9Alerta de seguridad informática	8FPH23-00733-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de enero de 2023
Última revisión	27 de enero de 2023

NOTA SOBRE EL CORRECTO USO Y DIVULGACIÓN DE ESTE DOCUMENTO

La información contenida en este informe fue procesada por el CSIRT de Gobierno analizando múltiples fuentes. La información puede ser modificada o actualizada a partir de nuevos antecedentes y análisis.

Las personas y organizaciones víctimas de suplantación, en los casos que corresponda, no tienen responsabilidad sobre esa acción ejecutada por el atacante. El uso de la imagen de los suplantados en este informe tiene el específico propósito de evitar que terceras partes sean afectadas por atacantes.

Las alertas de seguridad cibernéticas del CSIRT de Gobierno contienen información sobre incidentes y acciones maliciosas que podrían impactar en las organizaciones. Los receptores de esta información tienen la responsabilidad de evaluar la eventual aplicación de cuarentenas preventivas sobre los indicadores de compromiso (IoC) que se comparten en este documento, teniendo presente los impactos que pueda tener en la entrega de sus servicios o en la continuidad operativa de sus negocios. Una vez que sus plataformas de monitoreo no detecten actividad maliciosa sobre los IoC compartidos, se debe evaluar la posibilidad de levantar el bloqueo

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT de Gobierno) ha identificado una nueva campaña de phishing vía correo electrónico.

En esta campaña, los delincuentes indican falsamente a la víctima lo siguiente*: "BancoEstado le informa que hemos detectado actividad inusual en su acceso a la banca en linea por internet, por lo que procederemos a SUSPENDER el servicio hasta la correcta verificación de sus datos como medida de seguridad. VERIFICAR DATOS."*

De abrir el enlace, la persona es dirigida a un sitio falso semejante a uno del BancoEstado, donde se expone al robo de su usuario y contraseña (credenciales).

Advertencia sobre gestión de IoC

Los patrones expresados en forma de hash de un archivo pueden ser administrados con herramientas centralizadas y distribuidas, como firewall y antimalware. Las organizaciones deben tomar resguardo de incorporar un hash que pudiere estar vinculado a un archivo o DLL válida dentro de un sistema.

Al gestionar patrones potencialmente maliciosos con nombres de host o IP, se debe considerar que la relación entre nombre FQDN e IP puede cambiar en el tiempo, y que una dirección IP específica puede estar siendo usada por un proveedor de web hosting que puede tener más de un dominio asociado a dicha IP.

En consecuencia, se recomienda tener un orden de prioridades a la hora de ejecutar un bloqueo, considerando al menos:

- El uso de un dispositivo WAF que pueda discriminar el nombre FQDN potencialmente malicioso por sobre la IP.
- El uso de un firewall que permita integrar listas de bloqueo FQDN sin necesitar la conversión a IP.
- El uso de sistemas proxy que permitan bloquear el FQDN sin necesitar la conversión a IP.
- En última instancia, incorporar el bloqueo de la IP verificando que no corresponda a un esquema de web hosting, porque existe la posibilidad de bloquear los restantes dominios implementados que utilizan la misma dirección IP.

IoC Correo Electrónico

Antes de aplicar bloqueos, tenga presente el punto sobre advertencia de gestión de IoC.

URL redirección:

https://cartoonpuzzl3s[.]com/activacion/cuenta-bpwz/

URL sitio falso:

https://xtraillconver[.]com/1674842723/imagenes/_personas/home/default.asp

Datos del remitente:

Asunto	Correo de Salida	SMTP Host
✓ Aviso Importante: Cuenta Suspendido	apache@fl1per.net.net	[168.232.165.161]

Otros antecedentes

Certificado Digital

Fecha Valido	22 Ene 2023
Fecha Término	22 abr 2023
Emitido	cPanel, Inc.

Datos Alojamiento y Dominio

IP	[138.128.189.154]
Número de sistema autónomo (AS) IP	33182
Emitido Etiqueta del sistema autónomo IP	DIMENOC
Registrador IP	ARIN
País IP	US
Dominio	xtraillconver.com
Registrador Dominio	http://www.arsys.es

Imagen del mensaje

✓ Aviso Importante: Cuenta Suspendido

A AtencionAlClienteBancoEstado <BancoEstado@plusconsulting.c
Para [redacted]

Responder | Responder a todos | Reenviar | ...

vi. 27/01/2023 14:21

BancoEstado

Estimado Cliente: [redacted]

BancoEstado le informa que hemos detectado actividad inusual en su acceso a la banca en linea por internet, por lo que procederemos a **SUSPENDER** el servicio hasta la correcta verificación de sus datos como medida de seguridad.

Le recomendamos realizar este proceso de verificación con el objetivo de garantizar su seguridad y el acceso correcto a la banca en linea por internet y de nuestra App BancoEstado.

Recordarle que de no proceder con la verificación de sus datos, su cuenta será bloqueado y tendrá que apersonarse a la sucursal mas cercana de nuestra entidad para su verificación respectiva. BancoEstado nos preocupamos por tu Seguridad.

Verificar Datos

FALSO CSIRT

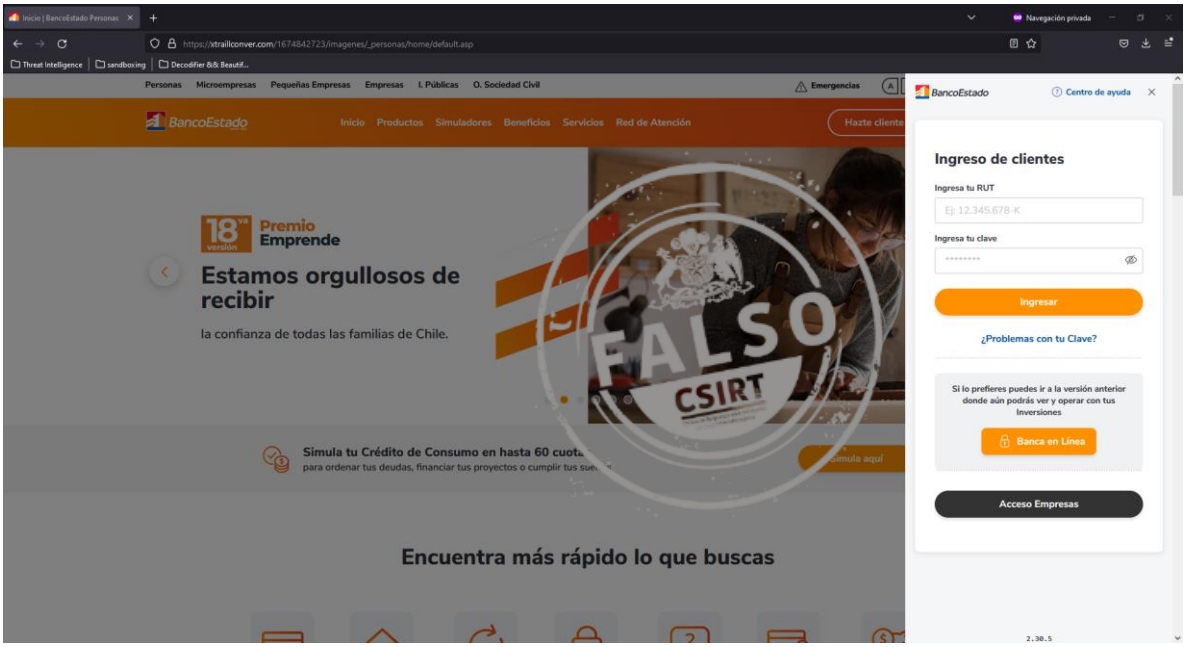
Desde la App es más fácil
Actívala con tu Clave de Cajero Automático

Encuéntrala en:
Google Play | App Store

www.bancoestado.cl

Atentamente, BancoEstado.

Imagen del sitio



Recomendaciones

- Los usuarios deberían procurar:
  - No abrir correos ni mensajes de dudosa procedencia.
  - Desconfiar de los enlaces y archivos en los mensajes o correo.
  - Solicitar que sus plataformas (Office, Windows, Acrobat, etc.) estén actualizadas.
  - Ser escépticos frente ofertas, promociones o premios que se ofrecen por internet.
  - Prestar atención en los detalles de los mensajes o redes sociales.
  - Solicitar que todas las plataformas de tecnologías y de detección de amenazas estén actualizadas.
  - Siempre intentar verificar que los sitios web que se visitan sean los oficiales.
  - Notificar oportunamente a sus encargados de ciberseguridad para que investiguen el incidente, comprueben si ha llegado a otros usuarios y apliquen las mitigaciones pertinentes. Algunas señales que debieran gatillar un informe inmediato:
    - Ha llegado un correo que a mi criterio es potencialmente un engaño (un correo de un banco del cual no soy cliente, un correo con un super premio, un correo con un bono del gobierno y claramente no es razonable, etc.).
    - Me contactan desde algún banco para confirmar alguna transferencia financiera que yo no he solicitado.
    - He ingresado mis credenciales en un sitio web que parecía real y me percaté después de su falsedad.
- Los administradores deben:
  - Implementar controles anti spoofing (DKIM, SPF y DMARC).
  - Revisar la información que se expone de sus usuarios en sus sitios y sistemas web.
  - Filtrar o bloquear los correos entrantes que sean clasificados como phishing.
  - Evaluar el bloqueo preventivo de los indicadores de compromisos.
  - Revisar los controles de seguridad de los antispam y sandboxing.
  - Instruir a sus usuarios sobre el phishing y ayudarlos a reconocerlos. Realizar concientización permanente para los usuarios sobre este tipo de amenazas.
  - Crear mecanismos amistosos para el reporte y el feedback, en un entorno donde no se busque la culpabilidad, sino que la solución.
  - Implementar 2FA.
  - Proteger a sus usuarios de sitios maliciosos usando proxy servers y manteniendo actualizados sus browsers.
  - Proteger sus dispositivos del malware.
  - Tener un protocolo de respuesta rápido ante estos incidentes.
  - Detectar rápidamente estos incidentes instando a los usuarios a que reporten rápidamente cualquier actividad sospechosa.
- Para obtener los IOC de este informe visita el siguiente enlace:
  - https://github.com/csirtcl/Fraude/blob/main/Phishing_8FPH23-00733-01.txt

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.01.27 15:33:30 -03'00'