

cert-fi

**INFORMATIONSSÄKERHETS-
ÖVERSIKT 2/2009**

3.7.2009

CERT-FI informationssäkerhetsöversikt 2/2009

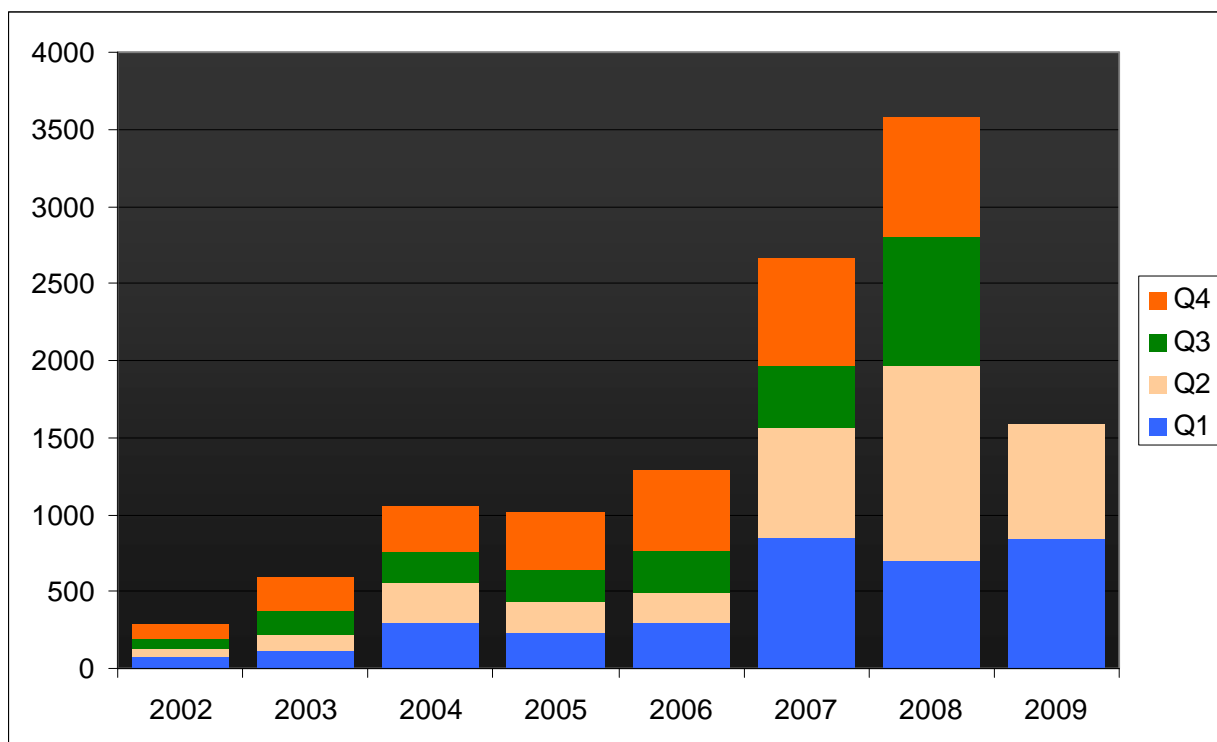
Inledning

Skadliga program sprids även med hjälp av reklam på www-sidor. Man har kunnat få ett skadligt program på sin dator från en annonsruta på en finländsk tidnings webbforum. Det kan vara svårt att avvärja *malvertising*-fenomenet eftersom den

som driver webbplatsen vanligen inte har kontroll över innehållet i annonserna.

CERT-FI får fortfarande meddelanden om datorer som infekterats av nätmasken Conficker. En kort tid spreds masken till och med via utrustning som såldes av en operatör.

Samordningen av reparationen av sårbarheter i anslutning till tillämpningar av protokollet TCP har varit en krävande uppgift. Reparationer av sårbarheter i programvaror från flera tiotals tillverkare kommer att publiceras.



Antalet fall som CERT-FI har behandlat har sjunkit från fjolåret och ligger nu på samma nivå som år 2007.

Skadliga program har distribuerats via reklam på www-sidor

I Finland har ett fall bekräftats där skadliga program distribuerats via en annons på en www-sida. Via en annonsruta som placerats på webbforumet för en finländsk tidning kunde man få ett skadligt program på sin dator. Det skadliga programmet laddades inte ned varje gång annonsen visades, utan programmet distribuerades slumpmässigt. Avsikten med detta är att göra det svårare att utreda brott mot informationssäkerheten.

Via utlagt reklam innehåll kan det komma skadligt innehåll på en webbsida som i övrigt är säker. Tills vidare har detta fenomen, som även är känt under namnet *malvertising*, varit sällsynt på finska webbplatser. För dem som sprider skadliga program är metoden effektiv, och de som driver webbsajter har svårt att skydda sig mot den.

De som driver webbplatser kan i allmänhet inte direkt påverka annonsernas innehåll, utan de erbjuder annonsplats på sidan och ingår avtal med en serviceleverantör som förmedlar reklam. Annonserna laddas ned från en extern server och deras innehåll kan variera beroende på nedladdningsgång eller beroende på från vilket land den besökande användarens IP-adress verkar vara ifrån.

Skadligt innehåll på knäckta www-servrar

Skadliga program är inte enbart ett problem för webbsidor med annonser. CERT-FI får varje vecka meddelanden om flera finska webbplatser på vilka man lyckats införa skadligt innehåll.

Skadliga program erbjuds för nedladdning från knäckta servrar, på vilka man kan införa innehåll med hjälp av SQL-injektion, dvs. genom att använda en oskyddad eller felaktigt programmerad hantering av indata på servern. Sidorna kan också manipuleras med användar-ID:n och lösenord som är avsedda för administration av webbplatsen och som har utretts med

hjälp av ett skadligt program som stjälar data.

De skadliga programmen erbjuds vanligen till användaren med hjälp av ett iframe-element som lagts till i sidans källkod. Elementet har gjorts osynligt i webbläsaren genom att redigera CSS-stilmallen. Det dolda iframe-elementet innehåller en maskerad javascript-kommandoserie eller en länk via vilken det egentliga skadliga programmet laddas ned på datorn.

Användaren upptäcker nödvändigtvis inte något som avviker från det normala, och det skadliga programmet kan laddas ned utan att användaren klickar på någon av de länkar som finns på sidan.

Skadliga program som distribueras från knäckta webbplatser försöker ofta utnyttja kända sårbarheter i webbläsare eller tilläggskomponenter till webbläsare, t.ex. Flash och Java. Användaren kan minska sannolikheten för en infektion genom att se till att alltid ha den senast uppdaterade versionen av webbläsaren, operativsystemet och antivirusprogrammet på sin dator.

Om man lyckas införa skadligt innehåll på en populär webbplats, kan det skadliga programmet få stor spridning via webbplatsen. Automatiska skadliga program som letar efter webbplatser som kan knäckas beaktar emellertid inte webbplatsernas popularitet, utan skadligt innehåll kan införas på alla webbplatser som är sårbara.

För att webbplatserna ska kunna hållas fria från skadliga program är det av största vikt att webbplatsens och serverns administratör är aktiv, att serverprogrammen uppdateras och att förändringar som gjorts i www-sidornas innehåll kontrolleras.

Data läckte från vårdslöst skyddad server

I maj offentliggjordes ett fall, där det var möjligt att från en www-server ladda ned filer som inte var avsedda att vara offentliga.

I detta fall var orsaken att webbplatsens säkerhetsinställningar hade gjorts så vårdslöst att det var möjligt att bläddra i mapparna på servern och ladda ned filer från dem. Fall av detta slag är inte särskilt sällsynta och även CERT-FI blir tidvis underrättad om liknande fall.

Nätmasken Conficker är fortfarande vanlig

Nätmasken Conficker, som sattes i omlopp i december och som även är känd under namnet Downadup, är fortfarande vanlig. CERT-FI får dagligen meddelanden om infekterade datorer.

Under det andra kvartalet såg man dessutom det första tecknet av att datorer som infekterats av Conficker utnyttjats för brottslig verksamhet. Via ett peer-to-peer-nätverk som nätmasken skapat laddades ett skadligt program för sändning av skräppost ned på de infekterade datorerna, som sedan användes för att genomföra en skräppostkampanj. Av en okänd anledning hade det skadliga programmet för sändning av skräppost dock programmerats att förstöras en månad efter installation. Det har endast förekommit ett enskilt fall av detta slag, och utöver detta har datorer som infekterats av Conficker inte systematiskt använts för annan brottslig verksamhet.

CERT-FI har under det andra kvartalet skickat användare över 22 000 rapporter i anslutning till nätmasken Conficker. I finländska nätverk har man konstaterat datorer som infekterats av nätverksmasken på cirka 5 300 olika IP-adresser. Under det första kvartalet skickade CERT-FI cirka 14 000 rapporter, som gällde 3 600 olika adresser.

Conficker fanns en kort tid även på butikshyllan

Ett av nätmasken Confickers spridnings sätt är att den kopieras på USB-minneskort. I maj fick CERT-FI kännedom om ett fall, där ett minneskort som en mobiltelefonoperatör levererade tillsammans med ett USB-modem för datakommunikation inte bara innehöll det antivirusprogram som operatören tillhandahöll utan även nätmasken Conficker.

Operatören hann sälja några tiotals infekterade minneskort. Operatören har kontaktat de kunder som kunnat få ett skadligt program tillsammans med den köpta utrustningen. Vid den tidpunkt de infekterade modemerna såldes kunde de vanligaste antivirusprogrammen redan identifiera den aktuella versionen av det skadliga programmet, och därför fick fallet sannolikt endast begränsade konsekvenser.

Ghostnet gällde även finländare

Den förra informationssäkerhetsöversikten informerade om en omfattande serie av dataintrång som utförts genom riktade attacker. Med hjälp av det fjärrstyrda skadliga programmet Ghost försökte man stjäla data från de attackerade organisationerna. Enligt den information som CERT-FI har finns det inga finländska aktörer bland dem som distribuerat det skadliga programmet.

CERT-FI fick meddelande om två kapade datorer i finländska nätverk, visserligen långt senare efter att fallet kommit ut i offentligheten. Informationen förmedlades till de aktuella parterna.

Publiceringen av sårbarheter i anslutning till protokollet TCP närmar sig

Processen för samordning av reparationen av sårbarheter i anslutning till tillämpningar av TCP-protokollstacken har fortskridit väl med hänsyn till att ärendet är mycket mångfacetterat. Man har dock varit tvungen att senarelägga publiceringen av åtgärderna. Detta är vanligt då en sårbarhet gäller flera mjuk- och hårdvaruleverantörer.

CERT-FI har kontaktat 65 leverantörer i anslutning till sårbarheter och aktiva åtgärder har därefter vidtagits i samarbete med 38 leverantörer. Största delen av leverantörerna har redan åtgärdat sårbarheterna, men en del arbetar fortfarande med att ta fram en pålitlig reparationsmekanism. CERT-FI har för avsikt att publicera informationen om reparationerna samordnat och därför är det slutliga publiceringsdatumet ännu inte helt säkert.

Mjukvaruleverantörer har även gjort olika bedömningar om sårbarheternas allvarighet. Man har visat att det genom att utnyttja sårbarheterna är möjligt att orsaka allvarliga störningar i många program, operativsystem och aktivutrustningar.

CERT-FI har publicerat ett utlåtande om sårbarheterna. Utlåtandet uppdaterades senast i juni. En länk till utlåtandet finns på sidan www.cert.fi.

De allvarliga sårbarheter i programvaror som har framkommit under den senaste tiden har fått uppmärksamhet även på EU-nivå. EU-kommissionen ordnade i slutet av mars ett workshop-seminarium¹ om sårbarheter. I seminariet deltog experter från CERT-FI och andra inledare från Finland.

Medvetenheten om hoten mot informationssäkerheten i anslutning till datormobiler ökar

Experter inom dataskydd har redan länge påtalat de ökande hoten mot informationssäkerheten i anslutning till datormobiler, t.ex. det ökande antalet sårbarheter och skadliga program. Datorer har varit lockande mål för dem som vill skada datanätets funktion och ägna sig åt databrottslighet, medan datormobiler i stort sett har besparats från skadlig verksamhet.

Datormobilerna börjar emellertid påminna om datorer till sina egenskaper och användningssätt, vilket gör dem alltmer lockande som mål för dataattacker. Under den senaste tiden har allt fler hot mot informationssäkerheten i datormobiler offentliggjorts. Bakom denna utveckling ligger den ökade forskningen kring informationssäkerhet.

Under det andra kvartalet år 2009 har man i offentligheten presenterat datasäkerhetsproblem som gäller datormobilernas inställningsmeddelanden och WAP push-meddelanden. De förknippas med fjärrstyrning av telefoninställningarna och

¹ http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/impl_activites/vulnerabilities_workshop/index_en.htm

applikationer som bygger på WAP-protokollet samt på användarnas okunskap om eventuella risker i anslutning till att användaren godkänner inställningsmeddelanden som skickats i avsikt att göra skada.

Inställningsmeddelandena är vanligen SMS-meddelanden från operatören. Med dessa meddelanden kan man förmedla inställningar som behövs bland annat för användning av internet, t.ex. namnserverinställningar. Meddelanden kan emellertid även skickas i avsikt att vilseleda användaren, och genom att byta ut de namnserverar som telefonen använder kan man leda användaren till skadliga www-platser. I vissa telefonmodeller är det också möjligt att fjärrstyra telefonens funktioner med inställningsmeddelanden.

Största delen av mobiltelefonutrustningarna på marknaden kontrollerar ursprunget av mottagna inställningsmeddelanden och ber dessutom en bekräftelse av användaren innan inställningstextmeddelandet godkänns. En försiktig användare har anledning att godkänna mottagna inställningstextmeddelanden endast då mobiltelefonen för första gången kopplas till en ny operatörs nätverk eller då användaren själv bett att operatören skickar inställningarna till telefonen.

Allt vanligare att använda datanätverk för politiska ändamål

De politiska oroligheterna i Estland och Georgien åren 2007 och 2008 syntes även i datanätverken. Nätverken och informationssamhällets tjänster stördes bland annat genom blockeringsattacker. Knäckta www-sidor användes för att publicera politiska budskap. Det var emellertid inte nödvändigtvis statliga aktörer som låg bakom denna verksamhet.

Presidentvalet i Iran i maj 2009 förde fram datanätverksaktivism av ett nytt slag. Sociala nätverkstjänster och publiceringstjänster blev en kanal för privatpersoner att förmedla information och åsikter om händelserna i Iran under det exceptionella tillstånd som rådde i landet.

Diskussionsgrupper och bloggar användes även för att störa spridningen av motsatta

åsikter. På webbplatser gavs vanliga datoranvändare instruktioner om hur de kan använda sin arbetsstation och internetförbindelse för blockeringsattacker. Botnät användes i relativt liten omfattning i attackerna. I stället genomfördes attacker t.ex. med hjälp av webbplatser som programmerats att generera http-begäran.

Lettisk distributör av skadliga program kopplades från nätet

CERT-FI hjälpte utländska myndigheter att utreda ett fall där ett skadligt program användes för att stjäla bankuppgifter. Programmet spreds via en lettisk serviceleverantörs nätadresser.

Vid utredningsarbetet framgick det att samma nät användes som distributionsplattform för flera olika skadliga program. CERT-FI kontaktade den lettiska CERT-gruppen och serviceleverantörens internetoperatör. Det blev klart att flera anmälningar lämnats in med anledning av att operatören bedriver aktiv verksamhet som äventyrar informationssäkerheten i nätet.

Slutresultatet var att serviceleverantörens internetoperatör stängde av serviceleverantörens internetförbindelser på grund av brott mot användarvillkoren.

Autoreporter fick pris

Tjänsten Autoreporter, som producerats av CERT-FI, har fått pris i en tävling som ordnats av FIRST (Forum of Incident Response and Security Teams) och CERT/CC (CERT Coordination Center)². Tävlingen sökte efter bästa förfaranden för att upptäcka och förhindra dataintrång.

Framtidsutsikter

Mängden av skräppost på internet halverades tillfälligt i slutet av fjolåret när operatörer som distribuerar skadligt innehåll avstängdes från nätet. Sedan dess har mängden skräppost stigit tillbaka till den tidigare nivån. Ungefär nio meddelanden av tio är reklampost som mottagaren inte

har beställt, meddelanden som skickas i avsikt att sprida skadliga program eller meddelanden som lockar till brottslig verksamhet.

Inom internationella samarbetsorgan kan man se tecken på att intresset att finna lösningar på problemet ökar. De gemensamma metoderna att åtgärda missbruk är dock tills vidare outvecklade. ICANN, som samordnar förvaltningen av adresser och domännamn på internet, samt APWG (Anti-phishing Working Group), som fokuserar på bekämpning av datastölder, håller på att skärpa sina verksamheter.

APWG håller på att starta ett projekt, där domännamn som registrerats med felaktig information och används för phishing skulle kunna stängas inom några timmar från att svindel har upptäckts och rapporterats. ICANN planerar att precisera övervakningen och handledningen av företag som tillhandahåller tjänster för registrering av domännamn. Båda aktörerna lyfter fram behovet av ett nära samarbete särskilt med nationella CERT-enheter såsom CERT-FI.

2

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

CERT-FI kontakter per kategori	1-6/2009	1-6/2008	Förändring
Intervju	61	46	+33%
Sårbarhet eller hot	65	271	-76%
Skadligt program	1055	1187	-11%
Rådgivning	178	151	-59%
Beredning av attack	24	59	-69%
Dataintrång	65	102	-32%
Blockeringsattack	40	41	-2%
Övriga informationssäkerhetsproblem	46	21	+119%
Social Engineering	59	83	-29%
Sammanlagt	1593	1961	-19%

Anmälningar om skadliga program utgjorde fortfarande största delen av de informationssäkerhetsincidenter som CERT-FI behandlade under början av år 2009. Mer statistisk information finns på adressen www.cert.fi.