Alerta de seguridad informática	**8FFR-00080-001**
Clase de alerta	**Fraude**
Tipo de incidente	**Falsificación de Registros o Identidad**
Nivel de riesgo	**Alto**
TLP	**Blanco**
Fecha de lanzamiento original	**05 de Octubre de 2019**
Última revisión	**05 de Octubre 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 Security**, 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

https[://]personasecurity[.]inscripcionrut[.]com
w2bancochile[.]inscripcionrut[.]com
w3bancochile[.]inscripcionrut[.]com

Domain inscripcionrut.com

inscripcionrut / com / Subdomains

record type	TTL	value		
A	14400	108.167.180.118		
NS	86400	ns8371.hostgator.com	Zones on DNS server	108.167.180.100
NS	86400	ns8372.hostgator.com	Zones on DNS server	108.167.180.101
MX	14400	0 mail.inscripcionrut.com		
TXT	14400	v=spf1 a mx include:websitewelcome.com ~all		
SOA	86400	Mname: ns8371.hostgator.com Rname: root.gator4186.hostgator.com Serial number: 2019100302 Refresh: 86400 Retry: 7200 Expire: 3600000 Minimum TTL: 86400		

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

Certificado

Certificates

crt.sh ID	Logged At ⇧	Not Before	Not After	Issuer Name
1954100980	2019-10-03	2019-10-03	2020-01-01	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1954100971	2019-10-03	2019-10-03	2020-01-01	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

Certificates

crt.sh ID	Logged At ⇧	Not Before	Not After	Issuer Name
1900524290	2019-09-12	2019-09-11	2019-12-10	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1874039685	2019-09-12	2019-09-11	2019-12-10	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

Certificates

crt.sh ID	Logged At ⇧	Not Before	Not After	Issuer Name
1853810088	2019-08-27	2019-08-27	2019-11-25	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1816496140	2019-08-27	2019-08-27	2019-11-25	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

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

IP´s

108[.]167[.]180[.]118

Domain personasecurity.inscripcionrut.com is located on IP address << 108.167.180.118 >>	
Block start	108.167.128.0
End of block	108.167.191.255
Block size	16384 Domains in block
Block name	HGBLOCK-4
AS number	26337
Parent block	108.0.0.0 - 108.255.255.255
Organization	WEBSITEWELCOME.COM
City	Houston
Region/State	Texas
Country	US , United States
Reg. date	2011-12-27
Host name	no record
Web server	nginx/1.10.3

Domain w2bancochile.inscripcionrut.com is located on IP address << 108.167.180.118 >>	
Block start	108.167.128.0
End of block	108.167.191.255
Block size	16384 Domains in block
Block name	HGBLOCK-4
AS number	26337
Parent block	108.0.0.0 - 108.255.255.255
Organization	WEBSITEWELCOME.COM
City	Houston
Region/State	Texas
Country	US , United States
Reg. date	2011-12-27
Host name	no record
Web server	nginx/1.10.3

Domain w3bancochile.inscripcionrut.com is located on IP address << 108.167.180.118 >>	
Block start	108.167.128.0
End of block	108.167.191.255
Block size	16384 Domains in block
Block name	HGBLOCK-4
AS number	26337
Parent block	108.0.0.0 - 108.255.255.255
Organization	WEBSITEWELCOME.COM
City	Houston
Region/State	Texas
Country	US , United States
Reg. date	2011-12-27
Host name	no record
Web server	nginx/1.10.3

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

Localización

San José, California, Estados Unidos

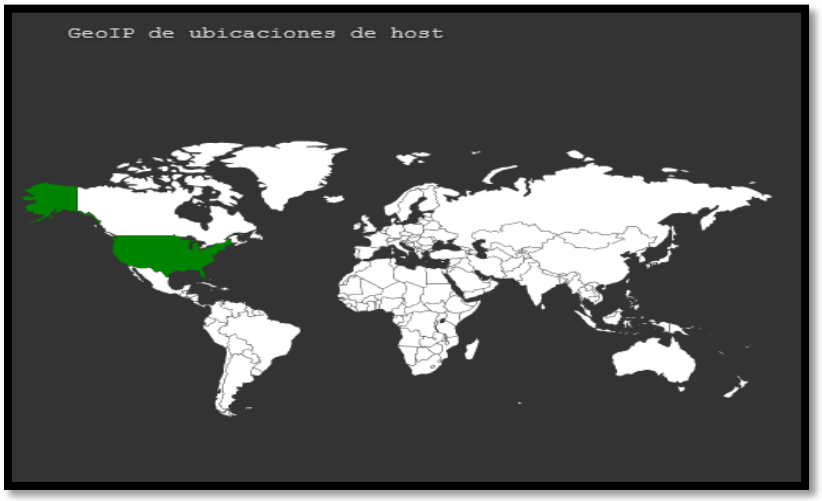
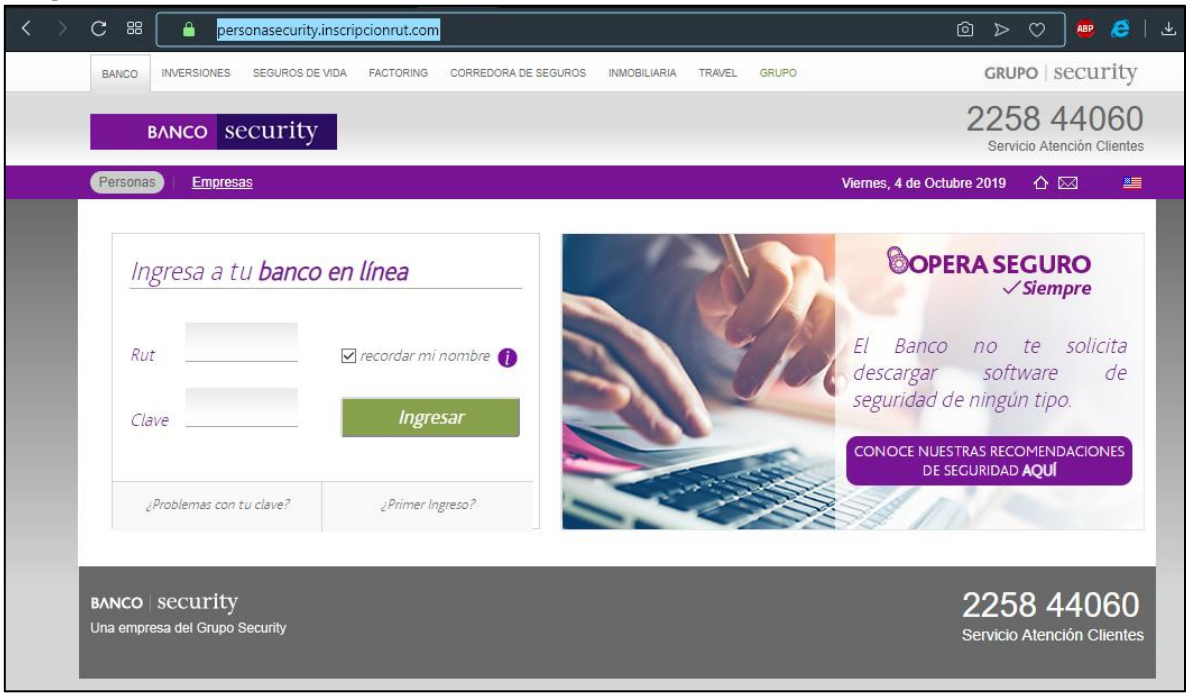


Imagen del sitio



Whois

```
soc@misp:~$ whois -h whois.publicDomainRegistry.com inscripcionrut.com
Domain Name: INSCRIPCIONRUT.COM
Registry Domain ID: 2427555993_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.publicdomainregistry.com
Registrar URL: www.publicdomainregistry.com
Updated Date: 2019-08-27T19:16:00Z
Creation Date: 2019-08-27T19:15:59Z
Registrar Registration Expiration Date: 2020-08-27T19:15:59Z
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: alesandra
Registrant Organization: fravatel
Registrant Street: avenida lima 221 santa isabel
Registrant City: lima
Registrant State/Province: Lima
Registrant Postal Code: 00051
Registrant Country: PE
Registrant Phone: +51.965662142
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: sandrariveralopezjjc8343@gmail.com
Registry Admin ID: Not Available From Registry
Admin Name: alesandra
Admin Organization: fravatel
Admin Street: avenida lima 221 santa isabel
Admin City: lima
Admin State/Province: Lima
Admin Postal Code: 00051
Admin Country: PE
Admin Phone: +51.965662142
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: sandrariveralopezjjc8343@gmail.com
Registry Tech ID: Not Available From Registry
Tech Name: alesandra
Tech Organization: fravatel
Tech Street: avenida lima 221 santa isabel
Tech City: lima
Tech State/Province: Lima
Tech Postal Code: 00051
Tech Country: PE
Tech Phone: +51.965662142
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: sandrariveralopezjjc8343@gmail.com
Name Server: ns8371.hostgator.com
Name Server: ns8372.hostgator.com
DNSSEC: Unsigned
Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com
Registrar Abuse Contact Phone: +1.2013775952
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2019-10-04T16:54:39Z <<<

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

Registration Service Provided By: BLUEHOST MEXICO

The data in this whois database is provided to you for information 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: 2019.10.05 11:57:51 -03'00'