Alerta de seguridad informática	8FFR-00130-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de Noviembre de 2019
Última revisión	28 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.

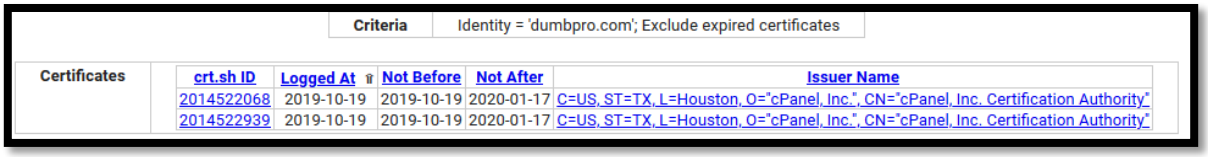
Indicadores de Compromisos

URL´s

URL Sitio Clonado:
http[://]dumbpro[.]com/wp/wp-content/plugins/kirki/core/servicio/nuevo/servicios[.]aumento[.]bancochile[.]cl/b7hqgb790i/lcf3v_persona/login_taqa/index/login0nkm

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

Certificados



Criteria	Identity = 'dumbpro.com'; Exclude expired certificates

Certificates

crt.sh ID	Logged At	Not Before	Not After	Issuer Name
2014522068	2019-10-19	2019-10-19	2020-01-17	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
2014522939	2019-10-19	2019-10-19	2020-01-17	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 de Chile

IP

23.94.187.130

A / AAAA Record	Provider	ASN
23.94.187.130 (US) used by 544 domains	ColoCrossing (US)	AS36352

NS Record	IP Address	Provider	ASN
ns501.globalhostingservers.com used by 504 domains	23.94.187.158 (US)	ColoCrossing (US)	AS36352
ns500.globalhostingservers.com used by 504 domains	23.94.187.130 (US)	ColoCrossing (US)	AS36352

MX Record	IP Address	Provider	ASN
dumbpro.com (pref: 0) used by 1 domain	23.94.187.130 (US)	ColoCrossing (US)	AS36352

SPF Record

```
v=spf1 ip4:23.94.187.130 +a +mx ~all
```

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

Localización

Buffalo, New York, Estados Unidos

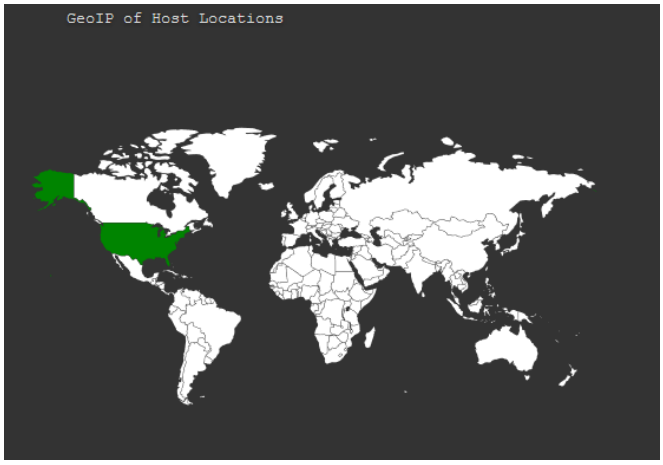
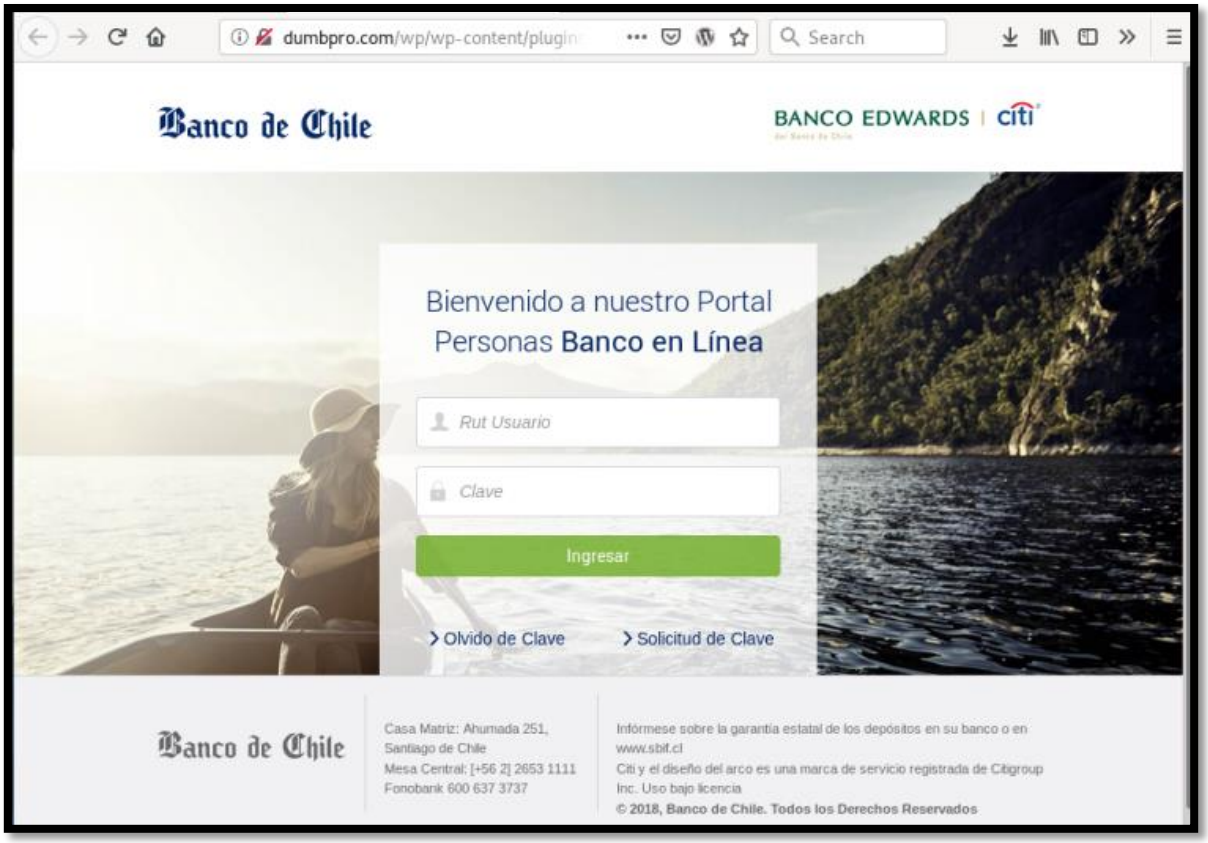


Imagen del sitio



Whois

```
Domain Name: dumbpro.com
Registry Domain ID: 2390339342_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Updated Date: 2019-05-13T14:12:07Z
Creation Date: 2019-05-13T14:12:06Z
Registrar Registration Expiration Date: 2020-05-13T14:12:06Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited
Registrant Organization:
Registrant State/Province: Uttar Pradesh
Registrant Country: IN
Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=dumbp
ro.com
Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=dumbpro.co
m
Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=dumbpro.com
Name Server: NS500.GLOBALHOSTINGSERVERS.COM
Name Server: NS501.GLOBALHOSTINGSERVERS.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: 2019.11.28 08:58:15 -03'00'