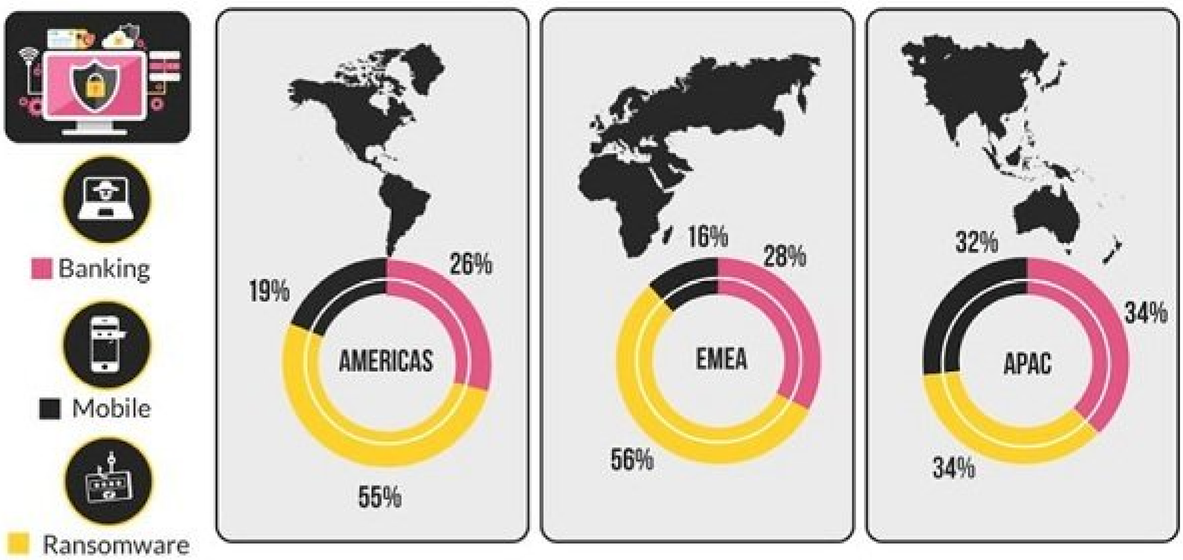
دو ابزار مکمل یا رقیب

ضدویروس یا ضدبدافزار ،کدام‌یک را باید انتخاب کنیم؟

هر زمان صحبت از امنیت سایبری به میان می‌آید، برخی از کاربران این پرسش‌ها را مطرح می‌کنند که بهترین ابزار دفاعی برای محافظت از سامانه‌های سازمانی و شخصی چیست؟ آیا نصب یک ضدبدافزار یا ضدویروس به تنهایی کافی است؟ نصب هم‌زمان دو ابزار امنیتی تداخلی به وجود نمی‌آورد؟ بهترین بسته امنیتی ارائه شده متعلق به چه شرکتی است؟ و ده‌ها سوال دیگر که پیرامون این مبحث قرار دارند. در این مقاله قصد داریم به بیانی ساده به این پرسش پاسخ دهیم تا خوانندگان با ذهنی روشن ابزار موردنیاز خود را انتخاب کنند.

گزارش شرکت‌های امنیتی بیانگر این موضوع است که حملات بدافزاری رو به افزایش است و ما برای محافظت از سامانه‌های خود به برنامه‌های امنیتی قدرتمندی نیاز داریم. پیاده‌سازی کمپین‌های پیچیده فیشینگ که حتی مجرب‌ترین کاربران را فریب می‌دهند از یک سو و نرم‌افزارهایی که هیچ‌گونه وصله‌ای برای برطرف‌کردن آسیب‌پذیری‌های آن‌ها نصب نشده از سویی دیگر، تنها ذره‌ای از مشکلات پیش روی سازمان‌ها هستند. پژوهش‌های انجام شده نشان می‌دهند، حملات سایبری در چند سال گذشته رشد چشمگیری داشته‌اند و انتظار می‌رود این نرخ رشد همچنان پایدار باشد. (شکل 1)



1.

[illegible].

یک حمله بدافزاری قدرتمند به راحتی سازمان‌ها و کاربران زیادی را قربانی می‌کند. حمله‌ای که باعث به سرقت رفتن اطلاعات زیادی می‌شود و مشکلات مالی یا تداخل در انجام تراکنش‌های مالی به‌وجود می‌آورد. بهترین راهکار مقابله با حملات آنلاین به‌کارگیری بسته‌های امنیتی قدرتمند است. بسته‌های امنیتی می‌توانند در قالب یک محصول یکپارچه یا ترکیبی از یک **ضدویروس** و **ضدبدافزار** یا ترکیبی از هر دو حالت روی سامانه‌ها نصب شوند. هر زمان صحبت از نصب یک محصول امنیتی به میان می‌آید، بیشتر مردم تصور می‌کنند، دو اصطلاح ضدویروس و ضدبدافزار به یک مفهوم واحد اشاره دارند، در حالی که شرح وظایف هر یک از این ابزارها مشخص است. اما کدام‌یک گزینه بهتری برای نصب روی سامانه‌مان است؟ برای انتخابی درست داشتن باید تفاوت‌ها، نقاط قوت و ضعف هر یک از ابزارها را به درستی بشناسید و بدانید هر یک از این ابزارها برای پاسخ‌گویی به چه مشکلی استفاده می‌شوند.

ضدویروس چیست و چگونه کار می‌کند؟

قبل از آن‌که به بررسی تفاوت‌های یک **ضدویروس** و بدافزار بپردازیم، در ابتدا به این مسئله اشاره می‌کنیم که ویروس و بدافزار چه تفاوتی با یکدیگر دارند؟
ویروس کامپیوتری: یک قطعه نرم‌افزاری با قابلیت خود تکثیری که برای آسیب‌رساندن به کامپیوترها و سامانه‌های اطلاعاتی از آن استفاده می‌شود. اینترنت، دانلودها، ضمیمه‌های ایمیلی آلوده، فایل‌ها و اسناد اصلی‌ترین راه‌های شیوع ویروس‌ها هستند.
بدافزار: نرم‌افزاری که با هدف تخریب ساخته می‌شود. پیام‌های تبلیغاتی مزاحم، کرم‌ها، تروجان‌ها، باج‌افزارها همگی در زیرمجموعه بدافزارها طبقه‌بندی می‌شوند. هر ویروس رایانه‌ای می‌تواند یک بدافزار باشد، در حالی که هر بدافزاری نمی‌تواند یک ویروس باشد. **ضدویروس**، نرم‌افزاری است که با هدف محافظت از سامانه‌ها در برابر ویروس‌های کامپیوتری طراحی شده است. اما به دلیل این‌که دنیای سایبری با انواع مختلفی از تهدیدها و بدافزارها روبه‌رو است، دامنه فعالیت **ضدویروس‌ها** گسترش پیدا کرده است. **ضدویروس‌ها** می‌توانند، تروجان‌ها، بدافزارهای روباینده کلیدها، روت‌کیت‌ها، حملات فیشینگ و بات‌نت‌ها (با عملکرد محدود) را شناسایی کنند. **ضدویروس‌ها** در برخی موارد یک برنامه **ضدبدافزاری** نامیده می‌شوند و مردم به اشتباه فکر می‌کنند که **ضدویروس‌ها** می‌توانند هر نوع بدافزاری را شناسایی کنند، در حالی که این‌گونه نیست. **ضدویروس‌ها** نمی‌توانند هر نوع آلودگی را شناسایی کنند و در شناسایی اشکال پیشرفته‌تر بدافزارها با مشکل روبه‌رو می‌شوند. اما در نقطه مقابل **ضدبدافزارها** چنین مشکلی را ندارند.

مطلب پیشنهادی

ناشناخته، اما قدرتمند و کاربردی
پنج ابزار جادویی امنیتی که هیچ‌گاه روی سیستم خود نصب نکرده‌اید

قابلیت‌های اصلی یک برنامه ضدویروس چیست؟
پویش سامانه‌ها برای پیدا کردن ویروس‌ها (Virus Scanning):

این فرآیند در پس‌زمینه انجام شده و یک برنامه یا فایل تنها زمانی باز می‌شود که **ضدویروس** به‌طور کامل سامانه شما را پویش کرده باشد. بیشتر **ضدویروس‌ها** ویژگی پویش بلادرنگ را ارائه می‌کنند، در نتیجه در کمترین زمان ممکن از وجود فایل‌های مخرب روی سامانه خود آگاه خواهید شد.

مسدود کردن و ممانعت از اجرای فایل‌های اسکریپتی مخرب(Blocks Malicious Script Files And Prevent Them From Running):

اسکریپت‌های مخرب راه را برای ورود انواع مختلفی از تهدیدات هموار می‌کنند. در بیشتر موارد این اسکریپت‌ها با ایجاد یک در پشتی به هکرها اجازه می‌دهند انواع مختلفی از فایل‌های مخرب را به درون سامانه‌تان وارد کنند.

تحلیل اکتشافی (Heuristic analysis):

بیشتر نرم‌افزارهای **ضدویروس** از این تکنیک برای شناسایی ویروس‌هایی که هنوز شناسایی نشده‌اند یا گونه‌های مختلفی از ویروس‌های یک خانواده استفاده می‌کنند. در اغلب موارد **ضدویروس‌ها** مجبورند نشانه‌ها یا رفتارهای مشکوکی را که شناسایی کرده‌اند برای شرکت تولیدکننده نرم‌افزار ارسال کنند تا کارشناسان امنیتی نشانه‌ها را بررسی کنند.

به‌روزرسانی خودکار (Automatic Updates):

برای نوسازی بانک اطلاعاتی **ضدویروس** برای ردیابی و تشخیص تهدیدات جدیدی که در زمان نصب **ضدویروس** هنوز کشف نشده‌اند، استفاده می‌شود.

حذف بدافزار (Malware Removal):

به این دلیل مهم است که **بدافزارها** انواع متنوع و زیادی دارند که هر یک صدمات جبران‌ناپذیری وارد می‌کنند. بیشتر **ضدویروس‌های** رایگان با هدف شناسایی و قفل کردن بدافزارها ساخته می‌شوند و قابلیت حذف بدافزارها را از روی سامانه‌ها ندارند. کاربران برای حذف **بدافزارها** مجبور هستند نسخه حرفه‌ای **ضدویروس‌ها** را خریداری کنند.

بانک اطلاعاتی بدافزارهای شناخته شده (Database Of Known Malware):

شامل اطلاعاتی در ارتباط با بدافزارهای شناخته شده است. **ضدویروس‌ها** هر فایل را با محتویات این بانک اطلاعاتی مقایسه می‌کنند تا مطمئن شوند فایل‌های یک سامانه آلوده نیستند.

محافظت در برابر باج‌افزارها(Ransomware Protection):

قابلیتی که بیشتر در ضدویروس‌های تجاری قرار دارد و مانع از رمزگذاری فایل‌ها از سوی باج‌افزارها می‌شود. این قابلیت هرگونه مورد مشکوک شناسایی‌شده‌ای را که قصد ویرایش فایل‌ها را داشته باشد یک فعالیت خطرناک تعبیر کرده و مانع اجرای این‌کار می‌شود.
ضدویروس‌ها در بیشتر موارد چهار قابلیت محافظت در برابر حملات فیشینگ، محافظت از مرورگرها در برابر حملات XSS، پویش سامانه‌ها به لحاظ وجود آسیب‌پذیری‌ها و بهینه‌سازی سیستم را
ارائه می‌کنند.

ضدبدافزار چیست و چگونه کار می‌کند؟

یک محصول **ضدبدافزاری** راه‌حل‌های متنوعی همچون قابلیت‌های ضدجاسوسی، ضدفیشینگ، ضدهرزنامه و مقابله با تهدیدات روزصفر را در قالب یک بسته واحد در اختیارتان قرار می‌دهد. در حالت کلی، یک **ضدبدافزار** خوب شامل قابلیت‌های زیر است:

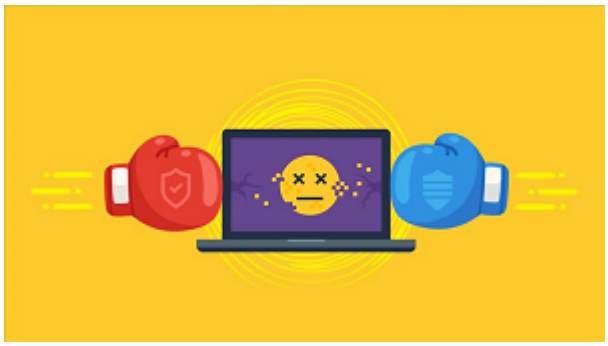
- پویش، شناسایی و حذف تروجان‌های کشف شده، مقابله با پیام‌های تبلیغاتی مزاحم، جاسوس‌افزارها و سایر تهدیدات بدافزاری پیشرفته
- محافظت از سامانه‌ها در برابر نسل دوم تهدیدات بدافزاری

- حذف بدافزارها بدون مشکل خاصی
- به‌روزرسانی خودکار برای تشخیص ساده تهدیدات آنلاین
- مسدود کردن دسترسی به سرورها و سایت‌های آلوده و محدود کردن ترافیک اینترنت در زمان شناسایی یک رفتار مشکوک
- ارائه مکانیسم‌های قدرتمند برای انجام مطمئن تراکنش‌های مالی آنلاین
- محافظت از سامانه‌ها در برابر حمله‌های فیشینگ و مسدود کردن دریافت ایمیل یا پیام از سایت‌های مخرب
- محافظت از سامانه‌ها در برابر کیت‌های اکسپلویت پیشرفته
- محافظت از سامانه‌ها در برابر سایت‌هایی که قربانی حمله‌های بدافزاری شده‌اند
- ارائه یک بانک اطلاعاتی تخصصی از علائم و نشانه‌های بدافزارها.

هر ابزار **ضدبدافزاری** قابلیت‌های خاص خود را ارائه می‌کند و قابلیت‌های یکسانی را در اختیارتان قرار نمی‌دهند. برای مثال، برخی از شرکت‌های امنیتی در زمان طراحی محصولات **ضدبدافزاری** تمرکزشان تنها روی کاربرانی است که تراکنش‌های مالی آنلاین انجام می‌دهند، در حالی که گروه دیگری با هدف مقابله با تهدیدات روز صفر محصولات خود را به بازار عرضه می‌کنند.

چرا **ضدبدافزارها** و **ضدویروس‌ها** دو ابزار امنیتی مکمل یکدیگر هستند؟ آیا کاربران فضای مجازی به هر دو ابزار احتیاج دارند؟

محصولات **ضدبدافزار** به عنوان راهکاری برای حذف برنامه‌های مخرب شهرت دارند، در نتیجه نمی‌توانند جایگزینی برای **ضدویروس‌ها** باشند و نقش مکمل **ضدویروس‌ها** را دارند. این حرف به معنای آن است که شما می‌توانید برای محافظت از سامانه‌های خود از چند لایه امنیتی محافظ برای مقابله با انواع مختلفی از تهدیدات بدافزاری استفاده کنید. **ضدبدافزارها** می‌توانند گونه‌های جدید و پیشرفته بدافزارها را شناسایی و حذف کرده و ایمنی یک سامانه کامپیوتری را دوچندان کنند. برخی از ابزارهای **ضدبدافزاری** باج‌افزارها را پیش از آن‌که شروع به رمزگذاری اطلاعات کنند، شناسایی می‌کنند. در نقطه مقابل، **ضدویروس‌ها** برای مقابله با تهدیدات آنلاین رایج (کرم‌ها، تروجان‌ها، ویروس‌ها و کی‌لاگرها) بهترین راه‌حل امنیتی هستند.



اگر ضدویروس‌ها و ضدبدافزارها با یکدیگر روی سامانه‌ای اجرا شوند، ناسازگاری به وجود نمی‌آورند؟

یک برنامه **ضدبدافزاری** نباید به‌عنوان جایگزینی برای یک **ضدویروس** در نظر گرفته شود. **ضدبدافزارها** با نرم‌افزارهای **ضدویروسی** 100 درصد سازگار بوده و در زمان نصب از بابت ناسازگاری یا تداخل بدون هیچ‌گونه مشکلی قادر به استفاده هستند.

دیدگاه کارشناسان امنیتی در این زمینه چیست؟

اسکات کراودر، مدیر ارشد فناوری شرکت BMC می‌گوید: «شما هنوز هم برای مقابله با انواع مختلفی از تهدیدات کلاسیک به وجود **ضدویروس‌ها** نیاز دارید. با این حال، نباید از تهدید بزرگ روزصفر بدافزارها غافل شوید.»

مدیر ارشد شرکت سیمانتک می‌گوید: «**ضدویروس‌ها** قادر به شناسایی 45 درصد از تهدیدات بدافزاری هستند، این حرف به معنای آن است که یک سیستم بدون وجود **ضدبدافزارها** یک هدف ساده برای هکرها است.»

رابرات اوکلاهان، برنامه‌نویس اسبق فایرفاکس می‌گوید: «مستندات خیلی کمی وجود دارد که نشان می‌دهند سامانه‌ها با اتکا بر محصولات **ضدویروسی** و بدون نیاز به نصب هرگونه ابزار امنیتی قادر به دفع بیشتر حملات هستند. در نتیجه وجود یک **ضدبدافزار** روی یک سامانه ضروری است.»

توجه داشته باشید که با نصب یک **ضدویروس** تنها یک راه‌حل امنیتی را برای مقابله با تهدیدات استفاده کرده‌اید،

هیچ راه‌حل امنیتی به تنهایی قادر نیست از یک سامانه به درستی محافظت کند، در نتیجه وجود یک **ضدبدافزار** برای مقابله با تهدیدات پیشرفته و روز صفر
ضروری است.

ضدویروس‌ها چه مزایا و معایبی دارند؟

از مهم‌ترین مزایا و معایب **ضدویروس‌ها** می‌توان به موارد زیر اشاره کرد:
• **ضدویروس‌ها** به سادگی نصب می‌شوند و در بیشتر موارد با سیستم‌عامل‌ها سازگار هستند.
• **ضدویروس‌ها** با پویش فایل‌ها احتمال آلوده شدن سامانه‌ها به ویروس‌ها، تروجان، کی‌لاگرها و سایر تهدیدات مخرب را کم می‌کنند.
• بیشتر برنامه‌های **ضدویروسی** به شکل رایگان (با امکانات محدود) عرضه می‌شوند.
• **ضدویروس‌ها** مکانیسم‌های امنیتی برای مقابله با هرزنامه‌ها و حمله‌های فیشینگ ارائه می‌کنند.
از مهم‌ترین معایب **ضدویروس‌ها** می‌توان به موارد زیر اشاره کرد:
• **ضدویروس‌ها** در تشخیص سریع و بلادرنگ حمله‌های جدید و پیشرفته با مشکل روبه‌رو هستند.
• **ضدویروس‌ها** نظارتی مستمر روی سامانه‌ها دارند که باعث کندشدن سرعت سامانه‌ها می‌شوند.
• **ضدویروس‌ها** برای پویش‌های چندمنظوره به زمان قابل توجهی نیاز دارند. (به ویژه، اگر سامانه‌ای از هارددیسک‌ها استفاده کند.)

ضدبدافزارها چه مزایا و معایبی دارند؟

گزارش شرکت سیمانتک نشان می‌دهد، حمله‌های هکری شکلی هدفمند و پیشرفته به خود گرفته‌اند. حمله‌هایی که با هدف سرقت اطلاعات کاربران و سازمان‌ها اجرا می‌شوند. هکرها سعی می‌کنند از آسیب‌پذیری‌های روز صفر و پیاده‌سازی بدافزارهایی بر مبنای این آسیب‌پذیری‌ها اطلاعات کاربران را سرقت کرده یا اسناد را رمزگذاری کنند. کاربران می‌دانند که وجود **ضدویروس‌ها** برای محافظت از سامانه‌های آن‌ها ضروری است، با این‌حال، نسبت به وجود **ضدبدافزارها** اطلاعات کمی دارند. اما **ضدبدافزارها** چه مزایا یا معایبی دارند؟
مزایا
• رویکرد **ضدبدافزارها** بر حفاظت پیگشیرانه در برابر حمله‌های آنلاین متمرکز است.
• **ضدبدافزارها** با اتکا بر الگوریتم‌های پیشرفته سعی می‌کنند پیش از آن‌که یک بدافزار فرصت پیدا کند که آسیبی به سامانه‌ها وارد کند، آن‌را بلوکه کنند.
• بدافزارها مکانیسمی قدرتمند برای محافظت از تراکنش‌های مالی و محافظت از اطلاعات مالی کاربران ارائه می‌کنند.
• بیشتر **ضدبدافزارها** چند لایه امنیتی را پیرامون یک سامانه به وجود می‌آورند، در حالی که یک ضدویروس سنتی قادر به انجام این‌کار نیست.
• **ضدبدافزارها** می‌توانند به شکل بلادرنگ از سامانه‌ها در برابر حمله‌های **ضدبدافزار** محافظت کنند.
معایب
• پویش‌هایی که به شکل سفارشی انجام می‌شوند، در عمل سرعت سامانه‌ها را کاهش می‌دهند.
• نسخه‌های رایگان **ضدبدافزارها** یک مکانیسم حفاظتی بلادرنگ را ارائه نمی‌کنند.
• عملکرد **ضدبدافزارها** برای مقابله با ویروس‌ها به خوبی **ضدویروس‌ها** نیست.
مهم‌ترین مزیت **ضدبدافزارها** به شناسایی الگوهای پیچیده و پیشرفته بدافزارها بازمی‌گردد. **ضدبدافزارها** در زمینه پیدا کردن تبلیغ‌افزارها و جاسوس‌افزارها که رفتاری متفاوت از ویروس‌ها دارند، عملکرد خوبی دارند. برای مثال، **ضدبدافزار** Malwarebyte برنامه‌ای مکمل برای یک **ضدویروس** است. ابزاری که تهدیدات روزصفر را شناسایی کرده و یک لایه دفاعی خوب پیرامون سامانه‌ها به وجود می‌آورد.

مطلب پیشنهادی

ترکیب و ادغام بهترین پکیج‌های امنیتی با یکدیگر
چگونه یک چتر دفاعی قدرتمند برای سامانه‌های کامپیوتری ایجاد کنیم؟

باید ضدویروس‌ها و ضدبدافزارها را خریداری کنیم یا به شکل رایگان از هر دو محصول استفاده کنیم؟

هر زمان تصمیم می‌گیرید یک محصول امنیتی خریداری کنید، قیمت حرف اول را می‌زند. در بیشتر موارد انتخاب یک محصول خوب امنیتی برای کاربران کار دشواری است، زیرا به دانش فنی نیاز دارد. از سویی برخی از کاربران و شرکت‌ها تصور می‌کنند، خرید این محصولات خرج اضافی است، اما صبر کنید؛ وضعیتی را تصور کنید که فایل‌ها و اسناد مربوط به پروژه‌ها در اثر یک حمله باج‌افزاری کدگذاری شده‌اند. اکنون دو گزینه پیش رو دارید: باج مربوطه را پرداخت کرده و امیدوار باشید که فایل‌ها دومرتبه در دسترس‌تان قرار خواهند گرفت یا اگر فردی دوراندیش بوده‌اید، از نسخه پشتیبان استفاده کنید. آمارها نشان می‌دهند از هر چهار قربانی یک حمله باج‌افزاری، تنها یک نفر شانس آن‌را پیدا می‌کند که پس از پرداخت باج مربوط به فایل‌های خود دسترسی پیدا کند.
در سایر موارد کاربران پس از پرداخت باج هیچ‌گاه به فایل‌های خود دسترسی پیدا نخواهند کرد. بیشتر شرکت‌های امنیتی در زمان عرضه **ضدویروس‌ها** و **ضدبدافزارهای** رایگان از همان موتور پردازشی‌تحلیلی استفاده می‌کنند که در نسخه تجاری از آن بهره می‌برند. با این حال، نسخه‌های رایگان هر دو محصول بیشتر نقش یک هشداردهنده را دارند. در حالی که **ضدویروس‌های** رایگان قدرتمندی در بازار وجود دارند، با وجود این، نسخه‌های تجاری **ضدویروس‌ها** و **ضدبدافزارها** یکسری قابلیت‌های برجسته ارائه می‌کنند که از مهم‌ترین آن‌ها می‌توان به ارائه یک سامانه مرکزی برای محافظت از پلتفرم‌های مختلف دسکتاپ و موبایل اشاره کرد. یکی دیگر از نقاط قوت محصولات تجاری پشتیبانی فنی از مشتریان است.

سخن آخر

با توجه به این‌که بررسی تنظیمات یک سیستم، بررسی سایت‌ها و فایل‌های مخرب و اتخاذ استراتژی‌های امنیتی برای مقابله با تهدیدات کار پیچیده‌ای است و شما به شکل دستی قادر به انجام این‌کار نیستید، وجود یک **ضدویروس** برای سیستم نقش حیاتی دارد. برای مقابله با تهدیدات سایبری که به شکل مستمر در حال توسعه و پیشرفت هستند، به یک محصول **ضدبدافزاری** نیاز است تا یک سپر دفاعی مناسب پیرامون سامانه‌ها به وجود آورد. دقت کنید، با نصب همزمان هر دو ابزار روی یک سیستم خطر آلودگی می‌یابد، اما خطر همواره وجود دارد. در نتیجه، سعی کنید به جای آن‌که به واسطه یک حمله همه فایل‌های‌تان از دست بروند و افسوس بخورید، به فکر تامین امنیت سیستم باشید

تاریخ انتشار:

07 اردیبهشت 1398

نشانی منبع:
https://www.shabakeh-mag.com/security/15013/%D8%B6%D8%AF%D9%88%DB%8C%D8%B1%D9%88%D8%B3-%DB%8C%D8%A7-%D8%B6%D8%AF%D8%A8%D8%AF%D8%A7%D9%81%D8%B2%D8%A7%D8%B1-%D8%8C%DA%A9%D8%AF%D8%A7%D9%85%E2%80%8C%DB%8C%DA%A9-%D8%B1%D8%A7-%D8%A8%D8%A7%DB%8C%D8%AF-%D8%A7%D9%86%D8%AA%D8%AE%D8%A7%D8%A8-%DA%A9%D9%86%DB%8C%D9%85%D8%9F