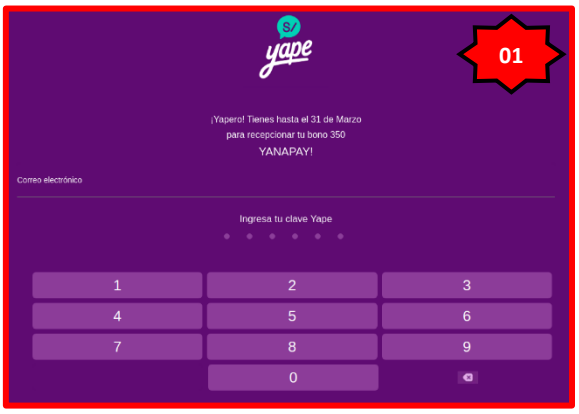
	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 070	Fecha: 22-03-2023
		Página 6 de 8

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Detección de sitio web fraudulento del bono Alimentario YANAPAY		
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 subfamilia	G02
Clasificación temática familia	Fraude		

Descripción

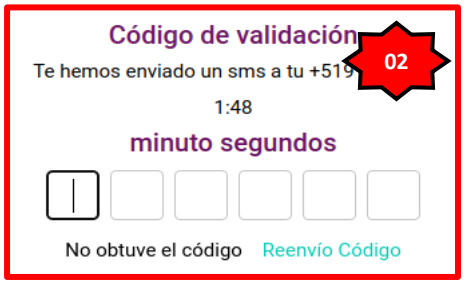
1. A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que actores de amenazas vienen llevando a cabo una campaña de Phishing, a través de los diferentes navegadores web, suplantando la identidad del aplicativo móvil "YAPE", indicando que la posible víctima tiene hasta el 31 de Marzo para recepcionar el apoyo económico otorgado por el Gobierno denominado "Bono 350 YANAPAY", con la finalidad de obtener información sensible de los usuarios como los datos del documento nacional de identidad (fecha de nacimiento, fecha de emisión), correo electrónico, numero de celular, Tarjetas de crédito o débito (número de tarjeta, fecha de caducidad y código de verificación de la tarjeta), etc.

2. Detalles del proceso del Phishing.



Paso N.º 01

Para acceder a la plataforma web fraudulenta de YAPE, solicitan a la víctima ingresar el correo electrónico y la clave para poder ingresar.



Paso N.º 02

Luego de colocar las credenciales, el atacante le enviara un código de validación aparentemente a su número de telefónico personal.

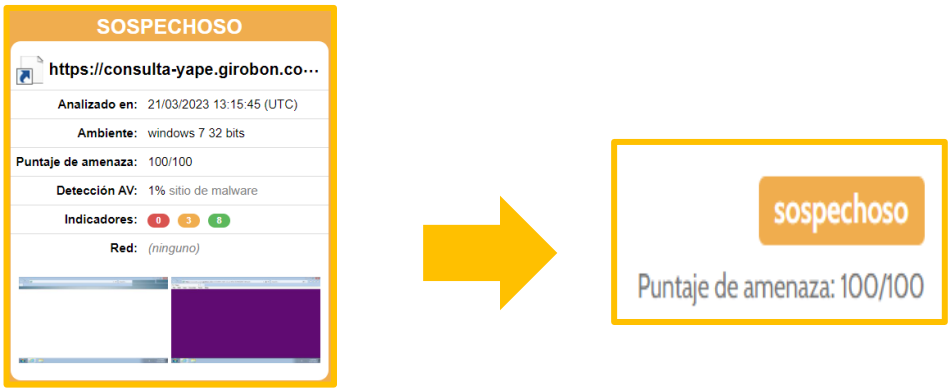
Paso N.º 03

Por último, Al colocar el código de validación, es redirigido al sitio oficial de la página web del Bono de 350, aludiendo un aparente error de autenticación; sin embargo, los datos ya fueron capturados.

La URL sospechosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, obteniendo como resultado como **PHISHING**

- **URL:** hxxps://consulta-yape[.]girobon[.]com/s/fe2b5931-fa93-44aa-92dd-b2092e3987d4/auth
- **Dominio:** girobon[.]com
- **IP:** 172[.]67[.]206[.]190
- **Servidor:** cloudflare
- **Tipo de contenido:** Texto/Html.
- **SHA-256:** 3dbde68b8c2a7fb6669427e5137f633d6efdf40d4de4ecd694241175a4c98ac8

- **OTRAS DETENCIONES**



3. Que es un Phishing:

Es un término informático que distingue a un conjunto de técnicas que persiguen el engaño a una víctima ganándose su confianza haciéndose pasar por una persona, empresa o servicio de confianza, para manipularla y hacer que realice acciones que no debería realizar.

4. Apreciación de la información:

- La presente campaña de Phishing, permite a los actores de amenazas obtener información de los beneficiarios del Bono "Yanapay" de S/ 350.00 Nuevos soles.

- La propagación del sitio web fraudulento se realiza mediante mensajes de textos SMS o a través de las aplicaciones de mensajería instantánea entre ellos WhatsApp, Telegram, Messenger.

5. Algunas Recomendaciones:

- Evitar acceder a enlaces que llegan inesperadamente por correo electrónico u otros medios.
- No proporcionar datos personales (contraseñas, tarjetas, cuentas bancarias, etc.) por correo, teléfono o SMS.
- Contar con una solución de seguridad confiable tanto en los dispositivos de escritorio como en teléfonos.
- Introducir datos personales únicamente en webs seguras.
- Ante cualquier sospecha de haber caído en el engaño del Phishing, accede a tu cuenta y cambia la contraseña.

Fuentes de información	▪ Análisis propio de redes sociales y fuente abierta