadliga program som stjälar information. Anmälningarna kan även omfatta information som insamlats av skadliga program. Den information som de skadliga programmen kommit åt består vanligen av inloggningsuppgifter för elektroniska tjänster, såsom användar-ID:n och lösenord. De skadliga programmen samlar emellertid också uppgifter från blanketter som används med webbläsare, såsom e-postmeddelanden, webbutiksbeställningar och nätbanksblanketter.

CERT-FI har sedan början av 2008 fram till slutet av augusti innevarande år slutbehandlat cirka 1 800 sådana ärenden där ett skadligt program som stjälar information har förmedlat användarens uppgifter till utomstående. Största delen av de tjänster som varit föremål för attackerna har varit olika slags webbaserade gemenskapstjänster. En betydande del av alla de fall som CERT-FI har behandlat har riktats mot en internationell tjänst som ett finländskt bolag tillhandahåller. Största delen av det totala antalet fall utgörs således av utländska användare av denna tjänst.

När man granskar fallen bör man notera att andelen inloggningsuppgifter som hänför sig till banktjänster är liten i förhållande till alla stulna uppgifter. Kreditkortsuppgifter saknas helt i de uppgifter som mottagits av CERT-FI, eftersom det finns andra etablerade rapporteringskanaler för dessa ärenden.

Fördelningen av uppgifter mellan olika aktörer



Vanligt med webbsidor som smittats av skadliga program

Det blir allt vanligare att datorn smittas av skadliga program när man besöker en angripna webbplats som sprider skadliga program. Med hjälp av ftp-koder som stulits av det skadliga programmet inbäddas i webbplatsens kod till exempel en Javascript-kod som laddar ner det skadliga programmet eller så sätts en länk som laddar ner det skadliga programmet i en dold iframe-tag.. Smittorisk finns om tilläggsdelarna i den sporadiska besökarens webbläsare eller programmen som är avsedda att visa innehållet, såsom Adobe Acrobat eller Adobe Flash Player, är sårbara och om antivirusprogrammet inte är uppdaterat.

När datorn smittats av ett skadligt program kan programmet följa med terminalens nättrafik och stjäla ftp-koder och lösenord. Programmet kan också skicka skräppost från terminalen, installera ett skadligt program som liknar ett informationssäkerhetsprogram eller förfälska resultaten av sökningar i sökmaskiner på internet för att leda användaren till falska webbplatser. De skadliga programmets funktionsmekanismer varierar med programmen.

Programmen i den skadliga programfamiljen Zeus kan också samla användar-ID:n och lösenord genom att spara tangenttryckningar och skicka dem till kommandoservern för senare missbruk. Stulna användar-ID:n kan dessutom användas för att attackera andra webbplatser genom att lägga till annat innehåll på dem.

Optimering av sökmaskinernas resultat används för att sprida skadliga program

De sökresultat som sökmaskinerna ger användarna har redan under några år använts för att sprida skadliga program. Under innevarande år har fenomenet blivit vanligare och även antagit nya former. Skadliga program distribueras via angripna www-sidor eller www-sidor som särskilt skapats för detta syfte. De som distribuerar skadliga program strävar efter att lyfta dessa sidor högst upp på listan över sökresultat med hjälp av sökmaskinsoptimering.

Vid sökmaskinsoptimering matar man in sökord om aktuella händelser på skadliga sidor. När användare som söker efter ytterligare information om ett aktuellt ämne sedan följer sökresultaten hamnar de på www-sidor som genom att utnyttja sårbarheter i webbläsaren strävar efter att smitta ner besökarens terminal eller vilseleda användaren att själv installera det skadliga programmet.

Webbläsare och sökmaskiner identifierar en del av de falska sidorna

Webbsidor som smittats av skadliga program kan vara svåra att upptäcka. Till sitt yttre avviker sidorna inte nödvändigtvis alls från normala, rena sidor. Fenomenet kallas också drive-by-download.

Det är emellertid skäl att notera att sökmaskinsbolagen under det gångna året betydligt har satsat på att kontrollera de sidor som sökresultaten ger för att hitta skadliga program eller metoder för missbruk genom vilka skadliga program kan smitta. Idag varnar de vanligaste sökmaskinerna användaren för att det bland sökresultaten finns en sida vars innehåll har konstaterats vara skadligt. Även webbläsaren kan varna för skadligt innehåll.

I vissa fall strävar man efter att kringgå sökmaskinernas säkerhetskontrollmekanismer. Detta sker så att länkarna som används för att distribuera skadliga program och som syns i sökmaskinens resultat leder till sidor som endast omdirigerar användaren till nya sidor med det skadliga programmet. Den server som ansvarar för den sista webbplatsen i kedjan kontrollerar värdet på Referrer-fältet i HTTP-begäran. Utifrån detta erbjuds besökare som omdirigerats endast från vissa sidor en sida som sprider skadliga program.

Städning av webbplatsen räcker inte, man måste också förhindra att den angrips på nytt.

Det är eventuellt inte tillräckligt att städa innehållet på en webbplats som smittats av ett skadeprogram. Den som upprätthåller webbplatsen ska informeras om att koder och lösenord som behövs för uppdatering har hamnat i fel händer och att apparaten har smittats. Då det sättet hindrar man sidorna från att angripas på

nytt. Lösenordet som gäller ftp-koden ska också bytas.

Myndigheterna reagerar på tillhandahållandet av skadligt innehåll

I början av juni avlägsnades amerikanska 3FN som tillhandahåller hosting-tjänster från webben genom ett myndighetsbeslut på initiativ av FTC, dvs. USA:s handelskommission. Enligt FTC hade tjänsteleverantören aktivt skyddat kriminella genom att inte reagera på så kallad takedownbegäran. I FTC:s klagomål anklagades tjänsteleverantören för distribution av bland annat skadliga program, barnpornografi och skräppost. Företaget anklagades för att medvetet upprätthålla ett nätverk av kapade maskiner, dvs. botnät, och kommandoservrar för botnät.

Operatörens förbindelser avbröts genom domstolsbeslut. Avbrytandet av förbindelserna hade omedelbar inverkan på mängden skräppost som skickades från botnätet Cutwail. Effekten var emellertid inte lika stor som i fallet med tjänsteleverantören McColo som bortkopplades i november 2008. I dess nätverk fanns flera botnät som skickade skräppost, och efter avstängningen föll mängden skräppost temporärt med upp till en tredjedel.

Det som var exceptionellt med bortkopplingen av operatören 3FN från nätet var att det skedde genom myndighetsbeslut. I fallet McColo och beträffande en annan amerikansk tjänsteleverantör Intercage, bidrog den internationella informationssäkerhetsgemenskapens fortlöpande meddelanden om skadlig trafik och kriminell verksamhet till bortkopplingen.

CERT-FI offentliggjorde resultaten av omfattande sårbarhetssamordningsprojekt

I augusti offentliggjorde CERT-FI resultaten av ett mer omfattande sårbarhetssamordningsprojekt i anslutning till XML-bibliotek. Omfattningen berodde på att XML-språk används för hantering av information och dokument i många slags datasystem. Därtill kan programbibliotekens sårbarhet i allmänhet få vidsträckt effekt, eftersom sårbara bibliotek ofta används i tio- eller hundratals programtillämpningar.

I september offentliggjordes resultaten av ett långvarigt sårbarhetssamordningsprojekt i anslutning till servertillämpningar av protokollet TCP. TCP är ett förbindelseförfarande för nätet som används för dataöverföring i de flesta webbtillämpningar, och därför omfattade detta fall flera programtillverkare.

Målet för sårbarhetssamordningen är att få tillverkarna att testa sina produkter och åtgärda eventuella sårbarheter i dem. CERT-FI har varit i kontakt med hundra programtillverkare under samordningen av TCP-sårbarheten. Hittills har 13 programtillverkare publicerat ett utlåtande eller programkorrigeringar utifrån de uppgifter som erbjöds dem.

Även risken för misslyckanden ökar i stora sårbarhetssamordningsprojekt. Med misslyckande avses vanligen att detaljerade uppgifter gällande sårbarheten delvis eller i sin helhet avslöjas för tidigt. Ett för tidigt avslöjande av detaljerna kan leda till att sårbarheten utnyttjas i attacker.

De två nu offentliggjorda projekten lyckades och målen uppnåddes. I ingetdera fallen har alla detaljer gällande sårbarheten ännu offentliggjorts. Samordningen av sårbarheter i anslutning till protokollet TCP och arbetet för att finna sårbara tillverkare fortsätter. Ett sårbarhetsutlåtande om projektet finns på sidan www.cert.fi.

Blockeringsattack mot en finländsk webbplats

CERT-FI har aktivt deltagit i utredningen av en blockeringsattack mot ett finländskt företag. Attacken riktades inte enbart mot den finländska tjänsten utan också mot flera utländska webbplatser.

Samordningsarbetet i anslutning till händelsen fortsätter. Arbetet inleddes väl – botnätet som attackerade tjänsten identifierades mycket snabbt genom internationellt samarbete.

I blockeringsattacker kan man genom snabbt samarbete med den egna leveran-

tören av internetjänster och CERT-FI effektivt begränsa effekterna av attacken.

Om organisationens verksamhet i hög grad är beroende av nättjänster som fungerar i alla förhållanden finns det orsak att diskutera beredskapsåtgärder med tjänsteleverantören redan i förväg.

Blockeringsattacker som riktar sig mot Finland är ganska sällsynta.

Kommunikationsverket deltog i beredskapsövningen Tieto 2009

Kommunikationsverket deltog i början av oktober i Tieto övningen.

Målet med övningen var att effektivisera samarbetet mellan myndigheterna och förvaltningen vid skötsel av problem som hänför sig till datasystemen. Övningen, som ordnas med två års intervall, hölls förra veckan.

Utöver försvarsmakten, statens dataadministration och ministerierna deltog företag inom datateknikbranschen såsom teleoperatörer och leverantörer av ICT-tjänster i övningen.

Framtidsutsikter

Skadliga program som stjälar information och kampanjer för att distribuera sådana program med hjälp av skräppost och www-sidor förekommer troligen allmänt även under slutet av året. Meddelanden som maskerats som julhälsningar eller julerbjudanden från företag är typiska sätt att sprida skadligt innehåll. Skadliga program kan också distribueras med länkar i meddelanden.

Om det i allmänt använda program, såsom webbläsare, dess tilläggsdelar eller program avsedda för bläddring i dokument finns en öppen sårbarhet, kan de skadliga programmen utnyttja detta och även spridas i stor utsträckning.

Även till mobiltelefoner kan man skicka länkar i form av sms som leder till skadligt innehåll.

Kontakter med CERT-FI per kategori	1-9/2009	1-9/2008	Muutos
Media	78	67	+16%
Sårbarhetsanmälan	107	323	-67%
Skadligt program	1451	1719	-16%
Rådgivning	250	243	+3%
Skanning	29	71	-59%
Dagaintrång	101	147	-31%
Blockeringsattack	63	72	-13%
Informationssäkerhetsproblem	82	33	+148%
Social ingenjörskonst	118	127	-7%
Sammanlagt	2279	2802	-19%

Anmälningar om skadliga program utgör största delen av incidenten som CERT-FI handlar.