Pressmeddelande

Kontakt:
US: 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

Symantec MessageLabs årliga rapport: Webbsäkerhetsåret 2009

Spamrobotarna slår tillbaka med vassare överlevnadsteknik; fler varianter av skräppost och virus

MOUNTAIN VIEW, Calif., 8 december 2009– Symantec Corp. (Nasdaq: SYMC) publicerar idag sin årliga rapport om internetsäkerhet: MessageLabs Intelligence för 2009. Rapporten kartlägger hur internetbrottslingar under 2009 vässade sina verktyg för överlevnad och drev en strategi byggd på volym och varietet.

Rapporten belyser turbulent spam/skräppost-aktivitet under året, med en medelnivå på 87.7 procent, med toppar och dalar på 90.4 procent i maj och 73,3 procent i februari. Av de 107 miljarder spammeddelanden som dagligen distribuerades över världen under 2009, stod infekterade datorer för 83,4 procent. Nedstängingar av internetleverantörer som hyste spamrobotar, som t.ex. av McColo under slutet av 2008 och av Real Host i augusti 2009, ledde till att spammarna tvingades utvärdera och förbättra sina backupstrategier, vilket möjliggjorde att de kunde återhämta sig redan efter några timmar istället för veckor eller månader. Man förutspår nu att spamrobotarna kommer bli mer självständiga under 2010, på så sätt att varje nod kommer innehålla en inbyggd självgående kodning som gör det möjligt för noden att själv koordinera och förlänga sin egen överlevnad.

De tio största spamrobotarna fortsatte att styra över internetsäkerhetslandskapet under 2009, varav Cutwail, Rustock och Mega-D är de värsta. Dessa tre kontrollerar i dagsläget minst fem miljoner infekterade datorer. Cutwail var den drivande kraften bakom spam och skadlig kod (”malware”) under 2009 och ansvarade för 29 procent av all skräppost, eller 8 500 miljarder spammeddelanden, mellan april och november 2009.

Cutwail använde också sin styrka till att distribuera skräppost innehållande trojanen ”Bredolab”, som göms i bifogade .ZIP-filer i e-mailen. Bredolabtrojanen utgjorde ett av de största hoten under 2009 och var utformad på ett sätt som gav avsändaren total kontroll över mottagardatorn, som därmed kunde exponeras för ytterligare skadlig kod och spionprogram. Andelen spam som spred Bredolab ökade stadigt under hela 2009 och nådde sin högsta nivå i oktober, då cirka 3,6 biljoner e-postmeddelanden som innehöll denna trojan cirkulerade i världen.

(More)

”2009 var det år då cyberkriminella vässade sina tekniker istället för att enbart förlita sig på stora distributioner och attacker. Årets varianter var mer sofistikerade, teknologiskt avancerade och varierade”, säger Paul Wood, senioranalytiker på MessageLabs Intelligence inom Symantec. ”Vi stoppade fler än 21 miljoner olika typer av spamkampanjer under 2009, mer än dubbelt så många jämfört med 2008. Vi såg även en 23-procentig ökning i skadlig kod (”malware) jämfört med förra året. De kraftiga ökningarna antyder att den ökade tillgången på specialiserade verktygslådor gjorde det enklare än någonsin för cyberbrottslingarna att skapa och sprida spam, virus och annan skadlig kod.”

Det största säkerhetshotet i år var Conficker/Downadup, en mask som tillåter skaparen att installera mjukvara på infekterade datorer på avstånd. Confickermasken uppstod i slutet av 2008, och en uppdatering i april 2009 gav den ökad funktionalitet för att lättare undgå upptäckt. Conficker är ett särskilt bekymmer eftersom det fortfarande inte framgått hur man planerar att använda de infekterade datorerna. Conficker Working Group, som har bidragit till att minska Confickers påverkan under 2009, uppskattar att det totalt handlar om mer än sex miljoner infekterade datorer.

Under första halvan av 2009 gav finanskrisen upphov till många nya skräppost-attacker då spammare och andra cyberkriminella utnyttjade den allmänna osäkerheten kring den globala ekonomins nedgång. I februari var det spam innehållande länkar till ett antal välkända sökmotorer som levererade de flesta av de tidiga spammeddelandena baserade på lågkonjunkturen. Under 2009 innehöll 90.6 procent av alla spam en URL, främst driven av anstormning under den andra halvan av året då förkortade URL:s användes vilket hjälpte till att dölja den verkliga hemsidan som användaren skulle besöka och gjorde det svårare för traditionella spamfilter att identifiera meddelandet som skräppost. URL-förkortningar användes flitigt i sociala nätverk och mikrobloggar och är populära bland kriminella på nätet på grund av det inbyggda förtroendet som finns i relationen mellan användarna på den här typen av webbsidor.

Utöver den globala finanskrisen bidrog världshändelser, högtider och nyheter till flera spamteman under 2009, exempelvis Alla Hjärtans Dag, svininfluensan och Michael Jackson och Patrick Swayzes bortgång. De cyberkriminella utnyttjade detta och det första exemplet, en brasiliansk banktrojan som distribuerades via infekterade hyperlänkar, dök upp dagen efter Michael Jacksons bortgång.

“Även om förfining och innovation är i förgrunden av några av attackerna vi ser, spelar förutsägbarheten en stor roll för det dagliga hotlandskapet”, säger Wood. ”Säkerhetsindustrin som helhet talar om temaattacker såsom Alla hjärtans dag, jul, och kändisars död, förekomsten och volymen av dessa attacker antyder att internetbrottslingar fortfarande uppnår de mål de önskar, annars hade de ändrat sina metoder.”

Såkallad CAPTCHA-kod (Completely Automated Public Turing test to tell Computer and Humans Apart) hamnade i fokus i år då verktyg för att knäcka CAPTHCA-kod kom i omlopp på svarta marknaden, vilket hjälpte internetbrottslingar att skapa stora volymer av fejk-konton för webmail, instant messaging och sidor för sociala nätverk. Under året uppstod företag som specialiserat sig på att förmå verkliga personer att skapa verkliga konton på stora webmejltjänster på dygnet-runt basis. Dessa jobb har ofta annonserats som databehandlingsarbete och varje person får två till tre amerikanska dollar per 1 000 skapade konton. Dessa konton säljs sedan vidare till kriminella för 30-40 amerikanska dollar. Vissa större webbsidor har redan börjat undersöka alternativ till de ”förvrängda bokstäverna och numren”, som större bibliotek av fotografier där användaren måste kunna analysera och interagera med bilden på ett sätt som skulle vara en stor utmaning för ett dataprogram.

De största trenderna under 2009

Webbsäkerhet: Andelen illvilliga webbsidor som dagligen stoppades steg till 2 465 jämfört med 2 290 under 2008, en ökning med 7,6 procent. MessageLabs stoppade illvilliga webbhot på 30 000 enskilda domäner. 80 procent av dessa domäner etablerades lagligt och de resterande 20 procenten bestod av nya domäner som startades med uteslutande illvilligt syfte.

Spam/skräppost: Den årliga spamnivån låg på 87.7 procent under året, en ökning med 6.5 procent från förra årets nivå (81.2 procent). I april märktes en ökning av bildspam, som stod för 56.4 procent av all skräppost den 5 april jämfört med den årliga nivån på 28.2 procent.

Virus: Medelnivån för virus under 2009 var ett infekterat e-postmeddelande på 286,4 (0,35 procent) vilket motsvarar en minskning med 0,35 procent jämfört med 2008 då medelnivån låg på ett e-postmeddelande på 143,8 (0,70 procent). Nedgången kan härledas till övergången till att utveckla fler varianter (23 procent ökning under 2009 jämfört med 2008) men färre illvilliga e-postmeddelanden per ”strain” (cirka 5 827 illvilliga e-postmeddelanden per strain under 2009 jämfört med 10 436 email per strain under 2008)

Phishing/nätfiske: Under 2009 var antalet nätfiskeattacker en på 325,2 (0,31 procent) e-postmeddelanden jämfört med en på 244,9 (0,41 procent) 2008. Mer än 161 miljarder attacker var i omlopp under 2009.

Message Labs årliga Intelligence Report innehåller mer detaljer om trenderna och statistiken ovan. Rapporten i sin helhet finns tillgänglig här http://www.messagelabs.com/Threat_Watch/Intelligence_Reports

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.