PERÚ | Presidencia del Consejo de Ministros | Secretaría de Gobierno y Transformación Digital

Siempre con el pueblo

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Centro Nacional de Seguridad Digital

asbanc

Lima, 28 de julio de 2022

N° 203-2022-CNSD

La presente **Alerta Integrada de Seguridad Digital** corresponde a un análisis técnico periódico realizado por el Comando Conjunto de las Fuerzas Armadas, el Ejército del Perú, la Marina de Guerra del Perú, la Fuerza Aérea del Perú, la Dirección Nacional de Inteligencia, la Policía Nacional del Perú, la Asociación de Bancos del Perú y el Centro Nacional de Seguridad Digital de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, en el marco de la Seguridad Digital del Estado Peruano.

El objetivo de esta alerta **es informar a los responsables de la seguridad digital de las entidades públicas y las empresas privadas sobre las amenazas en el entorno digital** para advertir las situaciones que pudieran afectar la continuidad de sus servicios en favor de la población.

Las marcas y logotipos de empresas privadas y/o entidades públicas se reflejan para ilustrar la información que los ciudadanos reciben por redes sociales u otros medios y que atentan contra la confianza digital de las personas y de las mismas empresas **de acuerdo con lo establecido por el Decreto de Urgencia 007-2020**.

La presente Alerta Integrada de Seguridad Digital es información netamente especializada para informar a las áreas técnicas de entidades y empresas.

Contenido

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 203	Fecha: 28-07-2022
		Página 04 de 07

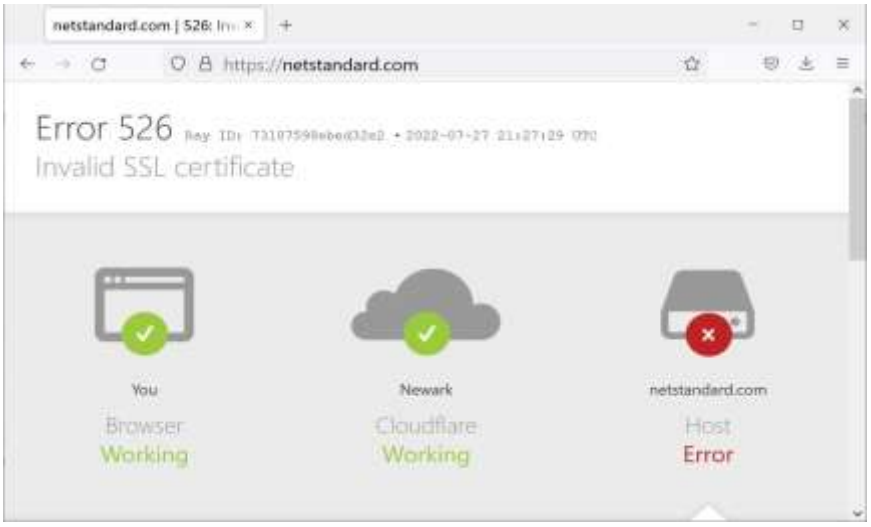
Componente que reporta	**CENTRO DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ**		
Nombre de la alerta	MSP de Kansas cierra los servicios en la nube para defenderse de los ataques cibernéticos		
Tipo de ataque	Malware	Abreviatura	Malware
Medios de propagación	Correo electrónico, redes sociales, entre otros		
Código de familia	C	Código de Subfamilia	C01
Clasificación temática familia	Código Malicioso		

Descripción

A través del monitoreo y búsqueda de amenazas en el ciberespacio del día 27 de Julio del 2022, se tomó conocimiento de un proveedor de servicios administrados estadounidense NetStandard sufrió un ataque cibernético que provocó que la compañía cerrara sus servicios en la nube MyAppsAnywhere, que consisten en servicios alojados de Dynamics GP, Exchange, Sharepoint y CRM.

SITUACIÓN:

Según un correo electrónico enviado a los clientes de MyAppsAnywhere compartido en Reddit, la compañía detectó signos de un ataque cibernético el martes por la mañana y cerró rápidamente los servicios en la nube para evitar la propagación del ataque. La compañía que ha contratado a su proveedor de seguros para ayudar a identificar la fuente del ataque y volver a poner los sistemas en línea. Si bien la compañía dice que solo los servicios de MyAppsAnywhere se ven afectados, el ataque parece haber tenido un impacto más amplio, con el sitio principal de la compañía cerrado también.



La compañía ha estado organizando llamadas de Zoom cada hora para actualizar a los clientes sobre las interrupciones, y BleepingComputer dijo que la compañía ahora está comprometida con una firma de ciberseguridad de terceros proporcionada por su compañía de seguros.

Como NetStandard no comparte más detalles, no está claro qué tipo de ataque se ha producido. Sin embargo, los investigadores de seguridad creen que esto es probablemente un ataque de ransomware, como comúnmente vemos con ataques cibernéticos como el de NetStandard.

RECOMENDACIONES:

- No abrir correos electrónicos de remitentes desconocidos o irrelevantes.
- Evite abrir enlaces y archivos adjuntos de correo electrónico que no sean de confianza sin verificar primero su autenticidad.
- Utilizar soluciones antivirus de renombre en sus dispositivos conectados, incluidos PC, portátiles y dispositivos móviles.
- Tener actualizado el Sistema Operativo.

Fuentes de información	▪ https://www.bleepingcomputer.com/news/security/kansas-msp-shuts-down-cloud-services-to-fend-off-cyberattack/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 203	Fecha: 28-07-2022
		Página 05 de 07

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 Subfamilia	G02
Clasificación temática familia	Fraude		

Descripción

1. A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, los ciberdelincuentes se 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, el cual indican que el centro de facturación de la empresa requiere una verificación de actualización de datos bancarios de la posible víctima, como nombre y número la de tarjeta, fecha de vencimiento, código de seguridad, entre otros.

2. **Imagen**: Proceso del ataque Phishing:

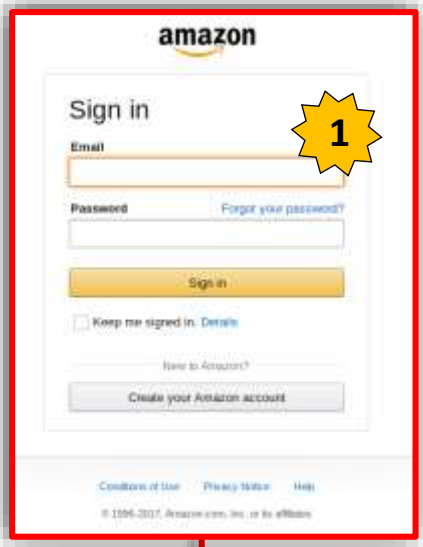


Imagen 1: Solicita dirección de correo electrónico y contraseña.

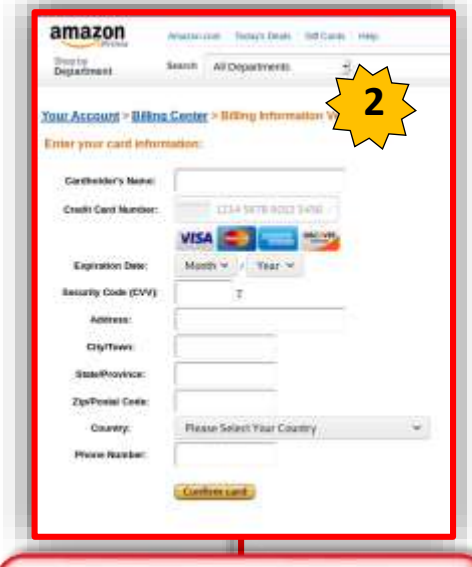


Imagen 2: Una vez hecho clic en <iniciar sesión> redirige a una supuesta página de Amazon, donde pide ingresar datos bancarios, a fin de realizar una verificación de cuenta.

Imagen 3: Luego, Indica que se ha confirmado con éxito la información de la cuenta bancaria.

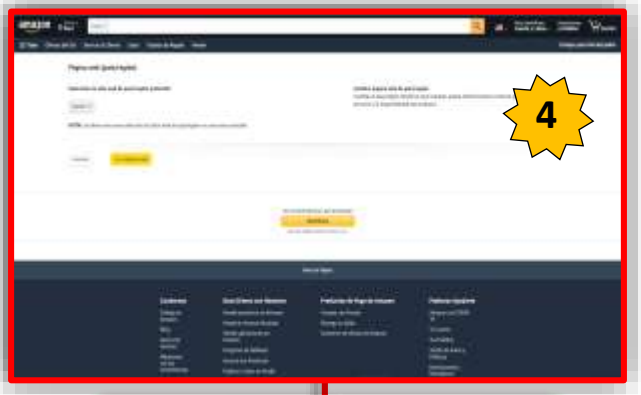


Imagen 4: Por último, es redirigido automáticamente a un supuesto sitio web de Amazon, donde la víctima puede verificar una serie de consultas como se aprecia en la imagen.

3. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, siendo catalogado como **SUPLANTACIÓN DE IDENTIDAD:**
   - **INDICADORES DE COMPROMISO:**
     - ✓ **URL:** hxxps[:]//neverwalkaolnh[.]ml[/]suythg[/]mazon[/]f039d
     - ✓ **Dominio:** nuncawalkaolnh[.]ml
     - ✓ **IP:** 213[.]165[.]239[.]54
     - ✓ **Código:** 200
     - ✓ **Longitud:** 167.65 KB
     - ✓ **SHA-256**: 6adc256f673f73a8cf0aade3b0cbcf5dd905a604f3fd341bf615503e80141ca9

   - **OTRAS DETECCIONES:**

4. **ALGUNAS 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.

Fuentes de información	▪ Análisis propio de redes sociales y fuente abierta

Índice alfabético