Alerta de seguridad informática	8FFR-00108-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de Noviembre de 2019
Última revisión	12 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

https[://]www[.]scotiafreeemail[.]com/site/choose-type[.]php

Domain scotiafreeemail.com

scotiafreeemail / com / Subdomains

record type	TTL	value		
A	900	80.211.129.33		
NS	900	ns1.amenworld.com	Zones on DNS server	81.88.63.34
NS	900	ns2.amenworld.com	Zones on DNS server	81.88.63.40
MX	900	10 mail-pt.securemail.pro		81.88.48.101
TXT	900	v=spf1 include:spf.webapps.net ~all		
SOA	900	Mname	ns1.amenworld.com	
		Rname	root.amen.fr	
		Serial number	2019110704	
		Refresh	86400	
		Retry	7200	
		Expire	2592000	
		Minimum TTL	300	

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

Certificado

Criteria: Identity = 'scotiafreeemail.com'

Certificates

crt.sh ID	Logged At	Not Before	Not After	Issuer Name
2083382035	2019-11-07	2019-11-07	2020-02-05	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2081384959	2019-11-07	2019-11-07	2020-02-05	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2080502287	2019-11-07	2019-11-07	2020-02-05	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2080502182	2019-11-07	2019-11-07	2020-02-05	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2074649160	2019-11-05	2019-11-05	2020-02-03	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2074649048	2019-11-05	2019-11-05	2020-02-03	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2072438905	2019-11-05	2019-11-04	2020-02-02	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2072453506	2019-11-05	2019-11-04	2020-02-02	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´s

80[.]211[.]129[.]33

Domain scotiafreeemail.com is located on IP address << 80.211.129.33 >>	
Block start	80.211.129.0
End of block	80.211.129.255
Block size	256 Domains in block
Block name	ARUBA-NET
AS number	31034
Parent block	80.211.128.0 - 80.211.191.255
Organization	Aruba S.p.A. - Cloud Services Farm2
City	Arezzo
Region/State	Toscana
Country	IT , Italy
Host name	host33-129-211-80.serverdedicati.aruba.it
Domain count	>= 2 Servers around
Domains	1 scotiafreeemail.com 2 scotiaseguridad.site

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

Localización

Arezzo, Toscana, Italia

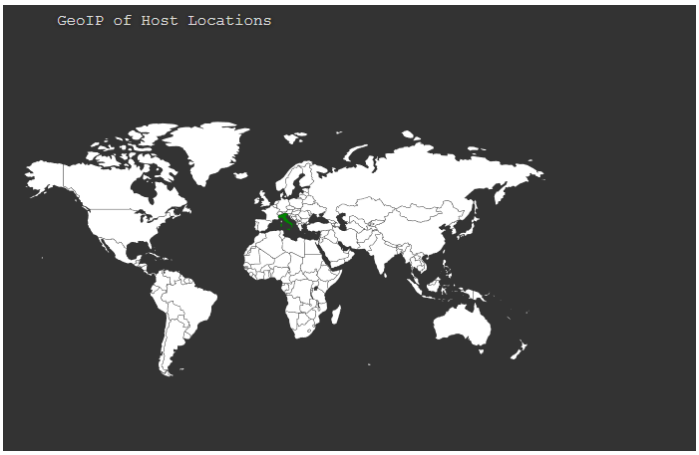
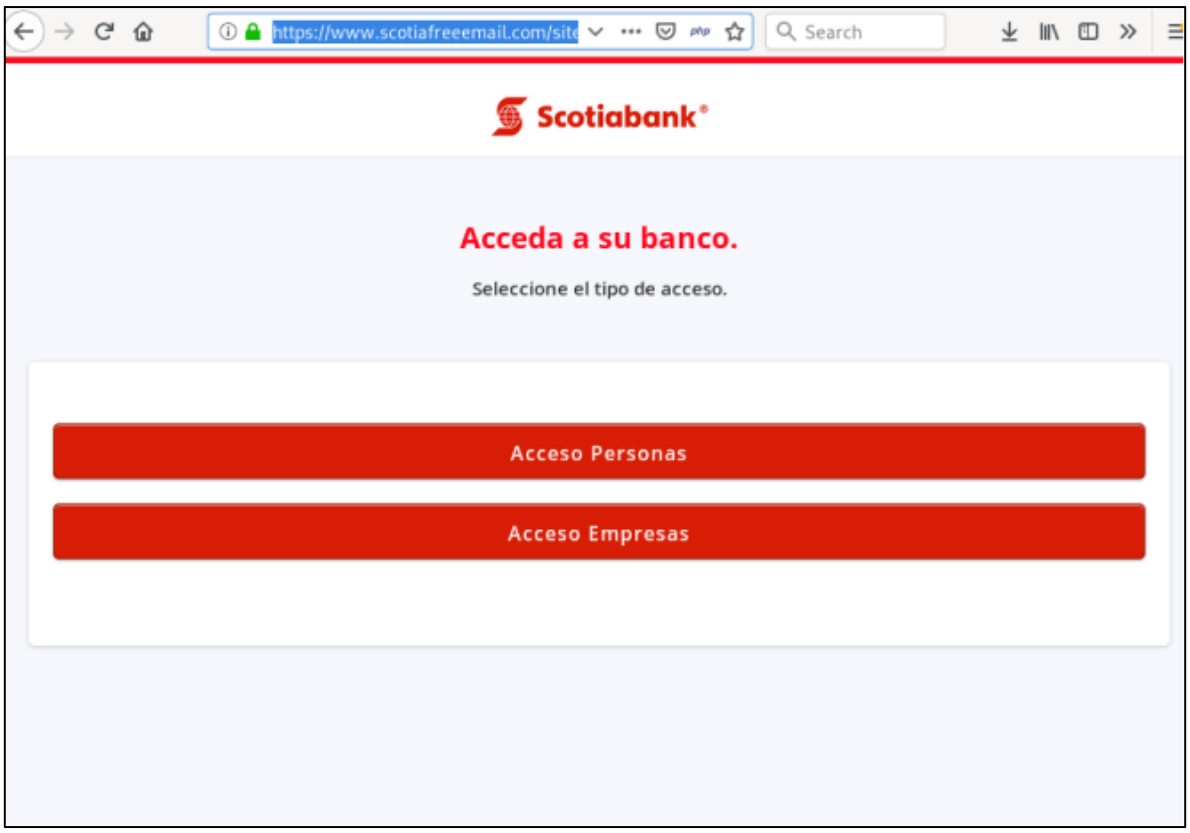


Imagen del sitio


https://www.scotiafreeemail.com/site
Search
Scotiabank
Acceda a su banco.
Seleccione el tipo de acceso.
Acceso Personas
Acceso Empresas

Whois

```
Domain Name: SCOTIAFREEEMAIL.COM
Registry Domain ID: 2451599351_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.register.it
Registrar URL: http://we.register.it
Updated Date: 2019-11-05T00:00:00Z
Creation Date: 2019-11-05T00:00:00Z
Registrar Registration Expiration Date: 2020-11-04T00:00:00Z
Registrar: REGISTER S.P.A.
Registrar IANA ID: 168
Registrar Abuse Contact Email: abuse@register.it
Registrar Abuse Contact Phone: +39.05520021555
Reseller:
Domain Status: ok https://icann.org/epp#ok
Registry Registrant ID:
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: mg
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: BR
Registrant Phone: REDACTED.FORPRIVACY
Registrant Phone Ext:
Registrant Fax: REDACTED.FORPRIVACY
Registrant Fax Ext:
Registrant Email: redacted for privacy
Registry Admin ID:
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: mg
Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: BR
Admin Phone: REDACTED.FORPRIVACY
Admin Phone Ext:
Admin Fax: REDACTED.FORPRIVACY
Admin Fax Ext:
Admin Email: redacted for privacy
Registry Tech ID:
Tech Name: REDACTED FOR PRIVACY
Tech Organization: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech City: REDACTED FOR PRIVACY
Tech State/Province: LISBOA
Tech Postal Code: REDACTED FOR PRIVACY
Tech Country: PT
Tech Phone: REDACTED.FORPRIVACY
Tech Phone Ext:
Tech Fax: REDACTED.FORPRIVACY
Tech Fax Ext:
Tech Email: redacted for privacy
Name Server: NS1.AMENWORLD.COM
Name Server: NS2.AMENWORLD.COM
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of whois database: 2019-11-11T20:45:45Z <<<
```

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: 2019.11.12 17:38:19 -03'00'