Alerta de seguridad informática	8FFR-00145-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de Diciembre de 2019
Última revisión	9 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 mencionadas, 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), con la colaboración del Área de seguridad de Sistemas del Departamento de informática y Aseguramiento de Estándares Tecnológico del Servicio de Impuestos Internos, han identificado la activación de seis portales fraudulentos asociados a una IP que intentan suplantar el sitio web oficial de SII, el que podría servir para robar credenciales de usuarios de esa entidad pública del Estado.

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

Indicadores de Compromisos

URL´s

URL Sitio Clonado:
siicl[.]org
cpanel[.]siicl[.]org
mail[.]siicl[.]org
webdisk[.]siicl[.]org
webmail[.]siicl[.]org
www[.]siicl[.]org

Certificados

Criteria	Identity = 'siicl.org'

Certificates	crt.sh ID	Logged At ⇧	Not Before	Not After	Issuer Name
	2047585492	2019-10-28	2019-10-28	2020-01-26	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
	2047584716	2019-10-28	2019-10-28	2020-01-26	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"

crt.sh ID	2047585492
Summary	Leaf certificate
Certificate Transparency	

Timestamp	Entry #	Log Operator	Log URL
2019-10-28 17:41:49 UTC	102907612	Cloudflare	https://ct.cloudflare.com/logs/nimbus2020
2019-10-28 17:41:49 UTC	27622012	Google	https://ct.googleapis.com/logs/xenon2020
2019-11-08 03:33:42 UTC	821183873	Google	https://ct.googleapis.com/pilot
2019-11-17 02:58:41 UTC	897004775	Google	https://ct.googleapis.com/rocketeer

Revocation

Report a problem with this certificate to the CA

Mechanism	Provider	Status	Revocation Date	Last Observed in CRL	Last Checked (Error)
OCSP	The CA	Check	?	n/a	?
CRL	The CA	Not Revoked	n/a	n/a	2019-12-04 19:11:39 UTC
CRLSet/Blacklist	Google	Not Revoked	n/a	n/a	n/a
disallowedcert.stl	Microsoft	Not Revoked	n/a	n/a	n/a
OneCRL	Mozilla	Not Revoked	n/a	n/a	n/a

SHA-256(Certificate)	D16CBE33280ADCF907FBAE43A1BF6A822D373FD57A5260DC5709EC65C420E1E6
SHA-1(Certificate)	50D24D5CAC8DC0DA99853831FF4288A45885C5F3

Ilustración 1 Certificado Utilizado en Url del sitio fraudulento que imita al SII

IP

45[.]58[.]121[.]194

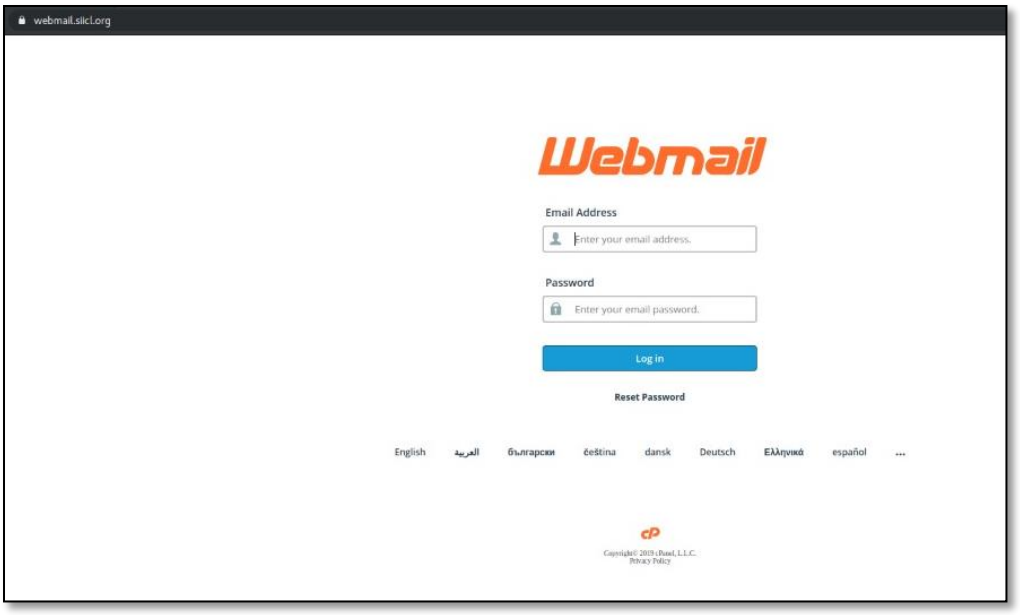
IP Address	45.58.121.194 - 367 other sites hosted on this server
IP Location	- Florida - Miami - Greg Ricks
ASN	AS23470 RELIABLESITE - ReliableSite.Net LLC, US (registered Aug 10, 2018)
Domain Status	Registered And Active Website
IP History	1 change on 1 unique IP addresses over 0 years
Hosting History	1 change on 2 unique name servers over 0 year
Website	
Website Title	SII | Servicio de Impuestos Internos
Server Type	LiteSpeed
Response Code	200

Ilustración 2 Ip de Origen donde se aloja Sitio Falso del SII

Localización

Miami, Florida, Estados Unidos

Imagen del sitio



Whois

```
Domain Name: SIICL.ORG
Registry Domain ID: D402200000011755683-LROR
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: www.namesilo.com
Updated Date: 2019-10-28T17:38:00Z
Creation Date: 2019-10-28T17:38:00Z
Registry Expiry Date: 2020-10-28T17:38:00Z
Registrar Registration Expiration Date:
Registrar: Namesilo, LLC
Registrar IANA ID: 1479
Registrar Abuse Contact Email: abuse@namesilo.com
Registrar Abuse Contact Phone: +1.4805240066
Reseller:
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Registrant Organization:
Registrant State/Province: Region Metropolitana
Registrant Country: CL
Name Server: NS1.QHOSTER.NET
Name Server: NS2.QHOSTER.NET
Name Server: NS3.QHOSTER.NET
Name Server: NS4.QHOSTER.NET
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form https://www.icann.org/wicf/)
>>> Last update of WHOIS database: 2019-12-09T22:21:29Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

Access to Public Interest Registry WHOIS information is provided to assist persons in determining the contents of a domain n
ame registration record in the Public Interest Registry registry database. The data in this record is provided by Public Int
erest Registry for informational purposes only, and Public Interest Registry does not guarantee its accuracy. This service i
s intended only for query-based access. You agree that you will use this data only for lawful purposes and that, under no ci
rcumstances will you use this data to (a) allow, enable, or otherwise support the transmission by e-mail, telephone, or facs
imile of mass unsolicited, commercial advertising or solicitations to entities other than the data recipient's own existing
customers; or (b) enable high volume, automated, electronic processes that send queries or data to the systems of Registry O
perator, a Registrar, or Afilias except as reasonably necessary to register domain names or modify existing registrations. A
ll rights reserved. Public Interest Registry reserves the right to modify these terms at any time. By submitting this query,
 you agree to abide by this policy.

The Registrar of Record identified in this output may have an RDDS service that can be queried for additional information on
 how to contact the Registrant, Admin, or Tech contact of the queried domain name.
```

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: 2019.12.09 19:46:34 -03'00'