Alerta de seguridad cibernética	8FFR20-00347-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de abril de 2020
Última revisión	18 de abril 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 portale 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 COMPROMISO

URL
homevirtual[.]chile-digital[.]net

IP
195[.]123[.]212[.]227

DOMINIOS DONDE SE ALOJA URL

Domain homevirtual.chile-digital.net

homevirtual / chile-digital / net / Subdomains

record type	TTL	value
A	14400	195.123.212.227

Domain chile-digital.net

chile-digital / net / Subdomains

record type	TTL	value		
A	14400	195.123.212.227		
NS	86400	ns1.chile-digital.net	Zones on DNS server	195.123.212.227
NS	86400	ns2.chile-digital.net	Zones on DNS server	195.123.212.227
MX	14400	0 chile-digital.net		
TXT	14400	v=spf1 +a +mx +ip4:195.123.212.227 ~all		

SOA	86400	Mname	ns1.chile-digital.net
		Rname	root.natru.vps.com
		Serial number	2020041715
		Refresh	3600
		Retry	1800
		Expire	1209600
		Minimum TTL	86400

CERTIFICADOS

Subject DN	CN=homevirtual.chile-digital.net
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	393299648379289314343176820782733055394703
Validity	2020-04-17 04:35:40 **to** 2020-07-16 04:35:40 (90 days, 0:00:00)
Names	homevirtual.chile-digital.net

IP DE ORIGEN DONDE SE ALOJA SITIO

Domain homevirtual.chile-digital.net is located on IP address << 195.123.212.227 >>

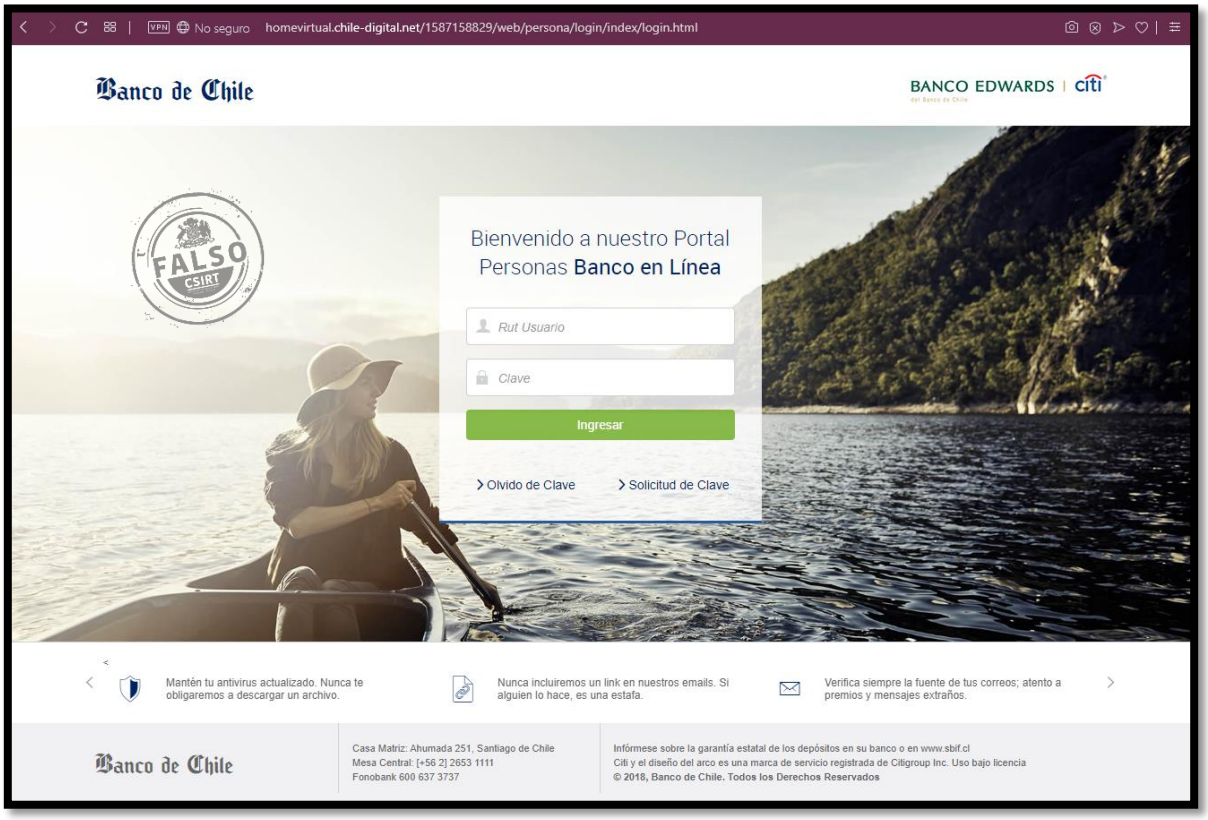
Block start	195.123.208.0
End of block	195.123.215.255
Block size	2048 Domains in block
Block name	GF-RIX-NET
AS number	50979
Parent block	195.123.208.0 - 195.123.247.255
Organization	* * As ISP we provide hosting, virtual and dedicated servers. * * Those services are self managed by our customers * therefore, we are not us

LOCALIZACIÓN

Kekava, Kekavas novads, Letonia

Location	Latvia (LV)
Latitude and Longitude	57, 25

IMAGEN DEL SITIO



WHOIS

```
Domain Name: CHILE-DIGITAL.NET
Registry Domain ID: 2514537246_DOMAIN_NET-VRSN
Registrar WHOIS Server: whois.domain.com
Registrar URL: www.domain.com
Updated Date: 2020-04-13T22:09:17
Creation Date: 2020-04-13T22:00:12
Registrar Registration Expiration Date: 2021-04-13T22:00:12
Registrar: Domain.com, LLC
Registrar IANA ID: 886
Reseller: Domain.com
Domain Status:
Registry Registrant ID:
Registrant Name: Domain Privacy Service FBO Registrant.
Registrant Organization: Domain Privacy Service FBO Registrant.
Registrant Street: 10 Corporate Drive
Registrant City: Burlington
Registrant State/Province: MA
Registrant Postal Code: 01803
Registrant Country: US
Registrant Phone: +1.6027165339
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: chile-digital.net@domainprivacygroup.com
Registry Admin ID:
Admin Name: Domain Privacy Service FBO Registrant.
Admin Organization: Domain Privacy Service FBO Registrant.
Admin Street: 10 Corporate Drive
Admin City: Burlington
Admin State/Province: MA
Admin Postal Code: 01803
Admin Country: US
Admin Phone: +1.6027165339
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: chile-digital.net@domainprivacygroup.com
Registry Tech ID:
Tech Name: Domain Privacy Service FBO Registrant.
Tech Organization: Domain Privacy Service FBO Registrant.
Tech Street: 10 Corporate Drive
Tech City: Burlington
Tech State/Province: MA
Tech Postal Code: 01803
Tech Country: US
Tech Phone: +1.6027165339
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: chile-digital.net@domainprivacygroup.com
Name Server: ns2.domain.com
Name Server: ns1.domain.com
DNSSEC: unsigned
Registrar Abuse Contact Email: compliance@domain-inc.net
Registrar Abuse Contact Phone: +1.6027165396
```

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: 2020.04.18 18:38:23 -04'00'