Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°161	Fecha: 11-07-2024
		Página: 4 de 9

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	El riesgo con Amazon Prime Day: Usuarios reportan que ciberdelincuentes engañan con links falsos		
Tipo de Ataque	Portal fraudulento	Abreviatura	PortalFrau
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 medida que nos acercamos al Amazon Prime Day del 16 al 17 de julio de 2024, los compradores online anticipan con impaciencia ofertas increíbles y exclusivas.

Además de presentar las llamadas ofertas "flash" (gangas por un periodo determinado de tiempo), rebajas en suscripciones, nuevos lanzamientos a precios reducidos y ofertas de todo tipo en artículos.

El pasado año, los clientes Prime lograron ahorrar más de 2.500 millones de dólares en este día en los más de 375 millones de artículos que adquirieron. Ese fue el Prime Day más importante de la historia.

En medio de tanto entusiasmo, existe un riesgo subyacente, los cibercriminales, para quienes se abre una puerta donde pueden realizar ataques de phishing. Estos atacantes emplean tácticas engañosas, como enviar correos electrónicos falsos o crear sitios web fraudulentos, con el objetivo de robar información personal o credenciales financieras.

2. DETALLES:

Cuando se acerca el famoso día, la compañía de seguridad Check Point ha detectado un aumento significativo en los ciberataques relacionados con la marca Amazon. Durante este mes de junio, surgieron más de 1.230 nuevos dominios asociados con Amazon, de los cuales el 85% fueron marcados como maliciosos o sospechosos de serlo.

Estos dominios fraudulentos imitan a la perfección las páginas legítimas de la plataforma de comercio, engañando a los usuarios para que ingresen sus credenciales de inicio de sesión y datos personales.

Algunos ejemplos de estos nuevos sitios maliciosos creados son:

- amazon-onboarding[.]com es un sitio fraudulento recientemente registrado, diseñado como una página de phishing que se hace pasar por Amazon y que apunta específicamente a credenciales relacionadas con el transportista.
- amazonmxc[.]shop es un sitio web falsificado de Amazon México, diseñado como una réplica de amazon.com.mx. Cuenta con un botón de inicio de sesión de perfil en la esquina superior derecha que, al hacer clic, recopila las credenciales de inicio de sesión de los usuarios.
- amazonindo[.]com es un sitio web fraudulento de Amazon. Dispone de un botón de inicio de sesión/registro de perfil en la esquina superior derecha que, al hacer clic, recopila las credenciales de inicio de sesión de los usuarios.

Indicadores de Compromiso asociado a Sitios Web Fraudulentos:

- shopamazon2[.]com
- microsoft-amazon[.]shop
- amazonapp[.]nl
- shopamazon3[.]com
- amazon-billing[.]top
- amazonshop1[.]com
- fedexamazonus[.]top
- amazonupdator[.]com

- amazon-in[.]net
- espaces-amazon-fr[.]com
- usiamazon[.]com
- amazonhafs[.]buzz
- usps-amazon-us[.]top
- amazon-entrega[.]info
- amazon-vip[.]xyz
- paqueta-amazon[.]com
- connect-amazon[.]com
- user-amazon-id[.]com
- amazon762[.]cc
- amazoneuroslr[.]com
- amazonw-dwfawpapf[.]top
- amazonprimevideo[.]com

Los ataques de phishing no se limitan a sitios web fraudulentos. En junio de 2024, se descubrió una campaña de phishing que distribuía archivos maliciosos bajo el nombre de Amazon con el siguiente hash MD5: 39af8a116a252a8aaf2328e661b2d5a2. Un archivo de ejemplo se llamaba Mail-AmazonReports-73074[264].pdf.

Estos archivos informaban a las víctimas de que su cuenta había sido suspendida debido a problemas con la información de facturación, instándolas a actualizar sus datos de pago a través de un enlace de phishing que dirigía a una página web fraudulenta: trk[.]klclick3[.]com.

El mensaje amenaza con el cierre de la cuenta si no se toman medidas inmediatas, creando una sensación de urgencia para incitar al usuario a responder rápidamente, por temor a la exposición de sus datos o la cancelación de la cuenta como consecuencia del incumplimiento.

3. RECOMENDACIONES:

- Revisar las URL con cuidado. Tener cuidado con los errores ortográficos o con los sitios que utilizan un dominio de nivel superior diferente (por ejemplo, .co en lugar de .com).
- Crear contraseñas seguras asegurándose que sea indescifrable antes del Prime Day.
- Verificar que la URL comience con “https://” y que haya un ícono de candado en la barra de direcciones. Esto acerca a una conexión segura y encriptada.
- Evitar compartir datos personales innecesarios, como su fecha de nacimiento o número de seguro social, con minoristas en línea.
- Tener cuidado con los correos electrónicos. Los ataques de phishing a menudo utilizan un lenguaje urgente para engañarlo y hacer que haga clic en enlaces o descargue archivos adjuntos. Verificar siempre la fuente.
- Ser Escéptico ante acuerdos poco realistas.
- Preferir las tarjetas de crédito a las de débito para realizar compras en línea, ya que ofrecen una mejor protección y menos responsabilidad en caso de robo.

Fuente de Información:	• hxxps://www.escudodigital.com/ciberseguridad/amazon-prime-day-mucho-cuidado-ciberdelincuentes-te-estan-esperando_59682_102.html • hxxps://www.infobae.com/tecno/2024/07/10/el-riesgo-con-amazon-prime-day-usuarios-reportan-que-ciberdelincuentes-enganan-con-links-falsos/ • hxxps://www.noticiassuper.com/2024/07/10/amazon-prime-day-2024-los-ciberdelincuentes-estan-preparados-y-tu/ • hxxps://computerhoy.com/ciberseguridad/ciberdelincuentes-miran-amazon-debes-protegerte-no-caer-estafas-prime-day-1395198