Pressmeddelande

CONTACT:
U.S.: Marissa Vicario
Symantec Corp.
+1 646 519 8116
mvicario@messagelabs.com

EMEA: Kirsten Doddy
Symantec
+ 44 (0) 203 009 6666
kdoddy@messagelabs.com

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

Symantecs MessageLabs Intelligence Report för augusti 2009

- Cutwails botnet skadat när internetleverantören lade ned, medan Donbot erbjuder medicinsk hjälp åt miljarder -

CUPERTINO, Calif. – 25 augusti 2009– Symantec Corp. (Nasdaq: SYMC) presenterade idag augustiupplagan av MessageLabs Intelligence Report. Analysen visar att aktivitetsnivån hos Cutwail, en av världens största botnets (nät av datorer som blivit övertagna) fallit med upp till 90 procent sedan en internetleverantör i Lettland dragit ur kontakten. Under augusti fortsatte emellertid en annan produktiv botnet med namnet Donbot att använda förkortade URL-adresser i sina spamutskick, med en distributionstopp på tio miljarder e-postmeddelanden på en enda dag.

Den lettiska internetleverantören Real Host lade ned verksamheten den 1 augusti efter att ha anklagats för kopplingar till ”command-and-control”-servrar med infekterade botnet-datorer, speciellt Cutwail som ansvarar för ungefär 15 till 20 procent av all skräppost (”spam”) idag. Efter nedläggningen föll de globala spamnivåerna med upp 38 procent inom 48 timmar.

”Cutwails aktivitetsnivå föll med så mycket som 90 procent efter att Real Host dragit ur kontakten. Men på bara ett par dagar var de tillbaka på banan och visade hur snabbt de kan återhämta och återskapa sig. Flera internetleverantörer har tidigare anklagats för att bistå botnet-aktiviteten, och att stänga dessa tjänster vid ett ovanligt beteende ingår i kriget mot cyberbrotten”, säger Paul Wood, senioranalytiker hos MessageLabs Intelligence på Symantec.

Trots denna korta variation i spamnivåerna ligger den totala siffran för augusti stadigt på 88,5 procent, på grund av aktivitetsnivåerna hos andra större botnets som Rustock, Mega-D och Donbot. Genom att utnyttja det ökade intresset för hälsofrågor i samband med den aktuella influensapandemin kunde Donbot distribuera sitt största spamutskick någonsin med förkortade URL-adresser – uppskattningsvis 10 miljarder läkemedelsinriktade skräppostmeddelanden på en dag. Ämnena som förekommer är *‘Health care – get meds now’*, *‘Save 89% on Meds’*, *‘Purchase Meds Online’*. Förkortade URL-adresser som leveransmetod har medfört att ett

(Forts.)

antal tjänster som erbjuder dessa varit tvungna stänga ned verksamheten då de inte kan hantera missbruket av deras verktyg.

Analysen från MessageLabs Intelligence visar också att cyberbrottslingar tre gånger hellre återanvänder skadliga program i andra domäner än utvecklar ny taktik. I augusti spärrades dagligen 3 510 webbplatser, där 36,1 procent av domänerna var nya. Liknande analys av skadliga program som dagligen spärras visar att bara 11,9 procent vara nya skadliga program.

Rapporten belyser också följande:

Skräppost: I augusti 2009 var den globala andelen av skräppost i e-posttrafiken från nya och okända källor 88,5 procent (1 av 1,13 e-postmeddelanden), vilket återspeglar en minskning på 0,9 procent sedan i juli.

Virus: Den globala andelen av e-postburna virus i e-posttrafiken från nya och tidigare okända källor var 1 av 296,6 e-postmeddelanden (0,34 procent), i princip oförändrat sedan i juli. I juli innehöll 14,8 procent av de e-postburna skadliga programmen länkar till skadliga webbplatser, en minskning med 0,4 procent sedan i juli.

Nätfiske (”phishing”): Ett av 341,2 e-postmeddelanden (0,29 procent) utgjorde någon form av nätfiskeattack, en minskning med 0,01 procent sedan i juli. Antalet e-postmeddelanden med nätfiske har minskat med 6,0 procent till 86,9 procent av alla e-postburna skadliga hot, till exempel virus och trojaner, som stoppades i augusti.

Webbsäkerhet: Analyser av aktiviteter inom webbsäkerhet visar att 45,4 procent av alla webbaserade skadliga program som stoppats var nya i augusti, en ökning med 44,7 procent sedan i juli. MessageLabs Intelligence har också identifierat ett genomsnitt på 3 510 nya webbplatser per dag som lagrar skadliga program och andra potentiellt oönskade program som spionprogram och annonssmusslingsprogram, en minskning med 0,01 procent sedan juli.

Geografiska trender:

- Hong Kong var det mest spamdrabbade landet under augusti även om nivåerna sjönk med 0,8 procent till 93,4 procent.
- Spamnivåerna i USA och Kanada steg till 89,5 procent respektive 88,7 procent. Majoriteten av övriga länder upplevde en minskning under augusti. Nivåerna i Storbritannien sjönk till 91,6 procent, i Tyskland till 90,4 procent, i Frankrike till 90,7 procent och i Nederländerna till 86,3 procent.

- Nivåerna i Australien och Japan sjönk till 90,6 procent respektive 89,2 procent.
- Även om aktiviteten i Kina minskade till 1 av 196,9 e-postmeddelanden, hamnade landet högst i virustabellen för augusti. Singapore och Schweiz försvarade sina positioner bland de fem mest drabbade länderna med virusnivåer på 1 av196,9 respektive 1 av 214,0 e-postmeddelanden. Storbritannien med nivåer på 1 av 219,3 och Förenade Arabemiraten med nivåer på 1 av 228,66 e-postmeddelanden kompletterar listan över de fem mest drabbade länderna under augusti.
- Virusaktiviteten ökade i Tyskland och i Nederländerna med nivåer på 1 av 275,5 e-postmeddelanden respektive 1 av 612,18. I USA minskade nivåerna något till 1 av 387,1 och ökade i Kanade där nivåerna uppnådde 1 av 309,9. Det land som var värst drabbat i juli, Australiern, hamnade i augusti på tolfte plats med nivåer på 1 av 308,3. I Hong Kong låg virusaktiviteten på 1 av 297,7 e-postmeddelanden och ökade i Japan till 1 av 400,76 e-postmeddelanden.

Vertikala trender:

- I augusti var tekniksektorn den mest skräppostdrabbade branschsektorn, med en andel på 93,4 procent.
- Skräppostnivåerna nådde 93,2 procent för utbildningssektorn, 92,5 procent för fordonssektorn, 90,7 procent för detaljhandeln, 89,8 procent för den offentliga sektorn och 88,7 procent för finanssektorn.
- Virusaktiviteten inom utbildningssektorn ökade till 1 av 120,0 infekterade e-postmeddelanden, vilket placerar den sektorn högst upp i virustabellen.
- Virusnivåerna för it-sektorn låg på 1 av 262,5, 1 av 490,3 inom detaljhandeln, 1 av 171,9 inom den offentliga sektorn och 1 av 288,4 inom kemi- och läkemedelssektorn.

MessageLabs Intelligence Report för augusti 2009 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.

###