	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°183	Fecha: 06-08-2023
		Página: 6 de 12

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de Alerta	Nueva campaña de Phishing que suplanta a la entidad bancaria de Interbank		
Tipo de Ataque	Phishing	Abreviatura	Phishing
Medio de Propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de Subfamilia	G01
Clasificación temática familia	Fraude financiero		

Descripción

1. A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que los ciberdelincuentes vienen llevando a cabo una campaña de envío masivo de correos electrónicos falsos, que pretenden ser de la entidad bancaria de Interbank, en el asunto del mensaje advierten ***"Le hacemos llegar una notificación debido a que su cuenta Interbank ha sido bloqueada, esto puede ser debido al ingreso sospechoso a su cuenta de terceros a través de banca por internet ",*** incluido un enlace oculto detrás del botón ***"Ingresa aquí"*** que, al ser pulsado, redirige a la víctima, a un sitio web falso de Interbank que simula ser el oficial, con el objetivo de robar las credenciales de acceso, información personal y/o financiera.

- Proceso del ciberataque:

Figura 1. Correo inicial que llega a la víctima.

Figura 2. Solicitud para ingresar las credenciales de acceso (DNI, y clave web).

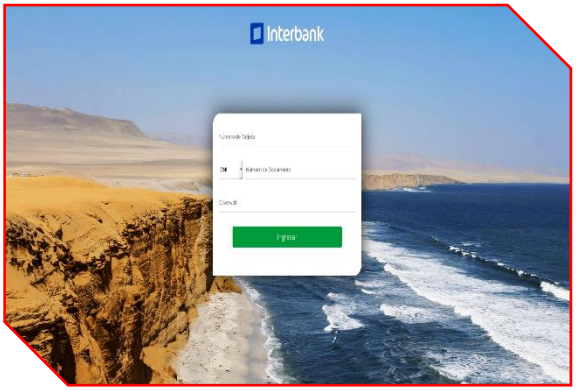


Figura 3. Seguidamente, parece validar los datos, pero en realidad la información fue robada por los ciberdelincuentes.

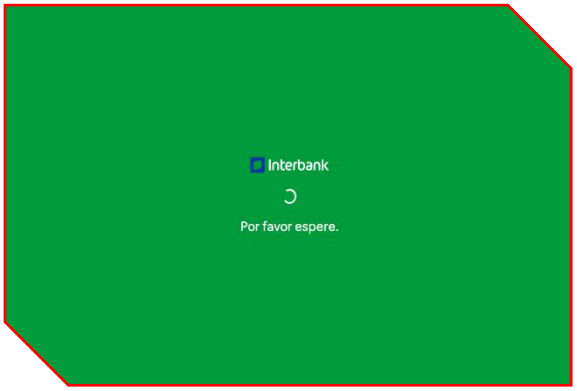
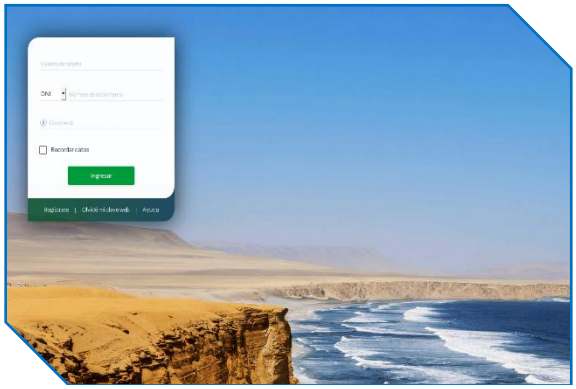


Figura 4. Al final, es redirigido al sitio web oficial Interbank, aludiendo un aparente error de autenticación.

- Comparación de los sitios web legítimo y falso del Banco Interbank:

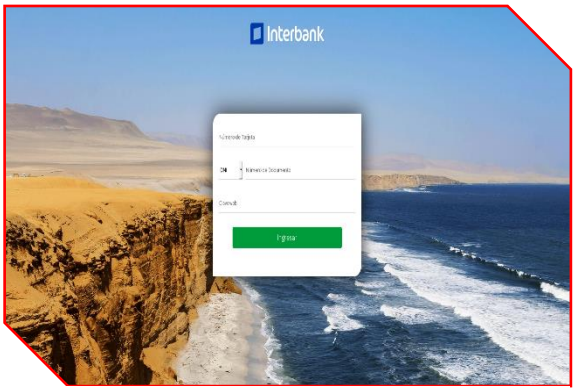
SITIO OFICIAL

URL: https://bancaporintenet.interbank.pe/login



SITIO FRAUDULENTO

URL: hxxps[:]//alertas-movil-interbank[.]com



- Existe similitud en imagen, logotipo, fondo, color y escritura.
- Tiene certificado de seguridad de protocolo HTTPS.
- El dominio se hace pasar por el sitio oficial, pero no coinciden.

2. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, siendo catalogado como **SUPLANTACIÓN DE IDENTIDAD:**

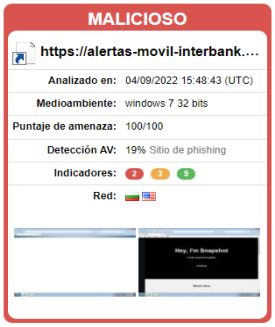
- Indicadores de compromisos:
  - **URL:** hXXps[:]//alertas-movil-interbank[.]com
  - **Dominio:** alertas-movil-interbank[.]com
  - **Dirección IP:** 45[.]88[.]202[.]115
  - **Código:** 200
  - **Longitud:** 6.11 KB
  - **SHA-256**: 176edfed461870dd89ebc2b709c3bd43354405e8f493aedf9cb04239b9b650ab

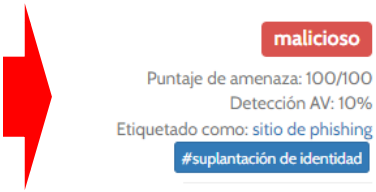
DETECCIÓN | DETALLES | COMUNIDAD

Análisis de proveedores de seguridad

alphaMountain.ai	Suplantación de identidad	Anti-AVL	Malicioso
Avira	Suplantación de identidad	BitDefender	Suplantación de identidad
G-datos	Suplantación de identidad	Búsqueda segura	Malicioso
Sophos	Suplantación de identidad	raíz web	Malicioso

- Otros resultados del análisis:





- Phishing:
    - Es un tipo de ataque de ingeniería social, que consiste en la utilización de envió masivo de email, los cuales se disfrazan para que parezcan proceder de una fuente de confianza. Estos emails están diseñados para engañar a las víctimas y conseguir que proporcionen información personal o financiera.
- Características de un Phishing:
    - Contiene errores ortográficos
    - No se respeta el formato (justificado)
    - Algunos emails son de alerta o urgencia
    - Tienen adjunto documento o URLs

3. RECOMENDACIONES:

- Evitar ingresar los datos de autenticación en las URL que recibas por correo electrónico.
- Escribir directamente la URL de la entidad en el navegador.
- Sospechar de todos aquellos mensajes alarmantes que tengan tono de urgencia y contengan faltas de ortografía o erratas.
- No divulgar la información a amigos, familiares o terceros.
- Utilizar un programa antivirus actualizado, ya que es la primera línea de defensa contra un ciberataque.

Fuente de Información	Análisis propio de redes sociales y fuente abierta

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°183	**Fecha: 05-08-2023** **Página: 9 de 12**

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de Alerta	Detección de falso servicio del correo electrónico de Microsoft		
Tipo de Ataque	Phishing	Abreviatura	Phishing
Medio de Propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de Subfamilia	G01
Clasificación temática familia	Fraude		

Descripción

1. ANTECEDENTES

A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que actores de amenazas vienen realizando una campaña de Phishing, activando un falso servicio del correo electrónico de la compañía Microsoft (Outlook, Hotmail, etc.), con la finalidad de obtener las credenciales de acceso (correos y contraseñas) de los usuarios de la compañía tecnológica.

2. DETALLES

El proceso del Phishing es el siguiente:

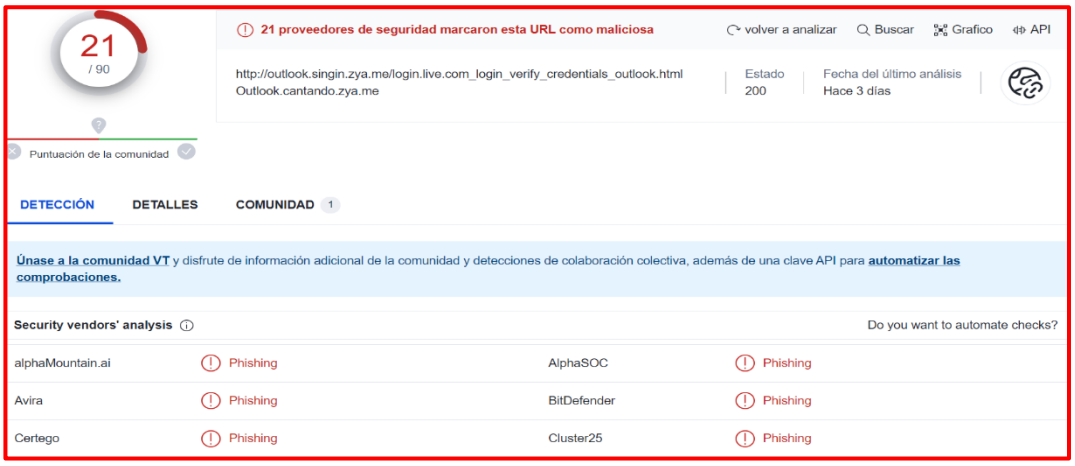
Solicita el correo electrónico de la víctima, para acceder al servicio en la web de la compañía Microsoft (Outlook, Hotmail, etc.)

Requieren la contraseña de acceso para el servicio web de Microsoft, para luego dar clic en <Iniciar sesión>; sin embargo, después de unos segundos redirige al servicio del correo electrónico de la compañía Microsoft.

A. Comparación del sitio web oficial y fraudulento.

- Existe diferencias entre la URL original y la fraudulenta.
- La URL del sitio web fraudulento NO POSEE protocolo de seguridad de red (https)
- Existe una similitud entre ambas páginas en imagen, fondo y colores de ambos sitios web.

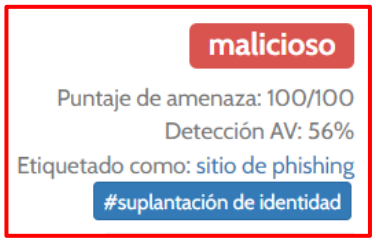
B. Proveedores de seguridad informática alertan como SUPLANTACIÓN DE IDENTIDAD - PHISHING.

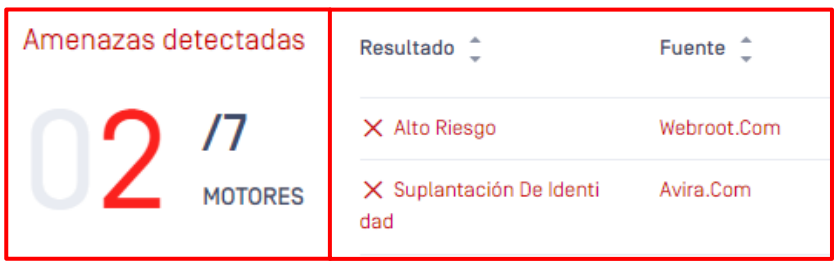


C. Indicadores de compromiso (IoC)

- Dominio : zya[.]me
- Servidor : nginx
- SHA-256 : 71ec5ad558904e0d11ff478e7d870b80797ea97b1500d09532f66eebd3bd962e
- IP : 185[.]27[.]134[.]60

D. Otras detecciones:





E. Apreciación de la información:

- La presente campaña de Phishing permite a los actores de amenazas obtener las credenciales de acceso del servicio del correo electrónico en la web de la compañía Microsoft (Outlook, Hotmail, etc.).

- La propagación del sitio web fraudulento se realiza mediante envió masivos de email, adjuntando enlaces de sitios web fraudulentos con la finalidad de obtener información sensible de las víctimas; asimismo, dicho enlace malicioso, es enviado a través de las plataformas digitales como el WhatsApp, Telegram, Messenger y mensajes de textos SMS.

3. RECOMENDACIONES:

- Verificar detalladamente las URL de los sitios web
- No abrir o descargar archivos sospechosos.
- No seguir las instrucciones de sitio web sospechoso.
- Mantener el antivirus actualizado.
- Descargar aplicaciones de fuentes confiables.
- Realizar las actualizaciones correspondientes desde fuentes originales.

Fuente de Información	Análisis propio de redes sociales y fuente abierta