Maintaining Access with Normal.dotm

Published: 2014-01-23 · Archived: 2026-04-06 15:33:49 UTC

I was playing around in Word yesterday and thought of a neat idea. To start off, what I am about to show you will blow away any user set macros in Normal.dotm. That being said, this is kind of cool.

Let me start with all of the code. Everything you need to setup and execute this attack can be found here:

https://github.com/enigma0x3/WordPersistence

You will need to host Invoke-Shellcode, the malicious Normal.dotm and persist.ps1 for this to execute correctly

**It is also important to note that you MUST create the malicious Normal.dotm by opening a new word document, creating a new macro, pasting in the code and then saving it as Normal.dotm. Once created, you can then host it.

The way this works is like so: You craft an excel document and send it off to the target. They open said document and it executes a payload. While you are sitting there with your meterpreter session, it does the following:

1. It changes the macro security settings in Word/Excel

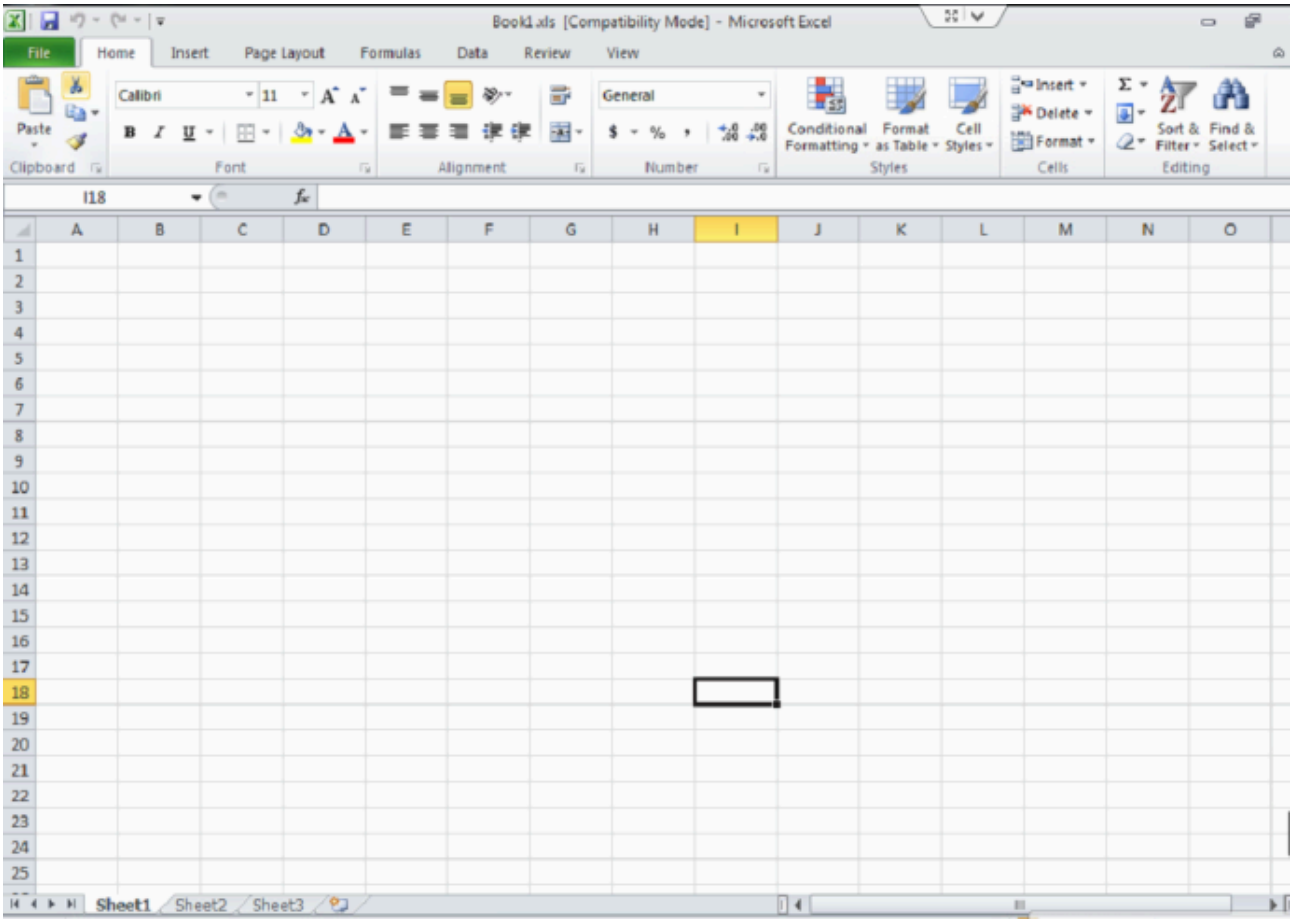
2. It creates a registry key that executes the hosted persistence script on startup

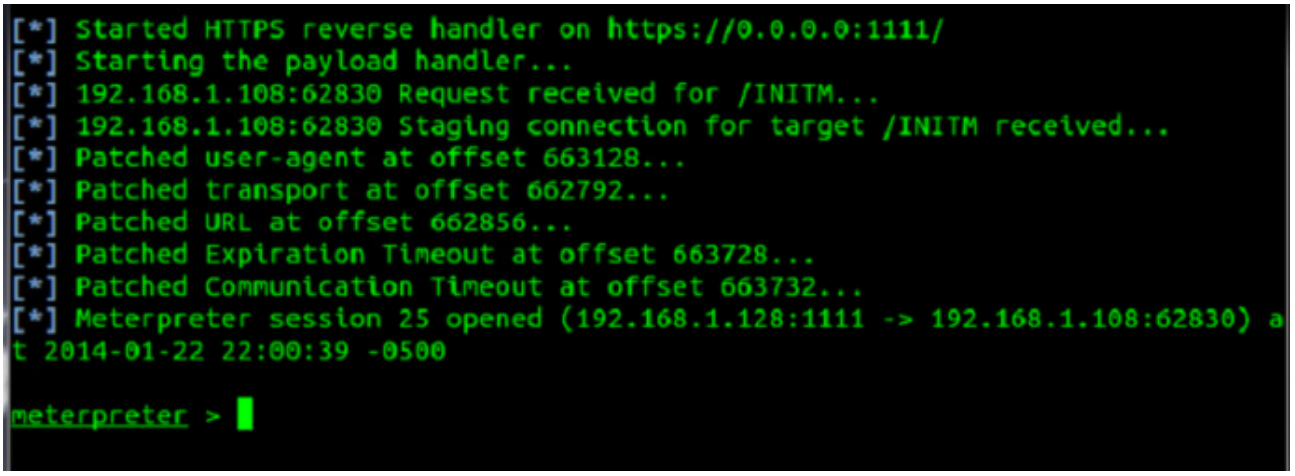
3. It drops a malicious Normal.dotm in C:\Users\{username}\AppData\Roaming\Microsoft\Templates

If you don’t know, Normal.dotm is the base template for all Word documents. If a macro sits in it, it executes EVERY SINGLE TIME Word is opened. Now, let me show you!

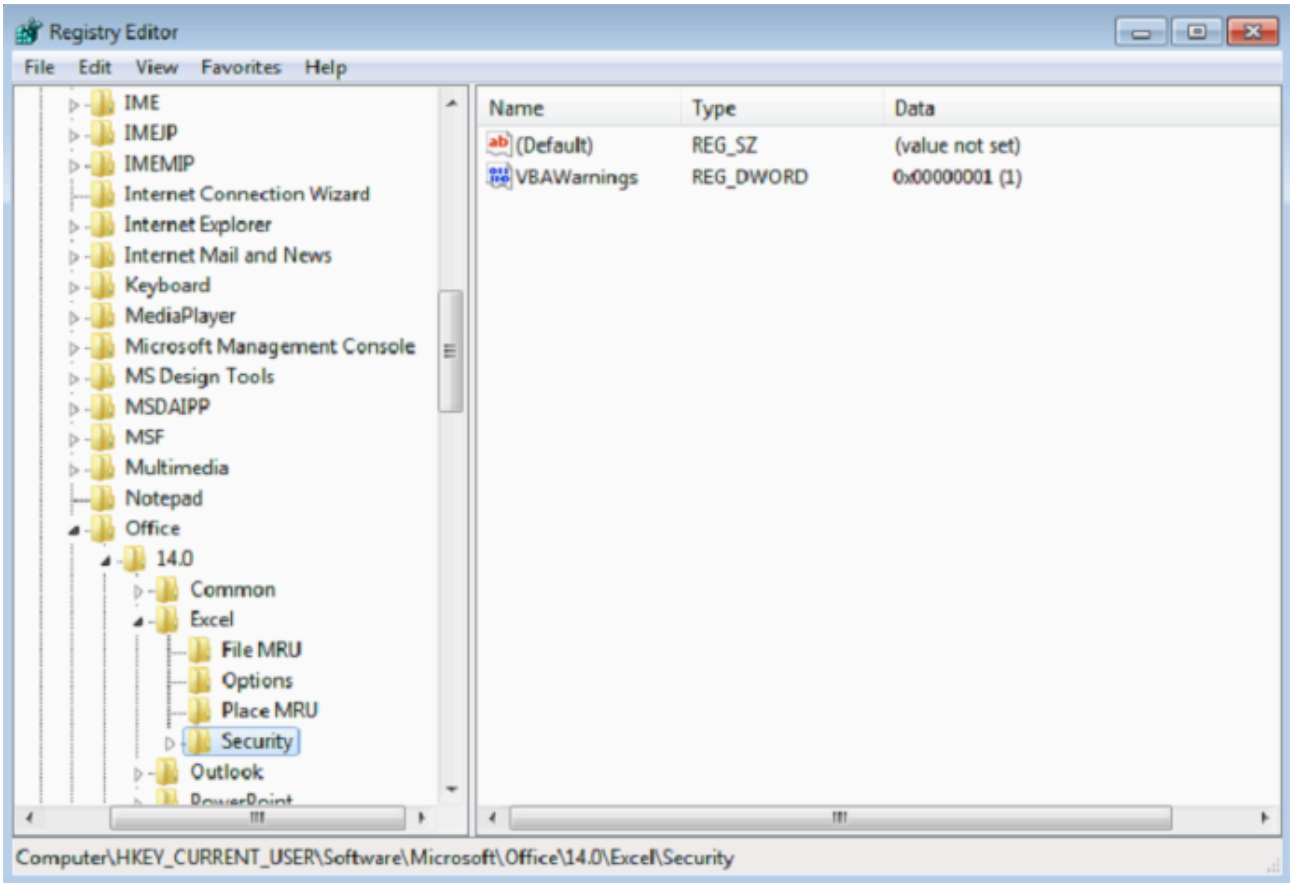
To start off, create your macro with the code on Github and send it. Once opened, here is what happens:

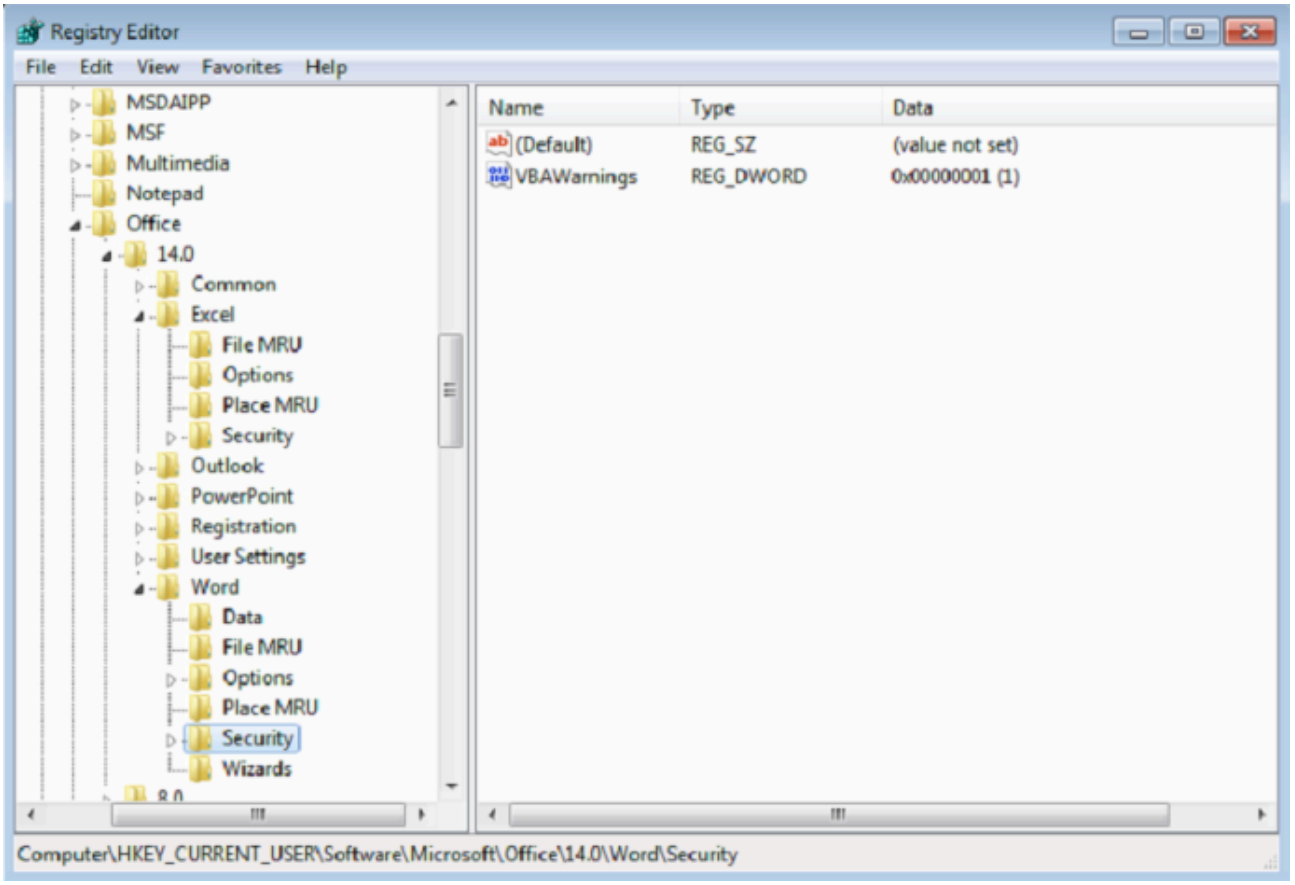
1. You get your shell



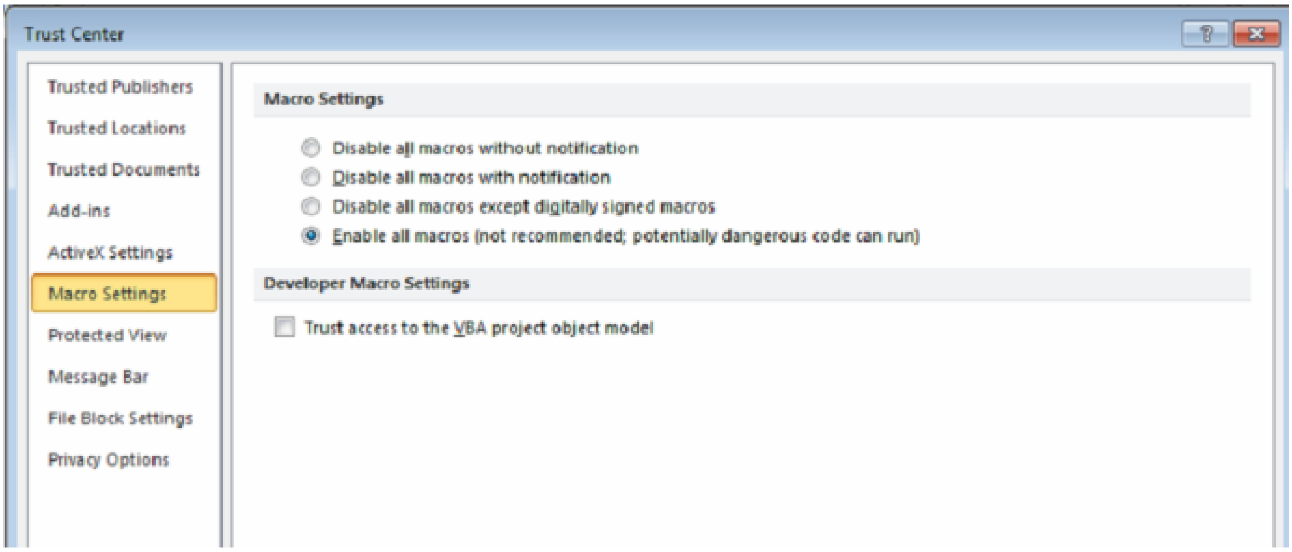


2. It then disables the macro security settings so the malicious Normal.dotm macro can execute on startup (and also changes the Excel settings just because)

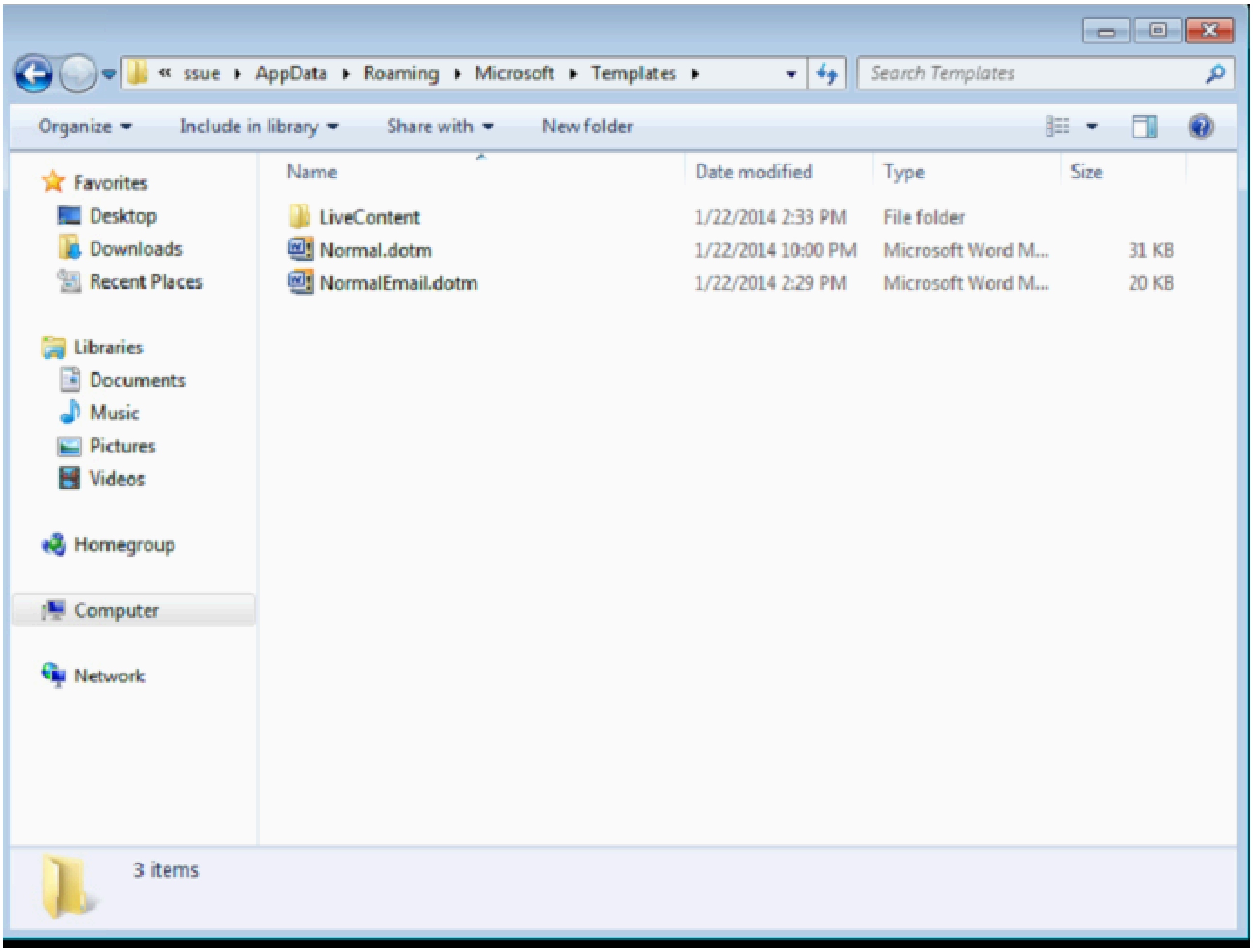

Registry Editor
File Edit View Favorites Help
IME
IMEJP
IMEMIP
Internet Connection Wizard
Internet Explorer
Internet Mail and News
Keyboard
MediaPlayer
Microsoft Management Console
MS Design Tools
MSDAIPP
MSF
Multimedia
Notepad
Office
14.0
Common
Excel
File MRU
Options
Place MRU
Security
Outlook
Name
Type
Data
(Default)
REG_SZ
(value not set)
VBAWarnings
REG_DWORD
0x00000001 (1)
Computer\HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Security


Registry Editor
File Edit View Favorites Help
MSDAIPP
MSF
Multimedia
Notepad
Office
14.0
Common
Excel
File MRU
Options
Place MRU
Security
Outlook
PowerPoint
Registration
User Settings
Word
Data
File MRU
Options
Place MRU
Security
Wizards
Name
Type
Data
(Default)
REG_SZ
(value not set)
VBAWarnings
REG_DWORD
0x00000001 (1)
Computer\HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Security

——————————————————————-AND BAM
———————————————————————————-



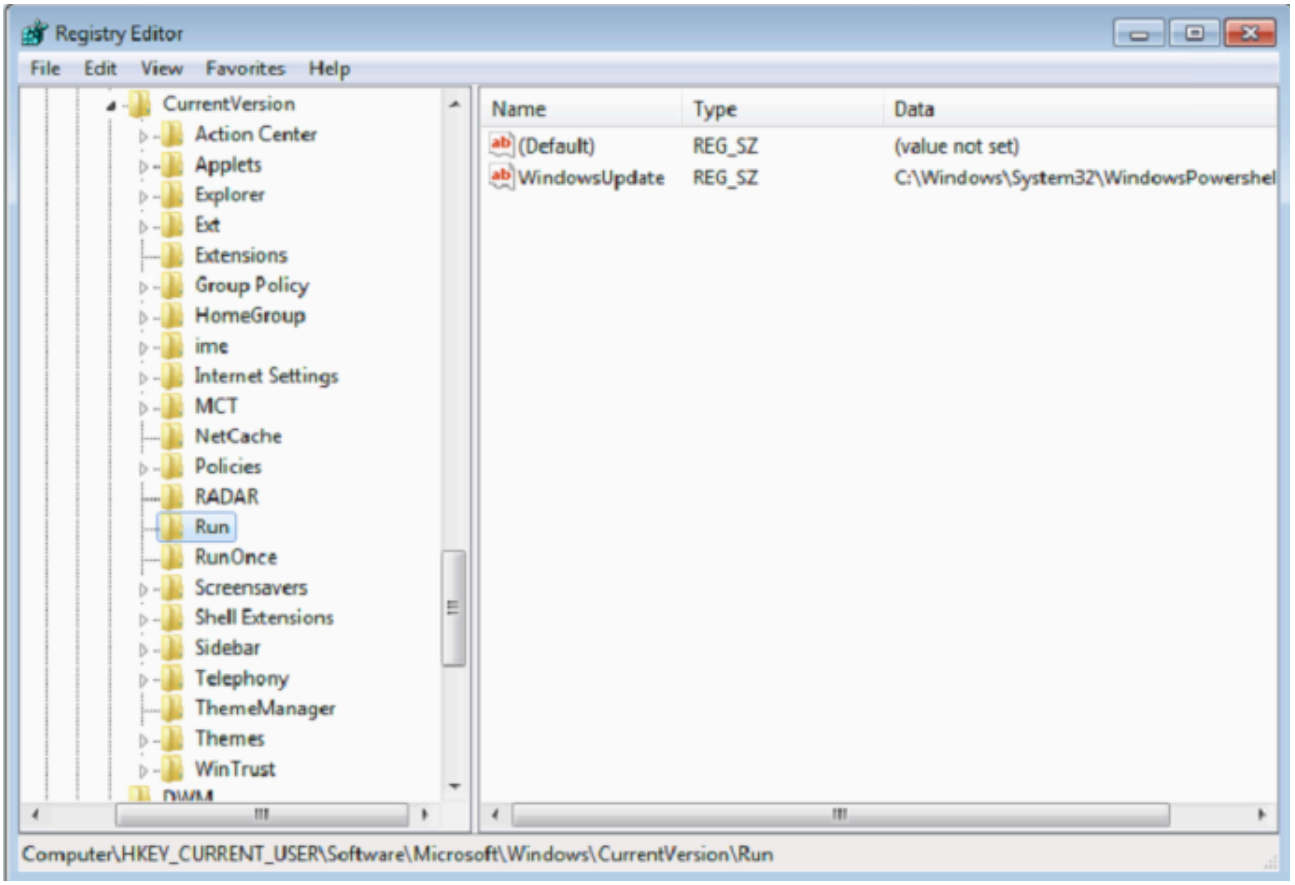
3. It also drops a malicious Normal.dotm (overwrites the old one) in C:\Users\{username}\AppData\Roaming\Microsoft\Templates



NOTHING FISHY HERE 🙂

**This new Normal.dotm file has a macro called AutoExec that executes our new payload. This payload will execute whenever word is opened or in this case, it gets called on startup by persist.ps1.

4. Finally, a registry key is created that executes persist.ps1 that you are hosting. What happens is on startup, persist.ps1 opens a new WINWORD instance pointing to Normal.dotm (which is now malicious) and tells it to execute the AutoExec macro. Once done, it quits. All of this happens in the background.



When the user reboots, it executes persist.ps1 (even though it isn't on disk) which calls Word to open Normal.dotm…all done in the background. Next thing you know, you are having a shell party. WEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEE

I hope you enjoy.

-Matt Nelson (@enigma0x3)

Source: https://enigma0x3.net/2014/01/23/maintaining-access-with-normal-dotm/comment-page-1/