Alerta de seguridad informática	8FFR-00146-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de Diciembre de 2019
Última revisión	10 de Diciembre 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

URL Sitio Clonado:
https[://]www[.]informaciondepi[.]com/profesional/imagenes/comun2008/banca-en-linea-personas[.]html

Domain www.informaciondepi.com

www / informaciondepi / com / Subdomains

record type	TTL	value	
CNAME	14400	informaciondepi.com	54.39.37.193

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

Certificados

Criteria	Identity = 'www.informaciondepi.com'

Certificates	None found

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

IP

54.39.37.193

Domain www.informaciondepi.com is located on IP address << 54.39.37.193 >>

Block start	54.0.0.0
End of block	54.63.255.255
Block size	4194304 Domains in block
Block name	MERCK2
AS number	16276
Parent block	54.0.0.0 - 54.255.255.255
Organization	Merck and Co., Inc.
City	Rahway
Region/State	New Jersey
Country	US , United States 40735
Reg. date	1992-03-17
Host name	morty.v2net.cl
Domain count	>= 2 Servers around
Domains	1 2019miservicios.com 2 www.informaciondepi.com

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

Localización

Montreal, Quebec, Canadá

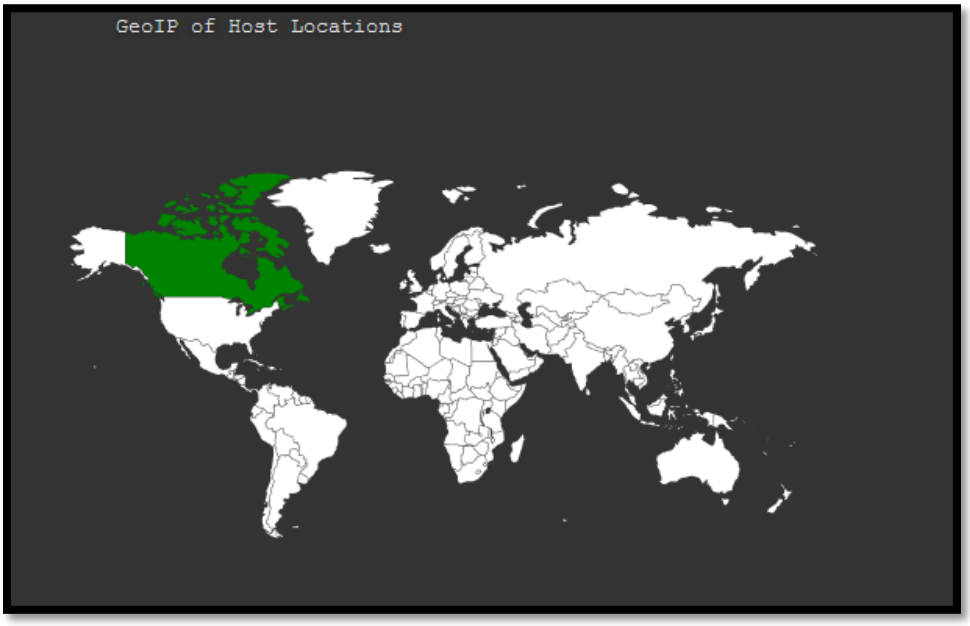
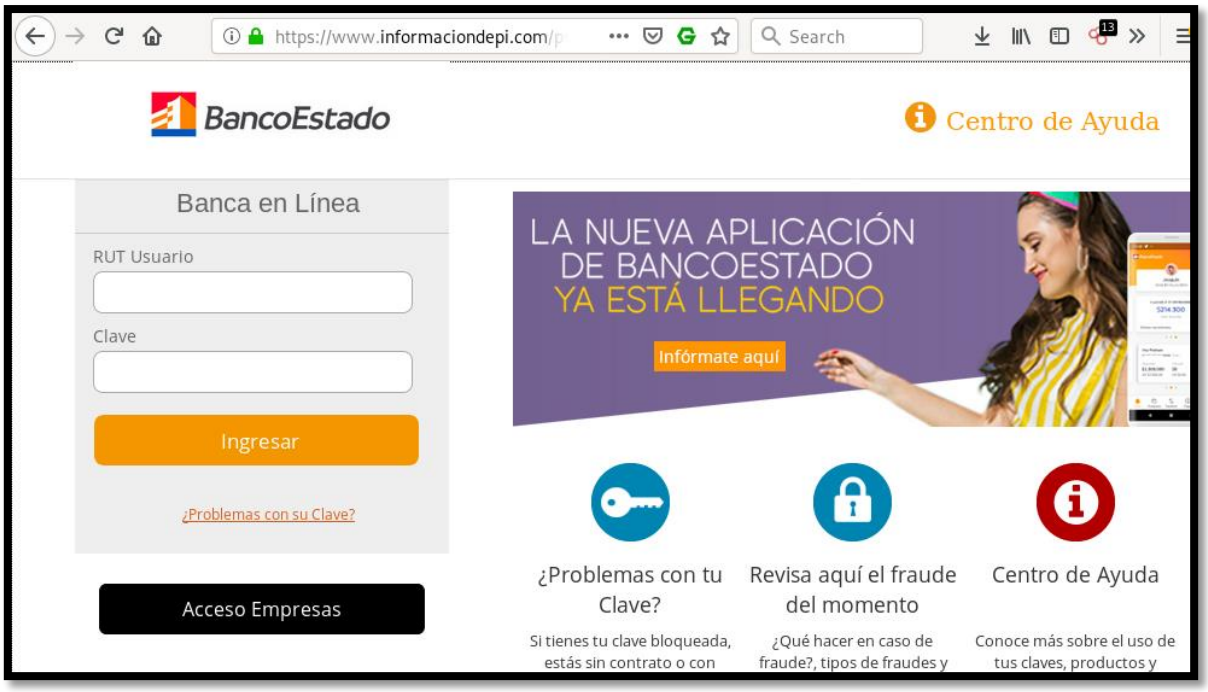


Imagen del sitio



Whois

```
Domain Name: informaciondepi.com
Registry Domain ID: 2463224538_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.registrar.eu
Registrar URL: http://www.registrar.eu
Updated Date: 2019-12-04T16:47:16Z
Creation Date: 2019-12-04T15:47:05Z
Registrar Registration Expiration Date: 2020-12-04T15:47:05Z
Registrar: Hosting Concepts B.V. d/b/a Openprovider
Registrar IANA ID: 1647
Registrar Abuse Contact Email: abuse@registrar.eu
Registrar Abuse Contact Phone: +31.104482297
Domain Status: ok https://icann.org/epp#ok
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: Informacion depilatoria
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: Las condes
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: CL
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext: REDACTED FOR PRIVACY
Registrant Email: https://contact-form.registrar.eu/?domainName=informaciondepi.com&purpose=owner
Registry Admin ID: REDACTED FOR PRIVACY
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: REDACTED FOR PRIVACY
Admin Fax: REDACTED FOR PRIVACY
Admin Fax Ext: REDACTED FOR PRIVACY
Admin Email: https://contact-form.registrar.eu/?domainName=informaciondepi.com&purpose=admin
Registry Tech ID: REDACTED FOR PRIVACY
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: REDACTED FOR PRIVACY
Tech Fax: REDACTED FOR PRIVACY
Tech Fax Ext: REDACTED FOR PRIVACY
Tech Email: https://contact-form.registrar.eu/?domainName=informaciondepi.com&purpose=tech
Name Server: ns22.v2net.cl
Name Server: ns21.v2net.cl
DNSSEC: unsigned

URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2019-12-09T13:03:49Z <<<
```

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: 2019.12.10 14:44:40 -03'00'