

cert-fi

**INFORMATIONSSÄKERHETSÖVERSIKT
1/2010**

9.4.2010

CERT-FI informationssäkerhetsöversikt 1 /2010

Inledning

Informationssäkerheten för registrerade användare av spelsidan Ålypää äventyrades då användaruppgifter i mars stals från spelsidan och publicerades. Över 125 000 användarnamn, lösenord och e-postadresser publicerades på internet.

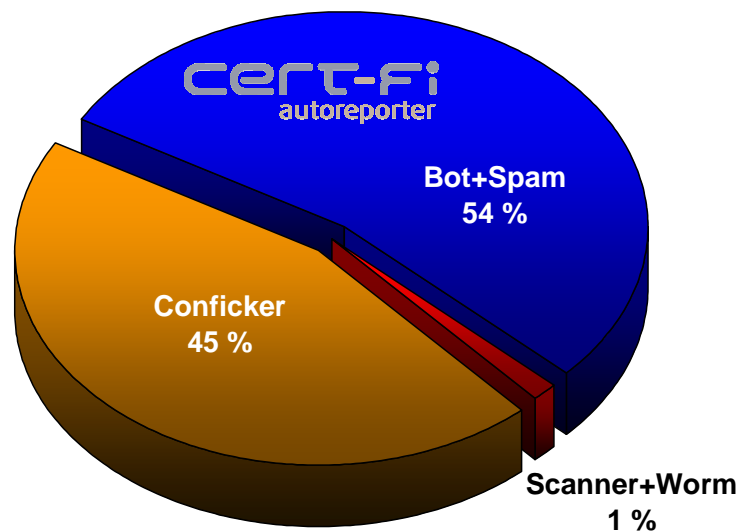
I februari kom det fram att över 100 000 kortsuppgifter hade stulits från en angripen dator på ett kafé i Helsingfors.

Mera uppmärksamhet behöver fästas vid informationssäkerheten när tjänster förverkligas. Från tjänster med dålig informationssäkerhet kan användarnas lösenord stjälas och innehåll kan olovligt skrivas in på webbsidorna. Användarna bör även fästa uppmärksamhet vid hurdana lösenord de använder. Alltför lätta lösenord och användning av samma lösenord på många olika tjänster ökar risken för missbruk.

Skadliga program som stör nätbanksförbindelser förekommer redan bland banker i Finland. Bankerna håller på att ta i bruk ytterligare säkerhetsåtgärder för att hindra olovliga kontouöverföringar. Tillsvidare finns det i Finland få skadliga program som kapar nätbanksförbindelser.

Av statistikuppgifterna från CERT-FI:s Autoreporter-system framgår, att antalet skadliga program som upptäcktes tydligt ökade år 2009 i jämförelse med föregående år. Nästan hälften av alla anmälningar om skadliga program handlade om nätmasken Conficker. Under 2009 sände CERT-FI nästan 100 000 anmälningar om datorer som smittats av det skadliga programmet Conficker.

Observationer per typ 2009



Nästan hälften av alla rapporter på skadliga program från 2009 gällde Conficker.

Lösenord från spelsidan Älypää spreds offentligt

I slutet av mars framkom ett fall, då någon hade lyckats stjäla från spelsidan alypaa.com användarnamn, lösenord och e-postadresser som hade använts vid registrering till tjänsten.

En fil som innehåll uppgifter om över 125 000 användare fanns tillgänglig via flera fildelnings-tjänster och informationen om det spreds snabbt på internet.

Man hindrade snabbt inloggning på webbsidan Älypää, men användarnas informationssäkerhet äventyrades även på grund av att många hade använt samma lösenord i andra nättjänster. Utgående från e-postadressen kunde man i många fall räkna ut användarnamnet och sedan pröva det lösenord som stulits från tjänsten Älypää.

CERT-FI fick till exempel kännedom om fall där man olovligt hade använt koderna till användarens Gmail-e-postkonto eller Facebook.

När det gäller lösenorden finns det övrigt att önska

Användarnamn och lösenord är det vanligaste sättet för webbtjänster att försäkra sig om användarens identitet. Man borde fästa större uppmärksamhet vid valet och förvaringen av lösenord.

Granskningen av de lösenord som stals från tjänsten Älypää visar, att det bland dem fanns sådana som var alltför lätta att gissa eller alltför korta. Man ska undvika att använda samma lösenord i olika tjänster och vara beredd på att vilket lösenord som helst kan knäckas eller att det på annat sätt kan komma i fel händer.

Brister i tjänstens förverkligande

Enligt uppgifter från CERT-FI kunde de som snokade rätt på tjänsten Älypääs lösenord utnyttja tjänstens föråldrade och *säkerhetsmässigt* bristfälliga förverkligande. Lösenorden har uppenbarligen funnits okrypterade i bakgrundssystemets databas. Databasen kunde man komma åt med en s.k. *SQL injection* som utnyttjar svagheter i granskningen av inmatningen.

Klotter på politikernas hemsidor

I mars framkom några fall, då någon olovligt hade matat in material på offentliga personers webbsidor.

Enligt uppgifter från CERT-FI användes i de fallen sidornas administratörlösenord, som man

hade kunnat gissa sig till eller tagit reda på annat sätt. Sidorna hade ändrats med hjälp av deras normala administratörsgränssnitt.

Bristfällig kontroll av inmatning kan möjliggöra informations- läckor och klotter

Allt fler webbtjänster har i bakgrunden en databas, som styrs med SQL-kommandon. Med hjälp av dem kan man söka eller ändra uppgifter i databasen.

Databasen kan innehålla material från webbsidor, användarnamn och lösenord till tjänsten eller uppgifter med vars hjälp sidor som visas för användaren skapas. Databasen kan man komma åt till exempel genom ett webbformulär eller via sidans URL-adress.

Om inmatningen från användaren inte kontrolleras tillräckligt noggrant, kan man mata in egna kommandon till databasen, som gör det möjligt att leta efter uppgifter eller olovligt ändra sidorna. Lösenord bör aldrig förvaras okrypterade i systemet.

Till CERT-FI kommer ständigt uppgifter om olika sidors sårbarhet för angrepp av typen SQL-injection. Det finns allmänt tillgängliga färdiga program för att leta efter svagheter och för att pröva sidornas funktion och det krävs inte särskilt stor sakkunskap för att använda programmen.

Uppgifter stjäls också med hjälp av skadliga program

Från servern på ett kafé i Helsingfors stals i februari över 100 000 kunders kontokortsnummer. Kontokortsnumren är det vanligaste bytet för skadeprogram som stjälar information. Kortnumren kan användas för inköp eller säljas vidare för brottsliga ändamål.

Allt fler observationer av skadliga program år 2009

Statistikuppgifterna från CERT-FI:s Autoreporter-system om skadliga program år 2009 visar, att antalet anmälningar om skadliga program tydligt ökade i jämförelse med föregående år.

Särskilt har nätmasken som är känd under namnet Conficker och som spreds kraftigt speciellt i början av år 2009 påverkat ökningen av antalet observationer.

Av de observationer av skadliga program som gjordes under året handlade hela 45 % om det skadliga programmet Conficker. En procent handlade om förberedelse för dataintrång och

resterande 54 % om inte närmare specificerade skadliga program av bot-typ, som till exempel använts för att sända spam.

Eftersom även Conficker kan anses vara ett skadligt program av bot-typen, är det lätt att konstatera, att skadliga program förknippade med botnet har tilldragit sig nästan all uppmärksamhet.

Under 2009 sände CERT-FI nästan 100 000 anmälningar om observationer av det skadliga programmet Conficker. Under året har man observerat att över 25 000 finländska IP-adresser har smittats av skadliga program.

CERT-FI försöker nå dem som är kroniskt smittade av skadliga program

Enligt CERT-FI:s observationer förekommer ofta samma adresser upprepade gånger i anmälningar som handlar om smitta med skadliga program.

Bland annat på grund av spridningen av det skadliga programmet Conficker har CERT-FI sedan slutet av år 2009 aktivt försökt kontakta innehavarna av de datorer, vilkas adresser ständigt förekommer i rapporter om skadliga program. Innevarande år försöker man fortfarande aktivt nå de användare som ständigt lider av skadliga program.

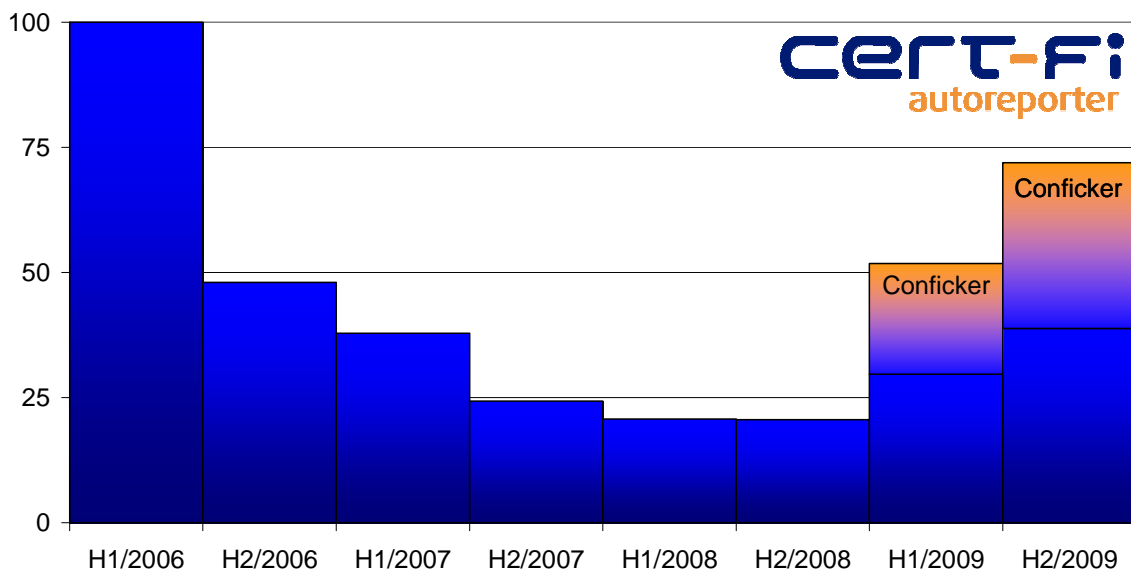
Conficker utgör fortfarande ett hot

Det skadliga programmet Conficker har smittat miljontals datorer i olika delar av världen. För de datorer som smittats med skadliga program väntar vidare programuppdatering och instruktioner. Tillsvidare har dock inte det botnet som Conficker-datorerna bildar utnyttjats i någon större utsträckning.

Det bör observeras att datorer som är smittade med Conficker är sårbara även för smitta av andra skadliga program, eftersom Conficker kopplar bort operativsystemets säkerhetsfunktioner.

Observationer av skadlig kod per bredbandskund

(H1/2006=100)



Med skadliga program försöker man komma åt finländska nätbankkunders pengar

Även hos finländska nätbanker förekommer redan skadliga program som används för att under nätbankssessioner göra olovliga penningöverföringar från användarens konto.

Enligt CERT-FI:s observationer är mängden skadliga program som är inriktade på nätbankskunder i Finland ganska liten, men fenomenet verkar ha blivit bestående.

Genom internationellt samarbete har man lyckats få bort flera sådana internetleverantörer från internet, vilkas tjänster har använts för att sprida skadliga program och för kapning av bankförbindelser.

Bankerna överväger motåtgärder för att förhindra olovliga penningöverföringar med hjälp av skadliga program. Man kan till exempel be om en bekräftelse av en ovanlig överföring med ett textmeddelande eller kontrollsamtal.

Med ett bekräftelseförfarande som är oberoende av nätbankförbindelsens miljö försöker man försäkra sig om att överföringen sker enligt användarens önskan.

Missbruk av textmeddelanden har ökat

Mängden spam i form av textmeddelanden har ökat under de senaste åren. Trenden har börjat märkas också för finländska mobiltelefonanvändare, för målet för textmeddelanden som sänds i bedrägeriavsikt är allt oftare ett finländskt mobiltelefonnummer och språket är finska.

CERT-FI har fått kännedom om ett fall, då ett finländskt mobiltelefonnummer missbrukades som avsändarens nummer för textmeddelanden som skickades i bedrägeriavsikt. Detta ledde till att mottagarna av bedrägerimeddelandena riktade stora mängder med arga textmeddelanden och telefonsamtal som svar till mobiltelefonnumret. På grund av meddelandena och telefonsamtalen som strömmade in blev det omöjligt att använda mobilanslutningen normalt.

De traditionella telefon- och mobilnäten är ofta planerade så, att man förutsätter att andra nät och annan nätutrustning är pålitliga. Därför har det i vissa situationer visat sig vara svårt att undersöka och hindra missbruk av telefonnäten.

Det är svårt att spåra den som stör, särskilt i situationer när han direkt kan använda en nätutrustning för mobilnätet, till exempel en textmeddelandecentral.

Början av året lugnt beträffande koordinering av sårbarheter

Under de senaste åren har CERT-FI behandlat flera sårbarheter med vittgående effekt som är förknippade med programvarubibliotek, filformat och protokoll. Innevarande år har dock med tanke på koordinering av sårbarheter börjat på mer sedvanligt sätt.

CERT-FI publicerade i januari 2010 information om två sårbarheter, av vilka den ena berörde Linux-kärnans IPv6 och den andra komprimeringsprogrammet GNU Gzip.

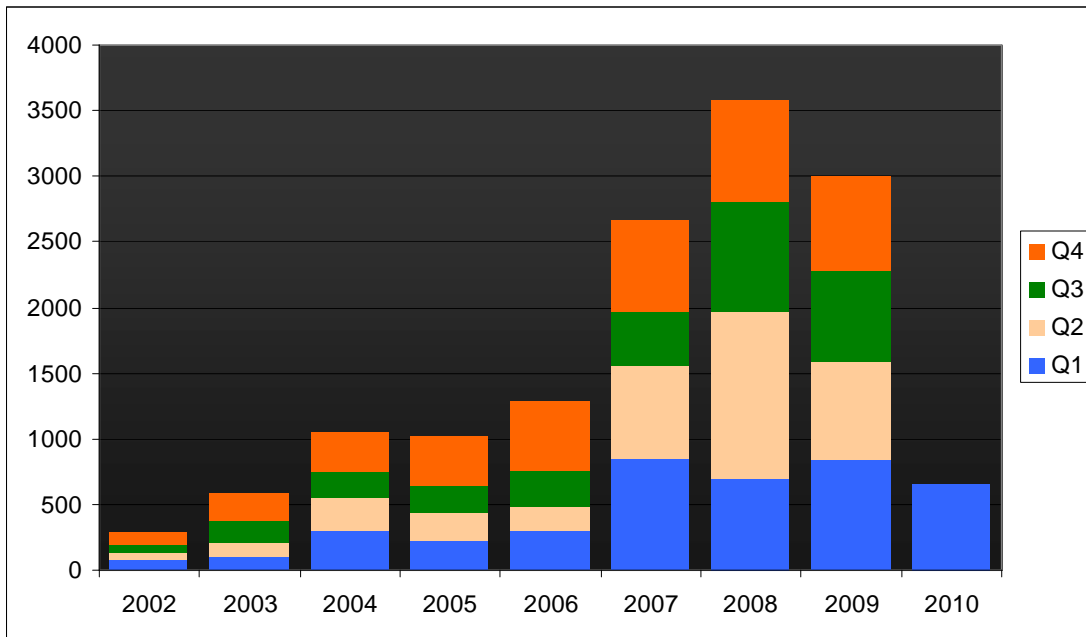
I vartdera fallet gjorde programtillverkaren korrigerade programversioner och de flesta operativsystemdistributörer införde snabbt korrigeringsarna som en del av de programpaket som de distribuerar, varvid hotet som orsakades användarna kunde hållas ganska litet under varje fas av koordineringsprojektet.

Framtidsutsikter

I en nära framtid kan ytterligare missbruk förknippat med de nyligen avslöjade lösenorden uppdagas. Genom att gissa sig till användarnamnet och lösenordet är det möjligt att kapa till exempel användarens e-postkonto och uppträda i användarens namn.

CERT-FI följer kontinuerligt med uppgifter om utveckling av skadliga program som stjälar och kapar bankförbindelser, och deltar i internationellt samarbete för att minimera de skador programmen orsakar

CERT-FI kontakter per kategori	1/2010	1/2009	Förändring
Intervju	32	35	-9 %
Sårbarhet eller hot	63	20	+215 %
Skadligt program	317	577	-45 %
Rådgivning	130	93	+40 %
Beredning av attack	11	10	+10 %
Dataintrång	36	28	+29 %
Blockeringsattack	15	23	-35 %
Övriga informationssäkerhetsproblem	10	23	-56 %
Social engineering	43	33	+30 %
Sammanlagt	657	842	-22 %



Mängden av fall som CERT-FI behandlade förblev på samma nivå som tidigare år. Rapporter på skadliga program utgör fortfarande nästan hälften av alla kontakter även om automatiseringen har ökats.