باج افزار (Ransomware) در چند سال اخیر به شدت گسترش یافته و مجرمان سایبری از این طریق به اخاذی از اشخاص می پردازند.

به صورت کلی کاری که باج افزار انجام می دهد این است که فایل های سیستم شما را رمزنگاری می کند و در قبال رمزگشایی و بازیابی داده ها از شما اخاذی و درخواست پرداخت هزینه و باج می کند.

در بیشتر موارد به دلیل وجود تکنولوژی های پیشرفته رمزنگاری استفاده شده در این نوع بدافزارها، رمزگشایی داده ها کاری دشوار است.

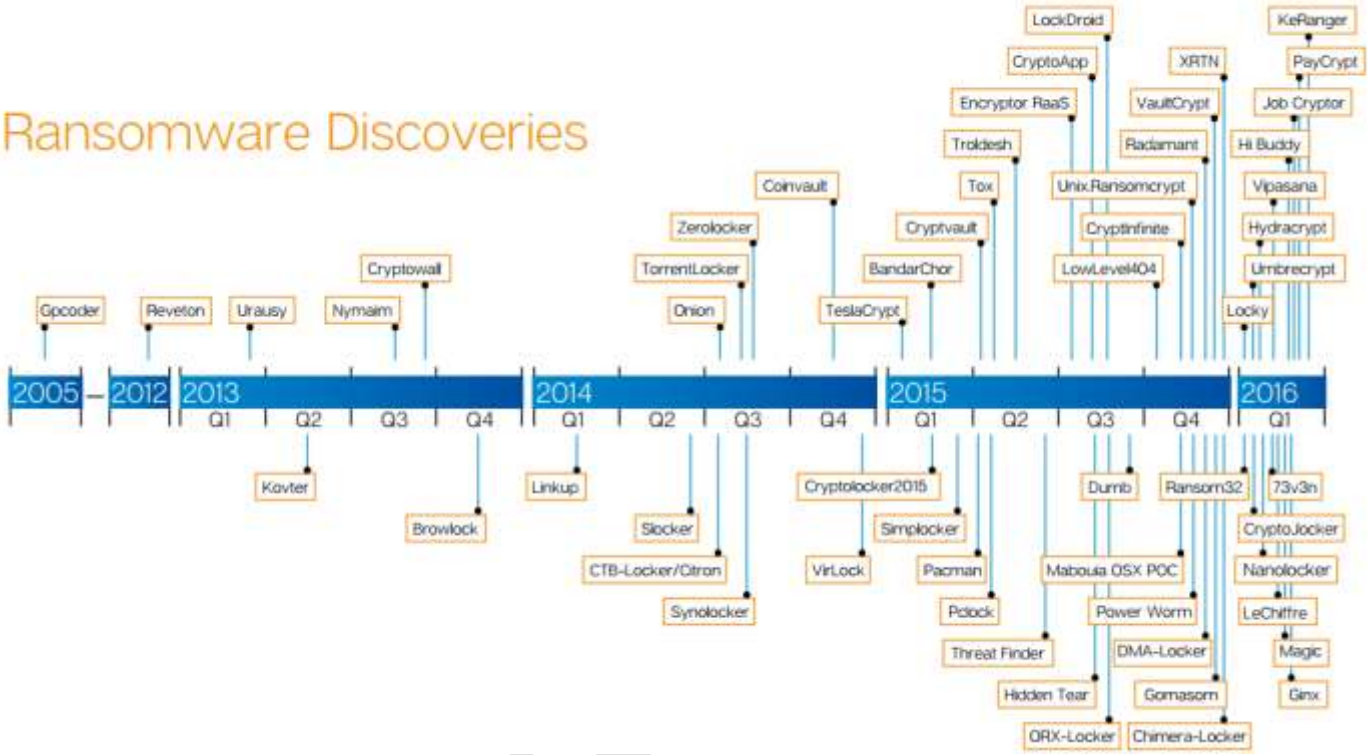
باج افزار دارای 2 مدل است:

1-**File Encrypting** : که در این روش فایلها رمزنگاری میشود.

2- **Screen Locker**: که صفحه نمایش کاربر قفل میشود واجازه کار کردن نمیدهد.که در این روش با تعویض ویندوز مشکل برطرف میشود و دسترسی به اطلاعات میسر میشود.(به این روش غیر رمزنگار نیز گفته میشود)

بحث اصلی ما در این مقاله مدل اول یعنی رمزنگاری داده ها میباشد.

متاسفانه باج افزارها مانند قارچ در حال رشد و نمو هستند و روز به روز نیز نسخه های جدید تر آنها در سر تا سر اینترنت منتشر میشود که از سال 2005 تا به حال ادامه داشته و متاسفانه تاکنون کاربران ایرانی زیادی هم گرفتار این باج افزارها شده اند.در سال 2016 که بیشترین ورژنها ایجاد شده همراه با سخت ترین نوع الگوریتم رمزنگاری



منبع عکس: https://heimdalsecurity.com/blog/anti-ransomware-protection-plan

باج افزار از دونوع رمزنگاری استفاده میکنند. 1- رمزنگاری متقارن 2-رمز نگاری نامتقارن

رمزنگاری متقارن(رمز نگاری کلید خصوصی):

از یک کلید برای رمز گذاری و رمزگشایی استفاده میشودو دارای سرعت بالاتری است.نمونه هایی از الگوریتم های متقارن شناخته شده عبارتند از Twofish، Serpent، AES، Blowfish، CAST5، RC4، DES، و IDEA

رمزنگاری نامتقارن(رمز نگاری کلید عمومی):

از دوکلید برای رمزگذاری و رمز گشایی استفاده میکند که دارای امنیت بالاتری است. نمونه هایی از الگوریتم های متقارن شناخته شده عبارتند از RSAو Diffie–Hellman

که مجرمان باج افزار از هر دو مدل استفاده میکنند.

مثلا باج افزارهای CryptoWallو CTB-Locker از نوع نامتقارن و CryptographicLocker و TorrentLocker از نوع متقارن هستند.

این مجرمین سایبری به علت آنکه برای دریافت پولهایی که میخواهند به عنوان باج دریافت کنند از روش دریافت پولهای دیجیتال(بیت کوین) استفاده میکنند کاملا ناشناس باقی مانده اند.

بیت کوین(Bitcoin)نوعی پول دیجیتال بر پایه شبکه همتا به همتا است و به کاربران امکان می‌دهد که بدون هیچ واسطه‌ای، انتقال پول غیرقابل بازگشت وغیرقابل ردیابی انجام دهند.یعنی فرستنده و گیرنده پول پنهان می مانند.جهت استفاده از آن باید دارای یک کیف پول دیجیتال شد.که شخص مورد نظر برنامه آن را روی کامپیوتر خود نصب میکند.

تعداد زیادی از باج افزارها با استفاده از روشهای مهندسی اجتماعی سعی در گول زدن قربانیان خود برای ورود به سیستم هایشان و در نهایت قفل کردن فایلها و باج خواهی از قربانی میکنند.

برای **مثال** روش یکی از باج افزارهای خطرناک با نام Petya را در زیر برایتان شرح میدهیم:

سناریوی این باج افزار برای فریب قربانی به شرح زیر است:

ابتدا یک ایمیل جعلی از طرف مجرمان سایبری برای تعداد زیادی از کاربران در سطح اینترنت ارسال میشود. مجرمان سایبری که باج افزار Petya را طراحی کرده اند معمولا ایمیل شرکتها و کسب و کارها را هدف قرار میدهند. از طرف برخی شرکتهای ایرانی هم گزارش شده است که برخی باج افزارها، ایمیل برخی شرکتهای ایرانی را نیز هدف قرار داده اند.

و اما در ادامه ...

کارمند و یا مدیر شرکت، ایمیل مجرمان سایبری را در قالب تقاضای فردی برای استخدام دریافت میکند. ایمیل حاوی یک لینک Dropbox است که ظاهرا آن فرد مدعی است که رزومه کاری خود را در آن لینک قرار داده و از خواننده ایمیل میخواهد برای مشاهده روزمه کاری اش به لینک موجود در ایمیل و فایل حاوی رزومه مراجعه نماید .

کلیک بر روی لینک و باز کردن فایل همان و آلوده شدن سیستم قربانی همان!

پس از آلوده کردن سیستم قربانی، باج افزار سعی میکند خودش را از طریق شبکه به دیگر سیستمهای موجود نیز برساند و آنها را نیز آلوده کند .

همچنین به محض اتصال فلش و یا دیگر درایوهای با پورتUSB ، باج افزار خود را به آنها نیز منتقل میکند و علاوه بر آلوده کردن آنها، در صورتیکه آن فلش به دستگاه دیگری متصل بشود ، قربانی بعدی را نیز میگیرد.

البته این تنها یکی از روشهای باج افزارها برای آلوده کردن سیستم قربانیست. چنین لینکهایی میتوانند به وفور در محیط های چت، شبکه های اجتماعی و یا سایتهای بی هویت نیز وجود داشته باشد.

باج افزارها پس از ورود به سیستم قربانی در ابتدا اقدام به جستجوی هارد دیسک شخص قربانی کرده و فایلهای مهم از جمله تصاویر، فایلهای آفیس، پروژه های نرم افزاری اتوکد، فتوشاپ، تری دی مکس و دیتا بیس ها از جمله SQL ودر نسخه جدید تر فایل های شرکت Vmware با فرمت ما vmdk و ماشین های مجازی Hyper-v شرکت ماکروسافت و گروپ پالیسیها و SYS Vol دامین کنترلرها و هر فایلی که از نظر آنها مهم است را پیدا میکند و رمز گذاری می کند. البته به سیستم عامل آسیبی نمیزند تا قربانی بتواند به راحتی باج را از طریق اینترنت برای مجرمین پرداخت نماید.

قابل ذکر است که این ویروس نیست که انتظار داشته باشیم آنتی ویروس جلوی آنرا بگیرد فقط باید کاربر دقت خود را بالا ببرد.(البته بعضی از ورژنهای قدیمی این باج افزار قابل شناسایی می باشد)

نحوه آلودگی باج افزار

باز کردن فایل های پیوست)یکی از موارد مهم فایلهای word میباشد (از افراد ناشناس در ایمیل

باز کردن لینکهای جعلی در سایتها یا شبکه های اجتماعی

استفاده از برنامه ها و بازیهای رایگان

علایم یک ایمیل مشکوک:

-1ایمیل که انتظار آنرا داشتید در غیر ساعت اداری دریافت شده.

-2دریافت ایمیل از فردی که نمی شناسید.

-3ناهماهنگی موضوع عنوان شده subject))با پیغام ایمیل

-4عدم شناخت نسبت به افرادی که ایمیل هم برای آنها ارسال شده).در قسمت cc نام افراد ناشناس نیز وجود داشته باشد(

-5دامنه فرستده ایمیل ناشناس و مشکوک باشد trevor .

mann<manntrevor8495@dneturbayb.id>

-6ایمیل که دارای فایل پیوست با قالبهای word-excel-zip و به ویژه دارای عبارت invoice باشد.

-7تشویق به کلیک بر روی لینک مشخص شده.

نکته خیلی مهم :اگر به هر دلیلی دستگاه شما به این باج افزار آلوده شد اولین کار که باید انجام دهید ارتباط خود با شبکه را قطع نمایید یعنی کشیدن کایل شبکه و یا خاموش کردن وایرلس دستگاه خود.

راه های پیشگیری از باج افزار

1- مهمترین و اصلی ترین مورد آموزش کاربران و حتی کارشناسان و ادمین ومدیران IT هست که باید دقت کافی در باز کردن ایمیل های ناشناس و سایت جعلی داشته باشند.

2- غیر فعال ماکرو در آفیس از طریق گروپ پالیسی در دامین(که در ادامه مقاله توضیح خواهم داد.)

البته این کار را روی لپ تاپ ها و PC های شخصی حتما انجام بدین.

3- داشتن آنتی ویروس آپدیت و کاملا به روز شده

4- فعال کردن آنتی اسپم در فایروال –میل سرور-آنتی ویروس

5- به روز بودن ونصب آخرین اصلاحیه های امنیتی ویندوزها

6- نصب نرم افزارهای زیر در صورت نیاز

Bitdefender BDAntiransomware

Mcafee Ransomware Interceptor

7- محدود کردن سطح دسترسی کاربران

لازم است که ذکر کنم اگر سیستم کاربری به باج افزار آلوده شود. تمام فایل هایی که دسترسی داره رمزگذاری و آلوده میشود از جمله File sharing ها –دیتابیس های SQL مالی – sharepoint و غیره وفایلهای VMDK برای شرکت مجازی سازی VMware

8 – و در آخر داشتن نسخه پشتیبان از تمامی فایلها به صورت مداوم

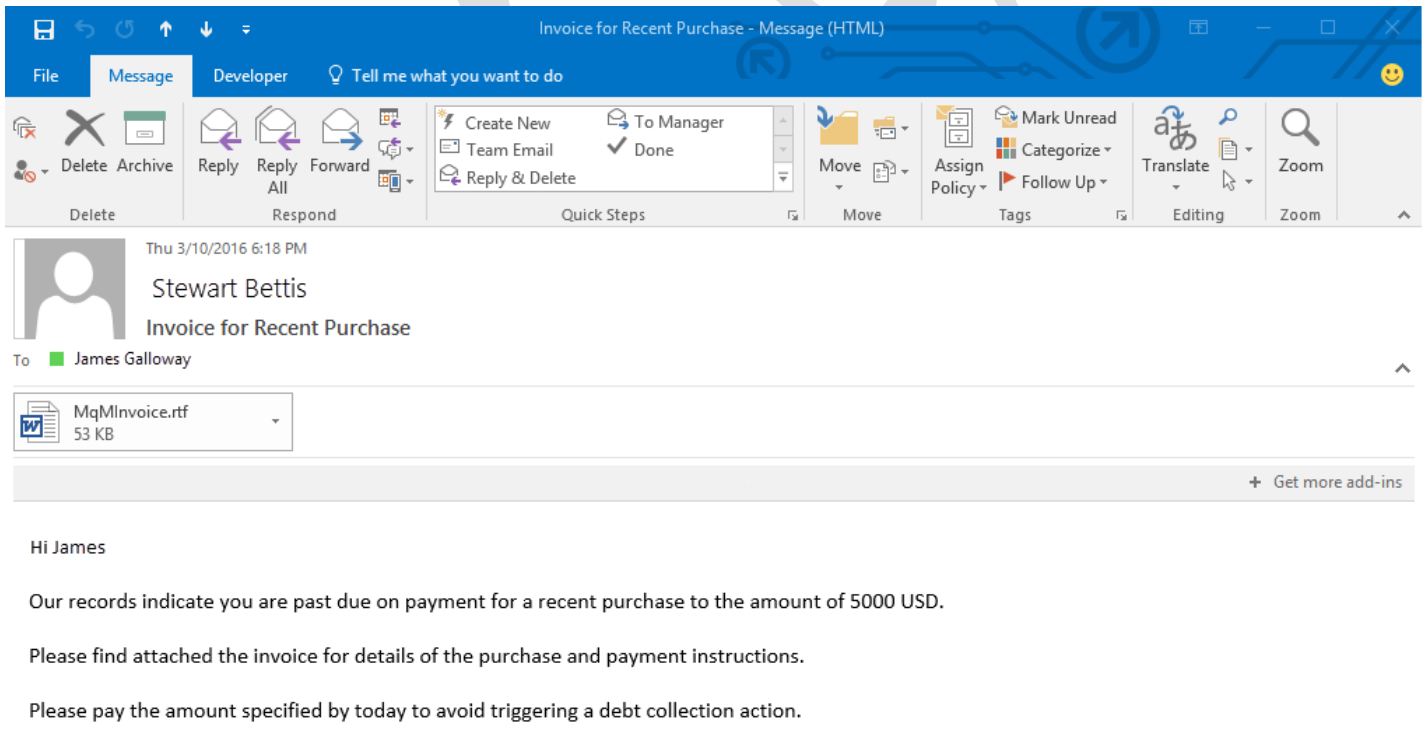
همونطور که ملاحضه میکنید حداکثر 96 ساعت به شما فرصت داده تا پول مجازی (باج)که واحد پولی آن بیت کوین و غیر قابل ردیابی هست رو واریز کنید.درغیر این صورت اصلا قابل بازگشایی رمز نخواهد بود

منظور از ماکروها چیست؟؟

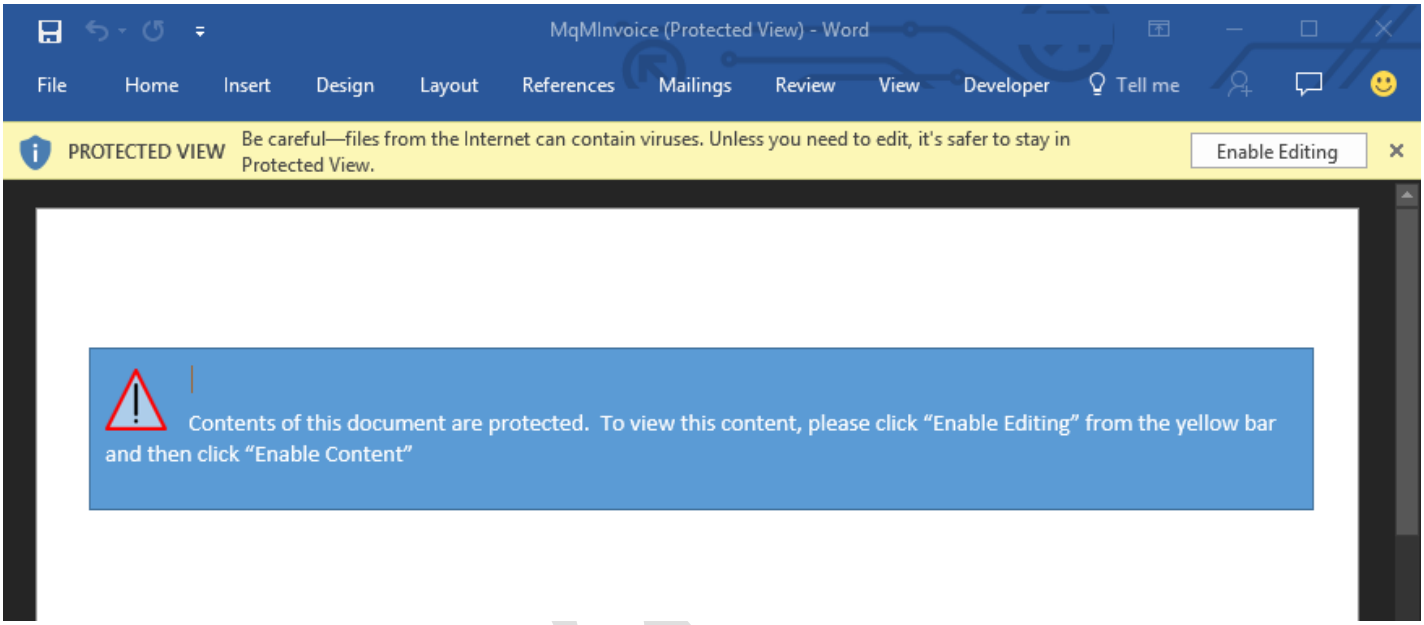
ماکرو (Macro) در حقیقت دستورات و عملیات ضبط شده‌ای است که در مواقع نیاز با یک کلیک فراخوانی می‌شوند .کاربرد آن‌ها مشخص است: مجموعه عملیاتی که باید هر بار تکرار کنید را در قالب یک ماکرو تعریف می‌کنید و از این پس به جای انجام آن همه کار، فقط کافی‌ست آن ماکرو را Runکنید.

به طور مثال فرض کنید همیشه بعد از دریافت یک مقاله، آن را بر اساس اصول تایپ فارسی تصحیح کنید. برای این کار، بیش از 30 کار تکراری نیاز است .مثلاً هر کجا "می شود" می‌بینید، به "می‌شود" تبدیل کنید تا فاصله مجازی رعایت شود و...

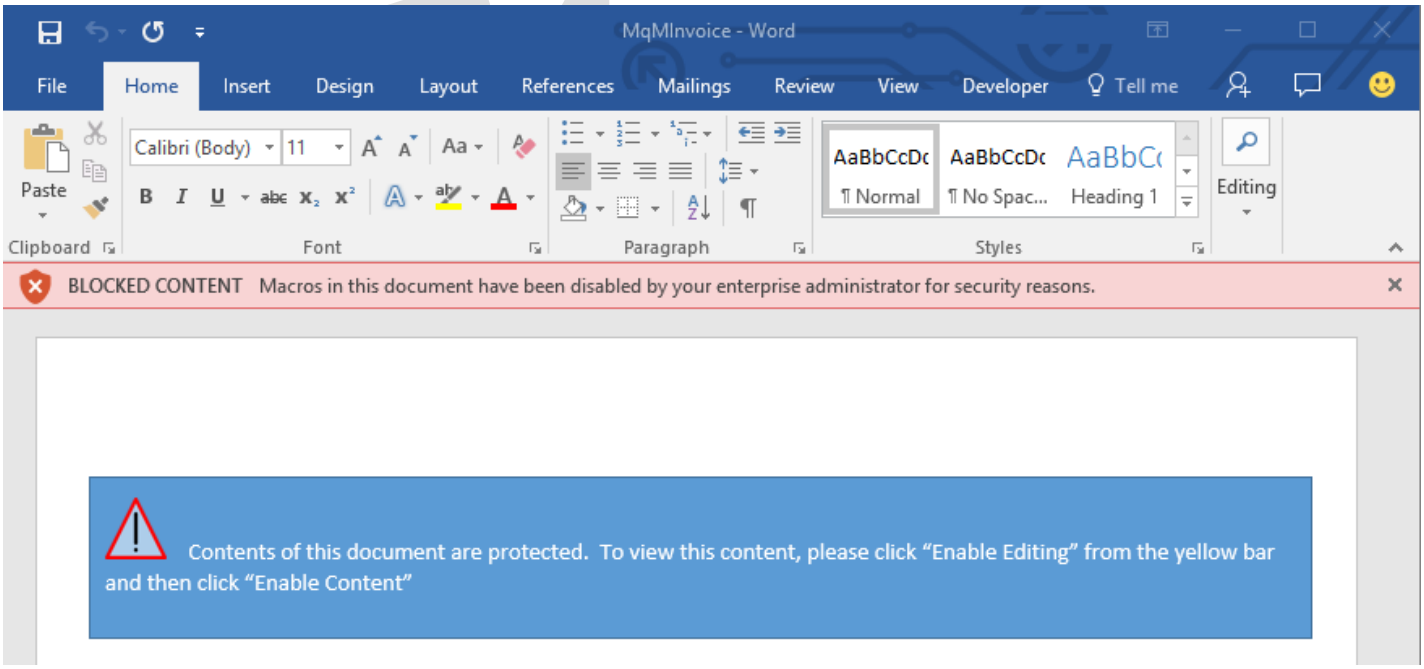
در شکل زیر یک ایمیل که دارای محتوای یک فایل ورد است برای شما ارسال شده.



زمانی که فایل را میخواهید باز کنید از شما درخواست فعال کردن ماکرو جهت دیدن محتوای متن را میدهد (شکل زیر).



که شما باید آن را غیر فعال کنید تا کاربر تصویر زیر را مشاهده کند.



نحوه غیرفعال کردن ماکرو با Group Policy در Word, Excel, PowerPoint

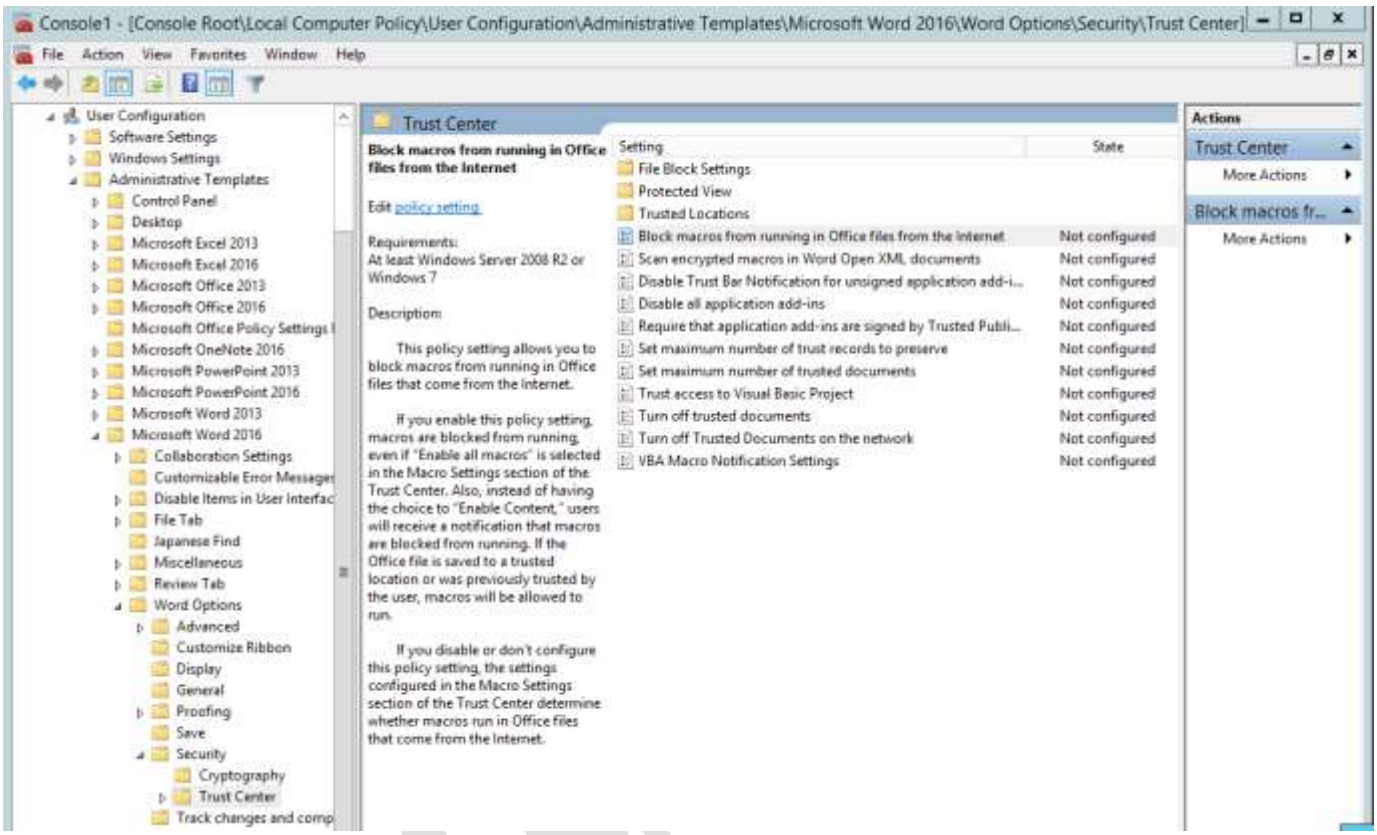
برای آفیس 2016 توضیح داده میشود که شما باید این کار رای برای ورژنی که در شبکه خودتان استفاده میکنید انجام بدهید.

ایتدا فایل Office 2016 Administrative Template files (ADMX/ADML) را از لینک زیر دانلود کنید.

https://www.microsoft.com/en-us/download/details.aspx?id=49030

طبق روش زیر انجام دهید.

1. Open the Group Policy Management Console, right-click the Group Policy Object you want to configure and click **Edit**.
2. In the **Group Policy Management Editor**, go to **User configuration**.
3. Click **Administrative templates** > **Microsoft Word 2016** > **Word options** > **Security** > **Trust Center.**
4. Open the **Block macros from running in Office files from the Internet** setting to configure and enable it.
5. Open **VBA Macro Notification Setting** ,enable it and Disable all with Notification



در صورت داشتن سوال میتوانید با **@network2000** (تلگرام) در تماس باشید.

با تشکر

رضا فتحی