Actividad Grupal- Vectores de Ataque

Casos Agencia Tributaria, BBVA y Netflix- Seguridad en los Sistemas de Información

Emilio Calvo de Mora Mármol
Alejandro Calvo Benito
Manuel Pérez Luque
Rocío Agraz Martos

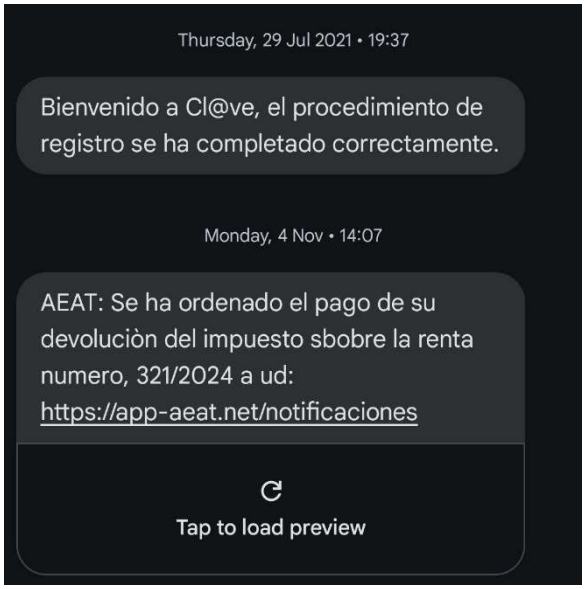
Enlace al repositorio de la actividad grupal

https://github.com/Rofraraf/Smishing-Vectores-Ataque

Caso de *Smishing*: Agencia Tributaria

En 2024 se detectó una campaña de SMS falsos que pretenden suplantar la identidad de la Agencia Tributaria mediante *spoofing*, suplantando a la misma Agencia Tributaria. De esta manera, el mensaje ilegítimo parece provenir del mismo número que utiliza la Agencia, llegando a aparecer en el mismo hilo o conversación con mensajes previos verdaderos.

Esta es una imagen de un mensaje ilegítimo que le llegó a un integrante del grupo de trabajo en la misma conversación en la que previamente le habían llegado mensajes legítimos:



Otro ejemplo de *smishing* en 2024 denunciado por la Agencia Tributaria es el reembolso de impuestos a mutualistas jubilados, solicitando datos de tarjetas bancarias y fotos de DNI. Aquí un ejemplo del tipo de mensajes que llegaban a los teléfonos móviles de las víctimas:

1. **Vector de Ataque:**

   En ambos casos es muy parecido, contando con:
   - Un **mensaje inicial**, que informa a la víctima de que se ha ordenado el pago de su devolución del impuesto sobre la renta.
   - Un **enlace** que lleva a la página falsa.

2. **Página Falsa:**

   - Una **página falsa** con el membrete de la Agencia Tributaria y el escudo de España, con un dominio que no pertenece a la Agencia Tributaria, con un formulario que pide el ingreso de datos como el método de pago, nombre del titular de la tarjeta, fecha de caducidad, código de seguridad...
   - En algunos casos, se llega incluso a realizar una llamada telefónica haciéndose pasar por un funcionario de la Agencia Tributaria.

Las consecuencias de este ataque de *smishing* suponen la obtención de los datos bancarios de la víctima no autorizados y copia del DNI.

Enlace al artículo en la sede de la Agencia Tributaria:
https://sede.agenciatributaria.gob.es/Sede/ayuda/consultas-informaticas/informacion-casos-phishing/2024.html

Enlace a artículo de prensa relacionado con esta estafa:
https://www.20minutos.es/tecnologia/ciberseguridad/ultima-estafa-viral-agencia-tributaria-sms-reembolso-263-euros-5646595/

Recursos Adicionales:

Página en github centrado en un laboratorio de hacking ético para aprender ciberseguridad:
https://github.com/Samsar4/Ethical-Hacking-Labs/blob/master/8-Social-Engineering/1-Using-SET.md

En la pestaña de Ingeniería Social se explica cómo clonar una página web, mandar un correo electrónico falso (sustituible en cualquier caso con un SMS para realizar el *smishing*) y redirigir a la página web clonada.

https://github.com/stirtcanada/smishing

https://github.com/spider863644/SMS-Attack

https://github.com/trustedsec/social-engineer-toolkit

Caso de *Smishing*: BBVA

En noviembre de 2024, una abogada de Barcelona, Helena Gimeno, fue víctima de una sofisticada estafa de *smishing (https://www.rac1.cat/societat/20241204/216894/roben-70000-euros-advocada-barcelona-sofisticada-estafa-clicar-pantalla-quedar-negra-elmon.html)* que le costó 70.000 euros. Recibió un SMS que parecía provenir de su banco, BBVA, solicitando la renovación de sus claves de seguridad. El mensaje incluía un enlace que, al pulsarlo, llevó a una página fraudulenta que imitaba la del banco. Tras ingresar sus datos, los estafadores accedieron a sus cuentas y realizaron transferencias no autorizadas.

Este caso destaca la creciente sofisticación de las estafas de *smishing*, donde los delincuentes no solo envían mensajes convincentes, sino que también utilizan técnicas como el ***spoofing*** para que el número de teléfono o el remitente parezca legítimo. Incluso pueden insertar los mensajes fraudulentos en hilos de conversación reales del banco, aumentando la credibilidad del engaño.

1. Vector de ataque:

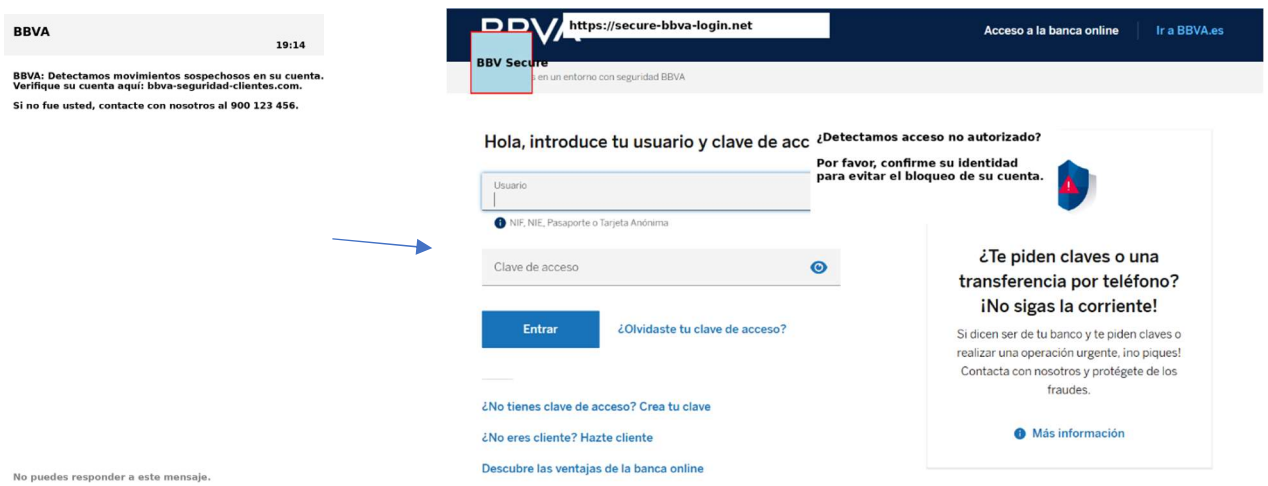
- **Mensaje inicial:**
  - Texto del SMS: *"BBVA: Se detectaron movimientos sospechosos. Verifique su cuenta aquí: bbva-seguridad-clientes.com."*
- **Acción del usuario:**
  - El usuario hace clic en el enlace proporcionado.
- **Redirección:**
  - El enlace lleva a una página falsa que imita la interfaz de inicio de sesión de BBVA.

2. Página falsa:

- **Elementos:**
  - Logo modificado: "BBV Secure".
  - URL fraudulenta: *"**https://secure-bbva-login.net******"*.
  - Campos para ingresar usuario y contraseña.
  - Mensaje de advertencia falso: "¿Detectamos acceso no autorizado? Confirme su identidad para evitar el bloqueo de su cuenta."

3. Consecuencias:

- Robo de fondos de la cuenta de la víctima.
- Riesgo de acceso a otras cuentas si se utilizan credenciales similares.



Recursos Adicionales:

1. BBVA Antipishing Script (GitHub) (https://github.com/JaimeTR/Antipishing): Un script diseñado para detectar páginas de phishing que imitan portales bancarios.
2. Evilginx2 (GitHub) (https://github.com/kgretzky/evilginx2): Herramienta avanzada para ataques de phishing man-in-the-middle, permitiendo capturar credenciales y tokens de sesión. Proporciona una visión técnica de cómo operan los ataques sofisticados dirigidos a bancos.

3. Phishing Simulation Toolkit (GitHub) (https://github.com/gophish/gophish): Plataforma para simular ataques de phishing, útil para analizar vectores de ataque en bancos.
4. King Phisher (GitHub) (https://github.com/rsmusllp/king-phisher): Plataforma para simular ataques de phishing en el mundo real, promoviendo la concienciación y permitiendo el control total sobre correos electrónicos y contenido del servidor.

5. Osint Framework (GitHub) (https://github.com/lockfale/osint-framework): Herramienta para realizar investigaciones OSINT, incluyendo análisis de vectores de ataque en phishing. Ayuda a comprender cómo los atacantes recopilan información antes de un ataque.

Caso de *Smishing*: Netflix

En diciembre de 2024, se detectó una campaña de *smishing* que suplantaba la identidad de Netflix (https://cincodias.elpais.com/smartlife/lifestyle/2024-12-05/cuidado-con-esta-estafa-se-hacen-pasar-por-netflix-para-vaciar-tu-cuenta-bancaria.html). Los estafadores enviaban SMS informando de un supuesto retraso en el pago y amenazando con la cancelación de la cuenta. El mensaje incluía un enlace que dirigía a una página web que imitaba a la de Netflix, solicitando las credenciales y datos de tarjeta de crédito de la víctima. Esta estafa afectó a usuarios en más de 23 países, incluyendo España.

1. Vector de ataque:

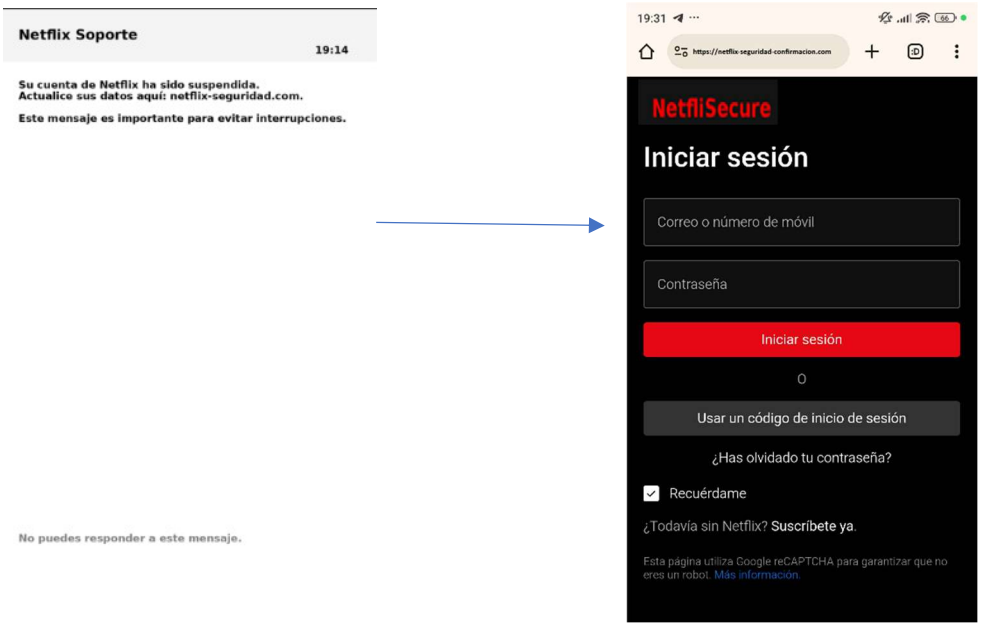
- **Mensaje inicial:**
  - Texto del SMS: *"Su cuenta de Netflix ha sido suspendida. Actualice sus datos aquí: netflix-seguridad-confirmacion.com."*
- **Acción del usuario:**
  - El usuario hace clic en el enlace proporcionado en el SMS.
- **Redirección:**
  - El enlace lleva a una página falsa que imita la interfaz oficial de Netflix.

2. Página falsa:

- **Elementos:**
  - Logo modificado: "NetfliSecure".
  - URL fraudulenta: *"https://netflix-seguridad-confirmacion.com".*
  - Campos para ingresar correo electrónico y contraseña.
  - Botón rojo con texto: "Actualizar ahora".

3. Consecuencias:

- Acceso no autorizado a la cuenta de Netflix.
- Robo potencial de información financiera si el mismo correo y contraseña se utilizan para otras plataformas.



Recursos Adicionales:

1. Netflix-Phishing-Page (GitHub) (https://github.com/1zu0/Netflix-Phishing-Page) – Repositorio que contiene una página falsa que imita la interfaz de inicio de sesión de Netflix

Ejemplo de cómo hacerlo:

Netflix-Phishing-Page: Este repositorio ofrece una página de phishing que emula la interfaz de inicio de sesión de Netflix.

- **Instrucciones para Configuración y Modificación**:
    1. **Acceso al Repositorio**: Visite el repositorio en Netflix-Phishing-Page.
    2. **Lectura de Instrucciones**: Cambie la extensión del archivo hwto a .txt para acceder a las instrucciones detalladas sobre la configuración y modificación de la página.
    3. **Redirección Personalizada**: Edite el archivo data.php para especificar la URL a la que desea redirigir al usuario después de capturar las credenciales.
    4. **Implementación en Servidor**: Suba todos los archivos del repositorio a su servidor para que la página de phishing funcione correctamente.

2. Fake Login Page Generator (GitHub) (https://github.com/wifiphisher/wifiphisher): Herramienta para crear páginas de inicio de sesión falsas utilizadas en ataques de pishing.

3. Phishing Templates Collection (GitHub) (https://github.com/gophish/hub): Conjunto de plantillas de phishing, incluidas opciones para servicios de streaming como Netflix.

4. Zphisher (GitHub) (https://github.com/htr-tech/zphisher): Herramienta para crear campañas de phishing con URLs acortadas, destacando en la simulación de enlaces de phishing como los empleados en *smishing*.
que utlizaremos más adelante para recrear un ataque.
5. Blackeye (GitHub) (https://github.com/EricksonAtHome/blackeye): Repositorio con plantillas de phishing, incluidad plataformas pupulares.
6. Articulo (https://carder.market/threads/chto-takoe-smishing-i-kak-ego-izbezhat.95297/) sobre el *smishing* y cómo prevenirlo.
7. Video educativo que analiza un ataque de *smishing* paso a paso (https://www.youtube.com/watch?v=NIP6mVnch8Q&ab_channel=s4vitar)
8. Video explicativo sobre los concepto básicos (https://www.youtube.com/watch?v=yYYEjz0sYJM&ab_channel=CyberMadhan) de *smishing*.
9. Este video (https://www.youtube.com/watch?v=ctHHWCdsg-s&ab_channel=ShelcyCalderon) presenta una simulación de un ataque *smishing*, mostrando como se opera y recomendaciones para no caer.
10. SocialFish(Github) (https://github.com/UndeadSec/SocialFish): Repositorio para la clonación de páginas web tanto como redes sociales, servicios en la nube, etc. Ofrece plantillas, es fácil de configurar y usar y tiene soporte para herramientas de tunelización como Ngrok y Localtunnel