| | |
|---|---|
| Alerta de seguridad cibernética | 8FFR20-00344-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 17 de abril de 2020 |
| Última revisión | 17 de abril de 2020 |

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 un portal fraudulento asociado a una IP que suplanta el sitio web oficial de Banco Scotiabank , 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 COMPROMISO

URL
scotiaenlineapersonas[.]scotil[.]com

IP
108[.]179[.]232[.]162

# DOMINIOS DONDE SE ALOJA URL

**Domain scotil.com**

scotil / com / Subdomains

| record type | TTL | value | | |
|---|---|---|---|---|
| A | 3600 | 108.179.232.162 | | |
| NS | 3600 | ns-uk.topdns.com | Zones on DNS server | 77.247.183.137, 108.61.150.91 |
| NS | 3600 | ns-usa.topdns.com | Zones on DNS server | 85.159.232.241, 108.61.12.163, 46.166.189.99 |
| NS | 3600 | ns-canada.topdns.com | Zones on DNS server | 109.201.142.225 |
| SOA | 7200 | Mname | ns-canada.topdns.com | |
| | | Rname | hostmaster.topdns.com | |
| | | Serial number | 2020041603 | |
| | | Refresh | 14400 | |
| | | Retry | 7200 | |
| | | Expire | 950400 | |
| | | Minimum TTL | 7200 | |

# CERTIFICADOS

| | |
|---|---|
| Subject DN | CN=scotiaenlineapersonas.scotil.com |
| Issuer DN | C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3 |
| Serial | 334989589205378944520980555153182687954821 |
| Validity | 2020-04-16 06:35:27 to 2020-07-15 06:35:27 (90 days, 0:00:00) |
| Names | scotiaenlineapersonas.scotil.com |

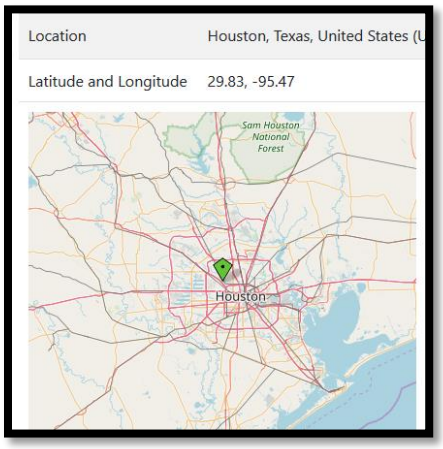
# IP DE ORIGEN DONDE SE ALOJA SITIO

**Domain scotiaenlineapersonas.scotil.com is located on IP address << 108.179.232.162 >>**

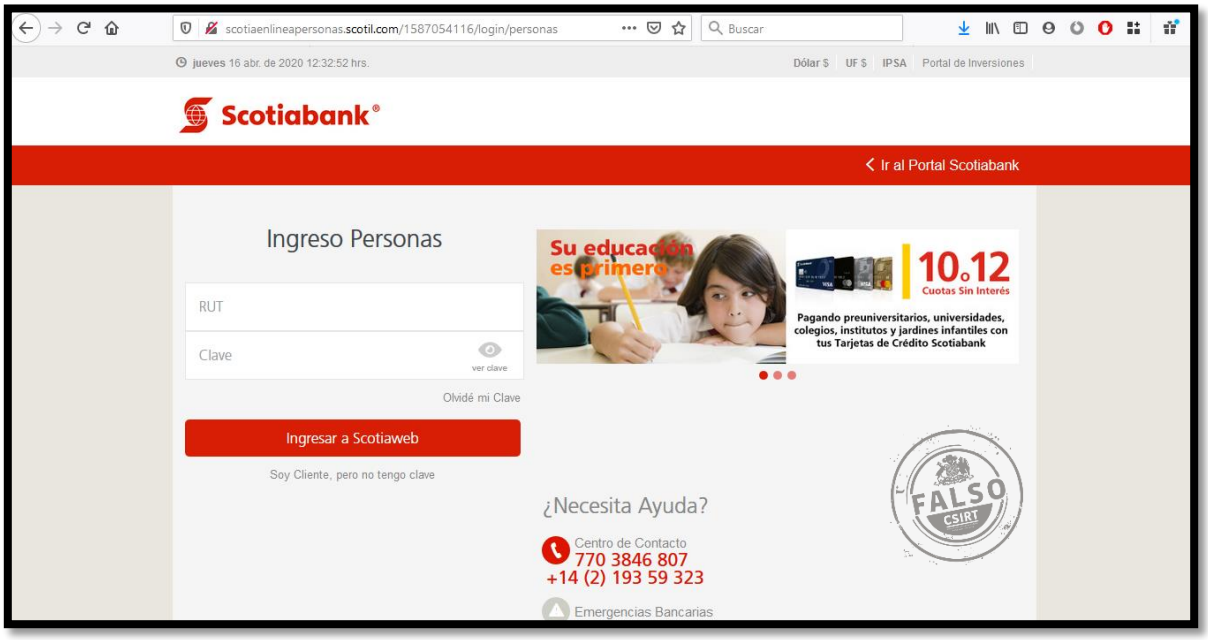
| | |
|---|---|
| **Block start** | 108.179.192.0 |
| **End of block** | 108.179.255.255 |
| **Block size** | 16384 Domains in block |
| **Block name** | HGBLOCK-5 |
| **AS number** | 46606 |
| **Parent block** | 108.0.0.0 - 108.255.255.255 |
| **Organization** | WEBSITEWELCOME.COM |

# LOCALIZACIÓN

Houston, Texas, Estados Unidos



# IMAGEN DEL SITIO



# WHOIS

```
Domain Name: SCOTIL.COM
Registry Domain ID:
Registrar WHOIS Server: whois.internet.bs
Registrar URL: http://www.internetbs.net
Updated Date: 2019-09-26T15:14:56Z
Creation Date: 2019-09-25T23:23:46Z
Registrar Registration Expiration Date: 2020-09-25T23:23:46Z
Registrar: Internet Domain Service BS Corp.
Registrar IANA ID: 2487
Registrar Abuse Contact Email: abuse@internet.bs
Registrar Abuse Contact Phone: +1.5167401179
Reseller:
Domain Status: ok - http://www.icann.org/epp#ok
Domain Status: clientTransferProhibited - http://www.icann.org/epp#clientTransfe
rProhibited
Registry Registrant ID:
Registrant Name: Not disclosed Not disclosed
Registrant Organization:
Registrant Street: Not disclosed, Not disclosed, Not disclosed
Registrant City: Not disclosed
Registrant State/Province: lima
Registrant Postal Code: 00000
Registrant Country: PE
Registrant Phone: +1.5163872248
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: 2e088834d6aefba09f6f55cd066d5850.gdrp@customers.whoisprivacyco
rp.com
Registry Admin ID:
Admin Name: Not disclosed Not disclosed
Admin Organization:
Admin Street: Not disclosed, Not disclosed, Not disclosed
Admin City: Not disclosed
Admin State/Province: lima
Admin Postal Code: 00000
Admin Country: PE
Admin Phone: +1.5163872248
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: 2e088834d6aefba09f6f55cd066d5850.gdrp@customers.whoisprivacycorp.co
m
Registry Tech ID:
Tech Name: Not disclosed Not disclosed
```

# 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: 2020.04.17 06:53:23 -04'00'