

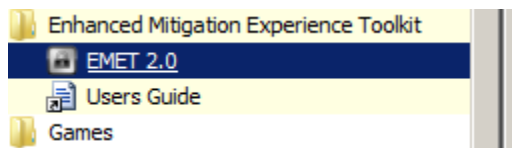
Enhanced Mitigation Experience Toolkit

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.

The screenshot shows the EMET System Status window. It has a 'System Status' section with three rows of settings:

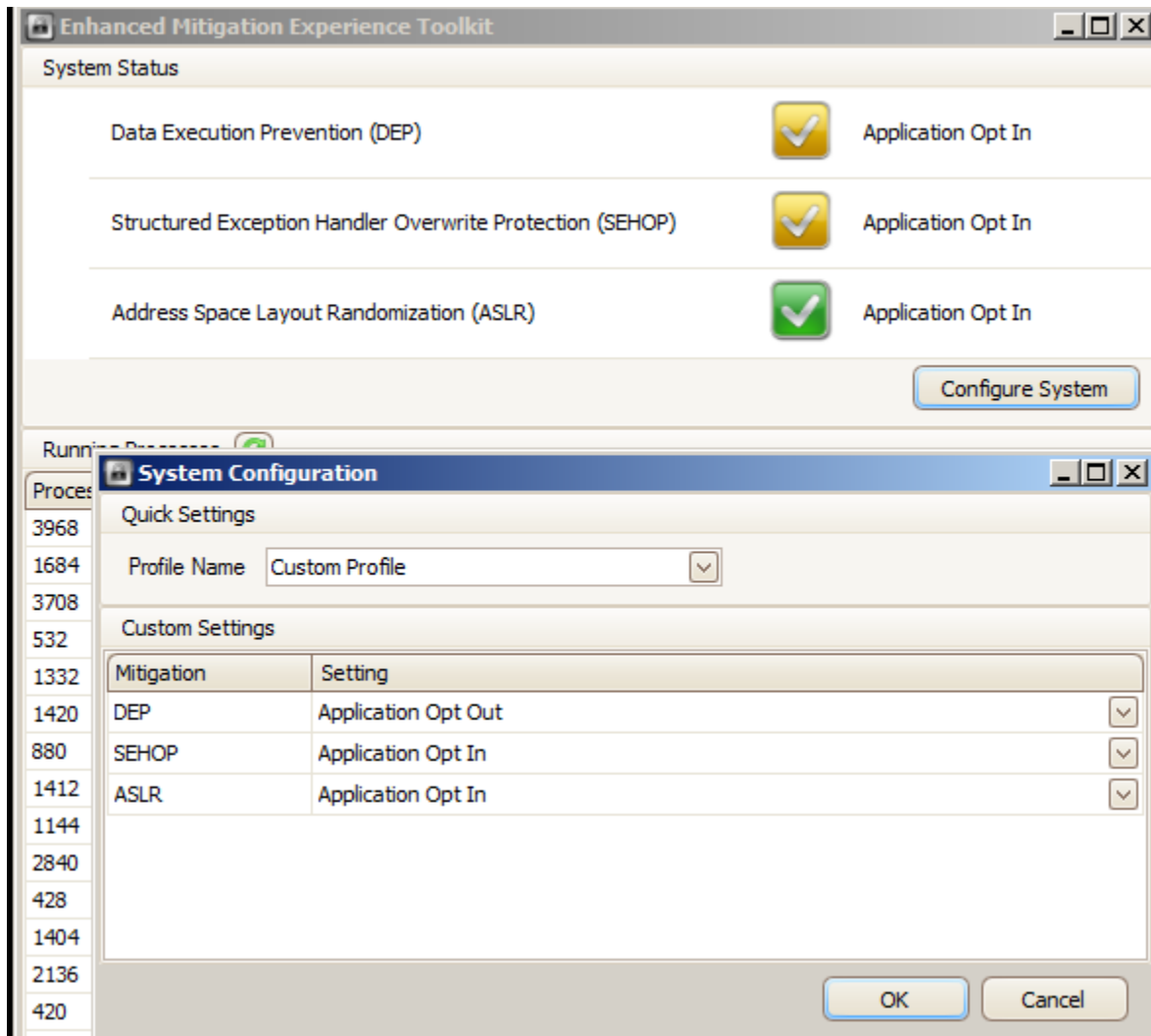
- Data Execution Prevention (DEP) with a yellow checkmark icon and 'Application Opt In' text.
- Structured Exception Handler Overwrite Protection (SEHOP) with a yellow checkmark icon and 'Application Opt In' text.
- Address Space Layout Randomization (ASLR) with a green checkmark icon and 'Application Opt In' text.

Below this is a 'Configure System' button. Underneath is a 'Running Processes' section with a refresh icon. It contains a table with the following data:

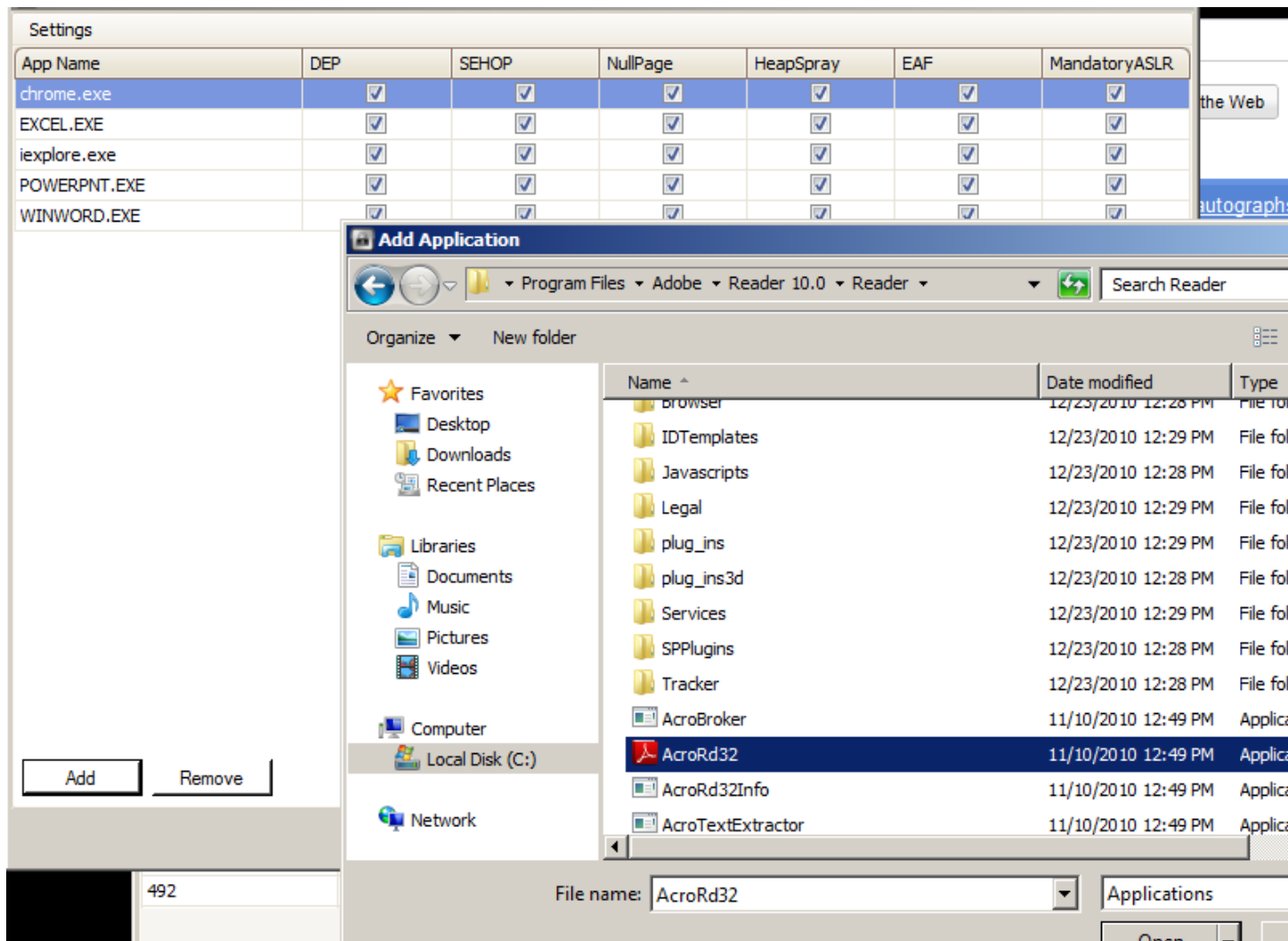
Process ID	Process Name	DEP	Running EMET
3968	chrome	✓	✓
1304	chrome	✓	✓
3596	chrome	✓	✓
3708	EMET_GUI	✓	
532	winlogon	✓	

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:

Name	Date modified	Type
misc	3/24/2010 9:28 PM	Application
MSACCESS	3/1/2010 5:09 AM	Application
MSOHTMED	1/10/2010 7:49 PM	Application
MSOSYNC	3/16/2010 3:58 AM	Application
MSOUC	3/16/2010 3:58 AM	Application
MSPUB	9/15/2010 3:20 PM	Application
MSQRY32	2/28/2010 2:14 AM	Application
MSTORDB	2/28/2010 2:15 AM	Application
MSTORE	2/28/2010 2:15 AM	Application
NAMECONTROLSERVER	3/2/2010 9:51 AM	Application
OIS	2/28/2010 2:21 AM	Application
ONENOTE	3/30/2010 9:29 AM	Application
ONENOTEM	3/29/2010 9:26 PM	Application
POWERPNT	3/9/2010 9:57 AM	Application
PPTICO	3/24/2010 9:28 PM	Application
SELF CERT	2/28/2010 2:13 AM	Application
SETLANG	2/28/2010 2:12 AM	Application
VPREVIEW	2/28/2010 3:13 AM	Application
WINWORD	8/12/2010 10:51 PM	Application

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&clid=0x409>

EMET Details: <http://support.microsoft.com/kb/2458544>

EMET in Action Video: <http://technet.microsoft.com/en-us/security/Video/ff859539>