Alerta de seguridad cibernética	8FFR20-00713-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de Septiembre de 2020
Última revisión	15 de Septiembre de 2020

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 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 (CSIRT), ha identificado la activación de un portal fraudulento asociado a un dominio que suplanta el sitio web oficial del Banco Santander, el que podría servir para robar credenciales de usuarios de esa entidad.

Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad bancaria aludida.

Indicadores de compromiso

Urls sitio falso:

info-santander[.]cf

Body SHA-256

6d363b8903202fc5aea7d88a249ee79146eb61def26229eaf95ce85209cc7a8c

Certificado Digital

Fecha Valido	:	lunes, 14 de septiembre de 2020 13:12:39
Fecha Termino	:	domingo, 13 de diciembre de 2020 13:12:39
Emitido	:	Let's Encrypt

Datos Alojamiento

IP	:	178[.]159[.]36[.]159
Número de sistema autónomo (AS)	:	48666
Etiqueta del sistema autónomo	:	MAROSNET Telecommunication Company LLC
País	:	Rusia
Registrador	:	RIPE NCC

Datos del Dominio

Nombre de dominio	:	INFO-SANTANDER[.]CF
Estado del dominio	:	Activo
Creado	:	No Registrado
Expira	:	No Registrado
Información del registrador	:	Centrafrique TLD B.V.
ID IANA	:	No Registrado
Correo electrónico	:	No Registrado
Servidores de nombres	:	NS01[.]FREENOM[.]COM NS02[.]FREENOM[.]COM NS03[.]FREENOM[.]COM NS04[.]FREENOM[.]COM

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.