| | |
|---|---|
| Alerta de seguridad informática | 8FFR20-00215-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 13 de febrero de 2020 |
| Última revisión | 13 de febrero 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 un portal fraudulento asociado a una IP que suplanta 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
aumento-solicita-credito-consumo-cl[.]retq[.]xyz/j1j50ankb1/0nbzi_persona/login_m1ln/index/loginbl7j/

## Redireccionador de URL´s

deepinsouthafrica[.]minademian[.]com/wp-includes/css/HbCeAH7UhzU4sEhwAJdxCfofhcN3xf9c/vewtzzFbMe9cAd9eL3Hobbo

**Domain aumento-solicita-credito-consumo-cl.retq.xyz**

aumento-solicita-credito-consumo-cl / retq / xyz / Subdomains

| record type | TTL | value | |
|---|---|---|---|
| CNAME | 300 | retq.xyz | 3.16.56.156 |

**Domain retq.xyz**

retq / xyz / Subdomains

| record type | TTL | value | | |
|---|---|---|---|---|
| A | 300 | 3.16.56.156 | | |
| NS | 300 | ns1jsv.name.com | Zones on DNS server | 162.88.61.47 |
| NS | 300 | ns2btz.name.com | Zones on DNS server | 162.88.60.47 |
| NS | 300 | ns4gvx.name.com | Zones on DNS server | 162.88.60.49 |
| NS | 300 | ns3bfm.name.com | Zones on DNS server | 162.88.61.49 |

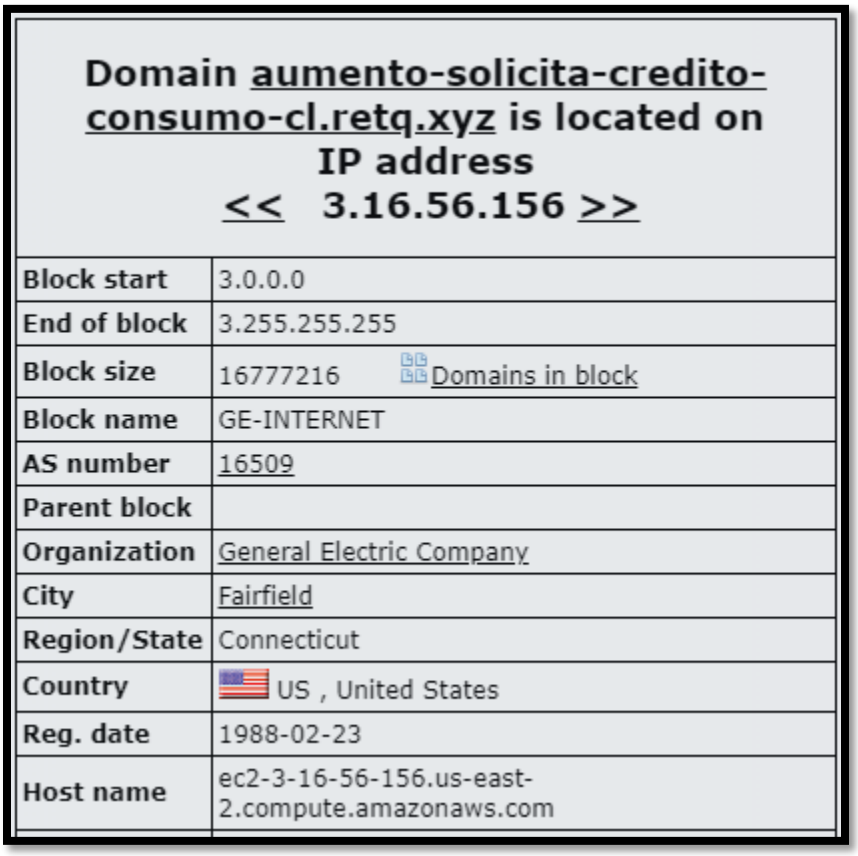
| SOA | 300 | Mname | ns1jsv.name.com |
|---|---|---|---|
| | | Rname | support.name.com |
| | | Serial number | 1581496891 |
| | | Refresh | 10800 |
| | | Retry | 3600 |
| | | Expire | 604800 |
| | | Minimum TTL | 3600 |

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

Certificados


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

IP
3[.]16[.]56[.]156



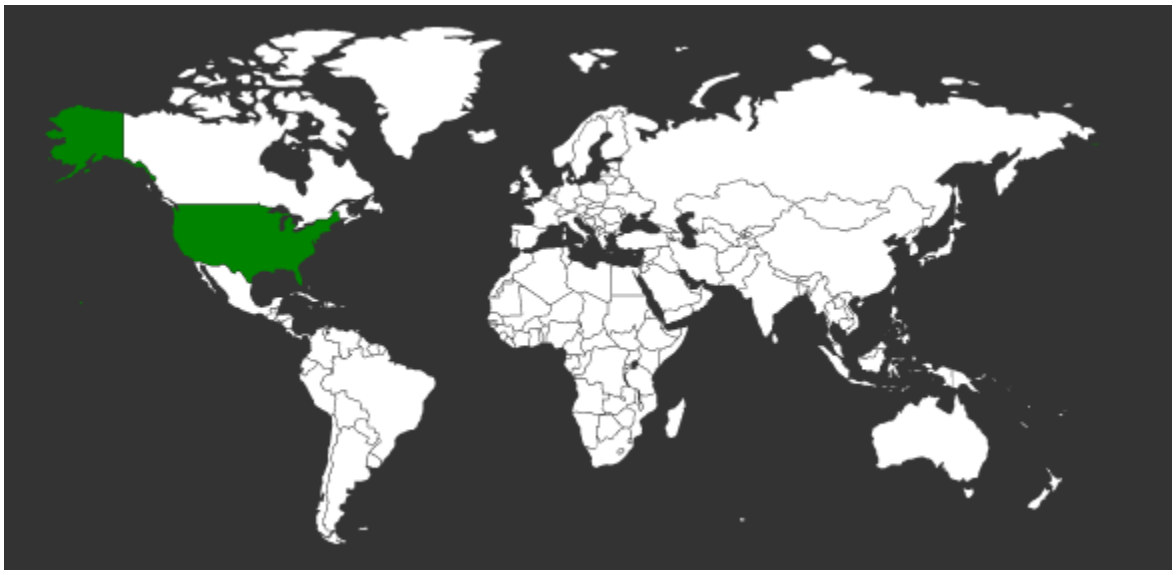
**Domain aumento-solicita-credito-consumo-cl.retq.xyz is located on IP address**
**<< 3.16.56.156 >>**

| | |
|---|---|
| **Block start** | 3.0.0.0 |
| **End of block** | 3.255.255.255 |
| **Block size** | 16777216 Domains in block |
| **Block name** | GE-INTERNET |
| **AS number** | 16509 |
| **Parent block** | |
| **Organization** | General Electric Company |
| **City** | Fairfield |
| **Region/State** | Connecticut |
| **Country** | US , United States |
| **Reg. date** | 1988-02-23 |
| **Host name** | ec2-3-16-56-156.us-east-2.compute.amazonaws.com |

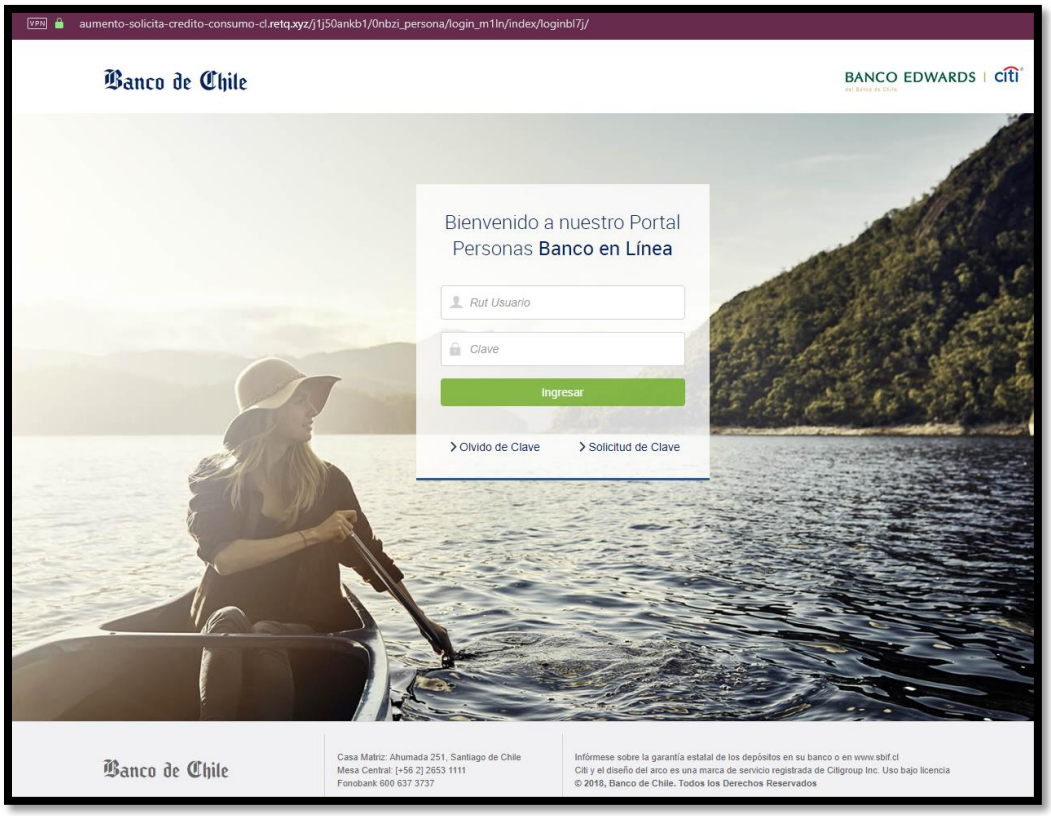
*Ilustración 3 Ip de Origen donde se aloja Sitio Falso del Banco de Chile*

## Localización

Columbus, Ohio, Estados Unidos



## Imagen del sitio



Whois

```
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

refer:        whois.nic.xyz

domain:       XYZ

organisation: XYZ.COM LLC
address:      2121 E Tropicana Ave
address:      Las Vegas
address:      NV 89119
address:      United States

contact:      administrative
name:         General Counsel
organisation: XYZ.COM LLC
address:      2121 E Tropicana Ave., STE2
address:      Las Vegas
address:      NV 89119
address:      United States
phone:        +1.7027632191
e-mail:       hello@xyz.com

contact:      technical
name:         CTO
organisation: CentralNic
address:      Saddlers House, 4th Floor
address:      44 Gutter Lane
address:      London EC2V 6BR
address:      United Kingdom
phone:        +44.2033880600
fax-no:       +44.2033880601
e-mail:       tld.ops@centralnic.com

nserver:      GENERATIONXYZ.NIC.XYZ 212.18.249.42 2a04:2b00:13ff:0:0:0:0:42
nserver:      X.NIC.XYZ 194.169.218.42 2001:67c:13cc:0:0:0:1:42
nserver:      Y.NIC.XYZ 185.24.64.42 2a04:2b00:13cc:0:0:0:1:42
nserver:      Z.NIC.XYZ 212.18.248.42 2a04:2b00:13ee:0:0:0:0:42
ds-rdata:     3599 8 1 3FA3B264F45DB5F38BEDEAF1A88B76AA318C2C7F
ds-rdata:     3599 8 2 B9733869BC84C86BB59D102BA5DA6B27B2088552332A39DCD54BC4E8D66B0499

whois:        whois.nic.xyz

status:       ACTIVE
remarks:      Registration information: http://nic.xyz

created:      2014-02-06
changed:      2019-10-14
source:       IANA

Domain Name: RETQ.XYZ
Registry Domain ID: D170632756-CNIC
Registrar WHOIS Server: whois.name.com
Registrar URL: http://www.name.com/
Updated Date: 2020-02-12T04:20:17.0Z
Creation Date: 2020-02-12T04:20:10.0Z
Registry Expiry Date: 2021-02-12T23:59:59.0Z
Registrar: Name.com LLC
Registrar IANA ID: 625
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: addPeriod https://icann.org/epp#addPeriod
Registrant Organization: Domain Protection Services, Inc.
Registrant State/Province: CO
Registrant Country: US
Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for infor
mation on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for informatio
n on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information
 on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Name Server: NS1JSV.NAME.COM
Name Server: NS2BTZ.NAME.COM
Name Server: NS3BFM.NAME.COM
Name Server: NS4GVX.NAME.COM
DNSSEC: unsigned
Billing Email: Please query the RDDS service of the Registrar of Record identified in this output for informat
ion on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Registrar Abuse Contact Email: abuse@name.com
Registrar Abuse Contact Phone: +1.4252982607
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2020-02-12T15:42:57.0Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

>>> IMPORTANT INFORMATION ABOUT THE DEPLOYMENT OF RDAP: please visit
https://www.centralnic.com/support/rdap <<<

The Whois and RDAP services are provided by CentralNic, and contain
information pertaining to Internet domain names registered by our
our customers. By using this service you are agreeing (1) not to use any
information presented here for any purpose other than determining
ownership of domain names, (2) not to store or reproduce this data in
any way, (3) not to use any high-volume, automated, electronic processes
to obtain data from this service. Abuse of this service is monitored and
actions in contravention of these terms will result in being permanently
blacklisted. All data is (c) CentralNic Ltd (https://www.centralnic.com)

Access to the Whois and RDAP services is rate limited. For more
information, visit https://registrar-console.centralnic.com/pub/whois_guidance.
```

## 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: 2020.02.13 13:35:52 -03'00'