روش‌های مقابله با باج‌افزارها

واقعیت این است که باج‌افزارها وجود دارند روزبروز هم در حال گسترش هستند. بنابراین مهم است که هر کاربر کامپیوتر، هر چند که فقط از یک سیستم در خانه یا محل کار استفاده می کند، درک درستی در ارتباط با چگونگی محافظت از سیستم خود در برابر باج‌افزار داشته باشد به طوری که روند باج‌گیری برای مهاجم سخت گردد. در ادامه این مطلب به روش‌های مقابله در برابر باج افزار اشاره می‌شود

- **اطمینان حاصل کنید که پشتیبان گیری می کنید!**

BACKUP! تهیه نسخه پشتیبان مهمترین وظیفه‌ای است که باید برای محافظت از اطلاعات خود در برابر رمزگذاری انجام دهید. واقعیت این است که اگر نسخه پشتیبان بروزی را داشته باشید، باج‌افزار بیشتر مزاحم خواهد بود تا یک تهدید. به این دلیل که شما می‌توانید سیستم را پاک‌سازی کرده و سپس اطلاعات خود را از نسخه پشتیبان بازیابی کنید. اما افزودن یک هارد دیسک اضافی به کامپیوتر و تهیه نسخه پشتیبان در آن کافی نیست زیرا باج‌افزارها تمام درایوهای سیستم از جمله درایوهای map network را هدف قرار داده و رمزگذاری می‌کنند و این بدان معنی است که نسخه‌های پشتیبان که در درایو محلی و شبکه ذخیره شده‌اند، نیزمی‌تواند رمزگذاری شود؛ بنابراین یا از استراتژی پشتیبان‌گیری ابر استفاده کنید و یا اگر می‌خواهید به ذخیره سازی محلی متکی باشید، مطمئن باشید که پس از پشتیبان‌گیری دستگاه‌های ذخیره‌سازی را قطع کرده‌اید یا کامپیوتر پشتیبان در هنگام اشتراکگذاری فایل‌ها غیرقابل دسترسی و ایزوله است.

- **از آنتی‌ویروسی استفاده کنید که دارای تشخیص رفتار باج‌افزار است**

اطمینان حاصل کنید که یک آنتی‌ویروس قابل اطمینان بر روی سیستم نصب شده است .جرایم اینترنتی درحال افزایش هستند و هر کامپیوتر نیاز به محافظ خوب دارد .پیشنهاد می‌شود از محصولی استفاده شود که دارای تشخیص رفتار خوب است تا بتواند باج‌افزارها حتی با نام تجاری جدید، که تلاش می‌کنند اطلاعات شما را رمزگذاری کنند، تشخیص داده و سپس آن را متوقف سازد.

- **همیشه بروزرسانی سیستم عامل را نصب کنید**

بسیاری از آلودگی‌های باج‌افزار از طریق اسکریپت‌هایی به نام کدهای exploit که آسیب‌پذیری‌های سیستم عامل را هدف قرار می‌دهند، نصب می‌شوند بنابراین بایستی بروزرسانی‌های جدید سیستم عامل خود را بلافاصله بعد از انتشار نصب کنید بسیاری از این بروزرسانی‌ها امنیتی هستند که از رایانه شما در برابر آسیب‌پذیری را محافظت می‌کند آسیب‌پذیری که به معنای واقعی کلمه اجازه می‌دهد تا مهاجم هر فرمانی را که می‌خواهد در رایانه شما اجرا کند. مایکروسافت بروزرسانی‌های امنیتی را در دومین سه شنبه هر ماه منتشر می‌کند، پس همیشه برای اعلان‌ها توجه داشته و بروزرسانی‌ها را به موقع نصب کنید.

- **برنامه‌ها را بر روی کامپیوتر خود بروز نگه دارید**

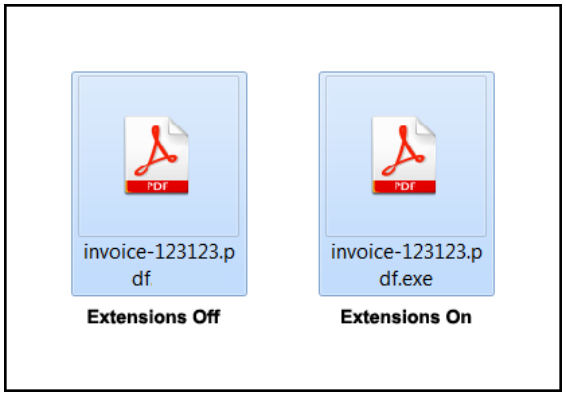
همانند آسیب‌پذیری‌های سیستم‌عامل، کیت‌های بهره‌برداری نیز آسیب‌پذیری‌هایی را در برنامه‌های معمول نصب شده بر روی سیستم‌ها مانند جاوا، Adobe Flash Player، Adobe Reader و غیره را هدف قرار می‌دهند. بنابراین لازم است که این برنامه ها را نیز به روز نگه دارید.

- **مطمئن شوید که فیلترهای SPAM شما کار می‌کنند**

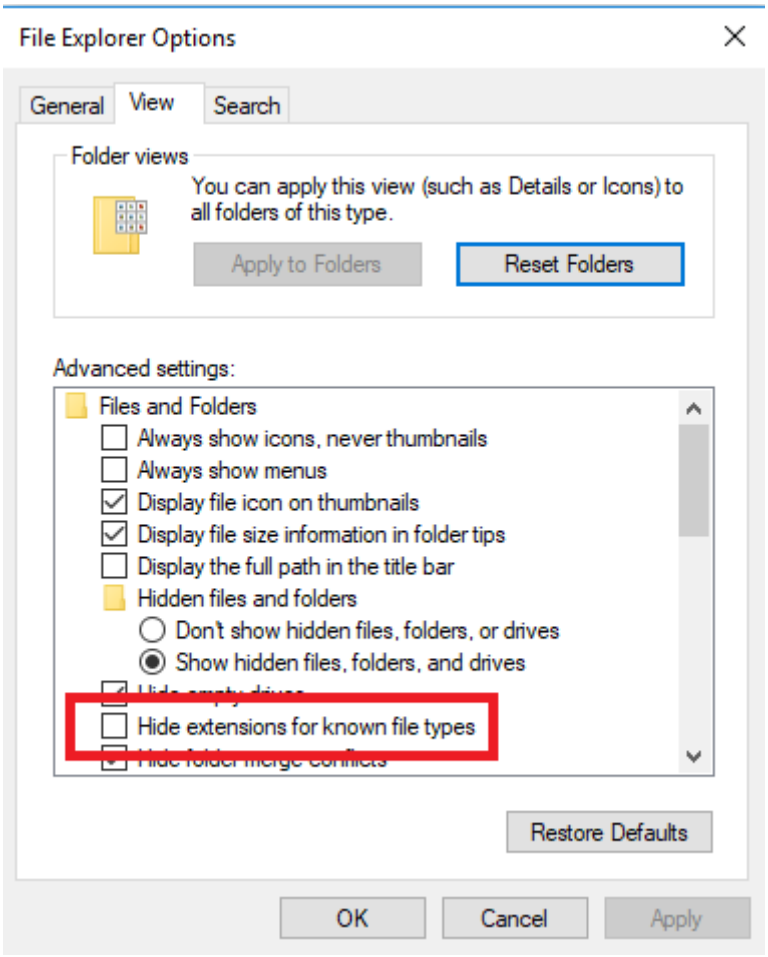
یکی از بزرگترین روش‌های توزیع برای باج افزار از طریق ایمیل‌های اسپم است که تظاهر به ارسال آگهی‌ها، رزومه، صورتحساب‌ها یا بلیط‌ها از سازمان‌های دولتی می‌باشد. اگر از یک فروشنده ایمیل وب مانند جیمیل، Outlook یا یاهو استفاده می‌کنید، بسیاری از این نوع ایمیل‌های اسپم برای شما فیلتر شده‌اند. اگر شما از یک سرویس استفاده نکنید که دارای فیلتر خوب SPAM باشد، این نوع ایمیل‌ها ممکن است باعث آلودگی سیستم گردند.

- **فعال کردن مشاهده پسوند برنامه‌ها**

به طور پیش فرض، ویندوز و macOS پسوند یک فایل را در هنگام مشاهده یک فایل نشان نمی‌دهند. مهاجمان از این شرایط برای فریب کاربران استفاده می‌کنند. بدین صورت که قربانی با تصور اینکه بر روی یک فایل در Word، Excel یا یک سند PDF کلیک می‌کند تا اطلاعات آن مشاهده کند. اما در واقع ، یک برنامه مخرب را اجرا کرده و ناخواسته بدافزاری نصب می‌گردد. در شکل زیر نمونه‌ای از نمایش پسوند فایل نشان داده شده است.



پیشنهاد می‌شود مشاهده پسوند فایل‌ها را فعال کنید تا مهاجمان با استفاده از این نوع فریبکاری نتوانند نرم‌افزارهای مخرب خود را به اجرا درآوردند. برای فعال کردن پسوند برنامه‌ها، می‌توانید در ویندوز در قسمت Folder Options گزینه Hide extensions for known file types را غیرفعال کنید.



- **پیوست‌ها را باز نکنید مگر با تأیید شخصی که آنرا به شما ارسال کرده است**

هنگامی که باج‌افزار از طریق SPAM توزیع می‌شود، در بسیاری از موارد فایل مخرب به صورت یک پیوست است. چنانچه پیوستی را دریافت کرده‌اید و مطمئن نیستید چرا فرستاده شده یا از طرف چه کسی است، باز نکنید مگر اینکه قبلا فرستنده پیام، آن را تایید کرده باشد یعنی فایل در سامانه‌های آنلاین (مانند ویروس توتال یا سامانه تحلیل‌گر فایل‌های اجرائی) اسکن شده و درهم ساز (MD5) آن بهمراه پیوست ارسال شده باشد.

- **مراقب آنچه که از اینترنت دانلود می کنید مراقب باشید**

دانلود رایگان از اینترنت همچنین ممکن است با دانلود یک باج‌افزار مخفی همراه باشد . برای دانلود برنامه ها از سایت های مطمئن استفاده کنید و همیشه موافقت نامه های مجوز را بخوانید.

- **vssadmin را در ویندوز تغییر نام دهید**

قابلیت Volume Shadow Copy توسط ویندوز برای ذخیره سازی پشتیبان گیری یا تهیه نسخه های قبلی از فایل ها در سیستم استفاده می شود که بعدا از این نسخه‌های پشتیبان می توان برای بازیابی داده های تغییر یافته استفاده کرد. توسعه دهندگان باج‌افزار نیز این موارد را می‌دانند و برای از بین بردن آن دستور vssadmin.exe را اجرا خواهند کرد تا همه فایل‌های Shadow Copy را بر روی سیستم قربانی حذف کنند تا از آنها برای بازگرداندن فایل های رمز شده استفاده نشود.

به استثنای نرم افزارهایی که بر روی vssadmin متکی هستند، به شدت پیشنهاد می‌شود که نام vssadmin را بدون از دست دادن قابلیت آن تغییر دهید. در مطالب آتی بیشتر در این مورد صحبت می‌شود.

- **غیر فعال کردن اسکریپت ویندوز**

بسیاری از آلودگی‌های باج‌افزار از طریق پیوست هایی که فایل های اسکریپت در Jscript یا VBS کد گذاری شده اند نصب می شوند. به استثنای مواردی که معمولا فایلهای Jscript یا VBS را اجرا می کنند پیشنهاد می‌شود که توانایی راه اندازی این نوع اسکریپت ها را در ویندوز غیرفعال کنید.

- **غیرفعال کردن Windows PowerShell**

همانند اسکریپت ویندوز، Windows PowerShell همچنین برای نصب باج‌افزار یا حتی رمزگذاری فایل ها استفاده می شود. اگر شما از PowerShell در رایانه خود استفاده نمی کنید، می توانید با اجرای این دستور ویندوز، اجرای اسکریپت های PowerShell (ps1) را غیر فعال کنید.

powershell Set-ExecutionPolicy -ExecutionPolicy Restricted

اگر آن را به درستی تنظیم کردید، هنگام اجرای یک اسکریپت PowerShell، پیامی خواهید دید که نشان می دهد اسکریپت PowerShell غیر فعال شده است.

البته توجه داشته باشید که اجرای اسکریپت PowerShell غیر فعال، می تواند برای برنامه های مشروع مشکلاتی را ایجاد کند. اگر اجرای اسکریپت PowerShell برای سیستم‌تان ضروری است، می توانید Set-ExecutionPolicy را به سطح دیگری تغییر دهید.

- **از کلمات عبور قوی استفاده کنید**

اطمینان حاصل کنید که از رمزهای عبور قوی برای محافظت از سیستم خود در برابر از دسترسی غیرمجاز استفاده می‌کنید. بداین دلیل که برخی از باج‌افزارها سیستم قربانی را از طریق اتصالات Remote Desktop که دارای رمزعبور ضعیف بودند آلوده کرده‌اند.

- **اگر به Remote Desktop نیاز ندارید، آن را غیرفعال کنید، در غیر اینصورت پورت را تغییر دهید!**

اگر از Remote Desktop استفاده نمی کنید، پس هیچ دلیلی وجود ندارد که آن را فعال کنید. اگر شما از آن استفاده می کنید، پس باید پورت پیش فرض آن را از ۳۳۸۹ به مقدار دیگری تغییر دهید. اکثر مهاجمان از اسکریپت ها یا اسکنر ها بر روی پورت پیش فرض Remote Desktop سیستم قربانی، برای جستجو استفاده می‌کنند با تغییر پورت، شما سیستم خود را برای این ابزار نامرئی ساخته اید.

- **راه اندازی سیاست های محدودیت نرم افزار در ویندوز**

سیاست های محدودیت نرم افزار یک روش است که به شما اجازه می دهد تا سیاست های مختلفی را ایجاد کنید که سیاست‌هایی که محدودیت شروع اجرا از یک پوشه را نیز دربر دارد..

- **یک برنامه لیست سفید برنامه در ویندوز ایجاد کنید**

در سیاست لیست سفید نرم افزار، شما ویندوز را مجددا تنظیم می‌کنید تا برنامه ها را تنها به برنامه هایی که تعیین شده‌اند اجرا گردد. این مانع از اجرای هر برنامه ناشناخته می شود و اساسا کامپیوتر شما را به طور کامل قفل می کند تا برنامه غیر مجاز اجرا نشود.

نتیجه

اگرچه ممکن است احساس کنید که مراحل زیادی وجود دارد، اما اغلب آنها نیاز دارند تا عادت های کامپیوتری خود را تغییر دهید. اگر این مراحل را دنبال کنید، نه تنها از باج‌افزار محافظت خواهید شد، بلکه شما نیز از تقریبا تمام سایر بدافزارها محافظت خواهید شد.

منبع: www.bleepingcomputer.com

مرکز آپا دانشگاه محقق اردبیلی