Proyecto Final

“Reporte de Práctica”

Universidad: Instituto ARTEK

Integrantes:

Diego Ramírez Gutiérrez

Yael Trujillo Díaz

Rodrigo Núñez Cárdenas

Daniel Bustamante Lagartt

Asesor: César Antonio Ríos Olivares

Fecha de Elaboración: Lunes 19 de junio de 2023

Resumen

En este reporte de práctica examinamos el impacto de las amenazas cibernéticas en la seguridad digital, centrándonos específicamente en el spam, el phishing y el spyware. Mediante una práctica simulada, desarrollamos una muestra intencional de prácticas maliciosas. Nuestros hallazgos revelan la alarmante facilidad para engañar a un cibernauta promedio, y su impacto en la integridad de los datos. Discutimos algunas estrategias y mejores prácticas para prevenir y mitigar el spam, identificar y evitar el phishing, y protegerse del spyware. Además, exploramos las implicaciones éticas asociadas con estas amenazas y la importancia de la concienciación y la educación en la seguridad cibernética.

***Palabras clave**: Amenazas cibernéticas; Seguridad digital; Spam; Phishing; Spyware; Práctica simulada; Prácticas maliciosas; Engaño; Integridad de los datos; Prevención y mitigación; Implicaciones éticas; Concienciación en seguridad cibernética; Educación en seguridad cibernética*

Abstract

In this practice report, we examine the impact of cyber threats on digital security, specifically focusing on spam, phishing, and spyware. Through a simulated practice, we develop an intentional sample of malicious practices. Our findings reveal the alarming ease of deceiving an average internet user and its impact on data integrity. We discuss strategies and best practices to prevent and mitigate spam, identify and avoid phishing, and protect against spyware. Additionally, we explore the ethical implications associated with these threats and the importance of awareness and education in cybersecurity.

***Keywords**: Cyber threats; Digital security; Spam; Phishing; Spyware; Simulated practice; Malicious practices; Deception; Data integrity; Prevention and mitigation; Ethical implications; Cybersecurity awareness; Cybersecurity education*

Introducción

En este informe, exploraremos el impacto de las amenazas cibernéticas en la seguridad digital, centrándonos específicamente en el spam, el phishing y el spyware. Estas amenazas representan desafíos significativos en el entorno digital actual y pueden comprometer la integridad de los datos y la privacidad de los usuarios. A medida que la tecnología avanza, los ciberdelincuentes han encontrado formas cada vez más sofisticadas de llevar a cabo estas actividades maliciosas.

El spam se refiere a cualquier forma de comunicación no solicitada que se envía de manera masiva, como correos electrónicos no deseados, mensajes de texto o publicaciones en redes sociales. Por otro lado, el phishing implica la manipulación de los usuarios para obtener información confidencial, como contraseñas o datos bancarios, a través de técnicas de ingeniería social. Por último, el spyware es un tipo de software malicioso diseñado para recopilar información personal sin el conocimiento ni el consentimiento de los usuarios.

Analizaremos cómo estas amenazas afectan la seguridad digital y exploraremos estrategias para prevenirlas y mitigar sus impactos. También examinaremos las implicaciones éticas asociadas con estas amenazas y destacaremos la importancia de la concienciación y la educación en la seguridad cibernética. Mediante el estudio de estos temas, buscamos proporcionar una visión integral de los desafíos actuales en el ámbito de la seguridad digital y promover mejores prácticas para proteger la información y salvaguardar la privacidad contra el robo de datos, la intrusión cibernética y el malware.

Planteamiento del problema

Como miembros de un área especializada en ciberseguridad tendremos como objetivo realizar dos códigos uno que nos permita detectar spam y en su contraparte enviar spam siendo este último indetectable para el servicio de mensajería gmail.

Para esto entender que es el spam y como gmail lo detecta será indispensable para el entendimiento del proyecto.

¿Qué es spam?

Es cualquier forma de comunicación no solicitada que se envía de forma masiva (correo electrónico masivo no solicitado). Su forma más frecuente es un correo electrónico de publicidad enviado a un gran número de direcciones (correo electrónico de publicidad no solicitado), pero el "spamming" también existe a través de mensajes instantáneos, de texto (SMS), redes sociales o incluso mensajes de voz. Enviar spam es ilegal en la mayoría de las jurisdicciones.

Hay diferentes estimaciones, pero hay quienes sugieren que cada día se envían más de 100 mil millones de mensajes de spam, lo que representaría hasta un 85 por ciento del tráfico diario de correo electrónico a nivel mundial.

Gmail clasifica como Spam todo correo electrónico que no esté verificado, ya sea porque el servidor SMTP no lo reconoce o no se haya introducido usuario o contraseña que autentique la identidad del mismo.

No todos los intentos tienen por qué ser con intenciones maliciosas: puede ser que la parte de datos que lleva la autenticación se haya perdido durante el envío y/o recepción.

¿Cómo detectar que un correo es spam?

- El dominio de la dirección de email no coincide con el de la empresa/entidad.
- Faltas de ortografía o de concordancia.
- El correo solicita información personal.
- El asunto del correo es de máxima alerta.
- Generalmente se incluyen archivos adjuntos.

¿Por qué los correos se van a spam?

Algunas de las razones por la que correos deseados van a spam son: Que el asunto es engañoso o que tiene un filtro que detecta spam como listas negras, donde están guardadas direcciones IPs que generan spam, o firewalls, sistemas que están hechos para bloquear el acceso no autorizado.

- Que el correo lo ha enviado una empresa y en él no venga un enlace para cancelar la suscripción a la lista de distribución.
- Que no se pueda configurar la autenticación del propio correo electrónico, que se encarga de permitir que los mails se envíen.
- Que el correo tenga muchas imágenes y esto es un filtro de spam porque suele ser un indicativo de que es un mail basura.

En esencia al ser el correo electrónico el principal medio de distribución de ataques como phishing, malware, virus y ransomware es necesario que el área de seguridad se encargue de tomar las acciones pertinentes para reducir al mínimo los riesgos que esto representa.

Aquellos consumidores que hacen clic en los vínculos de estos mensajes de texto spam descargan malware en sus dispositivos o son guiados a sitios web maliciosos. En algunos casos, los usuarios responden a los mensajes de texto, lo cual le permite al remitente saber que el número está en uso y es vulnerable.

Hay una gran variedad de herramientas para bloquear spam que pueden mejorar la forma en que los usuarios enfrentan el tema. Sin embargo, sin importar qué tan eficaz sea la tecnología de bloqueo de spam, los usuarios finales siempre tendrán que estar atentos a la posibilidad de recibir mensajes maliciosos, ya que ninguna herramienta es perfecta y los spammers están siempre inventando nuevas formas de enviar mensajes no deseados.

Resultados

Generar SPAM

```
import yagmail
email='g.cardenasartekedu@gmail.com'
contraseña ='sdbtvmolfafuiapw'
yag=yagmail.SMTP(user=email, password=contraseña)
destinatarios=['fusilmk42@gmail.com','monkeydonobiz@gmail.com']
asunto='Test de spam'
mensaje="<p>Estimados estudiantes, </p><p></p><p>Espero que se encuentren bien. Me dirijo a ustedes para informarles sobre la nueva actualización e
for x in range (1):
        yag.send(destinatarios,asunto,mensaje)
        print(x,' Correo mandado con exito.')
```

Ilustración 1.- Generación de SPAM

Código de "Generar SPAM" anexado en el archivo:* ***spam.py*

Detectar SPAM

```
from googleapiclient.discovery import build
from googleapiclient.errors import HttpError
from google.oauth2.credentials import Credentials
from sklearn.feature_extraction.text import CountVectorizer
from sklearn.naive_bayes import MultinomialNB
import base64
from Google import Create_Service

CLIENT_FILE='credentials.json'
API_NAME='gmail'
API_VERSION='v1'
SCOPES=['https://mail.google.com/']
service=Create_Service(CLIENT_FILE,API_NAME,API_VERSION,SCOPES)

# Definir las etiquetas que se buscarán
SPAM_LABELS = ['SPAM', 'TRASH']
# Obtener los mensajes con las etiquetas definidas
msgs = []
for label in SPAM_LABELS:
    results = service.users().messages().list(userId='me',
labelIds=[label]).execute()
    msgs.extend(results.get('messages', []))
# Procesar los mensajes
spam_emails = []
for msg in msgs:
    try:
        message = service.users().messages().get(userId='me',id=msg['id']).execute()
        payload = message['payload']
        headers = payload['headers']
        # Obtener el cuerpo del mensaje
        body = ''
```

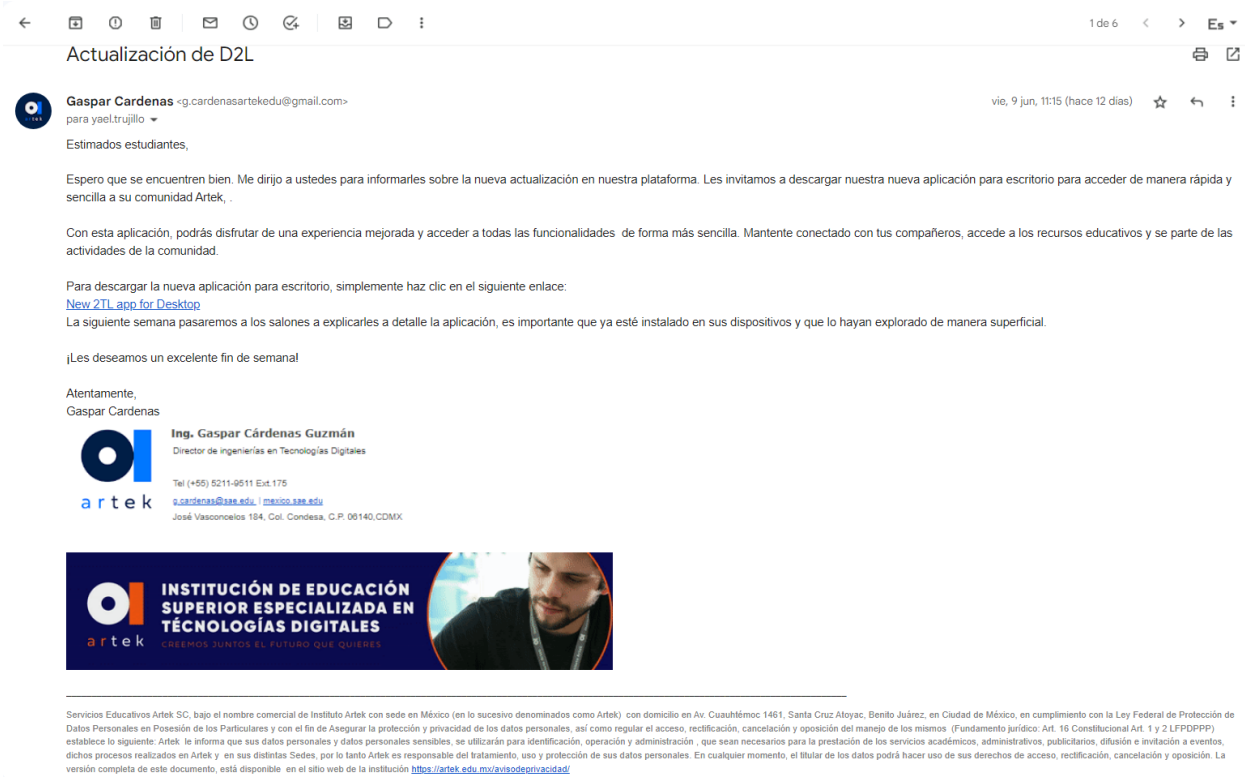
Ilustración 2.- Detector de SPAM

```python
for part in payload['parts']:
    #checo que la llave data este dentro del diccionario body
    if 'data' in part['body']:
        if part['body']['size'] > 0:
            print(body)
            body += base64.urlsafe_b64decode(part['body']['data']).decode('utf-8')
            subject = [header['value'] for header in headers if header['name'] =='Subject'][0]

            vectorizer = CountVectorizer()
            X = vectorizer.fit_transform([subject + ' ' + body])
            model = MultinomialNB()
            model.fit(X, [0])
            if model.predict(X)[0] == 1:
                spam_emails.append(message)

    except HttpError as error:
        print('An error occurred: %s' % error)
    # Mostrar los correos electrónicos SPAM detectados
    for email in spam_emails:
        print('SPAM:', email['snippet'])
```

Ilustración 3.- Detector de SPAM

Código de "Detectar SPAM" anexado en el archivo:* ***antispam.py*

Phising



Actualización de D2L

Gaspar Cardenas <g.cardenasartekedu@gmail.com>
para yael.trujillo

vie, 9 jun, 11:15 (hace 12 días)

Estimados estudiantes,

Espero que se encuentren bien. Me dirijo a ustedes para informarles sobre la nueva actualización en nuestra plataforma. Les invitamos a descargar nuestra nueva aplicación para escritorio para acceder de manera rápida y sencilla a su comunidad Artek, .

Con esta aplicación, podrás disfrutar de una experiencia mejorada y acceder a todas las funcionalidades de forma más sencilla. Mantente conectado con tus compañeros, accede a los recursos educativos y se parte de las actividades de la comunidad.

Para descargar la nueva aplicación para escritorio, simplemente haz clic en el siguiente enlace:
New 2TL app for Desktop
La siguiente semana pasaremos a los salones a explicarles a detalle la aplicación, es importante que ya esté instalado en sus dispositivos y que lo hayan explorado de manera superficial.

¡Les deseamos un excelente fin de semana!

Atentamente,
Gaspar Cardenas

Ing. Gaspar Cárdenas Guzmán
Director de ingenierías en Tecnologías Digitales

Tel (+55) 5211-9511 Ext.175
g.cardenas@sae.edu | mexico.sae.edu
José Vasconcelos 184, Col. Condesa, C.P. 06140,CDMX

artek

INSTITUCIÓN DE EDUCACIÓN SUPERIOR ESPECIALIZADA EN TÉCNOLOGÍAS DIGITALES
CREEMOS JUNTOS EL FUTURO QUE QUIERES

Servicios Educativos Artek SC, bajo el nombre comercial de Instituto Artek con sede en México (en lo sucesivo denominados como Artek) con domicilio en Av. Cuauhtémoc 1461, Santa Cruz Atoyac, Benito Juárez, en Ciudad de México, en cumplimiento con la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y con el fin de Asegurar la protección y privacidad de los datos personales, así como regular el acceso, rectificación, cancelación y oposición del manejo de los mismos (Fundamento jurídico: Art. 16 Constitucional Art. 1 y 2 LFPDPPP) establece lo siguiente: Artek le informa que sus datos personales y datos personales sensibles, se utilizarán para identificación, operación y administración , que sean necesarios para la prestación de los servicios académicos, administrativos, publicitarios, difusión e invitación a eventos, dichos procesos realizados en Artek y en sus distintas Sedes, por lo tanto Artek es responsable del tratamiento, uso y protección de sus datos personales. En cualquier momento, el titular de los datos podrá hacer uso de sus derechos de acceso, rectificación, cancelación y oposición. La versión completa de este documento, está disponible en el sitio web de la institución https://artek.edu.mx/avisodeprivacidad/

Ilustración 4.- Correo de Phishing

Ilustración 5.- Landing page de Phishing

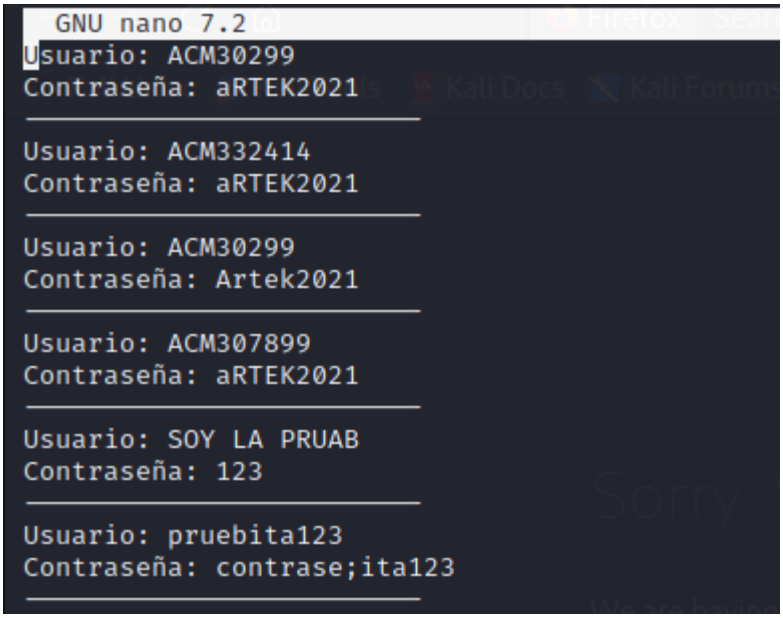


Ilustración 6.- Captura de claves de Phishing

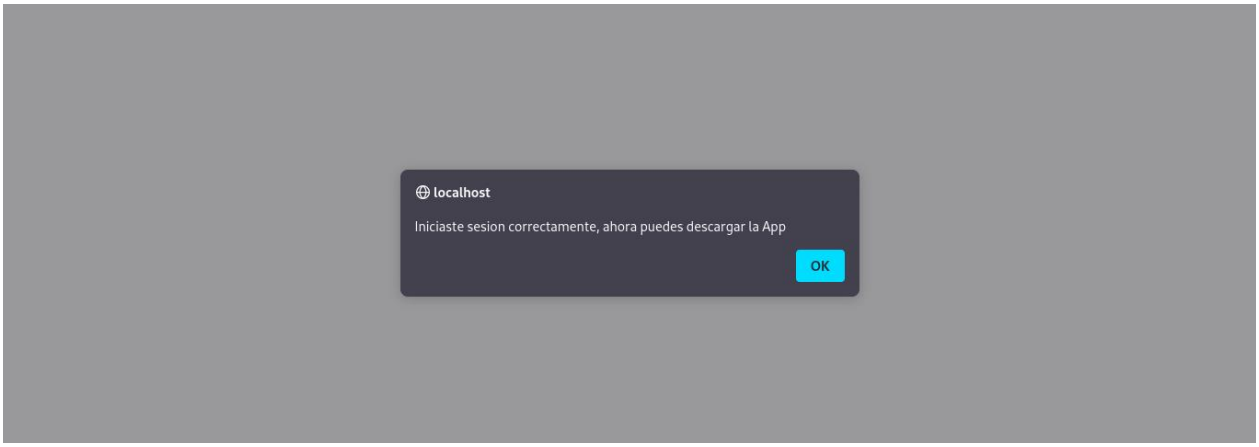


Ilustración 7.- Acción al "Iniciar sesión"

Ilustración 8.- Segunda página de Phishing

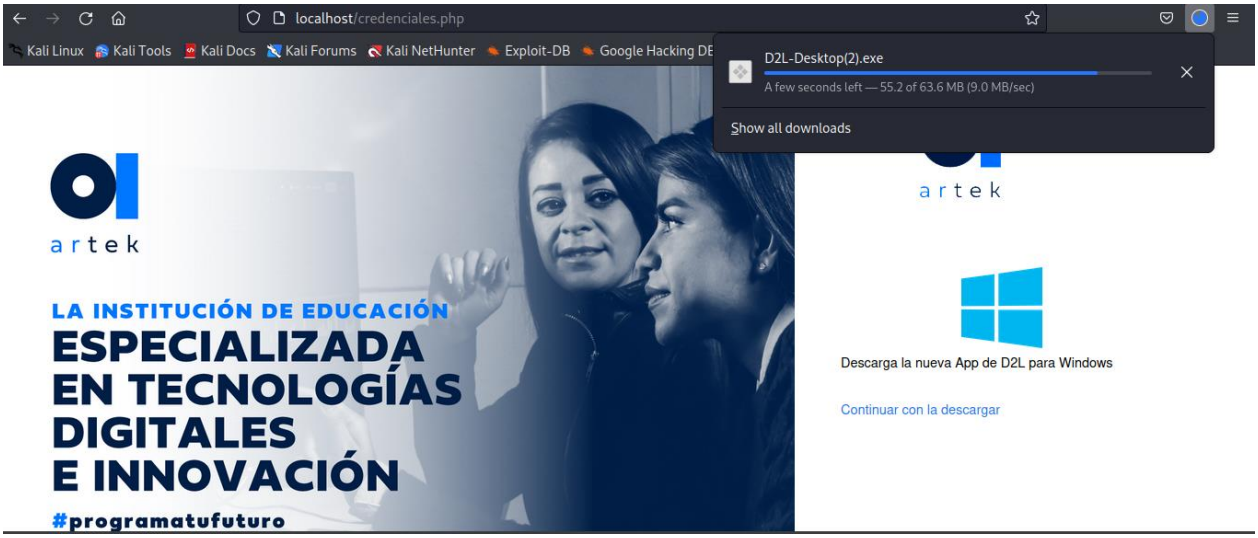


Ilustración 9.- Descarga de "Desktop.exe"

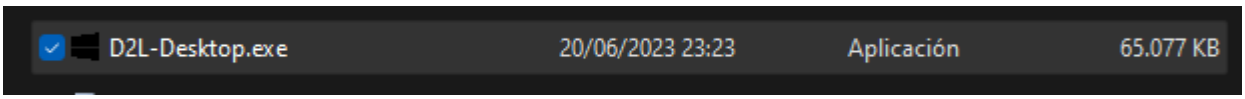


Ilustración 10.- Programa descargado para Instalación

Spyware

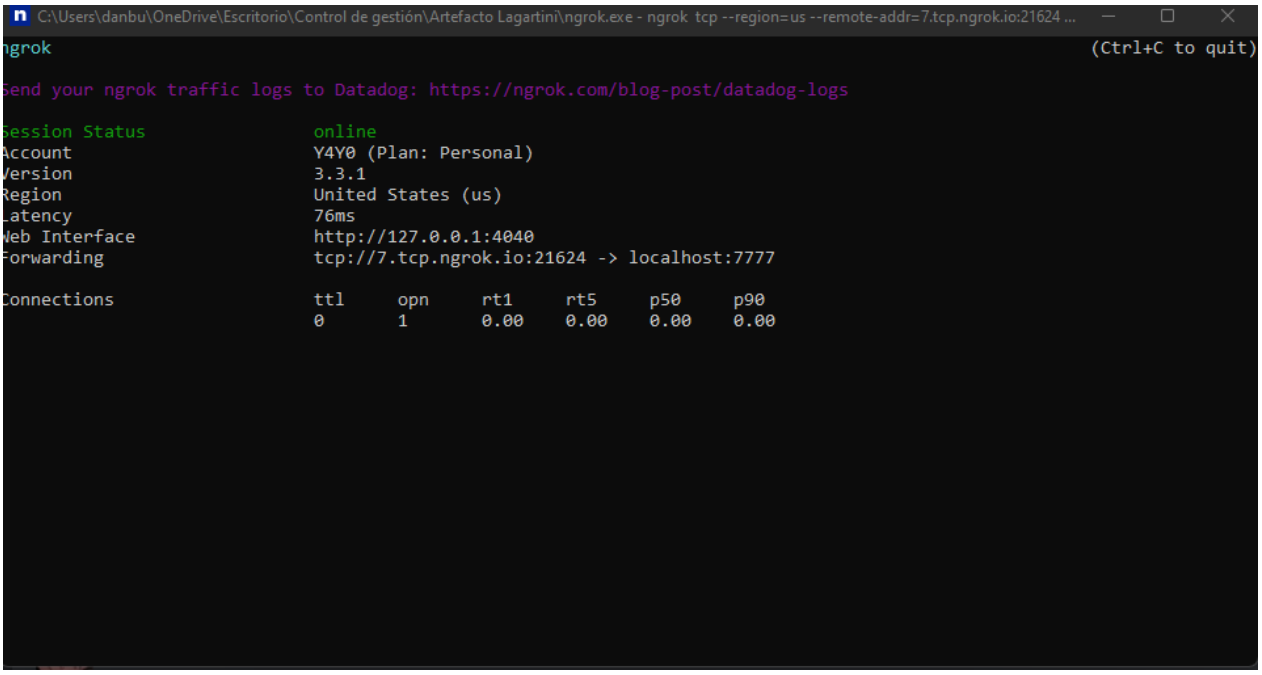


Ilustración 11.- Spyware

Ilustración 12.- Logeo de Spyware

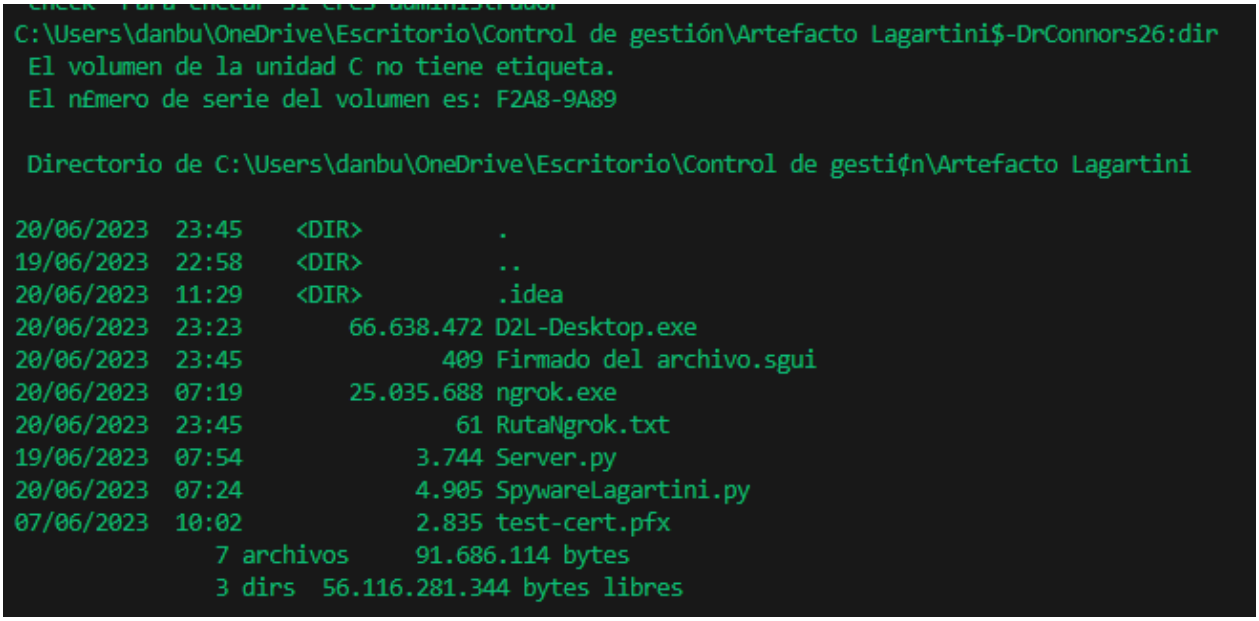


Ilustración 13.- Ingreso a usuario afectado 1

```
C:\Users\danbu\OneDrive\Escritorio\Control de gestión\Artefacto Lagartini$-DrConnors26:cd ..
C:\Users\danbu\OneDrive\Escritorio\Control de gestiÃ³n
C:\Users\danbu\OneDrive\Escritorio\Control de gestión$-DrConnors26:dir
 El volumen de la unidad C no tiene etiqueta.
 El n£mero de serie del volumen es: F2A8-9A89

 Directorio de C:\Users\danbu\OneDrive\Escritorio\Control de gesti¢n

19/06/2023  22:58    <DIR>          .
21/06/2023  13:58    <DIR>          ..
20/06/2023  23:45    <DIR>          Artefacto Lagartini
08/06/2023  08:04           327.186 diagrama de base de datos.pdf
19/06/2023  22:56            52.629 Portafolio de evidencias Daniel Bustamante Lagart.pdf
09/06/2023  11:34    <DIR>          pruebas
08/06/2023  08:09             3.699 SQLQuery2.sql
27/04/2023  21:27         1.174.825 Tarea1 Daniel Bustaante Lagart_S¡ntesis sobre los sistemas de informaci¢n .docx
04/05/2023  21:34           801.203 Tarea2 Daniel Bustaante Lagart_.docx
29/05/2023  17:12            34.251 Tarea2 Daniel Bustamante Lagart_S¡ntesis dobre casos de estudio de BPM en la ciberseguridad.docx
29/05/2023  17:16            34.355 Tarea3 Daniel Bustamante Lagart Sintesis sobre la nube.docx
09/06/2023  11:35    <DIR>          test
               7 archivos      2.428.148 bytes
               5 dirs  56.115.449.856 bytes libres
```

Ilustración 14.- Ingreso a usuario afectado 2

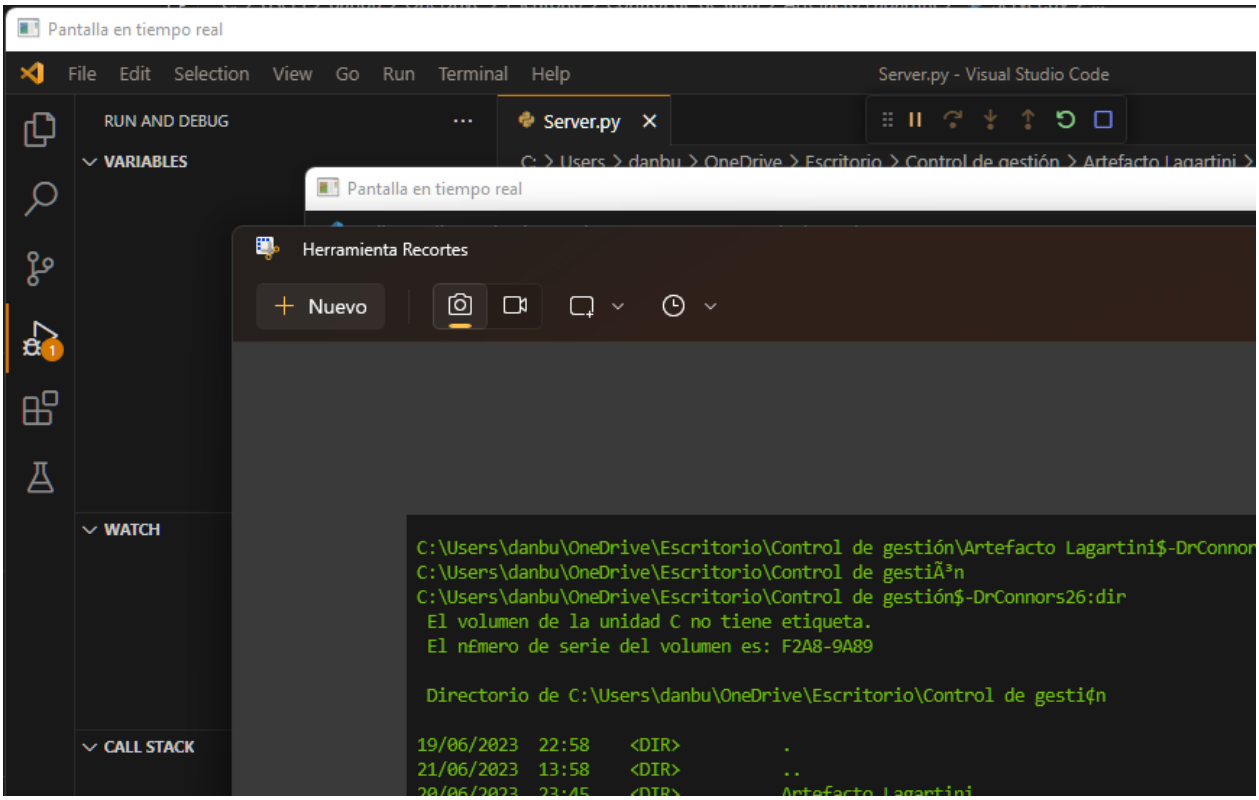


Ilustración 15.- Pantalla en tiempo real de usuario afectado

Conclusiones

El spam es una forma de comunicación no deseada que se envía en masa a través de varios medios, como el correo electrónico, mensajes de texto y redes sociales. Para las organizaciones, el spam puede tener efectos perjudiciales, como sobrecargar los servidores de correo y consumir tiempo y recursos de los empleados.

Para evitar caer en trampas de spam, se pueden implementar varias medidas. Esto incluye configurar filtros de correo electrónico efectivos, capacitar a los empleados sobre cómo identificar y evitar el spam, establecer políticas de uso de correo electrónico, mantener el software y sistemas de seguridad actualizados, y utilizar listas de bloqueo y listas blancas para gestionar los remitentes de spam.

Además, es importante fomentar la implementación de autenticación de remitentes y evitar la divulgación innecesaria de direcciones de correo electrónico. También se debe gestionar adecuadamente las suscripciones y listas de correo, asegurándose de que los empleados solo se suscriban a listas legítimas y confiables. Estas medidas ayudarán a las organizaciones a minimizar el impacto del spam y proteger su productividad y seguridad en la comunicación.

Referencias

Álvarez, Á. (2014, noviembre 13). ¿Por qué Gmail puede marcar un email como SPAM? Hostinet; Hostinet SLU. https://www.hostinet.com/formacion/correo-electronico/por-que-gmail-marca-email-spam/

¿Correo basura o spam? Definición de mensajes no deseados. (s/f). Eset.com. Recuperado el 22 de junio de 2023, de https://www.eset.com/es/caracteristicas/spam/

Informe de políticas: El desafío del spam. (2016, enero 29). Internet Society. https://www.internetsociety.org/es/policybriefs/spam/

Jiménez, J. (2021, diciembre 5). Qué pasa si abres un correo Spam en tu PC o móvil. RedesZone. https://www.redeszone.net/tutoriales/seguridad/que-pasa-abrir-correo-spam/

Los peligros de los mensajes de spam. (2023, abril 19). latam.kaspersky.com. https://latam.kaspersky.com/resource-center/threats/dangers-of-spam-texts

SMM. (2022, agosto 22). Los motivos por los que algunos correos se van directamente a la bandeja de spam. Marca. https://www.marca.com/tecnologia/2022/08/22/6303947222601dfd378b45a1.html