

Beyond good ol' Run key, Part 62

Published: 2017-04-19 · Archived: 2026-04-05 18:20:25 UTC

Update

This is not an RCE. If it was, I would not publish it on this blog 😊

Turns out “Simpsons already did it” and as pointed out by [@arekfurt](#) a *normal* template-based persistence is already implemented in [EmpireProject](#) and is based on [awesome work](#) of [@enigma0x3](#). Interestingly, enabling macros is not needed to deliver the same functionality (as explained below).

Dropping any macro sheet inside the XLSTART folder and opening it from there will not show the macro warning 😊

Old Post

Every once in a while we come across weird things that we not only discover accidentally, but are finding hard to understand. Today I was playing around with Word Macros and to my surprise I was able to accidentally run one, while my Macro Options were set to *Disable all macros with notification*.

Macro Settings

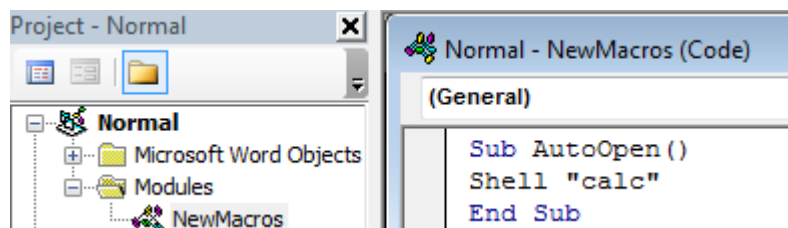
- Disable all macros without notification
- Disable all macros with notification
- Disable all macros except digitally signed macros
- Enable all macros (not recommended; potentially dangerous code can run)

Intrigued, I quickly realized that

instead of adding it to a test word document, I accidentally added it to the *normal* template file.

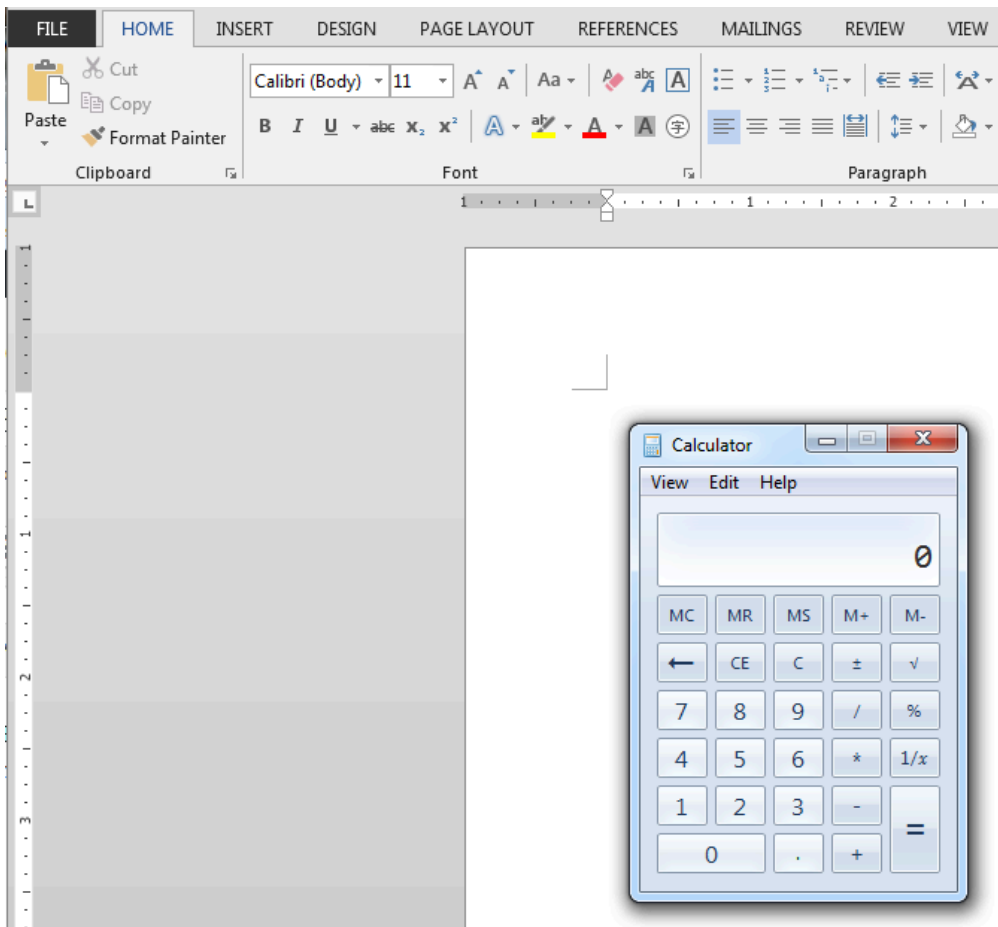
Could it be... ?

I rushed to add the *AutoOpen* macro to the *normal* template that will launch the Calculator anytime the template is used:



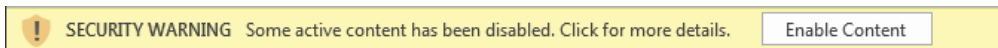
Now I only needed to open some word

document...



How nice!

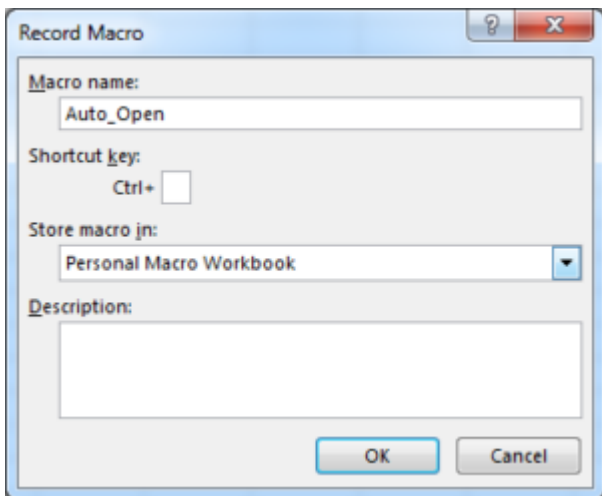
Interestingly, the Security Warning appears ONLY after I visit options while the document is open.



Swap calculator with anything else, and a new stealth persistence mechanism is born...

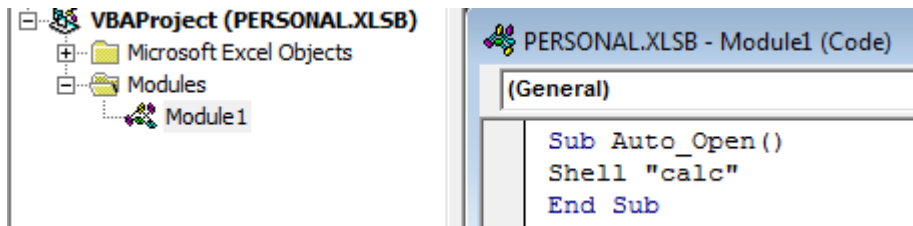
Now, what about Excel?

Excel doesn't have the *Normal* template equivalent by default, but you can add one. To do so, you just need to record any macro named *Auto_Open* and store it inside a personal template (by choosing 'Store macro in *Personal Macro Workbook*')



(alternatively, you can create a personal template directly on the system by placing a prepared XLSB file in a following location: `c:\Users\<USER>\AppData\Roaming\Microsoft\Excel\XLSTART\PERSONAL.XLSB`)

Then switch to the macro editor, and write the code as below:



This will ensure the Calculator will be executed anytime someone opens Excel, even if the macros are *cough*
cough disabled...

Source: <http://www.hexacorn.com/blog/2017/04/19/beyond-good-ol-run-key-part-62/>