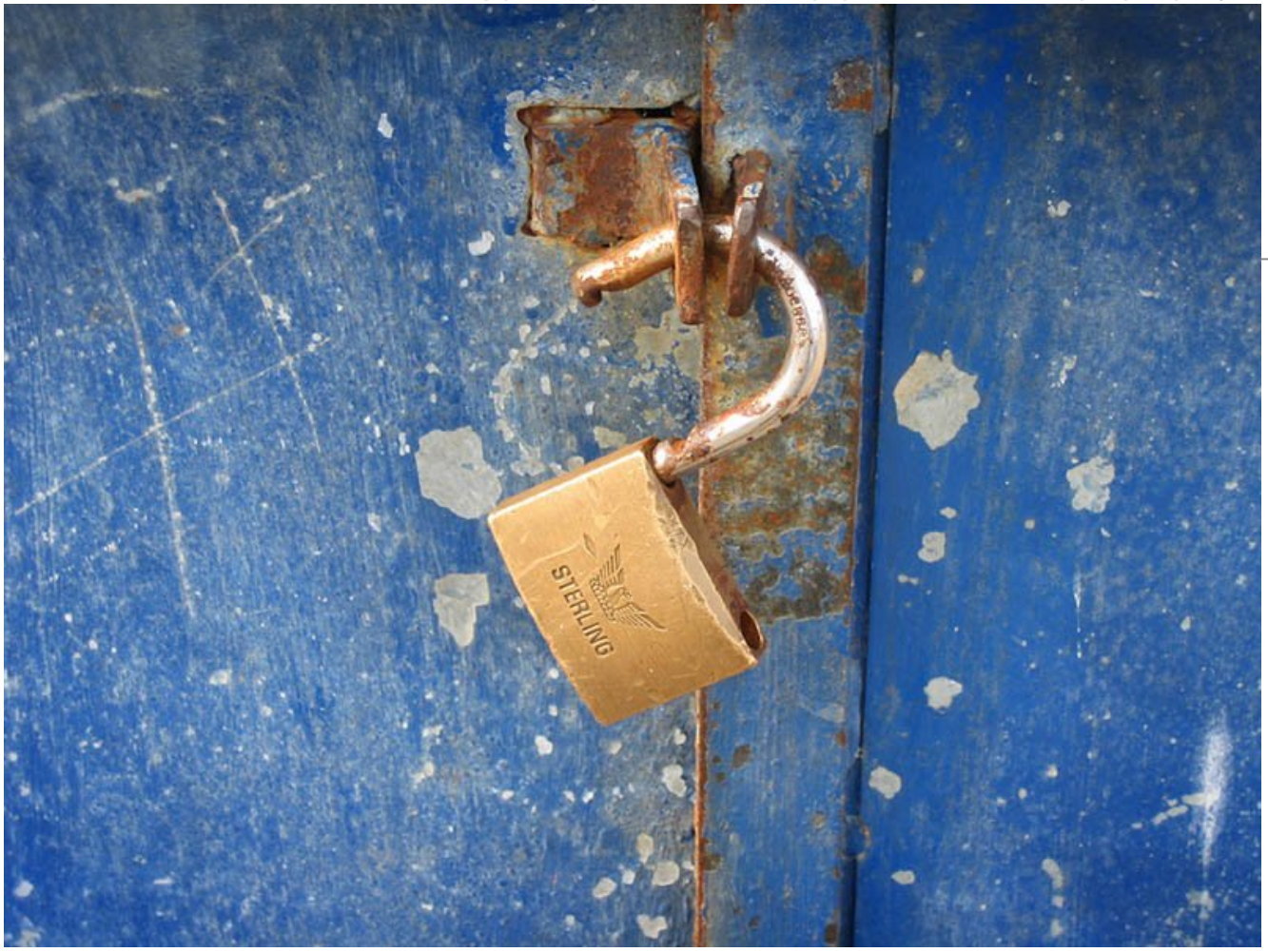
مایکروسافت هشدار می‌دهد

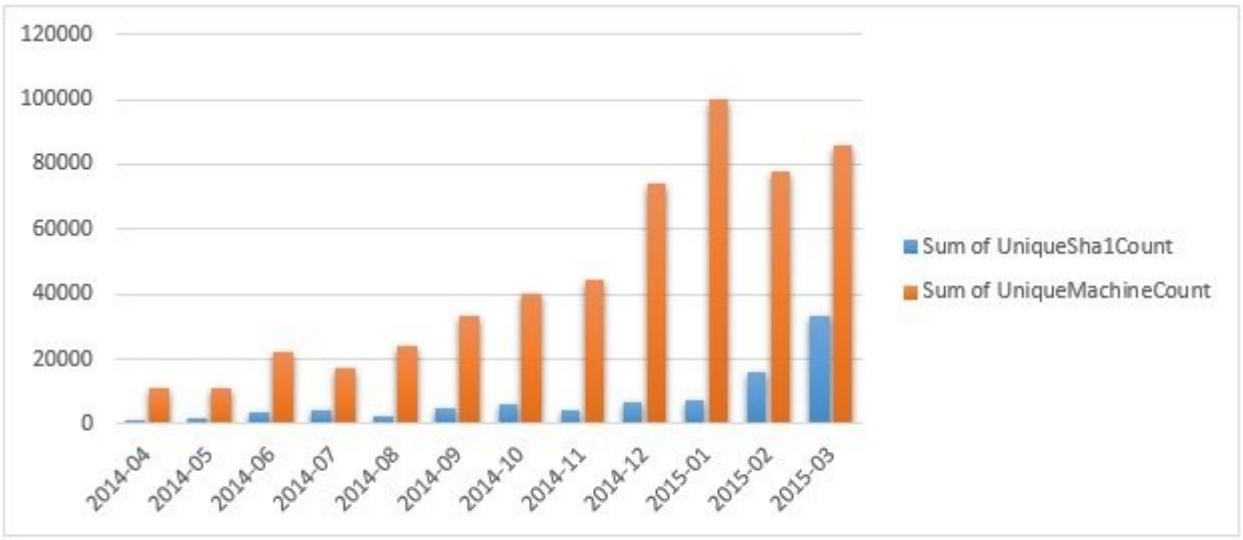
همه‌چیز درباره حملات بدافزارهای مبتنی بر ماکروها



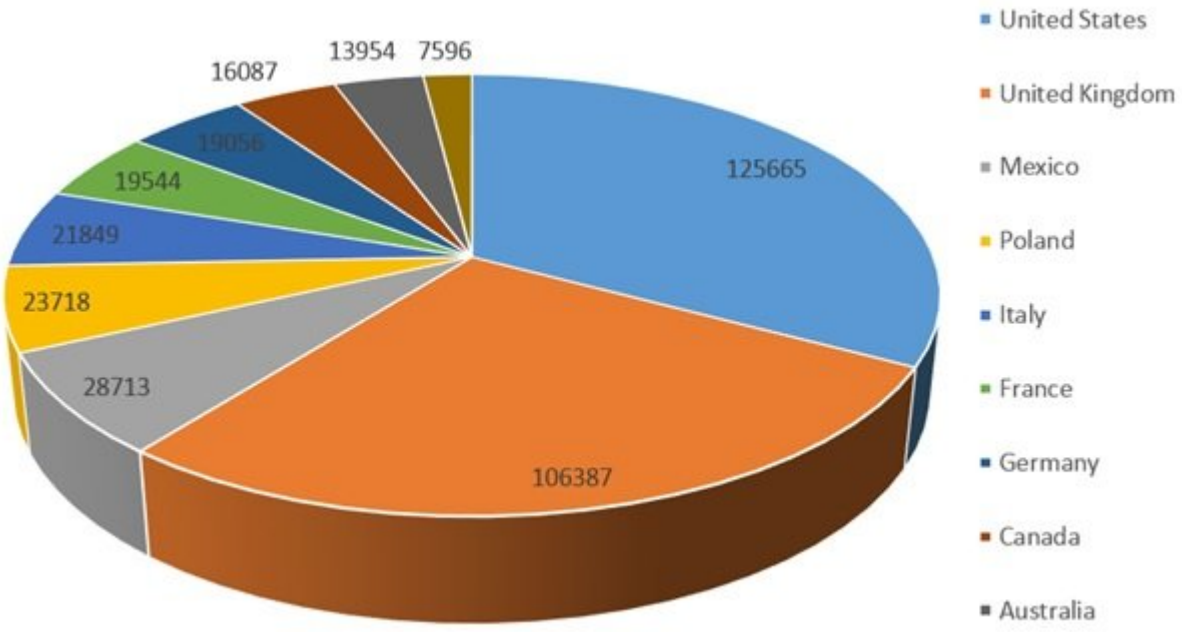
روند رو به رشد افزایش قدرت محاسباتی کامپیوترها و تجهیزات همراه باعث شده است تا زندگی برای حرفه‌ای‌ها ساده‌تر شود. اینترنت نه تنها کاربران را قدرتمند می‌سازد، بلکه انجام وظایف را هم ساده‌تر از گذشته می‌کند. همان‌گونه که قدرت و راحتی برای حرفه‌ای‌ها به همراه می‌آورد، برای هکرها نیز راحتی به همراه می‌آورد. پیاده‌سازی طیف گسترده‌ای از حملات بدافزاری و دستکاری گسترده ربات‌های تحت شبکه به جای آن‌که برای هکرها به یک کابوس وحشتناک و یک واقعیت سخت تبدیل شود، به یک کار بسیار ساده تبدیل شده است. به طور مثال، در سالی که گذشت حملات بدافزاری مبتنی بر ماکروها به طور چشمگیر و فزاینده‌ای قدرتمندتر از گذشته به وقوع پیوست.

ترفندهای مهندسی اجتماعی درها را به روی حملات بدافزاری ماکرو گشوده است. اما سؤال این‌جاست چگونه می‌توان این در را بست؟

اسناد مملو از بدافزارهای ماکرو، هدفشان ایمیل‌های کاربران بوده و از طریق ایمیل اسپم عمدتا به تحریک حس کنجکاوی هر کاربری می‌پردازند. ایمیل‌هایی که با عنوان فاکتور فروش، رزومه، صورت‌حساب‌های مالیاتی، تأییده‌های مالی و... ارسال می‌شوند؛ کاربران را به آسانی در خصوص خواندن ایمیل‌ها و باز کردن ضمیمه‌ها بدون آن‌که درباره آن فکر کنند، گمراه می‌سازند. کاربر سندی را باز می‌کند که ماکرو در آن فعال است، تصور کنید سند نیازمند یک تابع بوده و ندانسته یک بدافزار ماکرو را فعال کرده و اجرا کند. درست زمانی‌که تصور می‌کنید، بدافزار ماکرو یک موضوع تاریخ مصرف گذشته است، بهتر است نگاهی به چند ماه گذشته داشته باشید که چطور روند دانلود ماکروها نزدیک به 501240 هزار ماشین را در سرتاسر جهان آلوده ساخته است. نمودار زیر این روند افزایش ماکروها را از آوریل 2014 تا آوریل 2015 نشان می‌دهد.



البته اکثر قریب به اتفاق حملات بدافزار ماکرو در کشورهای ایالات متحده و انگلستان و کمترین نوع این حملات در کشور استرالیا به وقوع پیوسته است.

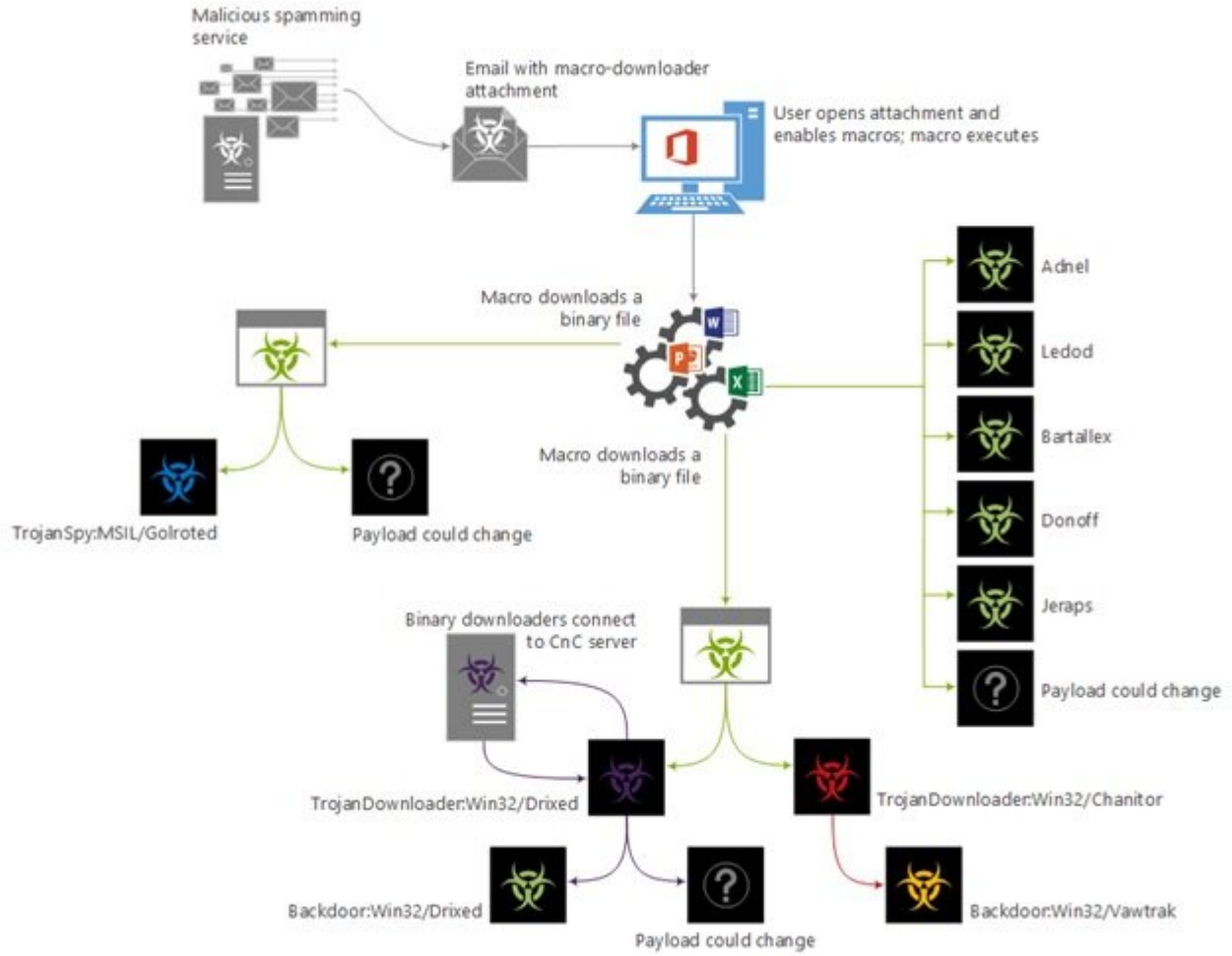


تصویر زیر میزان شیوع این آلودگی را در کشورهای مختلف نشان می‌دهد.

چرخه آلودگی بدافزار مبتنی بر ماکرو

به کارگیری ماکروها در آفیس مایکروسافت برای افزایش بهره‌وری در فرآیندهای اتوماسیون راهگشا است. با این‌حال، نویسندگان بدافزارها از این ویژگی سوءاستفاده می‌کنند. به همین دلیل است که مایکروسافت به طور پیش‌فرض Disable all macros with notification را فعال کرده است. دانلودکننده‌های ماکرو به عنوان دروازه‌ای برای ورود سایر نرم‌افزارهای مخرب به حساب می‌آیند. تصویر زیر نشان می‌دهد چگونه یک دانلود کننده ماکرو معمولی به یک سیستم وارد شده و اقدام به بارگیری بدافزارها می‌کند.

همانگونه که در تصویر زیر مشاهده می‌کنید، سرویس ارسال کننده اسپم کار خود را آغاز می‌کند، ایمیل همراه با ضمیمه macro downloader ارسال می‌شود، کاربر ضمیمه را باز کرده، ماکرو فعال شده و اجرا می‌شود. ماکرو یک فایل باینری را دانلود می‌کند. فایل باینری دانلود شده می‌تواند شامل انواع مختلفی از تهدیداتی که در ادامه به آن‌ها خواهیم پرداخت بوده یا برای اتصال به سرور CnC (سرنام Command and Control) مورد استفاده قرار گیرد.



همان‌گونه که اشاره کردیم، بدافزار ماکرو به عنوان یک ضمیمه ایمیل اسپم به کامپیوتر کاربر وارد می‌شود، دریافت کننده ایمیل اسپم با استفاده از تکنیک مهندسی‌اجتماعی گمراه شده و متقاعد می‌شود که ضمیمه را باز کند، در نتیجه ماکرو داخل سند فعال می‌شود. اما از جمله تروجان‌های دانلودکننده ماکروهای قدرتمند به موارد زیر می‌توان اشاره کرد:

- Adnel

این تهدید یک ماکرو مخرب بوده که توانایی دانلود و اجرای فایل‌ها را روی کامپیوتر قربانی دارد. این تهدید زمانی‌که یک فایل آفیس آلوده مایکروسافت را باز کنید اجرا می‌شود. Adnel در صفحات گسترده اکسل یا فایل ورد قرار می‌گیرد.

- Bartallex

بدافزاری از خانواده Bartallex بوده که توانایی دانلود و اجرای فایل‌ها را روی کامپیوترهای شخصی دارد. این تهدیدات به صورت جایگذاری شده در فایل‌های ورد از طریق ایمیل‌های اسپم ظاهر می‌شوند.

- Donoff

عملکردی همانند دو مورد قبل دارد.

- Jeraps

این تهدید اقدام به دانلود و نصب برنامه‌های مختلف روی کامپیوتر کاربر، بدون رضایت او می‌پردازد که بدافزارها نیز در فهرست این برنامه‌های نصب شده قرار دارند.

Ledod•

این تهدید نیز عملکردی مشابه Jeraps دارد.

زمانی‌که یک کد مخرب ماکرو اجرا می‌شود، می‌تواند برای بارگیری نهایی خودش مورد استفاده قرار گرفته یا برای بارگیری دیگر دانلودکننده‌های اجرایی مورد استفاده قرار گیرد. بارگیری تروجان TrojanSpy:MSIL/Golroted نمونه‌ای از این موارد به شمار می‌رود. این تهدید برای جمع‌آوری اطلاعات حساس و ارسال آن‌ها برای هکر مورد استفاده قرار می‌گیرد.

همچنین دانلود کننده‌های اجرایی وابسته به این ماکروها به شرح زیر هستند، هرچند محدود به این دو مورد نمی‌شوند:

TrojanDownloader:Win32/Drixed (برای نصب برنامه‌ها و بدافزارها بدون رضایت کاربر مورد استفاده قرار می‌گیرد)

TrojanDownloader:Win32/Chanitor (عملکردی همانند تهدید قبل دارد)

بعد از آن‌که بدافزار ماکرو دانلود شد، قسمت زیادی از کار انجام شده است. مابقی کار در ارتباط با بارگیری نهایی یا دانلود کننده اجرایی قرار دارد. تهدیدات دانلود شده توسط فایل‌های اجرایی شبیه به دو مورد زیر هستند، هرچند محدود به این دو مورد نمی‌شوند.

Backdoor:Win32/Drixed (این تهدید امکان دستیابی و کنترل بدون مجوز هکر را بر روی کامپیوتر کاربر فراهم می‌کند.)

Backdoor:Win32/Vawtrak (این تهدید نه تنها دستیابی به کامپیوتر کاربر را برای هکر امکان‌پذیر می‌سازد، بلکه اطلاعات شخصی کاربر از قبیل نام و گذرواژه‌هایی که برای سایت‌های بانکی مورد استفاده قرار داده است را نیز سرقت می‌کند.)

پیشگیری، چگونه می‌توان این در را بست؟

اگر درباره ترفندهای مهندسی اجتماعی که از طریق ضمیمه‌های اسپم برای باز کردن در به روی حملات بدافزارهای ماکرو اطلاع دارید، سؤال این‌جاست، چگونه می‌توانید از زیرساخت امنیتی سازمان نرم‌افزاری خود با بستن این در محافظت به عمل آورید؟

در خصوص فعال‌سازی ماکروها دقت کنید

تهدیدات ماکرو، به نظر می‌رسد عمدتا برای بارگیری مورد استفاده قرار می‌گیرند، اما بر خلاف کیت‌های اکسپلویت این نوع از تهدیدات ماکرو برای اجرا به رضایت کاربر نیاز دارند. برای اجتناب از اجرای این تهدیدات قبل از آن‌که ماکروها را فعال کنید، سعی کنید جزییات بیشتری را برای پیشگیری از آلوده شدن در مورد ماکرو به دست آورید. به دست آوردن اطلاعات بیشتر درباره گزینه‌های پیکربندی و فهمیدن سناریو زمانی‌که آن‌ها را فعال یا غیرفعال می‌کنید مفید هستند تا بدانید چگونه می‌توانید تنظیمات ماکروها را با استفاده از کلیدهای رجیستری و جزییات بیشتر کنترل کنید. مایکروسافت مقاله‌ای تحت عنوان "تنظیمات ماکرو را چگونه با استفاده از کلیدهای رجیستری می‌توان کنترل کرد"، دارد.

گذشته از آن، باز کردن ایمیل‌های مشکوک خطرات زیادی به همراه دارد. همچنین، ضمیمه ایمیل‌ها یا لینک‌هایی که از منابع غیرقابل اعتماد می‌آیند را باز نکنید.

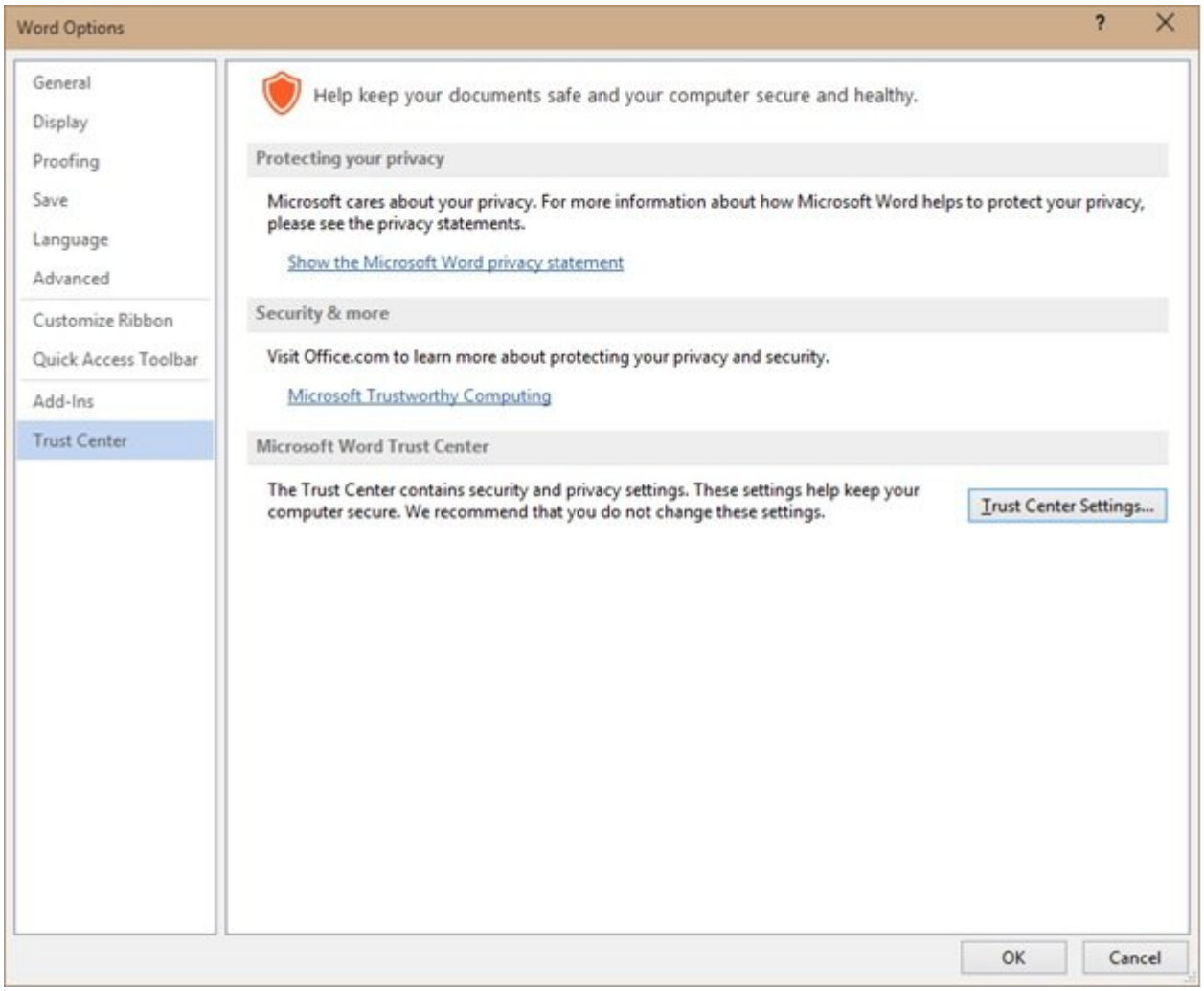
اگر مدیر امنیتی یک سازمان نرم‌افزاری هستید، چه باید انجام دهید؟

در بیشتر موارد ولی نه همیشه، بدافزار ماکرو در قالب یک سند doc که در آفیس 2007 و نسخه‌های قدیمی‌تر قرار دارد، ارسال می‌شود. نرم‌افزار امنیتی مایکروسافت خودتان را به‌روز کنید ، مایکروسافت این نوع از تهدیدات را شناسایی کرده و همیشه کاربران را تشویق به اجرای آخرین نسخه از یک نرم‌افزار برای محافظت از خودشان

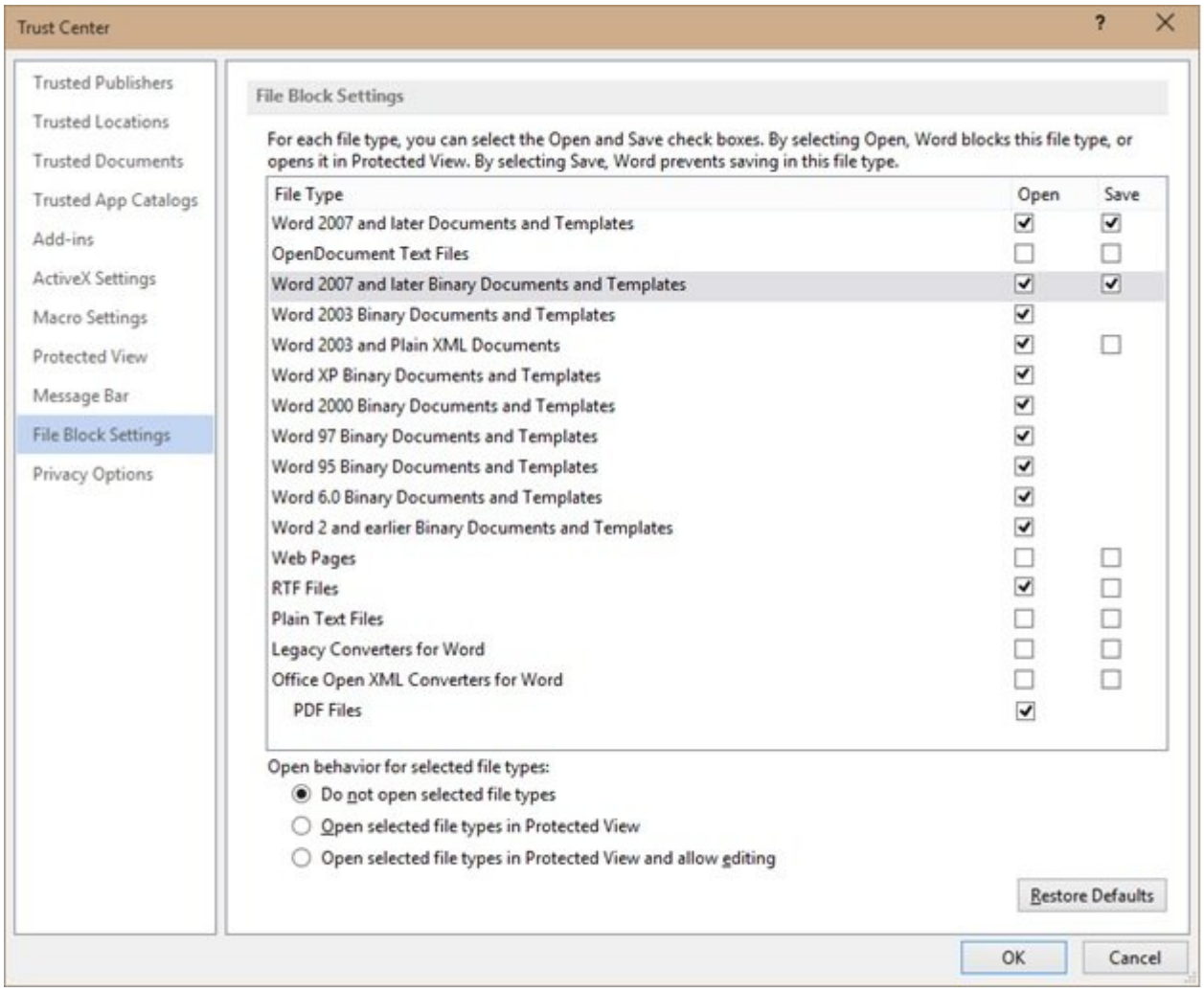
می‌کند. برای دریافت جزییات بیشتر در خصوص به‌روزرسانی از این آدرس استفاده کنید.

اطمینان حاصل کنید تنظیمات Trust Center برای بارگذاری نکردن نسخه‌های قدیمی‌تر آفیس پیکربندی شده باشد.

1.به Word Options رفته روی گزینه Trust Center و سپس Trust Center Settings کلیک کنید.



2. در پنجره Trust Center گزینه File Block Settings را انتخاب کنید. سپس نسخه‌ای از ورد که می‌خواهید آن‌را بلوکه کنید انتخاب کنید.



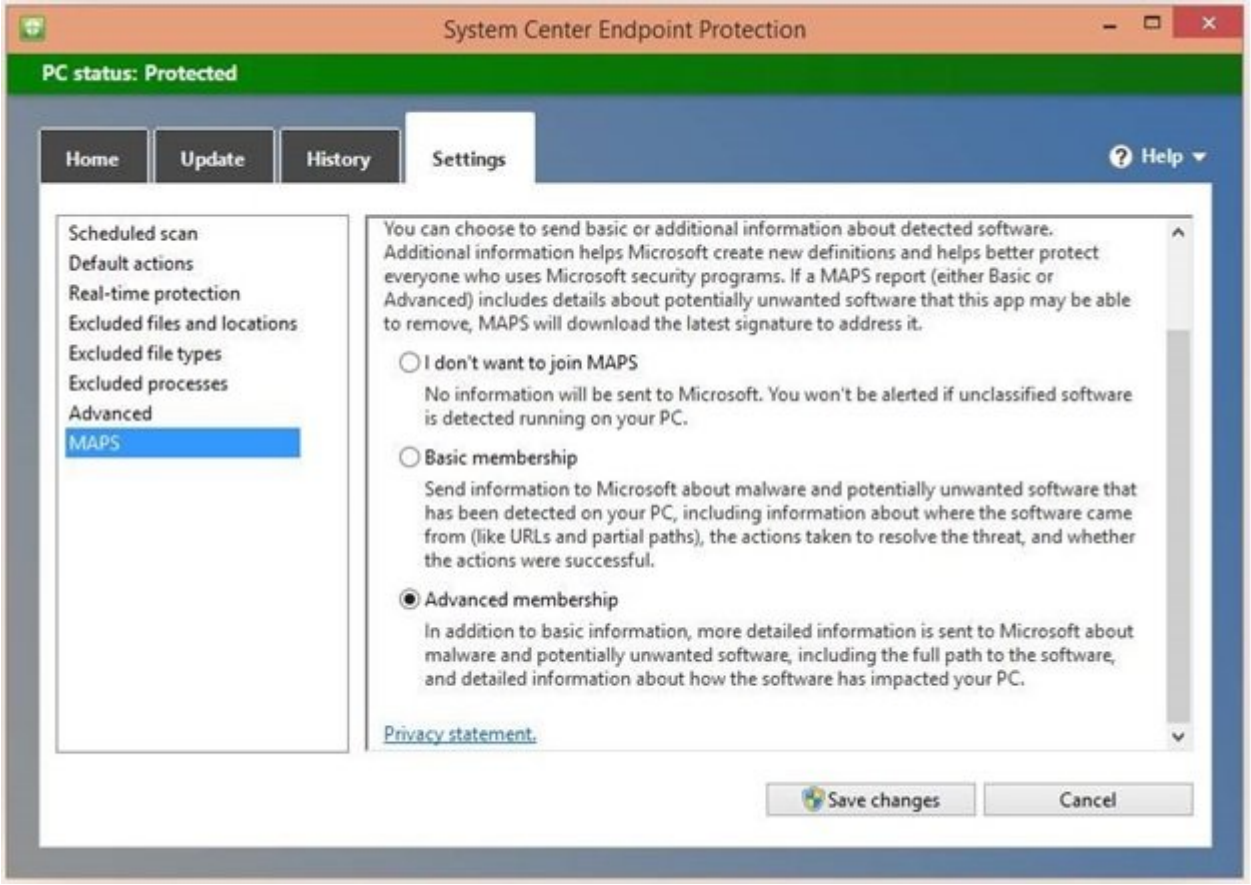
فرآیند باز کردن نسخه‌های قدیمی آفیس را بلوکه کنید.

از سرویس Exchange Online Protection متعلق به مایکروسافت که برای فیلتر کردن اسپم‌ها و حذف ویروس‌های کامپیوتری از پیام‌های ایمیل مورد استفاده قرار گرفته و برای هر کسب و کاری ضروری است استفاده کنید. این سرویس نیازی به نصب برنامه کلاینتی ندارد.

آفیس 365 با بهره‌مندی از تکنیک یادگیری ماشینی به شما در بلوکه کردن اسپم‌ها کمک می‌کند.

پیام‌های اسپم و پیام‌های غیراسپم را برای تجزیه و تحلیل به این آدرس برای مایکروسافت ارسال کنید.

ویژگی MAPS (سرنام Microsoft Active Protection Service) را فعال کنید. کاربران با استفاده از MAPS از مزیت‌های محافظت ابری مایکروسافت و محافظت در برابر جدیدترین بدافزارها ایمن خواهند شد. MAPS به طور پیش‌فرض روی Microsoft Security Essentials و ویندوز دیفندر (Windows Defender) در ویندوز 8.1 فعال است. برای اطمینان از این‌که آیا MAPS روی محصول امنیتی مایکروسافت فعال است یا خیر ، به زبانه Settings رفته و سپس MAPS را مشاهده کنید.



سخن آخر

در حالی‌که خیلی از کاربران تصور می‌کنند این نوع از حملات از بین رفته‌اند، در تاریخ 29 آوریل سایت scmagazine گزارش داد، بدافزار ماکرویی توسط ترند ماکرو شناسایی شده است که لینکی به یک صفحه دارپ‌باکس دارد و سعی در متقاعد کردن کاربر برای فعال کردن ویژگی ماکرو در آفیس مایکروسافت دارد. اگر ماکرو فعال شود، سند آلوده به بدافزار BARTALEX اقدام به آزادسازی بدافزار بانکی Dyre می‌کند. هرچند درگذشته سرویس‌های ابری چندین بار در حملات مورد استفاده قرار گرفته‌اند اما این اولین باری است که یک بدافزار ماکرو از دارپ‌باکس برای میزبانی استفاده می‌کند. برای دریافت اطلاعات بیشتر در خصوص این بدافزار به این آدرس مراجعه کنید.

حملات بدافزار مبتنی بر ماکرو به طور طبیعی محدود است، در نتیجه برای آن‌که در مقیاس بزرگ بتوانند عمل کنند باید از درجه بالایی از سادگی برخوردار باشند. به همین دلیل ایمیل، اسلحه‌ای است که مورد انتخاب توزیع کنندگان بدافزار ماکرو قرار دارد. فریب کاربران به این‌که آن‌ها سند خیلی مهمی را دریافت کرده‌اند کلید موفقیت این بدافزار به شمار می‌رود.

تاریخ انتشار:
19 اردیبهشت 1394

نشانی منبع: https://www.shabakeh-mag.com/security/608