Alerta de seguridad informática	8FFR-00129-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de Noviembre de 2019
Última revisión	27 de Noviembre 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 un portal fraudulento asociado a una IP que suplanta 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:
http[://]glovalcoin[.]site/touch/imagenes/comun2008/banca-en-linea-personas[.]html/
https[://]solicita-credito-consumo-cl[.]wcgx[.]xyz/imagenes/comun2008/personas-en-linea[.]html

Domain wcgx.xyz

wcgx / xyz / Subdomains

record type	TTL	value	
No records found			

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

Certificados

Criteria	Identity = 'glovalcoin.site'
Certificates	*None found*

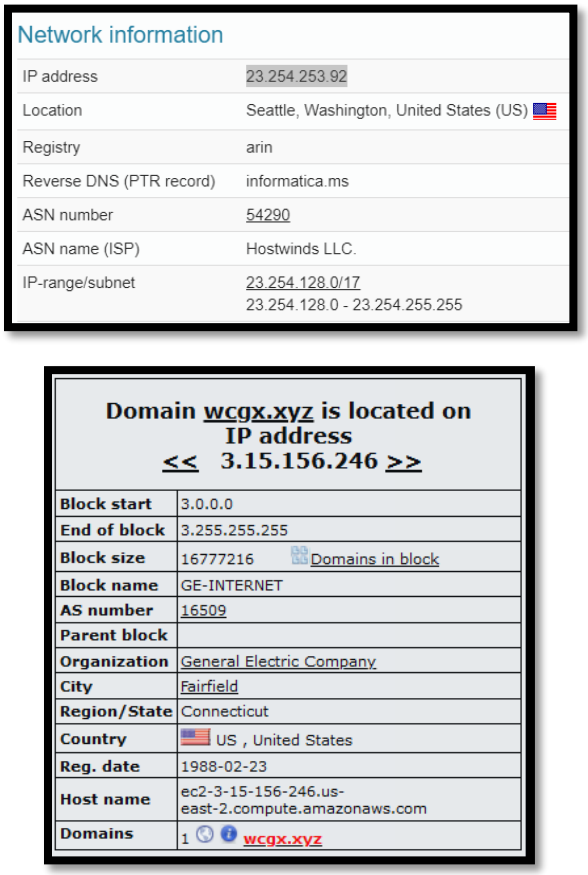
Criteria	Identity = 'wcgx.xyz'			
Certificates	crt.sh ID	Logged At	Not Before	Not After	Issuer Name
	2140947437	2019-11-22	2019-11-22	2020-02-20	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2140947317	2019-11-22	2019-11-22	2020-02-20	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

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

IP

23.254.253.92

3.15.156.246



Network information

IP address	23.254.253.92
Location	Seattle, Washington, United States (US)
Registry	arin
Reverse DNS (PTR record)	informatica.ms
ASN number	54290
ASN name (ISP)	Hostwinds LLC.
IP-range/subnet	23.254.128.0/17 23.254.128.0 - 23.254.255.255

Domain wcgx.xyz is located on IP address
<< 3.15.156.246 >>

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	ec2-3-15-156-246.us-east-2.compute.amazonaws.com
Domains	1 wcgx.xyz

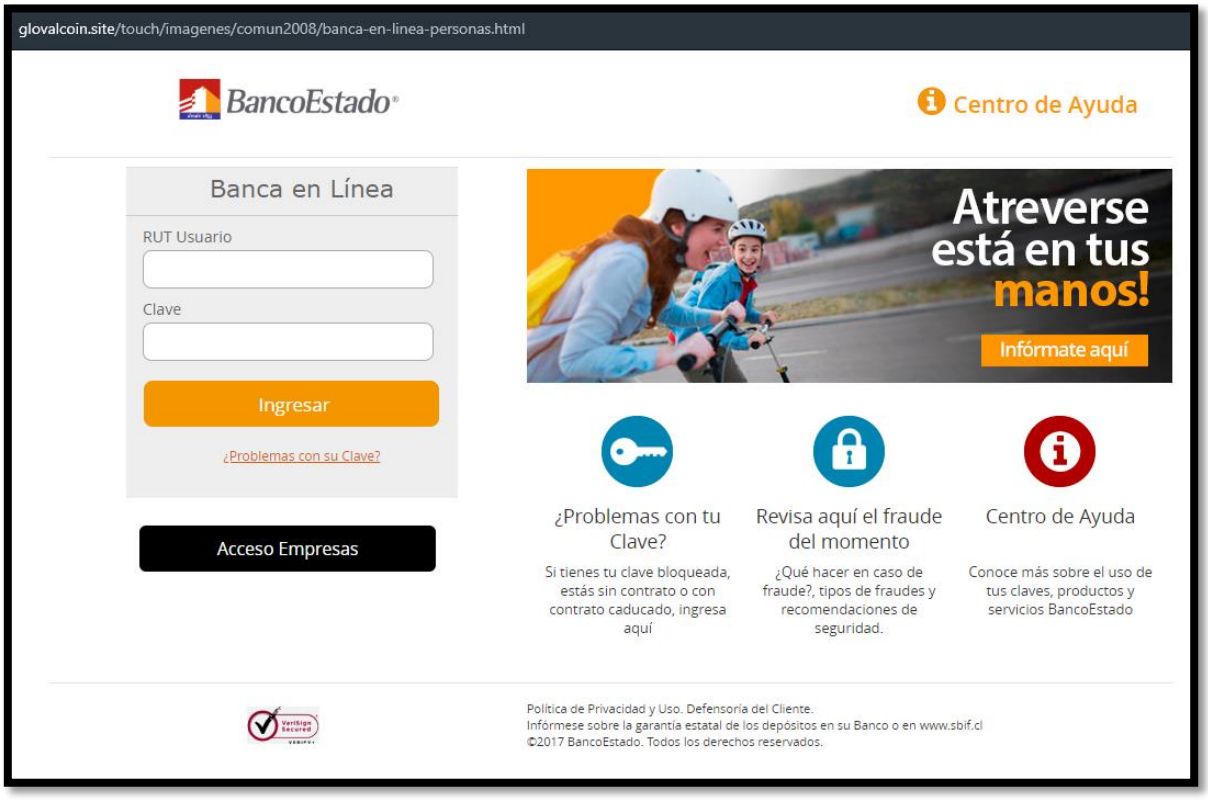
Ilustración 3 Ip de Origen donde se aloja Sitio Falso del Banco Estado

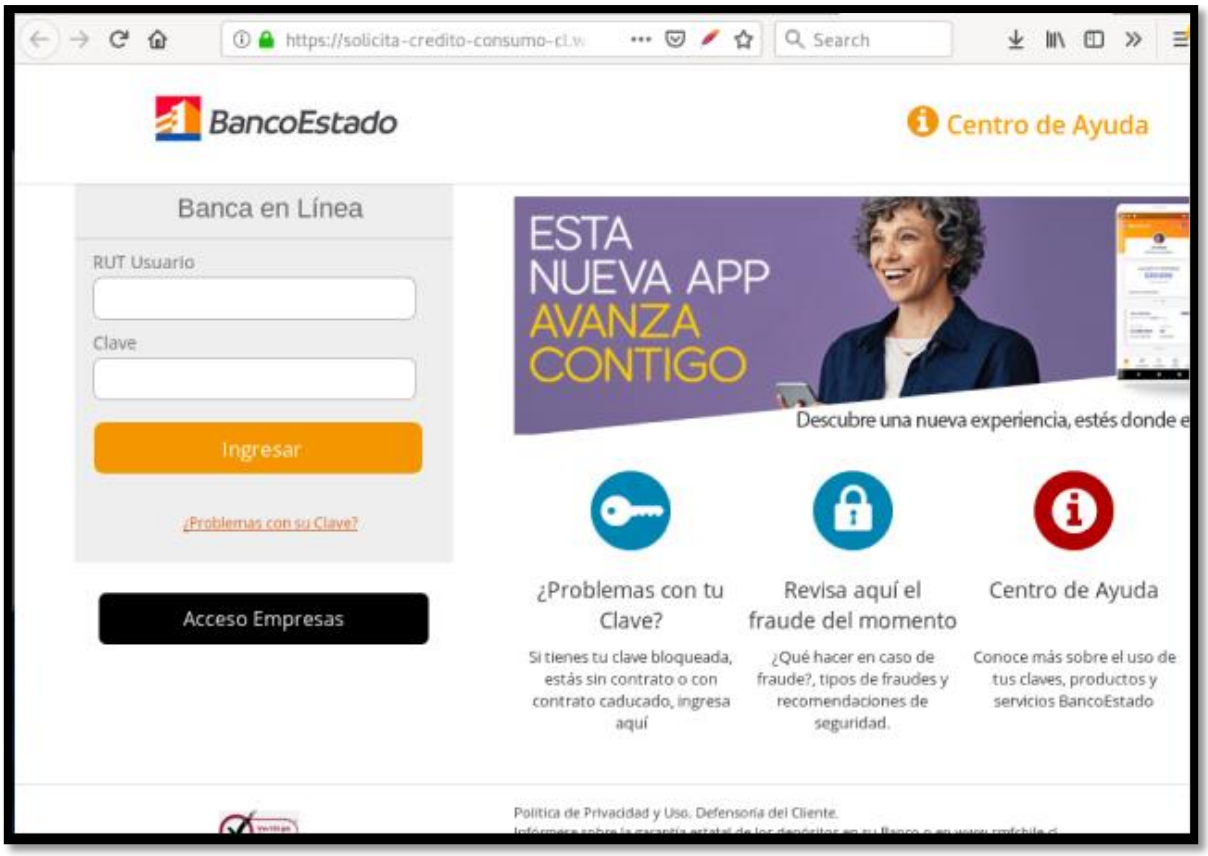
Localización

Seattle, Washington, Estados Unidos

Columbus, Ohio, Estados Unidos

Imagen del sitio




https://solicita-credito-consumo-cl.w
Search
BancoEstado
Centro de Ayuda
Banca en Línea
RUT Usuario
Clave
Ingresar
¿Problemas con su Clave?
Acceso Empresas
ESTA
NUEVA APP
AVANZA
CONTIGO
Descubre una nueva experiencia, estés donde e
¿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.

Whois

```
Domain Name: GLOVALCOIN.SITE
Registry Domain ID: D146602905-CNIC
Registrar WHOIS Server: whois.cdmon.com
Registrar URL: https://www.cdmon.com/
Updated Date: 2019-11-20T16:04:58.0Z
Creation Date: 2019-11-20T16:02:57.0Z
Registry Expiry Date: 2020-11-20T23:59:59.0Z
Registrar: 10dencehispahard SL (CDmon)
Registrar IANA ID: 1403
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:
Registrant State/Province:
Registrant Country: PE
Registrant 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.
Admin 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.
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: DALNS5.MASTERNS.COM
Name Server: DALNS6.MASTERNS.COM
DNSSEC: unsigned
```

```
Domain Name: WCGX.XYZ
Registry Domain ID: D146925421-CNIC
Registrar WHOIS Server: whois.name.com
Registrar URL: http://www.name.com
Updated Date: 2019-11-22T11:22:08Z
Creation Date: 2019-11-22T11:22:02Z
Registrar Registration Expiration Date: 2020-11-22T23:59:59Z
Registrar: Name.com, Inc.
Registrar IANA ID: 625
Reseller:
Domain Status: addPeriod https://www.icann.org/epp#addPeriod
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited
Domain Status: serverTransferProhibited https://www.icann.org/epp#serverTransferProhibited
Registry Registrant ID: Not Available From Registry
Registrant Name: Whois Agent
Registrant Organization: Domain Protection Services, Inc.
Registrant Street: PO Box 1769
Registrant City: Denver
Registrant State/Province: CO
Registrant Postal Code: 80201
Registrant Country: US
Registrant Phone: +1.7208009072
Registrant Fax: +1.7209758725
Registrant Email: https://www.name.com/contact-domain-whois/wcgx.xyz
Registry Admin ID: Not Available From Registry
Admin Name: Whois Agent
Admin Organization: Domain Protection Services, Inc.
Admin Street: PO Box 1769
Admin City: Denver
Admin State/Province: CO
Admin Postal Code: 80201
Admin Country: US
Admin Phone: +1.7208009072
Admin Fax: +1.7209758725
Admin Email: https://www.name.com/contact-domain-whois/wcgx.xyz
Registry Tech ID: Not Available From Registry
Tech Name: Whois Agent
Tech Organization: Domain Protection Services, Inc.
Tech Street: PO Box 1769
Tech City: Denver
Tech State/Province: CO
Tech Postal Code: 80201
Tech Country: US
Tech Phone: +1.7208009072
Tech Fax: +1.7209758725
Tech Email: https://www.name.com/contact-domain-whois/wcgx.xyz
Name Server: ns1cny.name.com
Name Server: ns2dqr.name.com
Name Server: ns3gxy.name.com
Name Server: ns4bty.name.com
DNSSEC: unSigned
Registrar Abuse Contact Email: abuse@name.com
Registrar Abuse Contact Phone: +1.7203101849
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2019-11-25T18:57:02Z <<<

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


The data in the Name.com, Inc. WHOIS database is provided by Name.com, Inc. for information purposes, and to assist persons in obtaini
ng information about or related to a domain name registration record. Name.com, Inc. does not guarantee its accuracy.  Users accessing
```

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