Alerta de seguridad informática	8FFR-00112-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de Noviembre de 2019
Última revisión	16 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[.]seguridadsms[.]pt/site/choose-type[.]php

Domain seguridadsms.pt			
seguridadsms / pt / Subdomains			
TTL	value		
900	80.211.129.33		
900	ns2.amenworld.com	Zones on DNS server	81.88.63.40
900	ns1.amenworld.com	Zones on DNS server	81.88.63.34
900	10 mail-pt.securemail.pro		81.88.48.101
900	v=spf1 include:spf.webapps.net ~all		
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 = 'seguridadsms.pt'				
Certificates	crt.sh ID	Logged At ⇧	Not Before	Not After	Issuer Name
	2083252887	2019-11-07	2019-11-07	2020-02-05	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2082696165	2019-11-07	2019-11-07	2020-02-05	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2078462891	2019-11-06	2019-11-06	2020-02-04	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2078462873	2019-11-06	2019-11-06	2020-02-04	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2074646435	2019-11-05	2019-11-05	2020-02-03	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2075256396	2019-11-05	2019-11-05	2020-02-03	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2072435526	2019-11-05	2019-11-04	2020-02-02	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2072482267	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 seguridadsms.pt 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

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

Localización

Arezzo, Toscana, Italia

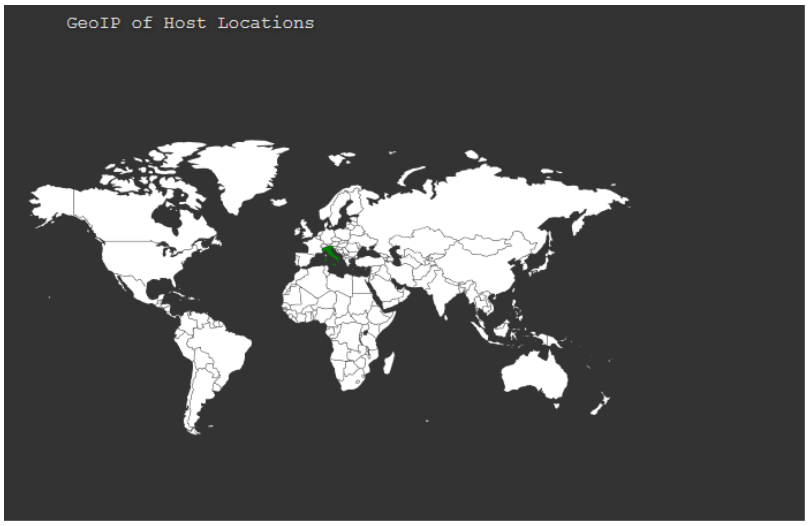
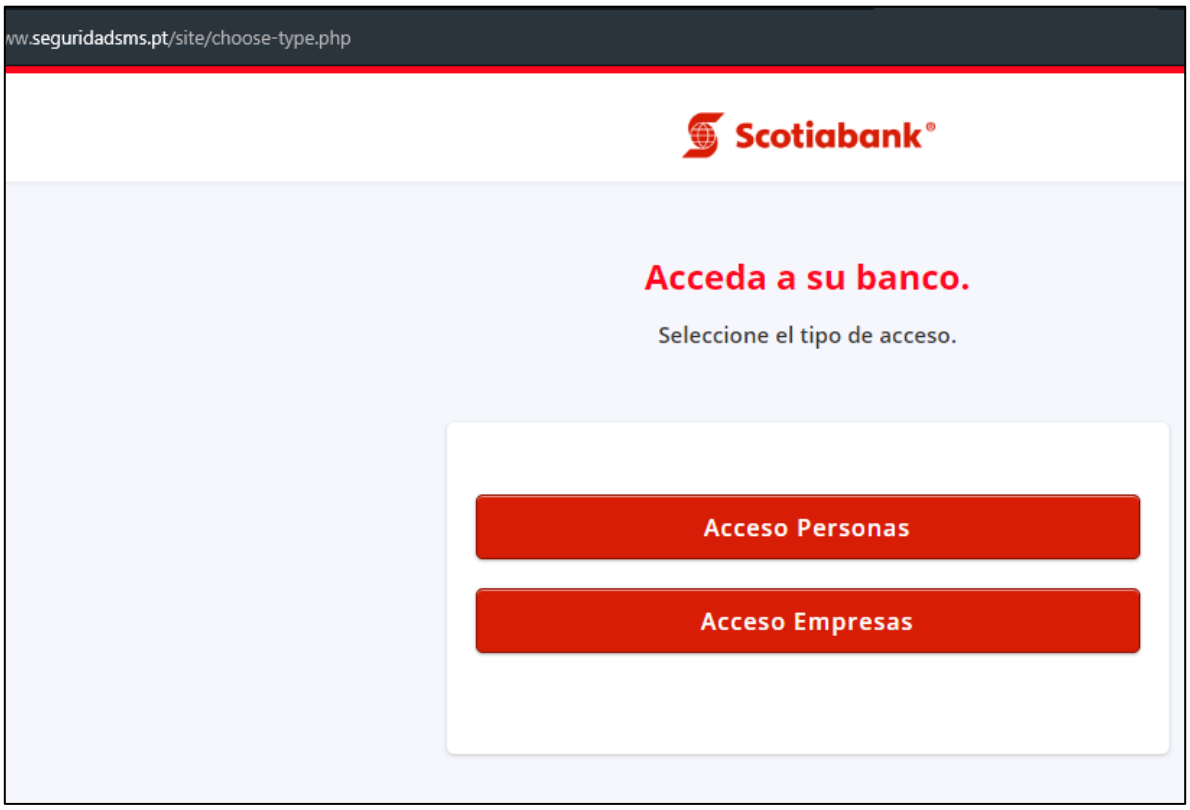


Imagen del sitio



Whois

```
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

refer:        whois.dns.pt

domain:       PT

organisation: Associação DNS.PT
address:      Rua Latino Coelho, nº13, 5ºpiso
address:      1050-132 Lisboa
address:      Portugal

contact:      administrative
name:         Luisa Lopes Gueifão
organisation: Associação DNS.PT
address:      Rua Latino Coelho, nº13, 5ºpiso
address:      1050-132 Lisboa
address:      Portugal
phone:        (+351) 211308200
fax-no:       (+351) 211312720
e-mail:       lgueifao@dns.pt

contact:      technical
name:         Eduardo Manuel Laureano Duarte
organisation: Associação DNS.PT
address:      Rua Latino Coelho, nº13, 5ºpiso
address:      1050-132 Lisboa
address:      Portugal
phone:        (+351) 211308200
fax-no:       (+351) 211312720
e-mail:       eduardo.duarte@dns.pt

nserver:      A.DNS.PT 185.39.208.1 2a04:6d80:0:0:0:0:0:1
nserver:      B.DNS.PT 194.0.25.23 2001:678:20:0:0:0:0:23
nserver:      C.DNS.PT 2001:500:14:6105:ad:0:0:1 204.61.216.105
nserver:      D.DNS.PT 185.39.210.1 2a04:6d82:0:0:0:0:0:1
nserver:      E.DNS.PT 193.136.192.64 2001:690:a00:4001:0:0:0:64
nserver:      F.DNS.PT 162.88.45.1 2600:2000:3009:0:0:0:0:1
nserver:      G.DNS.PT 193.136.2.226 2001:690:a80:4001:0:0:0:100
nserver:      NS.DNS.BR 200.160.0.5 2001:12ff:0:a20:0:0:0:5
nserver:      NS2.NIC.FR 192.93.0.4 2001:660:3005:1:0:0:1:2
nserver:      SNS-PB.ISC.ORG 192.5.4.1 2001:500:2e:0:0:0:0:1
ds-rdata:     40995 7 2 ABF415ED56E88C5F05434BBF62CDD90B574D6445A37AE5CC9B84638A
B5B9E656
ds-rdata:     40995 7 1 43DEDCEEBA41380680784AA531819A6ED8172B6D

whois:        whois.dns.pt

status:       ACTIVE
remarks:      Registration information: http://www.dns.pt/

created:      1988-06-30
changed:      2018-08-10
source:       IANA

Domain: seguridadsms.pt
Domain Status: Registered
Creation Date: 04/11/2019 23:41:20
Expiration Date: 04/11/2020 23:41:20
Owner Name:
```

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: 2019.11.16 14:13:30 -03'00'