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, 03 de febrero de 2024

030-2024-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°030	Fecha: 03-02-2024
		Página: 4 de 8

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	AnyDesk pirateado: el popular software de escritorio remoto exige el restablecimiento de contraseña		
Tipo de Ataque	Fuga de Información	Abreviatura	FugaInfo
Medios de propagación	Red, Internet, Redes sociales		
Código de familia	K	Código de Sub familia	K02
Clasificación temática familia	Uso inapropiado de recursos		

Descripción

1. **ANTECEDENTES**:

   El fabricante de software de escritorio remoto AnyDesk reveló el viernes que sufrió un ciberataque que comprometió sus sistemas de producción.

   La empresa alemana dijo que el incidente, que descubrió tras una auditoría de seguridad, no es un ataque de ransomware y que ha notificado a las autoridades pertinentes.

2. **DETALLES:**

   AnyDesk respondió al incidente realizando una auditoría de seguridad y colaborando con la firma de ciberseguridad CrowdStrike. Aunque la compañía tranquilizó a los usuarios al afirmar que no había evidencia de que los dispositivos de los usuarios finales se vieran afectados, confirmó el compromiso del código fuente y las certificaciones de firma de código. AnyDesk, alertando a sus más de 170.000 clientes en todo el mundo, tomó medidas rápidas, revocando certificados relacionados con la seguridad, reemplazando sistemas comprometidos y asegurando la integridad de la versión más reciente del software. la compañía indicó que revocará el certificado de firma de código anterior para sus binarios y que ya han comenzado a reemplazarlo por uno nuevo".

   Por precaución, AnyDesk también ha revocado todas las contraseñas de su portal web, my.anydesk[.]com, e insta a los usuarios a cambiar sus contraseñas si las mismas se han reutilizado en otros servicios en línea.

   También recomienda que los usuarios descarguen la última versión del software, que viene con un nuevo certificado de firma de código .

   AnyDesk no reveló cuándo y cómo se violaron sus sistemas de producción. Actualmente no se sabe si se robó alguna información después del ataque. Sin embargo, enfatizó que no hay evidencia de que ningún sistema de usuario final haya sido afectado.

   La empresa de ciberseguridad Resecurity dijo que encontró dos actores de amenazas, uno de los cuales se conoce con el alias en línea "Jobaaaaa", anunciando un "número significativo de credenciales de clientes de AnyDesk a la venta en Exploit[.]in", señalando que podrían usarse para "soporte técnico". estafas y envíos postales (phishing)".

   Se ha descubierto que el actor de amenazas ofrece 18.317 cuentas por 15.000 dólares en criptomonedas.

   "En particular, las marcas de tiempo visibles en las capturas de pantalla compartidas por el actor ilustran un acceso no autorizado exitoso con fecha del 3 de febrero de 2024 (divulgación posterior al incidente)", dijo la compañía. "Es posible que no todos los clientes hayan cambiado sus credenciales de acceso, o que este mecanismo aún estuviera en marcha por parte de los afectados".

   No está claro cómo se obtuvieron las credenciales, pero Resecurity dijo que los ciberdelincuentes podrían apresurarse a monetizar las credenciales de los clientes disponibles a la luz del hecho de que las contraseñas podrían restablecerse.

3. **RECOMENDACIONES:**

   - Implementar sistemas sólidos de detección de intrusiones.
   - Practicar una higiene estricta de sus contraseñas. Utilizar contraseñas únicas y complejas, y distintas para cada una de las cuentas, y cambiarlas periódicamente.
   - Habilitar la autenticación de dos factores cuando esté disponible.

Fuente de Información:	• hxxps://thehackernews.com/2024/02/anydesk-hacked-popular-remote-desktop.html

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°030	Fecha: 03-02-2024
		Página: 5 de 8

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Detección de sitio web fraudulento del Banco Crédito del Perú		
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 actores de amenazas vienen realizando una campaña de Phishing, suplantando el sitio web del Banco de Crédito del Perú (servicio online de préstamo personal), con la finalidad de robar información bancaria de los usuarios de la entidad financiera como números de tarjetas bancarias, clave intranet de seis dígitos, documento de identidad, etc.

2. **DETALLES:**

Paso N.º 01

Solicitan a la víctima registrar lo siguiente:

- El monto solicitado del préstamo.
- Cuotas por pagar
- Documento Nacional de identidad (DNI).
- Número de Celular.

Para luego dar clic en <**Empezar**>.

Paso N.º 02

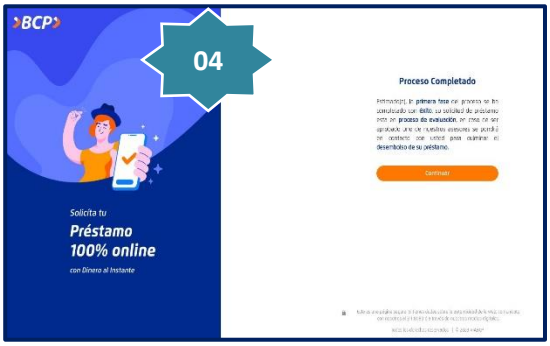
Instan a la víctima que registre datos como:

- El número de la tarjeta bancaria.
- Clave de seis dígitos del intranet.
- Código captcha

Para luego dar clic en <**Continuar**>.

Paso N.º 03

Una vez brindado los datos solicitados en el paso N.º 02, aparece una pantalla requiriendo información de la tarjeta bancaria como la fecha de expedición, el código de seguridad (CVV) la clave de cuatro dígitos utilizado en el cajero automático y correo electrónico, para luego dar clic en <**Continuar**>.



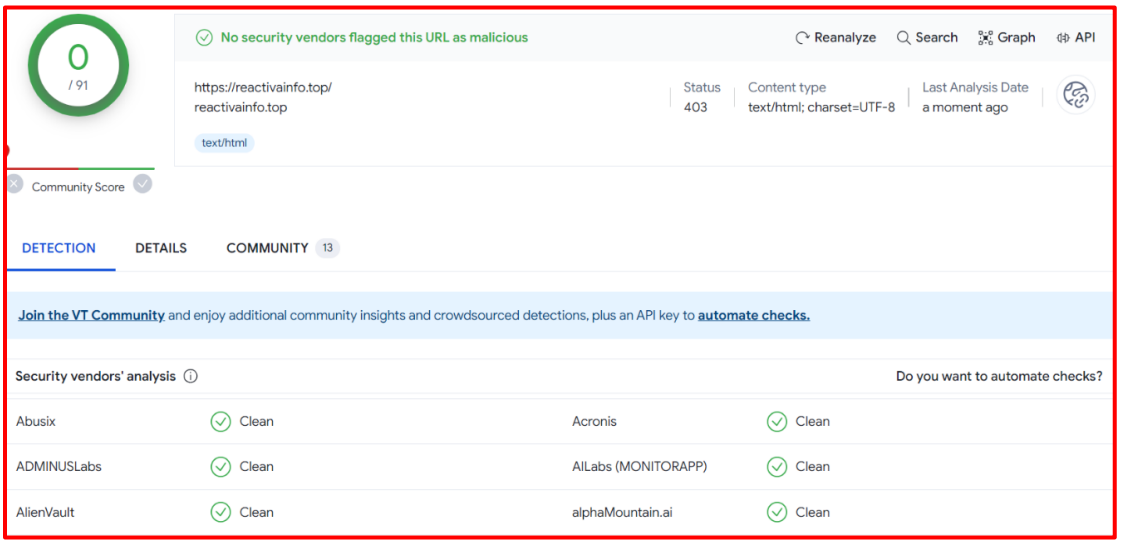
Paso N.º 04

Luego, aparece una pantalla indicando se ha completado con éxito el registro de datos y de ser aprobados el crédito, asesores de la entidad bancaria se pondrán en contacto con la víctima, para luego dar clic en <**Continuar**>. Redirigiendo al sitio web oficial de la entidad bancaria; sin embargo, los ciberdelincuentes obtuvieron los datos proporcionados por la víctima.

A. *Comparación del sitio web oficial y fraudulento*.

- Existe una diferencia entre la URL original y la URL fraudulenta.
- La URL del sitio web fraudulento posee protocolo de seguridad de red (https)
- Existe una similitud entre ambas páginas en imagen, fondo y colores de ambos sitios web.

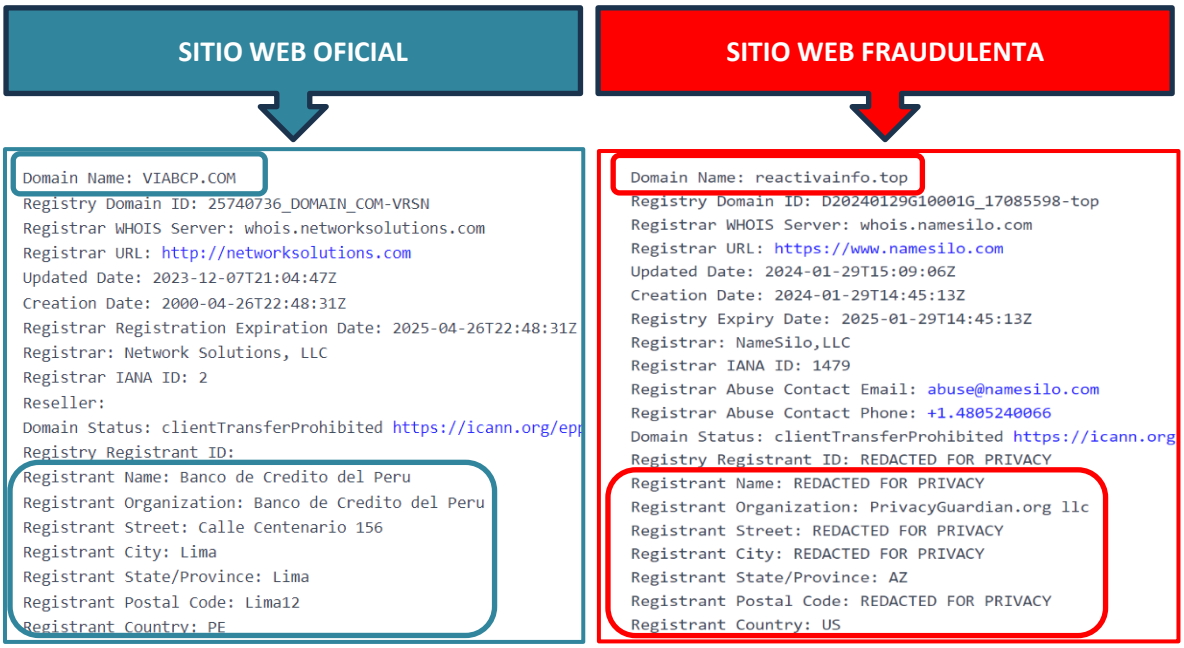
B. Hasta la formulación del presente documento, proveedores de seguridad informática NO HAN ALERTADO COMO SUPLANTACIÓN DE IDENTIDAD - PHISHING.



C. Indicadores de compromiso (IoC)

- Dominio : reactivainfo[.]top
- Servidor : Cloudflare
- IP : 104[.]21[.]87[.]199
- Tipo de tex. : Text/Html

D. Comparación de Dominios



3. RECOMENDACIONES:

- Verificar detalladamente las URL de los sitios web.
- No abrir o descargar archivos sospechosos.
- No seguir las instrucciones de sitio web sospechoso.
- No aceptar permisos de instalación de archivos desconocidos o dudosa procedencia.
- Mantener actualizado el sistema operativo y aplicaciones del equipo de cómputo.
- Mantener actualizado el sistema antivirus (el antivirus debe ser licenciado).

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

Índice alfabético