

Alerta de seguridad cibernética	8FFR20-00805-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de Octubre de 2020
Última revisión	20 de Octubre 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 loC 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 loC 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 pagina fraudulentas asociadas a un dominio que suplanta el sitio oficial de Microsoft, 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

http[:]//jmcnoack[.]cl/C/d23e2b5f89fe170f3521f59aff87694d/off.php

### Body SHA-256

f1945cd6c19e56b3c1c78943ef5ec18116907a4ca1efc40a57d48ab1db7adfc5

### Certificado Digital

Fecha Válido No Aplica

Fecha Término No Aplica

Emitido No Aplica

### Datos Alojamiento

IP 99.198.121.101

Número de Sistema Autónomo (AS) 32475

Etiqueta del Sistema Autónomo SingleHop LLC

País US

Registrador ARIN

### Datos del Dominio

Nombre de Dominio jmcnoack[.]cl

Creado 20-08-2020

Expira 20-09-2021

Información del Registrador Nic Chile

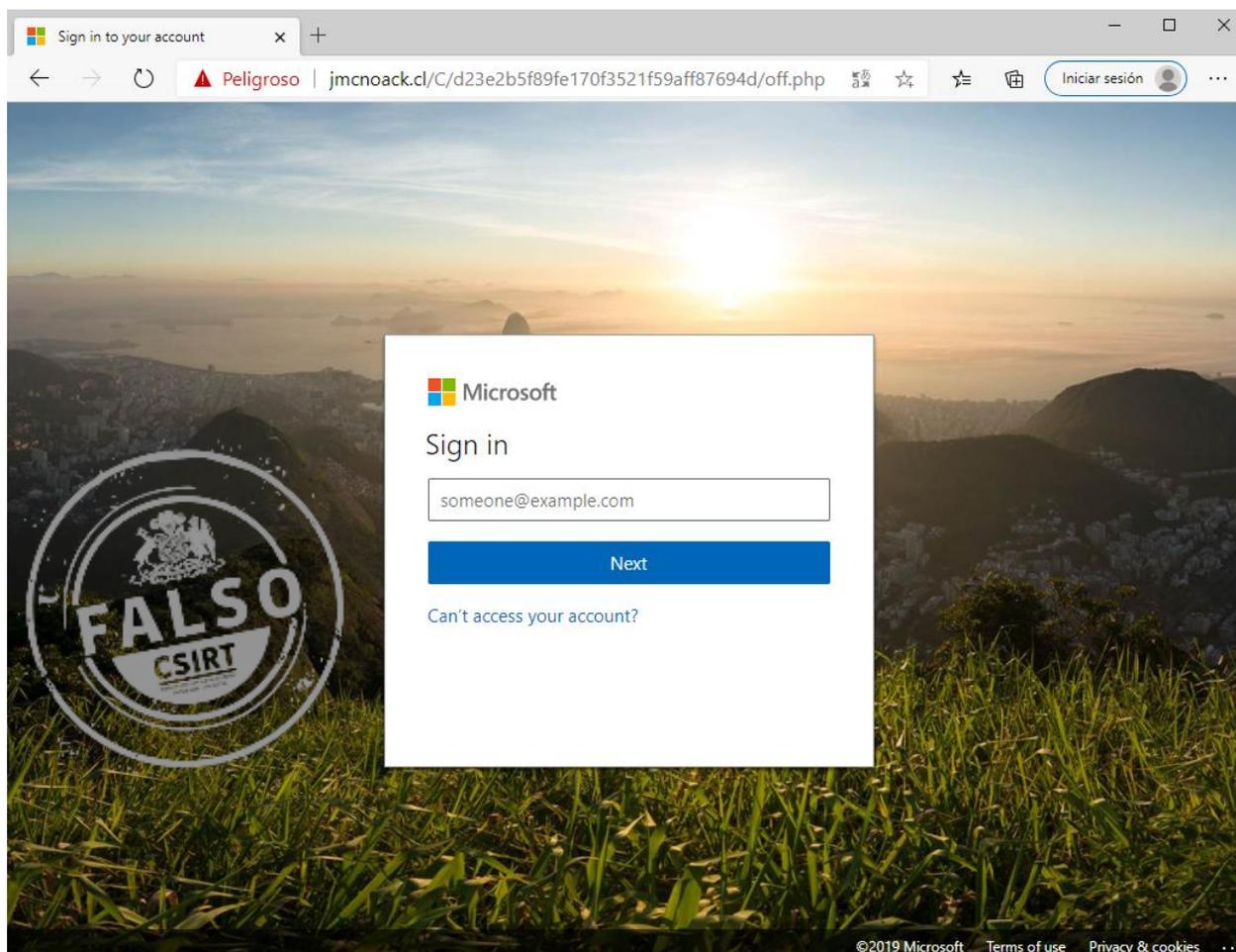
ID IANA No disponible

Correo Electrónico No disponible

Name Server ns1.msistemas.cl

ns2.msistemas.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.