کد خبر: ۱۰۳۲۰۱۹
سه شنبه ۱۴ آبان ۱۳۹۸ ۸:۰۰

راهکارهایی برای مقابله با خرابکارهای پنهان

برنامه‌ای که از فعالیت رایانه شما جاسوسی می‌کند، یکی از خطرناک‌ترین اشکال بدافزار است. شخص هنگام ورود این مخرب متوجه حذف شدن فایل‌های خود نخواهد شد. آن‌ها بی صدا روی سیستم شما پنهان می‌شوند و تمام فعالیت های شما را مشاهده و ضبط می کند.

به گزارش گروه علم و فناوری ایسکانیوز، نرم‌افزارهای جاسوسی می توانند از ربودن فید وب‌کم گرفته تا ثبت ورودی‌های صفحه کلید را دزدی کنند. آن‌ها این کار را به هدف جمع آوری اطلاعات شخصی برای سرقت هویت، به دست گرفتن حساب ها و یا افشای زندگی دیجیتالی شما انجام می‌دهند. برای به حداقل رساندن شانس برنامه ناخواسته در سیستم‌های خود با ما در این گزارش همراه باشید تا راهکارهایی را برای اینکار ارائه دهیم.

سیستم خود را ایمن کنید

در شروع باید محافظت کاملی برای رایانه خود برقرار کنید. بیشتر برنامه‌های آنتی ویروس برای و در برابر ها، هکرهای وب‌کم و سایر جاسوس‌افزارها محافظت خوبی ارائه می‌دهند، به خصوص اگر این نرم افزار را به‌روز کنید.

یک نرم افزار رایگان برای اکثر رایانه‌های خانگی باید سطح مناسبی از محافظت را ارائه دهد؛ اما پرداخت هزینه برای نسخه به‌روز شده این برنامه شانس ایمن ماندن شما را افزایش می دهد.

در ادامه به ۴ مورد از آنتی ویروس های موثر رایگان که همه آنها نمرات بالایی از محافظت را حتی در مقایسه با برنامه های عالی پولی مانند و دریافت می‌کنند، اشاره می‌کنیم. اگرچه هیچ یک از گزینه های زیر در مبارزه با جاسوس افزارها تخصص ندارند؛ اما همه دارای دفاع در برابر برنامه‌های مخرب هستند.

انتخاب‌های مناسب (همراه با ویندوز ۱۰)، (رایگان برای ویندوز و است، نسخه کامل هزینه سالیانه ۹۰دلار را دارد)، (رایگان برای ویندوز، نسخه به‌روز شده با پشتیبانی و هزینه آن ۹۰ دلار در سال است) و (برای ویندوز و ، نسخه به روز شده به ترتیب ۷۰ و ۶۰ دلار در سال هزینه دارد).

اگر این برنامه‌ها را به نسخه‌های پولی ارتقا دهید، می توانید مواردی مانند اسکن پیوند وب، گزینه‌های جامع‌تر برای جلوگیری از حملات فعال و حافظه امن را داشته باشید.

توصیه می کنیم در کنار محصول اصلی امنیتی محافظت ثانویه را نیز نصب کنید. برای ویندوز به صورت رایگان ارائه شده که در کنار

بسته آنتی ویروس معمولی شما کار می کند و اسکن های عمیق را به عنوان یک لایه اضافی برای دفاع در برابر کدهای مخرب انجام می‌دهد. اگر گمان می کنید رایانه شما از نرم افزارهای جاسوسی رنج می برد؛ اما ابزار آنتی ویروس معمولی شما آن را حل نمی‌کند، سعی کنید با برنامه امنیتی ثانویه ویندوز محافظت عمیق‌تری در سیستم خود برقرار کنید. در همین راستا به عنوان یک اسکنر اضافی در بالای بسته امنیتی فعلی شما عمل می کند و با کنترل مرورگر امکان پوشش هر نوع سیستم عامل را می دهد.

جلوگیری از عفونت

ممکن است حتی با وجود یک برنامه آنتی ویروس قوی نخواهید به جاسوس‌ها فرصتی دهید که در رایانه شما جایگاهی به‌دست آورند. اگر می‌خواهید چشم‌های کنجکاو را از سیستم خود دور نگه دارید باید تمام راه های احتمالی کد مخرب را کنترل کنید.

برای رایانه‌هایی که به صورت مشترک استفاده می شوند، حتما حساب‌های کاربری جداگانه درست کنید. از آن حسابها با گذرواژه محافظت کنید. در ویندوز، این کار را از طریق تنظیمات حساب‌ها و در ، اینکار را از طریق تنظیمات برگزیده سیستم کاربران و گروه ها انجام دهید.

مراقب پیوندهایی که از طریق رسانه‌های اجتماعی یا ایمیل دریافت می کنید، باشید؛ حتی اگر از افرادی که به آنها اعتماد دارید باشد. لینک های کلاهبرداری ممکن است حاوی جاسوس‌افزار باشد.

علاوه بر این، باید مراقب آنچه که در رایانه خود نصب و بارگیری می‌کنید، باشید. اگر می‌خواهید نرم افزار جدیدی امتحان کنید حتماً از قبل راجع به آن تحقیق و برای نصب حتماً آن را از وب سایت رسمی شرکت نرم افزاری که آن را طراحی کرده دریافت کنید. این مساله در مورد اکستنشن‌های مرورگر نیز صادق است. دسترسی این ابزارها به مرورگر می‌تواند امنیت آن را به خطر بیندازد؛ بنابراین موارد اضافی را با دقت آزمایش کنید.

قبل از نصب هر چیزی نظرات کاربران دیگر را مطالعه و در مورد سایت ها مطمئن شوید که دارای تاییدیه حرفه‌ای باشند.

آگاهی از علائم هشدار دهنده

علاوه بر اقدامات احتیاطی فوق الذکر در مورد نفوذ به سیستم خود، مراقب علائم حضور جاسوسی باشید.

زمانی که سیستم شما کند کار می‌کند یک علامت خطر است. البته رایانه های قدیمی با گذشت زمان به تدریج کند می شوند؛ اما افت ناگهانی عملکرد مهم است؛ همچنین به مکث‌های سخت افزاری زیاد هارد دیسک دقت کنید، به خصوص زمانی که رایانه شما برنامه‌های زیادی را اجرا نمی‌کند.

به طور کلی، نسبت به هرگونه رفتار عجیب به خصوص اجرا شدن برنامه هایی که مستقیم باز نکرده‌اید، حساس باشید. بازشدن ناگهانی یک پنجره دوباره ناپدید شدن آن اتفاقی مشکوک است؛ زیرا نشانه بارگذاری برنامه مخرب و سپس مخفی شدن آن است.

هر برنامه جاسوسی و راه اندازی آن در سیستم متفاوت است؛ بنابراین نمی‌توان چک لیست کلی در مورد آن ارائه داد. اما هرچه بیشتر موارد مشکوک را مشاهده کنید احتمال خطر بیشتر است. سایر موارد عجیب و غریب شامل حرکات غیر قابل توضیح ماوس یا درخواست ورود متن، تغییر در تنظیمات سیستم عامل و ظاهرشدن میانبرهای برنامه غیرعادی است.

جاسوس‌افزارها سعی خواهند کرد به طور نامرئی اجرا شوند؛ اما همچنان از حافظه و زمان استفاده می‌کنند. بنابراین بررسی کنید که چه برنامه ها و فرایندهایی روی رایانه شما اجرا می شوند. برای اینکار در ویندوز از استفاده کنید؛ سپس به زبانه ها بروید تا تمام برنامه ها و فرآیندهای موجود در حال استفاده را ببینید. در ، از ابزار مشابه استفاده کنید که با باز کردن (+) و جستجوی آن را پیدا خواهید کرد. در زیر تب ، لیستی از برنامه ها و فرآیندهای موجود در حال اجرا و همچنین میزان منابع سیستم رایانه خود را مشاهده کنید.

ابزارهای مخرب بیشتر اسامی دارند که ممکن است بی حد و حصر به نظر آیند. این بدان معناست که نمی‌توان لیست کاملی از اصطلاحات حاوی جاسوسی را ارائه داد. برای کنار آمدن با این مساله اسامی برنامه‌های کاربردی یا فرآیندهایی که به خاطر نمی‌آورید را در وب جستجو کنید.

خبر خوب این است که حتی وقتی نرم افزارهای جاسوسی هوشمند و پیشرفته تر می‌شوند مرورگرها و سیستم عامل ها نیز دارای ابزارهای امنیتی بیشتری خواهند شد. با وجود این همیشه باید سیستم، برنامه‌ها و ابزارهای امنیتی را با جدیدترین نسخه‌ها به‌روز نگه دارید.

انتهای پیام/