Alerta de seguridad informática	8FFR20-00227-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de Febrero de 2020
Última revisión	21 de Febrero 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 una IP que suplanta el sitio web oficial del 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

URLs

scotiachile[.]support[.]login[.]cl[.]recruitmentagency[.]net/scoticheyo2019

Domain recruitmentagency.net

recruitmentagency / net / Subdomains

record type	TTL	value		
A	14400	130.193.89.178		
NS	86400	dns2.certahosting.co.uk	Zones on DNS server	46.101.89.157
NS	86400	dns1.certahosting.co.uk	Zones on DNS server	95.172.30.61
MX	14400	0 recruitmentagency.net		
TXT	14400	v=spf1 +a +mx +ip4:130.193.89.178 +include:spf.antispamcloud.com ~all		

SOA	86400	Mname	dns1.certahosting.co.uk
		Rname	servers.certahosting.co.uk
		Serial number	2020022105
		Refresh	3600
		Retry	7200
		Expire	1209600
		Minimum TTL	86400

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

Certificados

Subject DN	CN=scotiachile.support.login.cl.recruitmentagency.net
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	407055911152134501355918473669554739298816
Validity	2020-02-21 06:07:08 **to** 2020-05-21 06:07:08 (90 days, 0:00:00)
Names	scotiachile.support.login.cl.recruitmentagency.net

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

IP

130[.]193[.]89[.]178

Domain
scotiachile.support.login.cl.recruitmentagency.net
is located on
IP address
<< 130.193.89.178 >>

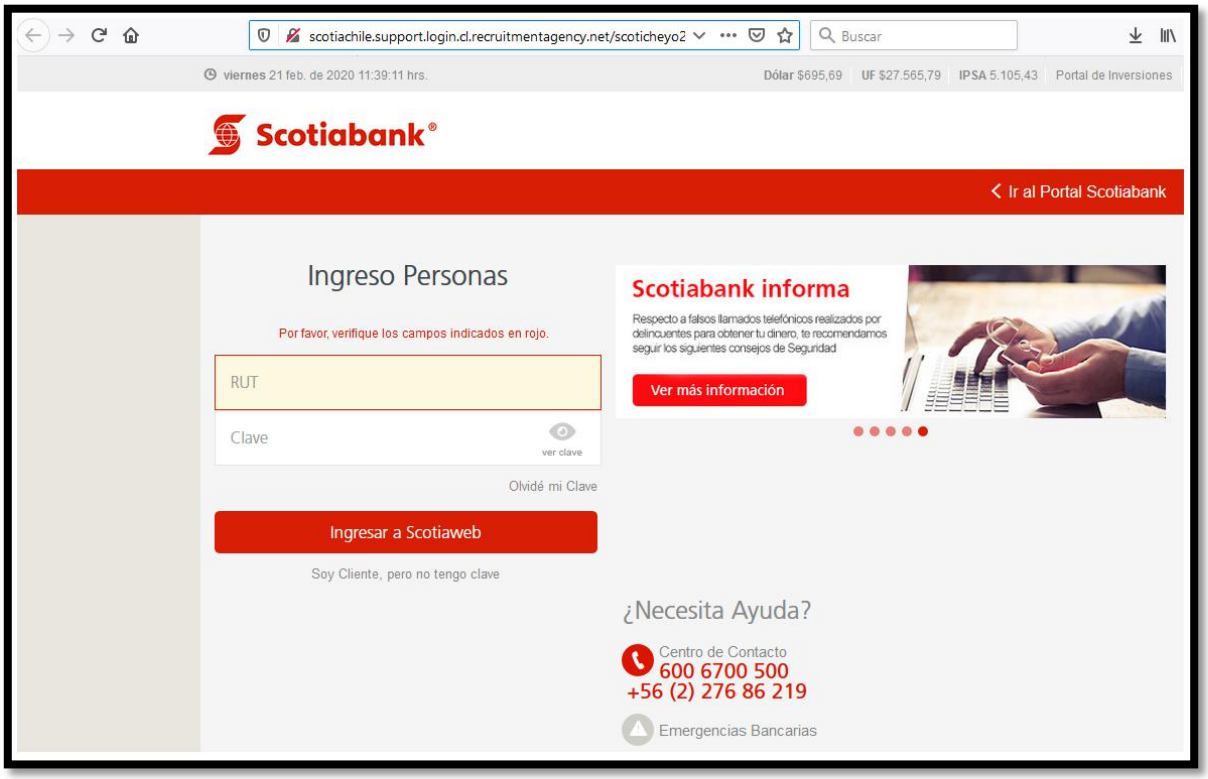
Block start	130.193.89.176
End of block	130.193.89.183
Block size	8 Domains in block
Block name	CERTA-HOSTING
AS number	34920
Parent block	130.193.80.0 - 130.193.95.254
Organization	Certa Hosting
City	London
Region/State	England
Country	GB , United Kingdom
Host name	cloud101.certahosting.co.uk
Web server	LiteSpeed
Powered by	PHP/5.5.38
Domain count	>= 11 Servers around
Domains	1 blportraits.co.uk 2 certainternet.com 3 email.moneyforgadgets.com 4 essentialoilsforthefrazzled.com 5 functionsmusic.com 6 jowestaway.com 7 martintolmuskmusic.com 8 nextdayphone.co.uk

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

Localización

United Kingdom, London, England

Imagen del sitio



Whois

```
Domain Name: RECRUITMENTAGENCY.NET
Registry Domain ID: 79679040_DOMAIN_NET-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Updated Date: 2019-11-14T17:24:47Z
Creation Date: 2001-11-13T19:45:36Z
Registrar Registration Expiration Date: 2020-11-13T19:45:36Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited
Registrant Organization: RecruitmentAgency.Net
Registrant State/Province:
Registrant Country: UK
Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=RECRUITMENTAGENCY.NET
Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=RECRUITMENTAGENCY.NET
Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=RECRUITMENTAGENCY.NET
Name Server: DNS1.CERTAHOSTING.CO.UK
Name Server: DNS2.CERTAHOSTING.CO.UK
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: 2020.02.21 18:41:26 -03'00'