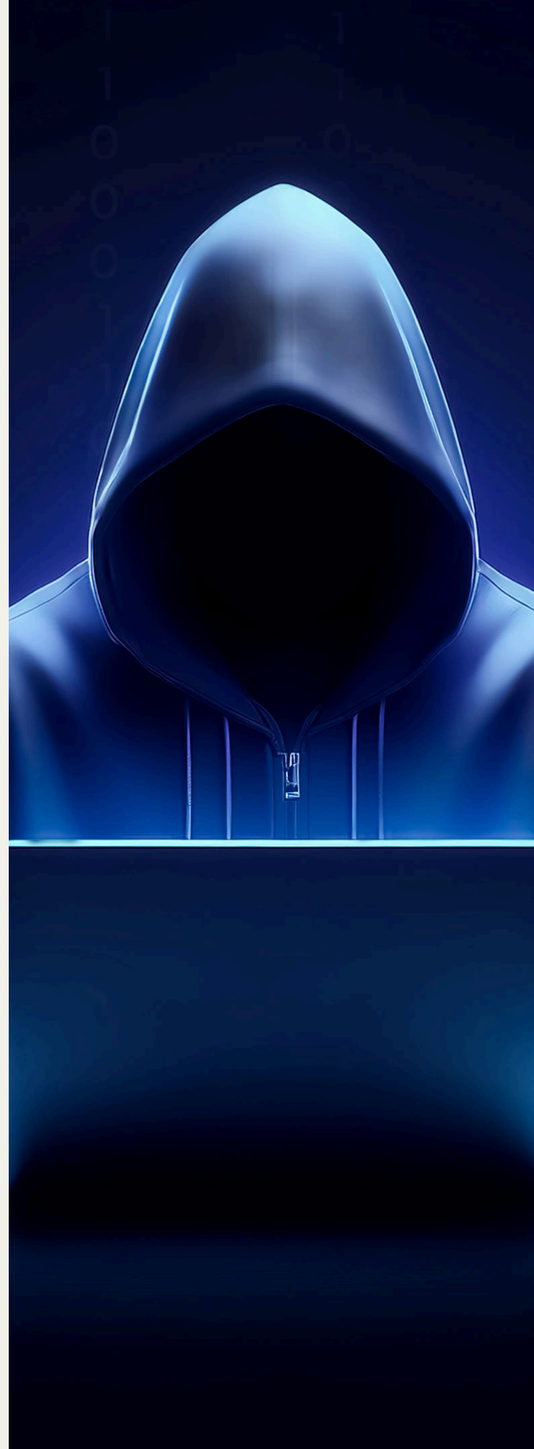
Instituto Tecnológico de Santo Domingo

Presentación Final

Ransom:\\Win64\\CryptoLocker.v1
doggie.exe



Harold Marzán
ICS202L-01 Laboratorio de Algoritmos Maliciosos

María F. Hamilton R. - 1117462

Objetivo del malware

Su objetivo es encriptar los archivos del directorio en el que se ejecute el malware y forzar al usuario a que pagué para poder desencriptar sus archivos.
En caso de que el usuario decida no pagar, ocurría un BSOD y perderá los archivos encriptados.

Encriptación

Fernet encryption

El código utiliza ***Fernet encryption***, que es parte de la biblioteca cryptography. Fernet es una implementación de encriptación simétrica basada en AES (Advanced Encryption Standard) con una longitud de clave de 128 bits.

Beneficios de Fernet encryption

Fernet abstrae datos complicados del cifrado y con unas pocas líneas de código se puede encriptar y desencriptar. Fernet puede trabajar con cualquier tipo de dato, ya sea texto (codificado en UTF-8) o datos binarios, como imágenes o documentos.

Tecnologías y Librerías Utilizadas

Python 3.13.1 64-bit

VMware Workstation Pro

01

cryptography.fernet

- Proporciona herramientas para el cifrado y descifrado simétrico utilizando AES en modo CBC con autenticación HMAC.

02

os

- Proporciona herramientas para interactuar con el sistema operativo.

03

tkinter

- Módulo estándar de Python para construir interfaces gráficas de usuario (GUIs).

Tecnologías y Librería Utilizadas

Python 3.13.1 64-bit

VMware Workstation Pro

04

ctypes - windll

- Permite llamar funciones de bibliotecas dinámicas (DLLs) de Windows.

05

ctypes - c_int, c_uint, c_ulong

- Representan tipos de datos básicos de C (int, unsigned int, unsigned long) en Python y sirven para interactuar con bibliotecas de C del sistema que requieren estos tipos de datos.

06

ctypes, POINTER, byref

- POINTER: Define punteros hacia tipos de datos en C.
- BYREF: Pasa referencias (punteros) de variables en lugar de sus valores.

Tecnologías y Librería Utilizadas

Python 3.13.1 64-bit

VMware Workstation Pro

07

pylint

- Herramienta de análisis estático para Python que detecta errores en el código, identifica problemas de estilo y ofrece recomendaciones para mejorar la calidad y seguridad.

08

uncompyle6

- Herramienta para descompilar archivos .pyc y recuperar el código fuente original de Python.

09

pdb

- Usado para análisis dinámico es un depurador que permite pausar, inspeccionar scripts línea por línea.

Funciones Utilizadas

01

generate_key()

Genera una clave de cifrado segura para usar con el algoritmo de cifrado simétrico.

02

encrypt(data)

Encripta los datos pasados como parámetro utilizando la clave generada.

03

decrypt(data)

Desencripta los datos encriptados utilizando la clave generada.

Funciones Utilizadas

04

windll.ntdll.RtlAdjustPrivilege()

Ajusta los privilegios del proceso actual. Se utiliza aquí para otorgar privilegios que permitan provocar un BSOD (pantalla azul de la muerte).

05

windll.ntdll.NtRaiseHardError()

Provoca un error grave en el sistema, generalmente un BSOD.

06

remove_files_with_extensions(directory, extensions):

Elimina archivos con las extensiones especificadas en un directorio y sus subdirectorios.

Demostración

doggie.exe