

**CERT-FI**

**ÅRSÖVERSIKT 2008**

16.01.2009

# CERT-FI informations- säkerhetsöversikt 4/2008

## Inledning

Under år 2008 upptäcktes sårbarheter med omfattande konsekvenser för internets infrastruktur. Okorrigerad skulle den sårbarhet som gällde internets domännamntjänst (DNS) ha gjort det möjligt att vilseleda användaren eller dirigera e-post till fel adress. Till följd av sårbarheten publicerade CERT-FI en varning. DNS-programvaror uppdaterades snabbt till tryggare versioner, och sårbarheten hann inte utnyttjas i någon större utsträckning. Händelsen visade dock att internets domännamntjänst strukturellt är sårbar för försök att förfälska information. En sårbarhet som upptäckts i implementeringen av TCP-protokollet kan påverka många apparater och programvaror kopplade till internet.

Spridningen av skadligt innehåll på nätet har visat sig vara mera koncentrerad än man tidigare antog. Mängden skräppost på nätet minskade för en tid betydligt då tjänsteleverantören, som hade kommandoservrar för stora botnät, avlägsnades från nätet i november.

Också finländska webbservrars innehåll har olovligt ändrats upprepade gånger genom att serverprogram sårbarheter har utnyttjats. Intrång i servrar siktar i dag ofta på att utnyttja www-sidor för att sprida skadeprogram, och via dessa sidor koppla nya, angripna datorer till botnätverk. Alldeles i slutet av året upptäcktes en mask som sprider sig självt i lokalnät. Den infekterade arbetsstationer och datanät såväl i Finland som annastans i världen.

År 2008 publicerade CERT-FI två informationssäkerhetsvarningar, 156 meddelanden om sårbarheter och 83 artiklar under rubriken Tietoturva nyt! (på finska).

## Internets ålder märks i form av omfattande sårbarheter

De internetprotokoll och programvaror som internet grundar sig på har delvis använts över trettio år. Utgångspunkten var en helt annan då de utvecklades än för det nätverk vi har i dag. En strävan till enkelhet och så god prestanda som möjligt med långsamma förbindelser och datorer med begränsad processorkraft har styrt planeringen. I planeringsskedet fästes ingen större uppmärksamhet vid informationssäkerhet. Senare är det svårt att ändra eller avstå från protokoll och tillämpningar som har tagits i användning.

Nätets verksamhetsmiljö har blivit mera fientlig då användningen har expanderat. Därför medför bristerna i teknologiska lösningar, som gjorts tidigare, problem. De försvårar å ena sidan trygg användning av internet, och å andra sidan förebyggande av missbruk på nätet.

### **DNS-sårbarheter baserar sig på bristfällig identifiering av parterna**

Sommaren 2008 publicerade *Dan Kaminsky* en sårbarhet som gällde internets domännamntjänst (DNS), som väckte sensation i informationssäkerhetsbranschen. Den främsta orsaken var att namntjänsten använder UDP-protokollet. UDP förutsätter inte en dubbelriktad förbindelse, vilket gör det möjligt att sända DNS-förfrågningar, och i synnerhet de svar som hänför sig till dem, med en förfalskad IP-adress. Det är också mycket svårt att spåra UDP-protokollpaketens verkliga avsändare.

Namntjänstförfrågningarna och -svaren har en identifierare, som underlättar att koppla ihop frågor som riktats till namnservern med serverns svar. Vid den här sårbarheten var det i vissa fall för enkelt för angriparen att gissa sig till vilken identifierare som skulle komma att användas härnäst och att mata förfalskade svar till den som sände förfrågan. För att korrigera sårbarheten gjordes identifierarna mera slumpartade i DSN- programvaran.

Korrigeringsarna räcker emellertid inte för att täcka bristerna i själva protokollet.

Namntjänstförfrågningar kan fortfarande göras på basis av förfalskade adresser och namnservrarna kan sålunda utnyttjas vid blockeringsattacker. Det går inte att säkerställa serverns riktighet, vilket gör det möjligt att vilseleda användarna genom att dirigera namntjänstförfrågningar från användarens dator till en server som upprätthålls av vilseledaren. I slutet av året fick CERT-FI vetskap om ett skadegörande program, som genom att uppträda som en DHCP-server försökte ändra namnservrarna för datorer i lokalnätet till egen förmån. De här serverna gav förfalskade svar på vissa adressförfrågningar. Dessa användes sedan för att omdirigera användare, som t.ex. loggade in på en banks hemsida, till en riggad webbplats.

Den DNSSEC-utvidgning av informationssäkerheten som har planerats för DNS-protokollet hjälper att säkerställa att rätt server svarar på namnsverförfrågningarna. Emedan användningen av DNSSEC är förknippad med många utmaningar har den än så länge inte blivit allmänare. DNSSEC belastar namnservrarna mera än nu och förorsakar också mera trafik i nätet. Hanteringen av krypteringsnycklar är speciellt problematisk och också i någon mån en politisk fråga.

### **Problem upptäcktes i implementeringen av TCP-protokollet**

TCP-protokollet och dess implementeringar har förbättrats flera gånger under årens lopp. TCP har skapats för tillförlitlig dataöverföring, och bristerna i protokollet har närmast gällt dess komplexitet, inte tvärtom.

I september meddelade det svenska företaget *Outpost24* att man hade upptäckt sårbarheter som gällde implementeringar av TCP-protokollet. Information om sårbarheterna gavs på den svenska Sec-T- och den finska T2-informationssäkerhetskonferensen. Outpost24 kontaktade senare CERT-FI-enheten för att koordinera korrigeringen av sårbarheterna med de olika tillverkarna. Korrigeringsprocessen har framskridit såsom väntat. CERT-FI och dess internationella samarbetspartners har kontaktat tillverkarna av

programvara, så att de ska kunna bedöma hur sårbarheterna påverkar deras egna produkter. Närmare information om sårbarheterna torde publiceras under år 2009.

### **Sårbarheter i mobil programvara**

Mobila skadeprogram eller betydande sårbarheter har hittills varit sällsynta. Alldeles i slutet av året upptäcktes en sårbarhet i S60-operativprogrammet, som används i mobiltelefoner. Sårbarheten möjliggör en blockeringsattack mot dessa mobiltelefoner. Ett programmeringsfel som gällde textmeddelanden hittades i telefonens programvara. Ett textmeddelande som riggats på ett visst sätt och togs emot i en mobiltelefon med sårbar programvara medförde att telefonen inte efter det kunde sända eller ta emot meddelanden, förrän inställningarna hade nollats. De inhemska mobiloperatörerna har börjat filtrera meddelanden man vet att är skadliga.

CERT-FI har även fått vetskap om andra sårbarheter som påverkar informationssäkerheten i mobil utrustning. Tidtabellen för publiceringen är inte ännu fastslagen.

### **Koordineringen av sårbarheter arbetsdryg**

Koordineringen av sårbarheter har medfört mycket arbete för CERT-FI. I mars publicerades testmaterial, som sammanställdes av forskningsgruppen OUSPG vid Uleåborgs universitet, för testning av ett otal förpacknings- och arkivformat. Sårbarheter som upptäcktes med hjälp av testmaterialet har uppdaterats under året.

I maj publicerades sårbarheter upptäckta av Codenomcon Oy i både OpenSSL och GnTLS. OpenSSL och GnTLS är öppen källkod, som allmänt används för kryptering. Övriga tillverkare som använder koden i sin programvara kontaktades.

I september upptäckte Codenomcon Oy också en annan sårbarhet i ICMPv6 implementeringen av KAME-projektets öppna källkod. Under årets sista kvartal fick CERT-FI flera koordineringsuppdrag, vilka torde publiceras under år 2009.

## **Kommunikationens tillförlitlighet under luppen**

Den elektroniska kommunikationens tillförlitlighet har diskuterats i samband med förberedelserna för ändring av lagen om dataskydd vid elektronisk kommunikation. I början av år 2009 fick Sveriges signalspaningsorganisation (Försvarets radioanstalt) tillstånd att övervaka telekommunikation i fasta nät i Sverige. Också största delen av internettrafiken från Finland till andra länder sänds via Sverige. Signalspaningen kan speciellt riktas mot okrypterad kommunikation.

E-postmeddelanden kan sändas okrypterade mellan postservrarna. Genom att avlyssna internettrafiken kommer man då också åt innehållet i meddelandena. Det är möjligt att kryptera innehållet i konfidentiella meddelanden samt signera dem elektroniskt. Man ska, emellertid, komma överens om detta med mottagaren separat, eftersom ingen krypteringsmetod för e-postmeddelanden är så allmän att man utan vidare kan anta att mottagaren också använder den. Identifieringsuppgifterna för e-postmeddelandet, såsom mottagarens e-postadress, måste i alla fall sändas krypterade, för att meddelandet ska kunna levereras.

SMTP-protokollet som används vid förmedling av e-postmeddelanden fordrar ingen verifiering av den som sänder ett e-postmeddelande, vilket gör det möjligt att skicka meddelandena i vems namn som helst. E-post är också den största distributionskanalen för skadligt innehåll, t.ex. icke-önskad reklampost och annat skadeprogram. En övervägande del av skräpposten sänds med hjälp av botnät som skapats av enskilda användares datorer som varit föremål för intrång. Man försöker minska problemet med hjälp av program avsedda för filtrering av skräppost.

## Botnät har fortfarande stor betydelse

Under de senaste åren har diverse botnät befest sin ställning som ett viktigt redskap vid alla brott mot informationssäkerheten. Också dataintrång i servrar görs numera nästan enbart i avsikt att utvidga botnät, och inte för att komma åt eventuell information i serverna.

Sökmaskiner samlar uppgifter om sårbara servrar, som man försöker utnyttja för att sprida skadeprogram.

Användarna lockas till angripna webbplatser, som installerar skadeprogram i deras datorer. Skadeprogrammet tar sedan kontakt med den server som styr ifrågavarande botnät. De datorer som anslutits till ett botnät kan från den administrerande servern få ett kommando att samla och leverera information från datorn, sprida skadeprogram till nya servrar, sända skräppost eller starta blockeringsattacker mot önskade mål. Skadeprogrammen kan också spionera och till utomstående vidarebefordra information som sparats i datorn eller som matats in under en webbsession.

Nya versioner av skadeprogrammen sprids kontinuerligt, för att hindra antivirusprogrammet från att upptäcka dem. Skadeprogrammen kan också uppdatera sig automatiskt.

### **Mängden skräppost sjönk tillfälligt**

Serverhotel som ställer sig välvilliga eller likgiltiga till verksamheten, domännamn som registreras för brottsligt ändamål och samtrafikavtal operatörerna emellan är viktiga faktorer för avvärjning av IT-brottslighet. Botnät som skapats via användarnas angripna dator är också betydelsefulla. För att utvidga näten försöker man sprida skadeprogram till allt flera användares datorer.

Serverhotel som fokuserar på att distribuera skadligt material och nätoperatörer som erbjuder dem telekommunikationsförbindelser har visat sig vara viktiga faktorer. De här tjänsteleverantörerna kallas ibland "bullet-

proof hosting" eller "anti-abuse-resistant hosting".

*InterCage* som i september hade förlorat sin nätförbindelse fick i medlet av november sällskap av en annan tjänsteleverantör, *McColo*, från San Jose i Kalifornien. Avstängningen föregicks av artiklar skrivna av informationssäkerhetsforskare och media, om skadlig trafik som upptäckts i dessa tjänsteleverantörers nät. Bland McColos webbadresser hade man funnit kommandoservrar för flera botnät specialiserade på att sprida skräppost. Följden av att tjänsteleverantörens internetförbindelser bröts var ändå förvånande: enligt olika uppskattningar minskade den totala mängden skräppost i internet med ungefär hälften.

På ett par månader återgick mängden skräppost ungefär till den tidigare nivån. Det finns fortfarande flera hosting-tjänsteleverantörer i olika delar av världen som koncentrerar sig på skadliga tjänster eller accepterar dem.

Än så länge har man inte i Finland upptäckt tjänsteleverantörer som systematiskt skulle gynna skadliga tjänster. CERT-FI och de finländska internettjänsteleverantörerna har ett gott samarbete. De informationssäkerhetskränkningar som upptäckts i de finländska företags nät, som erbjuder hosting-tjänster, beror oftast på försummelse att uppdatera programvara och andra enstaka informationssäkerhetsbrister i webbtjänsterna.

### **Missbruk avsikten då domännamn registreras med förfalskade uppgifter**

Domännamn som registrerats med förfalskade uppgifter används allmänt för att sprida skadeprogram och för phishing. Identiteten hos den som registrerar ett domännamn eller kontaktuppgifternas riktighet kontrolleras sällan.

Skadeprogrammen innehåller ofta på förhand programmerade domännamn, med hjälp av vilka de senare försöker kontakta sin kommandoserver. Programmen kan också kontakta domännamn, som förefaller att vara

sporadiska, och som t.ex. har bildats på basis av datum och klockslag. Detta gör det svårare att avvärja kommandoservern, emedan den adress skadeprogrammet använder kan ändra dagligen och man eventuellt inte vet hur den är genererad.

Dylika domännamn har inte registrerats i Finland, utan skadeprogrammen har använt internationella domännamn. Enligt flera undersökningar är fi-domännamnet det tryggaste i världen.

### **Man ingriper ofta långsamt i missbruk**

Hittills har man ingripit rätt slumpmässigt och oorganiserat i "bullet-proof hosting"-tjänsteleverantörernas verksamhet. Anledningen till att internettjänsteleverantörerna ingriper i verksamheten är kommersiell, ty kunder som är involverade i verksamhet som förefaller brottslig kan försvåra operatörens verksamhet och skada dess rykte. Då Intercage och McColo kopplades från nätet tycks myndigheternas roll ha varit obetydlig. Eftersom avvärjningen av brott mot informationsnät är uppenbart ineffektiv har informationssäkerhetsforskare publicerat rapporter om skadlig trafik i ifrågavarande tjänsteleverantörers nät. Detta ser ut att ha drivit operatörerna av internettjänstförbindelser att bryta kontrakten med Intercage och McColo. Om man önskar få bort en enskild aktör från nätet är de stora teleoperatörerna med sina servicekontrakt i nyckelposition. En dylik handlingsmodell närmar sig emellertid någon form av att "ta rätten i egna händer".

ICANN, International Corporation for Assigned Names and Numbers, och europeiska RIPE, som administrerar IP-adresser har reagerat på några fall av missbruk. ICANN återkallade domännamnleverantören *Estdomains* rätt att registrera domännamn. De domännamn som registrerats av företaget har överförts till en annan tjänsteleverantör. RIPE har för sin del återkallat de IP-adresser som den illa ansedda tjänsteleverantören *Russian Business Network* har beviljat.

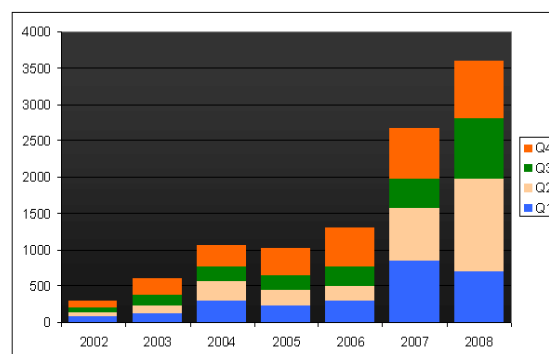
ICANN och RIPE grundar sina avgöranden på avtalsbrott som hör ihop med tekniska nätverksresurser. Men det räcker inte för att hålla vederbörande straffrättsligt ansvariga. Förutom aktiv övervakning av internettjänsteleverantörerna och CERT-aktörerna finns det behov av en avsevärd effektivisering inom det internationella polissamarbetet för att de kriminella organisationernas mångfasetterade verksamheten i datanäten på internationell nivå ska kunna påverkas effektivt.

### **Brist på IP-adresser, en stor utmaning väntar**

En övervägande del av internettrafiken baserar sig fortfarande på IP-protokoll v4, fastän versionen endast definierar en begränsad mängd IP-adresser. Trots de åtgärder som vidtagits för att kringgå problemet, t.ex. konvertering av adresser (NAT = Network Address Translator), håller IP-adresserna på att ta slut. För tillfället uppskattar man att adresserna räcker till ännu några år.

IP-protokoll v6 definierar en mycket större adressrymd och är planerad att ersätta nuvarande version. Protokollet används redan i någon mån, främst i experimentsyfte, men dess andel av trafiken på internet är försvinnande liten.

Ibruktagnandet av IPv6 blir ett utdraget projekt, som antagligen kommer att påverka alla datorer och nätverkskomponenter kopplade till internet. En del av komponenterna kan bli oanvändbara, och för största delen blir det åtminstone nödvändigt med en programuppdatering. Övergångstiden blir säkert också lång.



Jämfört med föregående år ökade antalet fall som CERT-FI behandlade.

Än så länge finns det inte mycket erfarenheter av IPv6-användning i större skala. Man kan anta att nya funktionella och informationssäkerhetsrelaterade brister upptäcks i själva protokollet och i planeringen av lösningar som baserar sig därpå.

Trots den lilla andelen IPv6-användare fick CERT-FI år 2008 kännedom om det första skadeprogram som utnyttjade IPv6-protokollet i Finland.

### **Skadliga program sprids via angripna webbsidor**

Spridning av skadliga program innebär ofta att skadeprogrammen utnyttjar sökmaskiner för att hitta t.ex. sårbarheter av typen SQL-injektion, som gör det möjligt att bearbeta webbplatsens innehåll. Då en sårbar server hittas fogas en liten JavaScript-hänvisning dess www-sidor, med avsikt att erbjuda dem som besöker sidorna att ladda ner ett skadeprogram. Den händer lätt att den som upprätthåller webbplatsen inte upptäcker den extra länk som fogats till www-sidorna.

Nya sårbarheter upptäcks hela tiden i de publikationssystem som allmänt används för att underhålla webbsidor. De gör det möjligt att foga en kod till sidorna. Därför är det viktigt att se till att anti-virusprogrammen är uppdaterade i såväl publikationssystem som därtill hörande stödprogram.

Sårbarheter i mjukvara används nödvändigtvis inte för att infektera användarens dator. Ett skadeprogram kan maskeras t.ex. som ett program som behövs för att titta på videofiler eller t.o.m. som ett nyttoprogram. Dessa program påstås fungera för avlägsnande av spionprogram, som brandvägg eller antivirusprogram. Användaren lockas att installera ett dylikt program i sin dator. I vissa fall händer det att användaren t.o.m. köper och betalar för att mjukvaran installeras. Ett skadeprogram följer ofta också med installationspaket för olovliga programkopior eller därtill hörande mjukvara för generering av olovliga licensnycklar.

Förutom via webbsidor och e-postmeddelanden spreds länkar till skadeprogram också via Instant Messaging system.

### ***En mask sprids vid årsskiftet***

Ett skadeprogram som sprider sig självständigt upptäcktes i lokalnätet i slutet av året. Programmet har infekterat datorer både i finländska och utländska nät. Maskens avsikt är att sprida sig mellan datorer på flera olika sätt. Efter att masken har infekterat en dator försöker den ta kontakt med adresser, som förefaller sporadiska, för att uppdatera sig. Dessa nätadresser bildas på basis av datum och klockslag.

### ***Bluffsidor och e-postmeddelanden har egentligen inte stört finländska användare***

De bluffsidor som har kopierat finländska elektroniska tjänster och som påträffades under året var inte särskilt trovärdiga. Största delen av de egentliga bluffsidorna förefaller att ha varit riktade mot kunder av internationella tjänster. Flera bluffsidor som har kopierat internationella tjänster har påträffats i angripna finländska webbservrar.

På vårvintern spreds e-postmeddelanden innehållande en länk via vilken datorn kunde smittas av ett skadligt program. Avsikten var att försöka kapa användarens nätbankförbindelser. Det här meddelandet om "en kärnkraftsolycka i S:t Michel" eller "Tatjana som söker sällskap" lockade många att installera ett skadeprogram i sin dator. Samma meddelande och skadeprogram spreds i många andra europeiska länder också.

### ***Aktivismen på nätet låg nere***

Under året riktades inga betydande blockeringsattacker mot finländska tjänster och inga webbplatser förvanskades. Finland var värd för OSSE-konferensen (Organisationen för säkerhet och samarbete i Europa). Inga informationssäkerhetsincidenter rapporterades.

I samband med konflikten i Georgien angreps en del lokala www-servrar och propagandamaterial matades in på webbsidorna.

## Framtidsutsikter

Enligt CERT-FI är spridningen av sådant skadeprogram till datorerna, som kan fjärradministreras och uppdateras, ett betydande hot mot informationssäkerheten.

Skadeprogrammen blir allt mer mångsidiga. När en dator en gång har infekterats kan den användas för flera typer av skadligt ändamål bara genom att uppdatera skadeprogrammets egenskaper.

Metoderna att sprida skadeprogram utvecklas hela tiden. Angripna webbsidor och lockande e-postmeddelanden kommer också i fortstättningen att utnyttjas. Omfattande kampanjer och distribution till mera avgränsade grupper kommer att användas för att infektera datorer.

Kontakter till CERT-FI	1-3/2008	4-6/2008	7-9/2008	10-12/2008	2008	2007	Förändring
Intervju	17	29	21	21	88	80	+10%
Sårbarhet eller hot	39	232	52	71	375	64	+485%
Skadligt program	460	727	532	437	2156	1678	+28%
Rådgivning	64	87	92	116	359	393	-9%
Beredning av attack	32	27	12	16	87	3	+2800%
Dataintrång	14	88	45	40	187	119	+57%
Blockeringsattack	15	26	31	24	96	64	+50%
Övriga informationssäkerhetsproblem	10	11	12	10	43	48	-10%
Social ingenjörskonst	47	36	44	62	189	197	-4%
Skräppost (ingen statistik 2008-)	-	-	-	-	-	18	-
<b>Totalt</b>	<b>698</b>	<b>1263</b>	<b>841</b>	<b>797</b>	<b>3580</b>	<b>2664</b>	<b>+34%</b>

Majoriteten av de fall CERT-FI har behandlat gällde olika skadeprogram och hot mot informationssäkerheten förorsakade av dem. Rapporterna om skadeprogram utgjorde redan två tredjedelar av alla kontakter.