Alerta de seguridad informática	8FPH22-00538-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de junio de 2022
Última revisión	09 de junio de 2022

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones, por lo cual se recomienda establecer una cuarentena preventiva respecto de los IoC mencionados, previa evaluación de impacto en servicios productivos; una vez que sus plataformas de monitoreo no detecten actividad maliciosa, se debe evaluar la posibilidad de liberar del bloqueo a los IoC consignados en el reporte respectivo, tales como servicios de hosting, de cloud o similares.

Estos casos de phishing no involucran directamente a las entidades ni al sistema bancario, sino que son técnicas de fraude indirecto, en las que en infraestructura externa a éstas se arma el mencionado phishing, para construir el engaño. Las entidades, en general, al tomar conocimiento de estos portales maliciosos articulan, dentro de sus potestades y marco legal vigente, las acciones necesarias para poder desarticularlos, pero ciertamente los usuarios también estamos llamados a estar atentos a estos intentos de engaño.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT de Gobierno), ha identificado una campaña de phishing vía correo electrónico que proviene, supuestamente, de Office Banking del Banco Santander.

En esta campaña, los delincuentes indican falsamente a la víctima que *"Office Banking Empresarial te invita a actualizar la situación de bloqueo en tu banca electrónica. Dicho bloqueo podría deberse a un intento de acceso no autorizado por ti, por lo cual es de suma importancia que accedas de inmediato con las credenciales correspondientes por medio del siguiente enlace".* Al seleccionar el link disponible, la persona es dirigida a un sitio falso, semejante al de Office Banking del Banco Santander, donde se expone al robo de su usuario y contraseña (credenciales).

Observación

Solicitamos tener en consideración las señales de compromiso en su conjunto.

Indicadores de compromiso

URL redirección:
https://bit[.]ly/3xqPN6L

https://yummiss[.]xyz/wp/index.php

URL sitio falso:
https://www.offlcebanklng.cl.nuniavillabali[.]com/

Asunto:
Su banca electronica ha sido bloqueada.

Correo de salida:
nuevo@autotransportesbouchot[.]com

SMTP Host:
[152.89.247.165]

Otros antecedentes

Certificado Digital

Fecha Válido	:	07-06-2022
Fecha Término	:	06-09-2022
Emitido	:	cPanel, Inc. Certification Authority

Datos Alojamiento y Dominio

IP	:	[103.253.212.219]
Número de sistema autónomo (AS) IP	:	58487
Etiqueta del sistema autónomo IP	:	Rumahweb Indonesia CV.
Registrador IP	:	APNIC
País IP	:	ID
Dominio	:	nuniavillabali[.]com
Registrador Dominio	:	CV. Rumahweb Indonesia

Imagen del mensaje

miércoles 08-06-2022 11:01

Banco Santander <nuevo@autotransportesbouchot.com>

Su banca electronica ha sido bloqueada.

Para

office banking

¡ Hola ! .cl

Officebanking Empresarial te invita a actualizar la situación de bloqueo en tu banca electrónica.

Dicho bloqueo podria deberse a un intento de acceso no autorizado por ti, por lo cual es de suma importancia que accedas de inmediato con las credenciales correspondientes por medio del siguiente enlace:

http://www.officebanking.cl/desbloquear/cuenta/id?=ATB6299MANNXD42

Sigue las instrucciones que ahí se te indicarán.

Realiza esta operación LO ANTES POSIBLE de lo contrario tu acceso y tus cuentas seran congelados incluyendo los recursos y fondos que contengan.

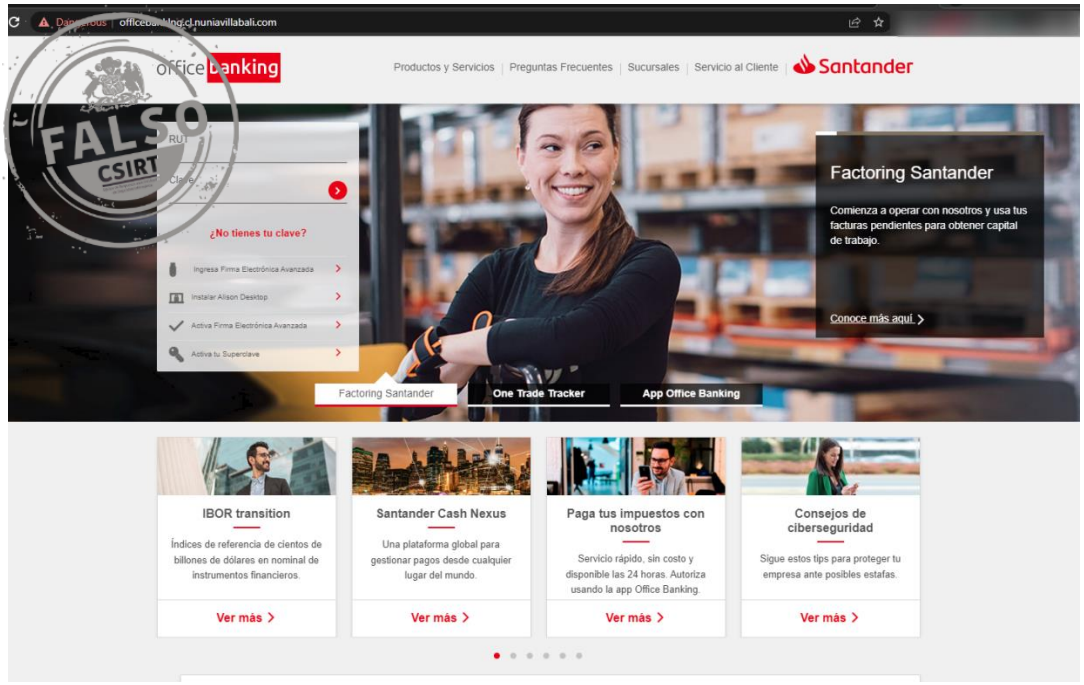
1. Recuerda tener tu Rut y Clave actualizados
2. Debes contar con tu Superclave al momento de realizar esta operación.
3. Tu acceso sera reestablecido una vez que hayas completado los pasos a seguir.

Aviso de seguridad:

Officebanking y Santander Chile garantizan la seguridad en tus operaciones en línea.

Officebanking 2022 todos los derechos reservados.

Imagen del sitio



Recomendaciones

- No abrir correos ni mensajes de dudosa procedencia.
- Desconfiar de los enlaces y archivos en los mensajes o correo.
- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).
- Ser escépticos frente ofertas, promociones o premios increíbles que se ofrecen por internet.
- Prestar atención en los detalles de los mensajes o redes sociales.
- Evaluar el bloqueo preventivo de los indicadores de compromisos.
- Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas.
- Revisar los controles de seguridad de los AntiSpam y SandBoxing.
- Realizar concientización permanente para los usuarios sobre este tipo de amenazas.
- Visualizar los sitios web que se ingresen sean los oficiales.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.06.09 08:59:13 -04'00'