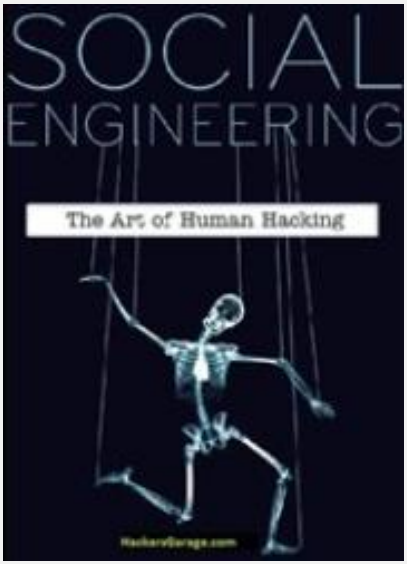


جمعه 30 اردیبهشت 1390 - 13:00

## [مایکروسافت: از هر 14 دانلود یکی آسیب‌رسان است]

بار دیگر یک وب‌سایت می‌گوید نرم‌افزار جدیدی را دانلود کنید تا فیلم جدید را ببینید یا نقصی را برطرف کنید، کمی تامل کنید. احتمال بسیار زیادی وجود دارد که این برنامه آسیب‌رسان و به اصطلاح بدافزار باشد.

بار دیگر یک وب‌سایت می‌گوید نرم‌افزار جدیدی را دانلود کنید تا فیلم جدید را ببینید یا نقصی را برطرف کنید، کمی تامل کنید. احتمال بسیار زیادی وجود دارد که این برنامه آسیب‌رسان و به اصطلاح بدافزار باشد.

به گزارش پی‌سی ورلد مایکروسافت سه‌شنبه 17 مه اعلام کرد از هر 14 برنامه‌ای که بوسیله کاربران ویندوز دانلود می‌شود، یکی از آنها آسیب‌رسان است. و با وجود اینکه مایکروسافت دراینترنت اکسپلور ویژگی را تعبیه کرده است تا به کاربران در مورد نرم‌افزارهای ناشناس و بالقوه غیرقابل‌اعتماد هشدار دهد، حدود 5 درصد کاربران این هشدارها را نادیده می‌گیرند و بدافزارها را دانلود می‌کنند.

پنج سال پیش، برای خلافکاران بسیار آسان بود که کدهای‌شان را به کامپیوترها نفوذ دهند. جستجوگرها عیب‌های زیادی داشتند، و بسیاری از کاربران توانایی رفع را نداشتند. اما از آن به بعد بازی موش و گربه امنیت اینترنت تحول پیدا کرده است: جستجوگرها ایمن‌تر شده‌اند، و نرم‌افزارها می‌توانند به طور خودکار نقص‌های شناخته‌شده را رفع کنند.

بنابراین به طور فزاینده‌ای، خلافکاران به جای نفوذ از راه خود جستجوگرها، سعی می‌کند که به افرادی که از آنها استفاده می‌کنند، نفوذ کنند. این شیوه را مهندسی اجتماعی می‌نامند، و مشکل بزرگ این روزهاست.

آلکس استاموس، یکی از بنیانگذاران، یک شرکت مشاوره امنیت اینترنت، که اغلب پس نفوذ افراد به شبکه‌های کامپیوتری شرکت‌ها، برای حل مشکل فراخوانده می‌شود، می‌گوید: "مهاجمان دریافته‌اند که واداشتن کاربران دانلود کردن تروجان‌ها سخت نیست.

به همین روش مهندسی اجتماعی بود که ویروس Koobface در فیس بوک منتشر شد. کاربران پیامی دریافتند می کردند که دوستی به آنها می‌گوید بروند و ویدئویی را مشاهده کنند. هنگامی فرد روی این پیوند کلیک می‌کرد، به آنها گفته می‌شد برای تماشای ویدئو لازم است یک نرم‌افزار پخش ویدئو را دانلود کنند. این نرم افزار در واقع یک برنامه آسیب‌رسان بود.

هکرهایی که از مهندسی اجتماعی استفاده می‌کنند، همچنین با نفوذ بر صفحات وب و بیرون زدن هشدارهای تقلبی ضدویروسی مانند پیام‌های سیستم عامل طعمه‌هایشان را شکار می‌کنند.

دانلود کردن این برنامه همان و آلوده شدن سیستم همان. خلافکاران همچنین از هرزنامه (اسپم) برای فرستادن تروجان‌ها استفاده می‌کنند، و موتورهای جستجو را برای پیوند دادن وب‌سایت‌های آسیب‌رسان که به نظر می‌رسد گزارش‌ها یا ویدئوهای جالب درباره اخبار داغ روز مثل عروسی سلطنیت یا مرگ اسامه بن لادن داشته باشند، فریب می‌دهند.

جوشوآ تالبوت، مدیری که در بخش "پاسخ امنیتی" شرکت سیمانتک کار می‌کند، می‌گوید: "هکرها بسیار فرصت‌طلب هستند، و از هر رویدادی که ممکن است برای فریب افراد از آن استفاده کرد، متوسل می‌شوند." هنگامی که سیمانتک رایج ترین 50 برنامه آسیب‌رسان را ردیابی کرد، مشخص شد که 56 درصد همه حمله‌ها شامل برنامه‌های اسب تروا (تروجان‌ها) بوده‌اند.

یک تکنیک مهندسی اجتماعی به نام "اسپیرفیشینگ" (spearphising) در شرکت‌ها مسئله‌ای جدی است. خلافکاران در این شیوه در مورد خصوصیات افرادی که می‌خواهند به آنها حمله کنند، به بررسی می‌پردازند، و بعد یک یک برنامه به طور خاص ساخته‌شده برای این افراد یا یک سند با کدبندی آسیب‌رسان که قربانی احتمالا می‌خواهد آن را باز کند- مثلا مطالبی از یک کنفرانس که این افراد در

آن شرکت کرده‌اند یا یک سند طرح‌ریزی از سازمانی که آنها می‌خواهند با آن معامله کنند- ایجاد می‌کنند.

اینترنت اکسپلور 9 ، یک برنامه غربالگری جدید- SmartScreen Filter Application Reputation- دارد که اولین خط دفاعی در برابر تروجان‌ها، ازجمله تروجان‌هایی است که در حملات اسپیرفیشینگ فرستاده می‌شوند.

اینترنت اکسپلور همچنین به کاربران هنگامی که برای رفتن به وب‌سایت‌های آسیب‌رسان ترغیب می‌شوند، روشی دیگری که هکرهای مهندسی اجتماعی با آن کاربران کامپیوتر را می‌توانند آلوده کنند، هشدار می‌دهد.

به گفته جب هابر، مدیر برنامه SmartScreen ، این برنامه اینترنت اکسپلورر در سال گذشته بیش از 1.5 میلیارد حمله وبی و دانلودی را مانع شده است.

به گفته او هنگامی که هشدار این برنامه بیرون می‌زند تا به کاربران بگوید این برنامه بالقوه آسیب‌رسان را اجرا نکنند، در نسبتی میان 25 تا 75 درصد احتمال دارد که این برنامه واقعا آسیب‌رسان باشد.

هابر می‌گوید کی کاربر معمولا یکی دوتا از این هشدارها در هر سال می‌بیند، و بهترین کار جدی گرفتن آنهاست.