Alerta de seguridad cibernética	8FFR20-00447-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de Junio de 2020
Última revisión	15 de Junio 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 dos portales fraudulentos asociados a dos IPs que suplantan el sitio web oficial del Banco de Chile , 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 compromiso

URLs
https[:]//hostalrestauranteentalara[.]com
https[:]//frdscd[.]online/accessweb/bancochile-web/persona/login/index[.]php

IPs
68[.]65[.]123[.]121
199[.]188[.]206[.]170

Dominio donde se aloja URL

Domain hostalrestauranteentalara.com

hostalrestauranteentalara / com / Subdomains

record type	TTL	value		
A	1799	199.188.206.170		
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
SOA	3601	Mname: dns1.registrar-servers.com Rname: hostmaster.registrar-servers.com Serial number: 1590847801 Refresh: 43200 Retry: 3600 Expire: 604800 Minimum TTL: 3601		

Domain frdscd.online

frdscd / online / Subdomains

record type	TTL	value		
A	1200	68.65.123.121		
NS	1800000	dns1.namecheaphosting.com	Zones on DNS server	156.154.132.200
NS	1800000	dns2.namecheaphosting.com	Zones on DNS server	156.154.133.200
MX	1200	0 mail.frdscd.online		
TXT	1200	v=spf1 +a +mx +ip4:68.65.123.83 +ip4:68.65.123.121 include:spf.web-hosting.com ~all		
SOA	1800000	Mname: dns1.namecheaphosting.com Rname: cpanel.tech.namecheap.com Serial number: 1592054048 Refresh: 86400 Retry: 7200 Expire: 3600000 Minimum TTL: 86400		

Certificado

TLS Certificate

```
Common Name = frdscd.online
Subject Alternative Names = frdscd.online, www.frdscd.online
Issuer = Sectigo RSA Domain Validation Secure Server CA
Serial Number = 01463268017CD9061DF7A3E3F80ECDB2
SHA1 Thumbprint = 87DF9C91C929FAD3F12F534CD32556F28DBCA440
Key Length = 2048
Signature algorithm = SHA256-RSA
Secure Renegotiation:
```

Certificate Name matches frdscd.online

Subject frdscd.online

Valid from 13/Jun/2020 to 13/Jun/2021

Issuer Sectigo RSA Domain Validation Secure Server CA

Subject Sectigo RSA Domain Validation Secure Server CA

Valid from 02/Nov/2018 to 31/Dec/2030

Issuer USERTrust RSA Certification Authority

Subject USERTrust RSA Certification Authority

Valid from 12/Mar/2019 to 31/Dec/2028

Issuer AAA Certificate Services

Ip de origen donde se aloja sitio

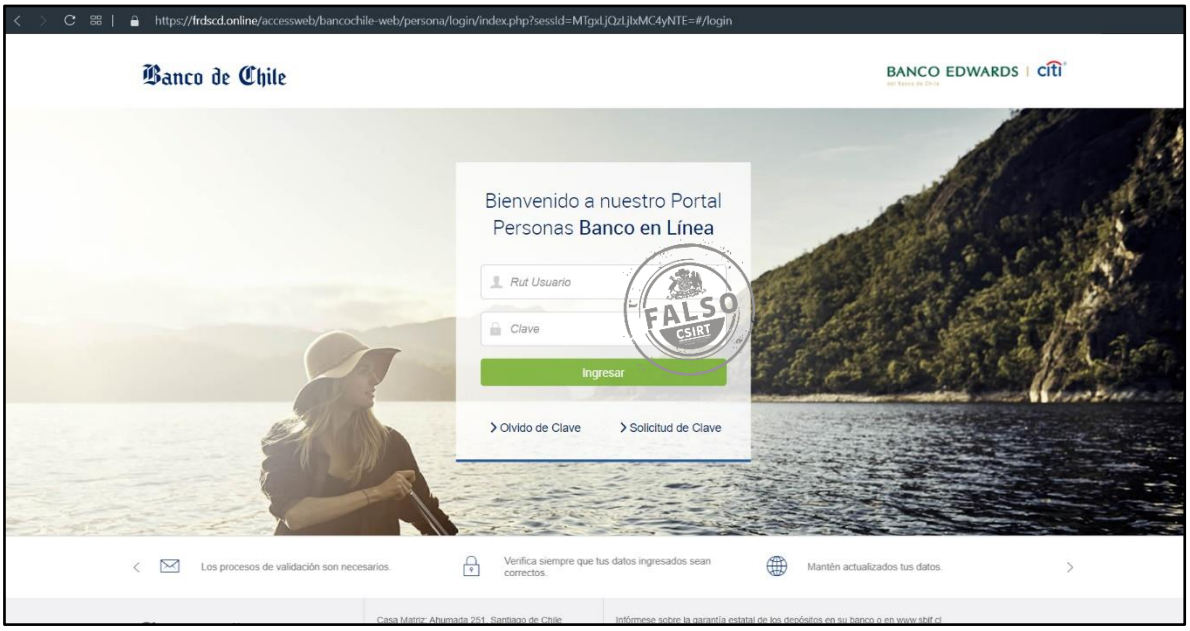
Domain hostalrestauranteentalara.com is located on IP address << 199.188.206.170 >>	
Block start	199.188.200.0
End of block	199.188.207.255
Block size	2048 Domains in block
Block name	NCNET-1
AS number	22612
Parent block	199.0.0.0 - 199.255.255.255
Organization	Namecheap, Inc.

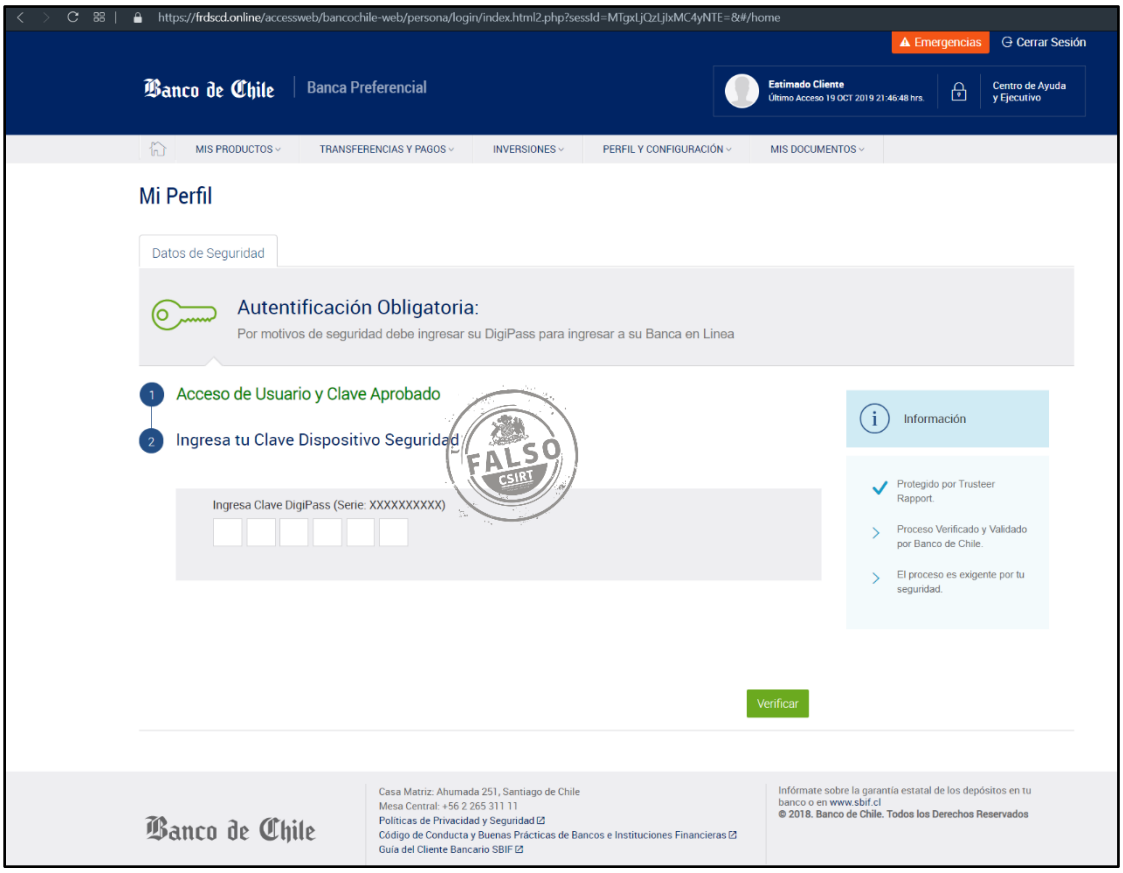
Domain frdscd.online is located on IP address << 68.65.123.121 >>	
Block start	68.65.120.0
End of block	68.65.123.255
Block size	1024 Domains in block
Block name	NCNET-7
AS number	22612
Parent block	68.0.0.0 - 68.255.255.255
Organization	Namecheap, Inc.

Localización

Atlanta, Georgia, Estados Unidos

Imágenes del sitio





Whois

```
Domain Name: FRDSCD.ONLINE
Registry Domain ID: D189483789-CNIC
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: https://namecheap.com
Updated Date: 2020-06-13T13:13:28.0Z
Creation Date: 2020-06-13T13:13:14.0Z
Registry Expiry Date: 2021-06-13T23:59:59.0Z
Registrar: Namecheap
Registrar IANA ID: 1068
Name Server: DNS1.NAMECHEAPHOSTING.COM
Name Server: DNS2.NAMECHEAPHOSTING.COM
DNSSEC: unsigned
```

```
Domain name: hostalrestauranteentalara.com
Registry Domain ID: 2501467320_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: 2020-03-09T12:52:20.00Z
Registrar Registration Expiration Date: 2021-03-09T12:52:20.00Z
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
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: 5c954223301d4e2fa3f6d6c43e560ded.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.