Alerta de seguridad informática	**8FFR-00073-001**
Clase de alerta	**Fraude**
Tipo de incidente	**Falsificación de Registros o Identidad**
Nivel de riesgo	**Alto**
TLP	**Blanco**
Fecha de lanzamiento original	**30 de Septiembre de 2019**
Última revisión	**30 de Septiembre 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 19 sitios fraudulentos asociados a una IP que suplanta el sitio web oficial del **Banco de Chile**, los que podrían 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

https[://]www[.]auto-usa[.]dp[.]ua/wp-includes/css/https/R1/index[.]php

https[://]consumo-valido[.]cf/hipotecario/www[.]bancoedwards[.]cl/Login[.]htm?login[.]bancochile[.]cl/bancochile-web/persona/login/index[.]html#/login

URL relacionadas con la campaña de phishing

consumo-valido[.]cf
consumo-valido-hipotecario[.]gq
consumohipoteca[.]cf
consumohipoteca[.]gq
consumo-valido[.]gq
consumo-valido-hipotecario[.]cf
consumohipotecariopersona[.]cf
consumohipotecariopersona[.]ga
www[.]consumohipoteca[.]cf
www[.]consumo-valido[.]cf
www[.]consumo-valido-hipotecario[.]gq
www[.]consumo-valido-hipotecario[.]ga
www[.]consumo-valido-hipotecario[.]cf
consumo-valido-hipotecario[.]ga
www[.]consumohipoteca[.]gq
www[.]consumohipotecariopersona[.]ga
www[.]consumohipotecariopersona[.]cf

Para obtener los sitios es necesario especificar el directorio a las url

"/hipotecario/www.bancoedwards.cl/Login.htm?login.bancochile.cl/bancochile-web/persona/login/index.html

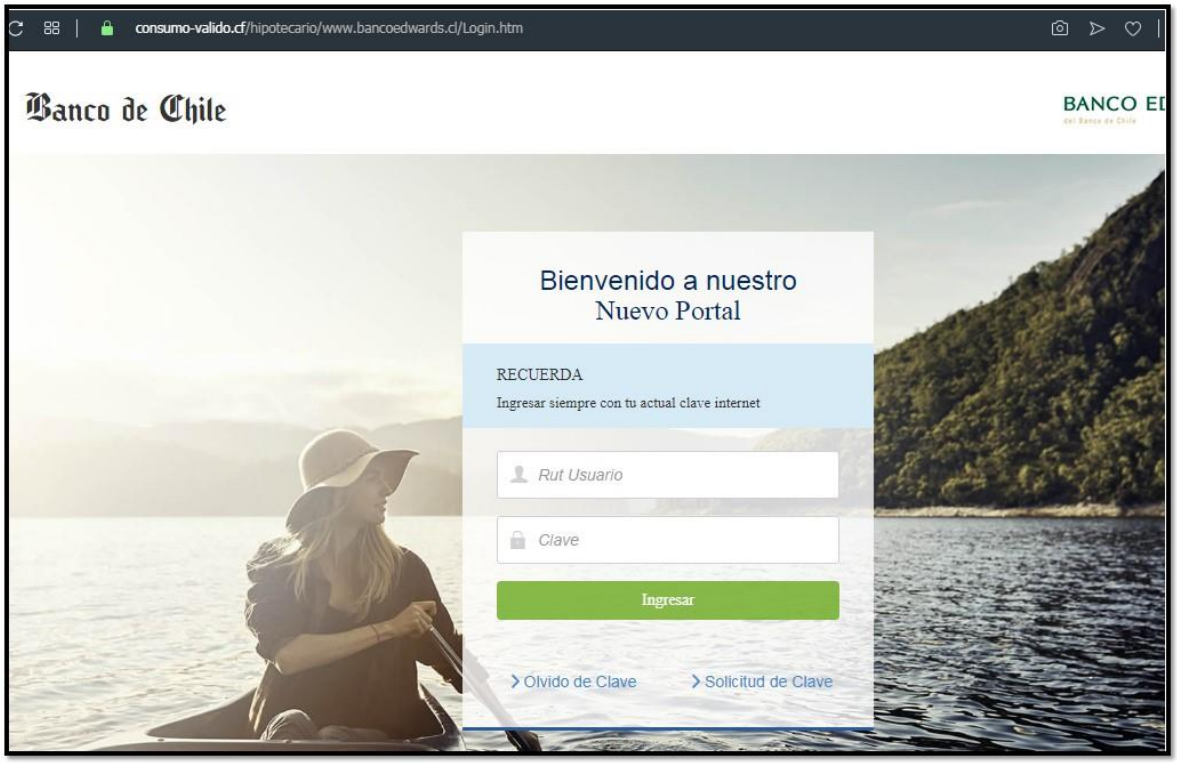
IP´s

91[.]234[.]99[.]106

Localización

Amsterdam, Noord-Holland, Holanda

Imagen del sitio



Whois

- https[://]www[.]auto-usa[.]dp[.]ua/wp-includes/css/https/R1/index[.]php

```
soc@ITQ-ivps2:~$ whois auto-usa.dp.ua
% Request from 2604:880:54::36a
% This is the Ukrainian Whois query server #F.
% The Whois is subject to Terms of use
% See https://hostmaster.ua/services/
%
% IN THE PROCESS OF DELEGATION OF A DOMAIN NAME,
% THE REGISTRANT IS AN ENTITY WHO USES AND MANAGES A CERTAIN DOMAIN NAME,
% AND THE REGISTRAR IS A BUSINESS ENTITY THAT PROVIDES THE REGISTRANT
% WITH THE SERVICES NECESSARY FOR THE TECHNICAL MAINTENANCE OF THE REGISTRATION AND OPERATION OF THE DOMAIN NAME.
% FOR INFORMATION ABOUT THE REGISTRANT OF THE DOMAIN NAME, YOU SHOULD CONTACT THE REGISTRAR.

% The object shown below is NOT in the UAEPP database.
% It has been obtained by querying a remote server:
% (whois.dp.ua) at port 43.
%
% REDIRECT BEGIN

% This is the Dnepropetrovsk Whois query server.
%

domain:           auto-usa.dp.ua
registrant:       dxp-717213-ofcpw
admin-c:          dxp-536725-cbnzz
tech-c:           dxp-690175-xqhuz
mnt-by:           dp.ukraine
nserver:          ns118.inhostedns.com
nserver:          ns218.inhostedns.net
nserver:          ns318.inhostedns.org
status:           ok
created:          2018-12-18 23:23:13+02
modified:         2018-12-18 23:23:13+02
expires:          2019-12-18 23:23:13+02
source:           DPNIC

% Registrar:
% ==========
registrar:        dp.ukraine
organization-loc: ТОВ "Хостінг Україна"
address-loc:      а/с 65
address-loc:      Київ
postal-code-loc:  04112
country-loc:      UA
phone:            +380.443927433
e-mail:           hostmaster@ukraine.com.ua
url:              http://www.ukraine.com.ua
source:           DPNIC

% Registrant:
% ===========
contact-id:       dxp-717213-ofcpw
person:           not published
address:          not published
e-mail:           not published
mnt-by:           dp.ukraine
created:          2018-12-18 23:23:04+02
modified:         2018-12-18 23:23:04+02
source:           DPNIC

% Administrative Contact:
% =======================
contact-id:       dxp-536725-cbnzz
person:           not published
```

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: 2019.09.30 21:56:20 -03'00'