	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°242		Fecha: 12-10-2023
			Página: 11 de 14
Componente que reporta	DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ		
Nombre de la alerta	Detección de sitio web fraudulento del aplicativo 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		

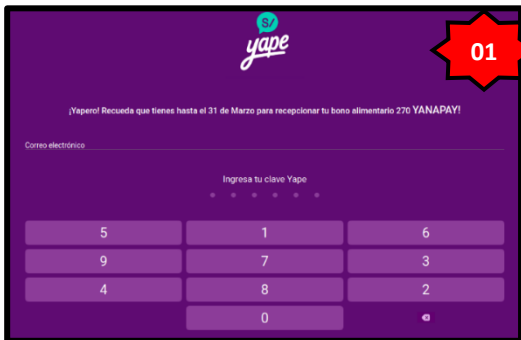
Descripción

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 el sitio web del bono alimentario de 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.

El Bono Alimentario, es un apoyo económico individual de S/ 270 para las personas mayores de edad que viven en pobreza y extrema pobreza, con el objetivo de reactivar su economía debido a la crisis económica.

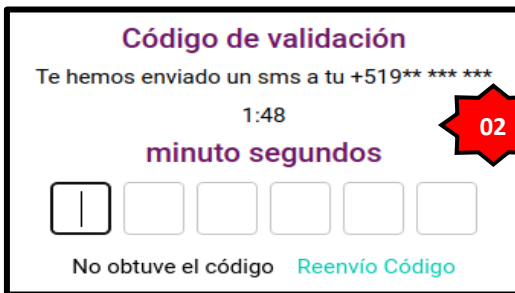
2. DETALLES:



01

Paso N.º 01

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



02

Paso N.º 02

Luego de colocar las credenciales, el atacante le enviara un código de validación aparentemente a su número telefónico personal, con la finalidad de ingresar a su APP de YAPE.



03

Paso N.º 03

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

A. La URL sospechosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, obteniendo como resultado que **NO SE ENCUENTRA REGISTRADA COMO PHISHING**



15 / 90

15 proveedores de seguridad marcaron esta URL como maliciosa

Reanalizar Buscar

https://ingresar-yape--emilioduran1810.repl.co/ Estado 429 Fecha del último a hace un momento

texto/html

Puntuación de la comunidad

DETECCIÓN DETALLES ENLACES COMUNIDAD 10+

Únase a la comunidad VT y disfrute de información adicional de la comunidad y detecciones colaborativas, además de una clave API para automatizar las com

Análisis de proveedores de seguridad ¿Quieres

Avira	Suplantación de identidad	BitDefender	Suplantación de identidad
Clúster25	Suplantación de identidad	CRDF	Malicioso
CyRadar	Malicioso	ESET	Suplantación de identidad
Fortinet	Suplantación de identidad	Datos G	Suplantación de identidad
Navegación segura de Google	Suplantación de identidad	Kaspersky	Suplantación de identidad

- URL: hxxps://ingresar-yape--emilioduran1810[.]repl[.]co/



Site	https://ingresar-yape--emilioduran1810.repl.co
Netblock Owner	Google LLC
Hosting company	Google
Hosting country	US

- Dominio: repl[.]co



Domain	repl.co
Nameserver	ns1.replit.com
Domain registrar	nic.co

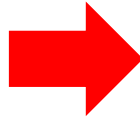
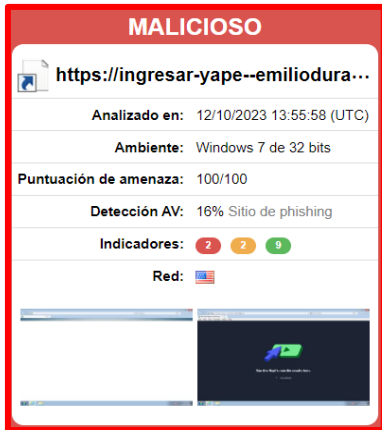
- IP: 35[.]186[.]245[.]55



IPv4 address (35.186.245.55)			
IP range	Country	Name	Description
::ffff:0:0:0/96	United States	IANA-IPV4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
35.0.0.0-35.255.255.255	United States	NET35	American Registry for Internet Numbers
35.184.0.0-35.191.255.255	United States	GOOGLE-CLOUD	Google LLC
35.186.245.55	United States	GOOGLE-CLOUD	Google LLC

- Código: 429
- Tipo de contenido: Texto/Html.
- SHA-256: 4b38c5790b96ecaeb627fa8cb22bcc1ee597b11c423c56f785915be540616197

B. OTRAS DETENCIONES



C. 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.

D. Apreciación de la información:

- La presente campaña de Phishing permite a los actores de amenazas obtener información de los beneficiarios del Bono alimentario “Yanapay” de S/ 270.00 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.

3. 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.

Fuente de Información:

Análisis propio de redes sociales y fuente abierta.