**Hoja de Trabajo 2 – Security Data Science**

1. Entre los ejemplos el ejecutable contine muchas más llamadas al API, que se enfocan más en llamadas al kernel. Mientras que el primero tiene un DLL que hace una llamada para poder escribir directamente sobre el disco duro. Si es sospechoso que el ejecutable este haciendo muchas llamadas al kernel y el otro este escribiendo directamente en el disco duro.
2. UPX es una manera de comprimir archivos y las personas que escriben malware lo utilizan para que los antivirus no los detecten tan fácil.
3. Este se puede clasificar en:
   1. Search Files to Infect
   2. Copy/Delete Files
   3. Read/Write Files

Gráfico, Gráfico de líneas

Descripción generada automáticamente

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

1. Esta librería provee acceso avanzado que es parte del kernel. Este es responsable de reiniciar o apagar la máquina.
2. El CryptReleaseContext es el que maneja los servicios de criptografía y la llave con la que se trabaja.
3. Con estas pruebas, este archivo es sospechoso y lo que puede hacer es que encripte la maquina y saque al usuario de la maquina al momento de ejecutarse.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Correo electrónico

Descripción generada automáticamente

Como se puede observar el Hash generado es el mismo al que se generó. El nombre del file es un owo\_im\_not\_ransomware\_xd.exe. El propósito del malware es entrar como un troyano y luego obtener las llaves del sistema y borrar grandes volúmenes de información.

1. Queda claro que las sospechas del punto 7 fueron confirmadas con el analizador.