Alerta de seguridad informática	8FPH-00065-001
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de Octubre de 2019
Última revisión	06 de Octubre de 2019

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), ha identificado una campaña de phishing a través de un correo electrónico cuyo mensaje intenta engañar a los usuarios del Banco Estado para cometer un fraude.

El correo indica que, producto de una actualización de los servidores la cuenta del usuario no estaría registrada correctamente y, por lo tanto, el banco se habría visto obligado a bloquearla temporalmente. El mensaje insta a la víctima a registrar nuevamente la cuenta, acción que solo puede ser realizada a través de este correo electrónico a través del enlace adjunto. El enlace para, supuestamente, restaurar la cuenta, redirige a la víctima a un sitio fraudulento donde las víctimas se exponen al robo de sus credenciales bancarias.

Observación

Solicitamos tener en consideración las señales de compromiso en su conjunto

Indicadores de compromisos

Url's:

http[:]//naponet[.]site/readme/Promociones/
http[:]//1verter[.]site/cron/imagenes/comun2008/banca-en-linea-personas[.]html

Smtp Host

hwsrv-614558[.]hostwindsdns[.]com
hwsrv-603734[.]hostwindsdns[.]com
hwsrv-615429[.]hostwindsdns[.]com
hwsrv-615432[.]hostwindsdns[.]com

Sender

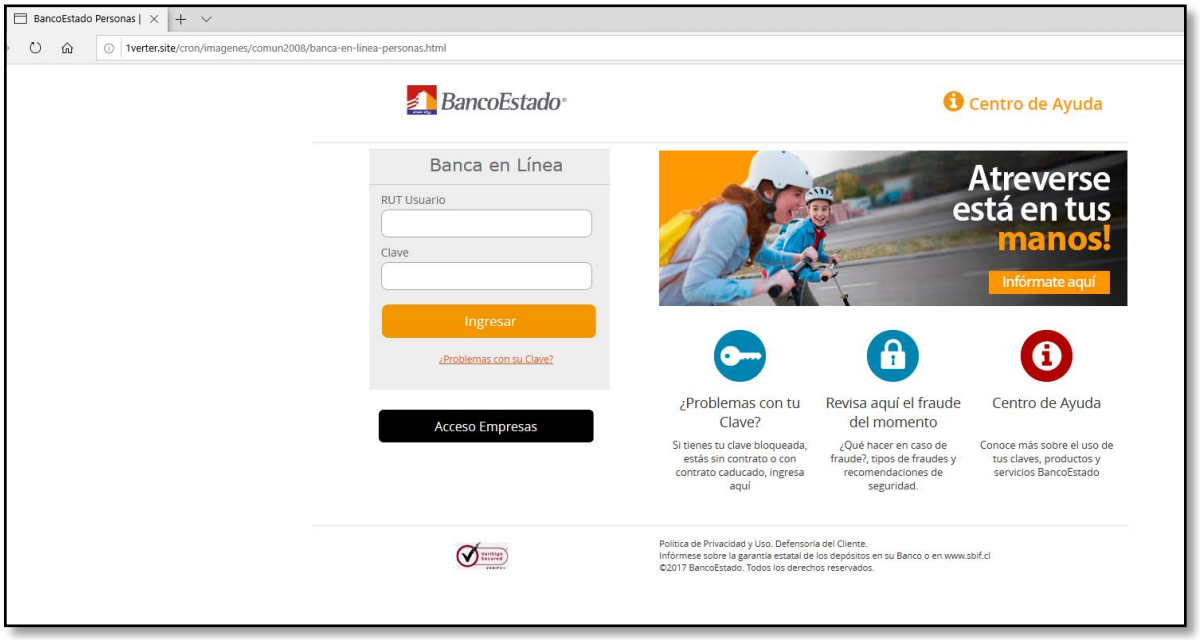
apache@hwsrv-614558.hostwindsdns[.]com
apache@hwsrv-603734.hostwindsdns[.]com
apache@hwsrv-615429.hostwindsdns[.]com
apache@hwsrv-615432.hostwindsdns[.]com

Subject:

✓ Fw: Cuenta Temporalmente Suspendido
✓ Fw: Cuenta Deshabilitado
✓ Aviso Importante: Cuenta Bloqueado

Imagen Phishing Correo

Imagen Sitio Web



Recomendaciones

- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras)
- 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 que sean los oficiales

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.10.06 13:16:25 -03'00'