Alerta de seguridad informática	8FPH21-00367-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Febrero de 2021
Última revisión	04 de Febrero 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 un correo electrónico que supuestamente proviene del Banco Santander.

El atacante busca persuadir a las personas para utilizar un enlace adjunto en el cuerpo del correo.

El mensaje del correo indica al usuario que se ha bloqueado su cuenta y sugiere su activación.

Al seleccionar el enlace para ver más detalles, las personas son dirigidas a un sitio falso, donde se exponen al robo de sus credenciales.

Observación

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

Indicadores de compromiso

Urls Redirección:
hxxps://bit[.]ly/2LM7GrO?l=www.santander.cl

Urls sitio falso:
hxxp://gaborestarsa2005[.]hu/wp-includes/www.santander.cl/pagina/login.asp

Smtp Host
[45.7.228.193]

Asunto
Fwd:Notificacion - SuperClave Bloqueada.

Otros antecedentes

URL Body SHA-256

5ade6c04e94d88e4a6e22bf473874ee49e8c9a8b14b9de9239b594a3dd798488

Certificado Digital

Fecha Válido	:	NO APLICA
Fecha Término	:	NO APLICA
Emitido	:	NO APLICA

Datos Alojamiento

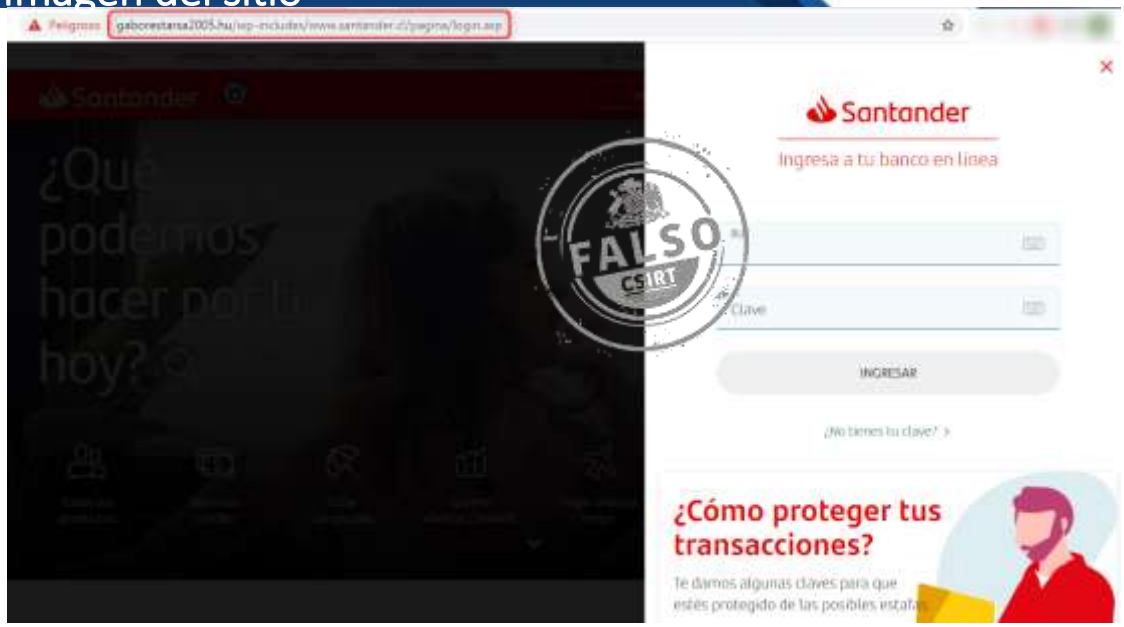
IP	:	[185.6.139.216]
Número de sistema autónomo (AS)	:	43711
Etiqueta del sistema autónomo	:	Szervernet Ltd
País	:	HU
Registrador	:	RIPE NCC

Datos del Dominio

Nombre de dominio	:	gaborestarsa2005[.]hu
Creado	:	2009-03-25
Expira	:	NO APLICA
Información del registrador	:	NO APLICA
ID IANA	:	NO APLICA
Correo electrónico	:	NO APLICA
Servidores de nombres	:	NO APLICA

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.