Alerta de seguridad informática	**8FFR-00032-001**
Clase de alerta	**Fraude**
Tipo de incidente	**Falsificación de Registros o Identidad**
Nivel de riesgo	**Alto**
TLP	**Blanco**
Fecha de lanzamiento original	**29 de Agosto de 2019**
Última revisión	**29 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 portal fraudulentos asociados a una IP que suplantan el sitio web oficial del Servicio de impuestos Internos 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
[http://]siicl.]net/]http[://]siicl[.]net/

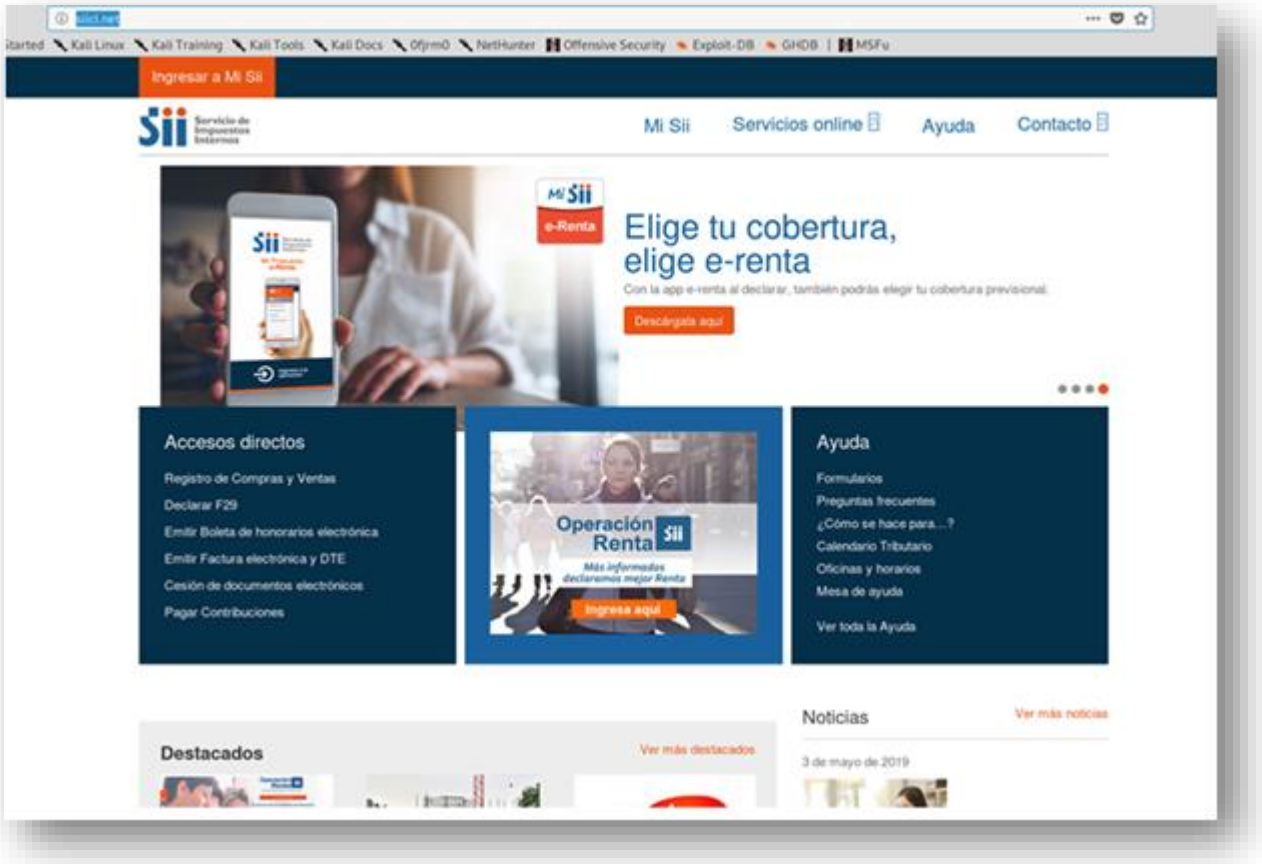
IP
188[.]241[.]39[.]220

Localización
London, England

Whois

```
soc@kali:~$ whois -h whois.namesilo.com siicl.net
Domain Name: siicl.net
Registry Domain ID: 2384346073_DOMAIN_NET-VRSN
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com/
Updated Date: 2019-08-25T07:00:00Z
Creation Date: 2019-04-25T07:00:00Z
Registrar Registration Expiration Date: 2020-04-25T07:00:00Z
Registrar: NameSilo, LLC
Registrar IANA ID: 1479
Registrar Abuse Contact Email: abuse@namesilo.com
Registrar Abuse Contact Phone: +1.4805240066
Reseller: QHOSTER.COM
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Juan de Dios Crisostomo Carrasco
Registrant Organization:
Registrant Street: Duran 13 Calle 2
Registrant City: Santiago
Registrant State/Province: Region Metropolitana
Registrant Postal Code: 000243
Registrant Country: CL
Registrant Phone: +56.954114121
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: mopavil975@gmail.com
Registry Admin ID:
Admin Name: Juan de Dios Crisostomo Carrasco
Admin Organization:
Admin Street: Duran 13 Calle 2
Admin City: Santiago
Admin State/Province: Region Metropolitana
Admin Postal Code: 000243
Admin Country: CL
Admin Phone: +56.954114121
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: mopavil975@gmail.com
Registry Tech ID:
Tech Name: Juan de Dios Crisostomo Carrasco
Tech Organization:
Tech Street: Duran 13 Calle 2
Tech City: Santiago
Tech State/Province: Region Metropolitana
Tech Postal Code: 000243
Tech Country: CL
Tech Phone: +56.954114121
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: mopavil975@gmail.com
Name Server: NS1.QHOSTER.NET
Name Server: NS2.QHOSTER.NET
Name Server: NS3.QHOSTER.NET
Name Server: NS4.QHOSTER.NET
DNSSEC: unsigned
```

Imagen


Ingresar a Mi Sii
Mi Sii
Servicios online
Ayuda
Contacto
Elige tu cobertura, elige e-renta
Descárgala aquí
Accesos directos
Registro de Compras y Ventas
Declarar F29
Emitir Boleta de honorarios electrónica
Emitir Factura electrónica y DTE
Cesión de documentos electrónicos
Pagar Contribuciones
Operación Renta
Ingresa aquí
Ayuda
Formularios
Preguntas frecuentes
¿Cómo se hace para...?
Calendario Tributario
Oficinas y horarios
Mesa de ayuda
Ver toda la Ayuda
Destacados
Noticias

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
- 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