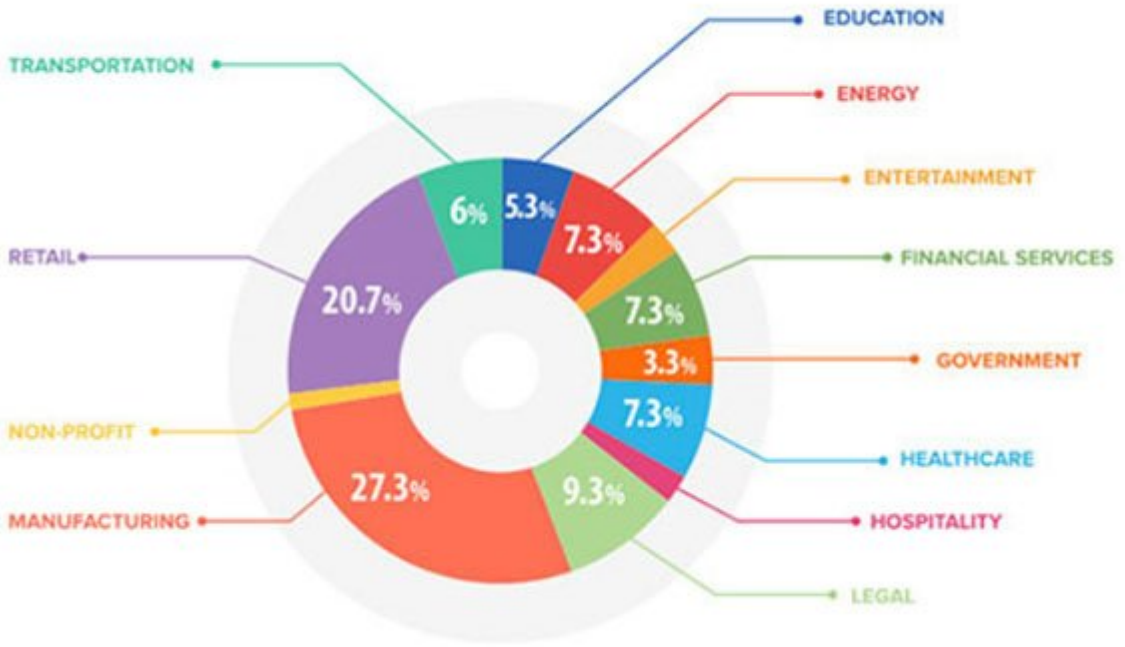
الگوی تهدیدی به مراتب قدرتمندتری از تهدید زئوس دارند

بدافزارهای بانکی در کمین سازمان‌ها

سازمان‌های امنیتی در حال کشف گونه‌های جدیدی از بدافزارهای بانکی هستند که عملکرد به مراتب قدرتمندتری از زئوس دارد. برنامه‌های مخرب همگی با هدف سرقت اطلاعات اعتباری مورد استفاده در حساب‌های آنلاین بانکی، از تکنیک ویژه انتقال و سیستم پاک‌سازی خودکار ACH (سرنام Automated Cleaning Hourse) استفاده می‌کنند.

در مطالعه‌ای که به‌تازگی شرکت امنیتی SecurityScorecard متخصص در ردیابی نفوذهای خطرناک انجام شده نشان می‌دهد که بیش از 4700 سازمان با نوع جدیدی از بدافزارهای پیش‌رفته آلوده شده‌اند. SecurityScorecard در این بررسی برای جمع‌آوری داده‌ها از بخش‌های مختلف یک سازمان از حفره‌ها یا کامپیوترهایی که تحت کنترل محققان بوده و بخشی از ماشین‌های آلوده یک شبکه را شکل داده به‌نام بات‌نت استفاده کرده‌اند. آلکس هید، مدیر بخش پژوهش SecurityScorecard، درباره این گزارش گفته است: «این شرکت همچنین کمپین‌های هرزنامه، آسیب‌پذیری در برنامه‌های تحت شبکه و کمپین‌های مخرب را با مانیتور کردن فرم‌های زیرزمینی هکرها و شبکه‌های اجتماعی مورد بررسی قرار داده است.» از دید هکرها، کاربر همیشه به دنبال ضعیف‌ترین لینک‌ها و نقاط برخورد است. در مطالعه‌ای که در پنج ماه نخست سال انجام شده، 11952 آسیب‌پذیری در 4703 سازمان کشف شده است. بعضی از این سازمان‌ها مشتریان SecurityScorecard و بقیه از شرکای این مشتریان هستند. در مدت زمانی که SecurityScorecard به ارزیابی شبکه مشتریان خود پرداخته متوجه شده است که این مشتریان اطلاعات خود را با شرکای خود به اشتراک قرار می‌دهند که باعث می‌شود دسترسی به سیستم‌های آن‌ها امکان‌پذیر شود. این مدل از ارتباطات به‌طور فزاینده از جمله اهداف مورد توجه هکرها است. کارت‌های اعتباری به‌طور گسترده در خانه و محل کار مورد استفاده قرار می‌گیرند، حال آن‌که این کارت‌ها نقایصی دارند که در نتیجه نفوذ را برای طرف‌های ثالث برای دسترسی به اطلاعات بانکی با استفاده از سیستم کاربران امکان‌پذیر می‌سازد. به‌تازگی خانواده‌ای جدید از بدافزارهای بانکی به نام‌های Bebloh، Dridex و TinyBanker در حال گسترش هستند.
Dridex از طریق هرزنامه گسترش یافته‌اند و شامل ضمیمه‌های آلوده به فایل‌های مخرب XML یا اسناد آفیس مایکروسافت هستند که همراه با ماکروها منتشر می‌شوند. میزان آلوده‌سازی Dridex در صنایع مختلف را در شکل زیر مشاهده می‌کنید.



درصد آلوده‌سازی Dridex

Bebloh گونه دیگری است که شناسایی آن کار چندان ساده‌ای نیست، به طوری که تغییرات کمی را در کامپیوترهای آلوده به وجود می‌آورد. TinyBanker تنها 20 کیلوبایت حجم دارد و پیدا کردن آن به‌سختی امکان‌پذیر است. همچنین، سازندگان آن به‌طور مرتب ردپای دیجیتالی آن را تغییر می‌دهند که همین موضوع باعث می‌شود تا بدافزار به‌راحتی از دام محصولات امنیتی بگریزد.
کسانی که اقدام به توزیع این بدافزارهای مخرب می‌کنند، برای اطمینان از این‌که بدافزارهای آن‌ها به‌طور کامل قابل شناسایی نباشند و کشف نشوند به‌سختی در تلاش هستند و سعی می‌کنند برنامه‌های خود را به‌طور کامل کشف‌ناپذیر (FUD سرنام Fully Undetectable) کنند (FUD گونه‌ای از رمزنگاری چندگانه داده‌ها است و از تکنیک تولید داده‌های تصادفی استفاده می‌کند. این شیوه رمزنگاری روی نرم‌افزارهایی مورد استفاده قرار می‌گیرد که در مدت زمان فرآیند اسکن توسط آنتی‌ویروس‌ها نباید شناسایی شوند). آن‌ها این کار را با استفاده از ابزارهای رمزنگاری که Crypters یا Packers نامیده می‌شوند و فایل‌ها را به شیوه‌ای فشرده می‌کنند که شناسایی آن‌ها با مشکل همراه باشد، انجام می‌دهند. همچنین، SecurityScorecard نمونه‌هایی از بدافزار Dyre را نیز شناسایی کرده است؛ گونه دیگری از بدافزار بانکی که بسیار قدرتمندتر از بدافزار مخرب زئوس عمل می‌کند. وزارت دادگستری ایالات متحده با محققان این گروه امنیتی در حال کار روی بات‌نت Gameover Zeus هستند که از نیمه دوم سال 2014 میلادی فعالیت خود را آغاز کرده است. آن‌ها در تلاش هستند این بدافزار را در اسرع وقت متوقف کنند. این بات‌نت و نرم‌افزارهای مخرب همراه آن تاکنون 100 میلیون دلار به سرقت برده‌اند.

تاریخ انتشار:

20 مرداد 1394

نشانی منبع: https://www.shabakeh-mag.com/security/1156