

Alerta de seguridad cibernética	8FFR20-00826-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de Noviembre de 2020
Última revisión	13 de Noviembre 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 fraudulenta asociada a un dominio .com que intenta suplantar al sitio de PayPal, 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://glassfilm\[.\]cl/wp-admin/webapp/update/](https://glassfilm[.]cl/wp-admin/webapp/update/)

### Body SHA-256

dad77b4e03da0b316a68760e47d7fa73d38b6aee78c004fbf5cb41b5a5d83ebf

### Certificado Digital

Fecha Válido	30/10/2020
Fecha Término	29/01/2020
Emitido	cPanel, Inc. Certification Authority

### Datos Alojamiento

IP	190[.]107[.]177[.]239
Número de Sistema Autónomo (AS)	265831
Etiqueta del Sistema Autónomo	SOC. COMERCIAL WIRENET CHILE LTDA.
País	CL
Registrador	LACNIC

### Datos del Dominio

Nombre de Dominio	GlassFilm[.]cl
Creado	14/01/2014
Expira	14/01/2022
Información del Registrador	No disponible
ID IANA	No disponible
Correo Electrónico	No disponible
Name Server	NS1.CPANELHOST.CL NS2.CPANELHOST.CL



## Login to your account

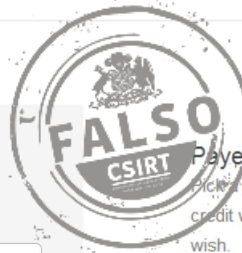
Email address

Password

Login

[Forgot your email address or password?](#)

[Open a free account](#)



### Payment All-in-one.

Pick a card, any, or a bank account or apply for a line of credit with our service. You spend your money as you wish.

### Simple. And usually free.

You can open a free PayPal account and choose your method of payment: you pay no commission on transactions when you make purchases.

## 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.