

Alerta de seguridad cibernética	8FFR21-00943-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Abril de 2021
Última revisión	30 de Abril de 2021

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 afectada 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 de Gobierno), ha identificado la activación de una página fraudulenta que intenta suplantar al Servicio de Impuestos Internos (SII), la que podría servir para robar credenciales de usuarios.

Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad aludida.

Indicadores de compromiso

URL sitio falso

https://sii-chile[.]com/AUT2000/InicioAutenticacion/IngresoSII.html?token=6c6c6f70657a40534f46544c414e442e434c

Certificado Digital

Fecha Válido 09-04-2021
Fecha Término 08-07-2021
Emitido Let's Encrypt

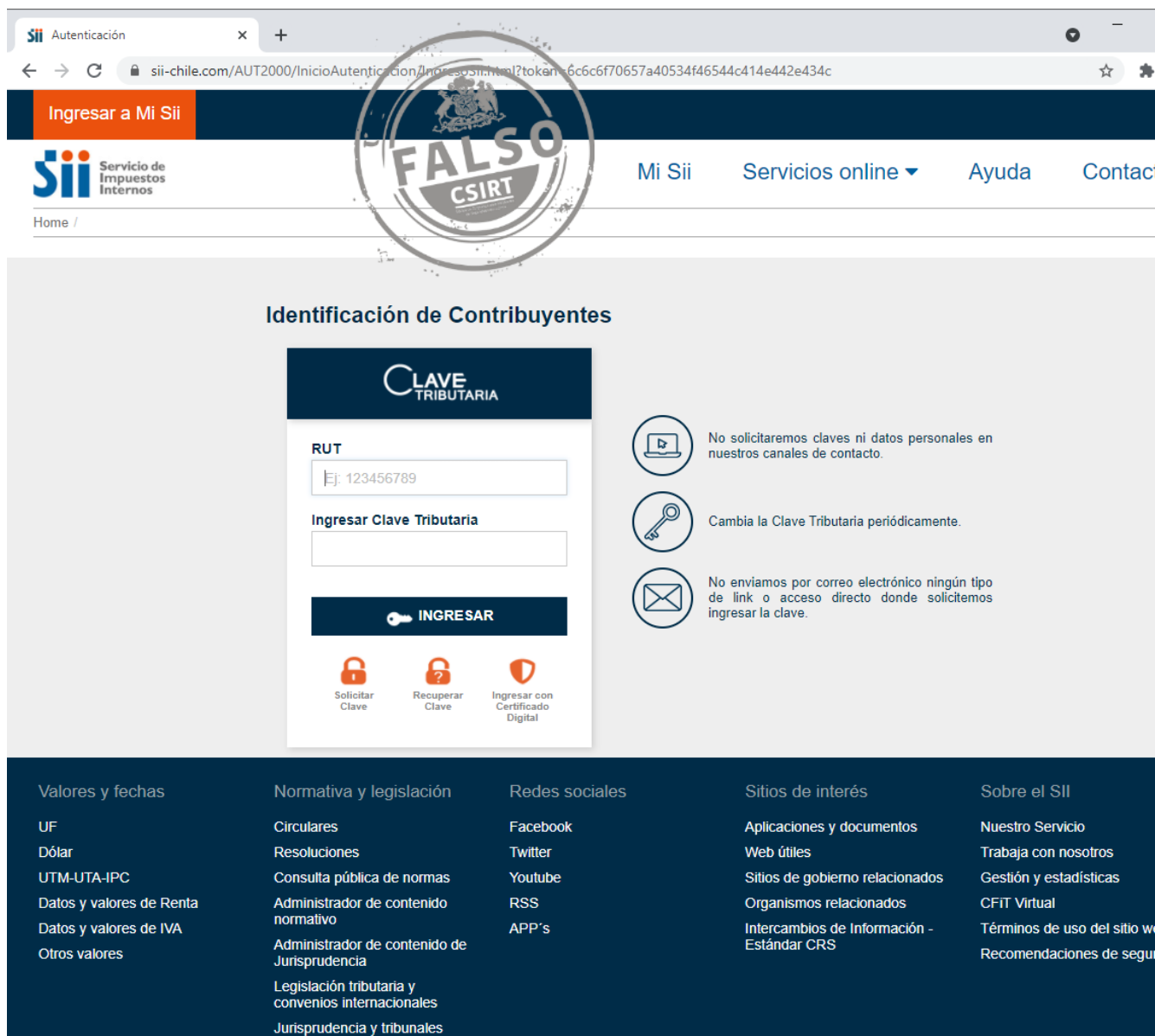
Datos Alojamiento

IP [69.164.215.190]
Número de Sistema Autónomo 63949
Etiqueta del Sistema Autónomo Linode, LLC
País US
Registrador ARIN

Datos del Dominio

Nombre de Dominio sii-chile[.]com
Creado 09-04-2021
Expira 26-04-2022
Información del Registrador NameSilo, LLC
ID IANA 1068
Correo Electrónico abuse@namesilo.com
Name Server ns2.linode.com
ns2.linode.com
ns3.linode.com

Imagen del sitio



The screenshot shows the Sii website's login page. At the top, there is a navigation bar with the Sii logo and the text 'Servicio de Impuestos Internos'. A large watermark reading 'FALSO CSIRT' is overlaid on the page. The main content area is titled 'Identificación de Contribuyentes' and features a 'CLAVE TRIBUTARIA' login form. The form includes a 'RUT' field with the example 'Ej: 123456789', a 'Ingresar Clave Tributaria' field, and an 'INGRESAR' button. Below the form are three options: 'Solicitar Clave', 'Recuperar Clave', and 'Ingresar con Certificado Digital'. To the right of the form, there are three informational icons: a laptop for 'No solicitaremos claves ni datos personales en nuestros canales de contacto.', a key for 'Cambia la Clave Tributaria periódicamente.', and an envelope for 'No enviamos por correo electrónico ningún tipo de link o acceso directo donde solicitemos ingresar la clave.' At the bottom, there is a footer with five columns of links: 'Valores y fechas', 'Normativa y legislación', 'Redes sociales', 'Sitios de interés', and 'Sobre el SII'.

Recomendaciones

- No abrir correos ni mensajes de dudosa procedencia.
- Desconfiar de los enlaces y archivos en los mensajes o correo.
- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).
- Ser escépticos frente ofertas, promociones o premios increíbles que se ofrecen por internet
- Prestar atención en los detalles de los mensajes o redes sociales
- 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.
- Realizar concientización permanente para los usuarios sobre este tipo de amenazas.
- Visualizar los sitios web que se ingresen sean los oficiales.