Alerta de seguridad cibernética	8FPH21-00433-01
Clase de alerta	Fraude
Tipo de incidente	smishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de septiembre de 2021
Última revisión	13 de septiembre 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 de Gobierno) advierte sobre una campaña smishing está siendo difundida a través de mensajes de texto que declaran falsamente provenir del BancoEstado.

Para lograr convencer a sus víctimas, el mensaje indica que el receptor tiene aprobado su IFE con abono inmediato a su cuenta Banco Estado, dejando un enlace adjunto en el mensaje de texto. De hacerse clic en el enlace, la víctima es dirigida 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

Texto del mensaje:
BancoEstado Estimado Cliente le informamos que tiene aprobado su IFE con abono inmediato a su cuenta Banco Estado solicítalo aquí: https://bit[.]ly/3k2dueU

URL de SMS:
https://bitly[.]com/3trinkD

URL sitio falso:
https://inicio.web-estadon[.]fun/

Otros antecedentes

Certificado Digital

Fecha Valido	:	08-09-2021
Fecha Termino	:	08-09-2021
Emitido	:	Cloudflare Inc ECC CA-3

Datos Alojamiento

IP	:	[104.21.74.85]
Número de sistema autónomo (AS)	:	13335
Etiqueta del sistema autónomo	:	CLOUDFLARENET
País	:	US
Registrador	:	ARIN

Datos del Dominio

Nombre de dominio	:	inicio.web-estadon[.]fun
Creado	:	09-09-2021
Expira	:	09-09-2022
Información del registrador	:	Namecheap
ID IANA	:	1068
Correo electrónico	:	abuse@namecheap.com
Servidores de nombres	:	elijah.ns.cloudflare.com serenity.ns.cloudflare.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.