

Alerta de seguridad cibernética	8FFR20-00483-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de Julio de 2020
Última revisión	10 de Julio 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 loC 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 loC consignados en el reporte respectivo, tales como servicios de hosting, de cloud o similares.

Estos casos de fraude 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 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 un portal fraudulento asociado a un dominio que suplanta el sitio web oficial de **Banco de Chile**, el que podría servir para robar credenciales de usuarios de esa entidad.

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

Indicadores de compromiso

Urls sitio falso:

acceso.banconchile[.]net/mypes-an95ZqWYoJJqq5JnpLKX

Body SHA-256

9c880b42f8091b8fbe07a7f87e36b016396297a0bf86d63936f9c266ad732d3c

Certificado Digital

Fecha Valido : 2020-07-09
Fecha Termino : 2020-10-07
Emitido : -

Datos Alojamiento

IP : 86[.]106[.]20[.]170
Número de sistema autónomo (AS) : 9009
Etiqueta del sistema autónomo : M247 Ltd
País : Rumania
Registrador : NameSilo, LLC

Datos del Dominio

Nombre de dominio : banconchile[.]net
Estado del dominio : Activo
Creado : 2020-07-05
Expira : 2021-07-05
Información del registrador : NameSilo, LLC
ID IANA : 1479
Correo electrónico : email@privacyguardian[.]org
Servidores de nombres : ns1[.]dnsowl[.]com
ns2[.]dnsowl[.]com
ns3[.]dnsowl[.]com

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.