

CERT-FI
INFORMATIONSSÄKERHETSSÖVERSIKT
11 april 2008

CERT-FI informationssäkerhetsöversikt 1/2008:

CERT-FI fick veta om ett fall där en tredje part gjorde kontoöverföringar under en nätbankssession utan att användaren märkte det. Än så länge har det dock varit fråga om enskilda attacker mot finländska banker.

CERT-FI publicerade en hel mängd sårbarheter som har samband med hantering av paketerings- och arkivformat. Data paketeras eller arkiveras i så gott som alla tillämpningar. Det betyder att sårbarheterna påverkar flera olika operativsystem och program. Sårbarheterna kan i helhet karakteriseras som avsevärda.

Ett flertal sårbarheter av typen cross site scripting fick publicitet. Dessa sårbarheter hade sitt ursprung i ett flertal populära finländska www-sidor. Dylika sårbarheter möjliggör inte intrång i en server men de kan utnyttjas för att göra blufförsök eller för att skada ryktet för ägaren till webbsidorna.

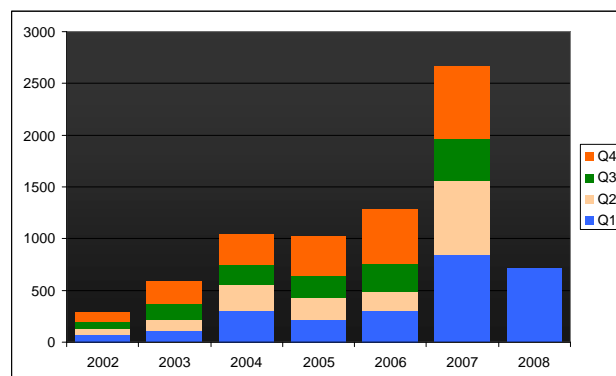
Finländska nätbanksförbindelser kapades med skadliga program

CERT-FI blev informerad om det första skadliga programmet som spionerar på finländska kunders nätbankssessioner. Länkar till www-sidor med det skadliga programmet (som klassificeras som en **banktrojan**) spreds i synnerhet till finländska adresser via skräppost. Bluffmeddelandena hänvisade antingen till en påstådd kärnolycka i S:t Michel eller till en begäran om att kontakta sällskapssjuka "Tatjana".

Det skadliga programmet styrde användarens nätbankssession via en dator som kontrollerades av angriparen. Under denna session kunde angriparen observera och ändra både uppgifter som visades åt användaren och uppgifter som överfördes till bankens nätbankstjänst. Angriparen kunde även göra olovliga kontoöverföringar från användarens konto.

Skadliga program som riktas mot nätbanker utvecklas så att man med ett och samma program försöker lura så många olika bankers kunder som möjligt. Det är lätt att bearbeta de skadliga programmen och därför är det också möjligt att rikta dem mot nya nätbanker endast med att göra ändringar i programmets inställningar. Ett program som har smittat en dator söker regelbundet en ny inställningsfil från nätet, vilket betyder att programmets beteende kan ändras och styras också efter själva infektionen. Det skadliga programmet som upptäckts i Finland har tidigare använts åtminstone mot tyska, schweiziska och holländska nätbanker. I början kände antivirusprogram inte igen den använda versionen och därför kunde antivirusprogrammen inte genast skydda datorn från att smittas.

Det är skäl att i fortsättningen anta att skadliga program avsedda för att kapa bankssessioner självständigt kan ändra innehållet i webbsidorna som visas för användaren, styra användarnas sessioner till www-servern som angriparen kontrollerar och att ändra innehållet i http-meddelanden från användaren. Kapningen lyckas trots att en SSL-krypterad förbindelse används. Än så länge har CERT-FI inte fått veta om helautomatiserade skadliga program som skulle vara riktade mot finländska nätbankskunder.



I CERT-FI:s system för hantering av incidenter registrerades 709 hanterade kontakter under årets första kvartal.

Sårbarheter i program som hanterar paketerings- och arkivformat

CERT-FI publicerade i samarbete med brittiska CPNI och japanska JPCERT en mängd sårbarheter som har samband med hantering av paketerings- och arkivformat. En del av sårbarheterna kan möjliggöra att angriparens programkod körs i datorn.

Arkivformaten hanteras i så gott som alla tillämpningar. Data komprimeras i allmänhet för att göra överföringen snabbare eller för att reducera det förvaringsutrymme som filerna kräver. Många program är därmed tvungna att behandla komprimerad data eller arkivfiler som omfattar flera olika filer.

Samtidigt med sårbarheterna publicerades också testmaterial som sammanstälts av forskningsgruppen OUSPG vid Uleåborgs universitet. Materialet har framställts med hjälp av testmetoder som utvecklats i samband med PROTOS-GENOME projektet. Hanteringen av filer från testmaterialet orsakade fel i ett flertal olika program. Testmaterialet omfattade över en miljon fall som testade problempunkterna i mer än tio olika arkivformat.

Tillverkarna fick ett tillfälle att testa sina egna produkter innan materialet publicerades. CERT-FI, CPNI och JPCERT tog kontakt med tiotals olika tillverkare av programvara. Målet var att ge information om testresultaten i synnerhet till stora tillverkare och även till sådana tillverkare som tidigare haft problem med sina produkter.

Testmaterialet publicerades för att förbättra kvaliteten vid hanteringen av arkivformat, inte för att hitta enskilda fel. Under projektets lopp upptäcktes att de tillverkare som var vana med att korrigera enskilda och noggrant specificerade programmeringsfel inte alltid kunde utnyttja den givna informationen eller testmaterialet. Det stora antalet kontaktade tillverkare utgjorde en stor utmaning för själva koordineringen.

Parterna i projektet tyckte att det offentliga testmaterialet som hänför sig till olika arkivformat förbättrar funktionssäkerheten hos de olika programmen. CERT-FI och OUSPG tänker fortsätta samarbetet gällande sammanställning och publicering av motsvarande testmaterial.

CERT-FI följer utvecklingen av läget nu efter att sårbarheterna har publicerats. Det är sannolikt att alla sårbarheter som gäller paketerings- och arkivformat inte ännu har hittats eller korrigerats. Det lönar sig att omedelbart installera de uppdateringar som tillverkarna erbjuder.

Många webbsidor har cross site scripting sårbarheter

Sampo Bank förnyade sitt datasystem och sin nätbank under påsken. När den nya nätbanken togs i bruk upptäcktes en cross site scripting (XSS) sårbarhet på webbsidan. Sårbarheten gjorde det möjligt för en tredje part att visa eget innehåll som en del av bankens sidor om användaren gick till webbsidan via en länk som var uppbyggd på ett visst sätt.

CERT-FI kontakter	Q1/2008	2007	2006	2005	2004	2003	2002
Intervju	17	80	51	46	59	48	27
Sårbarhet eller hot	39	64	87	134	33	13	8
Skadligt program	460	1678	536	212	216	115	34
Rådgivning	64	393	291	366	425	149	116
Beredning av attack	32	3	26	14	73	70	27
Dataintrång	25	119	45	49	31	30	46
Blockeringsattack	15	64	18	12	21	34	15
Övriga informationssäkerhetsproblem	10	48	67	129	141	98	3
Social ingenjörkonst	47	197	109	25	2	1	0
Skräppost	-	18	58	31	46	36	12
Totalt	709	2664	1288	1018	1047	594	228

Sårbarheten, som korrigerades snabbt, orsakade inget stort hot för användarna. Den stora publiciteten som incidenten fick ledde dock till att nätanvändarna började leta efter motsvarande sårbarheter på övriga webbsidor. CERT-FI har fått veta om flera tiotals fall på diverse finländska sidor.

Cross site scripting sårbarheter gör det möjligt att innehåll som en tredje part skapar visas för användaren som en del av den egentliga webbsidan. Att utnyttja sårbarheten kräver att användaren luras mata in den programkod som behövs i samband med attacken. Webbsidan returnerar sedan koden som körs i användarens webbläsare. Servern kontrollerar inte tillräckligt noggrant de uppgifter användaren matar in och därmed blir det möjligt att utnyttja sårbarheten. Programmeringsspråket JavaScript utnyttjas oftast i sårbarheterna.

XSS-sårbarheterna kan användas för att göra skämt med sidorna samt för att samla lösenord som behövs i tjänsten. Med skräppost är det möjligt att sprida en länk som innehåller en kort kod som utnyttjar sårbarheten. En begäran om att ge sitt lösenord som användaren ser på den autentiska www-sidan kan alltså i själva verket komma från angriparen. CERT-FI har inte fått veta om fall

där sårbarheter i banktjänster eller i andra tjänster skulle ha utnyttjats för andra ändamål än skämt.

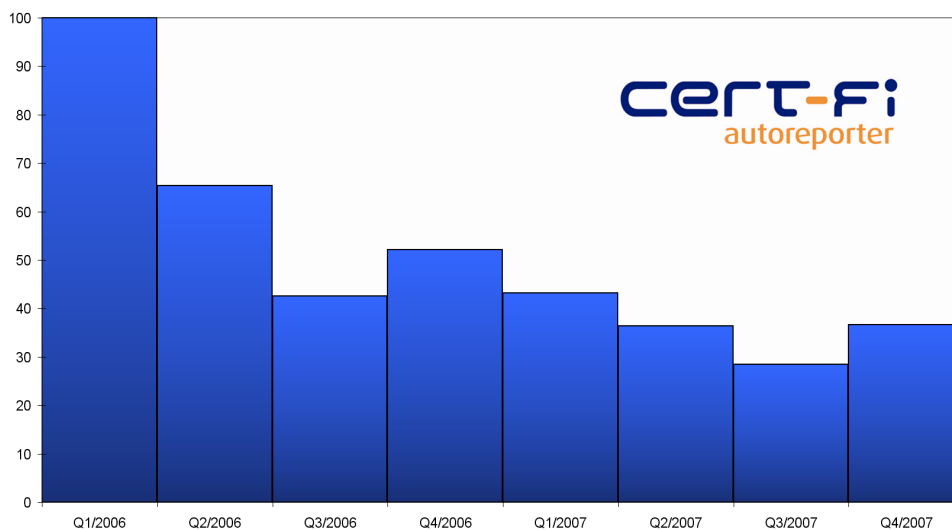
CERT-FI har förmedlat uppgifterna om sårbarheterna till dem som upprätthåller tjänsterna. Sårbarheterna har i allmänhet korrigerats, eventuellt har tjänsten tillfälligt tagits ur bruk.

Framtidsutsikter

Enligt CERT-FI:s uppskattning kan finländska tjänster allt oftare användas för brottslig verksamhet samt för systematisk spridning av skadliga program. Det är sannolikt att skadliga program sprids till finländska användare t.ex. via finskspråkig skräppost eller via finländska www-sidor. Sådana bluffar är sannolikt mycket trovärdiga. Också egenskaperna hos skadliga program som används för attackerna utvecklas ytterligare.

Fler sårbarheter för paketerings- och arkivformat kommer att hittas nu när testmaterialet har publicerats. Programtillverkarna publicerar korrigerade versioner av sina produkter. CERT-FI publicerar också inom den närmaste framtiden sårbarheter i vissa allmänna program som används för att skydda överföring av data.

Upptäckta skadliga program / bredbandskunderna, Q1/2006 = 100



Antalet upptäckta skadliga program i relation till bredbandskunderna har minskat under de senaste två åren.