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

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Centro Nacional de Seguridad Digital

asbanc
ASOCIACIÓN DE BANCOS DEL PERÚ

Lima, 12 de noviembre de 2023

270-2023-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

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°270	Fecha: 12-11-2023
		Página: 4 de 8

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Servicios financieros de ICBC afectado por LockBit 3.0		
Tipo de Ataque	Ransonware	Abreviatura	Ransonware
Medios de propagación	Correo electrónico, redes sociales, entre otros		
Código de familia	C	Código de Sub familia	C01
Clasificación temática familia	Código Malicioso		

Descripción

1. ANTECEDENTES:

El Banco Industrial y Comercial de China, el mayor prestamista del mundo por activos totales, capitalización de mercado y depósitos de clientes, anunció que su división de servicios financieros, llamada ICBC Financial Services, contuvo un ataque de ransomware que perturbó el mercado del Tesoro de EE. UU. y afectó algunas transacciones de renta fija y acciones.

El experto en seguridad Kevin Beaumont le dijo a BleepingComputer que la infraestructura de ICBC alojaba un servidor Citrix vulnerable al ataque 'Citrix Bleed'. El servidor se desconectó después del ataque.

En octubre, Citrix instó a los administradores a proteger todos los dispositivos NetScaler ADC y Gateway contra la vulnerabilidad CVE-2023-4966, que se explota activamente en los ataques.

El 10 de octubre, Citrix publicó un boletín de seguridad relacionado con una vulnerabilidad crítica, rastreada como CVE-2023-4966, en dispositivos Citrix NetScaler ADC/Gateway.

Los investigadores de Mandiant observaron la explotación de esta vulnerabilidad como día cero desde finales de agosto.

2. DETALLES:

Este ciberataque interrumpió la negociación de bonos del Tesoro. Por eso, el jueves, las operaciones manejadas por el banco más grande del mundo en el mercado más grande del mundo atravesaron Manhattan en una memoria USB.

Inmediatamente después de descubrir el ataque, ICBC "aisló los sistemas afectados para contener el incidente" dijo el banco estatal.

"El ataque impidió a ICBC FS liquidar operaciones del Tesoro en nombre de otros participantes del mercado, según comerciantes y bancos, y algunas operaciones de acciones también se vieron afectadas".

Los fondos de cobertura, los administradores de activos y otros participantes del mercado desviaron las operaciones debido al impacto del ataque a la liquidez del mercado de bonos del Tesoro. Fuentes comerciales confirmaron que el mercado en general continúa operando a pesar del incidente de seguridad.

ICBC dijo que "comprobó con éxito" las operaciones del Tesoro estadounidense ejecutadas el miércoles y las operaciones de financiación de repos realizadas el jueves. Un repo es un acuerdo de recompra, un tipo de préstamo a corto plazo para los comerciantes de bonos gubernamentales.

Sin embargo, varios medios de comunicación informaron que hubo interrupciones en las operaciones con los bonos del Tesoro de Estados Unidos. El Financial Times, citando a comerciantes y bancos, dijo el viernes que el ataque de ransomware impidió a la división ICBC liquidar transacciones del Tesoro en nombre de otros participantes del mercado.

ICBC no reveló quién estuvo detrás del ataque, pero dijo que ha estado "llevando a cabo una investigación exhaustiva y está avanzando en sus esfuerzos de recuperación con el apoyo de su equipo profesional de expertos en seguridad de la información"

Marcus Murray, fundador de la firma sueca de ciberseguridad Truesec, dijo que el ransomware utilizado se llama LockBit 3.0. Murray dijo que esta información proviene de fuentes relacionadas con Truesec, pero no pudo revelar quiénes son esas fuentes por razones de confidencialidad. El Financial Times informó, citando dos fuentes, que LockBit 3.0 también era el software detrás del ataque.

El equipo de ciberseguridad de VMware dijo en un blog el año pasado que LockBit 3.0 es un "desafío para los investigadores de seguridad porque cada instancia del malware requiere una contraseña única para ejecutarse, sin la cual el análisis es extremadamente difícil o imposible".

LockBit es la variedad de ransomware más popular y representa alrededor del 28% de todos los ataques de ransomware conocidos entre julio de 2022 y junio de 2023, según datos de la empresa de ciberseguridad Flashpoint.

Además, Mandiant indica que los actores de amenazas explotaron la vulnerabilidad CVE-2023-4966 para secuestrar sesiones autenticadas existentes y eludir la autenticación multifactor u otros requisitos de autenticación estrictos. Los investigadores advierten que estas sesiones pueden persistir después de que se haya implementado la actualización para mitigarla.

Mandiant también observó que los actores de amenazas secuestraban sesiones en las que los datos de la sesión fueron robados antes de la implementación del parche y posteriormente utilizados por el actor de amenazas.

3. RECOMENDACIONES:

- Hacer uso del doble factor de autentificación.
- Evitar abrir archivos adjuntos o enlaces sospechosos en correos electrónicos no solicitados o mensajes de redes sociales.
- Ejecutar la estrategia 3-2-1 de copias de seguridad, que consiste en realizar tres copias de seguridad de los datos, en mínimo dos medios de almacenamiento diferentes, y albergar una de las copias fuera del sitio o en la nube.
- Cifrar las copias realizadas. Así, incluso si se ven comprometidas, serían indescifrables e inútiles para el atacante.
- Mantener siempre actualizados los programas, tanto en los dispositivos como en los servidores, para evitar que los atacantes aprovechen las vulnerabilidades y se infiltren en su red.
- Utilizar un software antivirus confiable y mantenerlo activo y actualizado.
- Centrar la estrategia de defensa en la detección de movimientos laterales y el bloqueo de actividades fraudulentas de transferencia de datos confidenciales a Internet (fuga de informaciones). Es importante prestar especial atención al tráfico saliente para detectar las conexiones de los ciberdelincuentes en su red.
- Segmentar las redes para proteger mejor los sistemas críticos.
- Evaluar el uso de una red privada virtual (VPN) para prevenir la vulnerabilidad de servicios expuestos.
- Procurar la gestión de un plan que incluya detección, investigación y respuesta a amenazas 24/7, ya sea internamente o en asociación con un proveedor especializado de servicios de detección y respuesta gestionadas.
- En caso de infección, no pagar el rescate ni contactar con los ciberdelincuentes, ya que no hay garantía de que cumplan sus promesas. En su lugar, buscar ayuda profesional para eliminar el ransomware y restaurar los archivos cifrados.

Fuente de Información:	• hxxps://blog.segu-info.com.ar/2023/11/servicios-financieros-icbc-afectado-por.html • hxxps://securityaffairs.com/153986/hacking/icbc-ransomware-attack.html

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°270	Fecha: 12-11-2023
		Página: 6 de 8

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 se encuentran desarrollando una nueva 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:**

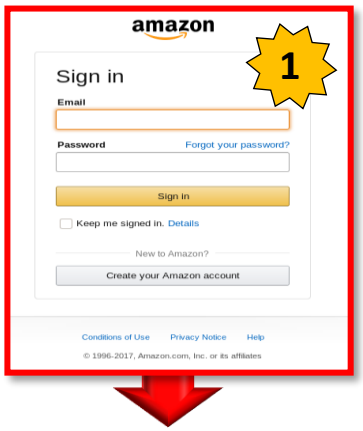


Imagen 1: Solicita dirección de correo electrónico y contraseña.

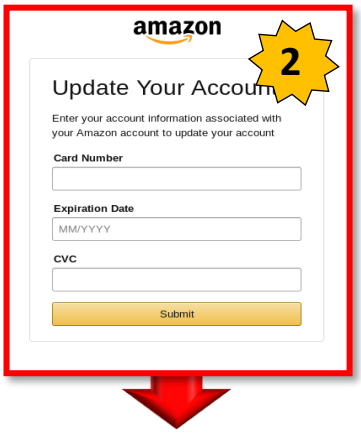


Imagen 2: Solicita datos bancarios como el número de tarjeta, fecha de caducidad y el CVC de la tarjeta.

Imagen 3: Solicita datos personales fecha de nacimiento, número telefónico, ciudad y más.

Imagen 4: Solicita ingresar las credenciales de acceso de la página (usuario y contraseña).

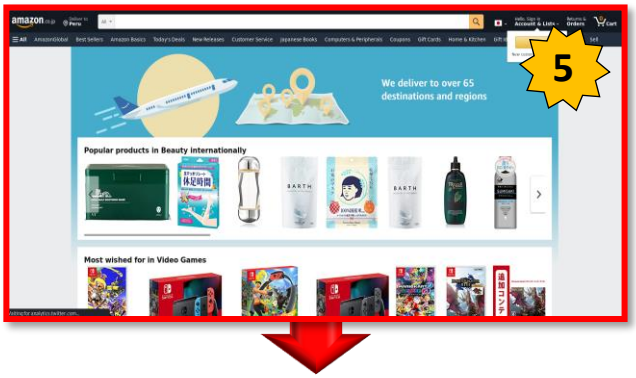


Imagen 5: Por último, es redirigido automáticamente a un supuesto sitio web de Amazon, donde la víctima puede verificar una serie de consultas como se aprecia en la imagen.

A. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, siendo catalogado como **SUPLANTACIÓN DE IDENTIDAD:**

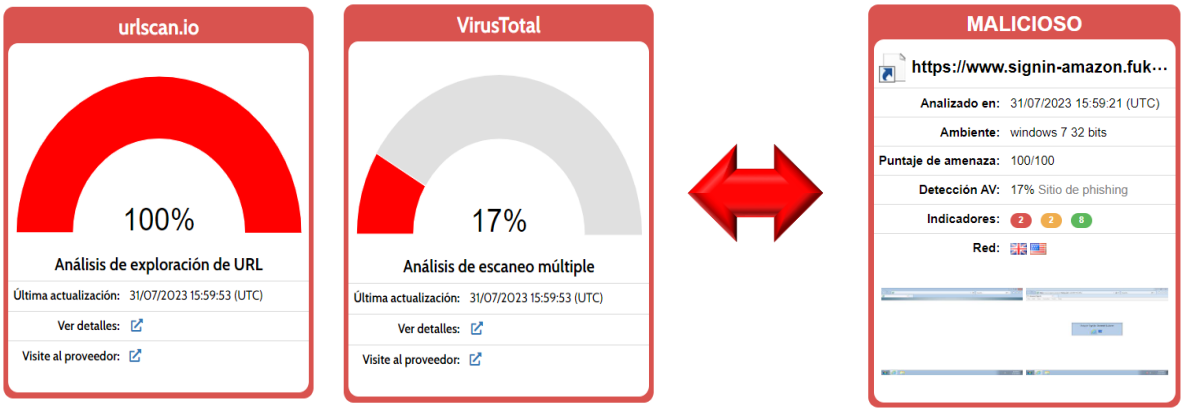
a) Indicadores de compromisos:

- **URL:** hxxps[:]//www[.]signin-amazon[.]fukrey[.]net/cadc696759cc67a/
- **SHA-256:** aa8382efb85b68185d7dcf13ecbbe6acf1df7ad3a7c1b0b68d9b59a91a9e185c
- **IP:**31[.]22[.]4[.]93

B. Se hallaron **16 proveedores** de seguridad que marcaron este dominio como malicioso.

AlphaSOC	Phishing	Avira	Phishing
BitDefender	Phishing	CyRadar	Malicious
Emsisoft	Phishing	ESET	Phishing
Forcepoint ThreatSeeker	Phishing	G-Data	Phishing
Google Safebrowsing	Phishing	Kaspersky	Phishing
Netcraft	Malicious	OpenPhish	Phishing
Sophos	Phishing	Trustwave	Phishing
VIPRE	Malicious	Webroot	Malicious

C. Otras detecciones:



3. RECOMENDACIONES:

- Mantener instalado un servicio de antivirus en el dispositivo.
- Verificar la información del sitio web 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.

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

Índice alfabético