

| | | | |
|---|--|--------------------------|----------|
|  | ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°158 | Fecha: 05-07-2023 | |
| | | Página: 24 de 28 | |
| Componente que reporta | DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ | | |
| Nombre de la alerta | Detección de una nueva campaña de Phishing a 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 | G02 |
| Clasificación temática familia | Fraude | | |
| Descripción | | | |

1. ANTECEDENTES:

A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, los ciberdelincuentes se encuentran desarrollando una nueva campaña de Phishing, a través de los diferentes navegadores web, quienes vienen suplantando la identidad de Amazon (Plataforma de comercio electrónico), con el objetivo robar credenciales de acceso, datos personales y bancarios del usuario.

2. DETALLES:



Imagen 1: Sitio web falso de Amazon solicita a la víctima, ingresar el correo electrónico, para continuar.



Imagen 2: Luego de haber ingresado el correo electrónico, requiere la contraseña, para iniciar sesión.



Imagen 3: Al ingresar, se visualizará un formulario, en el cual solicitará ingresar los datos personales del usuario.

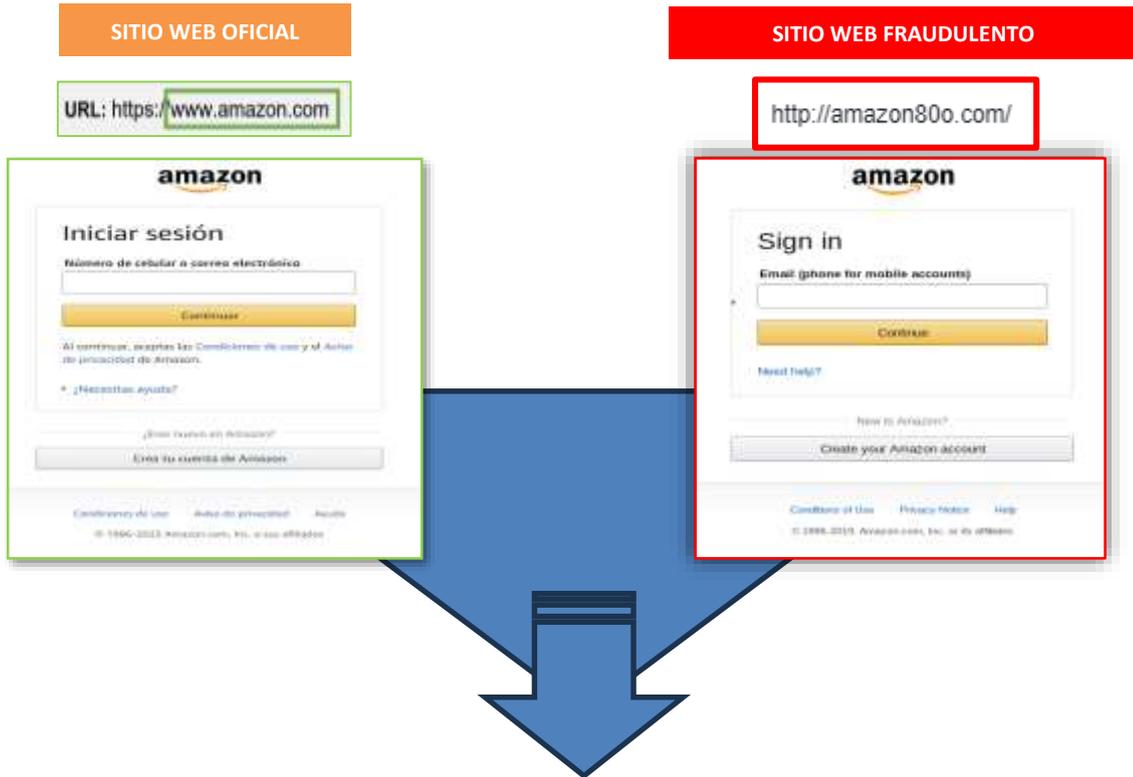


Imagen 5: Finalmente, es redirigido al sitio web oficial de Amazon, aludiendo un aparente error de autenticación; sin embargo, los datos fueron capturados por los ciberdelincuentes.



Imagen 4: Después de haber completado toda la información personal y/o bancario, requiere enlazar el correo electrónico ingresando la contraseña.

3. Comparación del sitio web oficial y fraudulento.



- Existe una diferencia entre la URL original y la URL fraudulenta.
- La URL falsa utiliza protocolo HTTPS, no significa que la web sea segura.
- Existe una similitud entre ambas páginas, en imagen, fondo y colores de ambos sitios web.

4. URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, siendo catalogado como SUPLANTACIÓN DE IDENTIDAD en ONCE (11) y MALICIOSOS en NUEVE (09).

| | | | |
|------------------------------------|-----------------------------|-------------------|-----------------------------|
| alphaMountain.ai | ① Suplantación de identidad | AlphaSOC | ① Suplantación de identidad |
| Avira | ① Suplantación de identidad | BitDefender | ① Malware |
| Clúster25 | ① Suplantación de identidad | CRDF | ① Malicioso |
| CyRadar | ① Malicioso | ESET | ① Suplantación de identidad |
| Buscador de amenazas de Forcepoint | ① Suplantación de identidad | Fortinet | ① Suplantación de identidad |
| G-datos | ① Malware | Seguridad Heimdal | ① Suplantación de identidad |
| kaspersky | ① Suplantación de identidad | Leonico | ① Suplantación de identidad |

a) Indicadores de compromisos:

I. URL: hxxp://amazon80o.com/



| | |
|----------------------------|---------------------------|
| Nombre de envío: | hxxp://amazon80o.com/ |
| Tamaño: | 45B |
| Tipo: | URL ⓘ |
| Mímica: | Texto sin formato |
| Sistema operativo: | ventanas |
| Último análisis antivirus: | 05/07/2023 19:55:18 (UTC) |
| Último informe de | 05/07/2023 19:54:45 (UTC) |

II. IP: 216.[.83[.]41[.]88



| | | | |
|-------------------------------|----------------------------|---------------------------------------|---|
| Site | http://amazon80o.com | Dominio | amazon80o.com |
| Propietario de bloque de red: | EstvNet LLC | Nombre del servidor: | rakumar.mars.onionboe-dns.com |
| Compañía anfitriona | Estv.net | registrar de dominio | PublicDomainRegistry.com |
| país anfitrión | ANDSOTROS LT | Organización del servidor de nombres: | whois.PublicDomainRegistry.com |
| Dirección IPv4 | 216.33.41.88 (FreeHost IP) | Organización | Privacy Protect, LLC (PrivacyProtect.org), 10 Corporate Drive, Burlington, 01803, EE. UU. |
| Sistemas autónomos IPv4: | AS64056 IT | administrador de DNS | glenderja33@gmail.com |

III. SHA-256: 76af2c357b43fd38d5a4d48a7f5cf3df6dc41a46c43f732f15baf9f352d97113
IV. SERVIDOR: nginx

5. Otras detecciones:

Asesor de estafa

100%

Puntaje de estafa de dominio

Última actualización: 05/07/2023 19:55:18 (UTC)

Ver detalles: [🔗](#)

Visite al proveedor: [🔗](#)

MALICIOSO

http://amazon80o.com/

Analizado en: 05/07/2023 19:54:45 (UTC)

Ambiente: windows 7 32 bits

Puntaje de amenaza: 100/100

Detección AV: 22% Sitio de phishing

Indicadores: 🔴 🟡 🟢

Red: 🇺🇸



malicioso

Puntaje de amenaza: 100/100

Detección AV: 41%

#suplantación de identidad

6. 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 legítima (organismo público o privado, entidad financiera, servicio técnico, etc.).

7. 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.

8. Algunas Recomendaciones:

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

Fuente de Información:

Análisis propio de redes sociales y fuente abierta