Alerta de seguridad cibernética	8FFR20-00829-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de Noviembre de 2020
Última revisión	14 de Noviembre de 2020

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 fraude no involucran directamente a las entidades aludidas ni al sistema bancario, sino que son técnicas de fraude indirecto, en las que en infraestructura externa a éstas se arma el mencionado fraude, 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), ha identificado la activación de una pagina fraudulenta asociada a un dominio .com que intenta suplantar al sitio financiero global **Wells Fargo**, el que podría servir para robar credenciales de usuarios.

Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad aludida.

Indicadores de compromiso

URL sitio falso

https[:]//cortinasrollerazteca[.]cl/ww/secure.connect/auth.present/ea037c6e33582d13b5b71f516a8b261f/First-page/

Body SHA-256

4d1fe238f99d330616e6a40bbb5428c6e2e25bda18b8d17138b8a0f18c5a3531

Certificado Digital

Fecha Válido	27/09/2020
Fecha Término	27/12/2020
Emitido	cPanel, Inc. Certification Authority

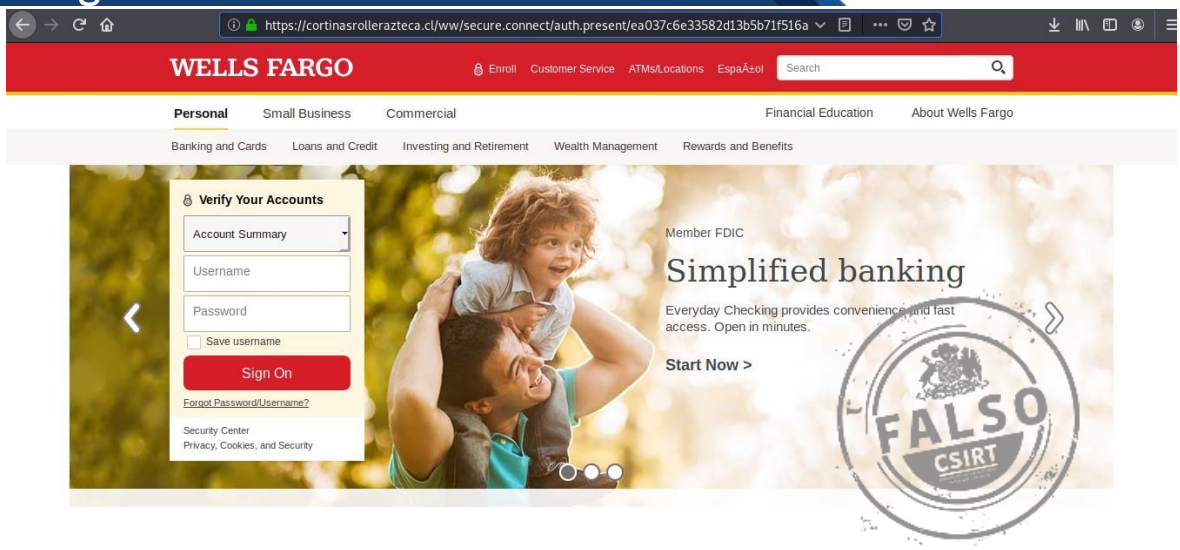
Datos Alojamiento

IP	200[.]32[.]181[.]200
Número de Sistema Autónomo (AS)	6429
Etiqueta del Sistema Autónomo	Telmex Chile Internet S.A.
País	CL
Registrador	LACNIC

Datos del Dominio

Nombre de Dominio	NutricionYTerapias[.]cl
Creado	03/12/2019
Expira	03/12/2021
Información del Registrador	NicChile
ID IANA	No disponible
Correo Electrónico	No disponible
Name Server	NS1.ACBHOST.CL NS2.ACBHOST.CL

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.