مقابله با باج افزار در ویندوز ۱۰ و ویندوز سرور ۲۰۱۹

باج افزار ها یکی از انواع مختلف بد افزارها می باشند که تاثیرات بسیار مخربی روی سیستم های کامپیوتری داشته و دسترسی ما را به اطلاعاتمان محدود می نمایند.

روش های گسترش باج افزار

- **ایمیل های اسپم که حاوی لینک ها و یا پیوست های مخرب می باشند :** بیش از ۷۰ الی ۸۰ درصد میزان آلوده شدن به باج افزارها از طریق ایمیل های اسپم آلوده، اتفاق می افتد، به این معنی که فایل مخرب یا به صورت یک فایل الصاق شده برای شما ارسال می کردد و یا اینکه این ایمیل حاوی لینکی می باشد که کاربر با کلیک بر روی آن یک فایل آلوده به باج افزار را بر روی رایانه دانلود می کند.
- **سوء استفاده از نرم افزارهای آسیب پذیر (استفاده از خلاهای امنیتی بر روی نرم افزارهایی مثل مرورگرهای اینترنتی) :** یکی دیگر از روشهای ورود باج افزارها توسط هکرها، استفاده از خلاء های امنیتی موجود بر روی نرم افزارهای نصبی ویا حتی خود سیستم عامل می باشد، هکرها با اسکن این اطلاعات با استفاده از ابزاری مانند Exploit ها و یافتن این آسیب ها، باج افزار ها را وارد سیستم خواهند کرد.
- **تغییر مسیر ترافیک اینترنت به سمت وب سایت های مخرب :** روش مرسوم دیگری برای ورود باج افزارها، هدایت قربانیان به سمت لینک های آلوده می باشد، به این معنی که یک قربانی بدون اینکه متوجه بشود با کلیک بر روی یک لینک آلوده، باج افزاری را بر روی سیستم خود دانلود می کند. و یا اینکه به وب سایتی هدایت می شود که حاول کدهای مخرب برای ورود به سیستم شما هستند.
- **وب سایت های قانونی که در صفحات وب خود سهوا کد مخرب تزریق کرده اند :** گاها دیده شده است، که هکرها با آلوده کردن وب سایت های قانونی بدون اینکه خودشان متوجه شوند باعث آلودگی در روی سیستم کابران شده اند.
- **استفاده از تبلیغات آنلاین برای گسترش بدافزارها:** یکی از دیگر از روشهای هوشمندانه استفاده از ابزار تبلیغ می باشد، برای اینکار با استفاده از تبلیغات دروغین و با دادن وعده های دروغین قربانیان را متقاعد به کلیک بر روی لینک و یا دانلود فایل یا نرم افزر حاوی باج افزار می کنند، مثلا اعلام می کنند، فایل حاوی کدهای فلان بازی آنلاین و.....
- **پیامهای SMS (این روش بیشتر گوشیهای هوشمند را هدف قرار می دهند) :**در بعضی از موارد هم دیده شده است برای بالا بردن میزان تعداد قربانیان، یک باج افزار از روی گوشی هوشمند قربانی اس ام اس هایی را از طرف صاحب گوشی به تمامی لیست تلفن شخص می فرستد که حاوی لینک دانلود باج افزار می باشد.
- **بات نت ها**
- **خود انتشاری :** انتشار از یک سیستم آلوده به سیستم دیگر.
- **Affiliate schemes in ransomware-as-a-service:** کسب درآمد با انتشار باج افزار، یکی دیگر از روشهای معمول در انتشار باج افزار می باشد، برای مثال باج افزار ها پس از آلوده کردن سیستم قربانیان اعلام میدارد در ازای آلوده کردن سیستم چند نفر دیگر توسط فرد قربانی می تواند در میزان باج تخفیف بگیرد، و یا حتی کلید رمزگشایی رایگان دریافت کند.
- **Drive-by downloads:** استفاده از Exploit برای اسکن سیستم ها، جهت شناسایی نقاط آسیب پذیر بر روی سیستم و یا شبکه های کاربران، برای نفوذ و آلوده کردن توسط باج افزار.

مقابله با باج افزار در ویندوز ۱۰ و ویندوز سرور ۲۰۱۹

مایکروسافت با عرضه ویندوز ۱۰ و ویندوز سرور ۲۰۱۹ نسل جدید Windows Defenderرا معرفی کرد .از نکات مثبت Windows Defender می‌توان به شناسایی ویروس های عمومی، یکپارچگی با ویندوز، استفاده کم از منابع ویندوز و محیط ساده و قابل فهم اشاره کرد .

در این نسخه جدید، تمرکز اصلی مایکروسافت بر روی ارتقای تنظیمات محدود سازی دسترسی نرم افزار ها به فایل ها و فولدرهای کاربر برای مقابله با باج افزارها بوده است. باج افزار ها ابزارهای مخربی هستند که وارد سیستم شما می‌شوند و اطلاعات شما را دریافت می‌کند. کمپانی سازنده به اطلاعات دسترسی پیدا می‌کند و همچنین اگر شما به صاحبان آن مبلغی را پرداخت نکنید فایل های شما را پاک می کنند. همچنین، **Windows Defender** اکنون از طریق بخشی به نام "Windows Defender Exploit Guard"تا زمان عرضه به روز رسانی های ویندوز، سیستم عامل را از معایب و حفره های امنیتی به روز رسانی قبل محافظت می‌کند.

دسترسی کنترل شده به فولدر ها

از بیلد ۱۸۰۹، Windows Defender دارای کنترل روی دسترسی اپلیکیشن ها به فایل ها و فولدرهای کاربر روی هارد خواهد بود. این قابلیت، یک لایه امنیتی جدید را به سیستم عامل اضافه می‌کند که مانع از دسترسی فایل های مخرب مانند باج افزارها به پوشه های ویندوز می‌شود.

زمانی که این قابلیت فعال شود، Windows Defender دسترسی ها و تغییراتی را که نرم افزارهای شما بر روی فایل های ذخیره شده‌تان روی پوشه های به خصوصی از ویندوز خواهند داشت به شما نشان خواهد داد. منظور از پوشه های به خصوص، پوشه هایی است که کاربر برای Windows Defender تعریف می‌کند. به این طریق، باج افزار ها هیچ گاه به فایل های شخصی شما دسترسی نخواهند داشت .اگر اپلیکیشنی که در لیست سیاه Windows Defender وجود دارد قصد اعمال تغییراتی روی این پوشه ها را داشته باشد، Windows Defender مانع آن خواهد شد و اعلانیه ای را نیز مربوط به این فعالیت های مشکوک دریافت خواهید کرد.

Windows Defender در حالت پیشفرض از عکس ها، فیلم ها و داکیومنت ها و همچنین پوشه های دسکتاپ محافظت خواهد کرد و همچنین میتوانید فولدر های جدید روی هارد ، هارد اکسترنال و یا شبکه خانگی خود را جهت محافظت به Windows Defender معرفی کنید.

اگرچه نرم افزارهایی که روزانه از آن ها استفاده می‌کنید و مورد اعتماد شما هستند توسط Windows Defender مسدود نمی‌شوند، اما اگر این اتفاق افتاد نیز، بخش کنترل دسترسی قابلیتی را دارد که می‌توانید آن نرم افزار را در لیست سفید قرار دهید تا به فایل های شما دسترسی داشته باشد.

فعال کردن Controlled folder access :

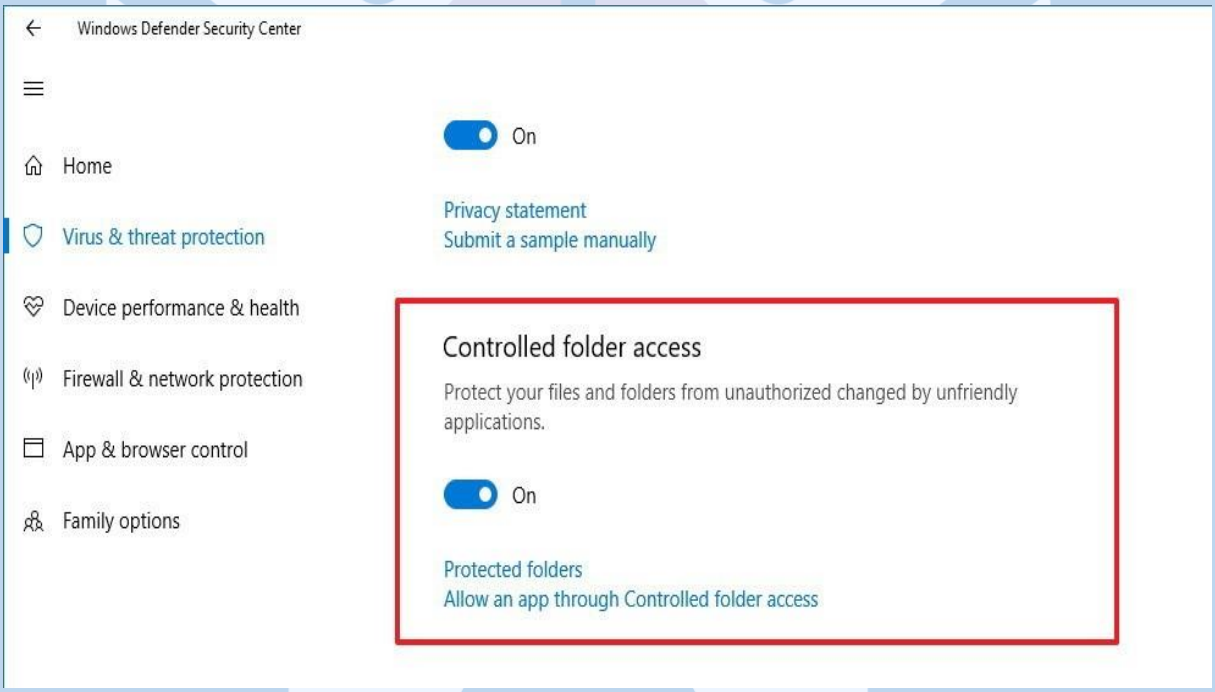
این قابلیت به طور پیشفرض غیر فعال است و برای فعال سازی آن نیاز به تاییدیه کاربر دارد.

برای فعال سازی این قابلیت ، ابتدا به مسیر زیر بروید:

Windows Defender Security Center > Virus & threat protection > Virus & threat protection settings

گزینه "**Controlled folder access**" را فعال کنید تا Windows Defender دسترسی ها را کنترل کند.

پس از تکمیل مراحل فوق، آنتی ویروس ویندوز دیفندر به طور مداوم فایل ها و پوشه را از دسترسی غیرمجاز برنامه های مخرب مانند ransomwareمحافظت می کند.



پس از اینکه مراحل بالا را طی کردید و قابلیت Controlled Folder Access را فعال نمودید، می‌توانید معین کنید که کدام فولدرها توسط این ویژگی محافظت شوند. برای این منظور روی گزینه‌ی «Protected folders» کلیک نمایید. بعد از زدن گزینه‌ی Protected folders، خواهید دید که به صورت پیش‌فرض فولدرهای سیستمی و فولدرهای شخصی مانند Documents، Pictures، Videos، Music، Desktop –که همگی در فولدر نام کاربری‌تان واقع شده‌اند، مورد محافظت قرار دارند.

افزودن مکان های جدید به این بخش جهت محافظت :

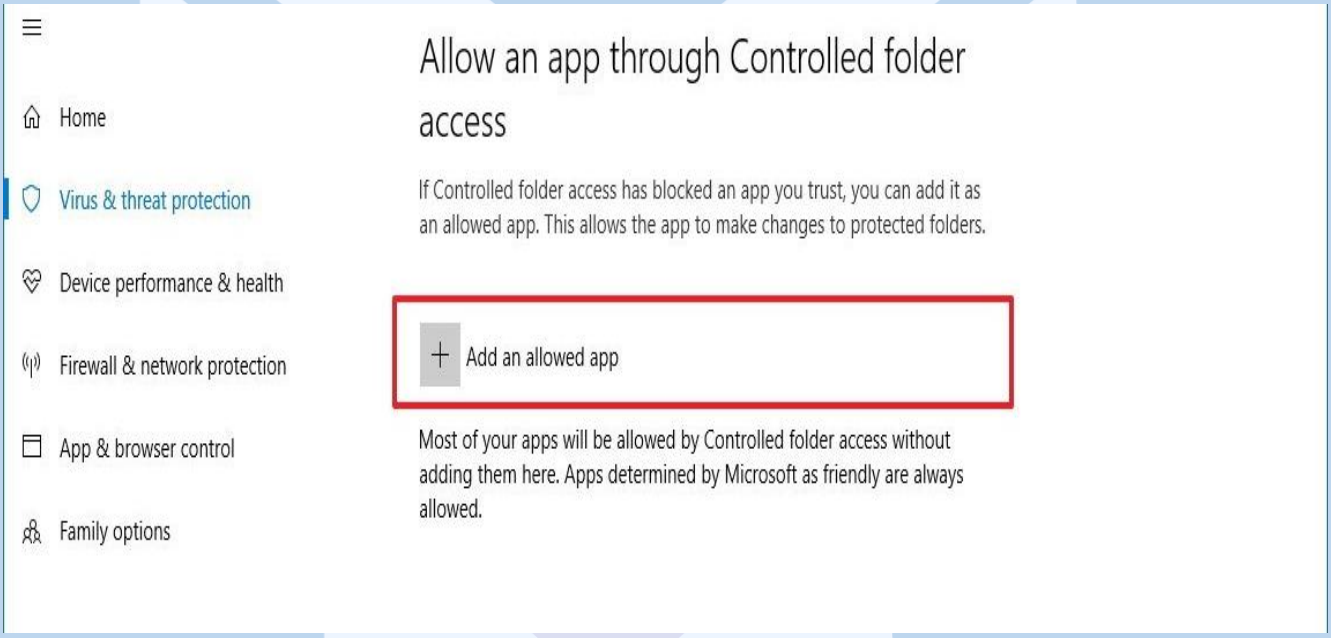
اگر داده‌های مهمی را در فولدر دیگری نگهداری می‌کنید و می‌خواهید این فولدر نیز تحت محافظت باشد، باید روی دکمه‌ی « Add a protected folder» کلیک نمایید و سپس دایرکتوری مدنظرتان را مشخص کنید.

برای این منظور روی بخش "**Virus & threat protection settings**" در سمت چپ Windows Defender کلیک کنید وارد آن شوید. روی گزینه "**Protected folders**" کلیک کنید و در پنجره باز شده روی گزینه "**Add a protected folder**" کلیک کنید و فولدرهای جدید را به Windows Defender معرفی کنید.

مجاز سازی اپلیکشن های مورد اعتماد شما:

اگر یکی از نرم افزارهای مورد اعتماد شما توسط Windows Defender مسدود شود، می‌توانید مجوز دسترسی آن را به فولدر هایتان از قسمت Allow an app through Controlled folder access ایجاد کنید

برای این کار در بخش Windows Defender "**Virus & threat protection settings**" روی گزینه "**Allow an app through Controlled folder access**" کلیک کنید و وارد آن شوید. در این بخش روی گزینه "**Add an allowed app**" کلیک کنید و فایل exe نرم افزار خود را به Windows Defender معرفی کنید.



این قابلیت تنها در زمانی کار می‌کند که Windows Defender آنتی ویروس اصلی شما باشد. اگر از یک نرم افزار شخص ثالث به عنوان آنتی ویروس روی دستگاه خود استفاده می‌کنید، این قابلیت برای شما در دسترس نخواهد بود و برای استفاده از این قابلیت، نسبت به حذف آنتی ویروس خود اقدام کنید.