مــراقب ایــن شش نــقطه خطــرناک در اینتــرنت باشید

خلاصه : چند سالی می‌شود که گوگل به جزء جدایی ناپذیر زندگی امروزه کاربران تبدیل شده است. تا جائیکه نتایج جستجوی آن پاسخ اکثر سوالات آن‌ها را در هر زمینه‌ای می‌دهد. اما همین فناوری به شدت پیچیده می‌تواند دردسرهای جدی هم به لحاظ امنیتی برای کاربران فراهم کند. کاربران اینترنت معمولاً برای یافتن عکس‌ها، ویدئوهای خنده دار، مقالات علمی و... خود در گوگل جستجو می‌کنند اما ممکن است در خلال همین جستجوها به یکباره سیستم آن‌ها با مشکلات جدی روبرو شود. بسیاری از متخصصان امنیتی، محیط مجازی را به میدان مین تشبیه کرده‌اند چراکه درست زمانیکه شما فکر می‌کنید همه جوانب امنیتی را رعایت کرده‌اید، به بدافزارهای کلاهبرداری آنلاین آلوده می‌شوید.

شماره : 29

تاریخ : 1392/11/27

موضوع : اینترنت

متن : مــراقب ایــن شش نــقطه خطــرناک در اینتــرنت باشید چند سالی می‌شود که گوگل به جزء جدایی ناپذیر زندگی امروزه کاربران تبدیل شده است. تا جائیکه نتایج جستجوی آن پاسخ اکثر سوالات آن‌ها را در هر زمینه‌ای می‌دهد. اما همین فناوری به شدت پیچیده می‌تواند دردسرهای جدی هم به لحاظ امنیتی برای کاربران فراهم کند. کاربران اینترنت معمولاً برای یافتن عکس‌ها، ویدئوهای خنده دار، مقالات علمی و... خود در گوگل جستجو می‌کنند اما ممکن است در خلال همین جستجوها به یکباره سیستم آن‌ها با مشکلات جدی روبرو شود. بسیاری از متخصصان امنیتی، محیط مجازی را به میدان مین تشبیه کرده‌اند چراکه درست زمانیکه شما فکر می‌کنید همه جوانب امنیتی را رعایت کرده‌اید، به بدافزارهای کلاهبرداری آنلاین آلوده می‌شوید. به گزارش روابط عمومی شرکت ایمن رایانه پندار نماینده رسمی و انحصاری شرکت پاندا سکیوریتی در ایران، از این رو به تازگی وزارت امنیت داخلی امریکا اقدام به بررسی درجه و میزان خطرآفرینی هر یک از محیطهای مجازی در فضای اینترنت کرده و براساس رنگ، درجه خطر هر یک را طبقه بندی کرده است. این گزارش همچنین شش نقطه پرخطر را در اینترنت معرفی و در نهایت راه مقابله و محافظت از کاربران را در هر یک از این فضاها عنوان کرده است. براساس طبقه بندی وزارت امنیت داخلی امریکا، وب سایت‌ها در پنج سطح آبی، سبز، زرد، نارنجی و قرمز از ایمن تا خیلی خطرناک دسته بندی شده‌اند. بر این اساس سطح آبی شامل وب سایت‌هایی است که کاملاً امن بوده و امکان وجود هیچ گونه خطر امنیتی در آن‌ها وجود ندارد. سطح بعدی سبز رنگ است که اگر کاربری به دنبال ریسک‌های امنیتی باشد، شاید بتواند نوع خفیفی از آن را پیدا کند اما به هیچ عنوان آسیب جدی به حساب نمی‌آید. سطح زرد رنگ وب سایت‌های خطرناکی را در بر می‌گیرد که به خودی خود آلوده نیستند اما لینک‌های رد و بدل شده در آنها می‌تواند آلوده باشد و یک کلیک کاربر می‌تواند او را با مشکلات جدی روبرو کند. سطح نارنجی وب سایت‌های خطرناک را در بر می‌گیرد. در این وب سایت‌ها آلودگی به کاربر بسیار نزدیک بوده و بهتر است کاربر اصلاً به آن‌ها مراجعه نکند و در نهایت سطح قرمز وب سایت‌های بسیار خطرناک و آلوده را شامل می‌شود که کاربر به محض بازدید از آن‌ها قطعاً آلوده خواهد شد. براساس این گزارش، وزارت امنیت داخلی امریکا به بررسی موقعیت‌های خطرناک و همچنین محیطهای ناامنی پرداخته است که کاربران در مواجهه با این محیطها و موقعیت‌ها باید هوشیاری بیشتری به خرج داده و بیشتر از قبل نکات امنیتی را رعایت کنند. در ادامه به بررسی هر یک از این موقعیت‌ها می‌پردازیم: – موقعیت اول: فایل‌های مخرب فلش محیط خطرآفرین: وب سایت‌های حاوی فایل‌های فلش طی سال‌های اخیر نرم افزارهای گرافیکی ادوبی فلش به هدف مطلوب بدافزارها تبدیل شده‌اند. بطوریکه این شرکت به طور مداوم در حال انتشار اصلاحیه های امنیتی است! اما آنچه در این نرم افزار محل خطر است، کوکی‌های فلش است که به سازندگان آن این امکان را می‌دهد تا تنظیمات کمتری بر روی فلش اعمال کنند و از این طریق سایت‌هایی که شما بازدید کرده‌اید را ردیابی کنند. بدتر از آن زمانیست که حتی با حذف کوکی‌های مرورگر، باز هم کوکی‌های فلش در پشت صحنه باقی می‌مانند. پس اگر شما از یک وب سایت حاوی فلش بازدید کردید، به منظور حفاظت در برابر حملات مبتنی بر فلش، پلاگین فلش مرورگر خود را بروز نگه داشته و قبل از هرگونه دانلود آن را با تنظیمات مرورگر خود بررسی کنید. – موقعیت دوم: لینک های کوتاه شده محیط خطرآفرین: توییتر از زمان ایجاد توییتر، کلاهبردان اینترنتی سعی می کنند تا با استفاده از لینک های کوتاه شده کاربران را برای کلیک بر روی لینک های مخرب ترغیب کنند. چراکه پنهان کردن بدافزارها پشت لینک‌های کوتاه کار بسیار ساده تری است. پس هر زمان که به سایت توییتر سر زدید به هیچ وجه بر روی هیچ لینکی کلیک نکنید. اگر هم می خواهید لینک های مخرب را از سالم تشخیص دهید از برنامه Tweet Deck که دارای ویژگی نمایش کامل لینک ها قبل از ورود به سایت است، استفاده کنید. موقعیت سوم: ایمیل‌ها و فایل‌های پیوست محیط خطرآفرین: Inbox ایمیل شما اگرچه کلاهبرداری های فیشینگ و حملات مخرب به ایمیل‌ها اتفاق تازه ای نیست اما روش‌های این کلاهبرداری ها دائماً در حال تحول است. بطوریکه این روزها پیام‌های عادی از پیام‌های مخرب قابل تشخیص نیستند. به همین دلیل به کاربران توصیه می‌شود به هرآنچه که به Inbox شان وارد می‌شود، اعتماد نکرده و به جای کلیک بر روی لینک‌های ارسال شده به صورت مستقیم به وب سایت مربوطه مراجعه کنند. موقعیت چهارم: موزیک‌ها، ویدئوها و نرم افزارها محیط خطرآفرین: وب سایت‌های دریافت (Download) موزیک، ویدئو و نرم افزار سایت‌های دریافت (Download) موزیک، ویدئو و نرم افزار، گنجینه ای از نرم افزارهای مخرب در لباس مبدل هستند! بسیاری از متخصصان امنیتی معتقدند وب سایت‌های این چنینی یکی از خطرناک‌ترین محیطها برای بازدید هستند. چراکه اغلب این وب سایت‌ها یک مدل مشخص از کسب و کار و همچنین اعتبار امنیتی کافی ندارند. اگرچه بهتر است به دلیل محتوای غیرقابل اعتماد این وب سایت‌ها به طور کامل از بازدید آن‌ها صرف نظر کنید اما اگر به هر دلیلی به این وب سایت‌ها سر زدید، بهتر است به منظور حفاظت از سیستم اصلی خود، از یک سیستم دوم با یک آنتی ویروس کاملاً بروز استفاده کنید. در نهایت فایل‌های دانلود شده را اسکن کرده و یکی دو روز بعد آن‌ها را باز کنید. چراکه نرم افزارهای مخرب به محض باز شدن به همه سیستم شما رسوخ می‌کنند اما با تاخیر در باز کردن آن‌ها، به آنتی ویروس اجازه می‌دهد مجوزهای لازم را مورد بررسی قرار دهد. موقعیت پنجم: بدافزارهای پنهان در فیلم‌ها و تصاویر غیراخلاقی محیط خطرآفرین: وب سایت‌های نامشروع سایت‌های نامشروع به خودی خود نسبت به سایر سایت‌های فعال و عمومی از درجه امنیت کمتری برخوردار هستند. اما این فرضیه تمام داستان نیست. اگرچه بازدید از این وب سایت‌ها به دلیل محتوای آن‌ها، بطورکلی مخرب است اما به دلیل اینکه هیچ خط

مشی امنیتی مشخصی ندارند علاوه بر محتوای مخرب می‌توانند حاوی برنامه‌های آلوده و بدافزار هم باشند. از این رو کاربران بهتر است به هیچ دلیلی به هر یک از این وب سایت‌ها وارد نشوند. موقعیت ششم: ویدئوهای آنلاین محیط خطرآفرین: وب سایت‌های به اشتراک گذاری ویدئو شاید برای شما پیش آمده، در حال تماشای یک ویدئوی آنلاین هشداری نمایش داده می‌شود مبنی بر اینکه برای دانلود این ویدئو نیازمند نرم افزار خاصی هستید. چراکه نرم افزار فعلی شما فایل مربوطه را پشتیبانی نمی‌کند. قانونی بودن نرم افزار معرفی شده به اعتبار وب سایتی که شما در حال بازدید از آن هستید بر می‌گردد. اگر در حال تماشای ویدئو از یک وب سایت نا آشنا هستید بهتر است به پیغام داده شده اعتنا نکرده و نرم افزار را دانلود نکنید. اما بطورکلی بهتر است برای تماشای ویدئوهای آنلاین به وب سایت‌های شناخته شده ای مثل Vimeo و یوتیوب مراجعه کنید. در نهایت اینکه اگرچه امروز اینترنت فاصله‌ها را کم و دسترسی‌ها را آسان کرده است اما هر لحظه از حضورمان در این فضا می‌تواند موقعیت مناسبی را در اختیار سودجویان قرار دهد. شش موقعیتی که توسط وزارت امنیت داخلی امریکا مورد بررسی قرار گرفت اگرچه ممکن است خطرآفرین باشند اما تمام پهنه گسترده اینترنت را شامل نمی‌شوند. از این جهت به نظر می‌رسد تنها راه حل مطمئن برای مقابله با کلاهبردان و نفوذگران، هوشیاری کاربران و استفاده به جا از ابزارهای امنیتی مناسب است.

نویسندگان : محمد رامندی