IDS202 - Algoritmos maliciosos

Docente: Harold Lawrence Marzan Mercado

Práctica/Asignación: Informe

Nombres: Samuel Junior Matheo

Apellidos: Charles Saint-Jean

Matrícula/ID: 1098628

Sección: 01

Fecha: 23/07/2022

Table of Contents

Introduccion

En el siguiente informe vamos a hablar de distintos aspectos concernientes a los ransomware. Se tocarán temas como el origen de estos, las variantes que existen, la anatomía del ataque de un ransomware y como estos programas maliciosos te infectan el dispositivo.

Marco teórico

Concepto

es un tipo de programa maligno que impide a los usuarios acceder a su sistema o a sus archivos personales y que exige el pago de un rescate para poder acceder de nuevo a ellos.

Origen

Troyano AIDS creado en 1989 por Joseph Popp. Popp envió 20 000 disquetes infectados con el texto "AIDS Information—Introductory Diskettes" (Información sobre sida: disquetes de introducción) a los asistentes a la conferencia internacional sobre sida de la OMS y llevó a cabo lo que ahora se considera el primer ataque de ransomware de la historia.

Tipos de ransomware

Crypto ransomware: Los ciberdelincuentes cifran los archivos de un ordenador de manera que a los usuarios les resulta imposible acceder a ellos.

Locker ransomware: Se trata de un programa maligno que impide a la víctima acceder al ordenador hasta que paga un rescate.

Scareware: Es un tipo de programa maligno diseñado para hacer creer a las víctimas que sus ordenadores se han infectado con ransomware y conseguir que paguen un rescate al atacante. Aunque técnicamente el scareware no es un tipo de ransomware, tiene el mismo efecto en las víctimas

Anatomía de un ataque ransomware

1. Distribución

Los atacantes engañan a los usuarios para que accedan a software malicioso mediante mensajes de correo que emplean el phishing, o mediante ingeniería social, sitios web falsos con enlaces maliciosos o dispositivos de almacenamiento externo (como una unidad USB) infectados.

2. Infección

A continuación, el usuario descarga sin saberlo un archivo ejecutable llamado "cargador" (o "descargador") que instala el ransomware.

3. Ejecución

La carga de ransomware que se ha copiado desde el archivo se oculta y se integra en el sistema.

4. Análisis y cifrado

Posteriormente, el programa maligno analiza el sistema y la red, y cifra los archivos.

5. Nota de rescate
Por último, se le muestra a la víctima una nota en la que se le solicita el pago por desbloquear los archivos.

Desarrollo

Metodología

Para realizar mi algoritmo malicioso lo primero que se realizó fue identificar el ambiente para el cual va a estar dirigido mi programa maligno. Para esta ocasión decidí optar por Windows 10. El lenguaje de programación empleado para el desarrollo de mi virus es Python 3.10.5 en conjunto con librerías que me ayudarán el proceso de encriptado como envío de información.

A continuación, una lista de las librerías de Python utilizadas para el desarrollo de mi malware:

- os: manipular archivos dentro de la máquina.
- random: generar número aleatorio.
- hashlib: crear un codigo hash para mi llave simétrica.
- Cryptodome: utilizado para encriptar mis archivos y mi llave simétrica.
- MIMEBase: utilizado para consumir la API de Gmail y poder enviar correos.
- MIMEMultipart: utilizado para consumir la API de Gmail y poder enviar correos.
- SMTP: utilizado para enviar y dar formato a la estructura del correo a enviar.
- Socket: usado para obtener el nombre y la dirección IP de la máquina.

Con todas las librerías a utilizar ya definidas pues simplemente fue cuestión de desarrollar 3 funciones principales para que mi algoritmo malicioso funcionara. Una función para encriptar mi llave, otra función para encriptar archivos y por último una función que recorre los directorios para traer los archivos a ser encriptados.

Proceso de encriptado

El método de encriptación empleado es bit a bit en bloques de 32 bits haciendo uso del algoritmo sha512 pues sustituyo la información original del archivo y directamente se encriptan. Una vez este proceso realizado, es necesario que el usuario tenga un archivo con la llave para poder desencriptar sus archivos.

Una vez se le proporciona este archivo al usuario, posterior a completarse la transacción, pues el programa abre la consola y presenta una entrada en la cual el usuario debe pegar la llave para poder desencriptar los archviso encripatados.

Conclusion

En primeras instancias, estos programas se crean con propósitos malignos los cuales tienen como objetivo perjudicar. Sin embargo, tras investigar e interactuar con estos se puede llegar a sacar un gran provecho en cuanto a conocimiento y adquisición de información con fines educativos. Existen muchas maneras de