	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°188	Fecha: 11-08-2023
		Página: 9 de 12

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	SUPLANTACIÓN DE IDENTIDAD DEL APLICATIVO MÓVIL YAPE		
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 identidad del aplicativo Móvil YAPE, indicando que las posibles víctimas tienen hasta el 30 de Agosto para recepcionar un subsidio monetario otorgado por el estado denominado "BONO ALIMENATRIO 270 YANAPAY", el cual tiene como finalidad robar las credenciales de inicio de sesión del aplicativo, como dirección de correo electrónico, clave, etc.

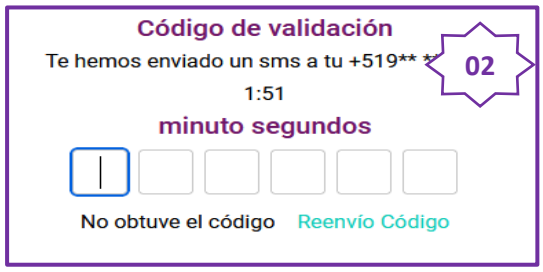
2. DETALLES:

El proceso del Phishing es el siguiente:

Paso Nº01

Ciberdelincuentes indican a las posibles víctimas que tienen hasta el 30 de Agosto para recepcionar un supuesto bono alimentario de **270 YANAPAY, donde solicitan lo siguiente:**

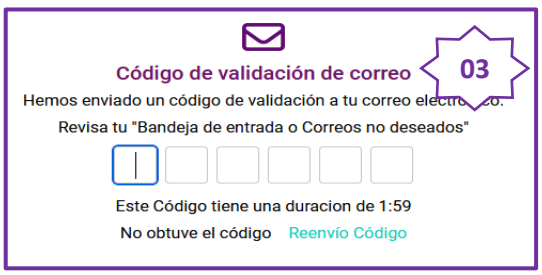
- Ingresar dirección de correo electrónico
- Registrar la clave del aplicativo Yape



Paso Nº02

Indica que se ha enviado un código de validación al número de teléfono:

- Solicita que registre el código de validación.



Paso Nº03

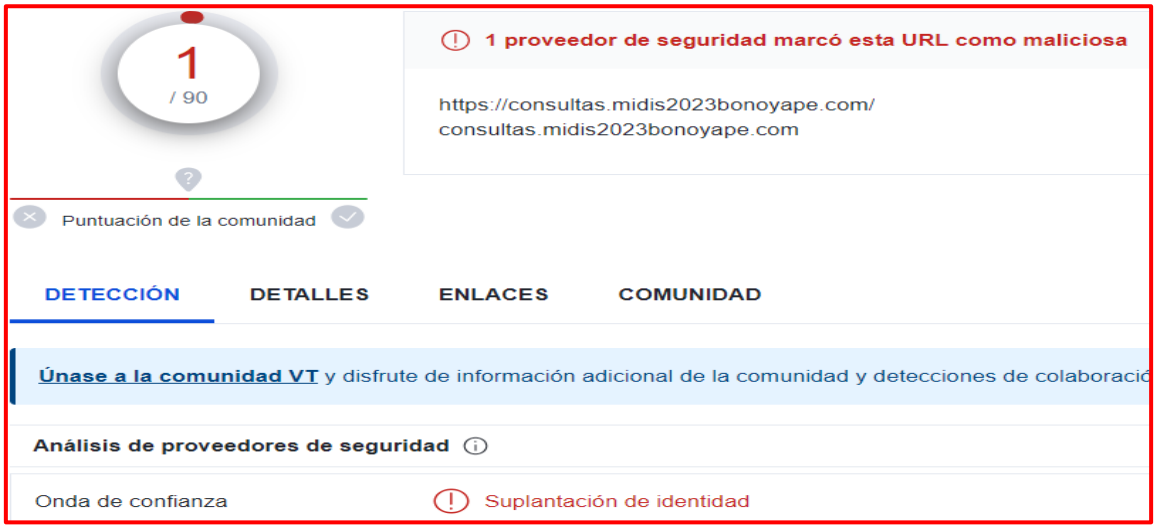
Indica que se ha enviado un código de validación al correo electrónico que se ha registrado:

- Solicita que registre el código de validación.

Paso Nº04

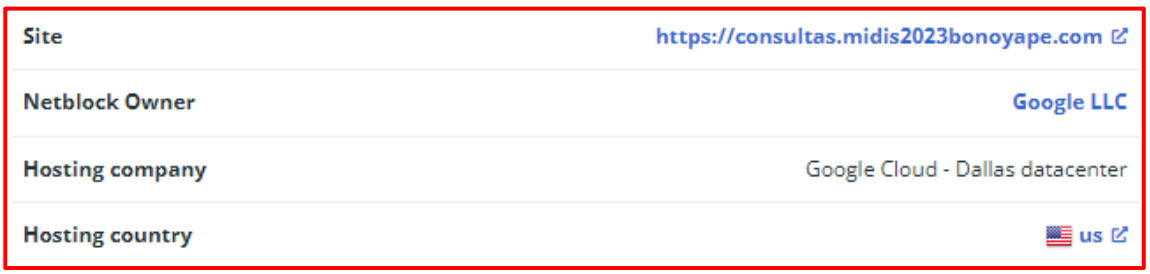
Una vez completado todos los pasos requeridos, el supuesto sitio web redirige de forma automática al sitio web del bono alimentario; sin embargo, los ciberdelincuentes ya obtuvieron los datos proporcionados por la víctima que luego son usados para realizar operaciones sin el consentimiento del titular.

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



B. Indicadores de compromiso (IoC)

- Dominio : midis2023bonoyape.com



- Servidor : nginx
- SHA-256 : aa7ae8ddbc7cfc029a113629fb38029724f334f4864eb8656d2436538301158b
- IP : 34[.]174[.]135[.]86

rango de IP	País	Nombre	Descripción
::ffff:0.0.0.0/96	Estados Unidos	IANA-IPV4-DIRECCIÓN ASIGNADA	Autoridad de asignación de números de Internet
↳ 34.0.0.0-34.255.255.255	Estados Unidos	NET34	Registro Americano de Números de Internet
↳ 34.128.0.0-34.191.255.255	Estados Unidos	GOOGL-2	Google LLC
↳ 34.174.135.86	Estados Unidos	GOOGL-2	Google LLC

C. Que es Phishing:

- Es una técnica de ingeniería social que usan los ciberdelincuentes para obtener información confidencial de los usuarios de forma fraudulenta y así apropiarse de la identidad de esas personas. Los ciberdelincuentes envían correos electrónicos falsos como anzuelo para "pescar" contraseñas y datos personales valiosos.

D. Apreciación de la información:

- La presente campaña de Phishing permite a los actores de amenazas obtener información bancaria del aplicativo móvil YAPE
- 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 seguir las instrucciones de sitio web sospechoso.
- 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.