

Alerta de seguridad cibernética	8FFR22-01102-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de septiembre de 2022
Última revisión	28 de septiembre de 2022

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigación propia del CSIRT de Gobierno. 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 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 del Gobierno de Chile (CSIRT de Gobierno) ha identificado la activación de una página fraudulenta que suplanta al Bank of America, lo que podría servir para robar credenciales de sus 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://ricardoparra[.]cl/img/home/safemode/
https://ricardoparra[.]cl/config/html
http://ricardoparra[.]cl/img/phpscrip/
https://ricardoparra[.]cl/php/form-process/

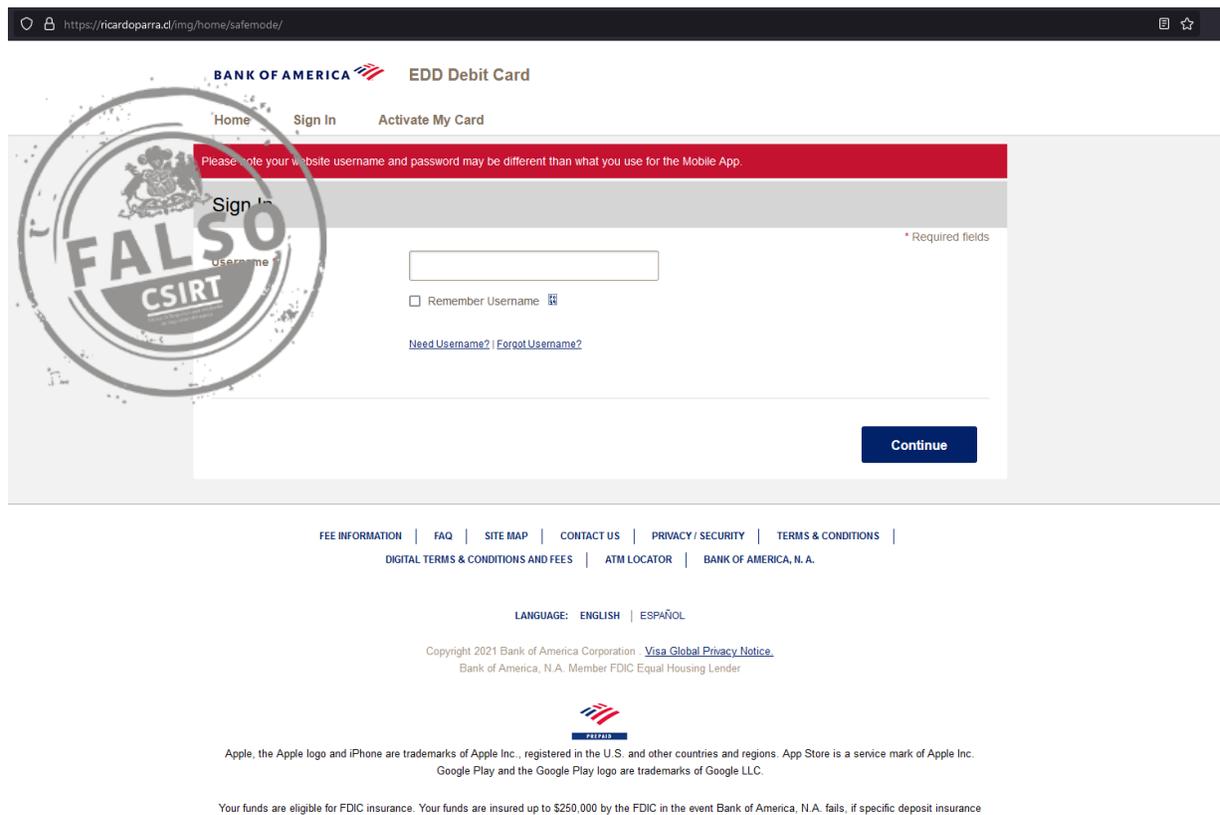
Certificado Digital

Fecha Válido	22-09-2022
Fecha Término	21-12-2022
Emitido	Let's Encrypt R3

Datos Alojamiento

IP	[131.72.236.88]
Número de Sistema Autónomo (AS) IP	263753
Etiqueta del Sistema Autónomo IP	SERVICIOS DE DATACENTER DATANETWORKS LIMITADA
Registrador IP	LACNIC
País IP	CL
Dominio	ricardoparra.cl
Registrador Dominio	https://www.nic.cl

Imagen del sitio



https://ricardoparra.cl/mg/home/safemode/

BANK OF AMERICA EDD Debit Card

Home Sign In Activate My Card

Please note your website username and password may be different than what you use for the Mobile App.

Sign In

Username * Required fields

Remember Username

[Need Username? | Forgot Username?](#)

Continue

FEE INFORMATION | FAQ | SITE MAP | CONTACT US | PRIVACY / SECURITY | TERMS & CONDITIONS |
DIGITAL TERMS & CONDITIONS AND FEES | ATM LOCATOR | BANK OF AMERICA, N.A.

LANGUAGE: ENGLISH | ESPAÑOL

Copyright 2021 Bank of America Corporation - [View Global Privacy Notice](#)
Bank of America, N.A. Member FDIC Equal Housing Lender


Apple, the Apple logo and iPhone are trademarks of Apple Inc., registered in the U.S. and other countries and regions. App Store is a service mark of Apple Inc.
Google Play and the Google Play logo are trademarks of Google LLC.

Your funds are eligible for FDIC insurance. Your funds are insured up to \$250,000 by the FDIC in the event Bank of America, N.A. fails, if specific deposit insurance

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.