Alerta de seguridad cibernética	8FFR20-00427-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de mayo de 2020
Última revisión	22 de mayo 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 detectado la activación de un portal fraudulento asociado a una IP que suplanta la entrega de bonos del Instituto de Previsión Social, el que podría servir para robar información sensible.

Lo anterior constituye una falsificación de la entidad gubernamental que podría afectar a los ciudadanos de Chile.

Indicadores de compromiso

URLs
bonosdechile[.]cl

IPs
138[.]186[.]9[.]45

Dominio donde se aloja url

Domain bonosdechile.cl

bonosdechile / cl / Subdomains

record type	TTL	value		
A	14400	138.186.9.45		
NS	86400	ns2.neptuno.denial.cl	Zones on DNS server	138.186.9.45
NS	86400	ns1.neptuno.denial.cl	Zones on DNS server	138.186.9.45
MX	14400	0 bonosdechile.cl		
TXT	14400	google-site-verification=aMTxMYpGx68iyBysgmkmh_Y620TnVXtbZyjK57f1G0Y		
TXT	14400	v=spf1 +a +mx +ip4:138.186.9.45 ~all		

SOA	86400		
		Mname	ns1.neptuno.denial.cl
		Rname	contacto.denialhost.com
		Serial number	2020051500
		Refresh	3600
		Retry	1800
		Expire	1209600
		Minimum TTL	86400

Certificados

TLS Certificate

```
Common Name = bonosdechile.cl
Subject Alternative Names = bonosdechile.cl, autodiscover.bonosdechile.cl,
  cpanel.bonosdechile.cl, cpcalendars.bonosdechile.cl,
  cpcontacts.bonosdechile.cl, mail.bonosdechile.cl, webdisk.bonosdechile.cl,
  webmail.bonosdechile.cl, www.bonosdechile.cl
Issuer = cPanel, Inc. Certification Authority
Serial Number = 9A2347A37EEF3964E0778B2B38D28E56
SHA1 Thumbprint = 584897070DEA551AEB5B914F8994EAAE605C4E04
Key Length = 2048
Signature algorithm = SHA256-RSA
Secure Renegotiation:
```

Certificate Name matches bonosdechile.cl

Subject bonosdechile.cl

Valid from 15/May/2020 to 13/Aug/2020

Issuer cPanel, Inc. Certification Authority

Subject cPanel, Inc. Certification Authority

Valid from 18/May/2015 to 17/May/2025

Issuer COMODO RSA Certification Authority

Subject COMODO RSA Certification Authority

Valid from 01/Jan/2004 to 31/Dec/2028

Issuer AAA Certificate Services

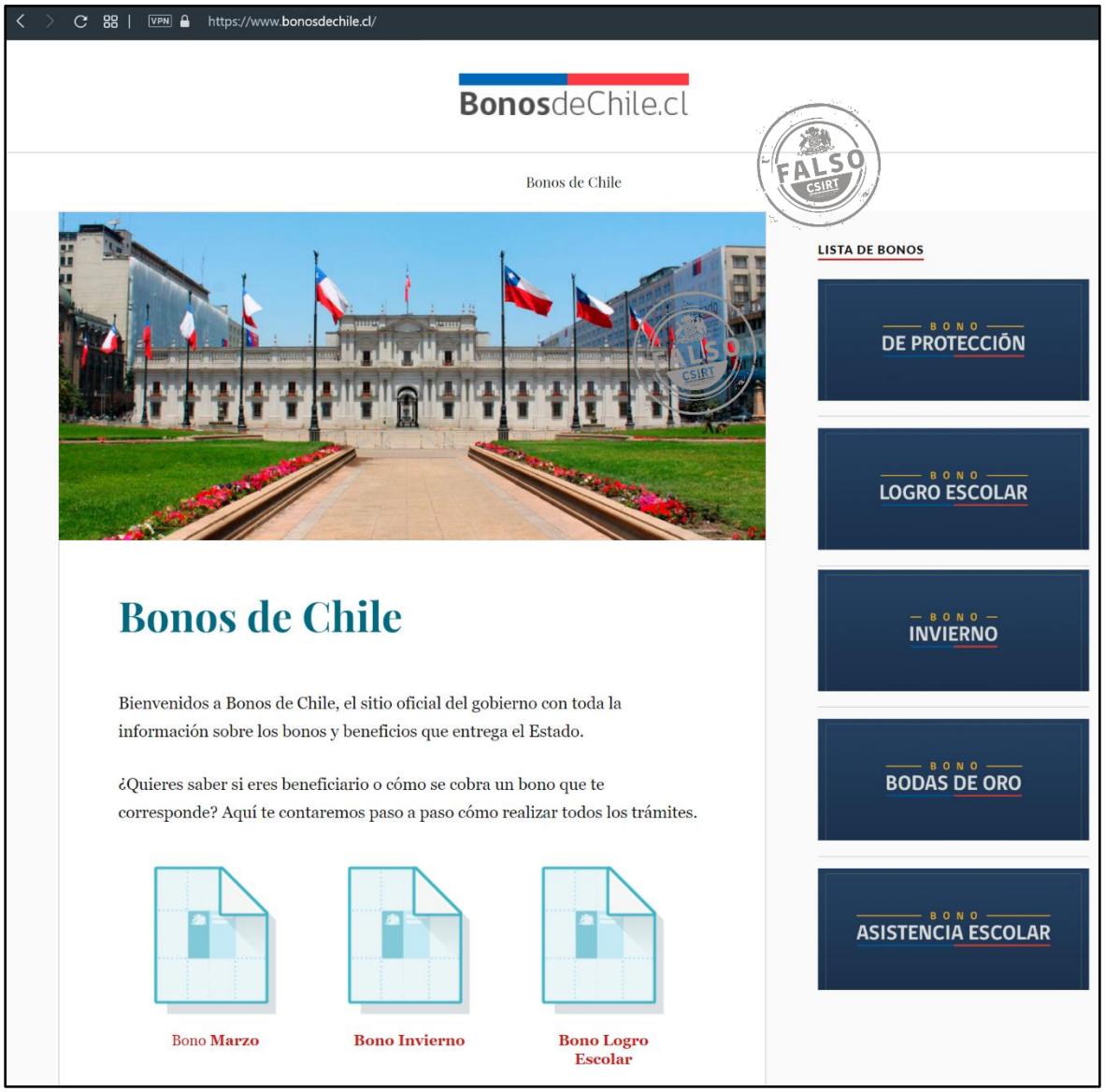
Ip de origen donde se aloja sitio

Domain bonosdechile.cl is located on IP address << 138.186.9.45 >>	
Block start	138.186.8.0
End of block	138.186.11.255
Block size	1024 Domains in block
Block name	
AS number	52511
Parent block	138.0.0.0 - 138.255.255.255
Organization	IRONSERVERS E.I.R.L

Localización

Santiago, Chile

Imagen del sitio



Whois

```
Domain name: bonosdechile.cl
Registrant name: Jos?? Tom??s Covacevich Vogt
Registrant organisation:
Registrar name: NIC Chile
Registrar URL: https://www.nic.cl
Creation date: 2020-04-28 20:08:12 CLST
Expiration date: 2021-04-28 20:08:12 CLST
Name server: ns1.denialhost.com
Name server: ns2.denialhost.com
```

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: 2020.05.22 17:00:16 -04'00'