

**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 و اجازه 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)

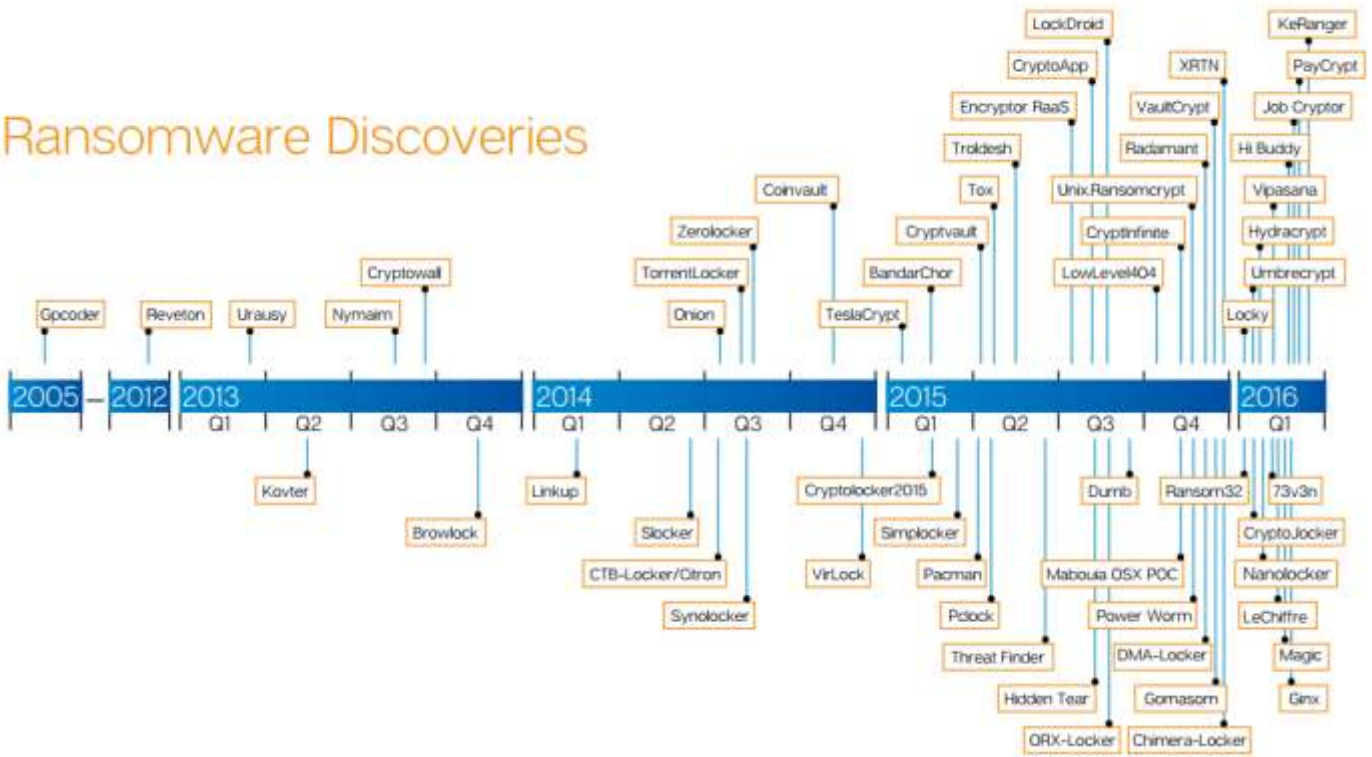
بحث اصلی ما در این مقاله مدل اول یعنی رمزنگاری داده ها میباشد.

متأسفانه 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 متأسفانه تاکنون کاربران ایرانی زیادی هم گرفتار

این باج افزارها شده اند. در سال 2016 که بیشترین ورژنهای ایجاد شده همراه با سخت ترین نوع الگوریتم رمزنگاری

## Ransomware Discoveries



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

باج افزار از دو نوع رمزنگاری استفاده میکنند. 1- رمزنگاری متقارن 2- رمزنگاری نامتقارن

### رمزنگاری متقارن (رمزنگاری کلید خصوصی):

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

IDEA

### رمزنگاری نامتقارن (رمزنگاری کلید عمومی):

از دو کلید برای رمزگذاری و رمزگشایی استفاده میکند که دارای امنیت بالاتری است. نمونه هایی از الگوریتم های متقارن شناخته شده عبارتند از Diffie-Hellman و RSA

که مجرمان باج افزار از هر دو مدل استفاده میکنند.

مثلا باج افزارهای CryptoWall و 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 می دهد که بدون هیچ واسطه ای، انتقال پول غیر قابل بازگشت و غیر قابل 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 میدهم:

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 ظاهراً آن فرد مدعی است که رزومه کاری خود را در آن لینک قرار داده و از خواننده ایمیل میخواهد برای مشاهده رزومه 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 پورت USB ، 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 و در 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 فایل های word میباشد) (از افراد ناشناس در ایمیل

باز کردن لینکهای جعلی در سایتها یا شبکه های اجتماعی

استفاده از برنامه ها و بازیهای رایگان

### علائم یک ایمیل مشکوک:

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

2- دریافت ایمیل از فردی که نمی شناسید.

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

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

5- دامنه فرستنده ایمیل ناشناس و مشکوک باشد trevor

`mann<mantrevor8495@dneturbayb.id>`

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

7- تشویق 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 کابل 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 و مدیران 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 گروه 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 و نصب 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 و فایل های VMDK

برای شرکت مجازی سازی VMware

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



The image shows a ransomware warning screen for CTB-Locker. At the top right, there are four small flags: Germany, Hungary, Italy, and the United States. The main heading in red text reads: "Your personal files are encrypted by CTB-Locker." Below this, the text explains that documents, photos, databases, and other important files have been encrypted with the strongest encryption and a unique key generated for this computer. It states that the private decryption key is stored on a secret Internet server and that nobody can decrypt the files until payment is made to obtain the key. A yellow warning message says: "You only have 96 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them." Below this, instructions are given: "Press 'View' to view the list of files that have been encrypted." and "Press 'Next' for the next page." A red warning triangle icon is followed by a red warning message: "WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION." At the bottom, there are three yellow buttons: "View", a timer showing "95 20 15", and "Next >>".

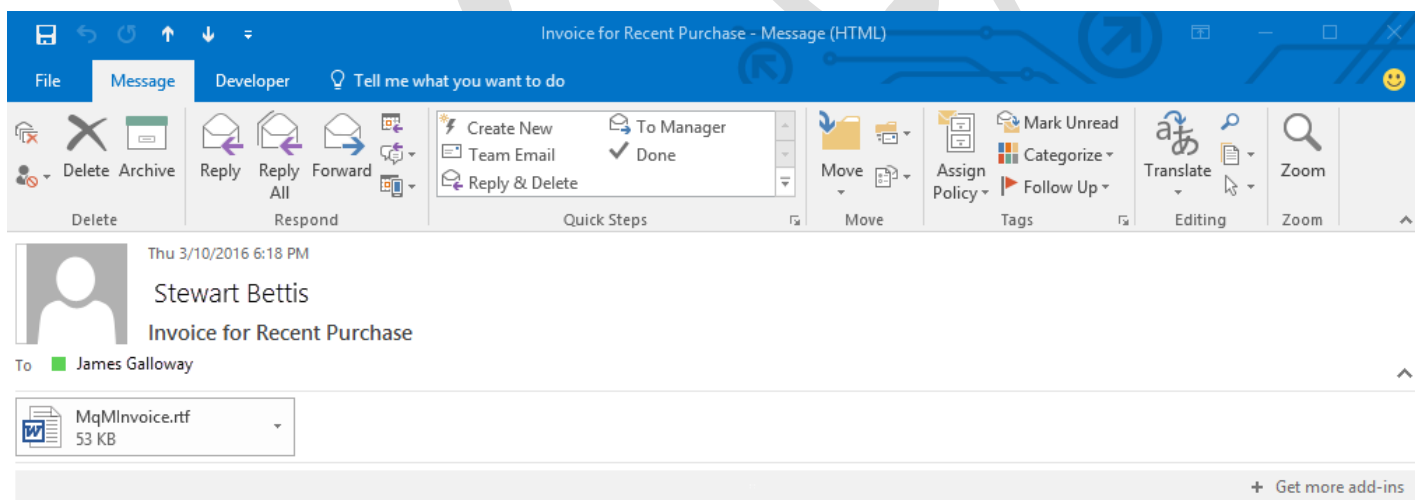
همونطور که ملاحظه میکنید حداکثر 96 ساعت به شما فرصت داده تا پول مجازی (باج) که واحد پولی آن بیت کوین و غیر قابل ردیابی هست رو واریز کنید. در غیر این صورت اصلا قابل بازگشایی رمز نخواهد بود

## 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 Run کنید.

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.



The screenshot shows an Outlook email window titled "Invoice for Recent Purchase - Message (HTML)". The interface includes a ribbon with "File", "Message", and "Developer" tabs. The "Message" ribbon is active, showing options like "Delete", "Archive", "Reply", "Reply All", "Forward", "Quick Steps", "Move", "Assign Policy", "Tags", "Editing", and "Zoom". The email content shows a sender "Stewart Bettis" with a profile picture, dated "Thu 3/10/2016 6:18 PM". The subject is "Invoice for Recent Purchase" and the recipient is "James Galloway". An attachment "MqMInvoice.rtf" (53 KB) is visible. At the bottom right, there is a link to "Get more add-ins".

Hi James

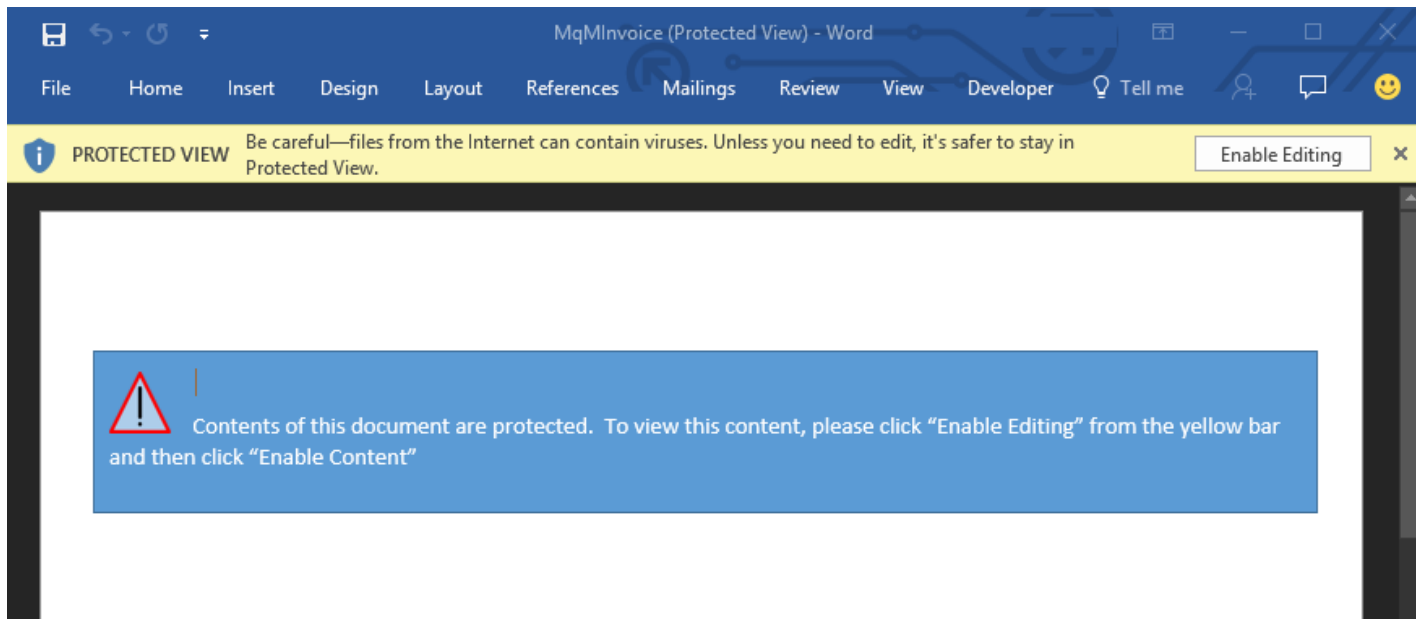
Our records indicate you are past due on payment for a recent purchase to the amount of 5000 USD.

Please find attached the invoice for details of the purchase and payment instructions.

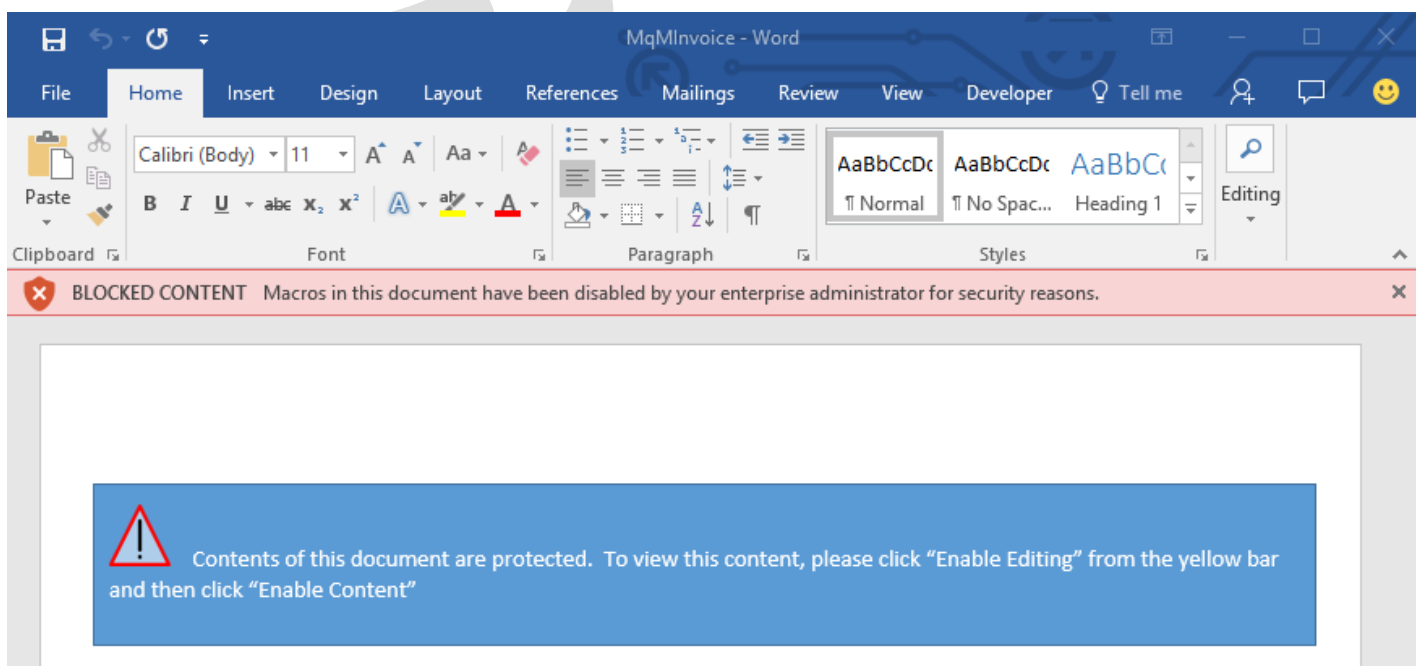
Please pay the amount specified by today to avoid triggering a debt collection action.



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

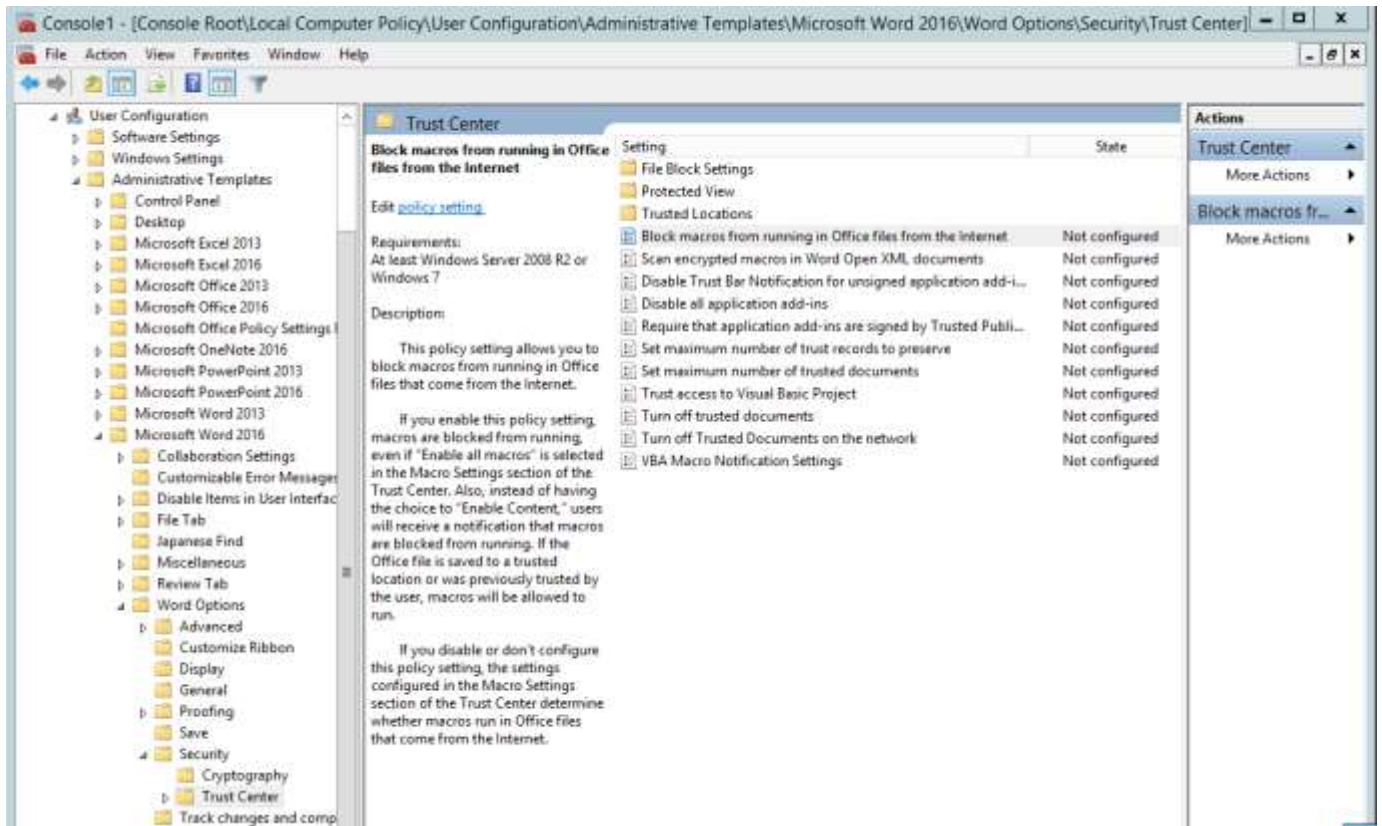
برای آفیس 2016 توضیح داده میشود که شما باید این کار را برای ورژنی که در شبکه خودتان استفاده میکنید انجام بدهید.

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](https://t.me/network2000) (تلگرام) در تماس باشید.

با تشکر

رضا فتحی