Alerta de seguridad informática	8FPH21-00369-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de enero de 2021
Última revisión	04 de enero de 2021

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), advierte sobre una campaña de phishing que se está difundiendo a través de correo electrónico que supuestamente proviene del Banco Estado.

El atacante busca persuadir a las personas para utilizar un enlace adjunto.

El mensaje del correo indica que el Banco Estado, debido a la alta demanda de Créditos COVID-FOGATE, hoy ha realizado la transferencia electrónica a su Cuenta Rut.

Al seleccionar el enlace para realizar la consulta, es dirigido a un sitio falso, donde se expone al robo de sus credenciales.

Observación

Solicitamos tener en consideración las señales de compromiso en su conjunto.

Indicadores de compromiso

Urls Redirección:
http://www.jazzbox-radio[.]fr/wp-content/themes/cli/enviar02.php?l=1058512047

Urls sitio falso:
http://paracels[.]one/wp-content/www.bancoestado.cl/pagina/imagenes/comun2008/banca-en-linea-personas.html

Asunto
Credito COVID-FOGAPE Aprobado.

Smtp Sender:
atnp@admin.afranaxtechnologies.com

Smtp Host:
[181.176.35.17]

Otros antecedentes

Certificado Digital

Fecha Válida	:	No aplica
Fecha Término	:	No aplica
Emitido	:	No aplica

Datos Alojamiento

IP	:	181.176.35.17
Número de sistema autónomo (AS)	:	262210
Etiqueta del sistema autónomo	:	VIETTEL PERÚ S.A.C.
País	:	PE
Registrador	:	LACNIC

Datos del Dominio

Nombre de dominio	:	paracels[.]one
Creado	:	16-07-2018
Expira	:	16-07-2021
Información del registrador	:	Hosting Concepts B.V. d/b/a Registrar.eu
ID IANA	:	1647
Correo electrónico	:	abuse@registrar.eu
Servidores de nombres	:	dns1.hostiq.ua Dns2.hostiq.ua

Imagen del mensaje

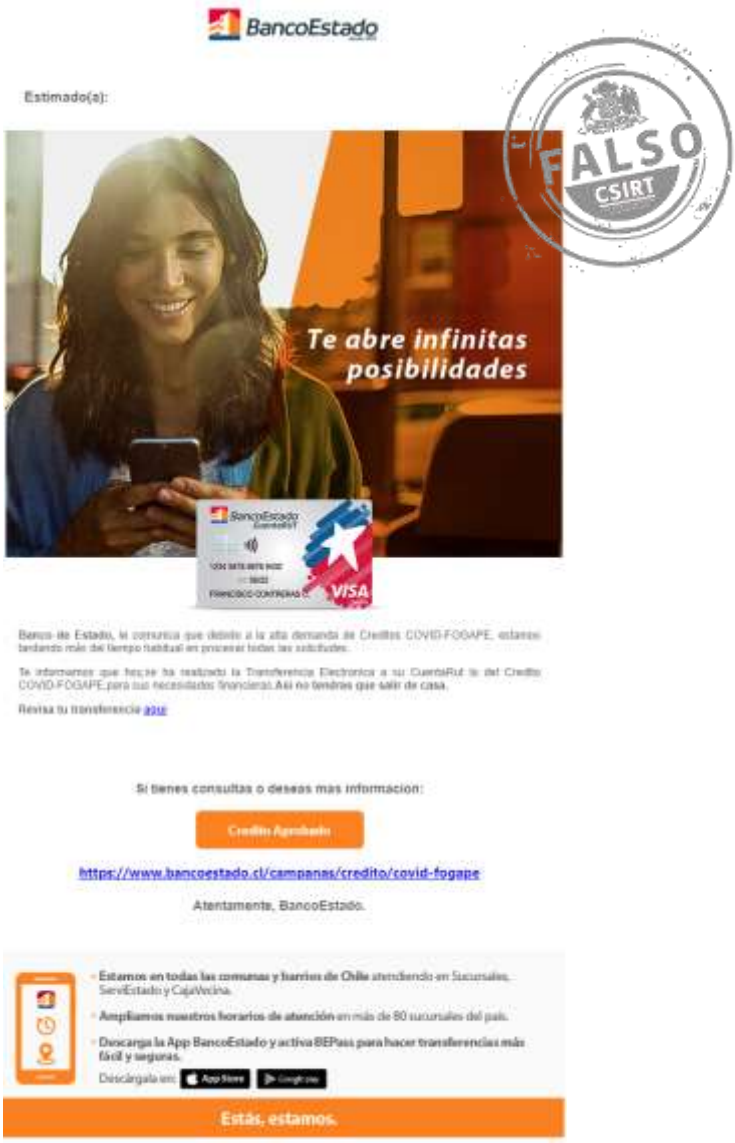

Imagen del sitio

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.