شنبه 04 اردیبهشت 1389 - 08:19

وب ؛ دنيايي در دسترس تبهكارها

گزارش جديد موسسه امنيت انفورماتيكي سيمانتک نشان مي دهد که 240 ميليون برنامه مخرب جديد در سال 2009 ايجاد شده اند و بنابراين دنياي وب به يک محيط در دسترس و ساده براي انجام تبهكاريهاي بزرگ تبديل شده است...

گزارش جديد موسسه امنيت انفورماتيكي سيمانتک نشان مي دهد که 240 ميليون برنامه مخرب جديد در سال 2009 ايجاد شده اند و بنابراين دنياي وب به يک محيط در دسترس و ساده براي انجام تبهكاريهاي بزرگ تبديل شده است.
به گزارش مهر، در گزارش Internet Security Threat Report volume XV سيمانتک آمده است: "فعاليتهاي جنايتكاري روي وب از سرقتهاي ساده به تبهكاريهاي بزرگ تبديل شده اند که به بزرگترين شركتهاي دنيا و سازمانهاي دولتي كشورها خسارات زيادي وارد مي كنند."
به نظر مي رسد اين اظهارات سيمانتک مربوط به حملات سايبري است که در دسامبر 2009 به موتور جستجوي گوگل و 20 شركت بزرگ ديگر آسيب رساندند.
دو حادثه مهمي که در سال گذشته در عرصه جرائم انفورماتيكي به ثبت رسيدند حملات برنامه مخرب Conficker در ابتداي سال 2009 و Hydraq در پايان سال است.
برپايه گزارش سيمانتک، جنايتكاران انفورماتيكي در سال گذشته توجه خود را به روي شركتها معطوف كرده بودند. اين گزارش نشان مي دهد که هكرها در حال شكار حجم بالايي از اطلاعات شخصي موجود در روي سايتهاي شبكه هاي اجتماعي هستند و با كمک اين اطلاعات حملات خود را از طريق موتورهاي جستجوي اين شبكه ها بر روي افرادي که در شركتهاي خاص نقشهاي كليدي را عهده دارند انجام مي دهند.
برنامه Hydraq رسوايي بزرگي در ابتداي سال 2010 به دست آورد. باوجود اين Hydraq تنها جديدترين مورد از يكسري طولاني از حملات سايبري پس از حملات "شبكه سايه" (Shadow Network) در سال 2009 و Ghostnet در سال 2008 است.

ابزارها

ابزارهايي که در انجام حملات آنلاين مورد استفاده قرار مي گيرند بيش از هميشه ساده شده اند به طوري که حتي هكرهاي بدون مهارت نيز مي توانند به رايانه ها نفوذ كرده و به آساني اطلاعات شخصي كاربران را سرقت كنند.
يكي از اين ابزارها "زئوس" (Zbot) نام دارد که مي تواند به راحتي و به قيمت حدود 700 دلار فروخته شود. اين ابزار، فرايند ايجاد برنامه هاي مخرب شخصي شده را به طور خودكار اجرا مي كند و به اين ترتيب مي تواند برنامه هايي را براي دسترسي هكرها به اطلاعات شخصي كاربران ايجاد كند.
به طوري که با استفاده از يک "كيت" زئوس، جنايتكاران رايانه اي ميليونها گونه جديد از "كدهاي مخرب" را ايجاد كرده اند. اين كدها كمک مي كنند که هكرها توسط نرم افزارهاي امنيتي شناسايي نشوند.
نتيجه استفاده از اين ابزار، رشد انواع مختلف برنامه هاي مخرب است به طوري که سيمانتک 240 ميليون برنامه خطرناک جديد را در سال 2009 ثبت كرد که اين ميزان نسبت به سال 2008 صد در صد رشد داشت.
Downadup که از زيرگروههاي برنامه هاي Conficker است که تا پايان سال 2009 بيش از 6/5 ميليون رايانه را آلوده كرد. همچنين اخبار بدي درباره سرقت هويت از طريق اين برنامه به گوش مي رسد به طوري که در 60 درصد از موارد رايانه هاي آلوده شده يک سرقت اطلاعات شخصي به ثبت رسيده است.

به روزسازيهاي امنيتي پيچيده

از سويي ديگر، گزارش سيمانتک نشان مي دهد که به روزسازي مداوم وصله هاي امنيتي براي بسياري از كاربران به يک عمليات پيچيده تبديل شده است به طوري که برپايه اين گزارش، حفظ يک سيستم رايانه اي ايمن در سال 2009 يكي از اقدامات وقت گير كاربران بوده است.
به علاوه بسياري از كاربران موفق نشدند رايانه خود را در مقابل نفوذهاي قديمي ايمن كنند. براي مثال وصله امنيتي Microsoft Internet Explorer ADODBStream Object File Installation Weakness که در 23 آگوست 2003 منتشر شد و وصله هايي که از دوم جولاي 2004 در دسترس قرار گرفته اند دومين عامل نفوذپذير وب- پايه سال 2009 بوده اند.

شركتها

گزارش Symantec State of Enterprise Security Report 2010 نشان مي دهد که 75 درصد از شركتها در سال 2009 مورد اشكال مختلف حملات انفورماتيكي قرار گرفته اند که اين حملات چيزي از فراتر از بمباران ثابت هرزنامه ها بوده است که همه روزه به كاربران خانگي هجوم مي آورند.
در سال 2009 هرزنامه ها 88 درصد از تمام ايميلهاي مورد بررسي سيمانتک را تشكيل داده اند. همچنين نتايج اطلاعات سيمانتک

حاكي از آن است از 107 ميليارد پيام هرزنامه اي كه به طور متوسط در يک روز در سطح جهاني ارسال شده است 85 درصد محتوي يک برنامه مخرب بوده اند.