	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°219	Fecha: 17-09-2023
		Página: 5 de 11

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Phishing, suplantado la identidad de la compañía multinacional Amazon		
Tipo de Ataque	Phishing	Abreviatura	Phishing
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de Sub familia	G01
Clasificación temática familia	Fraude		

Descripción

1. ANTECEDENTES:

A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, los ciberdelincuentes se encuentran desarrollando una nueva campaña de Phishing, a través de los diferentes navegadores web, quienes vienen suplantando la identidad de la compañía multinacional de comercio electrónico Amazon, con el objetivo de acceder u obtener credenciales de acceso, datos personales y bancarios de las posibles víctimas.

2. DETALLES:

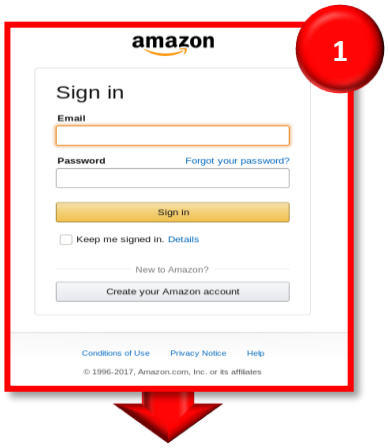


Imagen 1: Solicita dirección de correo electrónico y contraseña.

Imagen 2: Solicita datos bancarios como el número de tarjeta, fecha de caducidad y el CVC de la tarjeta.

Imagen 3: Solicita datos personales fecha de nacimiento, número telefónico, ciudad y más.

Imagen 4: Solicita ingresar las credenciales de acceso de la página (usuario y contraseña).

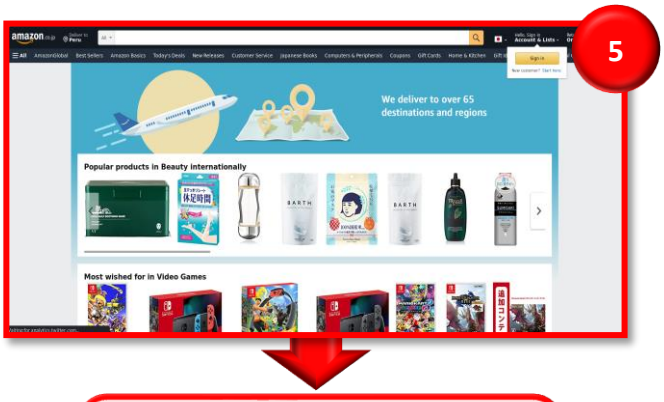
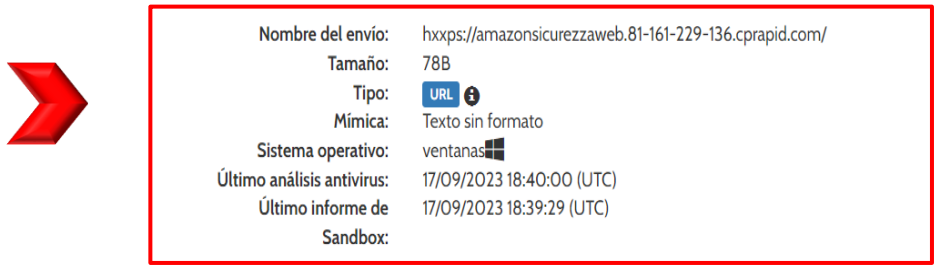


Imagen 5: Por último, es redirigido automáticamente a un supuesto sitio web de Amazon, donde la víctima puede verificar una serie de consultas como se aprecia en la imagen.

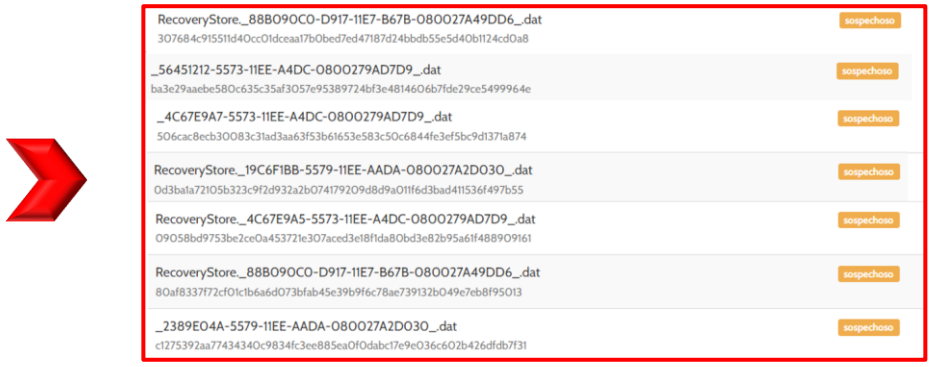
A. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, siendo catalogado como **SUPLANTACIÓN DE IDENTIDAD:**

a) Indicadores de compromisos:

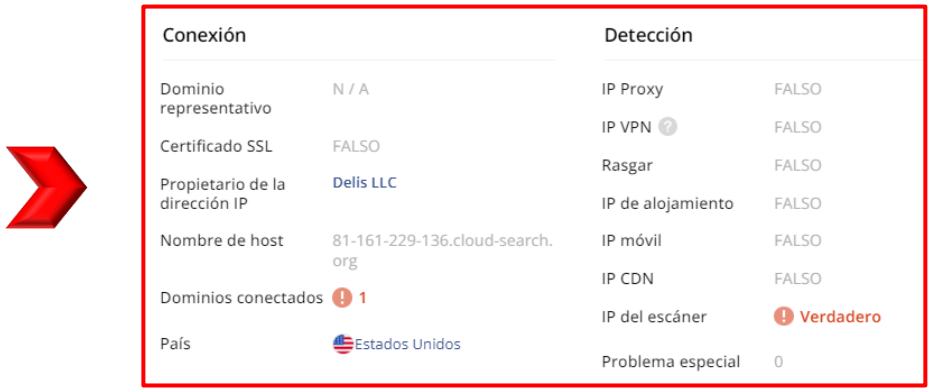
I. URL: hxxps[:]//amazonsicurezzaweb[.]81-161-229-136[.]cprapid[.]com/



II. SHA-256: 480c0607deec0d8ad43620bc29f7626fd4aa176ce355113f1d53d3edd6e642f6



III. IP: 81[.]161[.]229[.]136



IV. TIPOLOGÍA:

Se puede aprecia como la URL, esta alojada en un servidor ubicado en PAÍSES BAJOS.

B. Se hallaron **16 proveedores** de seguridad que marcaron este dominio como malicioso.

AlfaSOC	Suplantación de identidad	Avira	Suplantación de identidad
BitDefender	Suplantación de identidad	Clúster25	Suplantación de identidad
CRDF	Malicioso	Emsisoft	Suplantación de identidad
ESET	Suplantación de identidad	Fortinet	Suplantación de identidad
Datos G	Suplantación de identidad	Kaspersky	Suplantación de identidad
Netcraft	Malicioso	OpenPhish	Suplantación de identidad
Base de datos de phishing	Suplantación de identidad	búsqueda en seco	Malicioso
Sofos	Suplantación de identidad	VIPRE	Malicioso

C. Otras detecciones:

D. Cómo funciona el Phishing:

- Los correos electrónicos incluyen enlaces a sitios web preparados por los ciberdelincuentes en los que solicitan información personal.
- Medios de propagación del Phishing: WhatsApp, Telegram, redes sociales, SMS entre otros.
- Los ciberdelincuentes intentan suplantar a una entidad legitima (organismo público o privado, entidad financiera, servicio técnico, etc.)

E. Referencia:

Phishing o suplantación de identidad: Es un método que los ciberdelincuentes, utilizan para engañar a los usuarios para conseguir que revele información personal, como contraseñas, datos de tarjetas de créditos, números de cuentas bancarias, entre otros.

3. RECOMENDACIONES:

- Mantener instalado un servicio de antivirus en el dispositivo.
- Verificar la información del sitio web correspondiente.
- Acceder al sitio web a través de fuentes oficiales.
- No abrir enlaces de dudosa procedencia.
- No seguir indicaciones de sitios web fraudulentos.
- No compartir la información con terceras personas, amigos o familiares.

Fuente de Información:	Análisis propio de redes sociales y fuente abierta.

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°219	Fecha: 16-09-2023
		Página: 8 de 11

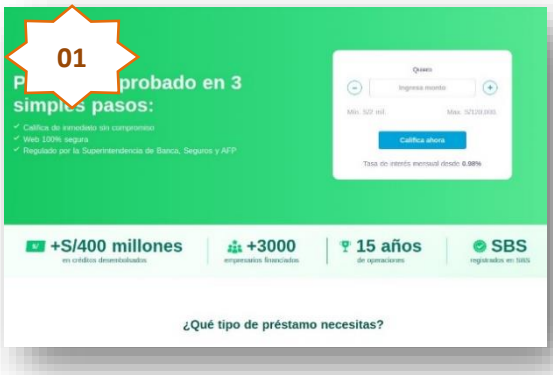
Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Detección de sitio web fraudulento del Banco Interbank		
Tipo de Ataque	Phishing	Abreviatura	Phishing
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de Sub familia	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 llevando a cabo una campaña de Phishing, suplantando el sitio web de solicitud de préstamos del Banco Interbank, con la finalidad de robar información sensible de los usuarios de la entidad financiera como números de documento de identidad, tarjetas bancarias, etc.

2. DETALLES:

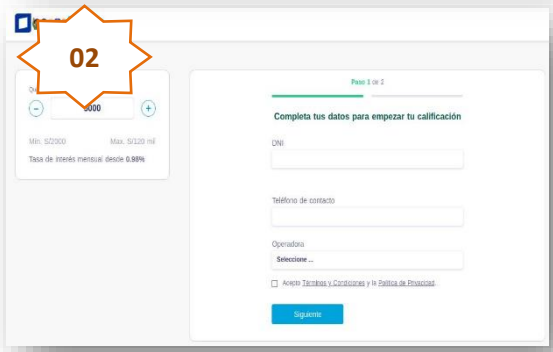


Paso Nº01

Solicitan a la víctima registrar lo siguiente:

- El monto del préstamo solicitado.

Para luego dar clic en <Calificar ahora>.

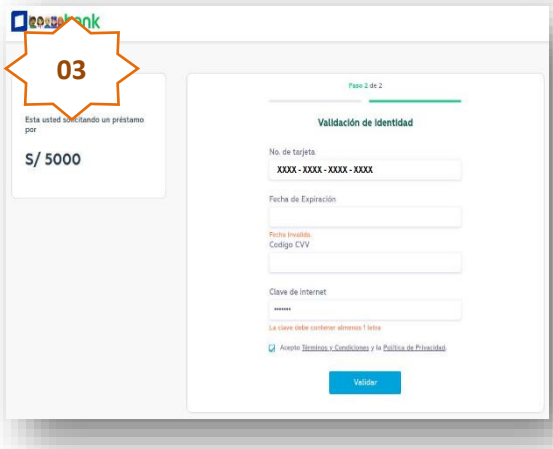


Paso Nº02

Solicita a la víctima datos como:

- El número del Documento Nacional de Identidad (DNI).
- Número de celular
- Operador telefónico

Para luego dar clic en <Siguiente>.



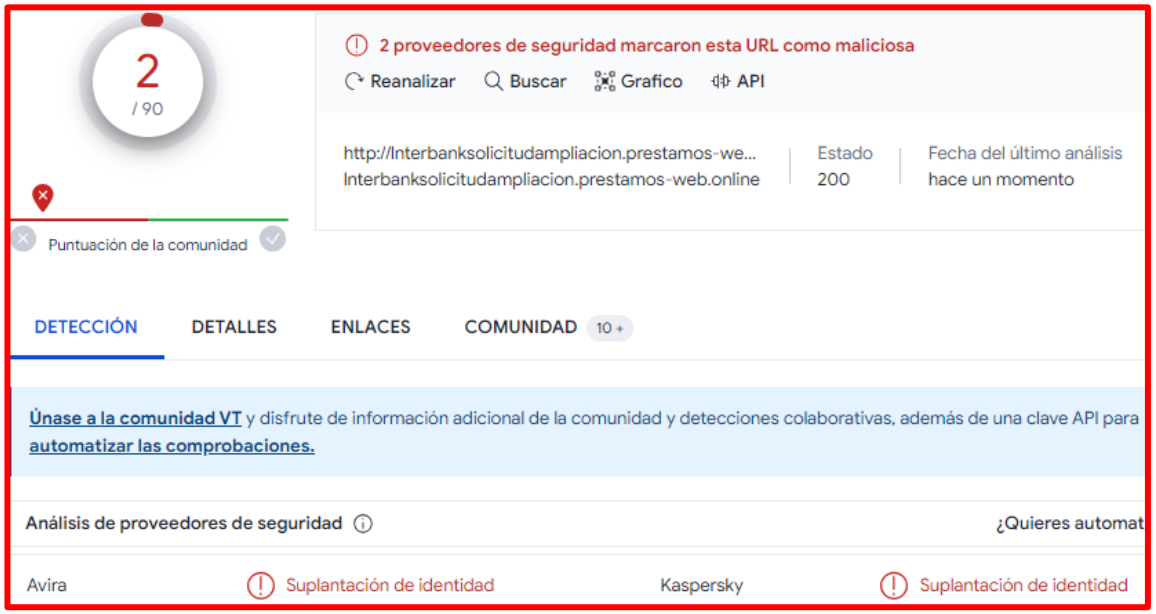
Paso Nº03

Una vez brindado los datos solicitados en el paso N.º 02, aparece una pantalla requiriendo información como el numero de la tarjeta bancaria, la fecha de expiración, el código de seguridad (CVV) y la clave de seis dígitos del intranet, para luego dar clic en <Validar>. Pero, pasado unos segundos, redirige al sitio web oficial de la entidad bancaria; sin embargo, los ciberdelincuentes obtuvieron los datos proporcionados por la víctima.

A. Comparación del sitio web oficial y fraudulento.

- Existe una diferencia entre la URL original y la URL fraudulenta.
- La URL del sitio web fraudulento posee protocolo de seguridad de red (https)
- Existe una similitud entre ambas páginas en imagen, fondo y color.

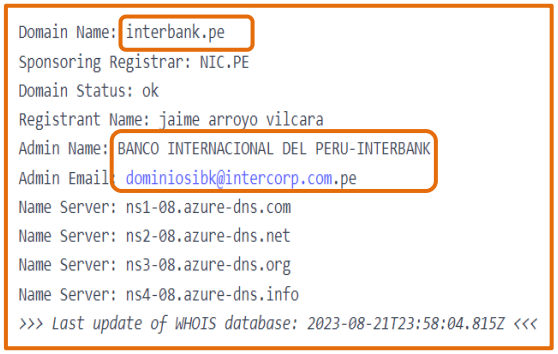
B. Proveedor de seguridad informática no alerta como SUPLANTACIÓN DE IDENTIDAD - PHISHING.



C. Indicadores de compromiso (IoC)

- Dominio : prestamos-web[.]online
- IP : 47[.]251[.]51[.]48
- Servidor : Apache
- SHA-256 : 912bb640cf3f2efca7beebe830ab4428c248fd640450a17ce01dda54e610a3e5
- Tipo Cont : Texto/Html
- Codigo : 200

D. Comparación de DOMINIOS



E. Apreciación de la información:

- La presente campaña de Phishing permite a los actores de amenazas obtener información bancaria de los usuarios del Banco Interbank.

- 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, a través de las aplicaciones de mensajería instantánea entre ellos WhatsApp, Telegram, Messenger, etc. y mensajes de textos SMS.

3. RECOMENDACIONES:

- Verificar detalladamente las URL de los sitios web.
- No abrir o descargar archivos sospechosos.
- No aceptar permisos de instalación de archivos desconocidos o dudosa procedencia.
- Mantener actualizado el sistema operativo y aplicaciones del equipo de cómputo.
- Mantener actualizado el sistema antivirus (el antivirus debe ser licenciado).
- Comunicar a la entidad financiera si ha realizado un registro de acceso en un sitio web sospechoso.

Fuente de Información:	Análisis propio de redes sociales y fuente abierta.