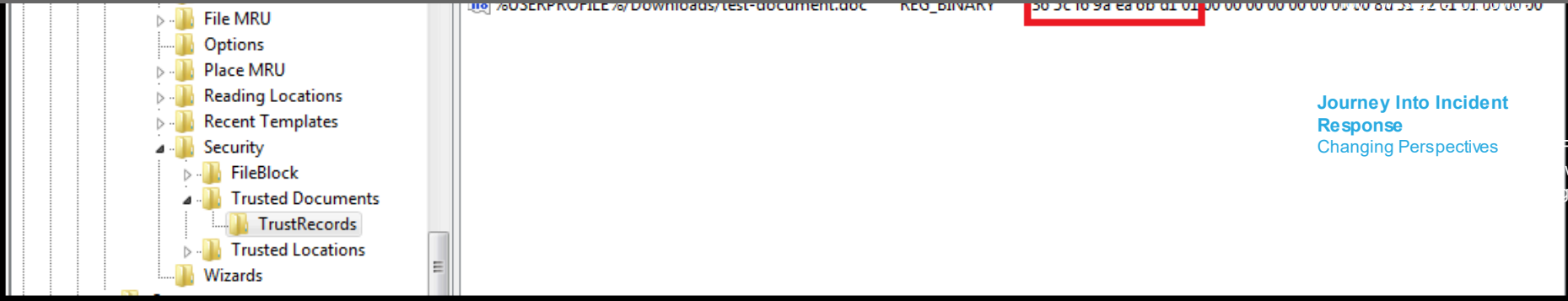


Ce site utilise des cookies provenant de Google pour fournir ses services et analyser le trafic. Votre adresse IP et votre user-agent, ainsi que des statistiques relatives aux performances et à la sécurité, sont transmis à Google afin d'assurer un service de qualité, de générer des statistiques d'utilisation, et de détecter et de résoudre les problèmes d'abus.

EN SAVOIR PLUS OK !



[Journey Into Incident Response](#)
Changing Perspectives

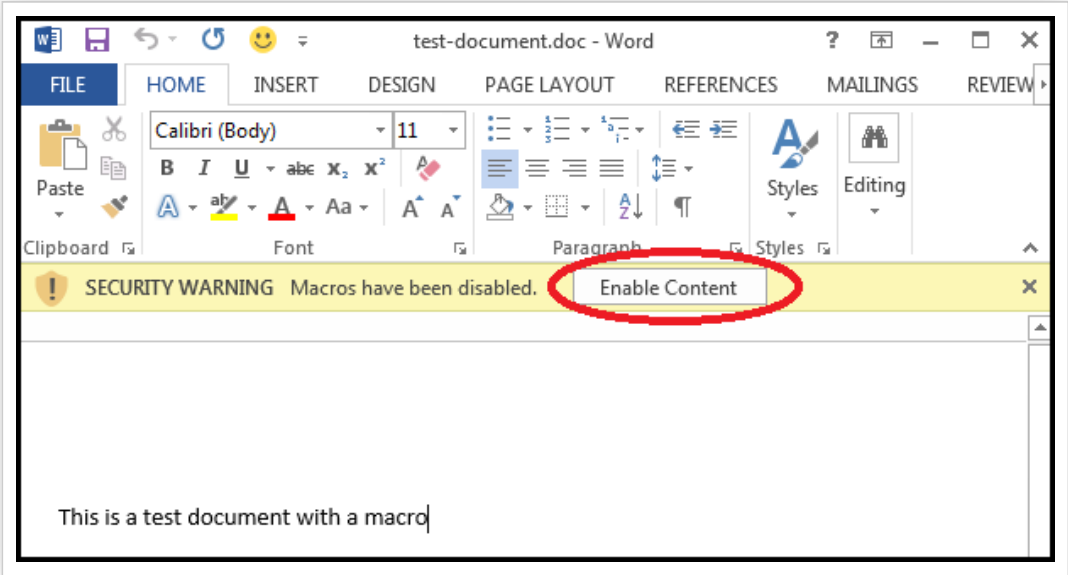
[JustAskWeg](#)
Workarounds to Workarounds (and some hints & reminders) - Every now and then, I get email from readers who have difficulties, and some areas come up more often. I also learn a few things as time goes by, and

The output from the Regripper plugin trustrecords is displayed below:

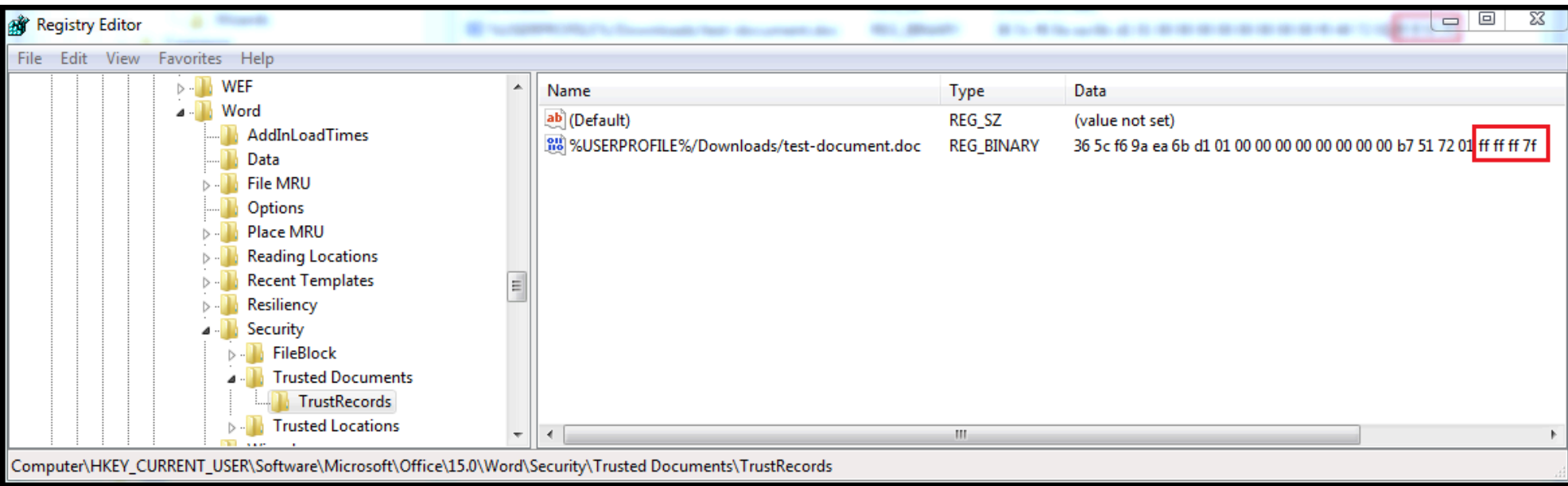
trustrecords v.20120716
Word
LastPurgeTime = Thu Oct 8 20:38:08 1970
Sat Feb 20 14:25:53 2016 -> %USERPROFILE%/Downloads/test-document.doc

At this point in time, I have NOT clicked the second button to enable macros, yet an entry was made under this key.

After I enable editing, a second banner pops up asking me if I would like to "Enable Content", which will enable the macros:



After I clicked this (based on my testing) the last for bytes in the binary data changes to FF FF FF 7F:



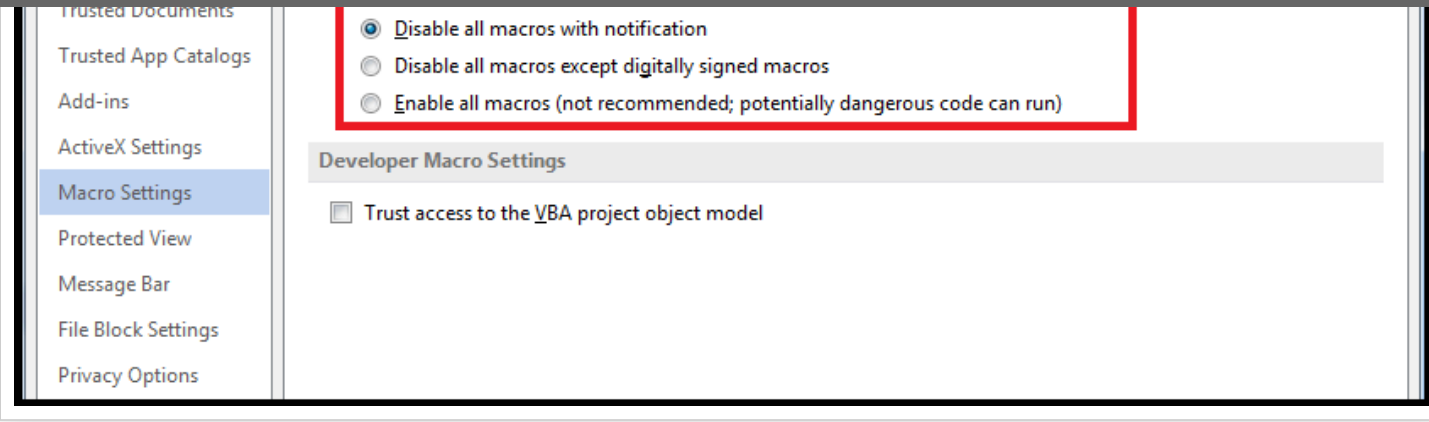
This means in order to determine if the user enable macros, these last four bytes needs to be checked.

Security Registry Key

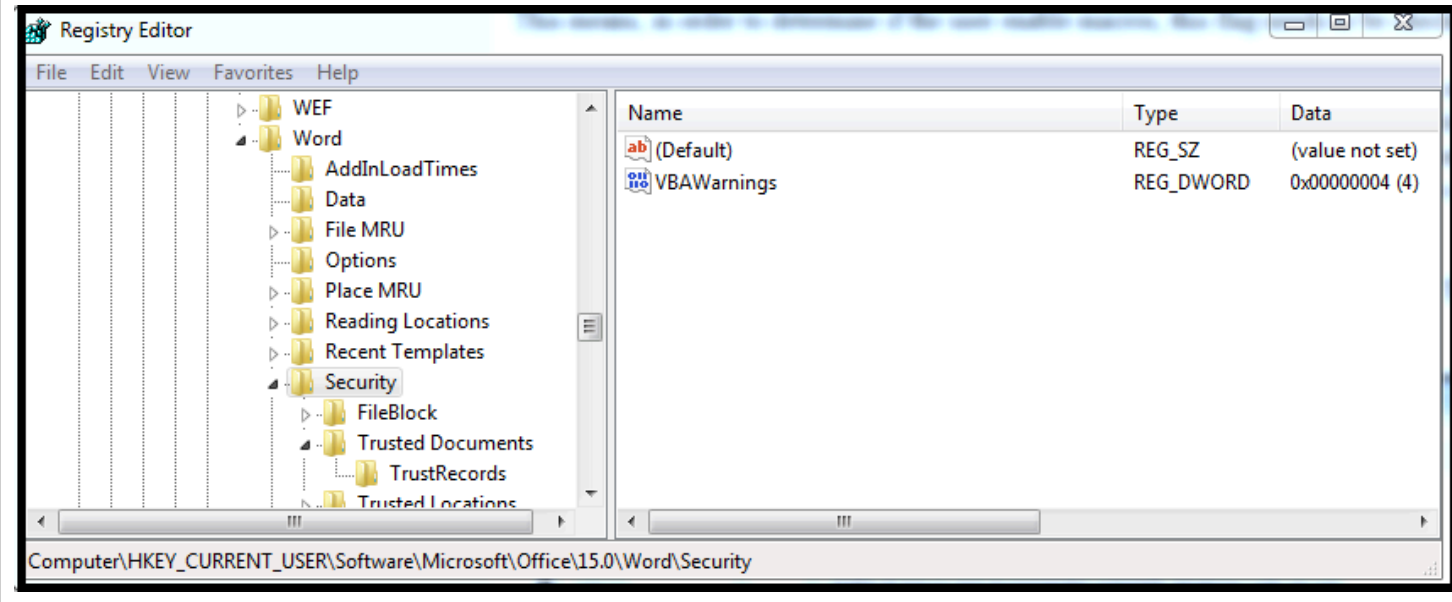
The user can completely bypass this yellow banner by disabling the macro notifications. This means that an entry will not be recorded under the Trusted Document key even though the user ran a malicious document containing macros downloaded from the Internet. These setting are controlled by the Trust Center under Options > Trust Center > Macro Settings. There are four security levels to choose from:

Ce site utilise des cookies provenant de Google pour fournir ses services et analyser le trafic. Votre adresse IP et votre user-agent, ainsi que des statistiques relatives aux performances et à la sécurité, sont transmis à Google afin d'assurer un service de qualité, de générer des statistiques d'utilisation, et de détecter et de résoudre les problèmes d'abus.

EN SAVOIR PLUS OK !



These setting are stored under the registry key HKCU\Software\Microsoft\Office\15.0\Word\Security\ . Based on my testing, if the user has not altered the default settings, this key does not contain the value "VBAWarnings". However, if changes are made to the default settings, an entry for VBAWarnings will appear, and will have a DWORD value:



Based on my testing with Word 2015, these are the Macro Settings and corresponding values for the registry flag:

- Disable all macros without notification : 4
- Disable all macros with notification: 2
- Disable all macros except digitally signed macros: 3
- Enable all macros: 1

I believe these setting are also [affect by a GPO](#), but I have not been able to confirm this yet through testing.

My testing was done using Office 2015 on Windows 7 and Office 2010 on Windows 10. These setting may also apply to Excel, Access and PowerPoint, but I have not tested these.

So, to summarize:

- 1) These artifacts may remain after the malicious document has been removed. They may also be shown in your timeline if you are using a tool like [regtime.exe](#) to add registry keys into your timeline.
- 2) If there is an entry for a document under Trusted Records, this does not necessarily mean that macros were enabled. The flag needs to be checked to make that determination.
- 3) If a document does not appear under this key, this does not mean that the macros were not able to run. They could still have ran if the default setting was altered to enable all macros by default.

Additional Resources:

[NTUSER Trust Records](#)


[Plan and configure Trusted Locations settings for Office 2013](#)

[HowTo: Determine User Access To Files](#)

Posted by [Mari DeGrazia](#) at [6:00 AM](#)



1 comment:

-  **dudyo** March 1, 2018 at 3:59 PM
- Looks like the registry change it the same for v16 as well. Thanks for posting this, it helped me figure out if a user clicked on the document or not.

Ce site utilise des cookies provenant de Google pour fournir ses services et analyser le trafic. Votre adresse IP et votre user-agent, ainsi que des statistiques relatives aux performances et à la sécurité, sont transmis à Google afin d'assurer un service de qualité, de générer des statistiques d'utilisation, et de détecter et de résoudre les problèmes d'abus.

EN SAVOIR PLUS

OK !

Newer Post

Home

Older Post

Subscribe to: [Post Comments \(Atom\)](#)

Awesome Inc. theme. Powered by [Blogger](#).