# Pressmeddelande

**Kontaktuppgifter:**

USA: Marissa Vicario
Symantec Corp.
+1 646 519 8116
mvicario@messagelabs.com

EMEA: Paul Wood
Symantec
+ 44 (0) 1452 627705
pwood@messagelabs.com

APAC: Andrew Antal
Symantec
+61 2 908 68239
aantal@messagelabs.com

**Symantec publicerar idag den årliga säkerhetsrapporten MessageLabs Intelligence 2010 Annual Security Report:**

*Botnäten visar sig vara motståndskraftiga och fortsätter att skapa problem under ännu ett år; sabotageprogram som skickas via e-brev ökar hundrafalt.*

**STOCKHOLM, Sverige – 13 december 2010 –** Symantec Corp. (Nasdaq: SYMC) publicerar idag sin årliga säkerhetsrapport *MessageLabs Intelligence 2010 Security Report.* Rapporten visar i detalj hur cyberkriminella har diversifierat sina attackmetoder för att fortsätta att distribuera stora mängder skräppost och sabotageprogram under hela 2010.

Rapporten visar att det förekommit variationer i skräppostnivåerna under året på grund av skiftningar i botnätsaktiviteten. Skräppostmängden hade sin topp under augusti månad 2010 med 92,2 procent när botnätet Rustock aggressivt förstärktes med nya varianter av sabotageprogram som snabbt aktiverades. Detta föranledde en allmän ökning av skräppostaktiviteten för helåret, med en genomsnittlig spamnivå på 89,1 procent, vilket är en ökning med 1,4 procent jämfört med 2009. Under huvuddelen av 2010 stod botnäten för 88,2 procent av allt skräppostutskick. I slutet av 2010 minskade mängden skräppost som kom från botnät till 77 procent av skräppostutskicken, tack vare stängningen av skräppostfilialen Spamit i början av oktober 2010. I slutet av 2010 så var det totala antalet aktiva botnät återigen ungefär samma som i slutet av 2009, med en ökning på cirka 6 procent under andra halvan av 2010. Det totala antalet botnät i världen är mellan 3,5 och 5,4 miljoner.

Under 2011 förutspår man att botnätsansvariga kommer att ta till steganografitekniker för att kontrollera sina datorer. Detta innebär att de kommer att dölja sina kommandon fullt synligt, kanske i bild- eller musikfiler som distribueras via fildelning eller webbplatser för socialt nätverkande. Tack vare denna metod kan de kriminella utfärda instruktioner till sina botnät i smyg, utan att behöva vara beroende av en internetleverantör som fungerar som värd för deras infrastruktur och därmed minimerar de riskerna för att bli upptäckta.

Även om antalet botnät och mängden material som distribuerats från dem har varierat under 2010 så är de tre största botnäten fortfarande desamma under den andra hälften av 2010. Rustock är alltjämnt det mest dominerande botnätet: skräppostutskicket från detta nät mer än fördubblades jämfört med föregående år till

mer än 44 miljarder spammeddelanden per dag och mer än en miljon kontrollerade datorer i nätet medan Grum är det näst största botnätet och Cutwail det tredje största. De ansvariga bakom Cutwail och Grum har även orsakat en ökning av mängden sabotageprogram som skickas ut i skräppost från botnät.

"Med framgångsrika och motståndskraftiga botnätsfunktioner från tidigare år som grund, har de cyberkriminella experimenterat med många metoder för att hålla skräppostkampanjerna aktiva och effektiva under detta år", säger Paul Wood, chefsanalytiker på MessageLabs Intelligence, Symantec Hosted Services. "Spammarna utnyttjade en mängd olika knep för att komma förbi skräppostfilter och lura potentiella offer, med allt från att dra maximal nytta av evenemang med stort nyhetsvärde, som fotbolls-VM, till att dra fördel av de allt mer populära tjänsterna för webbadressförkortning och de sociala nätverken".

Ett anmärkningsvärt säkerhetshot under detta år var viruset "Here You Have". Den 9 september 2010 använde man den gamla tekniken massmejl för att skicka ut skadlig kod och man nådde en topp på 2 000 blockerade e-brev per minut. Totalt blockerade MessageLabs AntiVirus-tjänst mer än 100 000 kopior av viruset innan det nådde ut till några klientnätverk. Den heuristiska regel som gjorde att viruset kunde upptäckas lades till i maj 2008, alltså mer än två år tidigare. Samma regel var återigen nyckeln till att kunna stoppa en serie attacker med förfalskad e-post från den nordamerikanska federala skattemyndigheten IRS i början av november.

Under 2010 identifierades över 339 600 olika hot i form av skadeprogram i skadliga e-brev som blockerats vilket innebar en hundrafaldig ökning jämfört med 2009. Denna enorma ökning beror till största delen på det växande antalet polymorfiska sabotageprogramsvarianter som normalt skapas från verktygsuppsättningar som gör det möjligt att generera en ny version av koden på ett snabbt och enkelt sätt. Ett exempel på en sådan variant är Bredolab-familjen av trojaner, ett botnät för allmänt syfte som vanligtvis distribueras via botnätet Cutwail. Denna stod för cirka 7,4 procent av alla sabotageprogram som skickades ut via e-post under 2010. Bredolab är en form av attackmetod som kallas PPI (*Pay Per Install*), det vill säga "betala per installation". Även om sabotageprogrammet är flexibelt till sin natur så är det utformat för att ta kontroll över offrets dator så att den kan användas av Bredolab-operatörerna eller hyras ut eller säljas till en annan angripare. Bredolab är ett exempel på ett sabotageprogram som ligger i en komprimerad fil och som över tiden har det gått från att vara en enkel typ av ett krypterat sabotageprogram packat med polymorfiska koder till att bli en skyddad version med en uppdaterad polymorfisk motor som är utformad för att uppträda på samma sätt men ändå undgå att identifieras som Bredolab. Den slutgiltiga versionen är en aggressiv polymorfisk packare som lanserades i slutet av 2010 och som massmejlades ut med hundratals varianter för att maximera spridningen.

Medan Bredolab skickades ut i enorma mängder så ökade också de riktade attackerna, som kännetecknas av distribution i små volymer. När de riktade attackerna, eller de avancerade ihålliga attackerna, först dök upp för fem år sedan så spårade MessageLabs Intelligence en eller två attacker per vecka. Under nästkommande år ökade detta antal till mellan en och två attacker per dag. Därefter ökade de riktade attackerna från 10 per dag

till ungefär 60 per dag under 2010 och i slutet av året blockerade MessageLabs Intelligence 77 riktade attacker varje dag.

"Samtidigt som de riktade attackerna ökar i antal så blir även utförandemetoderna flera och attackerna allt mer komplexa", säger Wood. "Normalt utförs riktade attacker mot mellan 200-300 organisationer per månad men industrisektorn varierar och normalt riktar angriparna in sig på personer med högre befattningar, även om det ofta sker via en allmän eller en assistents e-postbrevlåda. För fem år sedan var målet för attackerna oftast stora och välkända företag men idag har gruppen av attackerade företag blivit mycket större och i dagsläget går inget företag säkert, då alla kan utsättas för attacker".

Slutligen undersökte MessageLabs Intelligence surfningsbeteendet hos anställda som är alltmer flexibla, det vill säga, de reser mycket/jobbar ute på fältet eller så arbetar de hemifrån. Dessa jämfördes med personal som jobbar från kontoret. Resultat från undersökningen visar att mobila användare har ett liknande beteende som de som arbetar från kontoret och utgör därför inte något större hot mot företaget än de sistnämna. Däremot verkar anställda som arbetar från olika platser, både på och utanför kontoret, ha ett mer avslappnat surfningsbeteende när de arbetar utanför kontoret vilket gör dem till en större säkerhetsrisk för företaget. Resultatet visar att företag måste avgöra i vilken utsträckning de vill kontrollera sina medarbetares onlinebeteende med hjälp av webbpolicykontroller. Företagen inser att det finns ett behov av en mer flexibel tillgång till webben vilket gör att de under 2010 väljer ett mer förfinat tillvägagångssätt för att styra tillgången, med en ökad användning av "listor över tillåtna webbplatser" som ersätter den mer generella och omfattande metoden med "svartlistning" från tidigare år. Antalet riktlinjer som beviljats har ökat med i genomsnitt 0,8 procent per månad under 2010, jämfört med 0,6 procent per månad under 2009.

**De största trenderna 2010**

**Webbsäkerhet:** Under 2010 steg det genomsnittliga antalet webbplatser med skadlig kod som blockerades varje dag från 3 066 stycken jämfört med 2 465 stycken per dag under 2009, vilket är en ökning med 24,3 procent. MessageLabs Intelligence identifierade skadliga webbhot på 42 926 olika domäner, majoriteten av dessa var komprometterade, lagliga domäner.

**Spam/skräppost:** Under 2010 var den årliga, genomsnittliga, globala spammängden 89,1 procent, vilket är en ökning med 1,4 procent jämfört med 2009. I augusti nådde den globala mängden av skräppost sin topp med 92,2 procent i och med att skräppostutskicket från botnät ökade till 95 procent när en ny variant av botnätet Rustock spreds och snabbt började användas.

**Virus:** Under 2010 fanns det i genomsnitt ett sabotageprogram i vart 284,2:e-brev (0,352 procent), vilket nästan är samma snitt som under 2009 med 1 program i vart 286,4 e-brev (0,349 procent). Under 2010 blockerades över 115,6 miljoner e-brev av Skeptic™, vilket är en ökning med 58,1 procent jämfört med 2009.

Man identifierade 339 673 olika sabotageprogramsvarianter i de skadliga e-brev som blockerades. Resultatet är mer än en hundrafaldig ökning sedan 2009 som beror på det växande antalet polymorfiska varianter av sabotageprogram.

**Phishing/nätfiske:** Under 2010 var det genomsnittliga förhållandet för e-posttrafik som blockerades 1 på 444,5 (0,23 procent), jämfört med 1 på 325,2 (0,31 procent) under 2009. Cirka 95,1 miljarder nätfiskemeddelanden beräknades vara i cirkulation under 2010.

Den årliga rapporten från MessageLabs Intelligence Report innehåller mer detaljerad information om alla trender och siffror som nämns ovan, samt mer ingående information om trender för 2010. Den fullständiga rapporten finns på: http://www.messagelabs.com/intelligence.aspx

**Om Symantec**

Symantec är världsledande i att tillhandahålla lösningar för säkerhet, lagring och systemhantering. Symantec hjälper privatpersoner och företag att säkra och hantera sin information. Vår mjukvara och våra tjänster skyddar mer heltäckande och effektivt mot fler risker på fler områden, vilket inger trygghet överallt där information används eller lagras. Mer information finns på http://www.symantec.se.

###

**NOTE TO EDITORS:** If you would like additional information on Symantec Corporation and its products, please visit the Symantec News Room at http://www.symantec.com/news. All prices noted are in U.S. dollars and are valid only in the United States.



FORWARD-LOOKING STATEMENTS: Any forward-looking indication of plans for products is preliminary and all future release dates are tentative and are subject to change. Any future release of the product or planned modifications to product capability, functionality, or feature are subject to ongoing evaluation by Symantec, and may or may not be implemented and should not be considered firm commitments by Symantec and should not be relied upon in making purchasing decisions.