CERT/CC Blog

Vulnerability Insights

Who Needs to Exploit Vulnerabilities When You Have Macros?

POSTED ON JUNE 8, 2016 BY WILL DORMANN [/AUTHOR/WILL-DORMANN] IN BEST PRACTICES [HTTPS://INSIGHTS.SEI.CMU.EDU/CERT/BEST-PRACTICES/]

Recently, there has been a resurgence of malware that is spread via Microsoft Word macro capabilities [http://motherboard.vice.com/read/the-90s-hacking-trick-making-a-comeback-macros-malware]. In 1999, CERT actually published an advisory about the Melissa virus [https://www.cert.org/historical/advisories/CA-1999-04.cfm?], which leveraged macros to spread. We even published an FAQ about the Melissa virus [http://www.cert.org/historical/tech_tips/Melissa_FAQ.cfm] that suggests to disable macros in Microsoft Office products.

Why is everything old new again? Reliability of the exploit is one reason, but the user interface of Microsoft Office is also to blame.

Exploiting Vulnerabilities

Attackers like to target weaknesses in the design of an application whenever possible. Using implementation bugs, such as ones that can be found through fuzzing, can be viable for an attacker. Successful and reliable exploitation can rely on a number of variables, such as

- What OS is the target running?
- What version of the vulnerable software is being used?
- Is Microsoft EMET being used?

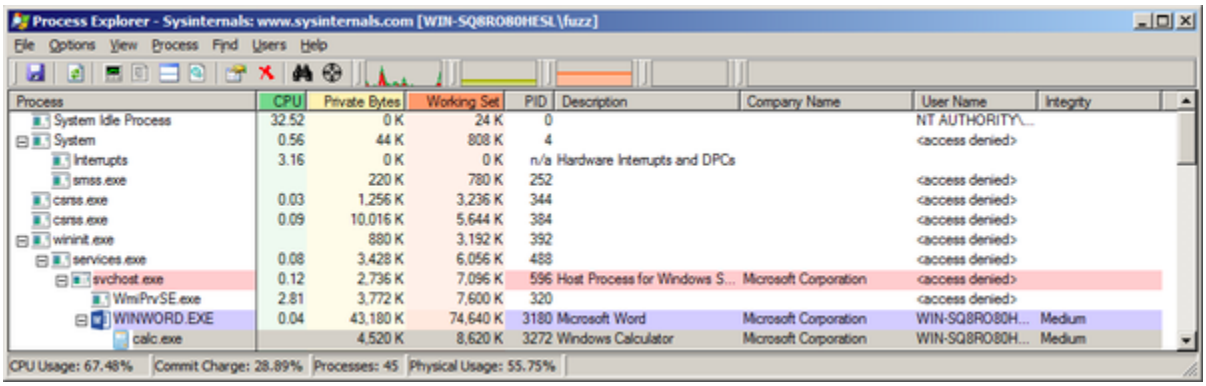
In some cases, an exploit for a vulnerability may only work on very specific targets. Attackers look for the widest range of compatibility for their exploits.

Exploiting Design Weaknesses

Design weaknesses are a much more valuable target for an attacker, as opposed to an implementation flaw that relies on memory corruption, for example. The benefit of such weaknesses is that they can work universally. For example, consider the Microsoft Windows design flaw that caused Windows to automatically execute code that is specified in shortcut files [http://www.kb.cert.org/vuls/id/940193]. This weakness was used by the Stuxnet [https://en.wikipedia.org/wiki/Stuxnet] worm.

Microsoft Office Macros

Malicious Microsoft Office documents that leverage macros are exploiting capabilities that are provided by Microsoft Office by design. Microsoft Office macros can help automate repetitive tasks, but in the end they are equivalent to running native code. As a proof of concept, I made a simple Word document that launches calc.exe by way of a one-line VBScript macro. The screenshot below is from Office 2013 running on Windows 7.



[https://insights.sei.cmu.edu/cert/2016/06/08/word2013_calc_macro.png]

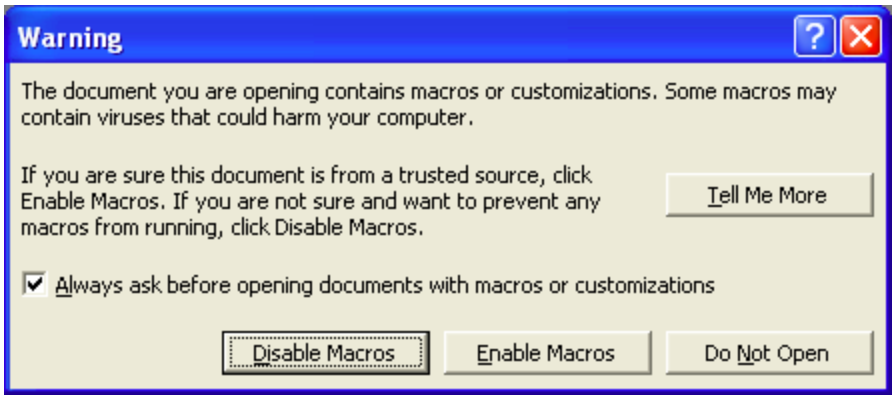
Word does give me a warning about the document having a macro, but how well does the program convey the potential dangers of enabling the macro?

A Trip Down Memory Lane

Microsoft Office has provided some level of warning to the user, and has required some steps to enable macros before they are executed. However, both of these aspects of enabling macros have changed over the versions of Office.

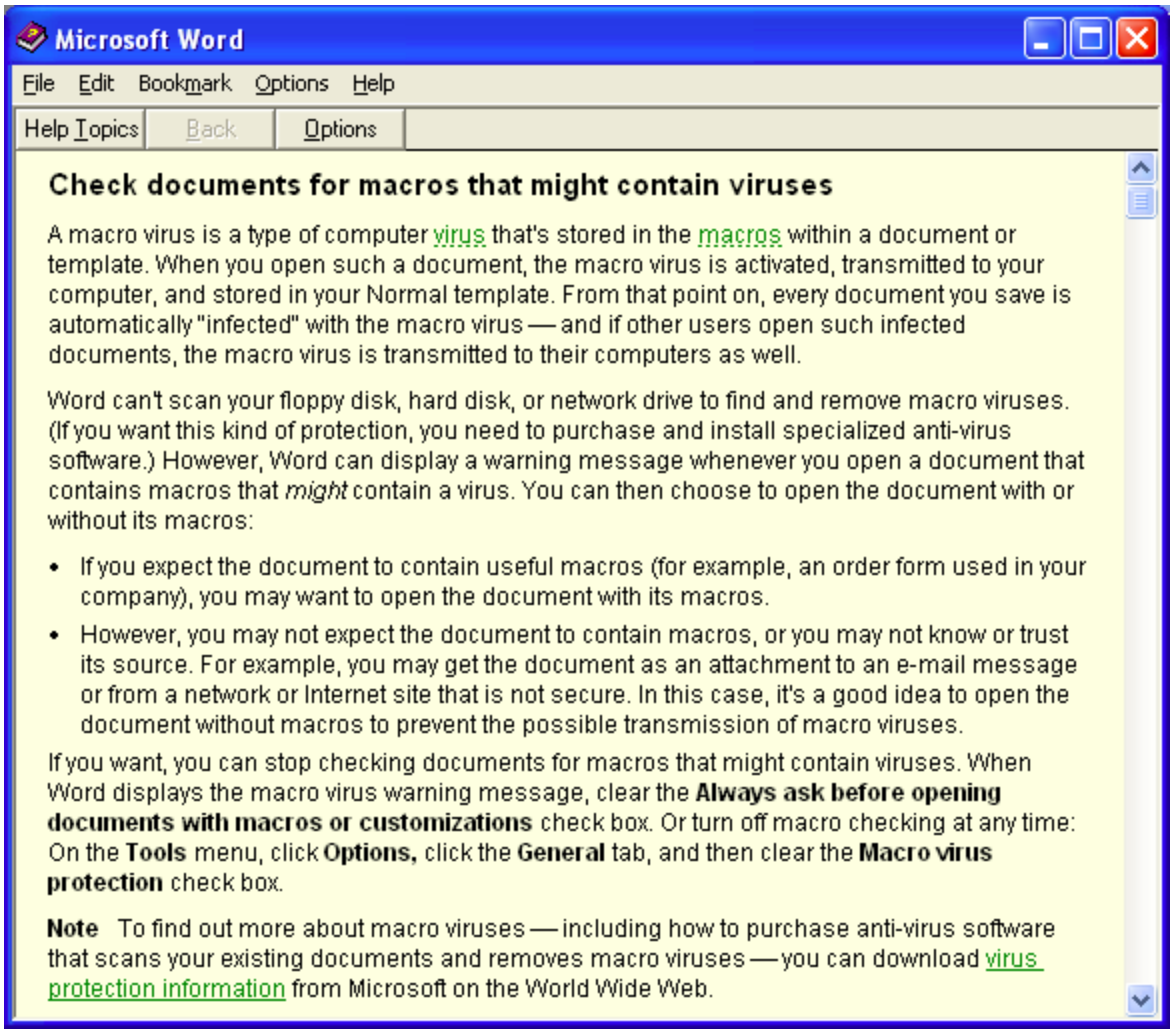
Office 97

Microsoft Office 97 was pretty clear that enabling macros can harm your computer:



The options to proceed include

- **Disable Macros** - Open the document, but with macros disabled
- **Enable Macros** - Open the document with macros enabled
- **Do Not Open** - Do not open the document
- **Tell Me More** - Give the user details about the risks of opening a document with macros:

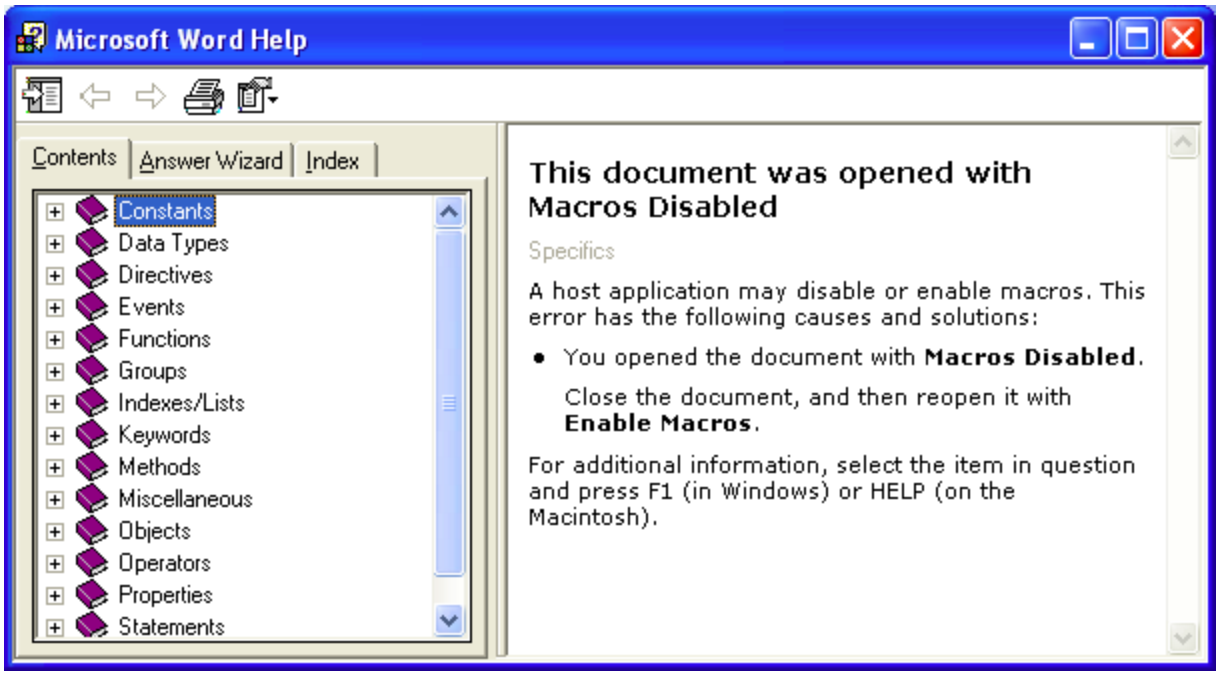


Even with these warnings, the Melissa macro virus still spread in 1999 [https://www.cert.org/historical/advisories/CA-1999-04.cfm].

Office 2000

Starting with Office 2000, the dialog was a little less informative. However, the possible actions to take are safer for the user:

- **OK** - Open the document, but with macros disabled
- **Help** - Give the user details about the risks of opening a document with macros:



Office XP

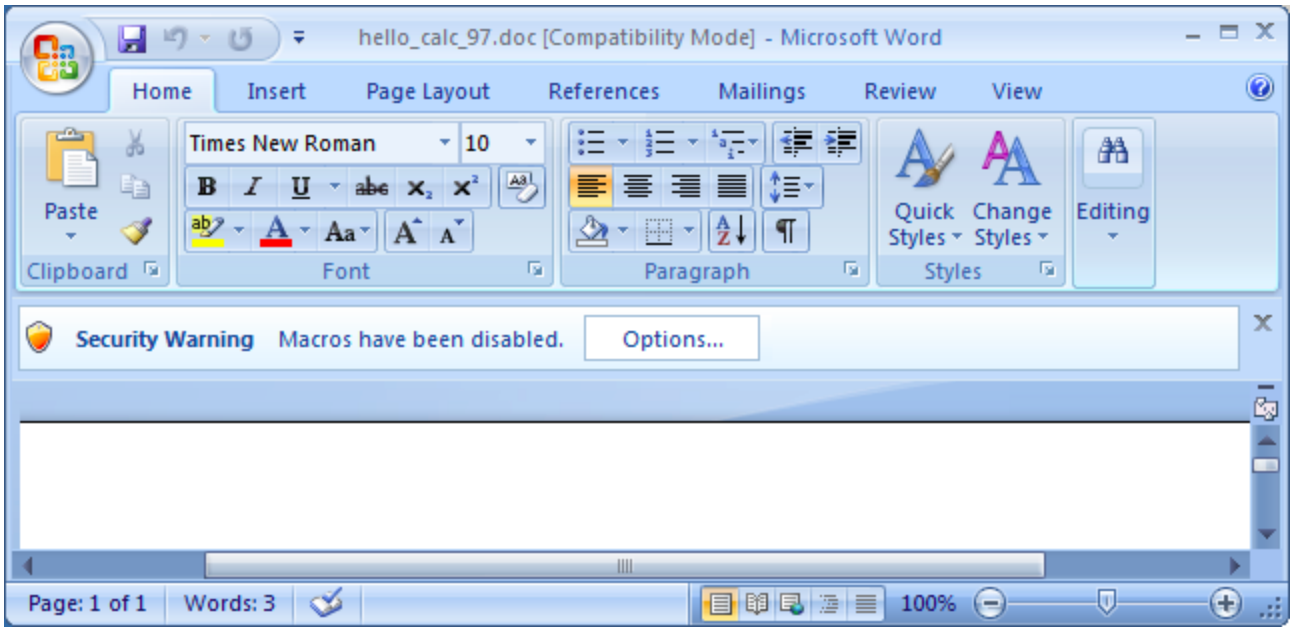
Office XP has similar dialogs, functionality, and help as Office 2000.

Office 2003

Office XP has similar dialogs, functionality, and help as Office 2000 and Office XP.

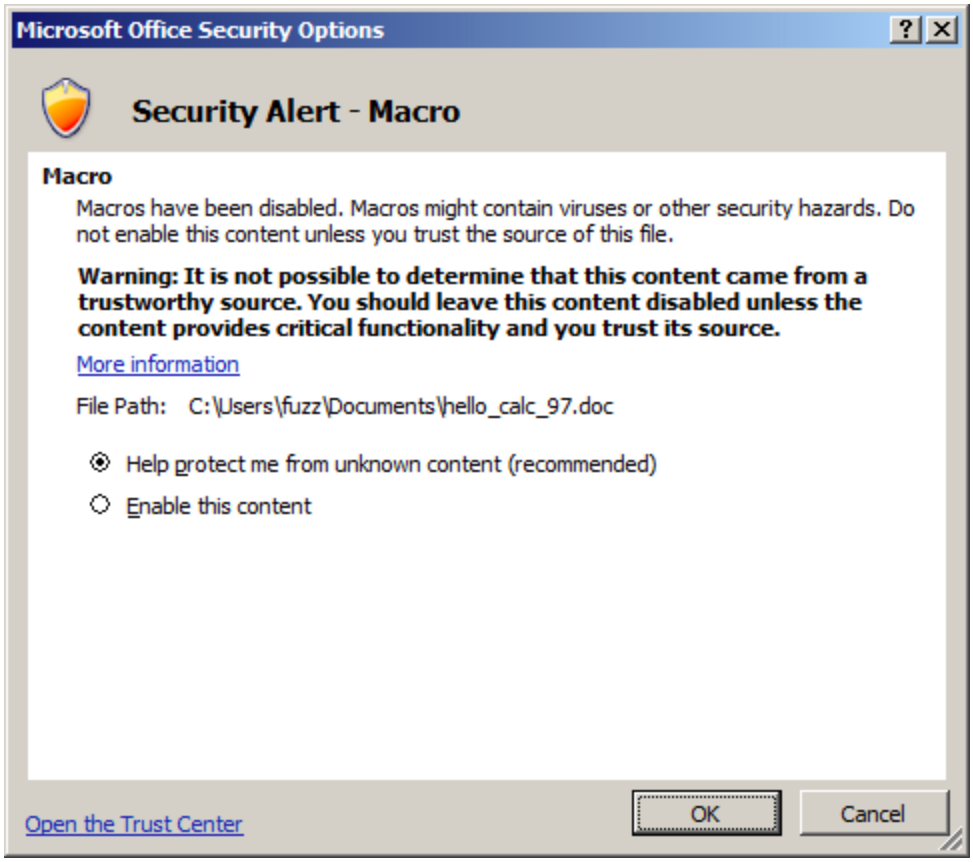
Office 2007

Office 2007 appears to be the first version of Office where the traditional dialogs have been abandoned. Presumably this was done to avoid the "dialog fatigue [https://blogs.msdn.microsoft.com/oldnewthing/20060526-03/?p=31063]" problem that could lead users to give in and make a poor decision.



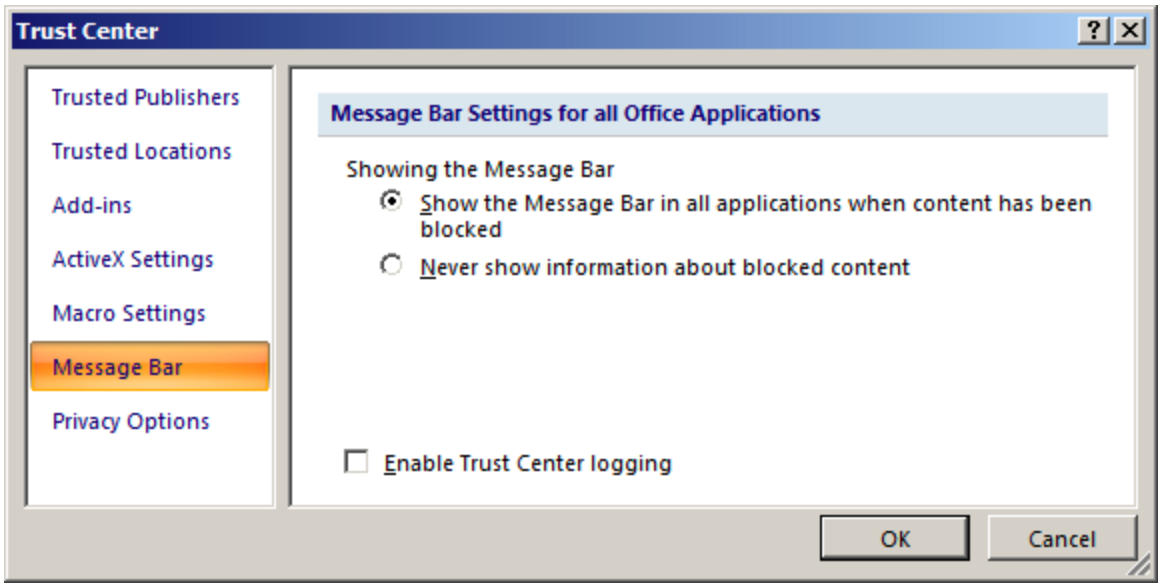
Here, the warning bar isn't very clear about the potential consequences of macros. But there is only one option to proceed:

- **Options** - Display additional information and options at the same time:



From this dialog, there are several options:

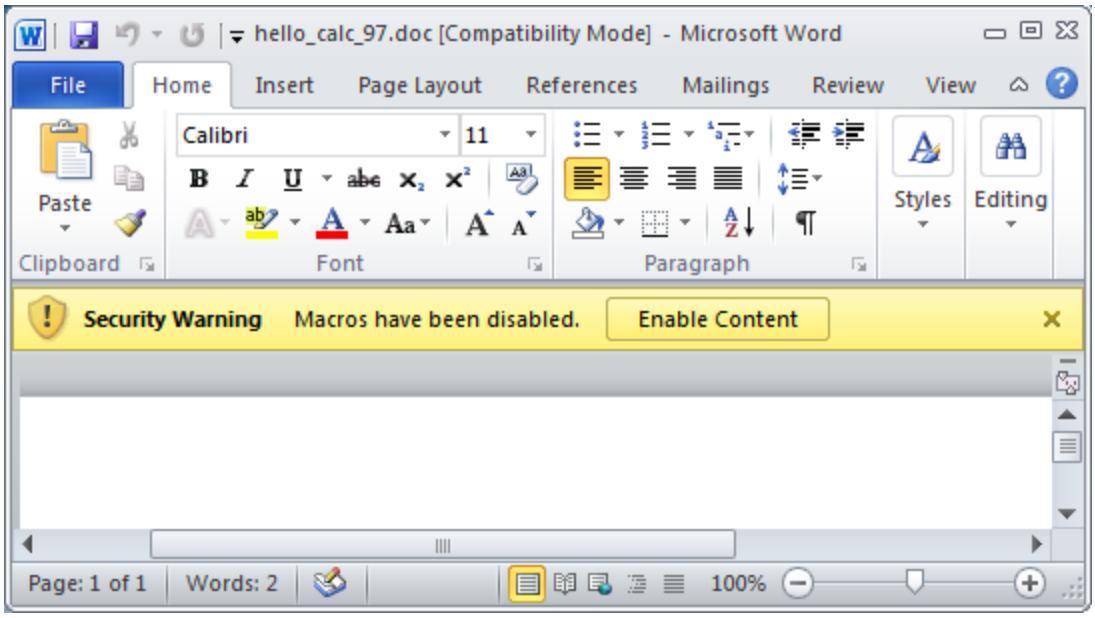
- **OK** - Open the document, but with macros disabled
- **Cancel** - Close dialog, but leave warning bar at the top
- **Enable this content** - Open the document with macros enabled once OK is clicked.
- **Open the Trust Center** - Open a dialog that allows macros to be disabled without prompting the user:



The Office 2007 options seem reasonable. The default is to block macros, but the user is given the option of enabling them on the same screen that clearly indicates the risk.

Office 2010

Presumably with the goal of simplifying the options presented to the user, Office 2010 changed the Message Bar functionality:



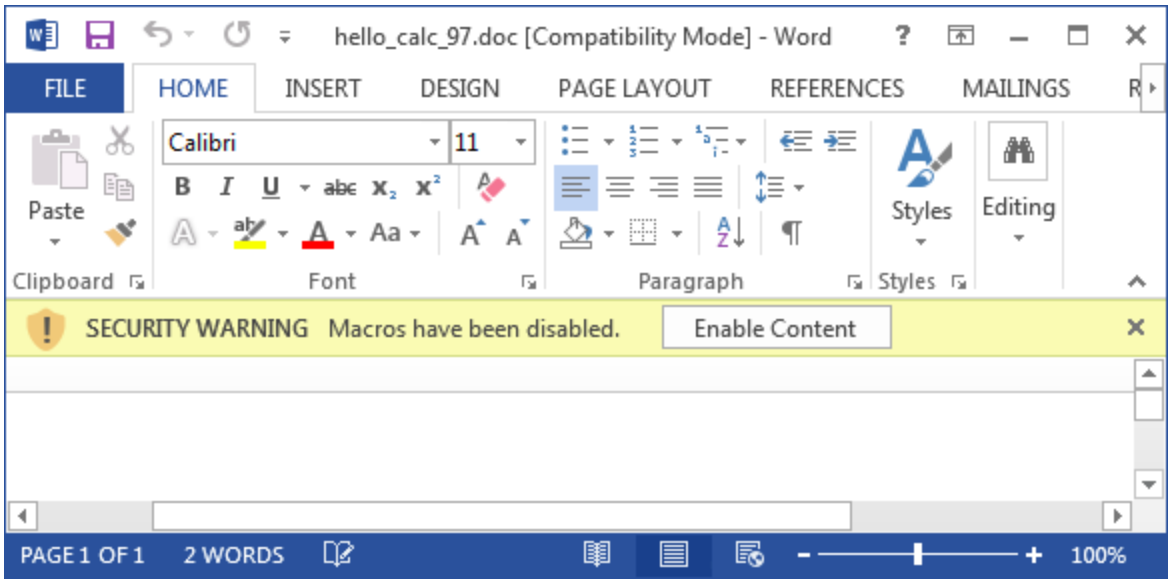
Here the user seems to be given one option:

- **Enable Content** - Run the macros present in the document

From a security perspective, this approach is a step backwards. The user is not given any information about the consequences of enabling macros, and the user is given only one obvious option: enable macros. This is dangerous. Attackers are using several social engineering techniques to convince users to click the "Enable Content" button as well.

Office 2013

The Office 2013 experience appears identical to that of Office 2010:



Macro Protections

Unfortunately, the default Microsoft Office settings for macros are not secure. Users of newer versions of Office (2010 or 2013) are even more likely to enable macros without understanding the consequences of doing so. Luckily, Microsoft has provided guidance for how to restrict macro functionality [https://blogs.technet.microsoft.com/diana_tudor/2014/12/02/microsoft-project-how-to-control-macro-settings-using-registry-keys/]. These changes can be rolled out via Group Policy, which should aid in enterprises being able to configure Office in a secure manner.

The options are

1. **Enable all macros**
2. **Disable all macros with notification**
3. **Disable all macros except those digitally signed**
4. **Disable all macros without notification**

Option 2 above is the less-secure default option for Microsoft Office. Option 4 above is the most secure, as it will eliminate the chance of a user inadvertently executing a malicious macro.

Some enterprises may have legitimate uses for Office macros, however. In such situations, questions that must be answered include

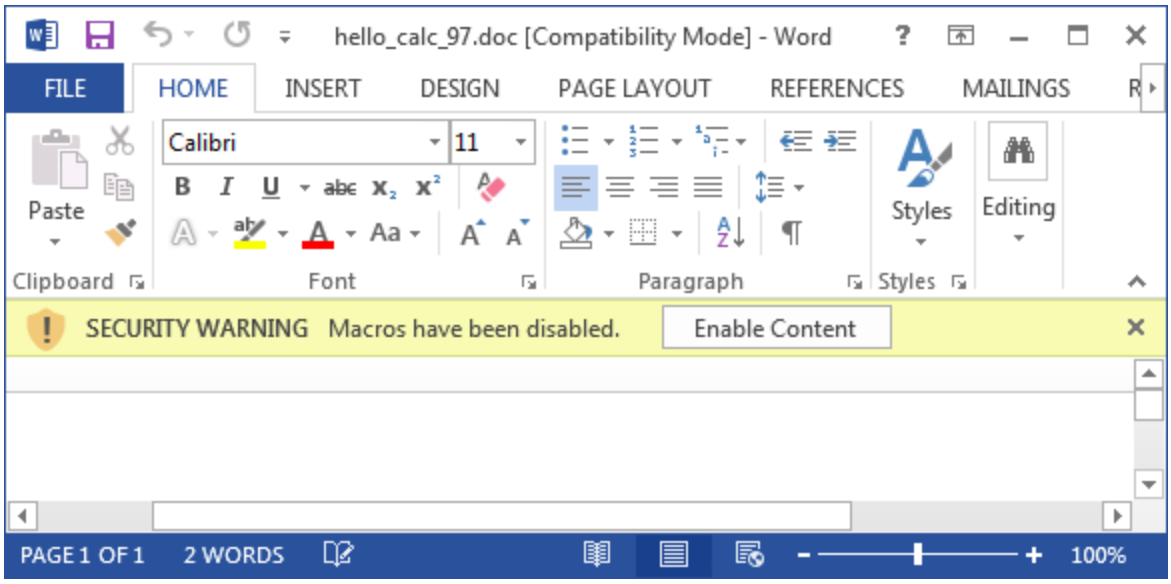
1. Who in my enterprise has a business need for macros?
2. Of those officially sanctioned uses for macros, what Microsoft Office applications need the macro capability?

The first question is important from an attack surface perspective. For example, let's say that my 10,000-person organization has 10 people in finance that need macro capabilities, but the other 9,990 people do not. It makes no sense to give everybody the ability to execute macros.

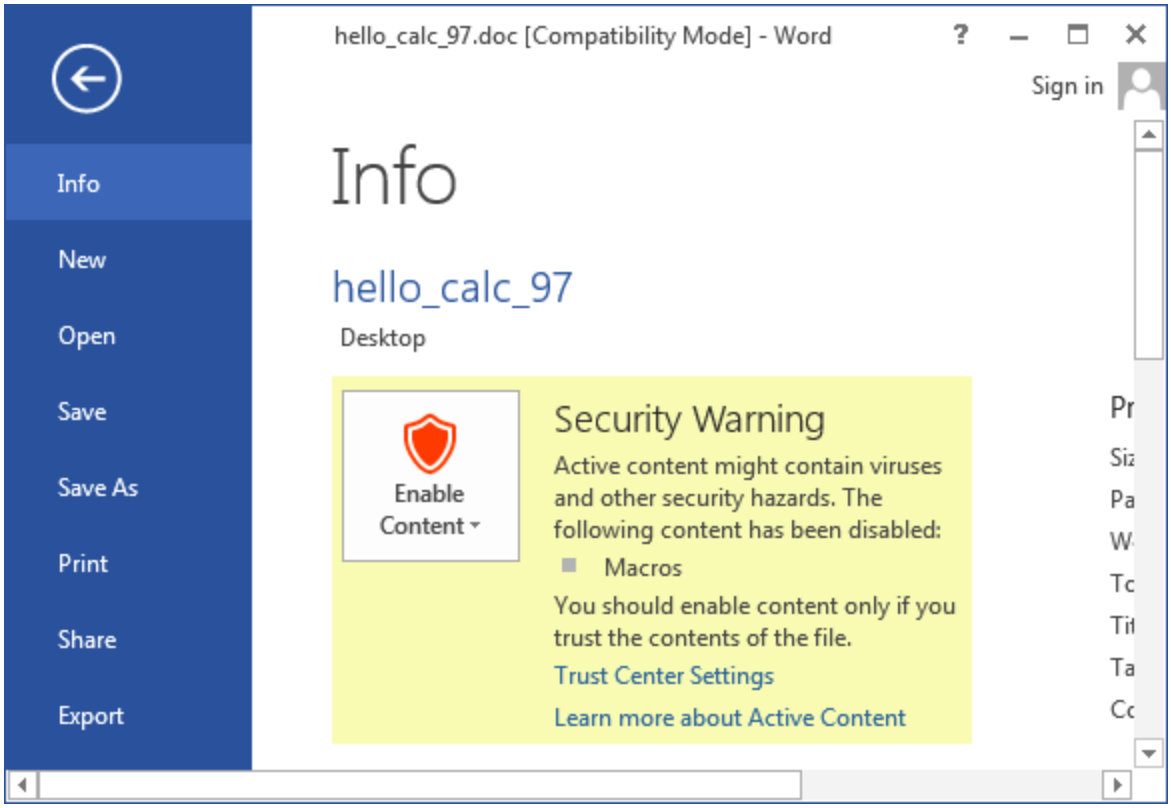
The second question also helps protect the systems that need some sort of Office macro capabilities. In the example above, let's say that the 10 people in finance only use macros in an Excel spreadsheet that they use. In this case, macros should be disabled without notification for all Microsoft Office components except Excel (e.g., Word, PowerPoint, Project). And for Excel itself, the more-secure setting would be "Disable all macros except those digitally signed." This way, the organization can sign the approved macros. When Excel opens a malicious file with an unsigned macro, the macros will be silently blocked.

Office 2010 and 2013 Revisited

As it turns out, both Office 2010 and Office 2013 can show the user details about what enabling macros can do. In the following example



the phrase "Macros have been disabled" is actually clickable. This doesn't seem obvious to me, and I suspect other users may not realize it as well. Only in the late stages of preparing this blog entry did I realize that "Macros have been disabled" is clickable. If the user does click on that phrase, a dialog is presented that explains the risks of enabling macros:



This information is hidden far enough away from the "Enable Content" button that I suspect not many people would even see it.

Conclusions

Macro viruses are back. See

- Keep Calm and (Don't) Enable Macros: A New Threat Actor Targets UAE Dissidents
- Macro Malware Strides in New Direction, Uses Forms to Store its Code
- PowerSniff Malware Used in Macro-based Attacks
- LinkedIn information used to spread banking malware in the Netherlands
- Microsoft Office Macro Security

The default behavior of Microsoft Office has usually allowed for inadvertent execution of malicious macros, but recent versions of Microsoft Office make it much easier for the user to make the wrong decision.

If you wish to protect your systems, restrict access to macros. Regardless of the level of information provided to an end-user, don't always rely on that user to make the right choice.

Solutions

Disable Microsoft Office macros
[https://blogs.technet.microsoft.com/diana_tudor/2014/12/02/microsoft-project-how-to-control-macro-settings-using-registry-keys/]
for as much of your organization as is practical. In particular, disable macros without notification for all Microsoft Office applications by default for all systems. For systems that do need macro capabilities:

- Only enable macros for certain users or groups.
- For those users or groups that need macro functionality, only enable macros for applications that need them. For example, if you have a business need for Excel macros, only allow macros in Microsoft Excel, and be sure that they are disabled for the other Office applications.
- Only allowing signed macros can reduce the fraction of attacks that could be successful. However, be aware that attackers may be able to obtain trusted signing keys for macros.
- As a last resort, consider using the Trusted Locations feature of the Microsoft Office Trust Center. When a document is loaded from a Trusted Location that is configured, macros will be enabled regardless of the macro settings specified in the Trust Center. Also note that Protected View is also disabled in the Trusted Location. While documents in a Trusted Location bypass a number of protections that Office provides, limiting macro-enabled documents to this location can greatly reduce the attack surface of your Microsoft Office deployment.

< Previous Article

About the Author

Will Dormann

Contact Will Dormann [https://www.sei.cmu.edu/contact.cfm]
Visit the SEI Digital Library for other publications by Will [https://resources.sei.cmu.edu/library/author.cfm?authorID=2547]
View other blog posts by Will Dormann [/author/will-dormann]