Pressmeddelande

KONTAKTER:

U.S.: 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 MessageLabs rapport om internetsäkerhet – april 2010:

Rustock slår Cutwail som det största och mest aktiva botnätet, Lovebug-viruset fyller 10 år

MOUNTAIN VIEW, Kalifornien – 27 April, 2010 – Symantec Corp. (Nasdaq: SYMC) publicerar idag sin rapport om säkerhetshot på webben under april månad. Analysen visar att Rustock har överträffat Cutwail och är nu det största botnätet både vad gäller mängden spam det skickar och antalet aktiva bottar det har under sin kontroll. Rustock har minskat effekten av enskilda bottar med 65 procent men samtidigt kompenserat detta genom att ökat antalet aktiva bottar med 300 procent. Samtidigt har Cutwail minskat i storlek med 600 000 bottar från 2 miljoner bottar i maj 2009 och står nu för endast 4 procent av all skräppost. Rustock är fortfarande den största sändaren av skräppost och står för 32,8 procent av all spam.

"Cutwail förlorade sannolikt förmågan att uppdatera en del av sina bottar i och med stängningen av ISP Real Host i augusti 2009 vilket har lett till en kraftig minskning av spam och en oförmåga att återhämta sig, säger Paul Wood, senioranalytiker på MessageLabs Intelligence inom Symantec Hosted Services. "Som en följd av detta har Rustock tagit över betydande volymer från spammare genom att med större kapacitet och lägre driftskostnader kunna lägga sig under marknadspriserna."

Grum och Mega-D är efter Rustock de andra och tredje största botnäten och står för 23,9 procent respektive 17,7 procent av all spam. Som en följd av försöken att stänga ner ISP har Mega-D färre bottar än både Rustock och Grum. Det är däremot det hårdast arbetande botnätet och pressar sina 240 000 aktiva bottar att skicka ut 430 spammail per minut. Grum har varit konsekvent under de senaste fem månaderna då varje bot skickat mellan 145 och 150 spammail per minut. Grum har däremot nyligen ökat antalet bottar som den förfogar över från 700 000 till 1 miljon, vilket gör den till det näst största botnätet.

I april analyserade MessageLabs rapport om internetsäkerhet även passive fingerprinting (PF), signering av skräpposttrafik, för att skaffa sig en bild av vilka operativsystem som körs på infekterade och spamsändande datorer. Många av de infekterade datorerna använder Windows och andelen spam med en PF signatur var ungefär lika stor som den andel av marknaden som Windows operativsystem har.

Symantec MessageLabs rapport om internetsäkerhet april 2010

"Spam har oftare skickats från datorer som använder Windows än från dem som använder andra operativsystem." säger Wood. "Men spam som inte identifierats att de skickats från botnät sågs mer sällan komma från Windows datorer än från kända botnät."

Ett spamindex visar sannolikheten för att en viss dator skickar skräppost och beräknas genom att jämföra förhållandet mellan spam från ett visst operativsystem och dess marknadsandel. I det nuvarande spamklimatet visar detta index att i förhållande till sin marknadsandel löper en Linuxdator fem gånger större risk att skicka spam än en Windowsdator. Men Linuxdatorer svarar för endast 5,1 procent av all skräppost. På grund av sin lägre marknadsandel finns det färre exempel på skadlig kod i omlopp som särskilt drabbar operativsystemet Linux. Fler ISP:s tvingar nu sina kunder att skicka sin e-posttrafik genom ISP:ns egna e-postserver ”smarthost", som möjliggör för dem att skicka e-post direkt via TCP-port 25. Många använder en hostad miljö där utvecklingskostnaderna kan sänkas genom användning av öppen källkod såsom Linux.

Slutligen är MacOS minst sannolik att skicka skräppost, baserat på både sitt globala bidrag till spam och enskilda datorer. Spamindex visar att nästan ingen skräppost skickats från MacOS datorer, men ca 0,001% av den undersökta skräpposten har detta ursprung.

Den 4 maj var det tio år sedan Symantec Hosted Services, dåvarande MessageLabs, stoppade och namngav ”Lovebug”-viruset, ett elakartad och massutskickat virus som förstörde för uppskattningsvis 45 miljoner e-post-användare och orsakade skador för miljarder dollar på en enda dag. Symantec Hosted Services var först med att fånga upp och namnge viruset och fann 13 000 kopior av viruset under loppet av en dag, vilket vid den tiden var ett enormt antal kopior.

Idag är det vanligt att MessageLabs Intellegence stoppar 1,5 miljoner skadliga e-postmeddelanden varje dag. Även om massutskickade virus såsom Lovebug är sällsynta, har cyberbrottslingar utvecklat sin teknik till mer skadliga, välriktade attacker och motiveras idag mer av ekonomisk vinning och identitetsstöld än av prestige. Den 4 maj 2000 innehöll 1 av 28 e-mail Lovebug-viruset. Som jämförelse innehöll under toppen av april i år 1 av 287,2 e-post ett virus. MessageLabs Intellegence fann totalt 36 208 unika släkten av virus i april i år.

När ”copycat-virus” dök upp under dagarna och månaderna som följde 4 maj 2000 hade MessageLabs molnbaserade antivirusverktyg, Skeptic ™, lärt sig av virusets kod och kunde därför granska koden hos nya virus och sätta allt misstänkt i karantän.

"Lovebug var verksam i kölvattnet av Melissa-viruset, ett lika destruktivt virus från föregående år" säger Wood. "Användarna var då mindre kunniga om farorna med misstänkta e-postbilagor och e-post från okända avsändare. Allmänheten var också mindre medveten om frågor som spam och DOS-attacker."

Symantec MessageLabs rapport om internetsäkerhet april 2010

Fler fakta som framkom i rapporten:

Spam/skräppost: I april 2010 uppgick andelen spam från nya och tidigare okända skadliga källor/avsändare till 89,9 procent (ett av 1,11 e-mail) en nedgång med 0,8 procentenheter sedan mars.

Virus: Den globala andelen e-postburna virus från nya och tidigare ej kända skadliga källor/avsändare var 1 av 340,7 e-mail (0,294 procent) i april, en ökning med 0,01 procentenheter sedan mars. I april innehöll 28,9 procent av alla e-postburna hot länkar till skadliga webbsidor, en ökning med 12,1 procentenheter sedan mars.

Phishing/nätfiske: I april utgjorde 1 av 455,2 e-mail (0,219 procent) försök till nätfiske vilket är en ökning med 0,03 procentenheter sedan mars. Sett som en del av alla e-postburna hot som virus och trojaner har andelen phishing-mail ökat med 5,7 procentenheter till 70,3 procent.

Webbsäkerhet: En analys av aktiviteter inom webbsäkerhet visar att 10,9 procent av alla beslagtagna webbaserade virus var nya i april, en minskning med 4,0 procentenheter sedan mars. MessageLabs Intelligence har också identifierat att i genomsnitt 1 av 675 nya webbplatser om dagen innehåller skadlig kod och andra icke önskade program som spionprogram och adware. Detta är en minskning med 12,7 procent sedan i mars.

Geografiska trender:

- Spamnivåerna i Italien steg till 95,5 procent i april och placerade därmed Italien som den mest spammade landet.
- I USA var 90,2 procent skräppost och i Kanada 88,9 procent. Spamnivåerna i Storbritannien steg till 89,4 procent.
- I Nederländerna stod spam för 91,5 procent av e-posttrafiken, medan spamnivåerna nådde 89,4 procent i Australien och 92,3 procent i Tyskland.
- Spamnivåerna i Hongkong nådde 91,0 procent och i Japan 86,9 procent.
- Virusaktiviteterna i Taiwan var 1 av 76,3 mail, vilket gör att det fortfarande är det land som är mest utsatt för e-postburna virus.
- Andelen virus var i USA 1 av 646,3 och i Kanada 1 av 416,2. I Tyskland var virusnivåerna 1 av 471,0, 1 av 1,120 i Nederländerna, 1 av 416,5 i Australien, 1 av 501,0 i Hongkong, 1 av 1,161 i Japan och 1 av 613,0 i Singapore.
- Storbritannien var det land som var mest utsatt för nätfiske-attacker, där de i april utgjorde 1 av 199,7 e-mail.

Symantec MessageLabs rapport om internetsäkerhet april 2010

Branschtrender:

- I april var verkstadsindustrin den mest spammade industrin, med spamnivåer på 94,9 procent.
- Spamnivåerna inom utbildningssektorn var 91,1 procent, 90,2 procent inom kemi- och läkemedelsindustrin, 90,7 procent inom IT-sektorn, 90,9 procent inom detaljhandeln, 88,4 procent inom den offentliga sektorn och 88,4 procent inom finanssektorn.
- I april var den offentliga sektorn mest utsatt för skadlig kod med ett av 99,1 e-mail blockerade som skadliga.
- Virusnivåerna inom kemi- och läkemedelsindustrin var 1 av 438,2, 1 av 487,5 inom IT-sektorn, 1 av 600,2 inom detaljhandeln, 1 av 109,6 inom utbildningssektorn och 1 av 365,9 inom finanssektorn.

Message Labs Intelligence rapport för april innehåller mer detaljerad information om alla trender och siffror som redovisas ovan, samt mer detaljerade geografiska och vertikala trender. Hela rapporten finns på http://www.messagelabs.com/intelligence.aspx.

Symantecs MessageLabs Intelligence är en välrenommerad källa till data och analyser av säkerhet, trender och statistik för meddelandesystem. MessageLabs Intelligence tar fram en mängd information om globala säkerhetshot utifrån direkta datafeeds från våra kontrolltorn världen över, som varje vecka genomsöker miljarder e-postmeddelanden.

Om Symantec

Symantec är världsledande i att tillhandahålla lösningar för säkerhet, lagring och systemhantering. Vi hjälper privatpersoner och företag att säkra och hantera sin informationsdrivna tillvaro. Vår mjukvara och våra lösningar skyddar mot flera risker, på flera punkter mer fullständigt och effektivt än någon annan vilket ger trygghet oavsett var informationen används eller är lagrad. Mer information finns på www.symantec.com.