

Fake FBI email Worm Exposed

24th Feb, 2005

Debasis Mohanty (a.k.a Tr0y)

www.hackingspirits.com

debasis@hackingspirits.com

Table of Contents

Introduction.....	3
Advisory – Fake FBI email Worm.....	4
Reversing The Malicious Code.....	8
Conclusion	10
About Author	10

Introduction

On 21st Feb, 2005 I came across a worm which impersonated a FBI email ID as a sender ID and claimed to have been sent by "M.John Stellford" from FBI. The message body text is given below:

Dear Sir/Madam,

we have logged your IP-address on more than 40 illegal Websites.

Important: Please answer our questions!
The list of questions are attached.

Yours faithfully,
M. John Stellford

++++ Federal Bureau of Investigation -FBI-
++++ 935 Pennsylvania Avenue, NW, Room 2130 Washington, DC 20535
++++ (202) 324-3000

On receipt of such a mail, any normal computer user will get scared at the first instant. Some might ignore it but some out of curiosity would go ahead in opening the attachment. That's it, END OF STORY!!! YOU ARE NOW INFECTED.

I have setup a Windows machine for malicious programs collection and analysis and in this paper I shall share my experience of reverse engineering and analysis of this new FBI email worm. Going further I shall also provide an advisory on how to remove this worm manually.

Advisory – Fake FBI email Worm

Description

The mail containing the attachment is a mass mailer worm which impersonates the sender's ID and appears to be sent by someone from FBI. The body texts read such that it entices the user to open the attachment and answer few of the questions asked by FBI. The attachment carries a payload of 51,688 Bytes Win32 executable with a fake extension as .txt (visible to the user).

Impact

As such, this worm is just a mass mailer and other than mass mailing there is no trace of stealing critical information from the victim's system.

Payload Details

File Size: 51.68 KB

File Extension: .txt [Space Inserted to Fake the Extension] .pif

File type: Win32 Executable

This worm uses two different languages (i.e. German and English) in the body text to send mails. One execution, the worm creates 3 copies of it and drops it in the following folder: “%WinDir%\msagent\win32\”. The 3 copies created are “csrss.exe”, “smss.exe” and “winlogon.exe”.

It makes the following entries in the system registry to start the program on system boot:

Key Name: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Key Value Name: winsystem.sys
Key Value Data: %WinDir%\msagent\win32\smss.exe

Key Name: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Key Value Name: winsystem.sys
Key Value Data: %WinDir%\msagent\win32\smss.exe

It creates 6 DAT files in the “%WinDir%\System” folder and in the original file extraction folder to store email IDs being fished out from the victim's system. The DAT files created are as follows:

datamx1.dat
datamx2.dat
datamx3.dat

goto1.dat
goto2.dat
goto3.dat

The email IDs found in the victim's machine is used by the worm for further spreading. It searches for email IDs in the following file types:

csv, bak, xhtml, cms, nws, vcf, ctl, dhtm, cgi, ppt, msg, jsp, vbs, pst, cfg, dsw, cls, ini, log, mdb, xml, wsh, pl, rtf, doc, nch, xls, txt, wab, eml, hlp, mht, php, asp, shtml, dbx

This worm comes with the following "subject", "sender ID", "attachment name" and "body text":

Subjects:

You visit illegal websites
Alert! New Sober Worm!
Your new Password
Mail_delivery_failed
Paris Hilton, pure!
Mail_delivery_failed

Sender ID:


police@FBI.gov
FBI@fbi.gov
web@fbi.gov
police@fbi.gov
Admin@fbi.gov
Officer@fbi.gov
security@microsoft.com
service@fantaseem.com
host@blockbuster.com

Attachment's name:

indictment_cit(some number here).zip
text-indictment_cit(some number here).zip
text.zip
text-(some number here).zip
patch_help_text.zip
register_text.zip
help-text.zip
header_text.zip

Body Texts:

a. Sample Screenshot 1: (Fake Mail Impersonating a FBI email ID)

From: Officer@fbi.gov **Fake FBI email ID**
To: mail@hackingspirits.com
Cc:
Subject: You visit illegal websites
Attachments:  indictment_cit7706.zip (51 KB) **Worm Attachment**

Dear Sir/Madam,

we have logged your IP-address on more than 40 illegal Websites.

Important: Please answer our questions!
The list of questions are attached.

Yours faithfully,
M. John Stellford

++-++ Federal Bureau of Investigation -FBI-
++-++ 935 Pennsylvania Avenue, NW, Room 2130 Washington, DC 20535
++-++ (202) 324-3000

b. Sample Screenshot 2: (Fake Mail Impersonating a Microsoft email ID)

From: security@microsoft.com Sent: Tue 2/22/2005 5:39 PM
To: mail@hackingspirits.com
Cc:
Subject: Alert! New Sober Worm!
Attachments:  patch_help-text.zip (51 KB) **Fake MS Patch containing Worm Payload**

ATTENTION!

Antivirus vendors are warning of a new variant of the "Sober" virus discovered today that can delete the hard disk.

Protection:
Download and read the zipped patch. It's very easy to install!

Thanks for your cooperation!

--- (c)2005 Microsoft Corporation. All rights reserved
--- Microsoft Corporation
--- One Microsoft Way
--- Redmond, Washington 98052-6399

- Attachment: No Virus found
- "HACKINGSPIRITS" Anti-Virus Service
- <http://www.hackingspirits.com> **Fake Virus Scan Result Appended**

Manual Removal Techniques

Here I shall discuss about manual techniques to remove this worm. Below given are the steps to remove the malicious file manually.

- a. The first step is always isolating the system by removing it from any network (e.g. dial-up, LAN, VPN or DSL etc) if connected.
- b. Disable system restore and reboot the system in safe mode (Since, in safe mode very minimal services runs preventing any unknown services to start during system startup).
- c. Go to Start => Run => Type "cmd.exe" and press "enter". Go to the "C:\>" prompt by typing cd\ and press "enter" in the command prompt.

Use the attrib command i.e. attrib /s "file name" (without quotes) to search for the following files:

Files to search-
datamx1.dat
datamx2.dat
datamx3.dat
goto1.dat
goto2.dat
goto3.dat
zippedso1.ber
zippedso2.ber
zippedso3.ber

Delete the above files once they are located in the system. After this go to "%WinDir%\msagent\" directory and look for the "Win32" folder and delete the entire folder including its contents.

- d. This worm makes entries in the registries to start on system boot. These entries can be removed from the following location:

HKEY_LOCAL_MACHINE => Software => Microsoft => Windows => CurrentVersion => Run
HKEY_CURRENT_USER => Software => Microsoft => Windows => CurrentVersion => Run

To remove the entries from the registries, go to Start => Run => Type "regedit" (without quotes) => press enter. Then go to the above mentioned keys and delete the key value "winsystem.sys" from both the registry locations.

- e. Purge recycle bin and restart window in normal mode. Connect to internet and update the Anti-Virus signature and once the signatures are up-to-date then do complete systems scan.

Reversing The Malicious Code

In this section I shall share few more technical details on the worm which I obtained after reverse engineering the payload. This section is meant mostly for malware and virus researchers but others can still read and understand it since, it is written in very simple language.

The attachment file is first saved on to the system's hard-disk and the attachment is extracted carefully to a test folder making sure it is not triggered accidentally. The payload is then opened using a debugger or dis-assembler like SoftIce, IDA Pro or OllyDbg. Here I have used OllyDbg for analysing the payload. Due to lack of time, I shall only give a brief overview of the findings.

Find below a step by step process of the analysis:

Step 1: Identifying the actual filetype

The file when viewed in normal windows mode seems to be .txt extension filetype but when viewed under DOS mode reveals the .pif extension which followed the space insertions after “.txt” extension. Refer the screenshot below.

```
C:\Test>dir
Volume in drive C has no label.
Volume Serial Number is 2C70-871C

Directory of C:\Test

02/26/2005  10:03 AM    <DIR>          .
02/26/2005  10:03 AM    <DIR>          ..
02/21/2005  06:00 AM           51,688 doc_data-text.txt
                .pif
02/26/2005  09:58 AM           51,918 sample.zip
                2 File(s)      103,606 bytes
                2 Dir(s)    2,215,063,552 bytes free

C:\Test>
```

The file called doc_data-text.txt has the .pif extension which appears after the .txt followed by lots of space insertion. The victim can't see the .pif extension since it is kept hidden by inserting lots of space inbetween .txt and .pif.

Step 2: Identifying the Win32 Binary

After opening it in the debugger it is found that the file is a Win32 executable developed using Visual Basic. The screenshot below displays the executable modules used by the worm. It is found that the worm has been developed using Visual Basic since, it uses a module called “MSVBVM60.DLL” and this module is used only by programs or applications developed using Visual Basic, without which the program won’t run.

Base	Size	Entry	Name	File version	Path
00400000	0002E000	0042C730	doc_data		C:\Test\doc_data-text.txt
73420000	00153000	73421AD8	MSUBUM60	6.00.9237	C:\WINDOWS\System32\MSUBUM60.DLL
77120000	00088000	77125541	OLEAUT32	3.50.5016.0	C:\WINDOWS\system32\OLEAUT32.dll
771B0000	00121000	771C0873	ole32	5.1.2600.1106	C:\WINDOWS\system32\ole32.dll
77C10000	00053000	77C1E94F	MSUCRT	7.0.2600.1106	C:\WINDOWS\system32\MSUCRT.DLL
77C70000	00040000		GDI32	5.1.2600.1106	C:\WINDOWS\system32\GDI32.dll
77D40000	0008C000	77D539F9	USER32	5.1.2600.1106	C:\WINDOWS\system32\USER32.dll
77DD0000	00080000	77DD103D	ADVAPI32	5.1.2600.1106	C:\WINDOWS\system32\ADVAPI32.dll
77E60000	000E6000	77E7AE60	kernel32	5.1.2600.1106	C:\WINDOWS\system32\kernel32.dll
77F50000	000A7000		ntdll	5.1.2600.1106	C:\WINDOWS\System32\ntdll.dll
78000000	00086000	78001E0F	RPCRT4	5.1.2600.1106	C:\WINDOWS\system32\RPCRT4.dll

MSVBVM60.DLL is used by those programs developed using VB

Step 3: Reversing

After analysing the assembly code, it is found that the code has undergone various transpositions and NOPs insertions. It seems the original binary is being packed using some sort of packers or obfuscators to prevent detection by the Anti-Viruses.

Refer the portion of the assembly code information below for details.

```
0042C730 $ 60 PUSHAD
0042C731 . BE 00104200 MOV ESI,doc_data.00421000
0042C736 . 8DBE 0000FEFF LEA EDI,DWORD PTR DS:[ESI+FFFE0000]
0042C73C . 57 PUSH EDI
0042C73D . 83CD FF OR EBP,FFFFFFFF
0042C740 . EB 10 JMP SHORT doc_data.0042C752
0042C742 90 NOP
0042C743 90 NOP
0042C744 90 NOP
0042C745 90 NOP
0042C746 90 NOP
0042C747 90 NOP
0042C748 > 8A06 MOV AL,BYTE PTR DS:[ESI]
0042C74A . 46 INC ESI
0042C74B . 8B07 MOV BYTE PTR DS:[EDI],AL
0042C74D . 47 INC EDI
0042C74E > 01DB ADD EBX,EBX
0042C750 . 75 07 JNZ SHORT doc_data.0042C759
0042C752 > 8B1E MOV EBX,DWORD PTR DS:[ESI]
0042C754 . 83EE FC SUB ESI,-4
0042C757 . 11DB ADC EBX,EBX
0042C759 > 72 ED JB SHORT doc_data.0042C748
0042C75B . B8 01000000 MOV EAX,1
0042C75D > 01DB ADD EBX,EBX
0042C75F . 75 07 JNZ SHORT doc_data.0042C76B
0042C761 . 8B1E MOV EBX,DWORD PTR DS:[ESI]
0042C763 . 83EE FC SUB ESI,-4
0042C765 . 11DB ADC EBX,EBX
0042C767 > 11C0 ADC EAX,EAX
0042C769 . 01DB ADD EBX,EBX
0042C76B . 73 EF JNB SHORT doc_data.0042C760
0042C76D . 75 09 JNZ SHORT doc_data.0042C77C
0042C76F . 8B1E MOV EBX,DWORD PTR DS:[ESI]
0042C771 . 83EE FC SUB ESI,-4
0042C773 . 11DB ADC EBX,EBX
0042C775 > 73 E4 JNB SHORT doc_data.0042C760
0042C777 > 31C9 XOR ECX,ECX
0042C779 . 83E8 03 SUB EAX,3
0042C77B . 72 0D JB SHORT doc_data.0042C790
0042C77D . C1E0 08 SHL EAX,8
0042C77F . 8A06 MOV AL,BYTE PTR DS:[ESI]
0042C781 . 46 INC ESI
0042C783 . 83F0 FF XOR EAX,FFFFFFFF
```

Conclusion

I have done several analyses on worms and malwares but never put the results on to paper but this time I thought of putting the analysis result on to the paper so that it can be used for educating various kinds of computer users. As most of my friends are network security experts but lack the knowledge of programming hence, I always make sure that I write articles as simple as possible so that all categories of computer users can understand it.

This worm seems to be a variant of Sober worm since it has many similarities with previous Sober worm variants. I have named it as "Fake FBI email worm" since it impersonates FBI email IDs as a sender ID while spreading. Due to lack of time I am not able to put all my findings on this "Fake FBI email" worm in this paper. To face such challenges against worms and malwares it is always advisable to keep the Anti-Virus up-to-date with signatures. Every computer user must understand the responsibility towards security and act against such techniques. Never open any attachments or execute any binaries received through emails unless you are sure of its authenticity. These days viruses and worms creators have started working on fuzzers to embed some sort of intelligence in the malicious codes which can evade various protections and infect systems. These days it is a big challenge for corporate and home computer users to prevent such malicious threats but in my opinion a user's responsibility towards security is always the last line of defense against such malicious attacks, it only depends how responsible are they to deal with such threats.

About Author

I am very ignorant and lazy when someone asks me about me. I believe, it hardly matters what am I but infact it really keep importance on what I share with the world.

Just to be brief, I was one time malicious program coder but these days researching on various techniques that can be used by malicious programmers to evade any Anti-Virus products. I spend most of my time on vulnerability research and analysing malwares and worms.

To know more about me visit: www.hackingspirits.com.

Mail me your comments @ debasis@hackingspirits.com or debasis_mty@yahoo.com .
