Alerta de seguridad informática	8FFR-00141-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 de Diciembre de 2019
Última revisión	5 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 dos IPs que suplantan el sitio web oficial de **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 Compromisos

URL´s

URL Sitio Clonado:
95[.]bien-renover[.]fr/wp-content/uploads/2016/15/banchile/www[.]bancochile[.]cl/
kellar[.]cloud/wp-admin/menu/banchile/www[.]bancochile[.]cl/
kao3131[.]info/wp-content/menu/servicio/cambioclave/www[.]bancoedwards[.]cl

Domain bien-renover.fr

bien-renover / fr / Subdomains

record type	TTL	value		
A	3600	82.165.148.169		
NS	3600	ns1056.ui-dns.de	Zones on DNS server	217.160.80.56
NS	3600	ns1076.ui-dns.biz	Zones on DNS server	217.160.81.76
NS	3600	ns1031.ui-dns.com	Zones on DNS server	217.160.82.31
NS	3600	ns1086.ui-dns.org	Zones on DNS server	217.160.83.86
MX	3600	10 mx00.1and1.fr		212.227.15.41
MX	3600	11 mx01.1and1.fr		217.72.192.67

SOA	86400		
		Mname	ns1076.ui-dns.biz
		Rname	hostmaster.1and1.com
		Serial number	2018051100
		Refresh	28800
		Retry	7200
		Expire	604800
		Minimum TTL	300

Domain kellar.cloud

kellar / cloud / Subdomains

record type	TTL	value		
A	600	34.80.251.255		
NS	3600	ns43.domaincontrol.com	Zones on DNS server	97.74.101.22
NS	3600	ns44.domaincontrol.com	Zones on DNS server	173.201.69.22

SOA	3600		
		Mname	ns43.domaincontrol.com
		Rname	dns.jomax.net
		Serial number	2019090501
		Refresh	28800
		Retry	7200
		Expire	604800
		Minimum TTL	600

Domain kao3131.info

kao3131 / info / Subdomains

record type	TTL	value		
A	600	34.80.251.255		
NS	3600	ns12.domaincontrol.com	Zones on DNS server	173.201.73.6
NS	3600	ns11.domaincontrol.com	Zones on DNS server	97.74.105.6

SOA	3600		
		Mname	ns11.domaincontrol.com
		Rname	dns.jomax.net
		Serial number	2019082900
		Refresh	28800
		Retry	7200
		Expire	604800
		Minimum TTL	600

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

Certificados

Subject DN CN=95.bien-renover.fr

Issuer DN C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

Serial 425746188375995766715128851677552171713967

Validity 2019-11-25 05:39:08 **to** 2020-02-23 05:39:08 (90 days, 0:00:00)

Names 95.bien-renover.fr
www.95.bien-renover.fr

Criteria Identity = 'kellar.cloud'

Certificates

crt.sh ID	Logged At ⇧	Not Before	Not After	Issuer Name
2072097409	2019-11-04	2019-11-04	2020-02-02	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2072097259	2019-11-04	2019-11-04	2020-02-02	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1856964560	2019-09-05	2019-09-05	2019-12-04	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1849794147	2019-09-05	2019-09-05	2019-12-04	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

Criteria Identity = 'kao3131.info'

Certificates

crt.sh ID	Logged At ⇧	Not Before	Not After	Issuer Name
2061672394	2019-11-01	2019-11-01	2020-01-30	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2061672788	2019-11-01	2019-11-01	2020-01-30	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1844851190	2019-09-02	2019-09-02	2019-12-01	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1838579994	2019-09-02	2019-09-02	2019-12-01	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

Ilustración 2 Certificado Utilizado en Url del sitio Falso del Banco de Chile

IP

82.165.148.169

34.80.251.255

Domain bien-renover.fr is located on IP address << 82.165.148.169 >>

Block start	82.165.144.0
End of block	82.165.157.255
Block size	3584 Domains in block
Block name	SCHLUND-CUSTOMERS
AS number	8560
Parent block	82.165.0.0 - 82.165.255.255
Organization	1&1 Internet AG
City	Strang
Region/State	Nordrhein-Westfalen
Country	DE , Germany
Host name	s18629718.onlinehome-server.info
Web server	Apache
Powered by	PleskLin

Domain kellar.cloud is located on IP address << 34.80.251.255 >>

Block start	34.0.0.0
End of block	34.191.255.255
Block size	12582912 Domains in block
Block name	HALLIBURTON
AS number	15169
Parent block	34.0.0.0 - 34.255.255.255
Organization	Halliburton Company
City	Mountain View
Region/State	California
Country	US , United States
Reg. date	1991-03-11
Host name	255.251.80.34.bc.googleusercontent.com

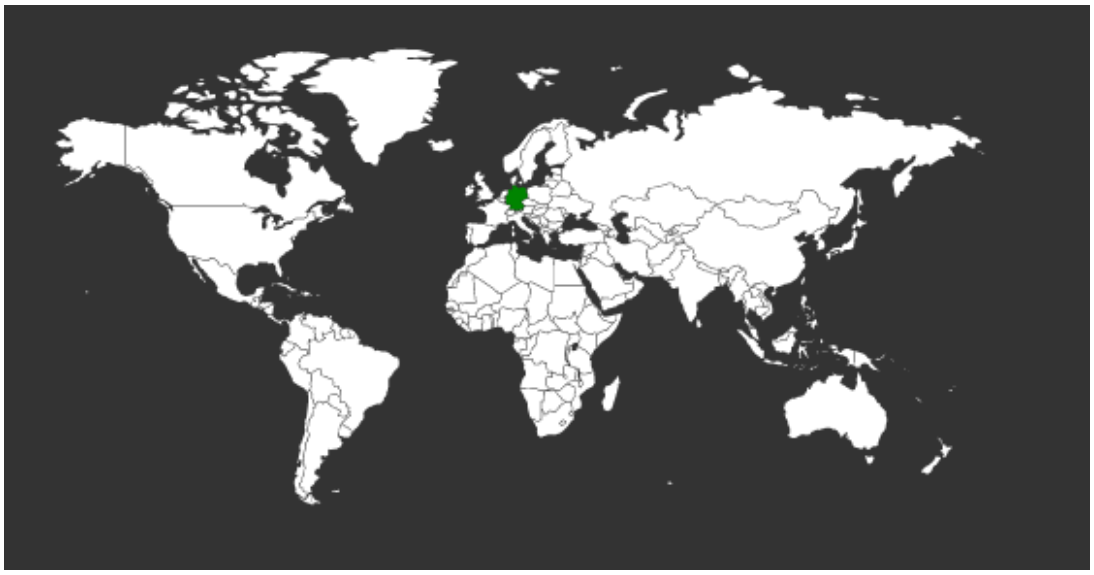
Domain kao3131.info is located on IP address << 34.80.251.255 >>

Block start	34.0.0.0
End of block	34.191.255.255
Block size	12582912 Domains in block
Block name	HALLIBURTON
AS number	15169
Parent block	34.0.0.0 - 34.255.255.255
Organization	Halliburton Company
City	Mountain View
Region/State	California
Country	US , United States
Reg. date	1991-03-11
Host name	255.251.80.34.bc.googleusercontent.com

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

Localización

Strang, Nordrhein-Westfalen, Alemania



Mountain View, California, Estados Unidos

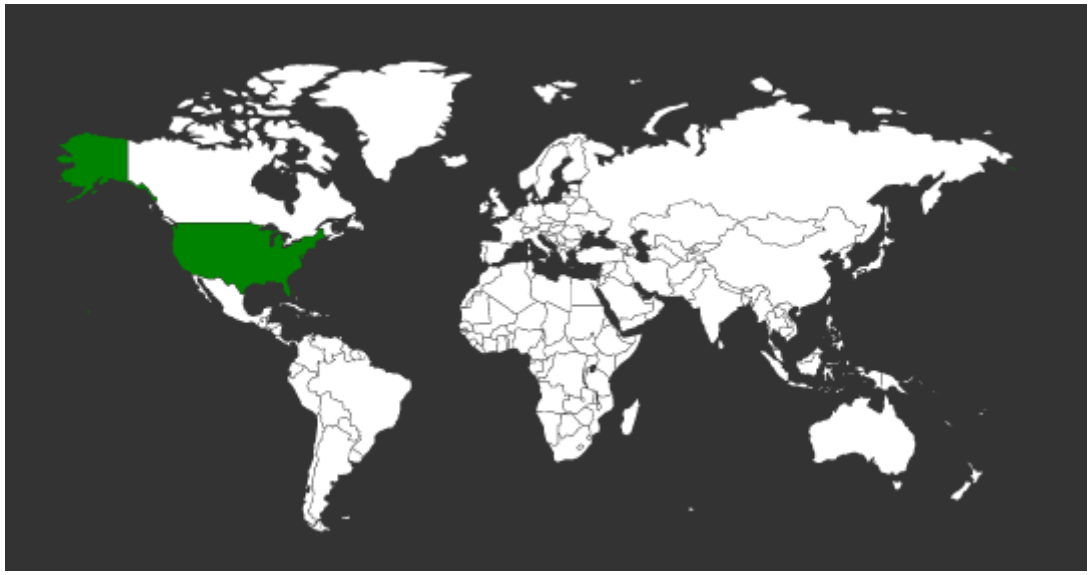
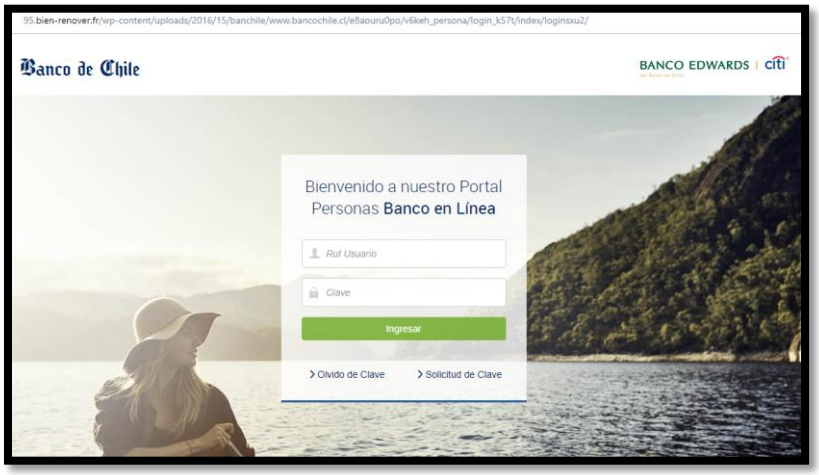
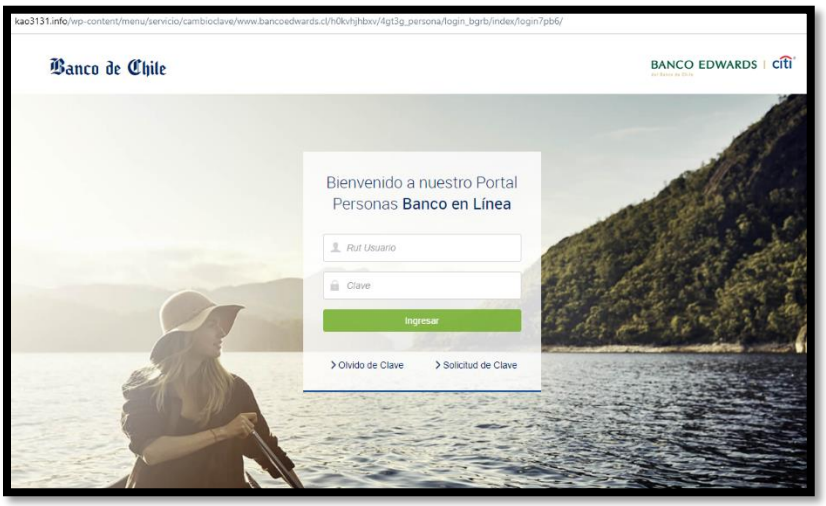
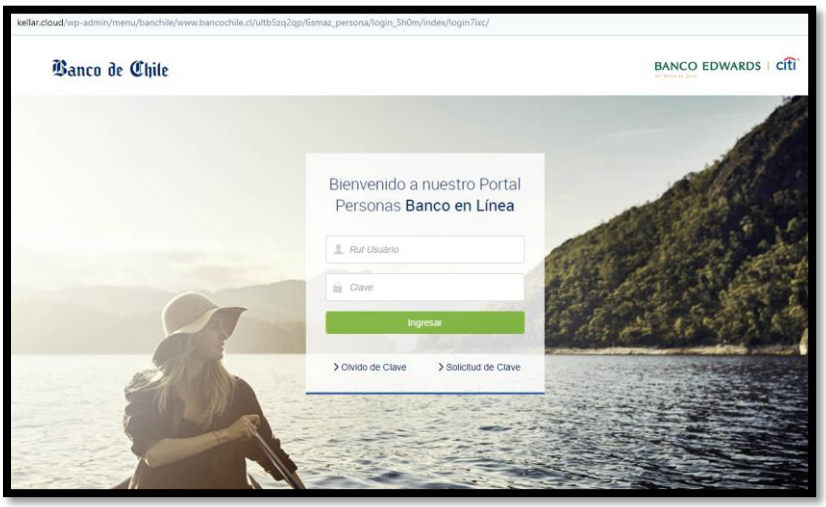


Imagen del sitio







Whois

```
%%
%% This is the AFNIC Whois server.
%%
%% complete date format : YYYY-MM-DDThh:mm:ssZ
%% short date format    : DD/MM
%% version              : FRNIC-2.5
%%
%% Rights restricted by copyright.
%% See https://www.afnic.fr/en/products-and-services/services/whois/whois-special-notice/
%%
%% Use '-h' option to obtain more information about this service.
%%
%% [2604:0880:000a:0006:0000:0000:0000:08f6 REQUEST] >> -V Md5.5.2 bien-renover.fr
%%
%% RL Net [##########] - RL IP [#########.]
%%

domain:      bien-renover.fr
status:      ACTIVE
hold:        NO
holder-c:    R16055-FRNIC
admin-c:     R16056-FRNIC
tech-c:      UIS153-FRNIC
zone-c:      NFC1-FRNIC
nsl-id:      NSL143901-FRNIC
registrar:   1&1 IONOS SE
Expiry Date: 2020-05-11T17:40:44Z
created:     2018-05-11T17:40:44Z
last-update: 2019-05-11T18:33:39Z
source:      FRNIC

ns-list:     NSL143901-FRNIC
nserver:     ns1076.ui-dns.biz
nserver:     ns1031.ui-dns.com
nserver:     ns1056.ui-dns.de
nserver:     ns1086.ui-dns.org
source:      FRNIC

registrar:   1&1 IONOS SE
type:        Isp Option 1
address:     Ernst-Frey Strasse 9
address:     76135 KARLSRUHE
country:     DE
phone:       +49 721 91374 50
fax-no:      +49 721 91374 215
e-mail:      hostmaster@lundl.de
website:     https://www.landl.fr/achat-nom-de-domaine#stage
anonymous:   NO
registered:  2001-01-17T12:00:00Z
source:      FRNIC

nic-hdl:     R16055-FRNIC
type:        ORGANIZATION
contact:     RT.isolation
address:     RT.isolation
address:     8 chemin du trou salé
address:     78350 Les Loges en josas
country:     FR
phone:       +33.677665159
e-mail:      technicien.habitat.francais@gmail.com
```

```
Domain Name: kellar.cloud
Registry Domain ID: DA0C6B7894FE640C9B9818E0D0BEB4972-NSR
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Updated Date: 2019-09-05T10:55:07Z
Creation Date: 2019-09-05T10:55:06Z
Registrar Registration Expiration Date: 2020-09-05T10:55:06Z
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:
Registrant State/Province:
Registrant Country: TW
Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/w
hois/results.aspx?domain=kellar.cloud
Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/
results.aspx?domain=kellar.cloud
Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/r
esults.aspx?domain=kellar.cloud
Name Server: NS43.DOMAINCONTROL.COM
Name Server: NS44.DOMAINCONTROL.COM
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2019-12-04T14:00:00Z <<<
```

```
Domain Name: kao3131.info
Registry Domain ID: D503300001144421707-LRMS
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Updated Date: 2019-08-23T10:25:25Z
Creation Date: 2019-08-23T10:25:24Z
Registrar Registration Expiration Date: 2021-08-23T10:25:24Z
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:
Registrant State/Province: Tai \u7063Sheng Tai Bei Shi
Registrant Country: TW
Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/w
hois/results.aspx?domain=kao3131.info
Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/
results.aspx?domain=kao3131.info
Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/r
esults.aspx?domain=kao3131.info
Name Server: NS11.DOMAINCONTROL.COM
Name Server: NS12.DOMAINCONTROL.COM
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2019-12-04T14:00:00Z <<<

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.
```

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: 2019.12.05 15:33:46 -03'00'