Alerta de seguridad informática	**8FFR-00087-001**
Clase de alerta	**Fraude**
Tipo de incidente	**Falsificación de Registros o Identidad**
Nivel de riesgo	**Alto**
TLP	**Blanco**
Fecha de lanzamiento original	**11 de Octubre de 2019**
Última revisión	**11 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 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

http[://]b3nefici0[.]info/tools/imagenes/comun2008/banca-en-linea-personas[.]html

Domain b3nefici0.info			
b3nefici0 / info / Subdomains			
record type	TTL	value	
No records found			

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

Certificado

Certificates	crt.sh ID	Logged At ⇧	Not Before	Not After	Issuer Name
	1979117357	2019-10-10	2019-10-10	2020-01-08	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
	1979117132	2019-10-10	2019-10-10	2020-01-08	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"

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

IP´s

23[.]254[.]253[.]92

Domain b3nefici0.info is located on IP address << 23.254.253.92 >>	
Block start	23.254.128.0
End of block	23.254.255.255
Block size	32768 Domains in block
Block name	HOSTWINDS-17-6
AS number	54290
Parent block	23.0.0.0 - 23.255.255.255
Organization	HostwindsLLC.
City	Tulsa
Region/State	Oklahoma
Country	US , United States
Reg. date	2013-11-13
Host name	informatica.ms
Domain count	>= 2 Servers around
Domains	1 b3nefici0.info 2 ns1.somanyservers.com

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

Localización

Seattle, Washington, Estados Unidos

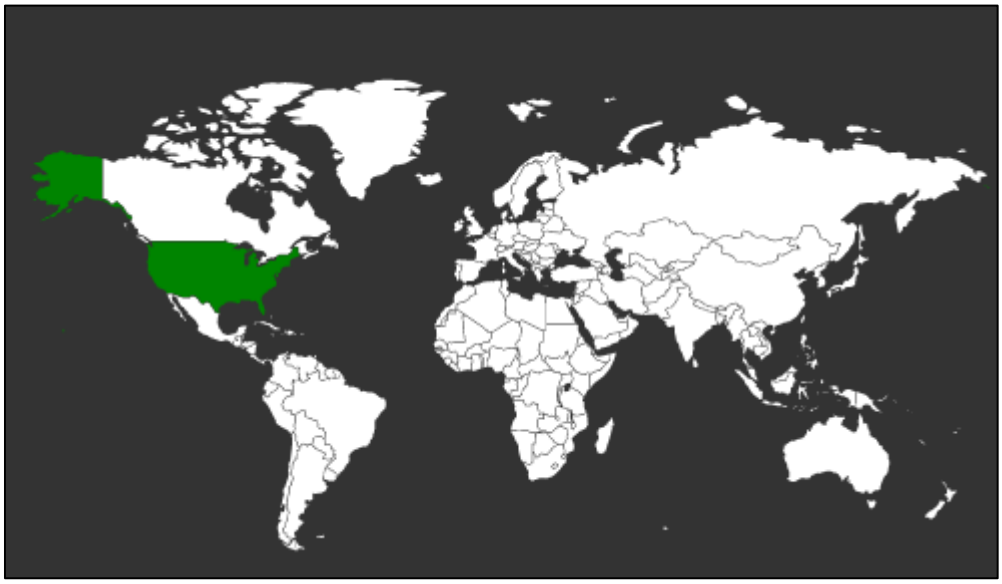
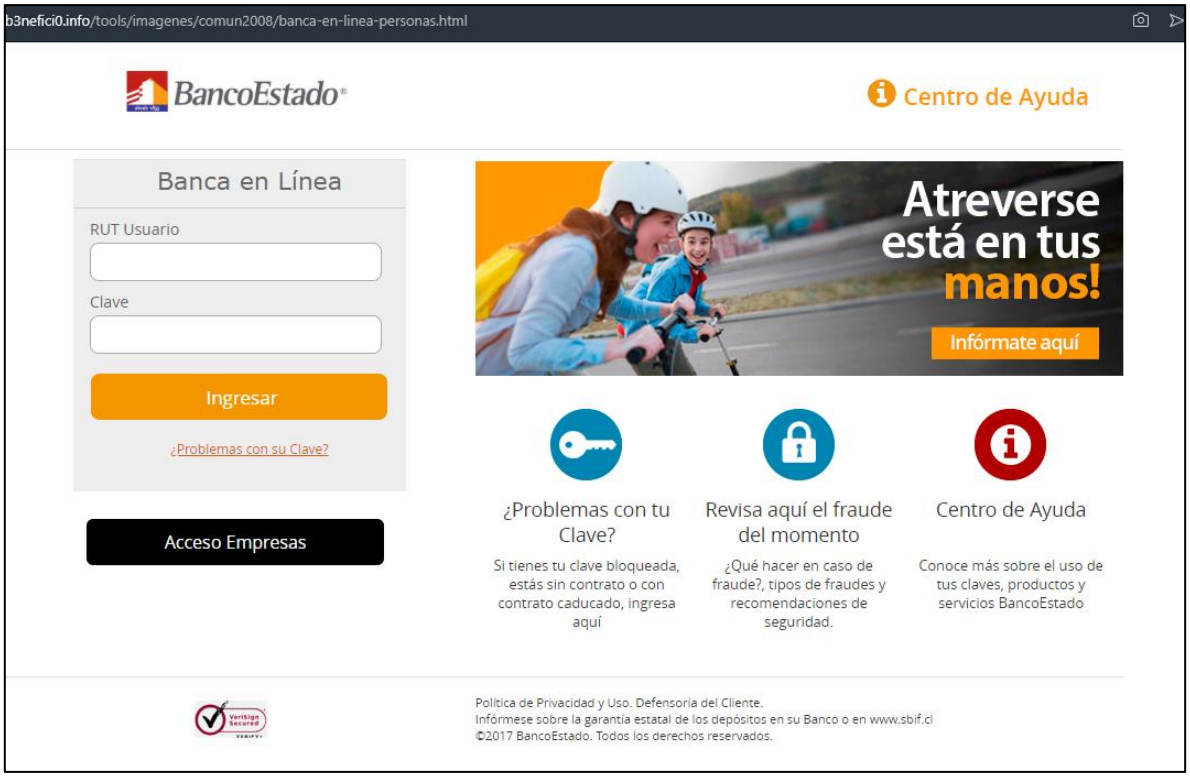


Imagen del sitio



Whois

```
Domain Name: B3NEFICI0.INFO
Registry Domain ID: D503300001181924531-LRMS
Registrar WHOIS Server: whois.scip.es
Registrar URL: https://www.dondominio.com
Updated Date: 2019-10-10T15:32:13Z
Creation Date: 2019-10-07T08:16:06Z
Registrar Registration Expiration Date: 2020-10-07T08:16:06Z
Registrar: DonDominio (SCIP)
Registrar IANA ID: 1383
Registrar Abuse Contact Email: abuse@scip.es
Registrar Abuse Contact Phone: +34.871-98-63-87
Reseller:
Domain Status: clientHold http://www.icann.org/epp#clientHold
Registry Registrant ID:
Registrant Name: Redacted for privacy
Registrant Organization:
Registrant Street: Redacted for privacy
Registrant City: Redacted for privacy
Registrant State/Province: Lima
Registrant Postal Code: Redacted for privacy
Registrant Country: PE
Registrant Phone: Redacted for privacy
Registrant Phone Ext:
Registrant Fax: Redacted for privacy
Registrant Fax Ext:
Registrant Email: Visit https://icann.online-validation.com/domain-contact/?domainname=b3nefici0.info
Registry Admin ID:
Admin Name: Redacted for privacy
Admin Organization: Redacted for privacy
Admin Street: Redacted for privacy
Admin City: Redacted for privacy
Admin State/Province: Redacted for privacy
Admin Postal Code: Redacted for privacy
Admin Country: Redacted for privacy
Admin Phone: Redacted for privacy
Admin Phone Ext:
Admin Fax: Redacted for privacy
Admin Fax Ext:
Admin Email: Visit https://icann.online-validation.com/domain-contact/?domainname=b3nefici0.info
Registry Tech ID:
Tech Name: Redacted for privacy
Tech Organization: Redacted for privacy
Tech Street: Redacted for privacy
Tech City: Redacted for privacy
Tech State/Province: Redacted for privacy
Tech Postal Code: Redacted for privacy
Tech Country: Redacted for privacy
Tech Phone: Redacted for privacy
Tech Phone Ext:
Tech Fax: Redacted for privacy
Tech Fax Ext:
Tech Email: Visit https://icann.online-validation.com/domain-contact/?domainname=b3nefici0.info
Registry Billing ID:
Billing Name: Redacted for privacy
Billing Organization: Redacted for privacy
Billing Street: Redacted for privacy
Billing City: Redacted for privacy
Billing State/Province: Redacted for privacy
Billing Postal Code: Redacted for privacy
Billing Country: Redacted for privacy
```

```
Domain Name: B3NEFICIO.INFO
Registry Domain ID: D503300001181924531-LRMS
Registrar WHOIS Server: whois.scip.es
Registrar URL: www.dondominio.com
Updated Date: 2019-10-10T13:32:13Z
Creation Date: 2019-10-07T08:16:06Z
Registry Expiry Date: 2020-10-07T08:16:06Z
Registrar Registration Expiration Date:
Registrar: Soluciones Corporativas IP, SLU
Registrar IANA ID: 1383
Registrar Abuse Contact Email: abuse@scip.es
Registrar Abuse Contact Phone: +34.871986387
Reseller:
Domain Status: clientHold https://icann.org/epp#clientHold
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: addPeriod https://icann.org/epp#addPeriod
Registrant Organization:
Registrant State/Province: Lima
Registrant Country: PE
Name Server: DALNS5.MASTERNS.COM
Name Server: DALNS6.MASTERNS.COM
DNSSEC: unsigned
```

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: 2019.10.11 09:32:49 -03'00'