Alerta de seguridad informática	8FFR-00139-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	4 de Diciembre de 2019
Última revisión	4 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 tres portales fraudulentos asociados a dos IP que suplantan el sitio web oficial de **Banco Estado**, 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:
www[.]naillounge bypinky[.]com/wp-content/www[.]bancoestado[.]cl/
estadochile[.]com
estadochile[.]com/pages/login

Domain naillounge bypinky.com

naillounge bypinky / com / Subdomains

record type	TTL	value		
A	10800	160.153.129.229		
NS	3600	ns76.domaincontrol.com	Zones on DNS server	173.201.75.48
NS	3600	ns75.domaincontrol.com	Zones on DNS server	97.74.107.48

SOA	3600	Mname	ns75.domaincontrol.com
		Rname	dns.jomax.net
		Serial number	2019100602
		Refresh	28800
		Retry	7200
		Expire	604800
		Minimum TTL	600

Domain estadochile.com

estadochile / com / Subdomains

record type	TTL	value		
A	1799	192.3.179.198		
NS	1800	dns1.registrar-servers.com	Zones on DNS server	216.87.155.33
NS	1800	dns2.registrar-servers.com	Zones on DNS server	216.87.152.33
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	2019120205
		Refresh	43200
		Retry	3600
		Expire	604800
		Minimum TTL	3601

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

Certificados

Subject DN	CN=estadochile.com
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	399226940546532817084012280722282621875642
Validity	2019-12-03 11:35:33 **to** 2020-03-02 11:35:33 (90 days, 0:00:00)
Names	estadochile.com

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

IP

160.153.129.229

192.3.179.198

Domain nailloungebypinky.com is located on IP address << 160.153.129.229 >>

Block start	160.153.0.0
End of block	160.153.255.255
Block size	65536 Domains in block
Block name	GO-DADDY-COM-LLC
AS number	26496
Parent block	160.0.0.0 - 160.255.255.255
Organization	GoDaddy.com, LLC
City	Scottsdale
Region/State	Arizona
Country	US , United States
Reg. date	2011-09-01
Host name	ip-160-153-129-229.ip.secureserver.net
Web server	Apache/2.4.23

Domain estadochile.com is located on IP address << 192.3.179.198 >>

Block start	192.3.179.0
End of block	192.3.179.255
Block size	256 Domains in block
Block name	CC-192-3-179-0-24
AS number	36352
Parent block	192.3.0.0 - 192.3.255.255
Organization	CC Customer
City	New York City
Region/State	New York
Country	US , United States
Reg. date	2014-02-17
Host name	192-3-179-198-host.colocrossing.com

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

Localización

Scotdale, Arizona, United States
New York City, New York

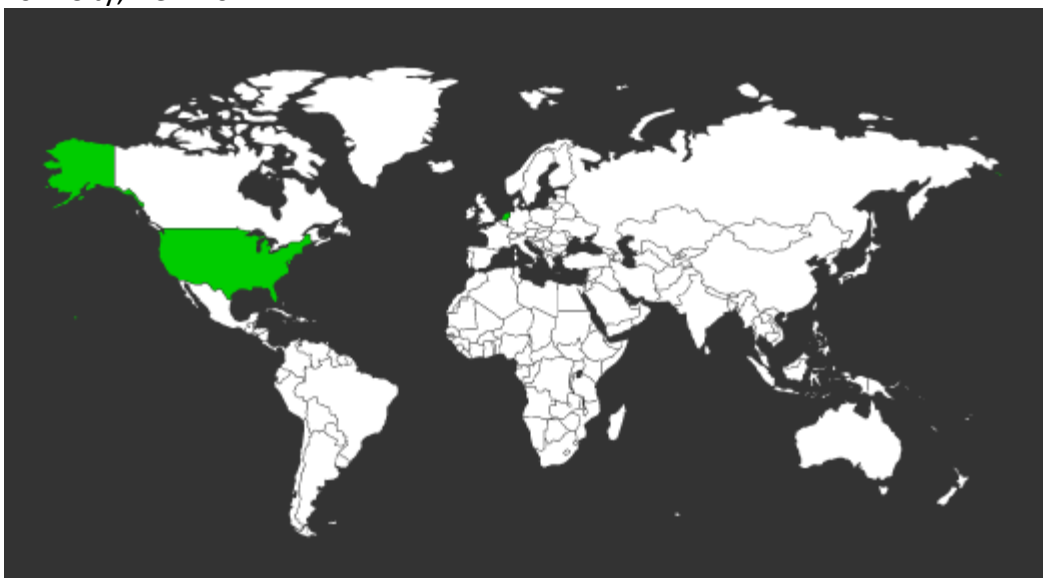
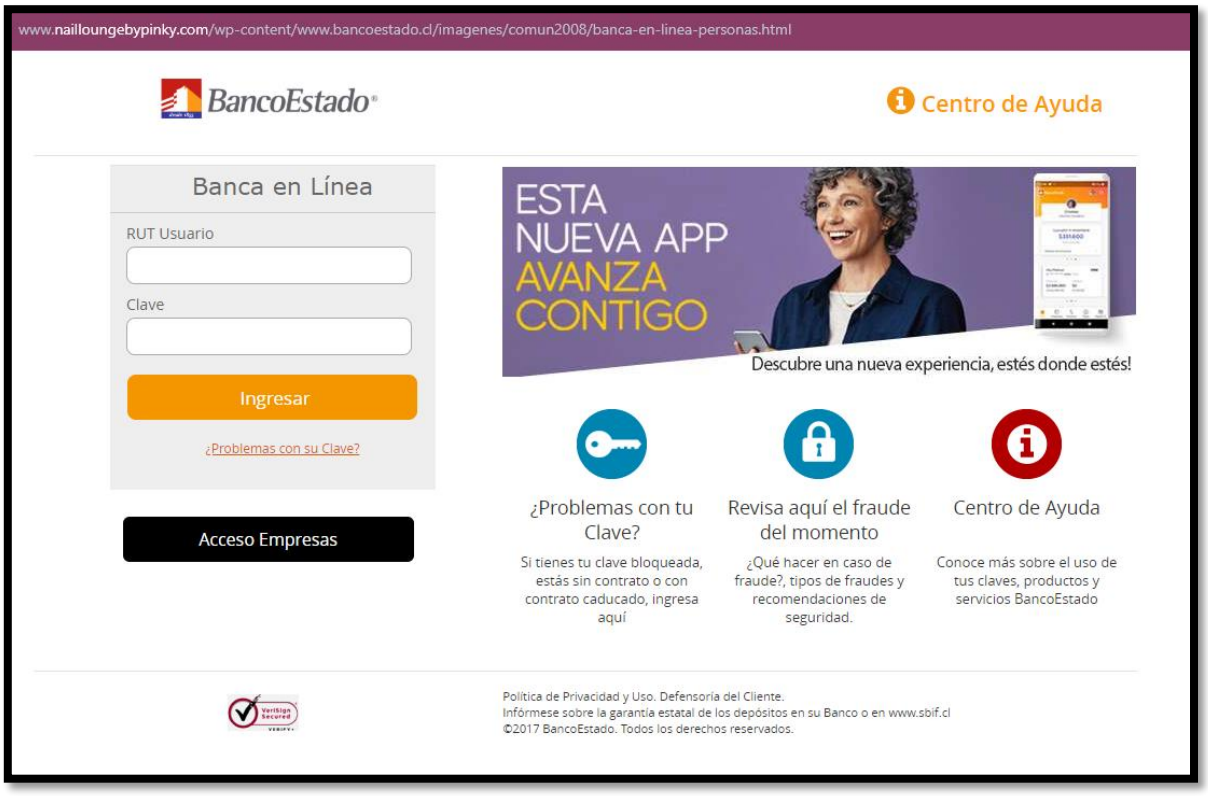
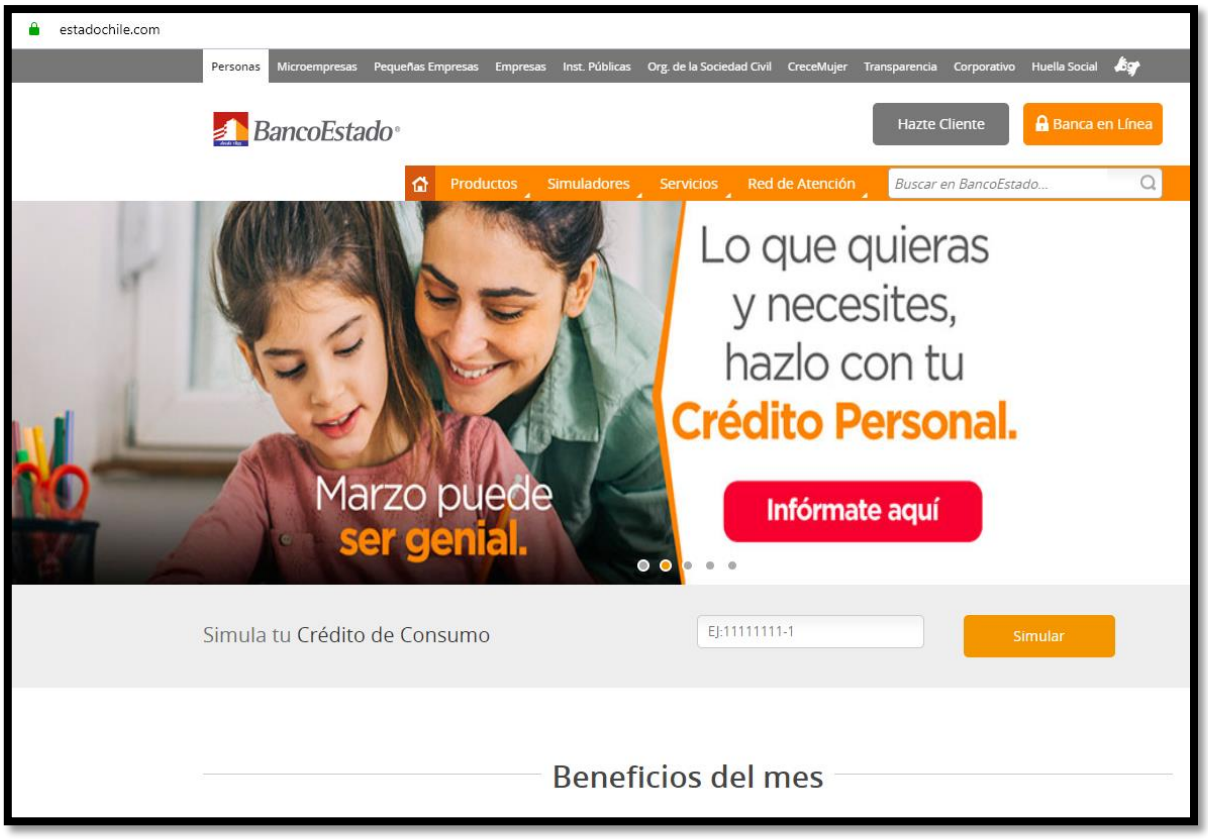
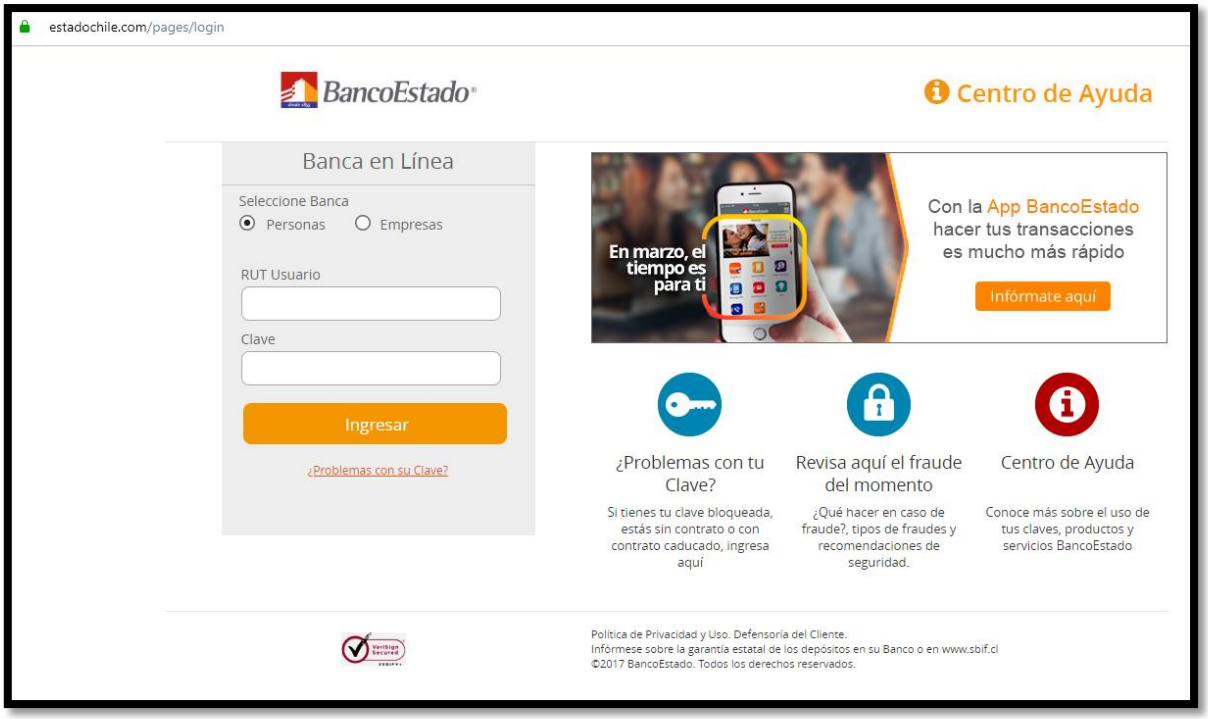


Imagen del sitio




estadochile.com
Personas
Microempresas
Pequeñas Empresas
Empresas
Inst. Públicas
Org. de la Sociedad Civil
CreceMujer
Transparencia
Corporativo
Huella Social
BancoEstado
Hazte Cliente
Banca en Línea
Productos
Simuladores
Servicios
Red de Atención
Buscar en BancoEstado...
Marzo puede ser genial.
Lo que quieras y necesites, hazlo con tu Crédito Personal.
Infórmate aquí
Simula tu Crédito de Consumo
EJ:11111111-1
Simular
Beneficios del mes


estadochile.com/pages/login
BancoEstado
Centro de Ayuda
Banca en Línea
Seleccione Banca
Personas
Empresas
RUT Usuario
Clave
Ingresar
¿Problemas con su Clave?
En marzo, el tiempo es para ti
Con la App BancoEstado hacer tus transacciones es mucho más rápido
Infórmate aquí
¿Problemas con tu Clave?
Si tienes tu clave bloqueada, estás sin contrato o con contrato caducado, ingresa aquí
Revisa aquí el fraude del momento
¿Qué hacer en caso de fraude?, tipos de fraudes y recomendaciones de seguridad.
Centro de Ayuda
Conoce más sobre el uso de tus claves, productos y servicios BancoEstado
Política de Privacidad y Uso. Defensoría del Cliente.
Infórmese sobre la garantía estatal de los depósitos en su Banco o en www.sbif.cl
©2017 BancoEstado. Todos los derechos reservados.

Whois

```
Domain Name: naillounGebypinky.com
Registry Domain ID: 2198017334_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Updated Date: 2018-12-10T19:12:31Z
Creation Date: 2017-12-09T19:36:05Z
Registrar Registration Expiration Date: 2019-12-09T19:36:05Z
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#clientTransferP
rohibited
Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhi
bited
Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibi
ted
Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhi
bited
Registrant Organization: concept Studio
Registrant State/Province: punjab
Registrant Country: PK
Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/w
hois/results.aspx?domain=naillounGebypinky.com
Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/
results.aspx?domain=naillounGebypinky.com
Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/r
esults.aspx?domain=naillounGebypinky.com
Name Server: NS75.DOMAINCONTROL.COM
Name Server: NS76.DOMAINCONTROL.COM
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2019-12-03T14:00:00Z <<<

For more information on Whois status codes, please visit https://www.icann.org/r
esources/pages/epp-status-codes-2014-06-16-en

Notes:

IMPORTANT: Port43 will provide the ICANN-required minimum data set per
ICANN Temporary Specification, adopted 17 May 2018.
Visit https://whois.godaddy.com to look up contact data for domains
not covered by GDPR policy.

The data contained in GoDaddy.com, LLC's WhoIs database,
while believed by the company to be reliable, is provided "as is"
with no guarantee or warranties regarding its accuracy.  This
information is provided for the sole purpose of assisting you
in obtaining information about domain name registration records.
Any use of this data for any other purpose is expressly forbidden without the pr
ior written
permission of GoDaddy.com, LLC.  By submitting an inquiry,
you agree to these terms of usage and limitations of warranty.  In particular,
you agree not to use this data to allow, enable, or otherwise make possible,
dissemination or collection of this data, in part or in its entirety, for any
purpose, such as the transmission of unsolicited advertising and
and solicitations of any kind, including spam.  You further agree
not to use this data to enable high volume, automated or robotic electronic
processes designed to collect or compile this data for any purpose,
including mining this data for your own personal or commercial purposes.
```

```
Domain name: estadochile.com
Registry Domain ID: 2462438083_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: 2019-12-02T15:31:17.00Z
Registrar Registration Expiration Date: 2020-12-02T15:31:17.00Z
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#clientTransferProh
ibited
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: 391leba4c81248ab8ccc71dbe05fdec7.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: 391leba4c81248ab8ccc71dbe05fdec7.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: 391leba4c81248ab8ccc71dbe05fdec7.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: 2019-12-03T09:57:19.47Z <<<
```

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: 2019.12.04 14:54:57 -03'00'