Pressmeddelande

KONTAKTUPPGIFTER:

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 – mars 2011:

Global skräppost sjunker en tredjedel när botnätet Rustock nedmonteras; Bagle blir det mest aktiva skräppostutskickande botnätet

STOCKHOLM, Sverige – 31 mars, 2011 –Symantec Corp. (Nasdaq: SYMC) publicerade idag sin rapport om säkerhetshot på webben under mars månad. Analysen avslöjar att botnätet Rustock skickade ut hela 13,82 miljarder skräppostmeddelanden per dag under mars månad innan det nedmonterades. Rustock stod för i genomsnitt 28,5 procent av den globala skräpposten som skickades ut från alla botnät tillsammans i mars. När botnätet upphörde att skicka ut skräppostmeddelanden den här månaden sjönk den globala skräppostvolymen med en tredjedel. Sedan den anmärkningsvärda nedmonteringen av Rustock har andra botnät ökat sina aktiviteter för att utnyttja luckan på marknaden. Bagle har nu tagit över från Rustock som det mest aktiva skräppostutskickande botnätet under 2011.

MessageLabs Intelligence upptäckte att den globala skräppostvolymen föll med 33,6 procent mellan den 15 och 17 mars efter att åtal väckts mot de som fjärrstyr botnätet Rustock. Under de närmaste dagarna efter nedmonteringen av Rustock stod skräpposten för ungefär 33 miljarder e-postmeddelanden per dag, i jämfört med i genomsitt 52 miljarder per dag veckan innan.

"Det återstår att se om brottslingarna bakom Rustock kan återhämta sig efter denna koordinerade ansträngning mot det som har blivit ett av de mest tekniskt sofistikerade botnäten under de senaste åren", säger MessageLabs Intelligences senioranalytiker Paul Wood, Symantec.cloud. "Rustock har utgjort en stor del av botnäts- och sabotageprogrambilden sedan januari 2006, vilket är mycket längre än någon av deras samtida motsvarigheter."

I MessageLabs Intelligences årsrapport om internetsäkerhet för 2010 fanns märkligt nog inte Bagle med bland de tio mesta aktiva skräppostutskickande botnäten i slutet av året. Vid 2010 års slut stod Rustock för hela 47,5 procent av all skräppost, och de skickade ut ungefär 44,1 miljarder e-postmeddelanden om dagen.

I mars analyserade MessageLabs Intelligence även skräpposttrafiken från de tio största spamutskickande botnäten. Sedan slutet av 2010 har det allt aktivare botnätet Bagle skickat ut ungefär 8,31 miljarder skräppostmeddelanden per dag, varav de flesta kan länkas tillbaka till läkemedelsprodukter. Bagle kontrollerar inte lika många bottar som Rustock och de har heller inte lika stora och dominerande trafiktoppar, men nivån på deras utskick har varit stadigare.

I mars skickades 83,1 procent av all global skräppost ut från botnät, vilket är en ökning med 6,1 procentenheter, att jämföra med 77 procent i slutet av 2010. Under 2010 skickade botnäten ut ungefär 88,2 procent av all global skräppost.

”Botnäten har varit, och fortsätter att vara, en destruktiv resurs för cyberbrottslingar och under årens lopp har de blivit en nödvändighet för spammare, då det utan botnäten skulle vara mycket svårt för spammarna att fortsätta med sin verksamhet. Botnäten används även för andra ändamål, som att lansera distribuerade DoS-attacker, förse olagligt webbplatsinnehåll till infekterade datorer (så kallade bottar), hämta personliga uppgifter från dem och installera spionprogram för att spåra användarnas aktiviteter”, säger Wood.

Fler fakta som framkom i rapporten:

Skräppost/spam: I mars 2011 minskade den globala skräppostandelen av all e-posttrafik från nya och tidigare okända skadliga källor med 2 procent (1 av 1,26 e-postmeddelanden).

Virus: Den globala andelen e-postburna virus i e-posttrafik från nya och tidigare okända skadliga källor var 1 av 208,9 e-postmeddelanden (0,479 procent) i mars, vilket är en ökning med 0,134 procentenheter sedan februari. I mars innehöll 63,4 procent av e-postburna sabotageprogram länkar till skadliga webbplatser, vilket är en minskning med 0,1 procentenheter sedan februari.

Klienthot: Klienten är ofta sista försvarslinjen och även det som analyseras sist. De hot man hittar här kan belysa det bredare spektrum av hot som företag konfronteras med, särskilt från blandade attacker. Attacker som når klienten har troligtvis redan överlistat andra skyddslager i bruk, som till exempel portfiltrering.

Hot mot klienter, som bärbara datorer, PC:s och servrar, kan ta sig in i organisationer på flera olika sätt, bland annat genom drive-by-attacker från manipulerade webbplatser, trojanska hästar och maskar som sprids genom att de kopierar sig själva till externa lagringsminnen. En analys av vilka sabotageprogram som blockerats oftast under den senaste månaden visade att Sality.AE återigen var det mest utbredda viruset. Sality.AE sprids genom att det smittar körbara filer och genom att det försöker att ladda ner potentiellt skadliga filer från internet.

MessageLabs använde tekniker som heuristisk analys och generisk spårning för att identifiera och blockera flera varianter från samma sabotageprogramserier, samt för att identifiera nya former av skadlig kod som försöker utnyttja vissa svagheter som kan identifieras generiskt. Ungefär 15,7 procent av de oftast blockerade sabotageprogramment under förra månaden identifierades och blockerades på detta sätt, med hjälp av klientsäkerhetsskydd.

Nätfiske/phishing: I mars var nätfiskeaktiviteten 1 av 252,5 e-postmeddelanden (0,396 procent), vilket är en minskning med 0,065 procentenheter sedan februari.

Webbsäkerhet: En analys av webbsäkerhetsaktiviteter visade att i genomsnitt 2 973 webbplatser om dagen förser sabotageprogram och andra potentiellt oönskade program, däribland spion- och annonsprogram, vilket är en minskning med 27,5 procent sedan februari. 37 procent av alla skadliga domäner som blockerades under mars var nya, vilket är en minskning med 1,9 procentenheter sedan februari. Dessutom var 24,5 procent av all webbaserade sabotageprogram som blockerades i mars nya, vilket är en minskning med 4,2 procentenheter sedan förra månaden.

Geografiska trender:

- Oman utsattes för flest skräppostutskick i mars, med en skräppostandel på 87,9 procent.
- I USA var 79,6 procent av all e-post skräppost. och i Kanada var siffran 79,4 procent. Skräppostnivån i Storbritannien var 79,1 procent.
- I Nederländerna stod skräpposten för 80,2 procent av all e-posttrafik, medan skräppostnivån uppgick till 80 procent i Tyskland, 78,9 procent i Danmark och 78,8 procent i Australien.
- Skräppostnivån uppgick till 80,6 procent i Hong Kong och 77,7 procent i Singapore. Skräppostnivån i Japan var 76,4 procent.
- I Sydafrika stod skräpposten för 79,5 procent av all e-posttrafik.
- Luxemburg blev det mest utsatta landet vad gäller e-postburna sabotageprogram under mars månad: 1 av 26,2 e-postmeddelanden blockerades på grund av potentiellt skadligt innehåll. Den kraftiga ökningen berodde på ett stort antal varianter av sabotageprogrammen Bredolab, Zeus och SpyEye, som uppmärksammades i en mängd olika länder, bland annat Sydafrika.
- I Storbritannien innehöll 1 av 98,8 e-postmeddelanden sabotageprogram. I USA låg virusnivåerna på 1 av 507,9 och i Kanada på 1 av 160,1. Virusnivåer uppgick till 1 av 352,7 i Tyskland, 1 av 916,8 i Danmark och 1 av 467,1 i Nederländerna.
- I Australien var 1 av 261,0 e-postmeddelanden skadliga, medan siffran låg på 1 av 357,3 i Hong Kong, 1 av 1 015 i Japan och 1 av 823,8 i Singapore.
- I Sydafrika innehöll 1 av 76,9 e-postmeddelanden skadligt innehåll.

Branschtrender:

- I mars var fordonsindustrin fortfarande den industrisektor som utsattes för mest skräppostutskick, med en skräppostandel på 82,3 procent.
- Skräppostnivån för utbildningssektorn var 81 procent, medan den låg på 79,6 procent för kemi- och läkemedelsindustrin, 79,8 procent för IT-sektorn, 78,8 procent för detaljhandeln, 78,1 procent för den offentliga sektorn och 78 procent för finanssektorn.
- I mars fortsatte den offentliga sektorn att vara den mest utsatta branschen för sabotageprogram då 1 av 27 e-postmeddelanden blockerades på grund av potentiellt skadligt innehåll.
- Virusnivån för kemi- och läkemedelindustrin var 1 av 302,2, medan den låg på 1 av 326,5 för IT-sektorn, 1 av 397 för detaljhandeln, 1 av 109,6 för utbildningssektorn och 1 av 318,9 för finanssektorn.

MessageLabs Intelligences rapport från mars 2011 innehåller mer detaljerade uppgifter om alla de trender och siffror som anges ovan, samt mer detaljerade geografiska och vertikala trender. Hela rapporten finns tillgänglig på http://www.messagelabs.com/intelligence.aspx.

Symantecs MessageLabs Intelligence är en respekterad data- och analyskälla för säkerhetsfrågor som rör elektroniska utskick samt trender och statistik. MessageLabs Intelligence tillhandahåller en mängd olika slags information om globala säkerhetshot. Informationen baseras på dataflöden i realtid från våra kontrolltorn runt om in världen som skannar miljarder med meddelanden varje vecka.

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

###

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.