

Alerta de seguridad informática	8FFR-00069-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Septiembre de 2019
Última revisión	24 de Septiembre de 2019

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigaciones 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 loC 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 loC 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 IPs 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

<http://webgoreds.com/Activacion/cuenta-zhfg/>

Redirecciona a:

<http://www.webgoreds.com/new/www.bancoestado.cl/imagenes/comun2008/banca-en-linea-personas.html>

<http://sictsystems.com/user/date/imagenes/comun2008/banca-en-linea-personas.html>

<http://cham0coin.com/single/imagenes/comun2008/banca-en-linea-personas.html>

IP's

107.180.26.74

198.58.84.227

138.255.101.202

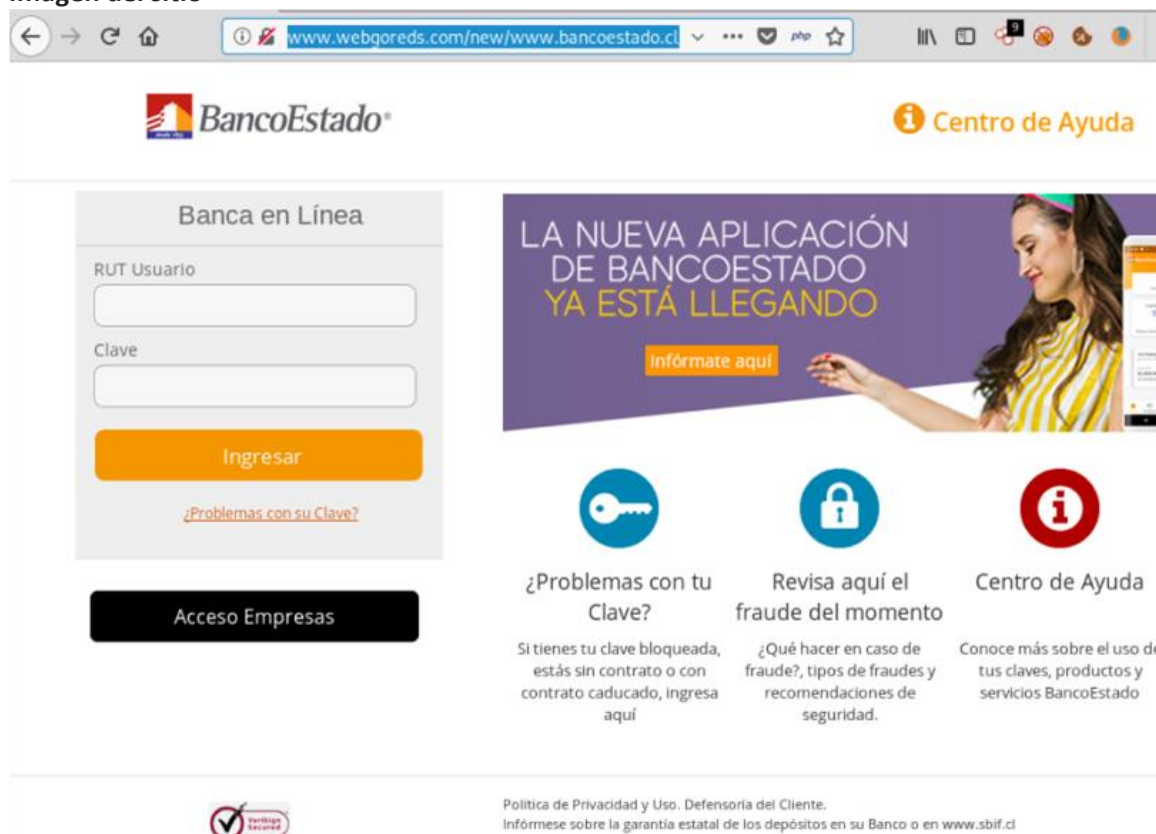
Localización

Scottsdale, Arizona, Estados Unidos

Austin, Texas, Estados Unidos

Santiago, Región Metropolitana de Santiago, Chile

Imagen del sitio



The screenshot shows the BancoEstado website. At the top left is the BancoEstado logo, and at the top right is a link to the 'Centro de Ayuda'. The main content area is divided into two sections. On the left is the 'Banca en Línea' login form, which includes fields for 'RUT Usuario' and 'Clave', an 'Ingresar' button, and a link for '¿Problemas con su Clave?'. Below the login form is a button for 'Acceso Empresas'. On the right is a promotional banner for 'LA NUEVA APLICACIÓN DE BANCOESTADO YA ESTÁ LLEGANDO' with an 'Infórmate aquí' button. Below the banner are three icons: a key for '¿Problemas con tu Clave?', a padlock for 'Revisa aquí el fraude del momento', and an information icon for 'Centro de Ayuda'. Each icon has a brief description of the service. At the bottom of the page, there is a 'Verificación Segura' logo and a footer with the 'Política de Privacidad y Uso' and 'Defensoría del Cliente' information, along with a link to 'www.sbif.cl'.



 Centro de Ayuda

Banca en Línea

RUT Usuario

Clave

Ingresar

[¿Problemas con su Clave?](#)

Acceso Empresas



¿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 de tus claves, productos y servicios BancoEsta



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.



 Centro de Ayuda

Banca en Línea

RUT Usuario

Clave

Ingresar

[¿Problemas con su Clave?](#)

Acceso Empresas



¿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

```
root@gsa:~# curl -i -L http://webgoreds.com/Activacion/cuenta-zhfq/  
HTTP/1.1 200 OK  
Date: Tue, 24 Sep 2019 13:31:50 GMT  
Server: Apache  
X-Powered-By: PHP/5.6.40  
Cache-Control: no-cache, private, must-revalidate  
Pragma: no-cache  
Expires: 0  
Upgrade: h2,h2c  
Connection: Upgrade  
Vary: Accept-Encoding,User-Agent  
Transfer-Encoding: chunked  
Content-Type: text/html; charset=UTF-8  
  
<meta http-equiv='Refresh' content='0; URL=http://webgoreds.com/new/www.bancoestado.cl/'>root@gsa:~#
```

```
$ whois -h whois.godaddy.com webgoreds.com
webgoreds.com
Domain ID: 2419591170_DOMAIN_COM-VRSN
Registrar Server: whois.godaddy.com
URL: http://www.godaddy.com
Creation Date: 2019-08-03T07:58:40Z
Expiration Date: 2019-08-03T07:58:40Z
Registration Expiration Date: 2020-08-03T07:58:40Z
Registrar: GoDaddy.com, LLC
Registrar ID: 146
Registrar Contact Email: abuse@godaddy.com
Registrar Contact Phone: +1.4806242505
Registrar Client Transfer Prohibited: http://www.icann.org/epp#clientTransferProhibited
Registrar Client Update Prohibited: http://www.icann.org/epp#clientUpdateProhibited
Registrar Client Renew Prohibited: http://www.icann.org/epp#clientRenewProhibited
Registrar Client Delete Prohibited: http://www.icann.org/epp#clientDeleteProhibited
Registrar Organization:
Registrar State/Province: La Libertad
Registrar Country: PE
Registrar Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=webgoreds.com
Registrar Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=webgoreds.com
Registrar Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=webgoreds.com
Registrar 875.DOMAINCONTROL.COM
Registrar 876.DOMAINCONTROL.COM
Registrar Address:
Registrar WHOIS Data Problem Reporting System: http://wdprs.internic.net/
Registrar Date of WHOIS database: 2019-09-24T13:00:00Z <<<
Registrar Information on Whois status codes, please visit https://www.icann.org/resources/pages/epp-status-codes-2014-
Registrar 243 will provide the ICANN-required minimum data set per
Registrar Specification, adopted 17 May 2018.
Registrar whois.godaddy.com to look up contact data for domains
Registrar GDPR policy.
Registrar Registered in GoDaddy.com, LLC's WhoIs database,
Registrar by the company to be reliable, is provided "as is"
Registrar free or warranties regarding its accuracy. This
Registrar provided for the sole purpose of assisting you
Registrar information about domain name registration records.
Registrar This data for any other purpose is expressly forbidden without the prior written
Registrar GoDaddy.com, LLC. By submitting an inquiry,
Registrar these terms of usage and limitations of warranty. In particular,
Registrar do not use this data to allow, enable, or otherwise make possible,
Registrar or collection of this data, in part or in its entirety, for any
Registrar as the transmission of unsolicited advertising and
Registrar offers of any kind, including spam. You further agree
Registrar to use this data to enable high volume, automated or robotic electronic
Registrar designed to collect or compile this data for any purpose,
Registrar using this data for your own personal or commercial purposes.
Registrar The registrant of the domain name is specified
Registrar in the "Registrant" section. In most cases, GoDaddy.com, LLC
Registrar is the registrant of domain names listed in this database.
$ █
```

```
Domain Name: sictsystems.com
Registry Domain ID: 1822889764_DOMAIN_COM-VRSN
Registrar WHOIS Server: WHOIS.ENOM.COM
Registrar URL: WWW.ENOM.COM
Updated Date: 2019-08-21T05:38:42.00Z
Creation Date: 2013-08-21T20:10:00.00Z
Registrar Registration Expiration Date: 2020-08-21T20:10:28.00Z
Registrar: ENOM, INC.
Registrar IANA ID: 48
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited
Registrant Name: Whois Agent (263148063)
Registrant Organization: Whois Privacy Protection Service, Inc.
Registrant Street: PO Box 639
Registrant Street: C/O sictsystems.com
Registrant City: Kirkland
Registrant State/Province: WA
Registrant Postal Code: 98083
Registrant Country: US
Registrant Phone: +1.4252740657
Registrant Phone Ext:
Registrant Fax: +1.4259744730
Registrant Email: wgdptmdkf@whoisprivacyprotect.com
Admin Name: Whois Agent
Admin Organization: Whois Privacy Protection Service, Inc.
Admin Street: PO Box 639
Admin Street: C/O sictsystems.com
Admin City: Kirkland
Admin State/Province: WA
Admin Postal Code: 98083
Admin Country: US
Admin Phone: +1.4252740657
Admin Phone Ext:
Admin Fax: +1.4259744730
Admin Email: wgdptmdkf@whoisprivacyprotect.com
Tech Name: Whois Agent
Tech Organization: Whois Privacy Protection Service, Inc.
Tech Street: PO Box 639
Tech Street: C/O sictsystems.com
Tech City: Kirkland
Tech State/Province: WA
Tech Postal Code: 98083
Tech Country: US
Tech Phone: +1.4252740657
Tech Phone Ext:
Tech Fax: +1.4259744730
Tech Email: wgdptmdkf@whoisprivacyprotect.com
Name Server: YNS1.YAHOO.COM
Name Server: YNS2.YAHOO.COM
DNSSEC: unsigned
```



```
soc@ITQ-ivps2:~$ whois -h whois.PublicDomainRegistry.com cham0coin.com
Domain Name: CHAMOCOIN.COM
Registry Domain ID: 2432832907_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.publicdomainregistry.com
Registrar URL: www.publicdomainregistry.com
Updated Date: 2019-09-13T14:06:57Z
Creation Date: 2019-09-13T14:06:56Z
Registrar Registration Expiration Date: 2020-09-13T14:06:56Z
Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com
Registrar IANA ID: 303
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: Not Available From Registry
Registrant Name: romero fajardo
Registrant Organization: manpower.srlt
Registrant Street: Argomedo N 588
Registrant City: santiago
Registrant State/Province: santiago
Registrant Postal Code: 3820000
Registrant Country: CL
Registrant Phone: +56.935949583
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: romero.gajardo88@gmail.com
Registry Admin ID: Not Available From Registry
Admin Name: romero fajardo
Admin Organization: manpower.srlt
Admin Street: Argomedo N 588
Admin City: santiago
Admin State/Province: santiago
Admin Postal Code: 3820000
Admin Country: CL
Admin Phone: +56.935949583
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: romero.gajardo88@gmail.com
Registry Tech ID: Not Available From Registry
Tech Name: romero fajardo
Tech Organization: manpower.srlt
Tech Street: Argomedo N 588
Tech City: santiago
Tech State/Province: santiago
Tech Postal Code: 3820000
Tech Country: CL
Tech Phone: +56.935949583
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: romero.gajardo88@gmail.com
Name Server: ns1.zglobalhost.com
Name Server: ns2.zglobalhost.com
Name Server: ns3.zglobalhost.com
Name Server: ns4.zglobalhost.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