Alerta de seguridad informática	8FFR20-00187-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de Enero de 2020
Última revisión	22 de Enero 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 tres portales fraudulentos asociados 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

scotiabank[.]personas-login[.]com
scotiabank[.]personas-login[.]com/pages/login-form-scotia
scotiabank[.]personas-login[.]com/pages/login-form-scotia-empresas

Domain personas-login.com

personas-login / com / Subdomains

record type	TTL	value		
NS	1800	dns1.registrar-servers.com	Zones on DNS server	156.154.132.200
NS	1800	dns2.registrar-servers.com	Zones on DNS server	156.154.133.200
MX	1800	10 eforward1.registrar-servers.com		162.255.118.51
MX	1800	10 eforward2.registrar-servers.com		162.255.118.52
MX	1800	10 eforward3.registrar-servers.com		162.255.118.51
MX	1800	15 eforward4.registrar-servers.com		162.255.118.61
MX	1800	20 eforward5.registrar-servers.com		162.255.118.62
TXT	1800	v=spf1 include:spf.efwd.registrar-servers.com ~all		
SOA	3601	Mname: dns1.registrar-servers.com Rname: hostmaster.registrar-servers.com Serial number: 1579538359 Refresh: 3600 Retry: 1801 Expire: 604800 Minimum TTL: 3601		

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

Certificados

Subject DN CN=scotiabank.personas-login.com
Issuer DN C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial 357600832507831216271347354534757144346082
Validity 2020-01-20 15:39:42 **to** 2020-04-19 15:39:42 (90 days, 0:00:00)
Names scotiabank.personas-login.com

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

IP

144.208.127.181

Domain scotiabank.personas-login.com is located on IP address << 144.208.127.181 >>

Block start	144.208.127.0
End of block	144.208.127.255
Block size	256 Domains in block
Block name	SH-335
AS number	395092
Parent block	144.208.0.0 - 144.208.127.255
Organization	Shock Hosting LLC
City	Piscataway
Region/State	New Jersey
Country	US , United States
Reg. date	2016-04-27
Host name	727770.com

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

Localización

Piscataway, New Jersey, Estados Unidos

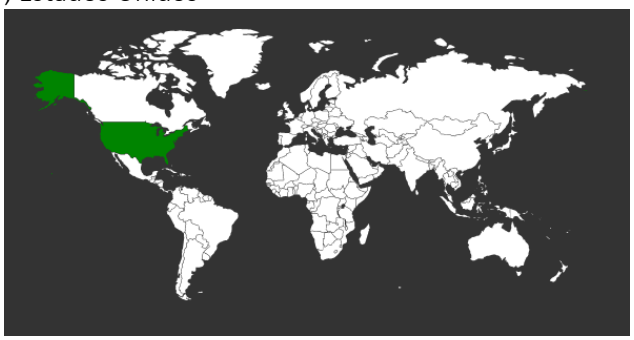
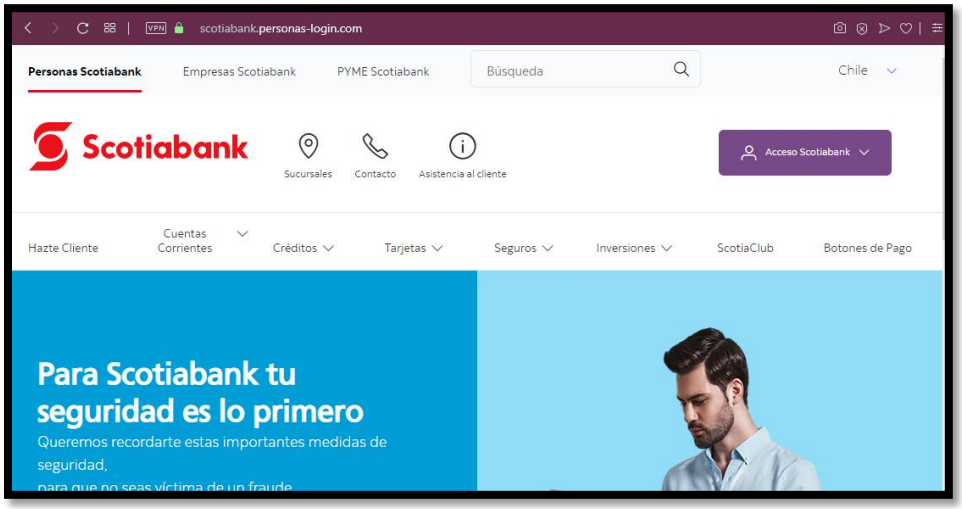
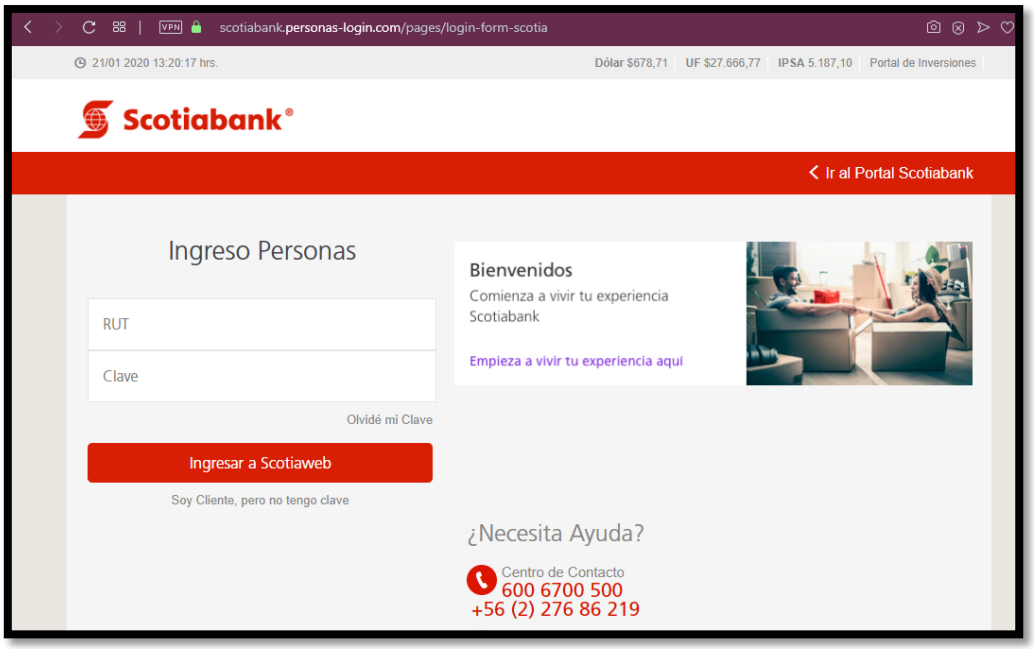
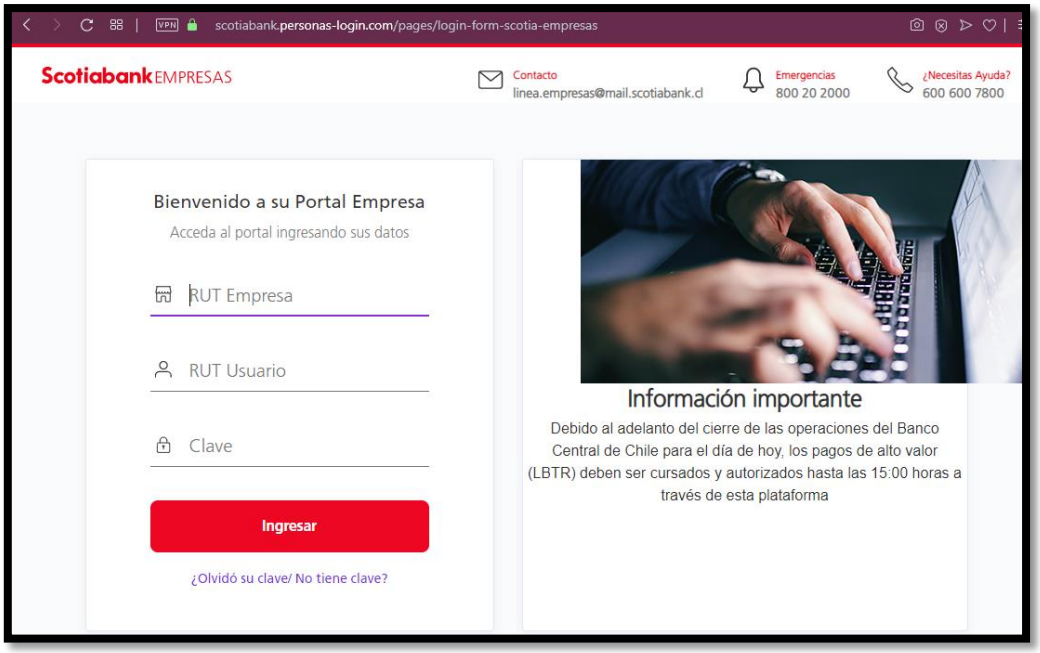


Imagen del sitio




scotiabank.personas-login.com/pages/login-form-scotia
21/01 2020 13:20:17 hrs.
Dólar $678,71
UF $27.666,77
IPSA 5.187,10
Portal de Inversiones
Scotiabank
Ir al Portal Scotiabank
Ingreso Personas
RUT
Clave
Olvidé mi Clave
Ingresar a Scotiaweb
Soy Cliente, pero no tengo clave
Bienvenidos
Comienza a vivir tu experiencia Scotiabank
Empieza a vivir tu experiencia aquí
¿Necesita Ayuda?
Centro de Contacto
600 6700 500
+56 (2) 276 86 219


scotiabank.personas-login.com/pages/login-form-scotia-empresas
ScotiabankEMPRESAS
Contacto
linea.empresas@mail.scotiabank.cl
Emergencias
800 20 2000
¿Necesitas Ayuda?
600 600 7800
Bienvenido a su Portal Empresa
Acceda al portal ingresando sus datos
RUT Empresa
RUT Usuario
Clave
Ingresar
¿Olvidó su clave/ No tiene clave?
Información importante
Debido al adelanto del cierre de las operaciones del Banco Central de Chile para el día de hoy, los pagos de alto valor (LBTR) deben ser cursados y autorizados hasta las 15:00 horas a través de esta plataforma

Whois

```
Domain name: personas-login.com
Registry Domain ID: 2480878065_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 0001-01-01T00:00:00.00Z
Creation Date: 2020-01-16T14:32:32.00Z
Registrar Registration Expiration Date: 2021-01-16T14:32:32.00Z
Registrar: NAMECHEAP INC
Registrar IANA ID: 1068
Registrar Abuse Contact Email: abuse@namecheap.com
Registrar Abuse Contact Phone: +1.6613102107
Reseller: NAMECHEAP INC
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: addPeriod https://icann.org/epp#addPeriod
Registry Registrant ID:
Registrant Name: WhoisGuard Protected
Registrant Organization: WhoisGuard, Inc.
Registrant Street: P.O. Box 0823-03411
Registrant City: Panama
Registrant State/Province: Panama
Registrant Postal Code:
Registrant Country: PA
Registrant Phone: +507.8365503
Registrant Phone Ext:
Registrant Fax: +51.17057182
Registrant Fax Ext:
Registrant Email: ee5036c22a0e44ddbc720ba5a8230697.protect@whoisguard.com
Registry Admin ID:
Admin Name: WhoisGuard Protected
Admin Organization: WhoisGuard, Inc.
Admin Street: P.O. Box 0823-03411
Admin City: Panama
Admin State/Province: Panama
Admin Postal Code:
Admin Country: PA
Admin Phone: +507.8365503
Admin Phone Ext:
Admin Fax: +51.17057182
Admin Fax Ext:
Admin Email: ee5036c22a0e44ddbc720ba5a8230697.protect@whoisguard.com
Registry Tech ID:
Tech Name: WhoisGuard Protected
Tech Organization: WhoisGuard, Inc.
Tech Street: P.O. Box 0823-03411
Tech City: Panama
Tech State/Province: Panama
Tech Postal Code:
Tech Country: PA
Tech Phone: +507.8365503
Tech Phone Ext:
Tech Fax: +51.17057182
Tech Fax Ext:
Tech Email: ee5036c22a0e44ddbc720ba5a8230697.protect@whoisguard.com
Name Server: dns1.registrar-servers.com
Name Server: dns2.registrar-servers.com
DNSSEC: unsigned
```

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: 2020.01.22 08:37:46 -03'00'