EMET 4.0: These Aren't the Exploits You're Looking For

By Russ McRee – ISSA Senior Member, Puget Sound (Seattle), USA Chapter

Prerequisites

Windows operating system

.NET Framework 4.0 or higher

In classic *Star Wars* parlance, have you been looking for improved tactics with which to wave off grievous Windows client exploits? Look no further; Microsoft's Enhanced Mitigation Experience Toolkit (EMET) 4.0 was released to the public on June 17, 2013 and quickly caught the attention of security aficionados and general press alike. *KrebsOnSecurity* even gave EMET full coverage[1] and as always Brian's quality work is well worth a read for the 101 perspective on EMET 4.0. So much of the basic usage, configuration, and feature set has already been covered or introduced that I'm going to simply refer you to the Kreb's post as well as Gerardo Di Giacomo's *Threat Mitigation with EMET 4.0*[2] as prerequisite reading material. I work with Gerardo at Microsoft, and as with all *toolsmiths* I sought insight on the tool in question. As his Threat Mitigation post had just gone live as we talked, I will simply draw a quick summary from there; you can read the rest for yourself. EMET is a "free utility that helps prevent memory corruption vulnerabilities in software from being successfully exploited for code execution. It does so by opting in software to the latest security mitigation techniques. The result is that a wide variety of software is made significantly more resistant to exploitation – even against zero-day vulnerabilities and vulnerabilities for which an update is not available or has not yet been applied. EMET offers protections for all currently supported Microsoft Windows operating systems, and supports enterprise deployment, configuration, and monitoring." I will give you the quick bullet list of features but will move quickly to what exploitation mitigations EMET 4.0 offers when tossing attacks via Metasploit against a protected system and applications. Following are feature highlights for EMET 4.0:

- **Certificate Trust**: Detect man-in-the-middle (MITM) attacks that leverage fraudulent SSL certificates.
- **ROP Mitigations**: Block exploits that utilize Return Oriented Programming exploitation techniques.
- **Early Warning Program**: Allows enterprise customers and Microsoft to analyze the details of an attack and respond effectively.
- **Audit Mode**: Provides monitoring functionalities for testing purposes.
- **Redesigned User Interface**: Streamlined configuration and improved accessibility.

Of note, the Early Warning Program sends information back to Microsoft. If yours is an organization that already does this via other enterprise means, this is already common-place behavior; but if your preference is to keep such data in house, you can disable Early Warning under the Reporting menu or use System Center Agentless monitoring to forward the telemetry data to an on-premise server that can be later used for forensics or post-mortem. In production environments, you may want to make use of Audit Mode before setting EMET to terminate programs when attacked. Audit Mode instead simply reports the exploitation attempt; helpful for monitoring potential compatibility issues between EMET and protected applications.

Installing EMET 4.0

Installing EMET is point-and-click simple. Just download,[3] ensure you have .NET Framework 4.0 or higher installed, accept installation defaults (Use Recommended Settings), and you're off to the races.

The *EMET 4.0 User's Guide* included on the download page is a required read as well. I ran EMET 4.0 on a Windows 7 SP1 Enterprise 32-bit VM with .NET Framework 4.0, Java 1.7.0_25, and Firefox 22 (really?).

For testing, I enabled the Maximum security settings under Quick Profiles. This sets Data Execution Prevention (DEP) to Always On and Structured Exception Handler Overwrite Protection (SEHOP) to Application Opt Out as seen in figure 1.

That said, on production systems, take baby steps. You can begin to add other applications than those protected by default (Internet Explorer, Java, Wordpad, Adobe Reader, Microsoft Office, etc.), but as mentioned above and in Kreb's article, phase apps in to ensure they do not struggle or crash with the added protection and "avoid the temptation to make system-wide changes."

1 http://krebsonsecurity.com/2013/06/windows-security-101-emet-4-0/#more-20368.

2 http://technet.microsoft.com/en-us/security/dn283932.

3 http://www.microsoft.com/en-us/download/details.aspx?id=39273.

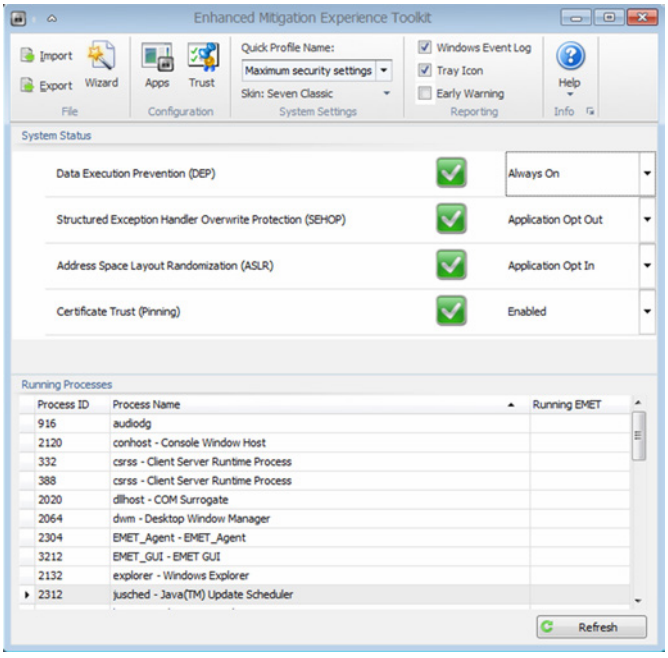

Figure 1 – EMET deployed and ready

EMET 4.0 mitigations and blocked attacks

First up, ye olde heap spray attack. Via Metasploit on my Kali Linux VM, I queued up the *Microsoft Internet Explorer Fixed Table Col Span Heap Overflow (MS12-037)* module.[4] This module "exploits a heap overflow vulnerability in Internet Explorer caused by an incorrect handling of the span attribute for col elements from a fixed table, when they are modified dynamically by JavaScript code" and utilizes ROP chains[5] as part of the attack. Drawing right from Rapid 7, as they describe heap-spray techniques for Metasploit browser exploitation, a heap spray is a way to manipulate memory by controlling heap allocations and placing arbitrary code in a predictable place. This allows the attacker, when controlling the crash, to trick a program into going to said predictable place and gain code execution.[6] Figure 2 represents the attempted delivery of such an attack via Metasploit.

On the Windows 7 VM, when browsing to my attacker server, `http://192.168.220.145:8080/JwJKD1Sjq`, via Internet Explorer, EMET immediately responded with an application mitigation, shut down IE, and popped a Tray Icon notification as seen in Figure 3.

4 https://github.com/OpenWireSec/metasploit/blob/master/modules/exploits/windows/browser/ms12_037_ie_colspan.rb.

5 https://www.corelan.be/index.php/security/corelan-ropdb/.

6 https://community.rapid7.com/community/metasploit/blog/2013/03/04/new-heap-spray-technique-for-metasploit-browser-exploitation.

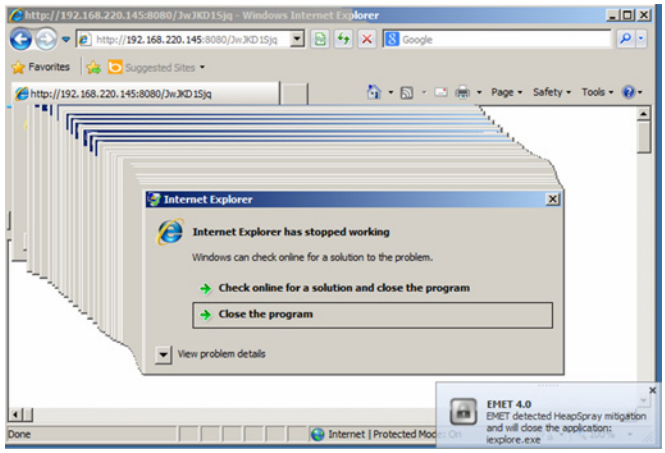

Figure 3 – EMET blocks heap-spray attack

Given that EMET also writes events to the Windows Application Event Log, enterprises are afforded an additional monitoring opportunity as a result. No matter your Windows event collection mechanism, be it Windows Event Collector, Audit Collection Services (ACS), OSSEC,[7] Snare and Splunk, or your preferred method, you can add an alerting mechanism (you may be feeding a SIEM) to give you a heads up when a client machine triggers an EMET event. Regardless, figure 4 represents the Event Viewer perspective on our attack from figure 2.

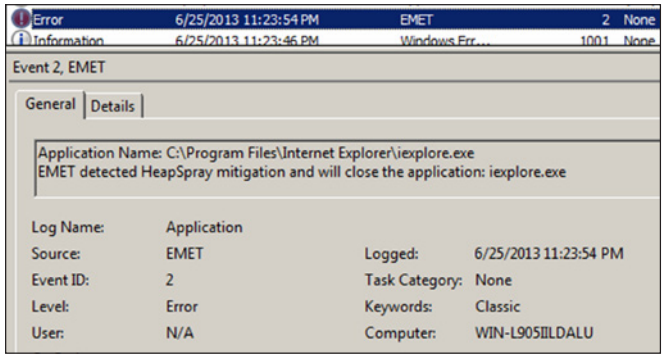

Figure 4 – EMET event in Event Viewer

Another example includes the Mandatory ASLR mitigation. Address space layout randomization (ASLR) randomly arranges the positions of key data areas, to include the base of the executable, as well as position of libraries, heap, and stack, in a process's address space. Note that, as indicated in the *EMET User's Guide*, EMET's mitigations only become active after the address space for the core process and the static dependencies has been set up. Mandatory ASLR does not

7 http://holisticinfosec.org/toolsmith/docs/october2009.html.

```
[+] [2013.06.26-00:50:33] Workspace:default Progress:1/2 (50%) Running Microsoft Internet Explorer Fixed Table Col Span Heap Overflow
[*] [2013.06.26-00:50:35] Started reverse handler on 0.0.0.0:1024
[*] [2013.06.26-00:50:35] Using URL: http://192.168.220.145:8080/JwJKD1Sjq
[*] [2013.06.26-00:50:35] Server started.
[*] [2013.06.26-00:50:49] 192.168.220.128  ms12_037_ie_colspan - Using JRE ROP
[*] [2013.06.26-00:50:49] 192.168.220.128  ms12_037_ie_colspan - Sending exploit to 192.168.220.128:49161...
```

Figure 2 – MS12-037 IE Col Span attack

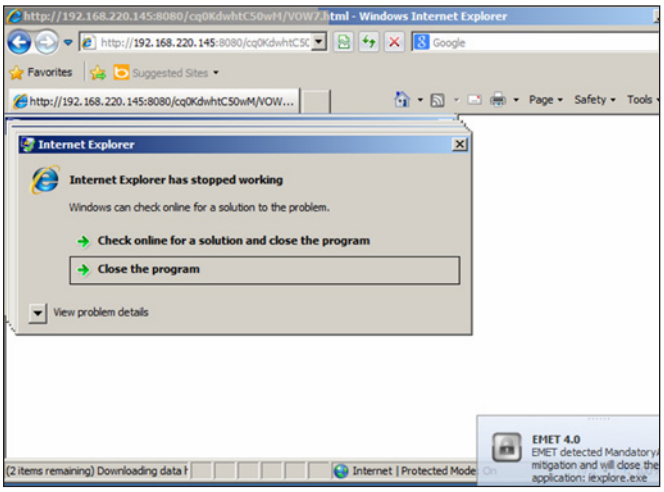

Figure 5 – EMET Mandatory ASLR notification

force address space randomization on any of these. Instead, Mandatory ASLR is intended to protect dynamically linked modules, such as plug-ins. When I browsed my Metasploit instance configured with the *Internet Explorer CSS Recursive Import Use After Free module (MS11-003)* enabled, Internet Explorer was again terminated as seen in figure 5.

Last but not least, I tested the Certificate Trust (Pinning) feature by manipulating the pinned certificates for login.live.com. EMET 4.0 protects the likes of Live, Yahoo, Skype, Twitter, Facebook, and Office 365 by adding extra checks during the certificate chain trust validation process, with the goal to detect man-in-the-middle attacks over an encrypted channel. By default, EMET pins the certificate for a website to the good, trusted Root CA certificate; login.live.com is pinned to Baltimore CyberTrust Root, Verisign, GlobalSign Root CA, and GTE CyberTrust Global Root, as these are the Root CA certificates that are expected to have issued a certificate for login.live.com. I arbitrarily removed these and imported a Thawte Windows Trusted Root Certificate (trusted by Windows). This resulted in EMET sounding off with another "I don't think so" as seen in Figure 6.

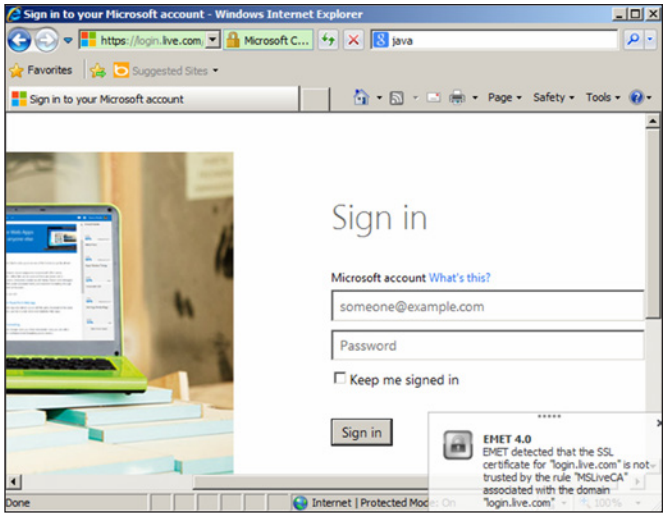

Figure 6 – EMET trusts you not

As Thawte is clearly not the Root CA that issued the certificate for login.live.com, EMET flagged the SSL cert. By pinning the right certificates' websites to their expected Root CA certificates, you can detect scenarios where a certificate is fraudulently issued from a compromised Root CA or one of its intermediates.

For you command line fans, you can choose to utilize `EMET_Conf.exe`. You'll need to set `C:\Program Files\EMET 4.0` in your PATH statement if you wish to call `EMET_Conf.exe` from any prompt. `EMET_Conf.exe` allows you to add applications, list those already added, list enabled mitigations and trusts, as well as remove, modify, import/export, and configure.

Remember, for those of you with enterprise deployment responsibilities, EMET can be deployed and configured with System Center Configuration Manager (SCCM), and EMET system and application mitigation settings can be configured via Group Policy.

In conclusion

The release of version 4.0 brings EMET squarely in sight for users who may have been hesitant to utilize or deploy it. Now's the time to investigate and engage (wait, that's *Star Trek*). EMET 4.0 adds a layer of protection that friend, and EMET's #1 fan, TJ O'Connor refers to as "creativity in defense," freaking creative even. Remember, test and tune before going full tilt boogie, but know that EMET adds defense-in-depth for one host or an entire enterprise, even in the face of zero-days.

Ping me via email if you have questions (russ at holisticinfosec dot org).

Cheers…until next month.

Acknowledgements

—Gerardo Di Giacomo, Security Program Manager, Microsoft Security Response Center (MSRC) Software Security Incident Response team

About the Author

Russ McRee manages the Security Analytics team (security incident management, penetration testing, monitoring) for Microsoft's Online Services Security & Compliance organization. In addition to toolsmith, he's written for numerous other publications, speaks regularly at events such as DEFCON, Black Hat, and RSA, and is a SANS Internet Storm Center handler. As an advocate for a holistic approach to the practice of information assurance Russ maintains holisticinfosec.org. He serves in the Washington State Guard as the Cybersecurity Advisor to the Washington Military Department. Reach him at russ at holisticinfosec dot org or @holisticinfosec.