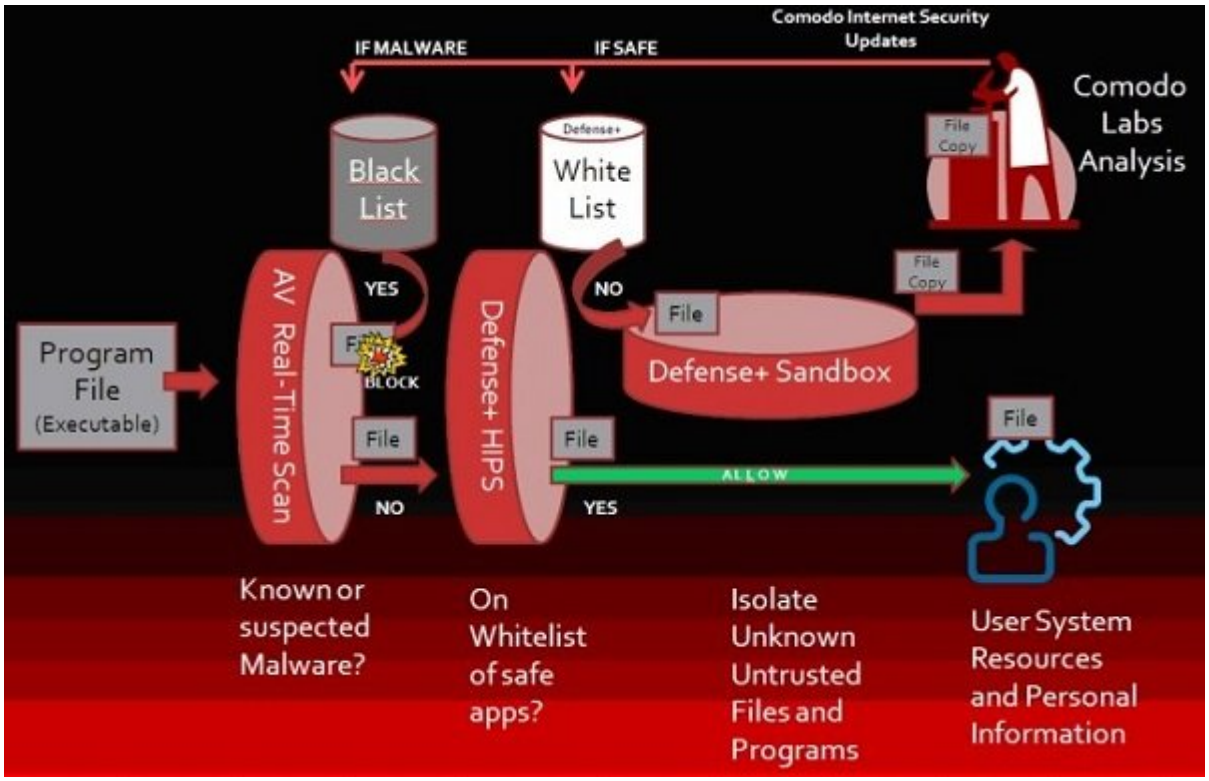
راهنمای آشنایی با ضدویروس‌ها

ضدویروس‌ها چگونه کار می‌کنند و بهترین ضدویروس را چگونه انتخاب کنیم؟

ضدویروس‌ها در زمان پویش رایانه‌تان، بخش‌های خاصی از کدهای درون فایل‌ها را با اطلاعاتی که درون پایگاه داده‌ای خود دارند، مقایسه کرده و اگر شباهتی میان دو قطعه کد پیدا کنند، فایل را آلوده به ویروس در نظر می‌گیرند. در این مرحله ضدویروس بر مبنای خط‌مشی‌هایی که برایش ترسیم شده یا فایل را پاک می‌کند یا آن را در وضعیت قرنطینه قرار می‌دهد. اما ضدویروس‌ها چگونه قادر به پیدا کردن ویروس‌ها هستند و بر مبنای چه ضوابط و معیارهایی باید یک ضدویروس خوب را انتخاب کرد. در این مقاله به بیانی ساده به دو پرسش مطرح‌شده پاسخ داده‌ایم.

ویروس‌ها چگونه توسط ضدویروس‌ها شکار می‌شوند؟

هر زمان یک برنامه یا به عبارت دقیق‌تر یک فایل اجرایی به سامانه‌ای وارد می‌شود، ضدویروس آن را پویش می‌کند. فایل‌های اجرایی که درون آن‌ها کدهایی وجود دارد که امضا آن‌ها با نمونه کدهایی که درون پایگاه داده یک برنامه ضدویروس قرار دارد، یکسان است، به‌عنوان یک فایل ویروسی شناخته‌شده و طبقه‌بندی می‌شوند. ضدویروس به فایل‌های اجرایی عاری از مشکل اجازه می‌دهد از سیستم دفاعی و سامانه ممانعت از حمله به میزبان موسوم به HIPS + Defense (سرنام Host Intrusion Prevention System) عبور کنند. ضدویروس به فایل‌های شناخته شده اجازه می‌دهد، در سیستم اجرا شوند (فایل‌های سیستمی و فایل‌های متعلق به نرم‌افزارهای شناخته شده)، اما مانع از آن می‌شود تا فایل‌های ناشناخته صرف‌نظر از سالم یا ناسالم بودن روی یک سیستم اجرا شوند، در این حالت فایل‌های فوق به سامانه دفاعی ضدویروس که به آن جعبه شن گفته می‌شود، هدایت می‌شوند. در این مرحله اگر کاربر مشخص کند که فایل‌های ایزوله شده بدون مشکل هستند، به فهرست سفید ضدویروس افزوده خواهند شد، درحالی‌که سایر فایل‌های انتقال پیدا کرده به جعبه شن برای بررسی‌های بیشتر به سرور شرکت سازنده ضدویروس انتقال پیدا خواهند کرد. برای روشن شدن بهتر این موضوع به شکل 1 دقت کنید. در شکل 1، فرآیند ورود یک فایل اجرایی را به سامانه‌ای که ضدویروس کومودو روی آن نصب‌شده، مشاهده می‌کنید که چگونه ضدویروس فوق از یک مکانیزم سخت‌گیرانه برای بررسی دقیق فایل‌های اجرایی استفاده می‌کند. درست است که عملکرد ضدویروس پیچیده است، اما فرآیندهای نشان داده شده در این عکس به استثنا زمانی که فایل برای تحلیل بیشتر برای آزمایشگاه ارسال می‌شود، در کسری از ثانیه انجام می‌شوند.



.1 □□□
□□ □□□□
□□□□□□□
□□□
□□□□□□□
□ □□ □□
□□□□□□□
□□□□
□□□□
□□□□
□□□□□□
□□
□□□□□□
□□□□□□□
□□ □□□
□□ □□
□□□ □□
□□□□□.

قابلیت‌های رایج ضدویروس‌ها

هر شرکت تولیدکننده نرم‌افزارهای امنیتی قابلیت‌های خاص خود را به بسته‌های امنیتی ازجمله ضدویروس اضافه می‌کند، اما برخی از قابلیت‌ها در همه ضدویروس‌ها مشترک هستند که از آن جمله می‌توان به پویش در پس‌زمینه سیستم‌عامل، پویش کامل سیستم و پایگاه اطلاعاتی درباره ویژگی‌های ویروس‌ها اشاره کرد.

پویش در پس‌زمینه سیستم‌عامل

ضدویروس‌ها فایل‌های باز و اجرا شده از سوی کاربر یا سیستم‌عامل را به‌طور خودکار در پس‌زمینه پویش می‌کنند. راهکار فوق به یک ضدویروس اجازه می‌دهد، یک لایه محافظتی بلادرنگ پیرامون سیستم‌تان به وجود آورده و به‌این‌ترتیب از سامانه‌تان در برابر تهدیدات محافظت می‌کند.

پویش کامل سامانه

سامانه‌هایی که نرم‌افزار ضدویروس روی آن‌ها در وضعیت محافظت بلادرنگ تنظیم شده است، لزومی به پویش کامل سامانه ندارند. پویش کامل سیستم زمانی که ضدویروس برای اولین بار روی سامانه‌ای نصب می‌شود یا بانک‌اطلاعاتی ضدویروس به‌تازگی به‌روز شده یا زمانی که سامانه مشکوک به آلودگی است یا نرم‌افزار مخربی روی آن نصب شده است، باید انجام شود. به‌عنوان‌مثال، کاربران ساکن در ایران به دلایل مختلفی از نرم‌افزارهای اصلی استفاده نمی‌کنند. در نتیجه به سراغ دانلود نرم‌افزارهایی می‌روند که قفل آن‌ها شکسته شده و فایل کرک درون یک فایل آرشیو قرار دارد. با توجه به این‌که نرم‌افزارهای ضدویروس به فایل‌های کرک حساس هستند، به‌محض دانلود فایل یا باز کردن یک فایل آرشیو آن را پویش کرده و چنین فایل‌هایی را پاک می‌کنند. به همین دلیل، کاربران نرم‌افزار ضدویروس سامانه خود را به‌طور موقتی غیرفعال می‌کنند تا فرآیند از آرشیو خارج کردن و فعال‌سازی نرم‌افزار به‌درستی انجام شود. اما اگر در چنین شرایطی بدافزاری درون فایل آرشیو قرار گرفته باشد، بدون اطلاع سامانه شما را آلوده می‌کند. بدافزار Neshta.C چند وقتی است شناسایی شده و گونه‌های مختلفی از آن منتشر شده، با این روش روی سامانه قربانیان نصب شده و مانع از اجرا شدن هرگونه فایل اجرایی روی سیستم کاربر می‌شود. زمانی که ضدویروس را غیرفعال کرده و فایلی از بستر اینترنت دانلود می‌کنید، بهتر است سامانه خود را به‌طور کامل پویش کنید.

مطلب پیشنهادی

دو ابزار مکمل یا رقیب
ضدویروس یا ضدبدافزار ،کدام‌یک را باید انتخاب کنیم؟

پایگاه اطلاعاتی متشکل از نمونه امضاهای ویروس‌ها

ضدویروس‌ها به پایگاه‌های اطلاعاتی خود موسوم به Virus Definitions برای شناسایی بدافزارها و ویروس‌ها وابسته هستند. به همین دلیل مهم است که این پایگاه داده‌ای به‌طور منظم به‌روز شود. پایگاه داده‌ای، مشخصات و خصایص ویروس‌ها و بدافزارها را طبقه‌بندی می‌کند که این طبقه‌بندی بر مبنای قواعد مشخص و بر مبنای خطرناک بودن ویروس‌ها انجام می‌شود.
اگر ضدویروس در زمان پویش فایل‌ها و برنامه‌ها با قطعه کدهایی روبه‌رو شود که مشخصات آن‌ها درون این پایگاه داده‌ای وجود داشته باشد، مانع از اجرای فایل شده و آن را قرنطینه می‌کند. اگر فایل از بستر اینترنت دانلود شده باشد، ضدویروس پیش از آن‌که فایل به‌طور کامل روی هارددیسک قرار بگیرد، آن را پویش کرده و اگر آلودگی پیدا کند، پیشنهاد می‌دهد کاربر از داشتن فایل صرف‌نظر کند تا بتواند آن را پاک کند. لازم به توضیح است واکنش ضدویروس‌ها در مواجه شدن با یک فایل آلوده با یکدیگر یکسان نیست.

شیوه برخورد با بدافزارها چگونه است؟

اصلی‌ترین وظیفه ضدویروس‌ها، مقابله با ویروس‌ها است، اما برخی از آن‌ها برای مقابله با بدافزارها راهکارهایی دارند که از آن جمله می‌توان به فرآیند تشخیص بر مبنای شناسایی بدافزار با اتکا بر پایگاه داده ضدویروس‌ها، شناسایی با اتکا بر یادگیری ماشین، شناسایی از طریق تحلیل و پیش‌بینی رفتار بدافزار، شناسایی بر مبنای فناوری جعبه شن و تکنیک‌های استخراج اطلاعات اشاره کرد.

شناسایی با اتکا بر پایگاه داده

این نوع شناسایی متداول‌ترین روشی است که برای شناسایی بدافزارها انجام می‌شود. این تکنیک مشابه شناسایی ویروس‌ها بوده و از طریق پویش همه فایل‌های اجرایی و بررسی آن‌ها با اطلاعات درون پایگاه داده انجام می‌شود. در این حالت هرگونه کد غیرمعمولی به‌عنوان یک تهدید شناخته شده و کد آن درون پایگاه داده ثبت می‌شود تا برای بررسی بیشتر برای سرورهای شرکت سازنده ارسال شوند. برخی از ضدویروس‌ها این کار را با اجازه کاربر انجام می‌دهند، درحالی‌که برخی دیگر بدون اطلاع داده‌های فوق را ارسال می‌کنند. ضدویروس‌ها در حالت عادی زمانی که فایل‌ها و برنامه‌ها اجرا شوند آن‌ها را پویش می‌کنند، اما در مورد فایل‌های دانلود شده از بستر اینترنت این کار به شکل آنی انجام می‌شود.

مطلب پیشنهادی

گوشی شما مخزن اسرار شما است، در حفظ آن کوشا باشید
چگونه از تلفن هوشمند خود در مقابل هکرها محافظت کنیم

شناسایی با اتکا بر یادگیری ماشین

شناسایی مبتنی بر یادگیری ماشین در تعامل با پایگاه داده ضدویروس فرآیند پویش را انجام می‌دهد. فناوری فوق که نسل جدید دیوارهای آتش به آن متکی هستند، به ضدویروس اجازه می‌دهد گونه‌های جدید یا نگارش‌های تغییر یافته بدافزارها را حتی زمانی که اطلاعات آن‌ها درون پایگاه داده ثبت نشده، شناسایی کنند. این فناوری برای تشخیص بدافزارها و برنامه‌های مخرب از رویکرد شبیه‌سازی استفاده می‌کند تا کدهای مخرب موفق نشوند رایانه کاربر را آلوده کنند.

شناسایی با اتکا بر تحلیل رفتار بدافزارها

این روش از تکنیک تشخیص نفوذ برای شناسایی استفاده می‌کند و برای شناسایی خصایص بدافزارهایی که در حال اجرا هستند، متمرکز است. این فناوری تنها زمانی که بدافزار روی سامانه‌ای در حال اجرا باشد، آن را شناسایی می‌کند.

شناسایی با اتکا بر جعبه شن

این فناوری در اغلب موارد در تعامل با سایر روش‌ها برای شناسایی بدافزارها استفاده می‌شود. عملکرد فناوری جعبه شن به این صورت است که فایل اجرایی به درون یک محیط ایزوله و شبیه‌سازی شده هدایت شده، در آن محیط اجرا شده و رفتار فایل ارزیابی می‌شود. در این محیط ضدویروس هرگونه فعالیت مخرب یا مشکوکی را بررسی می‌کند. اگر مورد خاصی وجود نداشته باشد، اجازه می‌دهد فایل روی یک سامانه در دسترس قرار گیرد.

تکنیک‌های داده‌کاوی

تکنیک داده‌کاوی جزو جدیدترین روش‌هایی است که برای شناسایی بدافزارها استفاده می‌شود. در این روش هرگونه فعالیت مشکوک و خارج از عرف فایل‌ها و برنامه‌ها بررسی می‌شود تا بدافزارها شناسایی شوند.
به‌عنوان‌مثال، بدافزارهای کاملا حرفه‌ای قادر هستند از تکنیک‌هایی همچون جعبه شن بدون مشکل عبور کنند و حتی برای مدت‌های طولانی یک رفتار عادی از خود نشان دهند و پس از گذشت مدت زمانی فعالیت‌های مخرب خود را به‌تدریج آغاز کنند.

چگونه بهترین ضدویروس را انتخاب کنیم؟

همان‌گونه که اشاره شد، هر ضدویروسی عملکرد خاص خود را داشته و قابلیت‌های مختلفی را ارائه می‌کند. بخش عمده‌ای از کاربران ایرانی سیستم‌عامل ویندوز را به‌عنوان سیستم‌عامل اصلی و کاری خود در نظر گرفته‌اند. برای این گروه از کاربران بهترین ضدویروسی که پیشنهاد می‌شود، ضدویروس بیت‌دیفندر است. چرا؟ به این دلیل که بیشترین تعداد بدافزار را نسبت به سایر ضدویروس‌ها شناسایی کرده، مانع از باز شدن فایل‌ها و پیوندهای مخرب شده، در زمان باز کردن سایت‌های مخرب به شما هشدار داده، یک امحاءکننده کاملا قدرتمند فایل‌ها را ارائه کرده و به یک فیلتر اطلاعات شخصی تجهیز شده است. بیت‌دینفدر کاملا سبک و روان طراحی‌شده و حتی زمانی‌که روی سیستم خود یک برنامه سنگین همچون یک بازی را اجرا کنید، بازهم بدون مشکل به کار خود ادامه می‌دهد.

ایده‌آل‌ترین ضدویروس برای گوشی‌های همراه

رشد روزافزون دستگاه‌های همراه باعث شده تا هکرها بدافزارها و ویروس‌های خاصی را برای دسترسی به گوشی‌های همراه، شنود اطلاعات کاربران و سرقت اطلاعات شخصی طراحی کنند. در حالت ایده‌آل و در صورت امکان پیشنهاد می‌شود برای دستگاه‌های همراه خود ضدویروس‌ها را همراه با لایسنس خریداری کنید تا مطمئن شوید اطلاعات‌تان و به‌ویژه تراکنش‌های مالی به شیوه ایمنی انجام می‌شوند. برخی از شرکت‌ها هر دو نسخه همراه و دسکتاپ ضدویروس‌ها را درون یک بسته واحد ارائه می‌کنند.
به‌عنوان‌مثال، با خرید ضدویروس Avast به نسخه رایگان ضدویروس ذکر شده دسترسی خواهید داشت و قادر خواهید بود هر دستگاه متصل به اینترنت را به آن تجهیز کنید. نسخه همراه همانند نسخه دسکتاپ ویژه سیستم‌عامل ویندوز در شناسایی بدافزارها، روت‌کیت‌ها و حتی ایمیل‌های جعلی عملکرد قابل قبولی دارد.

بهترین ضدویروس برای تراکنش مالی

ضدویروس‌های حرفه‌ای قابلیت‌های خاصی در اختیار کاربران قرار می‌دهند تا فارغ از هرگونه نگرانی تراکنش‌های مالی روزانه را انجام دهند. کسپرسکی، یکی از نام‌های شناخته شده در این زمینه است. ابزارها و قابلیت‌های ارائه شده از سوی ضدویروس این شرکت می‌توانند از اطلاعات حساس مالی شما زمانی‌که از کارت‌های اعتباری یا نرم‌افزارهای بانکی استفاده می‌کنید، محافظت کنند. اگر ضدویروس نصب شده روی سامانه به ابزارهای محافظت از بانکداری الکترونیکی تجهیز شده باشند، هکرها نمی‌توانند به‌سادگی اطلاعات حساس مالی را به سرقت ببرند. به‌عنوان‌مثال، صفحه‌کلید مجازی کسپرسکی اجازه می‌دهد به ایمن‌ترین شکل گذرواژه و نام کاربری را درون فیلدهای مربوط وارد کنید. این صفحه‌کلید مانع از آن می‌شود تا بدافزارهای رُباینده کلیدها (کی‌لاگرها) بتوانند کلیدهای تایپ شده را ربایش

کرده و به حساب‌های کاربری‌تان دسترسی پیدا کنند. کسپرسکی می‌تواند ایمیل‌های جعلی را که به‌طور مکرر از شما درباره وارد کردن جزئیات حساب‌های بانکی سوال می‌کنند، شناسایی کرده و آن‌ها را بلوکه کند.

مطلب پیشنهادی

مشابه‌ای برای انگل‌های دنیای واقعی
کرم اینترنتی چیست و چه خطراتی با خود به همراه دارد

بهترین ضدویروس برای عاشقان بازی‌های آنلاین

بازی‌های آنلاین به‌شدت نزد کاربران ایرانی محبوب شده است. به تدریج فرهنگ استفاده از سرویس‌های ابری و برنامه‌های مستقر در ابر در حال فراگیر شدن است و انجام بازی‌های آنلاین از این قاعده مستثنا نیستند.
ضدویروس‌هایی که معرفی کردیم، همگی یک قابلیت پویش بلادرنگ در اختیارتان قرار می‌دهند. اما قابلیت فوق برای انجام بازی‌های آنلاین چندان جالب نیست، زیرا پویش‌های مداوم ممکن است سرعت سیستم را کاهش داده و مهم‌تر از آن هشدارهای متعددی برای کاربران ارسال کند. برای این گروه از کاربران ضدویروس‌هایی که ویژگی‌های سکوت (Silent) یا بازی (Gaming) دارند، پیشنهاد می‌شود.
این مدل ضدویروس‌ها می‌توانند پویش‌ها و هشدارها را زمانی که سامانه کاربر به شدت مشغول است، غیرفعال کنند تا سیستم به‌واسطه این پویش‌ها کند نشده و همچنین درجه حرارت قطعات بیش‌ازاندازه افزایش پیدا نکند. آویرا یکی از بهترین ضدویروس‌هایی است که حالت بازی در آن قرار گرفته و در زمان انجام بازی‌های آنلاین هیچ‌گونه دردسری برای کاربر به وجود نمی‌آورد. آویرا، در مقایسه با نمونه‌های مشابه یک ویژگی شاخص دارد. آویرا ویژگی فوق را به شکل خودکار فعال می‌کند، زیرا درون بانک اطلاعاتی ضدویروس آدرس سایت‌ها و سرورهای مجاز بازی قرار گرفته است. البته امکان اضافه کردن سایت‌ها به شیوه دستی نیز وجود دارد.

بهترین ضدویروس‌ها برای پلتفرم مک

بیشتر ضدویروس‌ها برای پلتفرم ویندوز عرضه شده‌اند، بااین‌حال نسخه ویژه کامپیوترهای مک برخی از آن‌ها در دسترس است. ضدویروس‌هایی که رویکرد چندسکویی دارند، روی هر دو پلتفرم عملکرد خوبی دارند، اما تجربه نشان داده ضدویروس‌هایی که برای یک پلتفرم خاص طراحی شده‌اند، کارایی به‌مراتب بهتری دارند. ضدویروس Intego یکی از بهترین ضدویروس‌هایی است که برای سیستم‌عامل مک ارائه شده است. ضدویروس فوق به شکل بلادرنگ یک سامانه را پویش کرده و قبل از آن‌که بدافزارها شانس آلوده‌سازی یک سامانه را پیدا کند، آن‌ها را پاک می‌کند.

بهترین ضدویروس‌های رایگان

ضدویروس رایگان برای افرادی که توانایی خرید لایسنس‌های تجاری ندارند، مناسب است. به‌طورکلی، ضدویروس‌هایی که در این گروه قرار می‌گیرند به‌طور خودکار یک سامانه را پویش نکرده و مکانیزم حفاظتی بلادرنگ را ارائه نمی‌کنند. همچنین از سامانه کاربر در برابر سایت‌های مخرب محافظت نمی‌کنند، زیرا فاقد افزونه‌هایی هستند که باید روی مرورگر کاربر نصب شوند. فراموش نکنید بیشتر ضدویروس‌های رایگان تبلیغات متعددی را نشان می‌دهند که به‌مرور زمان آزاردهنده هستند. متاسفانه برخی از نمونه‌های رایگان فاقد پشتیبانی شرکت هستند که خود یک عیب بزرگ به شمار می‌رود.
در کنار معایبی که به آن‌ها اشاره شد، هنوز هم ضدویروس‌های رایگان یک ابزار مناسب برای محافظت از سامانه‌ها هستند. ضدویروس AVG یکی از بهترین گزینه‌های رایگان است. این ضدویروس به قابلیت‌های حفاظتی ویژه‌ای تجهیز شده که نمونه‌های رایگان فاقد چنین قابلیتی هستند. برای مثال، نرم‌افزار بهینه‌ساز سامانه‌ها، پشتیبانی از طریق ایمیل و پویش‌گر فایل‌هایی که قابلیت نصب روی حافظه‌های فلش را دارد از جمله نقاط مثبت این ضدویروس رایگان هستند. از دیگر قابلیت‌های این ضدویروس می‌توان به مراحل نصب ساده، توانایی شناسایی طیف گسترده‌ای از ویروس‌ها، رابط کاربری روان، پویش زمان‌بندی شده و کامل اشاره کرد.

یک ضدویروس خوب را چگونه تشخیص دهیم؟

بهترین روش برای انتخاب یک ضدویروس خوب، بررسی رتبه ضدویروس و توجه به یکسری معیارهای کلیدی است. اولین فاکتوری که باید به آن دقت کنید، قدرت ضدویروس در شناسایی، بلوکه کردن و از بین بردن تهدیدات است؛ دومین فاکتور توانایی ضدویروس در حذف به موقع بدافزارها است. ضدویروس تنها زمانی که فهرستی از همه بدافزارهای شناخته شده در اختیار داشته باشد قادر است به‌سرعت بدافزارها را پاک کند؛ سومین فاکتوری که باید به آن دقت کنید، میزان مصرف منابع سخت‌افزاری است.
ضدویروس‌هایی که فشار سنگینی به یک سیستم وارد کنند، باعث می‌شوند تا سرعت سیستم کاهش پیدا کرده و منابع مهمی همچون حافظه اصلی و پردازنده به‌سرعت مصرف شوند؛ چهارمین فاکتوری که باید به آن توجه داشته باشید در ارتباط با نوع تهدیداتی است که یک ضدویروس قادر به شناسایی آن‌ها است.
برای مثال، برخی از ضدویروس‌ها ضمن شناسایی ویروس‌ها توانایی شناسایی روت‌کیت‌ها، کی‌لاگرها و حتی باج‌افزارها را دارند؛ پنجمین فاکتور ابزارهای مکملی است که همراه با ضدویروس ارائه می‌شوند. برای مثال ضدویروس‌های حرفه‌ای ابزارهای کنترلی در اختیار والدین قرار می‌دهند تا فرزندان به سایت‌های غیرمجاز دسترسی نداشته باشند. برخی دیگر ابزارهای مدیریت گذرواژه، بهینه‌سازی سیستم و حذف همیشگی فایل‌ها را ارائه می‌کنند؛ ششمین فاکتور به حداقل هشدارهای کاذب باز می‌گردد. یک ضدویروس حرفه‌ای تنها به تهدیدات جدی و واقعی پاسخ می‌دهد

منبع:
comodo
toptenreviews
تاریخ انتشار:
26 مرداد 1398

نشانی منبع:
https://www.shabakeh-mag.com/security/15921/%D8%B6%D8%AF%D9%88%DB%8C%D8%B1%D9%88%D8%B3%E2%80%8C%D9%87%D8%A7-%DA%86%DA%AF%D9%88%D9%86%D9%87-%DA%A9%D8%A7%D8%B1-%D9%85%DB%8C%E2%80%8C%E2%80%8C%DA%A9%D9%86%D9%86%D8%AF-%D9%88-%D8%A8%D9%87%D8%AA%D8%B1%DB%8C%D9%86-%D8%B6%D8%AF%D9%88%DB%8C%D8%B1%D9%88%D8%B3-%D8%B1%D8%A7-%DA%86%DA%AF%D9%88%D9%86%D9%87-%D8%A7%D9%86%D8%AA%D8%AE%D8%A7%D8%A8-%DA%A9%D9%86%DB%8C%D9%85%D8%9F