| | |
|---|---|
| Alerta de seguridad informática | 8FPH20-00128-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 09 de Marzo de 2020 |
| Última revisión | 09 de Marzo 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 phishing 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 phishing, 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 una campaña de phishing a través de un correo electrónico supuestamente proveniente de Office Banking.

El mensaje informa que el banco le da la oportunidad de refinanciar las deudas con un crédito de consumo preaprobado con un cupo de hasta 9.440.000 pesos. Bajo ese argumento, el atacante intenta persuadir a la víctima de acceder a un enlace que se adjunta en el cuerpo del correo.

Al seleccionar el vínculo, la víctima es dirigida a un sitio semejante al del banco donde se expone al robo de sus credenciales.

## Observación
Solicitamos tener en consideración las señales de compromiso en su conjunto.

## Indicadores de compromisos

### Urls Redirecciones:
https://ajodl[.]oum[.]edu[.]my/wp-content/Office-Bankk/Aprobacion-online/cl/index[.]php

### Urls sitio falso:
https://www-portal-personas-office-clientes-chile-net[.]000webhostapp[.]com/logs-portal-office-bank/aprobado-creditos

### Sender
www-data@asee[.]org
apache@vps.cssup[.]in

### Smtp Host
[216.185.13.254]
[103.93.16.169]

### Subject
Pide tu Tarjeta de Crédito Preaprobada con Avance Diferido en Cuotas sin Intereses en CuentaRUT, Chequera electrónica o Cuenta Corriente ID #

### Imagen del correo

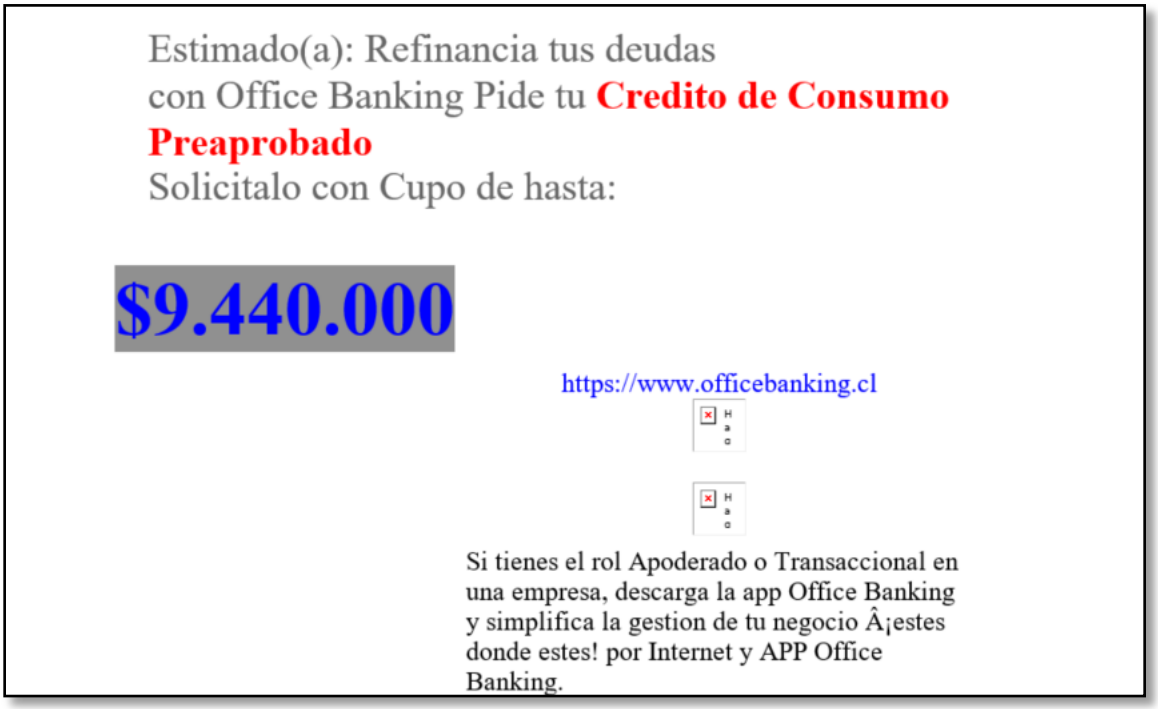
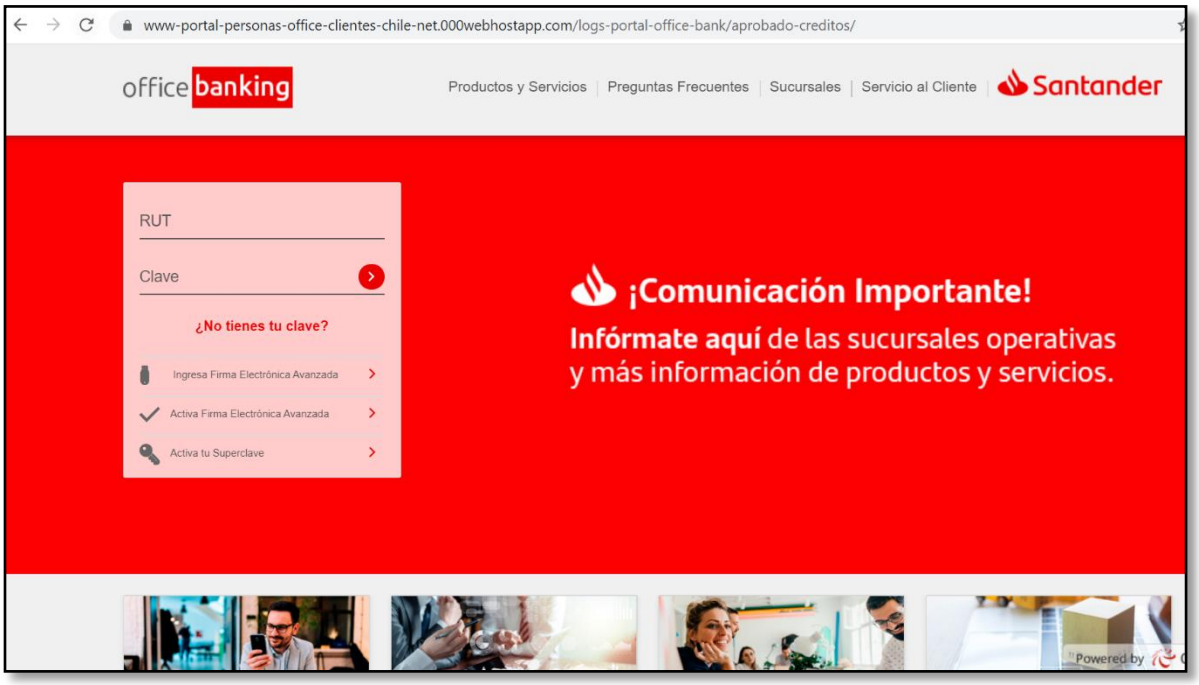


Imagen Sitio Web




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: 2020.03.09 18:00:20 -03'00'