# Analysis of

# 4141842e30edaf429309ea6bc2374ef5 / Attack.m.exe

**SyrianMalware.com - @SyrianMalware**

# Introduction

As the conflict in Syria moves into its third year, malware targeting the opposition and its supporters continues to be an ongoing concern for security researchers and human rights supporters. This report details what is perhaps the first such malware found in 2014.

## Sample Background

An activist who provides digital security assistance to the Syrian opposition sent the sample detailed in this report to SyrianMalware.com in early February. Another Syrian activist noticed the malicious process running in their Task Manager. However, the victim is unsure where it came from originally. This was the extent of the background provided about the sample. Although the sample was titled *Attack.m.exe* (MD5: 4141842e30edaf429309ea6bc2374ef5) when we received it, it is unknown if this was the original process name on the victim's computer.

```
$ file Attack.m.exe
Attack.m.exe: PE32 executable (GUI) Intel 80386 Mono/.Net assembly,
for MS Windows

$ md5sum Attack.m.exe
4141842e30edaf429309ea6bc2374ef5  Attack.m.exe
```

# Static Analysis

## Interesting Strings

A look at the strings contained within *Attack.m.exe* gives some indication of the program's functionality and software dependencies:

```
Microsoft.VisualBasic
Ya Houssen.exe
C:\Users\Syrian Malware\AppData\Local\Temporary Projects\Ya
Houssen\obj\x86\Debug\Ya Houssen.pdb
GetWindowText
get_FullName
get_Network
get_MachineName
get_UserName
get_Info
get_OSFullName
get_OSVersion
get_ServicePack
GetWindowText
GetForegroundWindow
v2.0.50727
```

The strings, which are prefixed with `get_` and `Get`, indicate that the application will likely exfiltrate information about the user, computer, and system activity. `v2.0.50727` refers to the .NET framework version required by the malware.

### Ya Houssen

It is interesting to note the presence of 'Ya Houssen' in the application's strings. Ya Houssen is an approximate transliteration of يا حسين a term used by Shia Muslims to evoke the name of Husayn ibn Ali ibn Abi Talib (الحسين بن علي بن أبي طالب). Husayn ibn Ali was a seventh-century Imam and highly-regarded figure in Shia Islam who represents sacrifice in the name of God. This is relevant in the context of the Syrian civil war, as the regime and opposition are largely divided along sectarian lines. Overall, armed support for the Syrian regime comes from Shia-aligned groups such as Hezbollah or the Iranian government. It is worth noting that Bashar al-Assad's own sect of Islam, Alawite, is an offshoot of Shi'ite Islam.

## VirusTotal

Submitting the malware to VirusTotal's scanner resulted in a detection ratio of 0/49. [The results of this scan are available here.]

# Dynamic Analysis

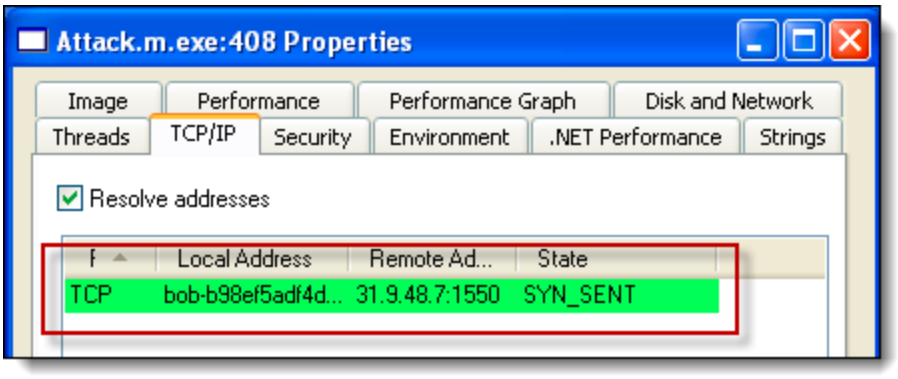
Our analysis was completed using a 32-bit Windows XP Service Pack 3 Virtual Machine.

## Disk Activity

We did not observe any indication that this sample attempts to write files onto the hard drive.

## Network Activity

Upon launching the sample, it immediately makes an outbound connection to 31.9.48.7 over TCP on port 1550. This initial network traffic is a "heartbeat," consisting of repeated SYN packets to the command-and-control (C&C) server. The server replies with a RST, ACK packet in response.




We can quickly ascertain that the destination IP address is located in Syria. Interestingly, this IP address is in the same */24* network segment as a C&C server used in December 2013, detailed in the report *Quantum of Surveillance*.

```
$ whois 31.9.48.7
inetnum:        31.9.0.0 - 31.9.127.255
netname:        SY-ISP-TARASSUL
descr:          Tarassul inetnet Service Provider
country:        SY
address:        Syrian Telecommunication Est
```

### Data Exfiltration

In time, the malware will begin exfiltrating information about the user's computer and currently opened applications (our test environment was configured with a username of *Bob* and an IP address of *192.168.0.11*):

```
192.168.0.11    31.9.48.7    TCP    185    1342 > 1880
!0/j|n\Syrian Malware
Team/j|n\BOB-B98EF5ADF4D/j|n\Bob/j|n\USA/j|n\Win XP ProfessionalSP3
x86/j|n\Yes/j|n\0.1/j|n\/j|n\/j|n\[endof]
```

```
192.168.0.11    31.9.48.7    TCP    250    1338 > 1550
!0/j|n\Ya Houssen/j|n\BOB-B98EF5ADF4D/j|n\Bob/j|n\USA/j|n\Win XP
ProfessionalSP3 x86/j|n\No/j|n\0.1/j|n\/j|n\Process Explorer -
Sysinternals: www.sysinternals.com
[BOB-B98EF5ADF4D\Bob]/j|n\[endof]
```

### File Downloading

The malware also has the ability to download additional binaries, as we observed roughly six minutes after execution:

```
31.9.48.7    192.168.0.11    TCP    1454    1550 > 1338:
RFP/j|n\MZ??????????????????????@????????????????????????????????
?????????????!??L?!This program cannot be run in DOS
mode.???$???????[??
...lines omitted…
```

By exporting the binary data out of the TCP stream using Wireshark, we were able to analyze the newly dropped file, revealing that it is a WinRAR SelF eXtracting (SFX) Archive. The file has a MD5 hash of a9e6f5d4c5996ff1a067d4c5f9ade821. (Available for further analysis at [http://syrianmalware.com](http://syrianmalware.com))

```
$ file dropped_file.rar
dropped_file.rar: PE32 executable (GUI) Intel 80386, for MS
Windows, RAR self-extracting archive

$ md5sum dropped_file.rar
a9e6f5d4c5996ff1a067d4c5f9ade821 *dropped_file.rar
```

Executing the new malicious binary results in the following files being written, including a *.lnk* file in the user's *Startup* folder to achieve persistence:

```
C:\Documents and Settings\Bob\Local Settings\Temp\system23.txt
C:\Documents and Settings\Bob\Local Settings\Temp\s.m.txt
C:\Documents and Settings\Bob\Local Settings\Temp\Skype.exe
C:\Documents and Settings\Bob\Local Settings\Temp\8cdf_appcompat.txt
C:\Documents and Settings\Bob\Local Settings\Temp\b8d3_appcompat.txt
```

```
C:\Documents and Settings\Bob\Start Menu\Programs\Startup\.Skype.exe.lnk
```

### DarkComet RAT Indicators

Two strings stood out in the malicious network traffic:

```
192.168.0.11    31.9.48.7    TCP    76    1339 > 4443:
D573BA5A4EFFC3FB629308

31.9.48.7    192.168.0.11    TCP    66    4443 > 1339
BF7CAB464EFB
```

An online search reveals these two strings are associated with DarkComet, a Remote Access Trojan (RAT) used extensively in the Syrian civil war. Specifically, these strings are used to “phone home” to the attacker’s DarkComet administrative console. We believe the presence of these strings positively indicates the malware as a DarkComet variant.

# Actors

## Syrian Malware Team

A string that immediately stands out in the malware's network traffic is `Syrian Malware Team`. An online search of this term leads to multiple sources that appear to be associated with the group.

### Facebook

The following page appears to be the group's official Facebook presence:

| https://www.facebook.com/malwareteam.gov.org.sy |
|---|

The page displays support for the Syrian regime and its allies, such as Hezbollah, Hassan Nasrallah, and Iran:


The following Facebook profiles appear to belong to individual members of Syrian Malware Team:

https://www.facebook.com/syrian.malware1
https://www.facebook.com/syrian.wolverine
https://www.facebook.com/syrian.hawks.9
https://www.facebook.com/syrian.wolf.1023
https://www.facebook.com/syrian.lion.1610

It seems that members of Syrian Malware Team even use Facebook to discuss their latest malware variants:


The highlighted link, available here, leads to VirusTotal results for one of the files observed in our target environment, `Skype.exe`. (MD5: 15d4140e9e6f88f9dbcc48a437562da2)

The group also uses Facebook to advertise their latest hacks of pro-opposition websites. In the following screenshot, they have successfully defaced Qalamoun Media Center, a pro-opposition media outlet:


### YouTube

There are also several YouTube videos associated with this group, uploaded by user "SyrianArmy2012":

https://www.youtube.com/watch?v=GX0xewps3BE
https://www.youtube.com/watch?v=SroHfTGHg_g
https://www.youtube.com/watch?v=AhzMehR6aRk

### SyriaTube

Other videos created by Syrian Malware Team can also be found on SyriaTube.net, a website that creates and distributes pro-regime propaganda. Videos by Syrian Malware Team are recordings of opposition members' computers that have been infected by malware. In each one, the victims are recorded in sexually explicit online conversations. Based on these videos, it seems that one of the primary goals of Syrian Malware Team's infection campaigns is to document members of the opposition in embarrassing and discrediting situations. An example of one of these videos is linked below, although there are several more (contains sexual content).

فضيحة جنسية : ابو الحسن احد اركان قيادة المجلس العسكري للجيش الحر في اللاذقية (translation: Sex Scandal: Abu Hassan, one of the leaders of the Free Syrian Army in Latakia)

# Resources


1. *Ya hussain*. (2013, January 09). Retrieved from http://en.wikipedia.org/wiki/Ya_Hussain
2. Galperin, E., Marquis - Boire, M. & Scott - Railton, J. (2013, December 28). Quantum of surveillance: Familiar actors and possible false flags in Syrian malware campaigns. Retrieved from https://www.eff.org/document/quantum-surveillance-familiar-actors-and-possible-false-flags-syrian-malware-campaigns