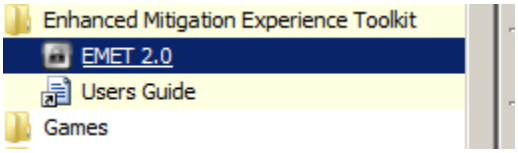
Enhanced Mitigation Experience Toolkit
Michael Ward
12/2010

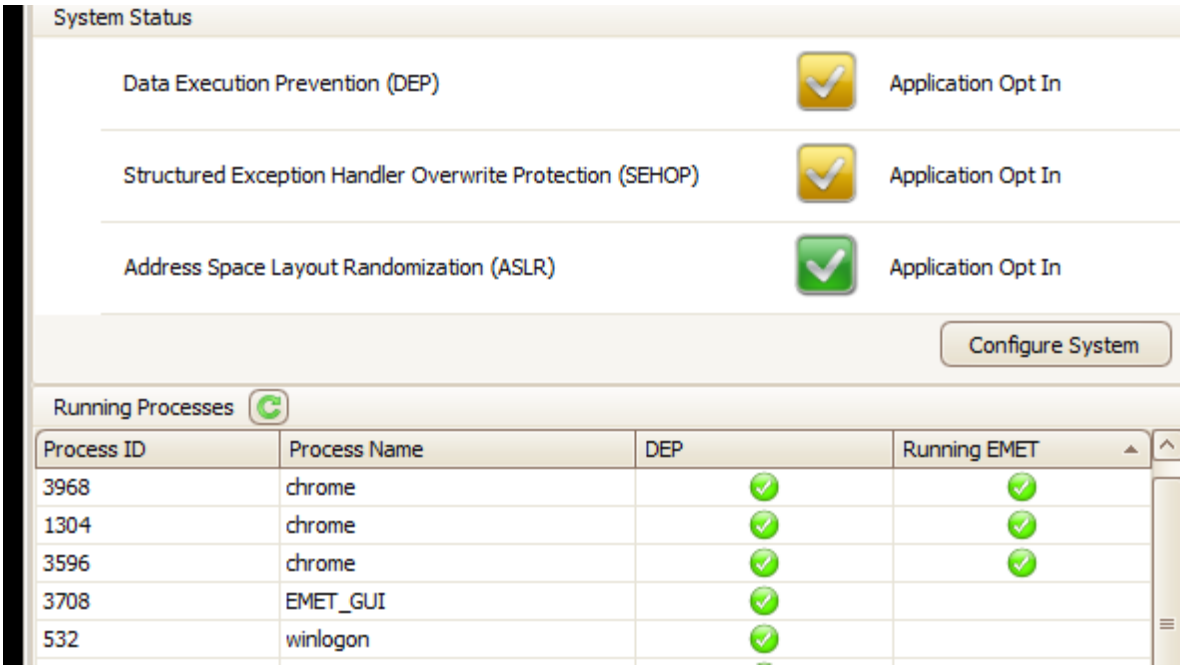
The Enhanced Mitigation Experience Toolkit (EMET) is a free utility from Microsoft to help protect the Windows Operating System (XP and newer) from malware attacks. From Microsoft, "EMET works by applying security mitigation technologies to arbitrary applications to block against exploitation through common attack vectors." After EMET has been downloaded and installed, it has to be configured to protect the user's system and the applications on that system.

Disclaimer: EMET may cause unpredictable behavior for some applications. If you experience frequent crashing or erratic behavior after protecting an application with EMET, you can easily disable EMET.

Launch EMET - The application can be found in the Start Menu.

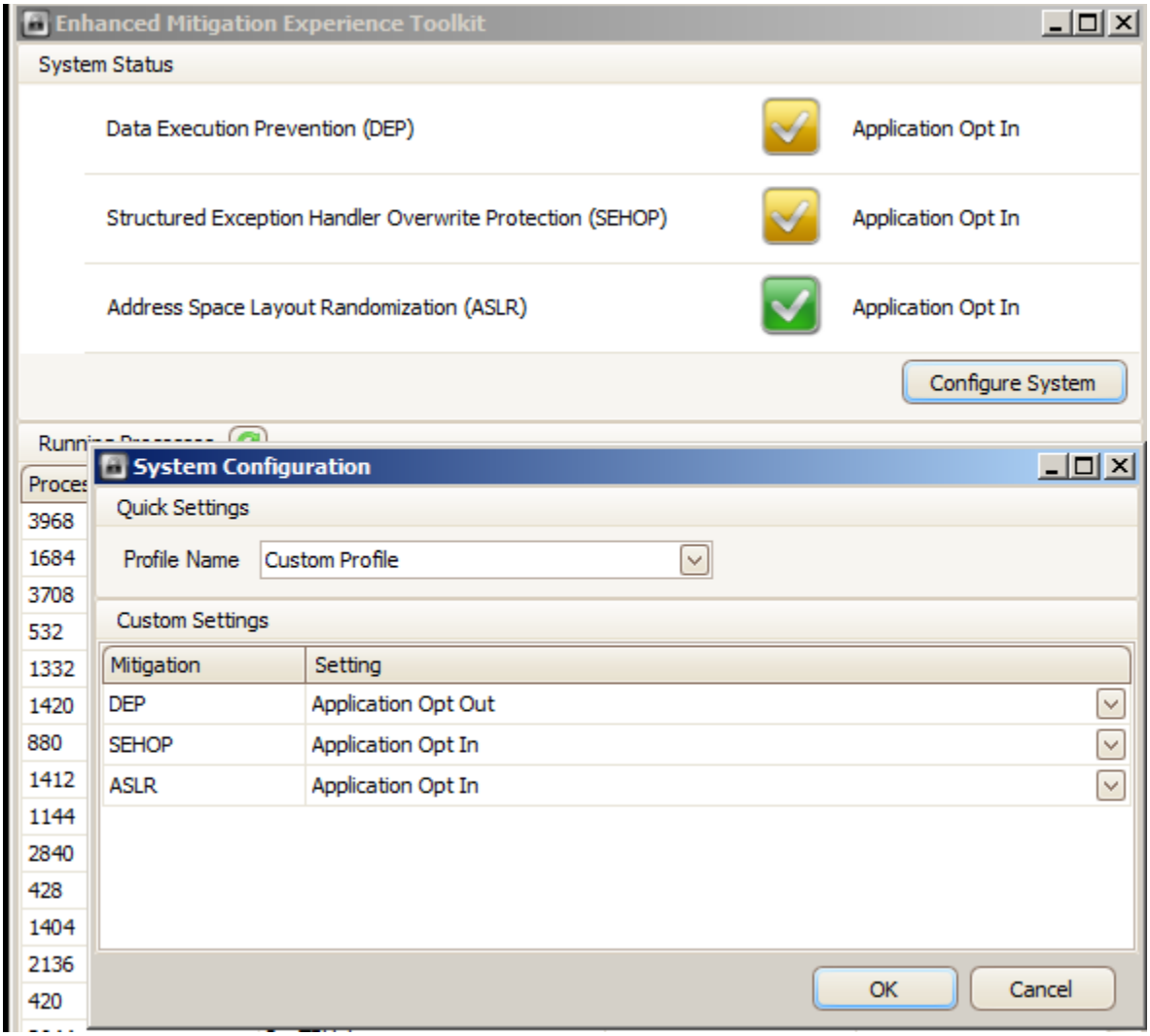


Here you can see EMET protecting Google Chrome.

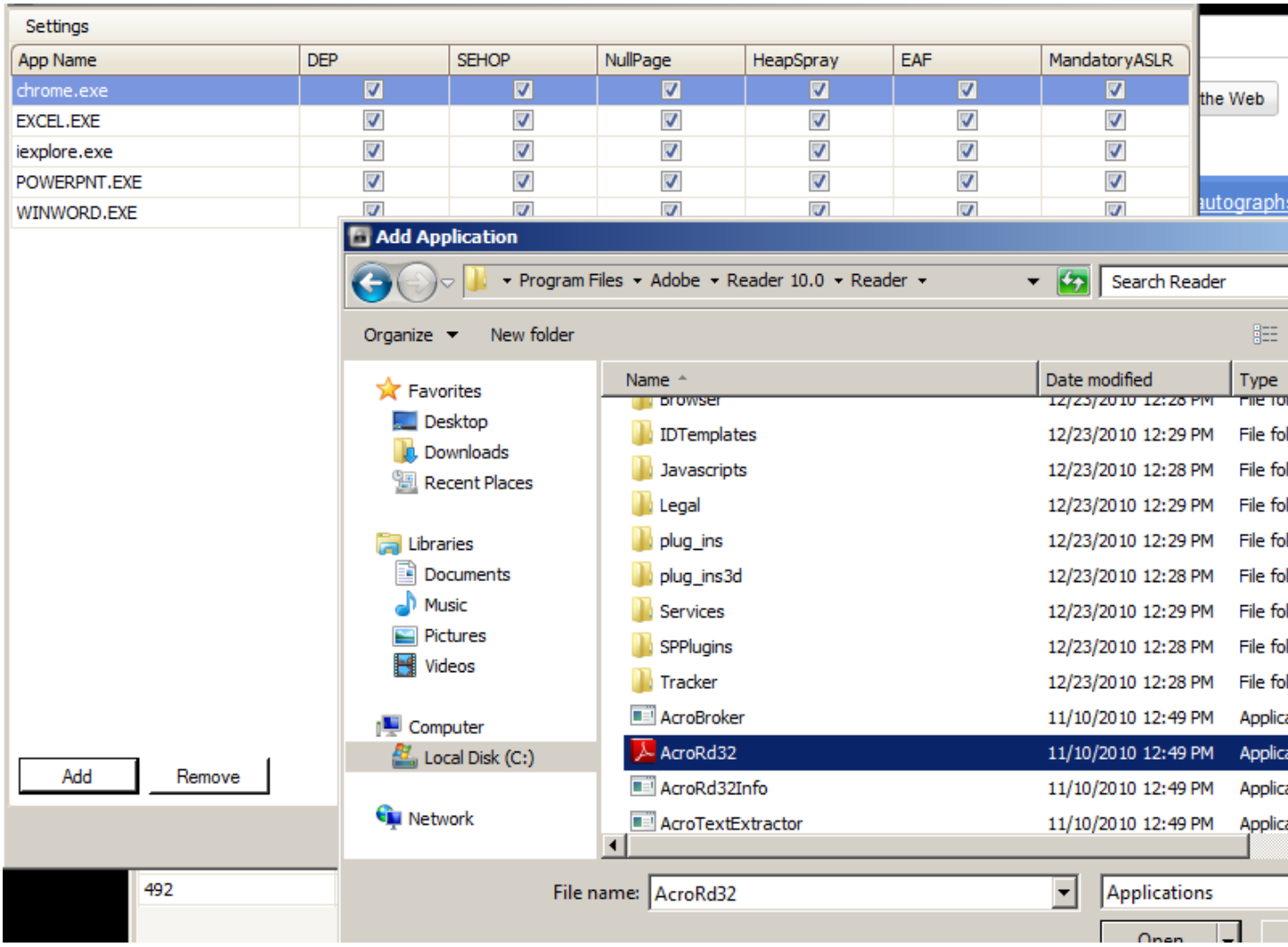


Configure OS Protection - Modern processors allow provide "Data Execution Prevention" (DEP) and Windows can randomize "where" programs are stored within RAM by using "Address

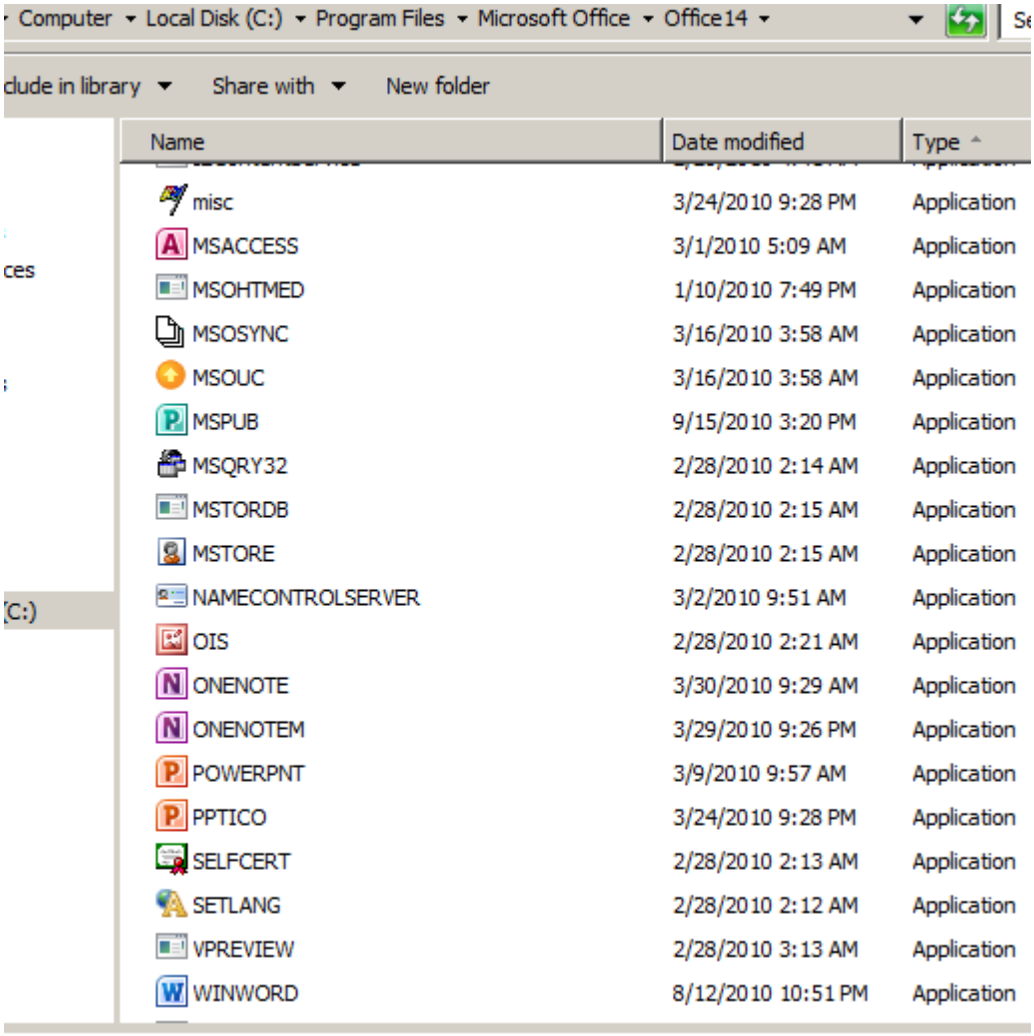
Space Layout Randomization" (ASLR). I suggest that DEP is set to "Application Opt Out" so that it is "on by default" for all applications. Once EMET is launched, click on "Configure System" and change the DEP settings using the drop down menu.



Protecting Applications - Microsoft suggests that you protect, at minimum, Internet Explorer and Adobe Acrobat Reader. Click on "Add" at the bottom left to protect an application. You'll have to navigate to the application (.exe) location. Here you can see Acrobat Reader being protected.



You can see that chrome, Excel, Word, and Powerpoint are already protected. Office applications can be found under:



Note: On 64-bit versions of Windows, Internet Explorer will be installed in both 32-bit and 64-bit versions. Both copies of "iexplore.exe" found in Program Files and Program Files (x86) need to be protected with EMET.

URLS:

Download: http://go.microsoft.com/fwlink/?LinkID=200220&clcid=0x409
EMET Details: http://support.microsoft.com/kb/2458544
EMET in Action Video: http://technet.microsoft.com/en-us/security/Video/ff859539