# Fake FBI email Worm Exposed

24<sup>th</sup> Feb, 2005

Debasis Mohanty (a.k.a Tr0y)

www.hackingspirits.com debasis@hackingspirits.com

# Table of Contents

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

#### 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)

```
Officer@fbi.gov ______Fake FBI email ID
From:
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)



## 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:

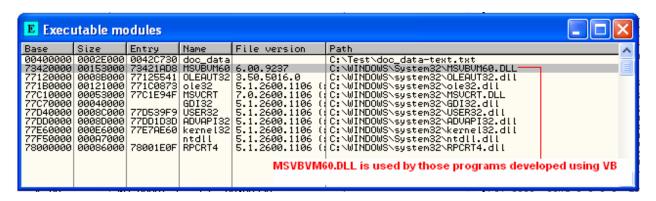
## **Step 1: Identifying the actual filetype**

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

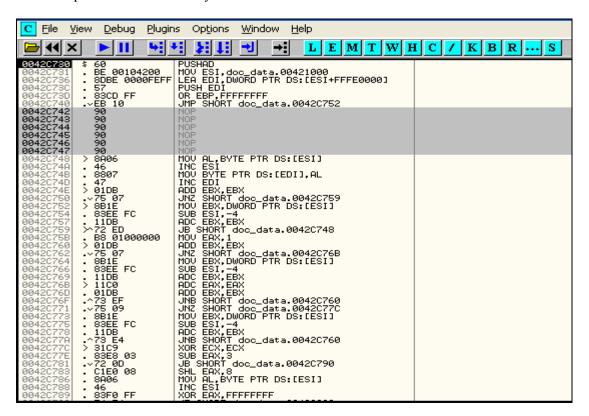
After opening it in the debugger it is found that the file is a Win32 executable developed using Visual Basic. The screenshot below displays the executable modules used by the worm. It is found that the worm has been developed using Visual Basic since, it uses a module called "MSVBVM60.DLL" and this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



#### **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.



#### 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.