یکشنبه 23 مهر 1396 - 09:13

آلودگی نرم افزار CCleaner

آلودگی نرم افزار CCleaner به تروجان

آلودگی نرم افزار CCleaner به تروجان

محققان امنیتی متوجه شدند که یک نسخه از برنامه محبوب بهبود دهنده سیستم بنام "CCleaner" به نرم افزارهای مخرب آلوده شده است.

در این خبر گزارش، ما نگاهی کوتاه به این مورد خواهیم داشت:

نرم افزار محبوب بهبود دهنده سیستم "CCleaner" حدود یک ماه می باشد که مسافر ناخواسته ای را با خود آورده است. محققان در Talos دریافتند که نسخه موجود در سایت رسمی دانلود شامل یک تروجان است. دو عامل وجود دارد که این مورد را جالب توجه می کند:

مورد اول اینکه، تعداد کاربران زیادی دارد. بر اساس اطلاعات تولید کننده، این نرم افزار در مجموع حدود دو بیلیون بار دانلود داشته و این عدد در حال افزایش است. از این رو، تعداد کاربران آسیب دیده بسیار بالا است. نسخه دستکاری CCleaner نیز با یک گواهی معتبر تائید شده است. این گواهی ها به منظور حصول اطمینان از اینکه یک برنامه از یک فروشنده قابل اعتماد است، می باشند.

بنابراین، کسی با دسترسی به یک گواهی سرقت رفته ، می تواند به جمعیت عظیمی از مخاطبین دسترسی پیدا کند (برنامه های بدون امضا توسط ویندوز اجرا نمی شوند، مگر اینکه با تنظیمات اضافی دستکاری شوند)

کاربران آنتی ویروس G DATA در امنیت می باشند:

نسخه دستکاری شده 5.33 از CCleaner بین 15 اوت و 12 سپتامبر عرضه شد. تمام بسته های امنیتی G DATA این نسخه را Win32.Backdoor.Forpivast.A تشخیص دادند.

یک نسخه اصلاح شده در حال حاضر منتشر شده است. به کاربران دارای نسخه آسیب دیده توصیه می شود به نسخه 5.34 به روز شوند. نسخه های رایگان برنامه به روز رسانی را به صورت خودکار نصب نمی کنند (در این حالت، کاربران باید فایل نصب به روز شده را به صورت دستی دانلود و نصب کنند)

دانلودهای لو رفته یک پدیده جدید نیست!

این واقعیت که نسخه آلوده 5.33 با یک گواهینامه معتبر امضا شده به چندین مسئله امنیتی بالقوه اشاره دارد که میتواند از یک فرایند افشا شده باشد.

با این حال، گسترش نرم افزارهای مخرب که با یک گواهی معتبر یا نسخه های مخرب از برنامه های قانونی که از طریق کانال های رسمی عرضه شده است، به هیچ وجه پدیده جدیدی نیست. در گذشته، مسائل مشابهی برای یک Torrent-Clientبرای Mac و همچنین توزیع لینوکس رخ داد. بدافزار "Petna" از زیرساخت های به روزرسانی یک نرم افزار حسابداری استفاده می کرد.

به نظر می رسد نویسندگان بدافزارها به کارهای بزرگتری دست خواهند زد تا تعداد زیادی از کاربران را در کوتاهترین زمان ممکن آلوده کنند. زنجیره عرضه نرم افزار یک هدف بسیار ارزشمند برای این منظور است.

اگر یک مهاجم موفق شود به زنجیره عرضه یک شرکت نفوذ کند، این عواقب بسیار وخیمی در پی خواهد داشت؛ این هم اتفاقی است که در گذشته رخ داده است.