Alerta de seguridad informática	8FFR-00105-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de Noviembre de 2019
Última revisión	07 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 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

http[://]w3bancodechile[.]verificacionrut[.]com/persona/login/

Domain verificacionrut.com

verificacionrut / com / Subdomains

record type	TTL	value		
A	14400	108.179.232.93		
NS	86400	ns8487.hostgator.com	Zones on DNS server	108.179.232.60
NS	86400	ns8488.hostgator.com	Zones on DNS server	108.179.232.61
MX	14400	0 mail.verificacionrut.com		
TXT	14400	v=spf1 a mx include:websitewelcome.com ~all		
SOA	86400	Mname: ns8487.hostgator.com Rname: root.gator4244.hostgator.com Serial number: 2019110207 Refresh: 86400 Retry: 7200 Expire: 3600000 Minimum TTL: 86400		

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

Certificado

Criteria: Identity = 'verificacionrut.com'

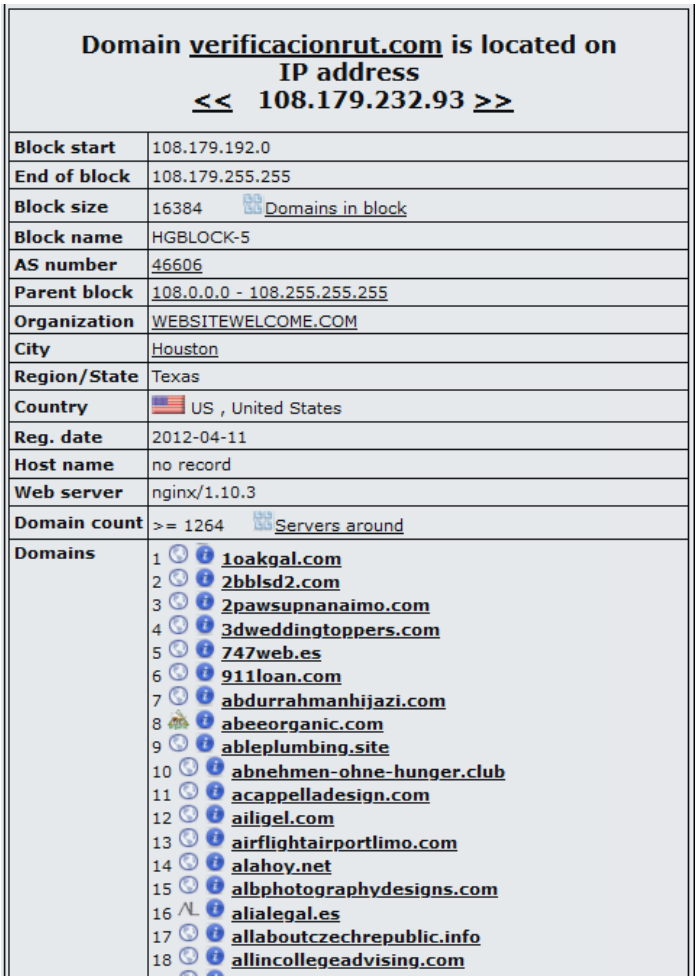
Certificates

crt.sh ID	Logged At	Not Before	Not After	Issuer Name
1984850402	2019-10-09	2019-10-09	2020-01-07	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1977297639	2019-10-09	2019-10-09	2020-01-07	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1824718435	2019-08-14	2019-08-14	2019-11-12	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1771146456	2019-08-14	2019-08-14	2019-11-12	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

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

IP´s

108[.]179[.]232[.]93



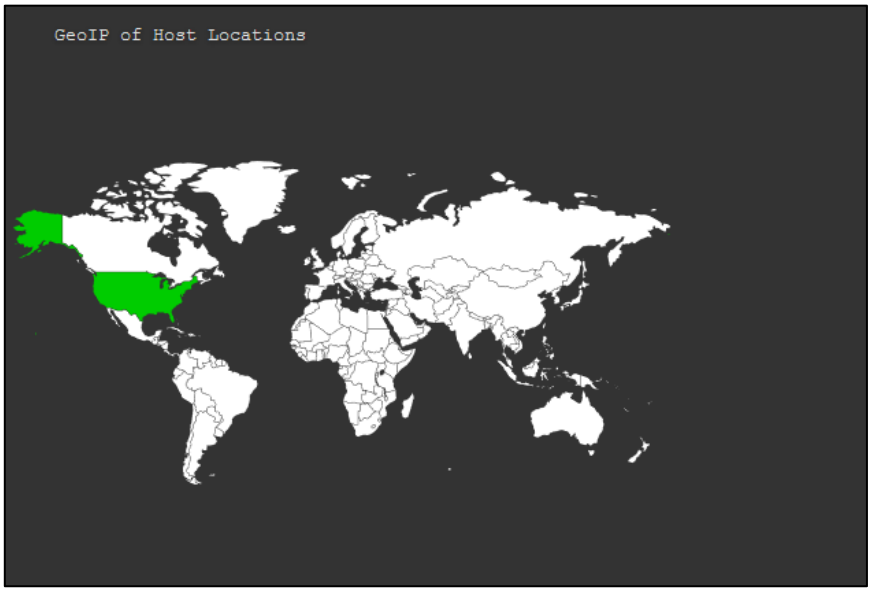
Domain verificacionrut.com is located on IP address
<< 108.179.232.93 >>

Block start	108.179.192.0
End of block	108.179.255.255
Block size	16384 Domains in block
Block name	HGBLOCK-5
AS number	46606
Parent block	108.0.0.0 - 108.255.255.255
Organization	WEBSITEWELCOME.COM
City	Houston
Region/State	Texas
Country	US , United States
Reg. date	2012-04-11
Host name	no record
Web server	nginx/1.10.3
Domain count	>= 1264 Servers around
Domains	1 1oakgal.com 2 2bblsd2.com 3 2pawsupnanaimo.com 4 3dweddingtoppers.com 5 747web.es 6 911loan.com 7 abdurrahmanhijazi.com 8 abeeorganic.com 9 ableplumbing.site 10 abnehmen-ohne-hunger.club 11 acappelladesign.com 12 ailigel.com 13 airflightairportlimo.com 14 alahoy.net 15 albphotographydesigns.com 16 alialegal.es 17 allaboutczechrepublic.info 18 allincollegeadvising.com

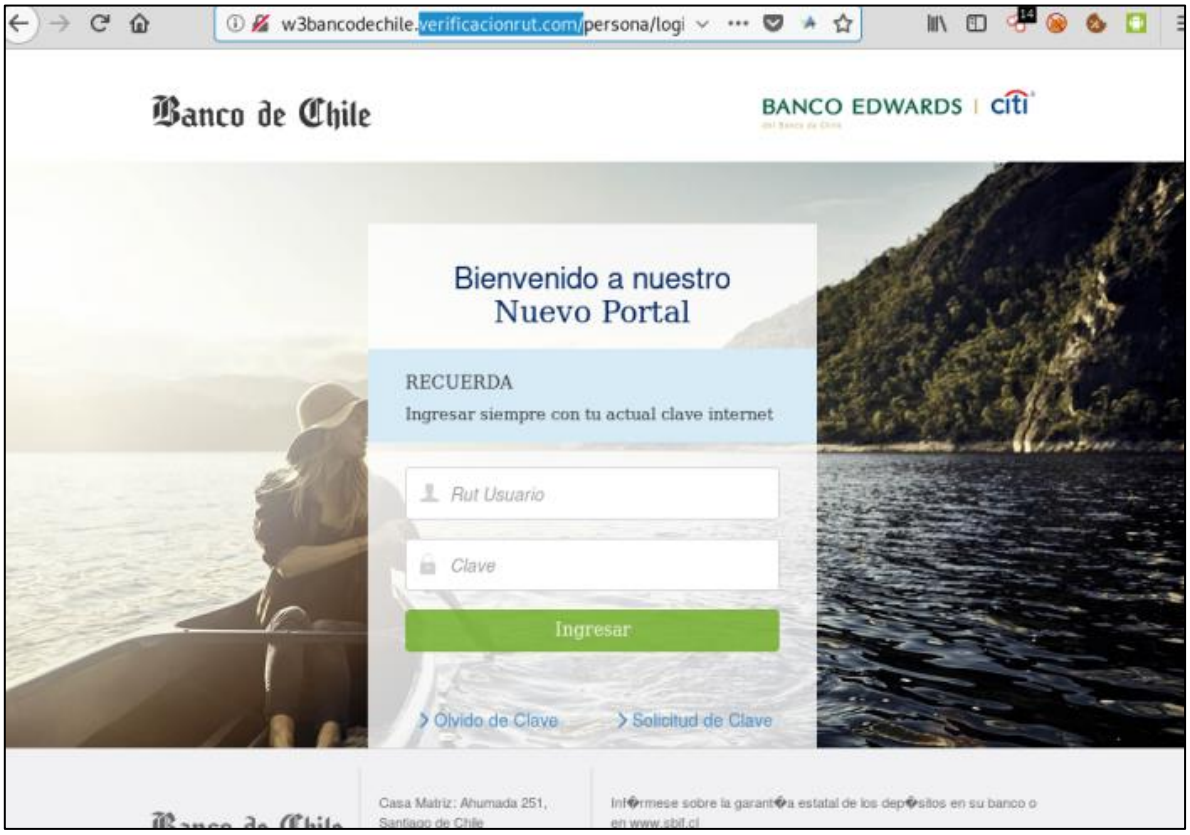
Ilustración 3 Ip de Origen donde se aloja Sitio Falso del Banco Estado

Localización

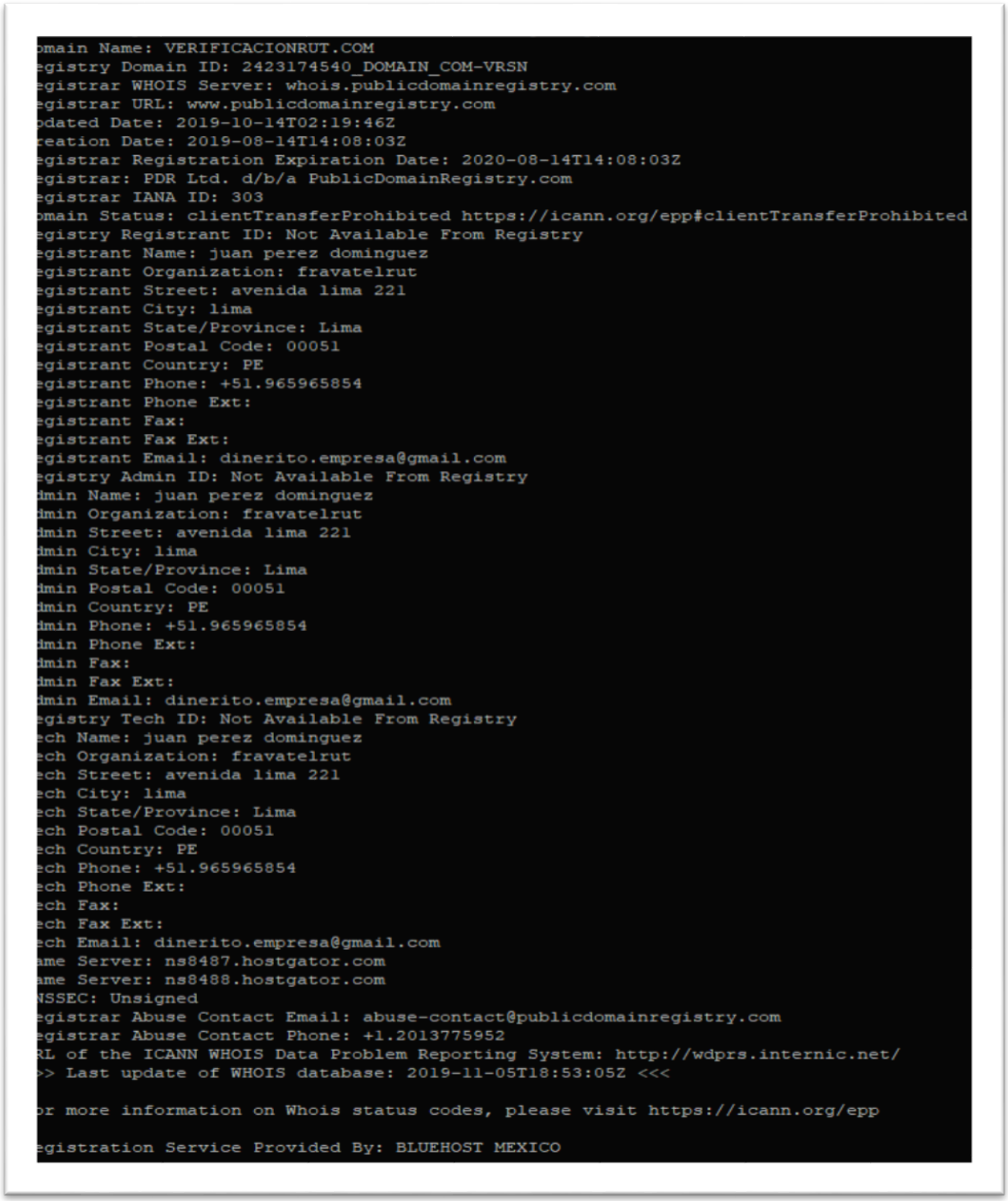
San Jose, California, Estados Unidos



Imagen



Whois



```
omain Name: VERIFICACIONRUT.COM
egistry Domain ID: 2423174540_DOMAIN_COM-VRSN
egistrar WHOIS Server: whois.publicdomainregistry.com
egistrar URL: www.publicdomainregistry.com
odated Date: 2019-10-14T02:19:46Z
reation Date: 2019-08-14T14:08:03Z
egistrar Registration Expiration Date: 2020-08-14T14:08:03Z
egistrar: PDR Ltd. d/b/a PublicDomainRegistry.com
egistrar IANA ID: 303
omain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
egistry Registrant ID: Not Available From Registry
egistrant Name: juan perez dominguez
egistrant Organization: fravatelrut
egistrant Street: avenida lima 221
egistrant City: lima
egistrant State/Province: Lima
egistrant Postal Code: 00051
egistrant Country: PE
egistrant Phone: +51.965965854
egistrant Phone Ext:
egistrant Fax:
egistrant Fax Ext:
egistrant Email: dinerito.empresa@gmail.com
egistry Admin ID: Not Available From Registry
dmin Name: juan perez dominguez
dmin Organization: fravatelrut
dmin Street: avenida lima 221
dmin City: lima
dmin State/Province: Lima
dmin Postal Code: 00051
dmin Country: PE
dmin Phone: +51.965965854
dmin Phone Ext:
dmin Fax:
dmin Fax Ext:
dmin Email: dinerito.empresa@gmail.com
egistry Tech ID: Not Available From Registry
ech Name: juan perez dominguez
ech Organization: fravatelrut
ech Street: avenida lima 221
ech City: lima
ech State/Province: Lima
ech Postal Code: 00051
ech Country: PE
ech Phone: +51.965965854
ech Phone Ext:
ech Fax:
ech Fax Ext:
ech Email: dinerito.empresa@gmail.com
ame Server: ns8487.hostgator.com
ame Server: ns8488.hostgator.com
NSSEC: Unsigned
egistrar Abuse Contact Email: abuse-contact@publicdomainregistry.com
egistrar Abuse Contact Phone: +1.2013775952
RL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>> Last update of WHOIS database: 2019-11-05T18:53:05Z <<<

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

egistration Service Provided By: BLUEHOST MEXICO
```

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: 2019.11.07 13:39:21 -03'00'