Alerta de seguridad informática	8FFR-00157-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de diciembre de 2019
Última revisión	19 de diciembre 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 dos portales fraudulentos asociados a una IP que suplantan el sitio web oficial del **Banco Santander**, 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:
santanderchile[.]sytes[.]net
santander[.]bancocl[.]net

Domain sytes.net

sytes / net / Subdomains

record type	TTL	value		
A	60	8.23.224.108		
NS	86400	nf1.no-ip.com	Zones on DNS server	194.62.182.53
NS	86400	nf2.no-ip.com	Zones on DNS server	45.54.64.53
NS	86400	nf3.no-ip.com	Zones on DNS server	204.16.253.53
NS	86400	nf4.no-ip.com	Zones on DNS server	194.62.183.53
NS	86400	nf5.no-ip.com	Zones on DNS server	204.16.253.53
MX	600	10 mail2.no-ip.com		69.65.5.119
TXT	360	v=spf1 include:no-ip.com -all		
SOA	60	Mname	nf1.no-ip.com	
		Rname	hostmaster.no-ip.com	
		Serial number	2086053747	
		Refresh	600	
		Retry	300	
		Expire	604800	
		Minimum TTL	600	

Domain bancocl.net

bancocl / net / Subdomains

record type	TTL	value		
A	1800	162.255.119.129		
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	1576627930	
		Refresh	3600	
		Retry	1801	
		Expire	604800	
		Minimum TTL	3601	

Ilustración 1 Dominio donde se Aloja Url de Santander, Falso y DNS que utiliza

Certificados

Subject DN	CN=santanderchile.sytes.net
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	280441775909439652798591978603782826544421
Validity	2019-12-17 16:05:02 **to** 2020-03-16 16:05:02 (90 days, 0:00:00)
Names	santanderchile.sytes.net

Subject DN	CN=santander.bancocl.net
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	311742007358136708435009714275329769615576
Validity	2019-12-18 11:45:19 **to** 2020-03-17 11:45:19 (90 days, 0:00:00)
Names	santander.bancocl.net

Ilustración 2 Certificado Utilizado en Url del sitio Falso de Santander

IP

144[.]208[.]127[.]162

Domain santanderchile.sytes.net is located on IP address << 144.208.127.162 >>

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	2n2m.com

Domain santander.bancocl.net is located on IP address << 144.208.127.162 >>	
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	2n2m.com

Ilustración 3 Ip de Origen donde se aloja Sitio Falso de Santander

Localización

Piscataway, New Jersey, Estados Unidos

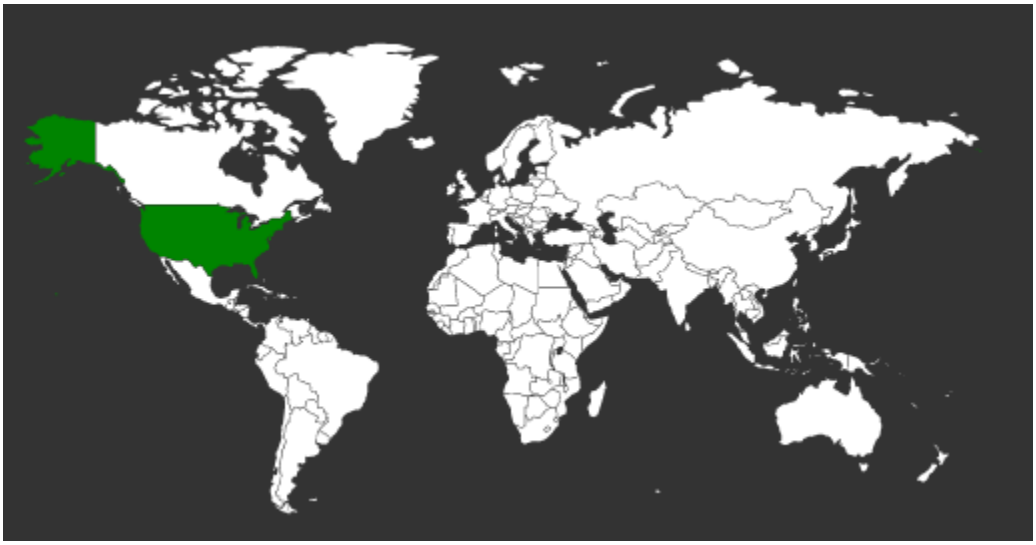
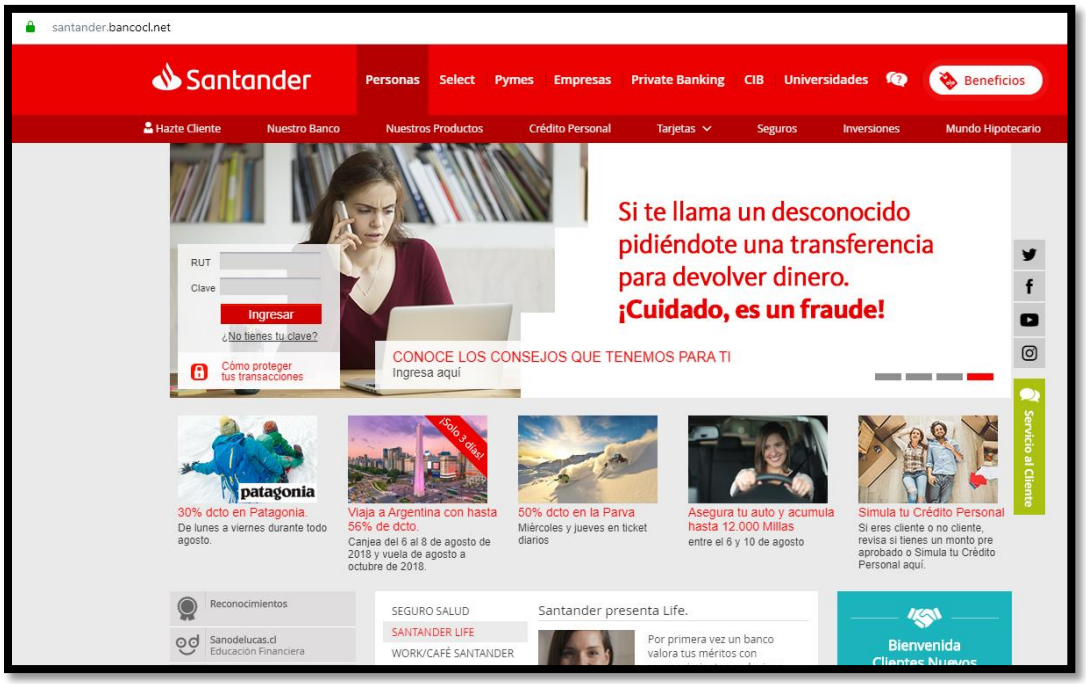


Imagen del sitio



Whois

```
Domain Name: sytes.net
Registry Domain ID: 5534045_DOMAIN_NET-VRSN
Registrar WHOIS Server: whois.srsplus.com
Registrar URL: http://srsplus.com
Updated Date: 2017-01-31T17:05:30Z
Creation Date: 1999-04-22T04:00:00Z
Registrar Registration Expiration Date: 2021-04-22T04:00:00Z
Registrar: TLDS LLC. d/b/a SRSPlus
Registrar IANA ID: 320
Reseller:
Domain Status: clientTransferProhibited http://icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Dan Durrer
Registrant Organization: No-IP.com
Registrant Street: 425 Maestro  Dr. Second Floor
Registrant City: Reno
Registrant State/Province: NV
Registrant Postal Code: 89511
Registrant Country: US
Registrant Phone: +1.7758531883
Registrant Phone Ext.:
Registrant Fax:
Registrant Fax Ext.:
Registrant Email: domains@no-ip.com
Registry Admin ID:
Admin Name: Dan Durrer
Admin Organization: No-IP.com
Admin Street: 425 Maestro  Dr. Second Floor
Admin City: Reno
Admin State/Province: NV
Admin Postal Code: 89511
Admin Country: US
Admin Phone: +1.7758531883
Admin Phone Ext.:
Admin Fax:
Admin Fax Ext.:
Admin Email: domains@no-ip.com
Registry Tech ID:
Tech Name: Dan Durrer
Tech Organization: No-IP.com
Tech Street: 425 Maestro  Dr. Second Floor
Tech City: Reno
Tech State/Province: NV
Tech Postal Code: 89511
Tech Country: US
Tech Phone: +1.7758531883
Tech Phone Ext.:
Tech Fax:
Tech Fax Ext.:
Tech Email: domains@no-ip.com
Name Server: nf3.no-ip.com
Name Server: nf2.no-ip.com
Name Server: nf4.no-ip.com
Name Server: nf1.no-ip.com
DNSSEC: Unsigned
Registrar Abuse Contact Email: abuse@web.com
Registrar Abuse Contact Phone: +1.8773812449
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2019-12-18T18:53:25Z <<<
```

```
Domain name: bancocl.net
Registry Domain ID: 2468583618_DOMAIN_NET-VRSN
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 0001-01-01T00:00:00.00Z
Creation Date: 2019-12-18T00:11:03.00Z
Registrar Registration Expiration Date: 2020-12-18T00:11:03.00Z
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: 4e6c90403ccb4bf39d38a239cd9be3b9.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: 4e6c90403ccb4bf39d38a239cd9be3b9.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: 4e6c90403ccb4bf39d38a239cd9be3b9.protect@whoisguard.com
Name Server: dns1.registrar-servers.com
Name Server: dns2.registrar-servers.com
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2019-12-18T12:00:28.85Z <<<
```

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.