	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°174	**Fecha: 24-07-2023**
		Página: 11 de 14

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de Alerta	Suplantación de la compañía de comercio electrónico "AMAZON"		
Tipo de Ataque	Phishing	Abreviatura	Phishing
Medio de Propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de Subfamilia	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 unas campañas de Phishing, suplantando la identidad de la compañía de comercio electrónico "Amazon", con la finalidad de robar credenciales de acceso de los usuarios, datos personales y cuentas bancarias vinculadas.

2. **DETALLES:**
   Proceso de estafa del Phishing.

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/

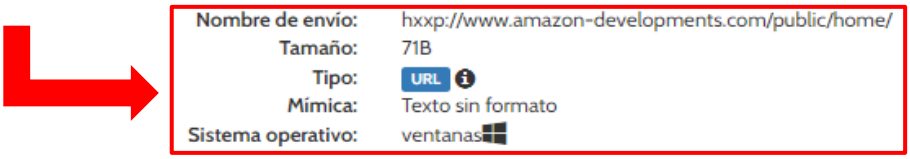
SITIO FRAUDULENTO

hxxps:// www[.]amazon-developments[.]com/public/home

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

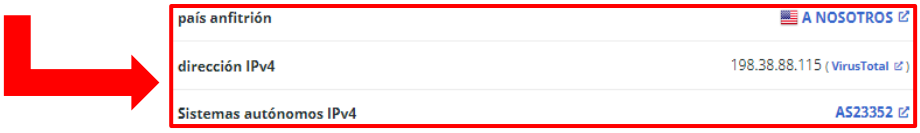
B. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, obteniendo la siguiente información:

- **URL Malicioso:** hxxps[:]www[.]amazon-developments[.]com/public/home/

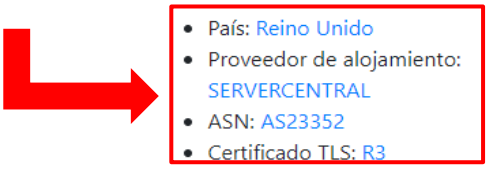


- **Dominio:** amazon-desarrollos[.]com

- **IP:** 198[.]38[.]88[.]115



- **Proveedor de Alojamiento:** SERVERCENTRAL

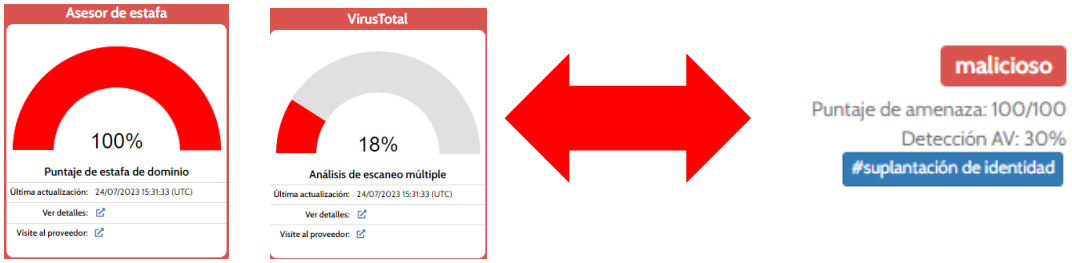


- **SHA 256:** a4c4e1a6f2571f166d68795705a796c2b7c7c0c6a96a1cc1d59d2c51326cf479

C. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, siendo catalogado como **SUPLANTACIÓN DE IDENTIDAD** en nueve (09), **MALICIOSA** en tres (03) y **MALWARE** dos (02) de ellas- **– PHISHING:**

alphaMountain.ai	Suplantación de identidad	AlphaSOC	Suplantación de identidad
Avira	Suplantación de identidad	BitDefender	Malware
Clúster25	Suplantación de identidad	CRDF	Malicioso
CyRadar	Malicioso	ESET	Suplantación de identidad
Buscador de amenazas de Forcepoint	Suplantación de identidad	G-datos	Malware
kaspersky	Suplantación de identidad	Leonico	Suplantación de identidad
Base de datos de phishing	Suplantación de identidad	seguro para abrir	Suplantación de identidad
Búsqueda segura	Malicioso	Sophos	Suplantación de identidad
VIPRE	Malicioso	raíz web	Malicioso

D. Otras detecciones:



3. RECOMENDACIONES:

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

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