Alerta de seguridad informática	**8FFR-00028-001**
Clase de alerta	**Fraude**
Tipo de incidente	**Falsificación de Registros o Identidad**
Nivel de riesgo	**Alto**
TLP	**Blanco**
Fecha de lanzamiento original	**26 de Agosto de 2019**
Última revisión	**26 de Agosto 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 46 portales fraudulentos asociados a 3 IP's que suplantan el sitio web oficial del **bancochile.cl** 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

Portalweb[.]live	
portalclientesbch[.]ns2[.]name	104[.]238[.]220[.]34
www[.]portalbanca[.]ns3[.]name	104[.]238[.]220[.]34
portalbanca[.]ns3[.]name	104[.]238[.]220[.]34
www[.]portalbanca1[.]dns05[.]com	104[.]238[.]220[.]34
portalbanca1[.]dns05[.]com	104[.]238[.]220[.]34
www[.]personasweb[.]dns05[.]com	104[.]238[.]220[.]34
personasweb[.]dnset[.]com	104[.]238[.]220[.]34
www[.]personasweb[.]dnset[.]com	104[.]238[.]220[.]34
personasweb[.]dns05[.]com	104[.]238[.]220[.]34
www[.]portalbanca1[.]ddns[.]info	104[.]238[.]220[.]34
portalbanca1[.]ddns[.]info	104[.]238[.]220[.]34
www[.]portalclientes[.]dns2[.]us	104[.]238[.]220[.]34
portalclientes[.]dns2[.]us	104[.]238[.]220[.]34
www[.]webportal[.]dns04[.]com	104[.]238[.]220[.]34
webportal[.]dns04[.]com	104[.]238[.]220[.]34
www[.]portalclientes1[.]ns02[.]us	104[.]238[.]220[.]34
portalclientes1[.]ns02[.]us	104[.]238[.]220[.]34
www[.]portalenlinea[.]ns02[.]info	104[.]238[.]220[.]34
www[.]webportal[.]dns05[.]com	104[.]238[.]220[.]34
webportal[.]dns05[.]com	104[.]238[.]220[.]34
www[.]portalbanca[.]ddns[.]name	104[.]238[.]220[.]34
www[.]portalbanca4[.]port25[.]biz	104[.]238[.]220[.]34
portalbanca4[.]port25[.]biz	104[.]238[.]220[.]34
www[.]portalbanca[.]ns1[.]name	104[.]238[.]220[.]34
www[.]clientesbchile1[.]ddns[.]ms	104[.]238[.]220[.]34
clientesbchile1[.]ddns[.]ms	104[.]238[.]220[.]34
portalbanca[.]ns1[.]name	104[.]238[.]220[.]34
clientesportal[.]ddns[.]info	104[.]238[.]220[.]34
www[.]clientesportal[.]ddns[.]info	104[.]238[.]220[.]34
www[.]portalpersonas[.]ns3[.]name	176[.]31[.]86[.]164
www[.]portalpersonas[.]ns1[.]name	176[.]31[.]86[.]164
www[.]portalpersonas[.]ns2[.]name	176[.]31[.]86[.]164
www[.]portalbanca3[.]ns01[.]info	104[.]238[.]220[.]34
portalpersonas[.]ns3[.]name	176[.]31[.]86[.]164
portalpersonas[.]ns1[.]name	176[.]31[.]86[.]164
portalpersonas[.]ns2[.]name	176[.]31[.]86[.]164
portalclientes[.]sendsmtp[.]com	104[.]238[.]220[.]34
portalbanca3[.]ns01[.]info	104[.]238[.]220[.]34
www[.]portalclientes[.]sendsmtp[.]com	104[.]238[.]220[.]34
www[.]portalbanca1[.]ns02[.]info	104[.]238[.]220[.]34
portalbanca1[.]ns02[.]info	104[.]238[.]220[.]34

www[.]portalbanca4[.]ns02[.]info	104[.]238[.]220[.]34
portalbanca4[.]ns02[.]info	104[.]238[.]220[.]34
portalenlinea[.]ns02[.]info	104[.]238[.]220[.]34
www[.]portalclientesbch[.]ns2[.]name	104[.]238[.]220[.]34

IP´s
204[.]16[.]169[.]2
104[.]238[.]220[.]34
176[.]31[.]86[.]164

Localización
San Marcos, California, Estados Unidos
Miami, Florida, Estados Unidos
Roubaix, Hauts-de-France, Francia

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