

واکسن ویروس اتوران



اجرای خودکار برنامه‌ها از دیسک‌های نوری (اتوران) از جمله امکاناتی بود که در ویندوز 95 غوغایی به پا کرد و با استفاده از آن، امکانات مختلفی در اختیار کاربران قرار گرفت.

جام جم آنلاین: اجرای خودکار برنامه‌ها از دیسک‌های نوری (اتوران) از جمله امکاناتی بود که در ویندوز 95 غوغایی به پا کرد و با استفاده از آن، امکانات مختلفی در اختیار کاربران قرار گرفت.

به مرور این قابلیت به تمامی نرم‌افزارها، بازی‌ها و دیگر اطلاعات ذخیره شده روی دیسک‌های نوری اضافه شد و به کاربران این امکان را داد تا به‌طور خودکار و بدون نیاز به داشتن دانشی از چگونگی اجرای اطلاعات موردنظر، آنها را اجرا کرده و به استفاده از آنها بپردازند.

این قابلیت با پیشرفت محصولات و رسانه‌های ذخیره‌ساز همچون حافظه‌های فلش روزبه‌روز بیشتر مورد استفاده کاربران قرار گرفت، به‌طوری‌که به روشی بسیار کارآمد و موثر برای انتشار ویروس‌ها از رایانه‌ای به رایانه دیگر تبدیل شد! متأسفانه این روزها برای هر کاربری از قابلیت اتوران حرف بزنید اولین چیزی که به ذهنش می‌آید ویروس‌هایی است که توسط این قابلیت انتشار می‌یابد و از رایانه‌ای به رایانه دیگر نیز منتقل می‌شود.

این نوع انتشار ویروس آنقدر خطرناک است که بسیاری از نرم‌افزارهای امنیتی و ضدویروس اولین اقدامی که برای حفظ امنیت سیستم‌عامل و رایانه به انجام می‌رساند، غیرفعال کردن قابلیت اجرای خودکار برنامه‌ها از CD، DVD، حافظه‌های فلش و... است.

همان‌طور که می‌دانید برای آلوده شدن به ویروس اتوران حتماً نباید رایانه خودتان آلوده به ویروس باشد، بلکه با یک‌بار اتصال حافظه فلش شخصی شما به یک رایانه آلوده، در کسری از ثانیه ویروس به حافظه فلش شما نیز منتقل شده و با اتصال آن به رایانه شما، کل رایانه را نیز آلوده می‌کند! اگر شما هم با این مشکل مواجهید و نگران آلوده شدن حافظه فلش خود هنگام اتصال به رایانه‌های دیگر هستید، می‌توانید از نرم‌افزار رایگان Bitdefender USB Immunizer کمک بگیرید.

نرم‌افزار فوق یکی از جدیدترین محصولات Bitdefender است که به شما این امکان را می‌دهد تا بسادگی از حافظه‌های فلش خود در برابر فایل‌های اتوران آلوده حفاظت کنید.

روش کار این نرم‌افزار به این صورت است که یک فایل با نام autorun.inf را که برای اجرای فایل‌ها به‌صورت خودکار مورد استفاده قرار می‌گیرد، به‌طور کامل خالی و فاقد محتوا روی حافظه فلش شما ایجاد کرده و با شیوه خاصی که این عملیات کپی انجام می‌شود مانع کپی شدن یا جایگزینی فایل دیگری با همین نام روی آن می‌شود.

در چنین شرایطی فایل حامل ویروس در سیستم‌های آلوده نمی‌تواند خودش را روی حافظه فلش شما کپی و از قابلیت اتوران در آن سوءاستفاده کند.

نرم‌افزار Bitdefender USB Immunizer نیاز به نصب ندارد و به‌محض اجرا همه حافظه‌های فلش متصل به رایانه را تشخیص داده و آنها را برای شما فهرست می‌کند.

حافظه‌های فهرست شده توسط نرم‌افزار با هاله‌ای نورانی به دو رنگ قرمز و سبز نمایش داده می‌شود که رنگ قرمز امن نبودن حافظه فلش شما را گوشزد می‌کند و رنگ سبز نشان‌دهنده آن است که عملیات ایمن‌سازی روی حافظه فلش شما انجام شده است البته برای ایمن‌سازی حافظه‌های فلش مشخص شده با نور قرمز رنگ باید یک‌بار روی نام آنها کلیک کنید!

از دیگر امکانات این نرم‌افزار، ایمن‌سازی تمامی حافظه‌های فلش به‌صورت خودکار است که برای فعال‌سازی آن باید روی آیکون چرخ‌دنده کوچکی که در بالای پنجره نرم‌افزار وجود دارد کلیک کرده و پس از آن در پنجره به‌نمایش درآمده گزینه مربوط را روی حالت ON قرار دهید.

توجه داشته باشید که این نرم‌افزار قادر به پاک‌کردن ویروس‌ها از روی حافظه‌های فلش و رایانه شما نیست و تنها کاری که انجام می‌دهد حفاظت از حافظه‌های فلش در برابر آلودگی به ویروس‌های اتوران و انتقال آنها از رایانه‌ای به رایانه دیگر است.

همچنین فایل اتوران ایجاد شده توسط این نرم افزار براحتی از حافظه فلش شما پاک نمی شود و برای حذف آن باید از روش هایی همچون حذف توسط سیستم عامل لینوکس یا مکینتاش یا فرمت کردن کامل حافظه فلش کمک بگیرید.

Bitdefender USB Immunizer در تمامی نسخه های 32 و 64 بیت سیستم عامل ویندوز اکس پی، ویستا و 7 قابل استفاده است و از فایل سیستم های مختلف FAT FAT32 NTFS نیز پشتیبانی می کند.

<http://mcaf.ee/6cyew>