Microsoft EMET

a view from the trenches

Branden Carter
March 5, 2015

A little about ITD…

Our Mission:

Your Safety

Your Mobility

Your Economic Opportunity

For more information: http://itd.idaho.gov

ITD's Computing Environment

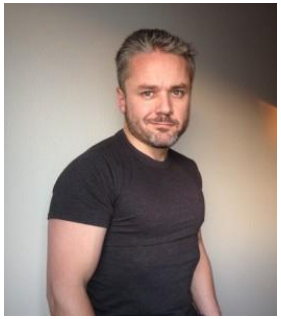
Approximately:

- 1600 Employees
- 2000 PCs
- Over 100 locations across all of Idaho
- 277,000 online DMV transactions last year

Why EMET

1. ITD had 64 different versions of a very specific, high caffeine program that was being hammered with zero days that weren't getting patched by the vendor. (Hint: an oracle couldn't even tell us when patches were going to be released)

2. 'Cause a few people who some might consider knowledgeable said it was a good idea.



What is EMET

Enhanced Mitigation Experience Toolkit

EMET anticipates the most common attack techniques attackers might use to exploit vulnerabilities in computer systems, and helps protect by diverting, terminating, blocking, and invalidating those actions and techniques.*

* Quoted from EMET 5.1 Users guide

What is EMET

- EMET uses in-memory application behavior to stop exploits.
- EMET also uses psuedo mitigations to stop some of the most common exploits.

What are the EMET mitigations?

System Mitigations	Application Specific Mitigations	All Application Mitigation Settings
Data Execution Prevention	***DEP***	Stop on Exploit/Audit Only
SEHOP	SEHOP	Deep Hooks (ROP)
ASLR	Null Page	Anti Detours (ROP)
Certificate Trust (Pinning)	*HeapSpray*	Banned Functions (ROP)
	EAF	
	EAF+	
	Mandatory ASLR	
	BottomUP ASLR	
	LoadLib (ROP)	
	MemProt (ROP)	
	Caller (ROP – 32 bit)	
	SimExecFlow (ROP – 32 bit)	
	StackPivot (ROP)	
	ASR	

Queue live demo…

- not as cool as it sounds ☺

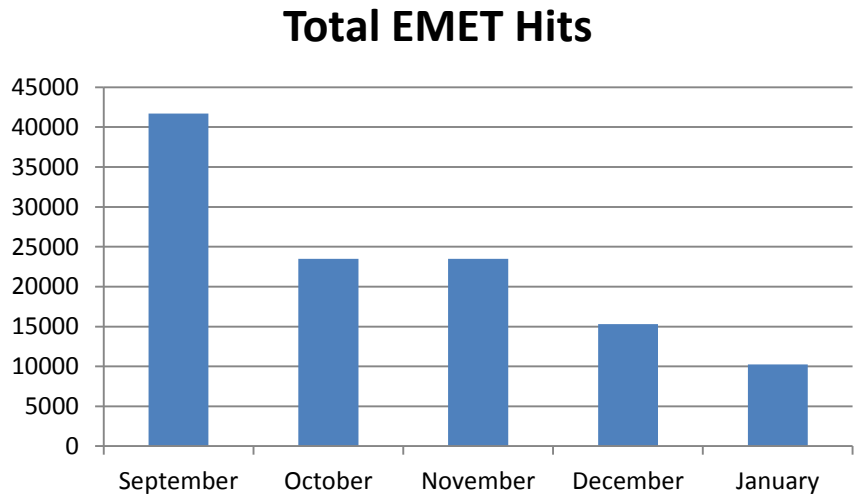
- Note: Microsoft defaults have been loaded to show what they look like.

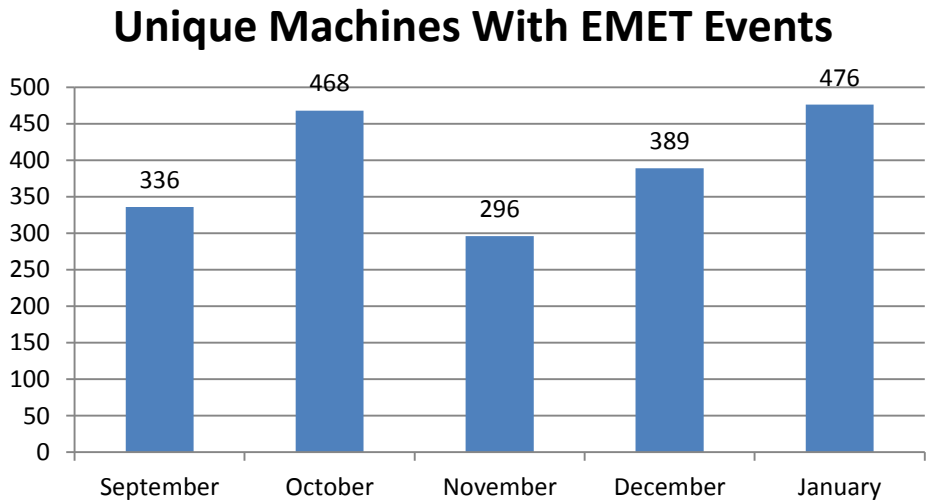
Deploying EMET

- Deployed like any other enterprise software
  - Step by Step for Microsoft SCCM and GPO deployments
- No central administration console!
  - Configuration tweaks are a challenge
  - Reporting is a challenge, but a federal TLA has made it much easier!
    - https://www.nsa.gov/ia/_files/app/spotting_the_adversary_with_windows_event_log_monitoring.pdf
  - Metrics are PAINFUL

Metrics

- EMET impacts approx. 10-20% of ITD PCs in a given month. Most mitigations are not seen by end users.
- Benefits of Metrics:
  - Indicators of malicious activity
  - Indicators of user interference (false positives)
  - Difficult to attribute – just ask my supervisor!



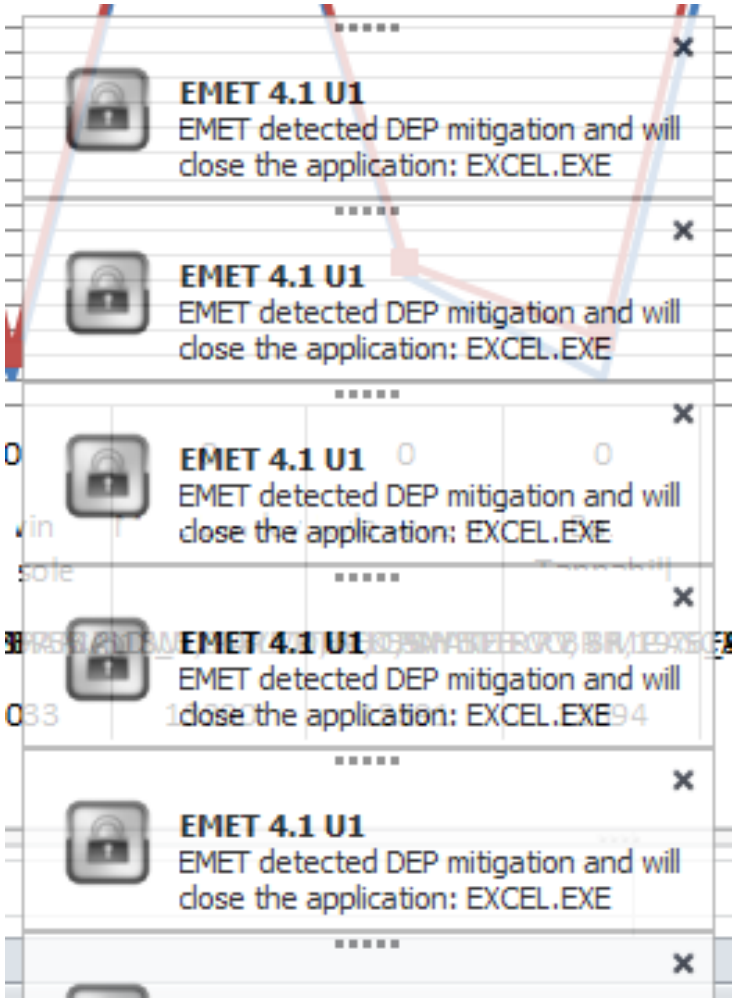


Where does EMET fit?

- EMET geared towards disrupting 0-day exploits in Applications
- EMET is not AntiMalware/AV/HIPS
- EMET is not signature based
- EMET will not detect pre-installed malware
- EMET is not a program that will prevent a local admin from installing malware attachments in emails

Lessons Learned: The Bad

- Can crash legitimate appliations (DEP, ASR) – Testing! Testing! Testing!
- Metrics are painful and time consuming
- Reporting is not 100%
- Technician acceptance
- Configuration drift
- Audit only caveats



Lessons Learned: The Good

- The price is right
- Buys time for patch testing/deployment for some vulnerabilities
- Can close the gap that other mitigations can leave
- Metrics can yield valuable information
- Did I say the price is right?

Final Words

- If you have have tackled things like patch and vulnerability management, have good AV/HIPS configuration and reporting, etc. EMET can help prevent exploits that might still be getting through.
- If you have a specific piece of old software that you think/know is vulnerable – EMET can help. Mitigations aren't limited to defaults.
- Realize that EMET takes time and management overhead. Don't get lost in the mountains of data!
- Focus on things like SANS top 20 controls – EMET isn't a cure all.

Questions?

Resources and Credits

- EMET Mitigations and Guidelines: http://support.microsoft.com/kb/2909257
- Microsoft EMET Users Guide (Program Files Directory)
- Bromium Critique of EMET 4.1

http://labs.bromium.com/2014/02/24/bypassing-emet-4-1/

- Brian Krebs EMET Overview

http://krebsonsecurity.com/2013/06/windows-security-101-emet-4-0/

- David Kennedy/TrustedSec: EMET 5.1 Installation Guide

https://www.trustedsec.com/november-2014/emet-5-1-installation-guide/

- NSA on Windows Event Log Analysis and Reporting

https://www.nsa.gov/ia/_files/app/spotting_the_adversary_with_windows_event_log_monitoring.pdf

And thanks to en.wikipedia.org and Microsoft Technet for datum on several of the specific mitigations!

Contact Information:

branden.carter [at] itd.idaho.gov brandenm [at] gmail.com