Bryce Montano

Project 2.5

## Phase I

To begin the assignment, we were given a hint that the malware would reveal itself on a certain date within April. Therefore, I ran the following command:

python utils/submit.py --clock "04-01-2016 13:39:56" --timeout 600 ../Phase2/TriggerMeTimbers.exe

And continued running the same command with the exception of the date (incrementing by one each time) until I found that on on **April 5th, 2016**, the Malware is triggered.

In the report, a file is dropped by the name of **C:\possible\_names\_rot13.txt**. The contents of the file were:

jvaqrsraqre.rkr gnfxzba.rkr oybbqerq.rkr inovna.iof Bhgybbx.rkr Zrffntr.rkr YBIR\_YRGGRE\_SBE\_LBH.rkr Qbphzragf.rkr Zvpebfbsg\_Hcqngr.rkr jva-sverjnyy.rkr nqborsynfu.rkr qrfxgbc.rkr wnin.rkr

Googling ‘Rot13’, I found that ROT13 is a substitution encryption scheme. I found a Rot13 decryption tool online here: <http://www.decode.org/> and entered the contents of the file:

Which yielded the following:

windefender.exe taskmon.exe bloodred.exe vabian.vbs Outlook.exe Message.exe LOVE\_LETTER\_FOR\_YOU.exe Documents.exe Microsoft\_Update.exe win-firewall.exe adobeflash.exe desktop.exe java.exe

Unfortunately, this did not provide me the information I needed. However, upon reviewing the ‘Strings’ section of the report, I found:

C:\possible\_names\_rot13.txt

639bae9ac6b3e1a84cebb7b403297b79

7b63d1cafe15e5edab88a8e81de794b5

9e925e9341b490bfd3b4c4ca3b0c1ef2

c8d46d341bea4fd5bff866a65ff8aea9

C:\decode\_these\_hashes.txt

With the first line obviously being the name of the possible\_names and underneath that, a list of hashes and another file (which I was unable to find in the specified location in the VM). I copied the hashes and entered them into an MD5 hash converter tool: <http://md5.gromweb.com/>

Which yielded the following message:

639bae9ac6b3e1a84cebb7b403297b79 = you

7b63d1cafe15e5edab88a8e81de794b5 = won

9e925e9341b490bfd3b4c4ca3b0c1ef2 = this

c8d46d341bea4fd5bff866a65ff8aea9= game