Ultimate Exploitable Quick Build Profile

The accompanying registry templates are designed to dramatically reduce the time required to properly configure Office, EMET, Adobe, and Internet Explorer for maximum malware detection. Use the templates along with this guide for a more efficient IVM customization experience. These settings have been tested with Windows 7 X64. It is recommended to use that as the basis for the exploitable profile.

# Office 2010 Installation procedure

Uninstall the Office Viewer applications using either the GUI, the command prompt, or by running the attached batch file. The recommended and easiest method is to the use the batch file.



If using the command line method, execute the following from a command prompt:

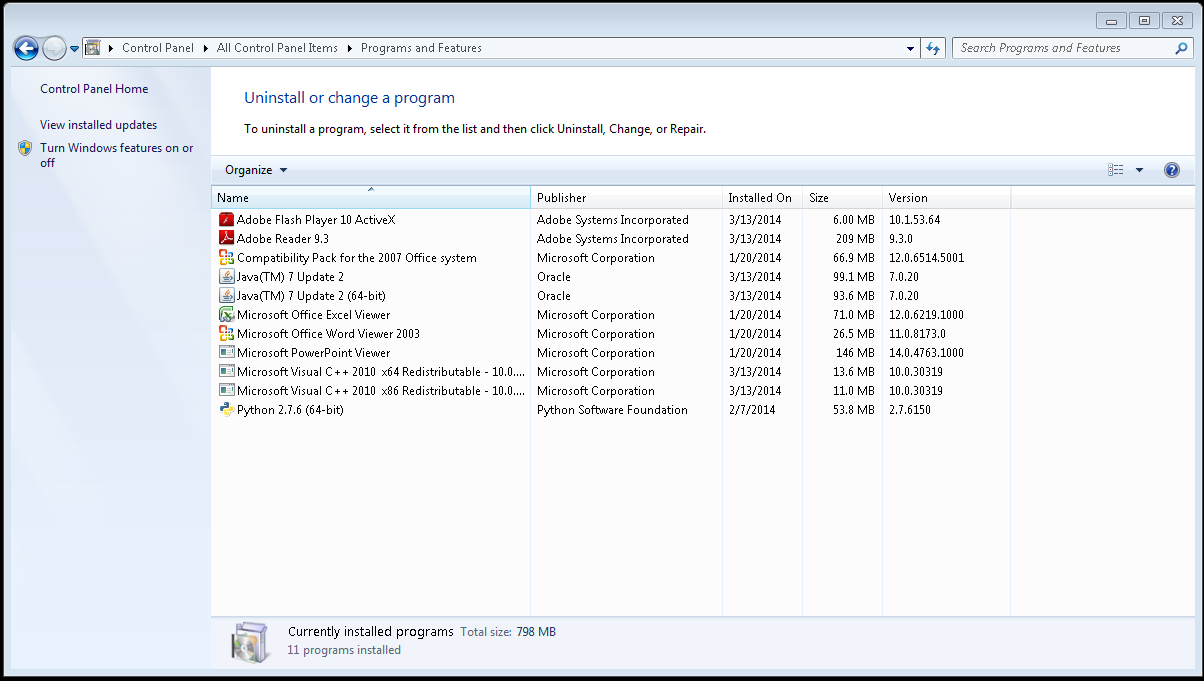
wmic product "Compatibility Pack for the 2007 Office system" call uninstall

wmic product "Microsoft Office Excel Viewer" call uninstall

wmic product "Microsoft PowerPoint Viewer" call uninstall

wmic product "Microsoft Office Word Viewer 2003" call uninstall

If using the GUI method, uninstall the four applications from Programs and Features.



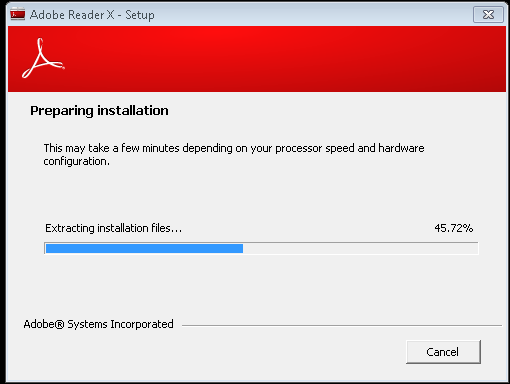
Run the installer for Office 2010. After it is complete, open Word, choose “Don’t make changes”, and then close Word.   


Run the Office 2010 registry template and reboot the iVM from the command prompt with shutdown /r.

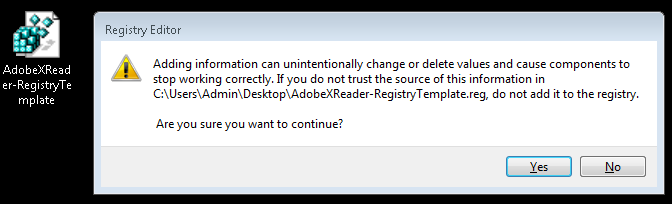
# Adobe Reader X (10.0) installation procedure.

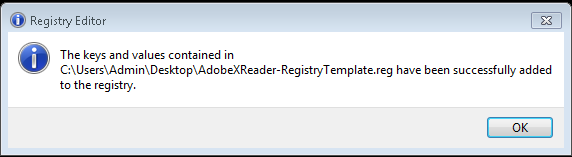
Uninstall Adobe Reader 9.3 using either Programs and Features or execute the following from the command prompt:   
  
wmic product “Adobe Reader 9.3” call uninstall

Run the Adobe Reader X installer.



Run the registry template after the installer completes.





Restart the IVM from the command prompt by issuing shutdown /r.

RDP back into the profile after the reboot and open Adobe Reader X.

From the Start window or command prompt run:

explorer.exe %appdata%\Adobe\Acrobat\10.0\

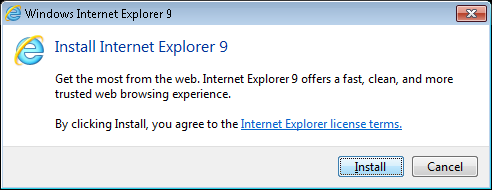
Copy the two .sav files to that folder.

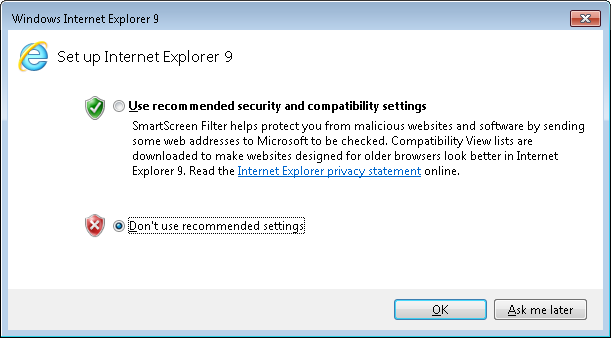


# Internet Explorer 8-11

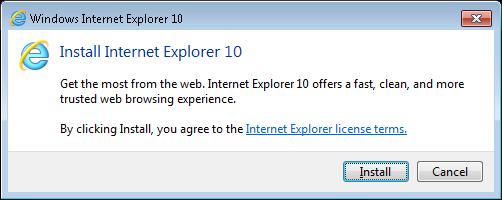
The IE registry templates will place the web browser in a highly vulnerable state. IE 8 and 9 share the same registry template while IE10 and IE11 have a unique registry template. Please note that is not required, nor recommended, to upgrade IE incrementally to later versions. For example, it is best to upgrade to IE11 directly from IE8, skipping upgrades for IE9 and IE10.

IE8: Run the IE8-9 registry template then restart the iVM with a shutdown /r.

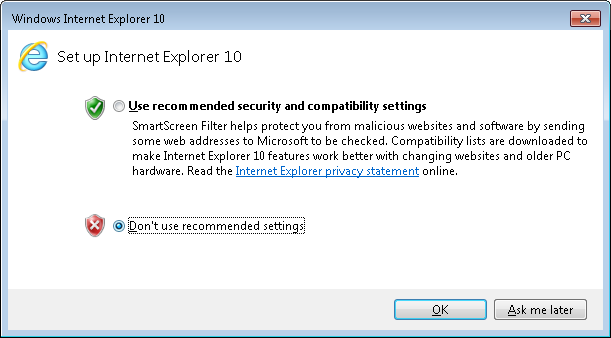
IE9: Upgrade the browser and restart the iVM when prompted.   
  
Open IE9 and select “Don’t use recommended settings”.



Close the browser and run the IE8-9 registry template, then restart the iVM with a shutdown /r.

IE10: Upgrade the browser and reboot when prompted.   


After reboot, open the browser and choose “Don’t use recommended settings”.

Run the IE10 registry template, open and close IE, and then restart the iVM with a shutdown /r.

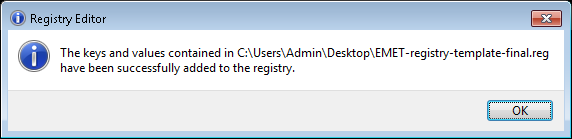
IE11: Upgrade the browser and reboot when prompted.   


After reboot, open the browser and choose “Don’t use recommended settings”. Run the IE11 registry template, and then restart the iVM with a shutdown /r. Open IE once after reboot and then close it.

# Installing EMET 5.5

Install Dotnet Framework 4.5 prior to installing EMET 5.5. Run the EMET 5.5 installer, choose Recommended Settings, and then close EMET. 

Run the EMET 5.5 registry template.

  
Restart the iVM with a shutdown /r from the command prompt.

# Optional – Higher resolution for IVM console screenshots

The default resolution for the iVM console is 1024x768. Run the Set-MAA-Console-Resolution registry template and reboot the IVM with shutdown /r. Please note that some screenshots may require the user to preview them in a new browser tab. Due to the size, the picture navigation buttons are hidden from view.

### Default 1024x768 screenshot:

### 1920x1080 screenshot: