Monday, February 22, 2016

More on Trust Records, Macros and Security, Oh My!

There is a registry key that keeps track of which documents a user has enabled editing and macros for from untrusted locations. This happens when the user clicks the "Enable Editing" button on the Microsoft Office Protect View warning:

These can include documents that are downloaded from the Internet, or sent via email. This registry key is affectionately known as "Trust Records". When a user clicks this warning, an entry is made under HKCU\Software\Microsoft\Office\15\Word\Security\Trusted Documents\TrustRecords that contains the file path to the document (the version number may vary - I've tested 14 and 15).

This is by no means a new artifact. There are several blog posts that discuss this artifact, including one by Andrew Case and Harlan Carvey - however, I believe I may have some new light to shed on this artifact. Well, I couldn't find the information by using Google, so it's new to me.

What I found was that an entry can exist under this key, ***but that does not necessarily mean that macros were enabled.*** In order to determine if macros were enabled, a flag/value needs to be checked in the binary data. Additionally, the Trust Center macro settings may need to be checked as well. The user can turn off this security prompt in the Trust Center and trust **all documents** by default. If this happens, no entry will be made under the Trust Records because all documents are trusted.

Why all the fuss over macros? Who uses them anyways??? Take for example the latest ransomware variant, Locky. Locky utilizes macros in a Word document to pull down it's payload. After a company get hits with something like this, they may want to know "How did this happen?" and "How can we prevent it in the future?".

The Trusted Records registry key can help answer these questions. Did the user take affirmative steps by enabling editing in the document? Did they take another step and enable the macros? If so, the company may need to spend more time training employees on better security practices. Was the system setup to trust all documents by default? If so, they may need to reconfigure their GPO.

The Trusted Records key can also contain references to artifacts that may no longer exist on the system, add context to your timeline, and demonstrates that a user explicitly interacted with the file.

Trusted Records Registry Key

In Word 2010 (v.14) and 2013 (v.15) there are actually two yellow banners presented to the user when macros are in a Word document. The first asks the user to "Enable Editing":

After this button is clicked, an entry is created in the registry with the document name, path and time stamp. According to some testing that Harlan did (and the testing I did confirmed this as well), the time stamp is the create date of the document, NOT the time the user enabled editing:

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
```

Search This Blog

Search

Blog Archive

- ► 2020 (1)
- ► 2019 (1)
- ► 2018 (3)
- ► 2017 (3)
- ▼ 2016 (8)
  - ► October (1)
  - ► September (2)
  - ► July (2)
  - ► June (1)
  - ► May (1)
  - ▼ February (1)
    - More on Trust Records, Macros and Security, Oh My!
- ► 2015 (5)
- ► 2014 (4)
- ► 2013 (6)
- ► 2012 (7)

About Me

Mari DeGrazia

I am a Cyber Security professional specializing in Digital Forensics and Incident Response. I also enjoy Raspberry Pi projects and playing poker. Follow me on twitter @maridegrazia. Opinions are my own and not the views of my employer.

View my complete profile

Subscribe To

Posts

Comments

My Blog List

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:

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 VBAWarrnings 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:

'X-Ways Forensics' Video Clips
Video 69 - Understanding and Using the Data Interpreter in X-Ways Forensics - Video 69 hopes to help new users, or new practitioners to the field, with understanding HOW the Data Interpreter of X-Ways Forensics actually does "inte...

Cheeky4n6Monkey - Learning About Digital Forensics
MonkeyAttempts To Digest Some Google Takeout (DetectedActivitys) - *Careful What You Eat, Monkey!* One of Monkey's co-workers (*Troy*) was able to provide investigators with a location of interest by looking at the dev...

Journey Into Incident Response
Changing Perspectives - In the Fall I was staring out my back window seeing my yard covered in orange leaves. This sight is one I see each year and I have always viewed as my year...

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

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)