Alerta de seguridad cibernética	8FFR21-00940-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de Abril de 2021
Última revisión	28 de Abril 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 de Gobierno), ha identificado la activación de una pagina fraudulenta que intenta suplantar a varias plataformas de correo, como Office365, Gmail, Hotmail, y Yahoo, lo que podría servir para robar credenciales de usuarios.

Lo anterior constituye una falsificación de las marcas institucionales que podría afectar a usuarios, clientes y a las entidades aludidas.

Indicadores de compromiso

URL sitio falso

https://smconecta[.]cl/ap/Login.php?sslchannel=true

Certificado Digital

Fecha Válido	16-04-2021
Fecha Término	16-07-2021
Emitido	cPanle, Inc. Certification Authority

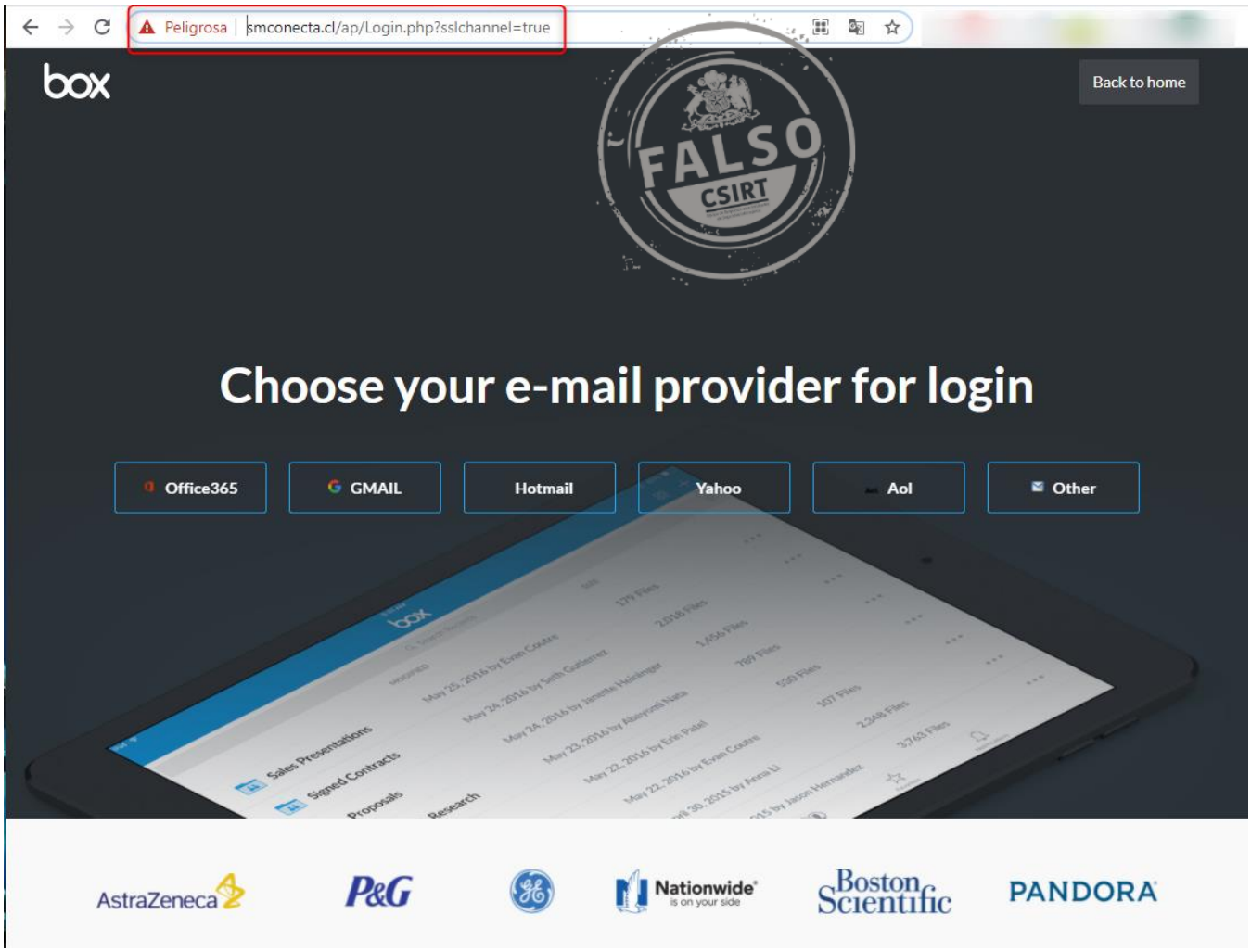
Datos Alojamiento

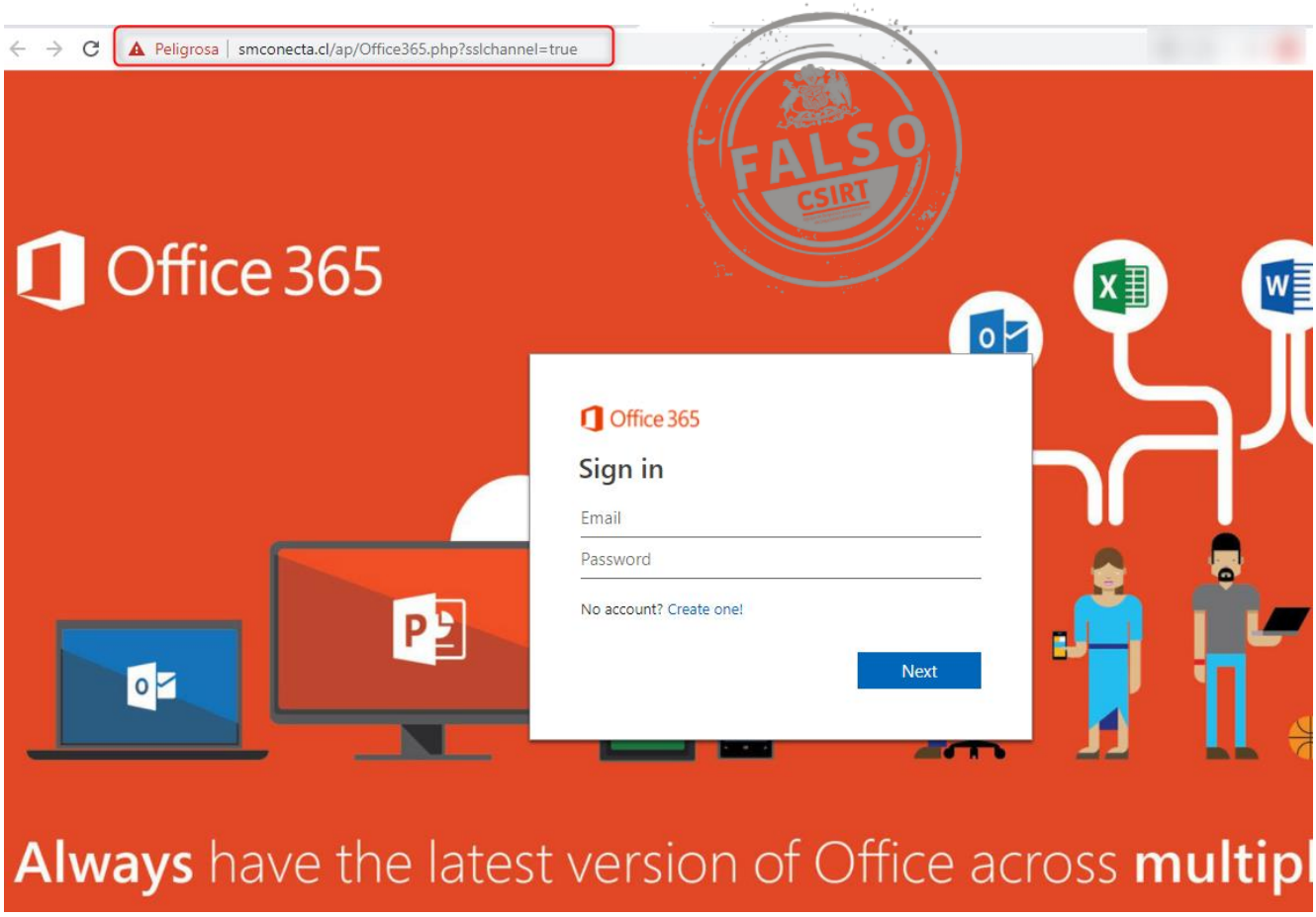
IP	[18.222.62.89]
Número de Sistema Autónomo (AS)	16509
Etiqueta del Sistema Autónomo	AMAZON-02
País	US
Registrador	ARIN

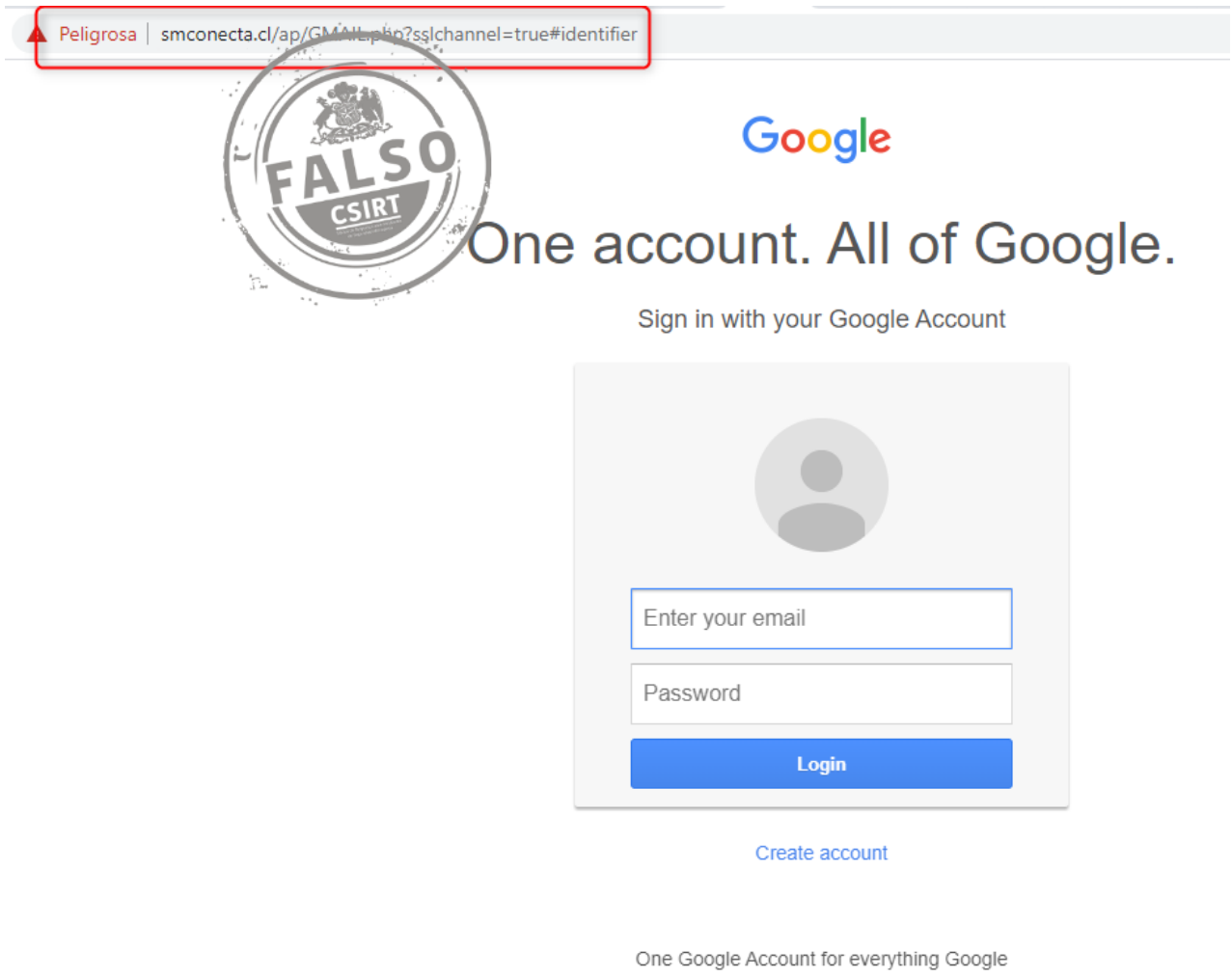
Datos del Dominio

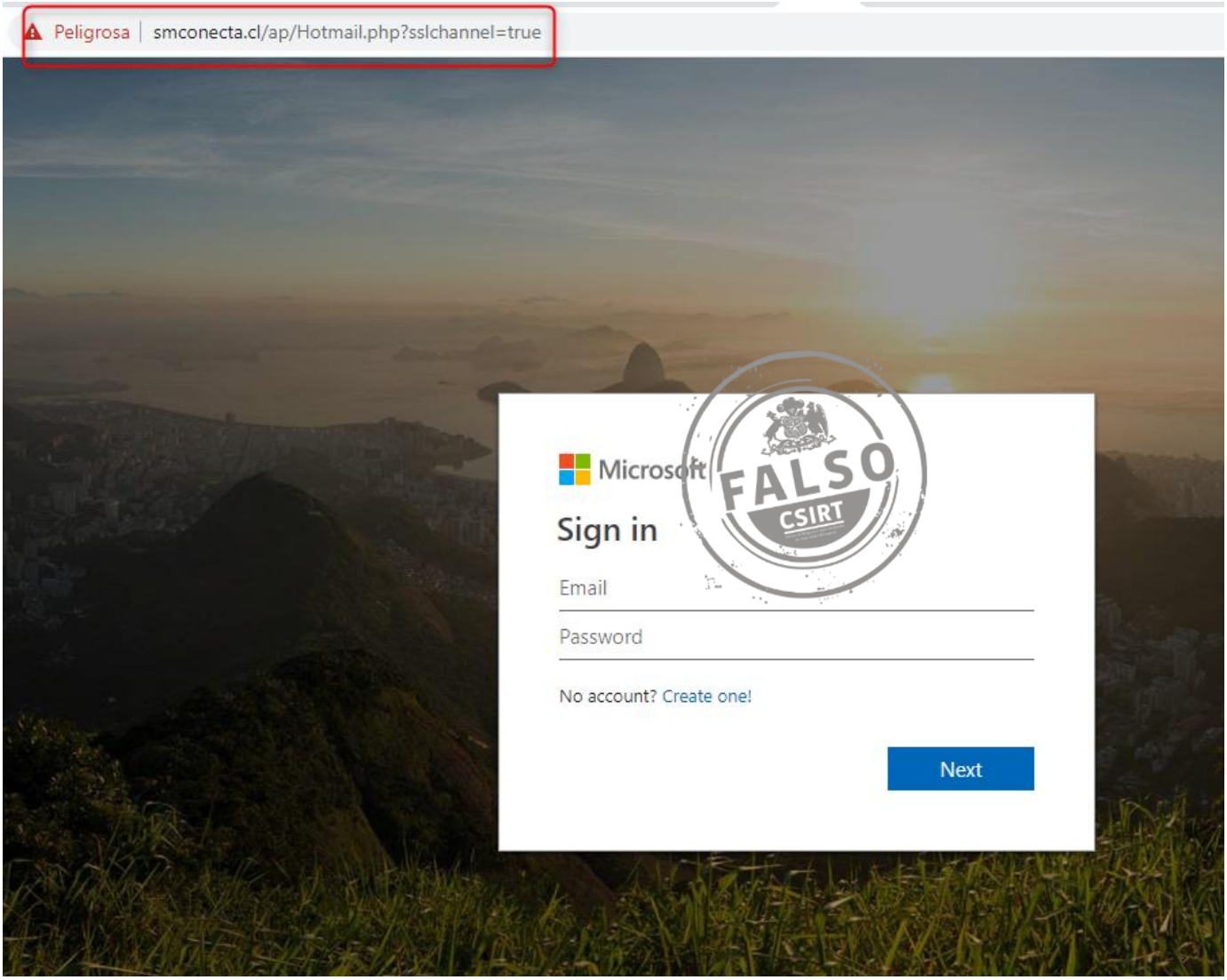
Nombre de Dominio	Smconecta[.]cl
Creado	22-08-2013
Expira	22-09-2021
Información del Registrador	NIC Chile
ID IANA	NO APLICA
Correo Electrónico	NO APLICA
Name Server	ns-1392.awsdns-46.org ns-1774.awsdns-29.co.uk ns-36.awsdns-04.com ns-901.awsdns-48.net

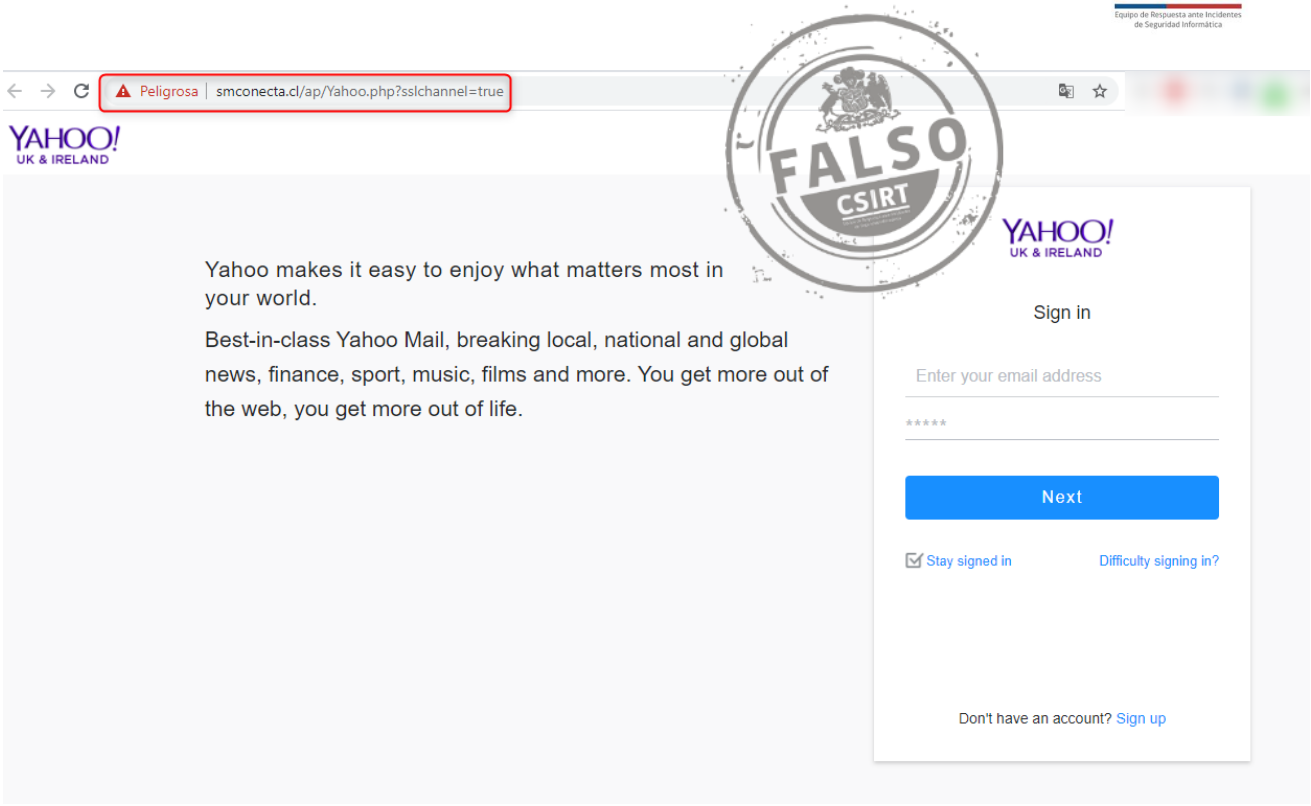
Imagen del sitio




Peligrosa | smconecta.cl/ap/Office365.php?sslchannel=true
FALSO
CSIRT
Office 365
Office 365
Sign in
Email
Password
No account? Create one!
Next
Always have the latest version of Office across multipl


Peligrosa | smconecta.cl/ap/GMAIL.php?sslchannel=true#identifier
FALSO
CSIRT
Google
One account. All of Google.
Sign in with your Google Account
Enter your email
Password
Login
Create account
One Google Account for everything Google


Peligrosa | smconecta.cl/ap/Hotmail.php?sslchannel=true
Microsoft
Sign in
Email
Password
No account? Create one!
Next
FALSO
CSIRT


Peligrosa | smconecta.cl/ap/Yahoo.php?sslchannel=true
YAHOO!
UK & IRELAND
FALSO
CSIRT
Yahoo makes it easy to enjoy what matters most in your world.
Best-in-class Yahoo Mail, breaking local, national and global news, finance, sport, music, films and more. You get more out of the web, you get more out of life.
YAHOO!
UK & IRELAND
Sign in
Enter your email address
*****
Next
Stay signed in
Difficulty signing in?
Don't have an account? Sign up

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: 2021.04.28 10:36:21 -04'00'