Part I:

The malware is triggered on April 25, 2016.

It then drops a file called “possible_names.txt”.
The contents of this file are possible trigger file names encrypted using ROT13 (a very common method of encryption used by malware).
These filenames are all real malware file names (except for the trigger name).

Contents of “possible_names.txt”:

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

Decrypted contents of “possible_names.txt”:

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

The trigger filename is “Outlook.exe”

Once the malware has the proper filename, it then drops a file called “crack-me.txt”
This is a list of 4 MD5 hashes that the student has to crack.

Since MD5 has been broken, it's pretty easy to find an online MD5 cracker to crack each hash (e.g., http://md5cracker.org/)

Contents of "crack-me.txt":

639bae9ac6b3e1a84cebb7b403297b79
7b63d1cafe15e5edab88a8e81de794b5
8fc42c6ddf9966db3b09e84365034357
c8d46d341bea4fd5bff866a65ff8aea9

Cracking the 4 MD5 hashes reveals the 3 strings "you", "won", "the", "game".

Online form submission solutions:

String 1: you
String 2: won
String 3: the
String 4: game

Part II:

There are three different malware base source codes used to construct the 8 malware samples (malware1, malware2, malware3, malware4, malware8, malware9, malware11, TriggerMeTimbers).
One is a VBS worm, another is a Point-of-Sale (POS) malware, and the last is another POS malware.

The students are tasked with simply categorizing each sample they ran in Phases I/II plus this bonus malware.

Online form submission solutions:

Note: The categories should be unnamed. Using the labels category1, category2, and category3 is good enough. So students can group the malware under whatever category label they would like, so long as the **same malware** is grouped together.

Category 1 (VBS worm) : malware2
Category 2 (Dexter POS) : malware1, malware3 (uses a vbs script to do sneaky things but is still Dexter at its core), malware4, malware8
Category 3 (Alina POS) : malware9, malware11, TriggerMeTimbers