## Lab_05-1

1. It saves a file from its resource section to “C:\Program Files\Google\Update\GoogleUpdate.exe”
2. By replacing GoogleUpdate.exe, the malware will be run every time a google update is run. This is a good signature because the expected contents of GoogleUpdate.exe are known and can be verified
3. It uses the mutex “WODUDE”
4. It replaces a known trusted file, which makes it hard to find without specifically looking for it. It also hides the console window
5. It uses SetWindowsHookExW to enable a callback on keypress and SetWinEventHook to enable a callback on window focus change
6. SetWindowsHookExW gets WH_KEYBOARD_LL. SetWinEventHook gets EVENT_SYSTEM_FOREGROUND, and apparently the value 2 is WINEVENT_SKIPOWNPROCESS|WINEVENT_OUTOFCONTEXT according to the answer key but I cannot find the values of those constants to know what their bitwise OR would be
7. It writes to a file in the current directory, whose name is the computer’s hostname

## Lab_05-2

1. It downloads a file from [http://malcode.rpis.ec/update_defender](http://malcode.rpis.ec/update_defender) and uses it to override “C:\Program Files\Mozilla Maintenance Service\maintenanceservice.exe”
2. It overrides a known and trusted file. This file can be verified as a signature
3. The 2nd mutex is needed to make sure only one enumeration of child windows is done at a time. This prevents issues from arising with multiple windows of a given program
4. It sends a message to a specified window and blocks until the message is processed
5. The messages are:
   a. 0xd2 is EM_GETPASSWORDCHAR which gets the character shown when user is typing a password
   b. 0xcc is EM_SETPASSWORDCHAR which sets the character shown when user is typing a password
   c. 0xc4 is EM_GETLINE which copies a line from an edit control into a buffer
6. It looks for a password box in the focused window using getpasswordchar, removes the mask with setpassword char, then copies the text before resetting the password character. It therefore steals the contents of password fields instead of logging keys like malware 1
7. It writes the data to a file in the current directory whose name is the hostname