Invincea and Microsoft EMET

An Exploit-tested Comparison of Invincea FreeSpace and Microsoft EMET 5.0 for Protecting against Web-based Attacks

September 2014
# Table of Contents

Summary ................................................................................................................................. 3  
Microsoft EMET Approach .................................................................................................. 3  
Technical Analysis ............................................................................................................... 4  
  System Configuration ....................................................................................................... 5  
The Exploit ......................................................................................................................... 6  
  Testing the EMET-only System ....................................................................................... 6  
  Testing with FreeSpace installed on EMET system ......................................................... 10  
Conclusion and more information .................................................................................... 13
Summary

As security practitioners, we believe Microsoft EMET can have a role in protecting against certain types of drive-by exploits of the browser, but we show in this white paper that it leaves uncovered broad classes of exploits that are commonly used in practice.

We do not assess the application compatibility challenges of EMET, nor the enterprise manageability concerns deploying EMET into production environments – essential considerations when operationalizing security technologies. Rather, we show how relatively conventional Java exploits can still bypass and exploit an EMET-protected web browser configured for standard Internet browsing.

Microsoft EMET Approach

The Enhanced Mitigation Experience Toolkit (EMET) is a memory protection tool released by Microsoft to protect applications against memory exploits. Most recent versions of Microsoft applications including Internet Explorer (IE) 10/11 and Microsoft Office already come pre-built with memory protection mechanisms including ASLR and DEP. Additionally, Windows 8.1 includes a number of operating system security enhancements as well. However, older versions of IE and MS Office can still benefit from EMET to protect against memory exploitation.

These security effectiveness tests were performed using a website hosting a Java exploit which installed a Remote Access Trojan (RAT). We then compared the protection capabilities of EMET against Invincea FreeSpace™ and show how FreeSpace has broad coverage against the range of exploits seen in practice including Java-based exploits.

We conclude that the Invincea-protected system was completely protected while the system protected by Microsoft EMET 5.0 alone was exploited and compromised prior to
detection or prevention. (Note that it’s not required to deploy EMET with Invincea to get the benefits of advanced threat prevention afforded by Invincea – one could deploy Invincea alone.)

Technical Analysis
For the experiment, we created a web site that hosts malicious code that exploits a known vulnerability against Java through the web browser which installs a RAT toolkit on the compromised system affording remote access and data exfiltration capabilities to the attacker. All of this occurs without any user interaction; simply visiting the malicious website automatically and transparently exploits the user system.

We run the experiment twice: first with the latest version of EMET 5.0 installed by itself (without FreeSpace), and then run the test again with FreeSpace installed co-resident with EMET, then document the results here. These two tests illustrates that exploits are able to bypass EMET’s protection but are still detected and blocked by Invincea.

EMET 5.0 provides a number of memory protection mechanisms as shown below.

<table>
<thead>
<tr>
<th>EMET Security Mitigations</th>
<th>Included</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Execution Prevention (DEP) Security Mitigation</td>
<td>✓</td>
</tr>
<tr>
<td>Structured Execution Handling Overwrite Protection (SEROP)</td>
<td>✓</td>
</tr>
<tr>
<td>NullPage Security Mitigation</td>
<td>✓</td>
</tr>
<tr>
<td>HeapSpray Allocation Security Mitigation</td>
<td>✓</td>
</tr>
<tr>
<td>Export Address Table Filtering (EAF) Security Mitigation</td>
<td>✓</td>
</tr>
<tr>
<td>Mandatory Address Space Layout Randomization (ASLR) Security Mitigation</td>
<td>✓</td>
</tr>
<tr>
<td>Bottom Up ASLR Security Mitigation</td>
<td>✓</td>
</tr>
<tr>
<td>Load Library Check – Return Oriented Programming (ROP)</td>
<td>✓</td>
</tr>
<tr>
<td>Memory Protection Check – Return Oriented Programming (ROP)</td>
<td>✓</td>
</tr>
<tr>
<td>Caller Checks – Return Oriented Programming (ROP)</td>
<td>✓</td>
</tr>
<tr>
<td>Simulate Execution Flow – Return Oriented Programming (ROP)</td>
<td>✓</td>
</tr>
<tr>
<td>Stack Pivot – Return Oriented Programming (ROP) Security Mitigation</td>
<td>✓</td>
</tr>
</tbody>
</table>

Figure 1: Memory protections afforded by EMET 5.0

Even with EMET in use and more recent versions of IE and Windows deployed, one considerable vulnerability remains – third party plug-ins such as Java and Flash – even though they can be configured to be protected by EMET. In fact the number of exploits against Java and other third party plug-ins dwarf exploits of native vulnerabilities found
in IE and MS Office. In the following tests, we show by experiment how typical exploits work in spite of having EMET protections in place.

**System Configuration**

Two separate virtual systems were used to perform these tests. Both systems run in VMWare Workstation and configured with a base installation of Microsoft Windows 7 32-bit Operating System. Both systems include Internet Explorer version 8 and Java version 6 update 23. These two applications were the focus for these tests.

One system runs Microsoft EMET 5.0 by itself; the second system runs an identically-configured EMET 5.0 installation plus Invincea FreeSpace.

On both systems, the EMET configurations were slightly modified to increase the level of protection from the standard installation, while FreeSpace is running with the default installation configuration.

The EMET configurations for these tests (highlighted in the screenshots below) are changed to provide maximum protection beyond the default installation configuration.

![Figure 2: Maximizing the protection configuration of EMET 5.0](image-url)
The Exploit
A Java-based exploit that leverages CVE-2013-2465 was hosted on a publically-accessible web site. Details on the vulnerability are available here:

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2465

Testing the EMET-only System
In Figure 4, we show successful exploitation of the IE 8 browser, the EMET UI and Process Explorer GUIs.

Upon browsing to the exploit URL in IE 8, Java is automatically loaded and subsequently creates a new process. The process creation itself is the result of the Java exploit that just executed – we see a window dialog opening that indicates the exploit was successful.

Note the three application processes running on the host in Figure 4, configured to be protected by EMET. The Process IDs (PID) of these processes match the displayed processes in Process Explorer.
Now let’s take a look at a new process running on the system – “jjacygb”. By hovering over the process in Process Explorer we can see the location of this file. The file location is `%localappdata%\temp`.

When the “Exploitation Successful” window is closed, the jjacygb process spawns iexplore.exe. A close examination of the hijacked iexplore process running reveals that it’s attempting to establish a connection to a server.
We are able to see that Command and Control (C2) was established by a network packet capture in Figure 7. The source IP address in the packet captures match the IP address of the iexplore process in Figure 6 above. We can also see 2 unique files being written to the desktop, TESTING.txt and MALICIOUS.txt.
The two documents that were created by the exploit on the desktop are shown in Figure 8 below. Both documents were later retrieved and removed from the system through the hijacked iexplore.exe process.

A “remote chat session” was then initiated through the hijacked iexplore.exe process. EMET ultimately was able to detect the chat session, but unfortunately the damage had already been done to the target system. One could imagine that a more stealthy remote application launch could be employed by the attacker to evade EMET detection at this point; nevertheless, this system was already compromised.
Testing with FreeSpace installed on EMET system

Next, we tested the same system configuration on a second virtual machine but used Invincea FreeSpace to protect the browser this time.

For this test with Invincea we have an IE 8 browser and Process Explorer open in Figure 10. We entered the same exploit URL in IE 8, Java is automatically loaded and attempts to create a process exactly as it did in the EMET-only test. **Unlike EMET, Invincea immediately detects and terminates the offending process.**

![Figure 10: Desktop screen capture](image)

For documentation purposes, we enabled full detail alerting within FreeSpace. With alerting enabled, we can easily see that an attempted infection was contained, detected and terminated. The alert below is what is showing in the bottom right corner of the screen from the image above. By clicking on the “Details...” link in this configurable alert, we can see additional information about the blocked infection attempt.

![Figure 11: Alert box](image)
Note that a full forensic capture is recorded by FreeSpace and uploaded to the Invincea Management Service (IMS) management console for analysis. As configured for this test, an optional setting of “terminate all threats as they are detected” is enabled. With this configuration all malware is immediately terminated upon execution thereby protecting the system under attack. Only the attack attempt has been recorded for analysis since the full attack lifecycle as seen in the EMET-only system was prevented from running on this system. Illustrated below in Figure 12 is the offending process that was terminated and the source website of the infection attempt.

![Invincea Alert](image)

**Figure 12: Summary of detected exploit**

From the IMS management console we can see additional details about the threat. First, in Figure 13 we can see a brief summary about the threat. We see the source domain, number of system changes, and the time the threat was triggered and received by the server.
By drilling down into the Events tab in Figure 14, the system provides additional forensic data about this threat to include executables and files written to the file system, registry modifications, processes launched, and outbound connections opened. In this test, no executables were written and there were no outbound connections due to Invincea terminating this initial exploit threat as it attempted to execute.

By clicking on any of the forensic information listed, we can obtain actionable information on the object. For this demonstration we’ll select the process that attempted to launch as a result of the Java exploit. Note the process name, path (located inside the Invincea Secure Virtual Container and not on the host), MD5 hash, and ability to look up additional information on the threat.
A full demonstration of the exploit is recorded in video and available here: 

**Conclusion and more information**

This white paper demonstrates that the additional layer of security provided by Microsoft EMET, while helpful for memory exploits, does not provide the necessary level of protection against common web-based threats including exploits against plug-ins and user-initiated executable launches.

In comparison, Invincea FreeSpace defeats these attacks by running untrusted content, including Java, inside a secure virtual container as shown in this whitepaper.

Invinccea demonstrates its ability to defeat known and unknown malware all without compromising usability. The website used for demonstration in this paper serves as a clear example of the thousands of exploited websites used to compromise users and organizations today. These types of compromised sites are leveraged daily in the form of spear-phishing, watering hole attacks, drive-by download exploits, poisoned search results, scareware/crimeware, social networking worms, and user-initiated infections.
Organizations will continue to be vulnerable and continue to get compromised without protection from these types of attacks. Free security products like EMET 5.0 provide a layer of security against memory-based exploits for programs compiled without ASLR and DEP protection, but it does not address significant threats from third party components such as Java.

For more information on the Invincea platform and protecting against user-targeted exploits and other forms of security threats, please contact:

- Website: www.invincea.com
- Email: info@invincea.com
- Phone: +1-855-511-5967 or +1-703-352-7680