| | |
|---|---|
| **Alerta de seguridad informática** | 8FPH-00073-001 |
| **Clase de alerta** | Fraude |
| **Tipo de incidente** | Phishing |
| **Nivel de riesgo** | Alto |
| **TLP** | Blanco |
| **Fecha de lanzamiento original** | 12 de Noviembre de 2019 |
| **Última revisión** | 12 de Noviembre 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.

## Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de phishing a través de un correo electrónico cuyo mensaje intenta engañar a los usuarios del Banco Scotiabank.

El correo informa a los clientes que, producto de la fusión de los bancos Scotiabank y BBVA, es necesario actualizar la cuenta en un período máximo de 24 horas, de lo contrario, esta sería bloqueada.

Los estafadores disponibilizan un enlace para actualizar la cuenta, exponiendo a los usuarios al robo de sus credenciales desde un sitio semejante al de Scotiabank

**Observación**

Solicitamos tener en consideración las señales de compromiso en su conjunto

**Indicadores de compromisos**

**Url's:**

https[:]//www[.]scotiaseguridad[.]site/site/choose-type[.]php

https[:]//www[.]scotiaseguridad[.]site/site/persona/acesso[.]php

https[:]//www[.]scotiaseguridad[.]site/site/empresa/acesso[.]php

http[:]//wwwdisc[.]chimica.unipd[.]it/dechem/-/https:/www.scotiabank[.]cl

**Sender**

root@webmasterfox01[.]webgulafox.com[.]br
root@webmasterfox02[.]webgulafox.com[.]br
root@webmasterfox03[.]webgulafox.com[.]br
root@webmasterfox04[.]webgulafox.com[.]br
root@webmasterfox06[.]webgulafox.com[.]br
root@webmasterfox08[.]webgulafox.com[.]b
root@webmasterfox09[.]webgulafox.com[.]br
root@webmasterfox10[.]webgulafox.com[.]br
root@server08[.]webmasterfox[.]com[.]br
root@server05[.]webmasterfox[.]com[.]br

**Smtp Host**

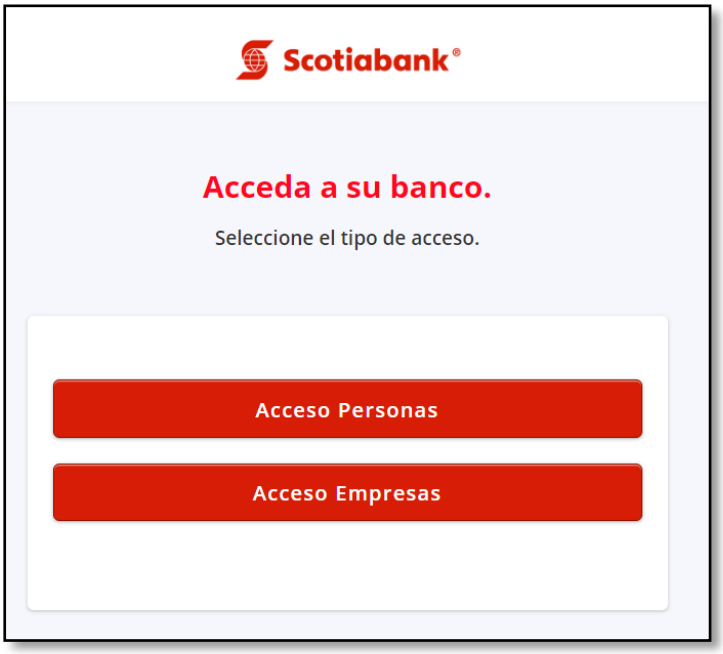
| | |
|---|---|
| li2040-55.members[.]linode[.]com | [172.105.79.55] |
| li2040-62.members[.]linode[.]com | [172.105.79.62] |
| li2038-205.members[.]linode[.]com | [172.105.77.205] |
| li2037-61.members[.]linode[.]com | [172.105.76.61] |
| li2040-163.members[.]linode[.]com | [172.105.79.163] |
| li2050-74.members[.]linode[.]com | [172.105.89.74] |
| li2024-98.members[.]linode[.]com | [172.105.68.98] |
| li2044-150.members[.]linode[.]com | [172.105.83.150] |
| li1957-217.members[.]linode[.]com | [172.105.3.217] |
| li1968-11.members[.]linode[.]com | [172.105.13.11] |

**Subject:**

Debido a la unificacion del banco Scotiabank con BBVA Bank, sera necesario realizar una autenticacion de seguridad

**Imagen Phishing Correo**


**Imagen Sitio Web**



**Recomendaciones**

- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras)
- 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 que sean los oficiales

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.11.12 20:08:20 -03'00'