



بر اساس گزارش منتشر شده Cyberoam در سه ماهه دوم سال ۲۰۰۹:

تاخیر در واکنش به تروجانهای جدید توسط محصولات ضد ویروس مشهور

Cyberoam ، ارائه کننده ابزار های مدیریت یکپارچه تهدیدات بر مبنای تکنولوژی انحصاری هویت کاربر، با همکاری شریک تجاری خود ، Commtouch ، گزارش روند رو به رشد ویروسها و تهدیدات اینترنتی در سه ماهه دوم سال ۲۰۰۹ منتشر کرد. از نکات برجسته این گزارش می توان به افزایش شدید تعداد ویروس های جدید که از طریق ایمیل منتشر می شود اشاره کرد که بیشتر نرم افزارهای بزرگ و مشهور ضد ویروس برای چندین ساعت قادر به دفاع و واکنش در مقابل آنها نبوده اند.

یکی از دلایل افزایش شیوع ین تروجانها تکنولوژی جدید آنهاست که محصولات ضد ویروس مختلف به طور متوسط زمانی بین ۴ تا ۸۰ ساعت برای کشف آنها اختصاص دادند. در مقابل ، Cyberoam با بهره گیری از ضد ویروس کسپرسکی و سیستم پیشرفته ضد هرزنامه خود (تکنولوژی کشف الگوی برگشتی - RPD) که توسط شرکت Commtouch ارائه شده، در اولین لحظات از شیوع هر ویروس یا تروجان، آنرا فوراً شناسایی و مسدود می کند. زیرا در ساعات اولیه انتشار ، میلیون ها نفر از کاربران آسیب پذیر می توانند آلوده شوند.

Abhilash Sonwane ، قائم مقام و مدیر محصولات ، Cyberoam می گوید: "ویروس های امروز ، کرماها و تروجانها ، نقاط ضعف ضد ویروس های سنتی را هدف قرار داده و از ناتوانی و تعلل آنها در واکنش به این تهدیدات جدید در بازه کوتاه زمانی نهایت بهره را می برند."

فراهم بودن بستر برای ادامه فعالیت یک تروجان یا ویروس زمینه ساز بروز تهدیدات دیگر خواهد بود. بر اساس

یکی از این ترند های کلاهبرداری، بواسطه کدی که در بین سایر کدهای صفحات وب یک سایت آموزشی بصورت مخفیانه قرار می گیرد، از سیستم امنیتی رد شده و مسیر برای سرقت های اطلاعاتی و ربودن شناسه و رمز کاربران، هموار می شود.

بنا بر این گزارش، می توان به گسترش استفاده هرزنامه ها از مضامین حوادث جاری از جمله مرگ مایکل جکسون و یا گسترش آنفلانزا خوکی که برای کاربران جذاب می باشد، اشاره کرد. در میان ۱۰ دسته بندی وب سایتها (Web 2.0)، بیشترین میزان آلودگی به کدهای مخرب، مربوط به وب سایت های حاوی فایل های چند رسانه ای مثل فیلم ها و موزیک ها می باشد که مراجعه کنندگان زیادی دارند.

Cyberoam با استفاده از تکنولوژی Commtouch RPD™ هرزنامه های جدید را در ابتدای شروع فعالیتشان، از طریق تعداد نمونه های منتشر شده شان تشخیص می دهد. نتیجه این است که شرکتها به کمک سیستم ضد هرزنامه Cyberoam محافظت کاملی در برابر تهدیدات با قالبها و زبانهای مختلف دریافت خواهند کرد. این موضوع بر خلاف ضد هرزنامه های رایج، که بر بررسی محتوی ایمیل تکیه دارد بوده و به معنای عدم نیاز به تجزیه و تحلیل حجم زیادی از اطلاعات و افزایش ترافیک اینترنت می باشد. همچنین شناسایی انواع اسپم ها در غالب تصویر، کدهای HTML و ... با هر زبانی از دیگر توانایی های این سیستم است.

برای کسب اطلاعات بیشتر به وب سایت www.cyberoam.com/ir مراجعه نمایید.