	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°038	Fecha: 13-02-2024
		Página: 10 de 13

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 vienen llevando a cabo una 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 01: Sitio web fraudulento que suplanta la identidad de Amazon, solicita a la víctima, registrar el correo electrónico o teléfono.

IMAGEN 02: Una vez ingresado el correo electrónico y hecho clic en <continuar>, requiere ingresar la contraseña para continuar con el acceso.

IMAGEN 03: Luego solicita actualizar el método de pago donde te solicita ingresar datos bancarios como nombre, número de tarjeta, fecha de vencimiento, número de teléfono, código postal y de seguridad.

IMAGEN 04: Por último, el sitio web solicita a la víctima registrar **la contraseña de la dirección de correo electrónico (gmail)**; donde al dar clic en continuar, redirige a la página web oficial de "Amazon" (siendo capturados todos los datos registrados)

*Se precisa que los ciberdelincuentes obtienen dos cuentas siendo la primera la compañía de comercio electrónico "AMAZON y la segunda el servicio de correo electrónico gratuito Gmail, proporcionado por el motor de búsqueda Google.

A. Comparación del sitio web oficial y fraudulento

SITIO OFICIAL

https://www.amazon.com/

SITIO FRAUDULENTO

http://hgz.ahr.mybluehost.me/amazion

Existe similitud entre ambos sitios web, en logotipo, fondo y escritura, pero la diferencia es que las URL son distintas.

B. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, obteniendo la siguiente información:

- **URL Malicioso:** hxxp://hgz[.]ahr[.]mybluehost[.]me[/]amazion

Site	http://hgz.ahr.mybluehost.me
Netblock Owner	Unified Layer
Hosting company	Newfold Digital
Hosting country	US

- **Dominio:** mybluehost[.]me

Domain	mybluehost.me
Nameserver	ns1.bluehost.com
Domain registrar	nic.me
Nameserver organisation	whois.domain.com

- **IP:** 162[.]241[.]244[.]85

IPv4 address (162.241.244.85)

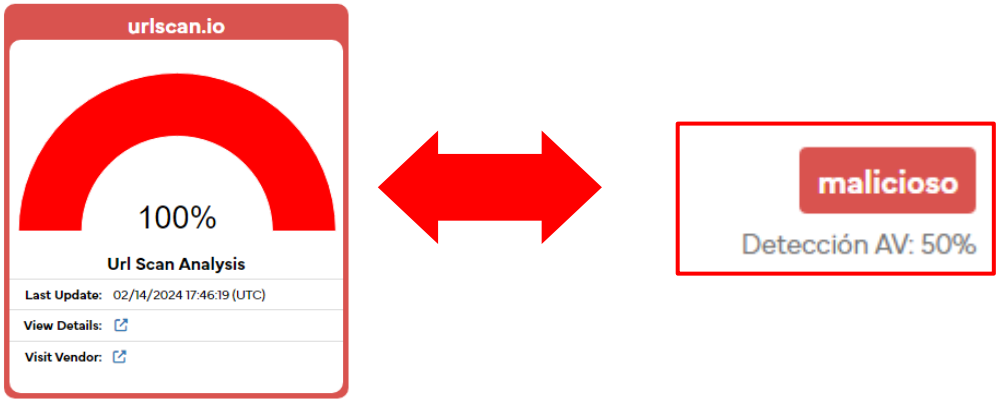
IP range	Country	Name	Description
::ffff:0.0.0.0/96	United States	IANA-IPV4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
↳ 162.0.0.0-162.255.255.255	United States	NET162	Various Registries (Maintained by ARIN)
↳ 162.240.0.0-162.241.255.255	United States	UNIFIEDLAYER-NETWORK-16	Unified Layer
↳ 162.241.244.85	United States	UNIFIEDLAYER-NETWORK-16	Unified Layer

- **SHA256:** f6173b04725ca4139fe136303416e2864fe4cc52a993c9101d231efc73781338

C. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, siendo catalogado como **SUPLANTACIÓN DE IDENTIDAD** en quince (15) y **MALICIOSO** en cinco (05)- – **PHISHING:**

alfaMontaña.ai	Suplantación de identidad	Avira	Suplantación de identidad
BitDefender	Suplantación de identidad	Clúster25	Suplantación de identidad
CRDF	Malicioso	CyRadar	Malicioso
Emsisoft	Suplantación de identidad	ESET	Suplantación de identidad
Buscador de amenazas Forcepoint	Suplantación de identidad	Fortinet	Suplantación de identidad
Datos G	Suplantación de identidad	Kaspersky	Suplantación de identidad
leonico	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	Suplantación de identidad	raiz web	Malicioso

D. Otras detecciones:



E. 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.).

F. 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:

- Verificar la información en la entidad 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.
- Mantener instalado un servicio de antivirus en el dispositivo.

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