Alerta de seguridad informática	8FFR-00127-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Noviembre de 2019
Última revisión	25 de Noviembre 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 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 una IP que suplanta el sitio web oficial de **Banco Scotiabank**, 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 Compromisos

URL´s

URL Sitio Clonado:
https[://]scotiabankchileweb[.]com/pages/login-form-scotia

Domain scotiabankchileweb.com

scotiabankchileweb / com / Subdomains

record type	TTL	value		
A	28800	192.3.179.198		
NS	38400	blue518835.earth.orderbox-dns.com	Zones on DNS server	162.251.82.246, 162.251.82.118, 162.251.82.119, 162.251.82.247
NS	38400	blue518835.venus.orderbox-dns.com	Zones on DNS server	162.251.82.248, 162.251.82.249, 162.251.82.120, 162.251.82.121
NS	38400	blue518835.mercury.orderbox-dns.com	Zones on DNS server	162.251.82.122, 162.251.82.123, 162.251.82.251, 162.251.82.250
NS	38400	blue518835.mars.orderbox-dns.com	Zones on DNS server	162.251.82.125, 162.251.82.252, 162.251.82.124, 162.251.82.253
SOA	7200	Mname	blue518835.mars.orderbox-dns.com	
		Rname	henriquevalentefalci.outlook.com	
		Serial number	2019112103	
		Refresh	7200	
		Retry	7200	
		Expire	172800	
		Minimum TTL	38400	

Ilustración 1 Dominio donde se Aloja Url del Banco Scotiabank, Falso y DNS que utiliza

Certificados

Criteria: Identity = 'scotiabankchileweb.com'

Certificates

crt.sh ID	Logged At	Not Before	Not After	Issuer Name
2136996062	2019-11-21	2019-11-21	2020-02-19	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

Ilustración 2 Certificado Utilizado en Url del sitio Falso del Banco Scotiabank

IP

192.3.179.198

Domain scotiabankchileweb.com is located on IP address << 192.3.179.198 >>	
Block start	192.3.179.0
End of block	192.3.179.255
Block size	256 Domains in block
Block name	CC-192-3-179-0-24
AS number	36352
Parent block	192.3.0.0 - 192.3.255.255
Organization	CC Customer
City	New York City
Region/State	New York
Country	US , United States
Reg. date	2014-02-17
Host name	192-3-179-198-host.colocrossing.com
Domains	1 scotiabankchileweb.com

Ilustración 3 Ip de Origen donde se aloja Sitio Falso del Banco Scotiabank

Localización

New York City, New York, Estados Unidos

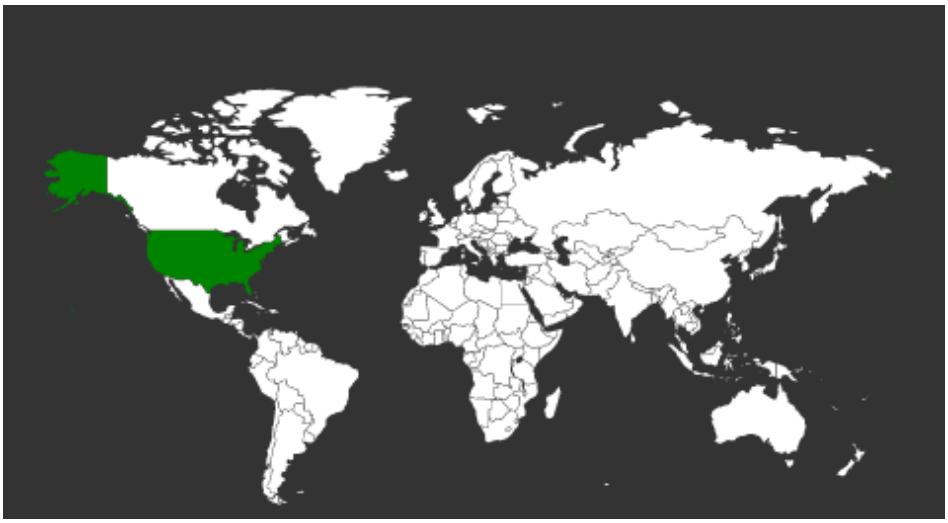
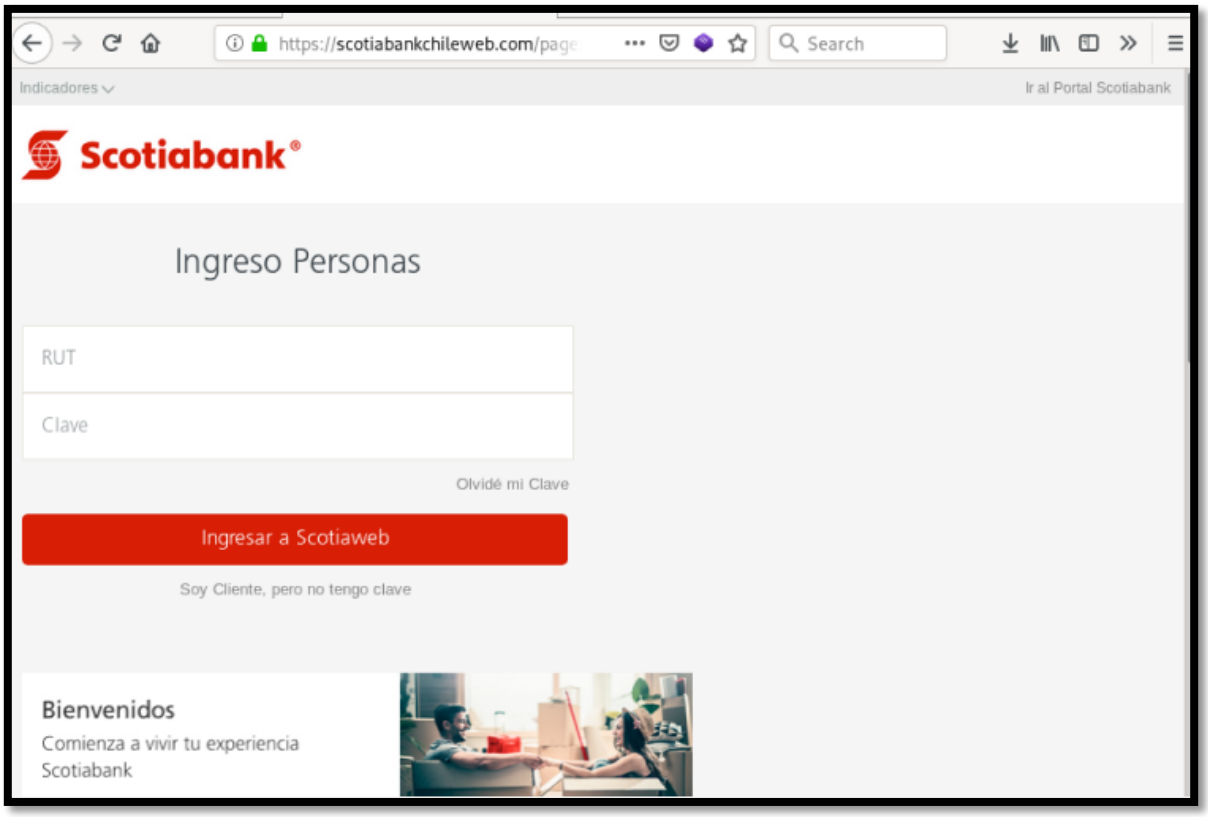


Imagen del sitio



Recomendaciones

- Evitar acceder al sitio anteriormente indicado e informar a los usuarios sobre su existencia, para evitar que se conviertan en víctimas del fraude.
- Ser precavidos frente a este tipo de páginas fraudulentas.
- Bloquear en los proxy o sistemas de control de contenido, hacia la URL maliciosa
- 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

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.11.25 06:01:54 -03'00'