| | |
|---|---|
| Alerta de seguridad cibernética | 8FFR22-01105-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 29 de septiembre de 2022 |
| Última revisión | 29 de septiembre de 2022 |

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigación propia del CSIRT de Gobierno. 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 del Gobierno de Chile (CSIRT de Gobierno) ha identificado la activación de una pagina fraudulenta que suplanta a un sitio de login de Microsoft.

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://maderasgsm[.]cl/hhh/wp-files/index.html?websrc=xFioJ1dnB9H3Efwx1M6UOx95WsEMhkr6f0lYJAOurCuS7wjEVRKc0BWKapKBAkl8SCPRKvlOvrPgRBR1sq672IfLCdeyV2YTSQLnuURjxhSZhDDOkJ4s0N0jlrRNIP65yNhh4RzhJhH0CPX9XoWBSoWaCzP3VGd7HFsg9h7N5rEuEpbwhhkvcwEEHwJfk5NYNj7g9HEir8sHeI1jrdRWpTnPm0qobsmeseksGHbNaw3Onvcs9yuNl0Z5LrzZYg7wxYSJpKH2kguVZ6ssIVk9Io2hz6sFYlLyjgYOlooVIHxWW1&dispatch=594&id=417055 |

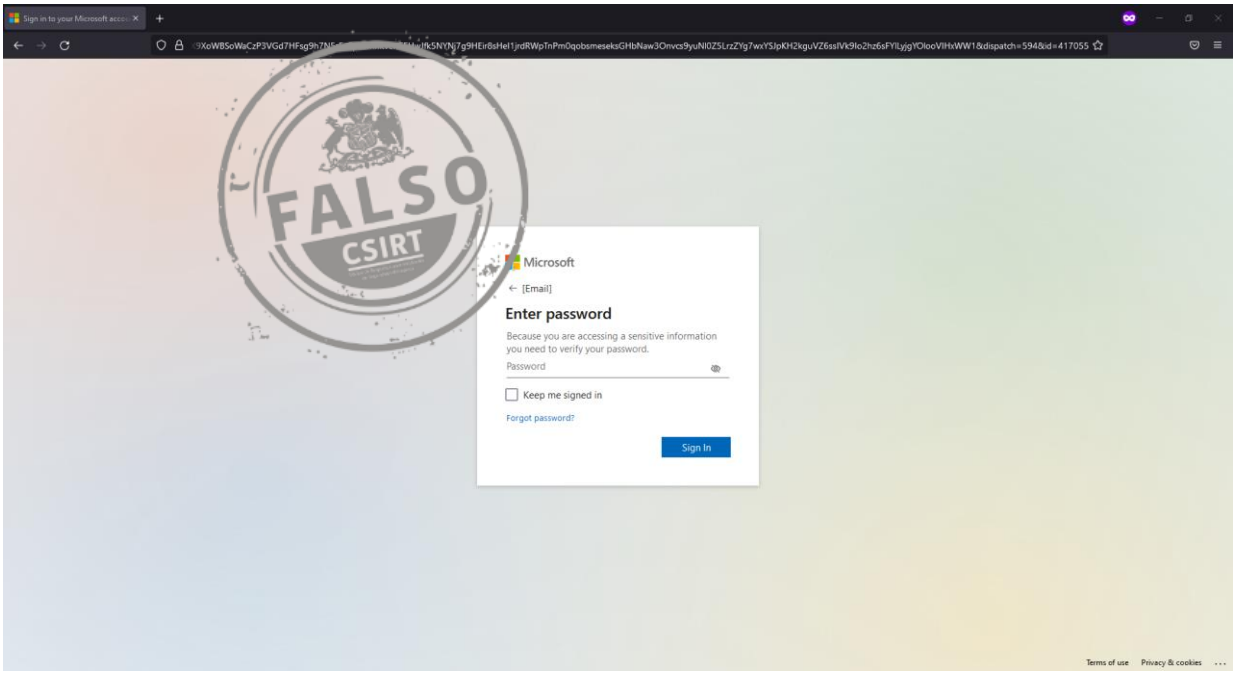
## Certificado Digital

| | |
|---|---|
| Fecha Válido | 12-08-2022 |
| Fecha Término | 10-11-2022 |
| Emitido | cPanel, Inc |

## Datos Alojamiento

| | |
|---|---|
| IP | [186.64.117.145] |
| Número de Sistema Autónomo (AS) IP | 52368 |
| Etiqueta del Sistema Autónomo IP | ZAM LTDA. |
| Registrador IP | LACNIC |
| País IP | CL |
| Dominio | maderasgsm.cl |
| Registrador Dominio | https://www.nic.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.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.09.29 17:14:09 -03'00'