

|                                 |  |
|---------------------------------|--|
| Alerta de seguridad cibernética | 8FFR21-00901-01                        |
| Clase de alerta                 | Fraude                                 |
| Tipo de incidente               | Falsificación de Registros o Identidad |
| Nivel de riesgo                 | Alto                                   |
| TLP                             | Blanco                                 |
| Fecha de lanzamiento original   | 19 de Febrero de 2021                  |
| Última revisión                 | 19 de Febrero de 2021                  |

## 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 una página fraudulenta en dominio chileno que intenta suplantar a la plataforma OneDrive, el que podría servir para robar credenciales de usuarios.

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

## Indicadores de compromiso

### URL sitio falso

[https://www.nbpropiedades\[.\]cl/document73839827722/proposal73682732/](https://www.nbpropiedades[.]cl/document73839827722/proposal73682732/)

### Certificado Digital

|               |                  |
|---------------|------------------|
| Fecha Válido  | 15-02-2021       |
| Fecha Término | 16-05-2021       |
| Emitido       | Let's Encrypt R3 |

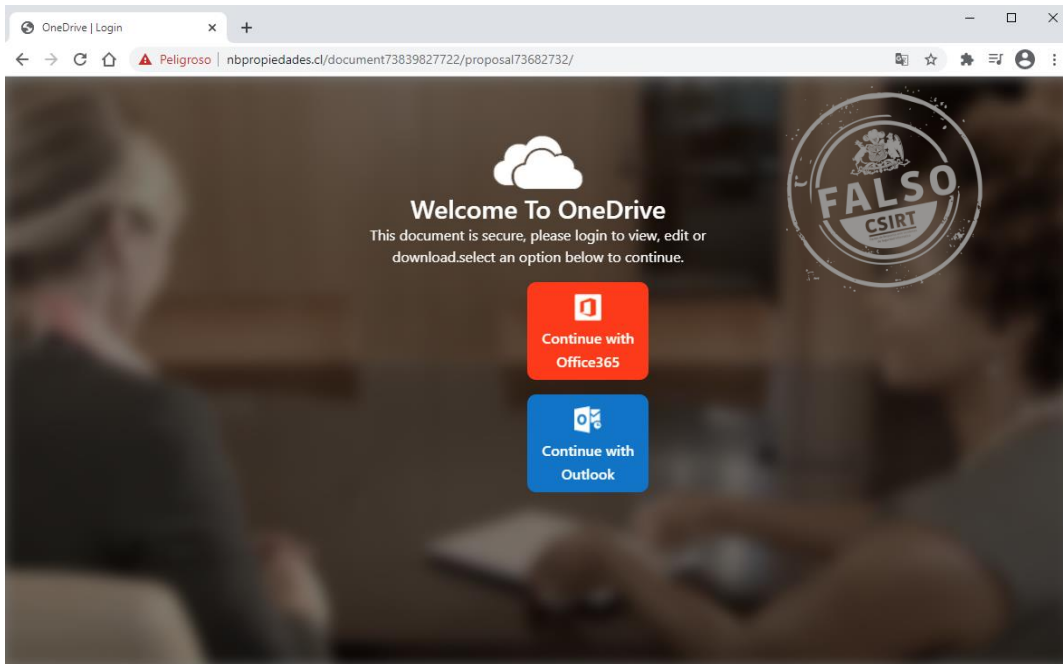
### Datos Alojamiento

|                                 |                  |
|---------------------------------|------------------|
| IP                              | [66.232.107.218] |
| Número de Sistema Autónomo (AS) | 29802            |
| Etiqueta del Sistema Autónomo   | HVC-AS           |
| País                            | CL               |
| Registrador                     | Lacnic           |

### Datos del Dominio

|                             |                                  |
|-----------------------------|----------------------------------|
| Nombre de Dominio           | nbpropiedades[.]cl               |
| Creado                      | 25-10-2019                       |
| Expira                      | 25-10-2021                       |
| Información del Registrador | Nic Chile                        |
| ID IANA                     |                                  |
| Correo Electrónico          | abuse@nic.cl                     |
| Name Server                 | ns2.secuela.cl<br>ns2.secuela.cl |

## Imagen del sitio



## Recomendaciones

- No abrir correos ni mensajes de dudosa procedencia.
- Desconfiar de los enlaces y archivos en los mensajes o correo.
- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).
- Ser escépticos frente ofertas, promociones o premios increíbles que se ofrecen por internet.
- Prestar atención en los detalles de los mensajes o redes sociales.
- 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 sean los oficiales.