



## CERT-FI ÅRSRAPPORT 2004

Typiskt för hot mot informationssäkerhet år 2004 var i synnerhet strävan efter ekonomisk nytta och mera professionell skadlig verksamhet, vilket medförde väldigt stora utmaningar för skydd mot informationssäkerhetshot. De mest uppenbara exemplen var problem som orsakades av skadliga bot-program vilka hade samband med utpressning och dataintrång mot internationella online-aktörer, såsom företag som utövar vadslagning på nätet.

En annan betydelsefull trend var ett ökat utnyttjande av sårbarheterna redan innan en programfix hade kommit ut. Samma trend kommer antagligen att fortsätta. Under det sista kvartalet utnyttjades sårbarheterna i Microsoft Internet Explorer –webbläsaren samt i programmeringsspråket PHP i avsevärd grad. Under det sista kvartalet offentliggjordes också Cabir-programmets källkod som var riktad mot mobiltelefoner. Hot mot mobiltelefoner genom skadliga program kommer förmodligen att öka under det löpande året.

Internationellt, dock inte i Finland, var ett av de största fenomenen sk. phishing, vilket syftar till att från Internetanvändare samla in känslig information för ekonomiskt utnyttjande.

### Skadliga program

I början av 2004 blev virusstatistik dystrare på grund av e-postmaskar som var delaktiga i ett sk. viruskrig. Det utkom flera variationer av Bagle-, Mydoom- och Netsky-virusar, vilka sökte infektera deras målsystem och ofta också eliminera andra skadliga program från systemet. De som skapar skadliga program sände meddelanden till varandra genom skadliga programkoder. Konkurrensen om sändningskanaler för spam ledde till ett viruskrig mellan dem som skapar skadliga program och dem som sänder spam.

Witty-nätverksmask började sprida sig vid slutet av mars. Masken utnyttjade en sårbarhet som upptäcktes i ISS:s säkerhetsprodukter bara en dag efter det att sårbarheten offentliggjordes. Masken spred sig snabbt över ett geografiskt omfattande område, även om ISS:s programvaror inte hör till de mest använda. För första gången spreds masken genom en befarad teknik, sk. mallista. Mållistan innehåller på förhand eftersökta sårbara system vilka masken infekterar för att få maximal spridningstighet i begynnelsekedet.

I maj började Sasser-nätverksmask sprida sig i omfattande grad och den orsakade stora problem även hos finländska företag och andra organisationer. Sasser utnyttjade en LSASS-sårbarhet i Windows-operativsystemet som hade publicerats två veckor tidigare. De flesta av de Sasser-epidemier som upptäcktes på organisationerna var en följd av att en infekterad bärbar dator hade kopplats till det interna nätet.

Hela året 2004 präglades kraftigt av sk. bot-program med flera tusen olika variationer. De mest beaktansvärda skadliga bot-programmen var Sdbot och Phabot jämte varianterna. Bot-egenskaperna blev väldigt mångsidiga under året. Ett infekterat datasystem omformades till ett bot-nätverk med flera tusen datasystem vilket angriparen kontrollerade genom en IRC-kanal. Bot-programmen spred sig så effektivt delvis därför att de som skapade programmen ville säkerställa att antivirusprogramvarorna inte kan identifiera en ny aktiv variant. Bot-programmen började utnyttja en sårbarhet mycket snabbt efter att sårbarheten hade publicerats. De nya varianterna kom ut så snabbt att det orsakade stora utmaningar för den traditionella antivirusprogramvarans förmåga att upptäcka sådana.



## Spam

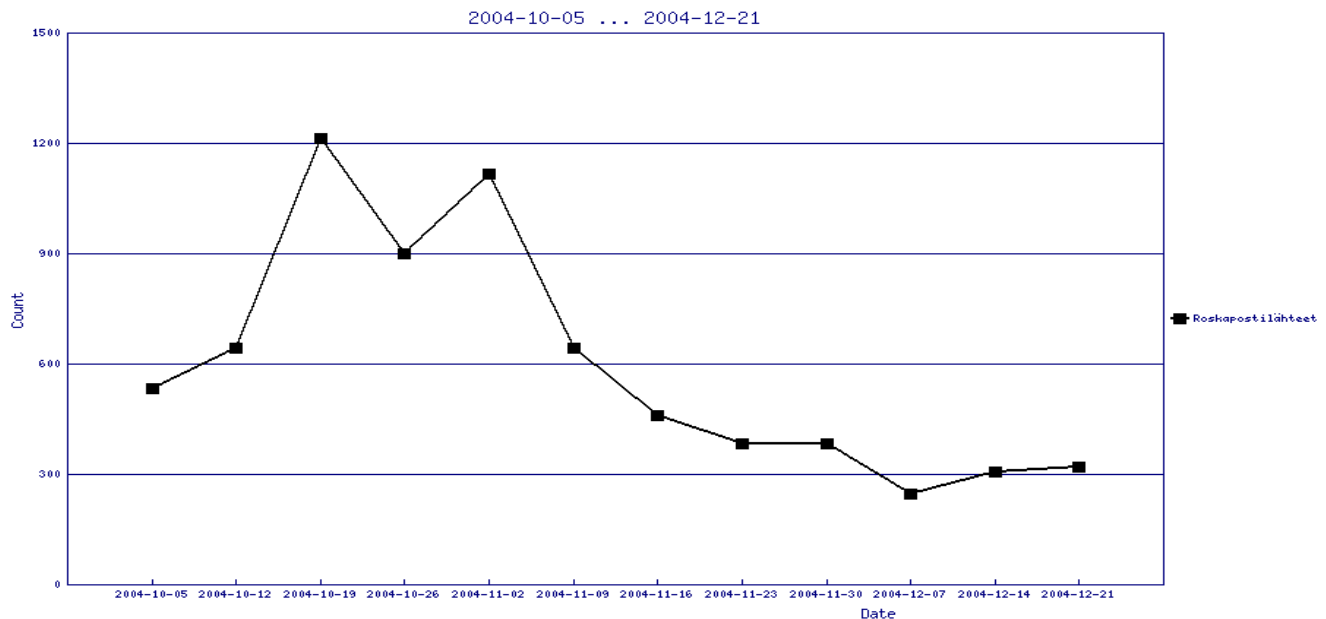
Skräppost ökade vidare till antalet under 2004, vilket orsakade högre belastning på tjänsteleverantörers, företags och andra organisationers e-postserver. Enligt CERT-FI:s observationer var det relativa antalet spam cirka 38 procent av alla e-postmeddelanden i Finland i slutet av året. För individuella spam uppgick det relativa antalet dock ibland rentav till 80 procent av alla e-postmeddelanden. Antal spam varierade dock i hög grad mellan olika målorganisationer. Också observationstidpunkten hade en stor inverkan på det relativa antalet, eftersom spam sänds ofta i skurar.

Internationella jämförelser visar att det relativa antalet spam annanstans i världen har varit cirka 40 – 60 procent av alla e-postmeddelanden med trafiktopp nästan 90 procent.

## Antal problemdatasystem i Finland

Enligt CERT-FI:s uppgifter varierade antalet datasystem som drabbats av skadliga bot-program för olika observationsperioder mellan 500 och 2 000 infekterade datasystem. Under årets sista kvartal fanns det i Finland färre bot-infekterade datasystem än tidigare, antalet var under 500.

Enligt de uppgifter som CERT-FI har fått uppskattades antal datasystem som fungerade som spamkällor vara i genomsnitt 500 per observationsperiod. Källorna uppgick som störst till cirka 1 000. Under det sista kvartalet minskade antalet klart. Då utfärdade Kommunikationsverket för teleföretagen en föreskrift om e-posttjänsternas informationssäkerhet och funktionsduglighet.



Figur 1. Datasystem som fungerade som källor för spam under det sista kvartalet 2004.



## De mest utnyttjade sårbarheterna

De mest utnyttjade sårbarheterna under 2004 var LSASS i Microsoft Windows operativsystemet samt flera sårbarheter i Internet Explorer. Windows LSASS utnyttjades i synnerhet genom olika skadliga program. Under det sista kvartalet utnyttjades särskilt sårbarheter i Internet Explorers IFRAME-element och HTML Help. IFRAME utnyttjades genom intrång i en server som delade ut reklambanners till flera populära webbplatser. En programkod som nyttjade sårbarheten inkluderades i banners.

Särskilt många attacker riktades mot SSH-tjänsten med avsikt att få fram användaridentifikation och lösenord för målsystemet. Attacken var inte riktad mot den egentliga sårbarheten i programvaran.

CERT-FI fick veta om flera betydelsefulla serier av dataintrång. De verktyg som användes vid intrång, t.ex. metoder vilka möjliggör passering av programbrandväggar, blev allt effektivare och allt svårare att upptäcka. Under det sista kvartalet dök det fram många metoder som fungerar i datasystem vilka är försedda med Microsoft Windows XP Service Pack 2.

Viktigt under det sista kvartalet var utnyttjandet av WINS-sårbarheten i Microsoft Windows operativsystemet och sårbarheter i programmeringsspråket PHP. Klart ökat utnyttjande av WINS konstaterades i början av december och i slutet av året. Utnyttjandet av sårbarheterna i PHP riktades i synnerhet mot sårbara phpBB-programvaror.

## Framtidsutsikter

Utvecklingen av skadliga bot-program kommer antagligen att fortsätta under det följande kvartalet. Angriparna försöker skydda bot-nätverkets kommandokanaler på ett mer aggressivt sätt: blockeringsattacker t.ex. riktas mot utomstående aktörer som försöker komma in på kommandokanalen.

Skadliga program mot mobiltelefoner utvecklas från dagens "Proof of Concept"-nivå. I framtiden kan det också förekomma attacker mot intelligenta telefoner med syfte att få ekonomisk nytta.

Phishing och strävan efter att få ekonomisk nytta ökar under det löpande året. Händelser som t.ex. naturkatastrofen i Asien vilka upprör hela världen, ger angriparna ett tillfälle att bluffa pengar från människor t.ex. så att de på www-sidorna presenterar sig som hjälporganisationer.

Organisationernas beredskapsåtgärder för hot mot Internet, såsom blockeringsattacker, kommer att framhåvas. Beredskapsåtgärderna kräver allt mera aktiva åtgärder och övning av olika situationer. Betydelsen av IRT-grupperna (Incident Response Team) förstärks.

Sårbarheterna utnyttjas i framtiden allt oftare redan innan programfix släpps. Informationssäkerhets-hot mot datanät riktas allt oftare till hemdatasystem. Användningen av en brandvägg, en trygg webb-läsare och ett uppdaterat antivirusprogram samt uppdatering av programvaror, trygga inställningar och riktiga behörigheter spelar en stor roll i hemdatasystem också i fortsättningen. Windows XP Service Pack 2 torde minska lyckade utnyttjanden av sårbarheter via nätet, såsom i fallen LSASS och RPC.