**CSS 579: Malware Reverse Engineering**

**Team Malware Project**

**Malware Details**

*Binary*: winword64.exe

*Source Code*: winword64.cpp

*Type*: Ransomware

*Overview*: Winword64.exe is a Windows ransomware malware that encrypts files in the SYSTEMDRIVE:\Users directory with particular extensions targeting common image, video, audio, and document files.

*Techniques Implemented*:

1. All strings within the program are encoded in a reverse Hex encoding to obfuscate the strings during static analysis.
2. The program begins by performing an analysis check to determine if it is being debugged or running in a VM. If the analysis check is true, then the program exits.
3. The program then decodes all of its strings into real, readable, strings.
4. The program processes command line arguments to determine its execution mode (encrypt, or decrypt with a key).
5. If Encrypting:
   * Uses the SHGetKnownFolderPath() API to find the User Profiles directory (c:\users on Windows 10, c:\documents and settings on Windows XP and older)
   * Searches the full Users directory for 21 file extensions targeting common image, video, audio, and document files.
   * Foreach file found:
     + Uses the CreateFileW() API to get a handle to the file, and a handle to a new file for storing the encrypted version.
     + Uses the APIs CryptAcquireContextW(), CryptCreateHash(), CryptHashData(), CryptDeriveKey(), ReadFile(), CryptEncrypt(), WriteFile(), CryptReleaseContext(), CryptDestroyKey(), and CryptDestroyHash() to create an encrypted version of each file.
     + All encrypted files are named using the original filename with a .encrypted file extension. For example, Image10.png would become Image10.png.encrypted.
   * The program sets persistence by writing data to the Registry into these Keys using the APIs x, y, and z:
     + X
     + Y
     + Z
   * The program sends a beacon message to report that an infection has completed. The beacon message includes the machine IP, machine name, current username, date/time, and number of files encrypted. The networking APIs used for the beacon message are x, y, and z.
   * Finally, the program displays a ransom message to the user.
6. If Decrypting:
   * The program removes the persistence values from the Registry by deleting these values using the APIs x, y, and z:
     + X
     + Y
     + z
   * Searches the full Users directory for all file with.encrypted extensions.
   * Foreach file found:
     + Uses the CreateFileW() API to get a handle to the encrypted file, and a handle to a new file for storing the decrypted version.
     + Uses the APIs CryptAcquireContextW(), CryptCreateHash(), CryptHashData(), CryptDeriveKey(), ReadFile(), CryptDecrypt(), WriteFile(), CryptReleaseContext(), CryptDestroyKey(), and CryptDestroyHash() to create a decrypted version of each file to restore the original file.
   * Finally, the program displays a message to the user letting them know that their files have been restored.