

## 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 فعالیت‌های شما را مشاهده و ضبط می‌کند.

به گزارش گروه علم و فناوری ایسکانیوز، نرم‌افزارهای جاسوسی می‌توانند از ربودن فید وب‌کم گرفته تا ثبت ورودی‌های صفحه کلید را دزدی کنند. آن‌ها این کار را به هدف جمع‌آوری اطلاعات شخصی برای سرقت هویت، به دست گرفتن حساب‌ها و یا افشای زندگی دیجیتال شما انجام می‌دهند. برای به حداقل رساندن شانس برنامه‌ناخواسته 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 آنتی‌ویروس برای و در برابر ها، هکرهای وب‌کم و سایر جاسوس‌افزارها محافظت خوبی ارائه می‌دهند، به خصوص اگر این نرم‌افزار را به‌روز کنید.

یک نرم‌افزار 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 می‌دهد.

در ادامه به ۴ مورد از آنتی‌ویروس‌های موثر رایگان که همه آنها نمرات بالایی از محافظت را حتی در مقایسه با برنامه‌های پولی دارند و دریافت می‌کنند، اشاره می‌کنیم. اگرچه هیچ‌یک از گزینه‌های زیر در مبارزه با جاسوس‌افزارها 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 سالانه ۹۰ دلار را دارد)، (رایگان برای ویندوز، نسخه به‌روز شده با پشتیبانی و هزینه آن ۹۰ دلار در سال است) و (برای ویندوز و ، نسخه به‌روز شده به ترتیب ۷۰ و ۶۰ دلار در سال هزینه دارد).

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

توصیه می‌کنیم 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 می دهد. اگر گمان می کنید رایانه شما از نرم افزارهای جاسوسی رنج می برد؛ اما ابزار آنتی ویروس معمولی شما آن را حل نمی کند، سعی کنید با برنامه امنیتی ثانویه ویندوز محافظت عمیق تری 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 به دست آورند. اگر می خواهید 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 رسانه های اجتماعی یا ایمیل دریافت می کنید، باشید؛ حتی اگر از افرادی که به آنها اعتماد دارید باشد. لینک های کلاهبرداری ممکن است حاوی جاسوس افزار باشد.

علاوه بر این، باید مراقب آنچه که در رایانه خود نصب و بارگیری می کنید، باشید. اگر می خواهید 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 اکستنشن های مرورگر نیز صادق است. دسترسی این ابزارها به مرورگر می تواند 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 حرفه ای 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 می کند یک علامت خطر است. البته رایانه های قدیمی با گذشت زمان به تدریج کند می شوند؛ اما افت ناگهانی عملکرد مهم است؛ همچنین به مکث های سخت افزاری زیاد هارد دیسک دقت کنید، به خصوص زمانی که رایانه شما برنامه های زیادی را اجرا نمی کند.

به طور کلی، نسبت به هرگونه رفتار عجیب به خصوص اجرا شدن برنامه هایی که مستقیم باز نکرده اید، حساس باشید. باز شدن 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 ظاهر شدن میانبرهای برنامه غیرعادی است.

جاسوس افزارها سعی خواهند کرد به طور نامرئی اجرا شوند؛ اما همچنان از حافظه و زمان استفاده می‌کنند. بنابراین بررسی کنید که چه برنامه‌ها و فرآیندهایی روی رایانه شما اجرا می‌شوند. برای اینکار در ویندوز از استفاده کنید؛ سپس به زبانه‌ها بروید تا تمام برنامه‌ها 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 برنامه‌ها و فرآیندهای موجود در حال اجرا و همچنین میزان منابع سیستم رایانه خود را مشاهده کنید.

ابزارهای مخرب بیشتر اسامی دارند که ممکن است بی‌حد 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 نرم افزارهای جاسوسی هوشمند و پیشرفته تر می‌شوند مرورگرها و سیستم عامل‌ها 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/