ترفند ویندوز

بالا بردن سرعت اینترنت در ویندوز

در ویندوز قابلیتی وجود دارد به نام QoS Packet Scheduler که این موضوع ۲۰٪ از پهنای باند اینترنت شما را محدود می‌کند. در صورتی که به این قابلیت نیازی ندارید با غیرفعال کردن آن می‌توانید با آزاد کردن پهنای باند گرفته شده سرعت اینترنت خود را تا حد چشم‌گیری بالا ببرید. در صورتی که از سرعت اینترنت خود ناراضی هستید از این ترفند بهره بگیرید.

بدین منظور:

۱. با فشردن کلیدهای ترکیبی Win+R وارد Run شوید.
۲. در Run عبارت gpedit.msc را تایپ کرده و OK را کلیک کنید.
۳. منتظر بمانید تا Group Policy اجرا شود.
۴. در بخش Local Computer Policy و زیر Computer Configuration گزینه Administrative Templates را گسترش دهید (با کلیک بر روی علامت + کار آن انجام دهید).
۵. در لیست باز شده گزینه Network را نیز گسترش دهید.
۶. حال در این لیست Qos Packet Scheduler را انتخاب کنید.
۷. به گزینه‌هایی که در سمت راست ظاهر می‌شوند دقت کنید.
۸. بر روی Limit reservable bandwidth کلیک راست کرده و Edit را انتخاب کنید.
۹. پس از این که پنجره Limit reservable bandwidth Properties باز شد گزینه Enabled را انتخاب کنید.
۱۰. مشاهده می‌کنید که با انتخاب آن در روبروی Bandwidth Limit مقدار پیش‌فرض آن یعنی ۲۰ درصد به نمایش در می آید.
۱۱. به جای عدد ۲۰ مقدار ۰ را تایپ کرده و OK را کلیک کنید.
۱۲. حال به Control Panel\Network and Internet\Network Connections رفته و بر روی کانکشنی که از طریق آن به اینترنت متصل می‌شوید راست کلیک کرده و دکمه Properties را انتخاب کنید.
۱۳. به برگه Networking بروید و دقت کنید که Qos Packet Scheduler فعال باشد (تیک کنار آن مشاهده شود).
۱۴. این پنجره را OK کنید.
۱۵. کامپیوتر خود را Restart کنید.

چند نکته:

این کار را می‌توانید با نرم‌افزارهای قدرتمند بهینه سازی ویندوز مثل TuneUp Utilities خیلی سریع‌تر و راحت‌تر انجام دهید.
برای بازگشت به حالت پیش‌فرض هم می‌توانید مسیر فوق را دنبال کرده و به جای ۰ عدد ۲۰ را قرار دهید یا گزینه Disabled را انتخاب کنید.

آشنایی با تروجان Ztrog که به خاطر ۵ سنت شما را آلوده می‌کند

تروجانی که شما را ارزان می‌فروشد

بسیاری از تبلیغات در سراسر اینترنت راه‌های آسانی را برای به دست آوردن پول ترویج می‌دهند. آن‌ها اغلب مایلند کاربران را به مکان‌های غیر طبیعی هدایت کنند و می‌گویند چند هزار دلار در روز درآمد دارند و شما هم به راحتی می‌توانید همین کار را انجام دهید. اما راه‌های آسان دیگری برای کسب درآمد وجود دارد که حداقل قابل قبول‌تر به نظر می‌رسد. به گزارش کسپرسکی آنلاین، به عنوان مثال، برخی خدمات وجود دارند که پیشنهاد می‌کنند که برای نصب برنامه‌ها پول پرداخت کنید. این مبلغ پول معادل با پر کردن جیب توسعه دهندگان است (حدود ۵ سنت برای هر اپلیکیشن) اما این کار تقریبا بدون دردسر است و به همین خاطر است که بسیاری افراد را مجذوب خود می‌کند. این نوع روش در میان کودکان محبوبیت بسیاری دارد، آن‌ها ۵۰ اپلیکیشن را نصب می‌کنند و تنها ۲.۵۰$ بابت این تعداد بازی پرداخت می‌کنند. اپلیکیشن گوگل پلی فروشگاهی است که در آن انواع مختلف برنامه ها وجود دارد. شما یکی از آن‌ها را دانلود می‌کنید، پس از نصب آن‌ها لیستی از برنامه‌هایی که شما می توانید آن‌ها را پرداخت کنید مشاهده می‌کنید. چند تا از آن‌ها را به دلخواه انتخاب می کنید و آن‌ها را نصب و پول را به جیب توسعه دهندگان اضافه می‌کنید. این روند کاملا پیش و پا افتاده است و مطمئنا بسیاری از ما تا به حال این کار را تجربه کرده‌ایم. در حقیقت بسیاری از توسعه دهندگان نرم افزارها هستند که تعداد دانلود اپلیکیشن‌های خود را در رتبه بالایی قرار می‌دهند و در برخی موارد حتی آن‌ها را افزایش می‌دهند، حتی اگر آن صادق نباشد. جای تعجب ندارد که توسعه دهندگان مایلند برای این کار هزینه‌ای پرداخت کنند. به نظر نمی‌رسد که مشکلی برای آن‌ها پیش آید، اینطور نیست؟

پرداخت پول برای دریافت بدافزارها؟

بله همینطور است. به نظر می‌رسد که در میان چیزهای دیگر، از جمله دانلود اپلیکیشن‌ها شما بدافزارهایی را هم دانلود کنید، که در این جا شاهد تروجان بدنامی به نام Ztorg هستیم. در چند ماه گذشته، تروجانی که ۵۰۰,۰۰۰ بار از گوگل پلی دانلود شد به عنوان راهنمایی بازی محبوب Poké-mon Go تغییر ظاهر پیدا کرده بود. اپلیکیشن راهنمای Pokémon Go تنها شامل برنامه Ztorg نبود. Roman Unuchek یکی از کارشناسان لابراتوار کسپرسکی که Ztorg را در اپلیکیشن‌ها کشف کرده بود، اپلیکیشن‌های مخرب دیگری را که از این طریق توزیع شده بودند را کشف کرد. او متوجه شد که هر برنامه جدیدی که ظاهر می‌شود با لباس مبدل Ztorg است و شخص جدیدی پشت این ماجرا نیست. این اپلیکیشن می‌تواند یک ویرایشگر عکس، قطب نما، یک بازی و یا هرچیزی باشد. مجرمان پشت این برنامه مخرب حتی تلاشی برای اضافه کردن کدهای مخرب به اپلیکیشن‌های مفید موجود نکردند. به جای این کار آنها برنامه‌های مخرب را از ابتدا نوشتند. در نتیجه، برخی از آن‌ها کاملا بی‌فایده بودند.

Ztorg چه کار می‌کند؟

همه این اپلیکیشن‌ها دو چیز مشترک دارند. اول اینکه تعداد دانلود آن‌ها به سرعت افزایش پیدا می‌کند (ده‌ها هزار نفر در روز)، دوم اینکه اگر شما به نظر کاربران در گوگل پلی نگاه کنید، اغلب کاربران برنامه‌هایی دانلود کرده‌اند که پولی، اعتباری و یا چیزی شبیه این‌ها بوده است. تروجان Ztorg تغییر نمی‌کند. پس از نصب آن، این تروجان اطلاعات مربوط به سیستم و دستگاه را جمع آوری و آن‌ها را به سرور command-and-control ارسال می‌کند. سرور به فایل‌هایی که بدافزار را برای به دست آوردن دسترسی بوت به دستگاه قادر ساخته است، واکنش نشان می‌دهد. پس از اینکه این کلاهبرداری انجام شد، آن‌ها می‌توانند هر کاری که دوست داشتند انجام دهند، به عنوان مثال، تبلیغات را نمایان کنند، تروجان‌های دیگری را دانلود کنند و ... . حال Ztorg جزو تروجان هایی است که از طریق تبلیغات گسترش می‌یابد. شما بر روی یک بنر تبلیغاتی کلیک می‌کنید، اپلیکیشن را دانلود، نصب و سپس آلوده می‌شوید. به همین راحتی! توسعه دهندگان Ztorg کاملا غیر عادلانه برخورد می‌کنند، آن هاعملکردهای مخرب را پنهان می‌کنند، به گونه‌ای که کاربر در زمان مطالعه اپلیکیشن متوجه هیچ مورد مشکوکی نمی‌شود. بیشترین بنرهای حاوی بدافزار به صورت مستقیم به صفحه دانلود اپلیکیشن لینک نمی‌شوند بلکه به صفحه‌ای که تغییر مسیر داده است هدایت می‌کند و پس از آن هم به صفحه دیگر. اینقدر این کار ادامه پیدا می‌کند تا کاربر به لینک دانلود می‌رسد. این کار برای گیج شدن کاربر برنامه ریزی شده است. علاوه براین، اپلیکیشن می‌تواند دانلود فایل‌های مخرب را از سرور C&C بیش از ۹۰ دقیقه به تاخیر بیندازد. جای تعجب دارد که چرا فروشگاه رسمی گوگل پلی باید چنین برنامه‌های مخربی را در خود جای دهد. متاسفانه تروجان‌ها در خفا کارهای خود را انجام می‌دهند.