Alerta de seguridad informática	8FPH22-00533-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de mayo de 2022
Última revisión	30 de mayo 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 phishing 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 phishing, 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 una campaña de phishing vía correo electrónico que proviene, supuestamente, de CorreosChile. En esta campaña, los delincuentes indican falsamente a la víctima que su envío aún está esperando su validación. Para confirmar el pago del envío, el atacante dispone de un enlace. Al ingresar, la persona es dirigida a un sitio falso, semejante al de CorreosChile, donde se expone al robo de sus datos bancarios.

Observación

Solicitamos tener en consideración las señales de compromiso en su conjunto.

Indicadores de compromiso

Sitio falso:
http://cmi.versatecnologia.com[.]br/js/CELLO/index/

Asunto:
Paquete pendiente de entrega

Correo de salida:
enquiry@gdigitalindia[.]com

SMTP Host:
[101.53.144.229]

Otros antecedentes

Certificado Digital

Fecha Válido	:	NO APLICA
Fecha Término	:	NO APLICA
Emitido	:	NO APLICA

Datos Alojamiento y Dominio

IP	:	[104.131.88.122]
Número de sistema autónomo (AS) IP	:	14061
Etiqueta del sistema autónomo IP	:	DIGITALOCEAN-ASN
Registrador IP	:	ARIN
País IP	:	US
Dominio	:	versatecnologia.com[.]br
Registrador Dominio	:	GLSCO44

Imagen del mensaje

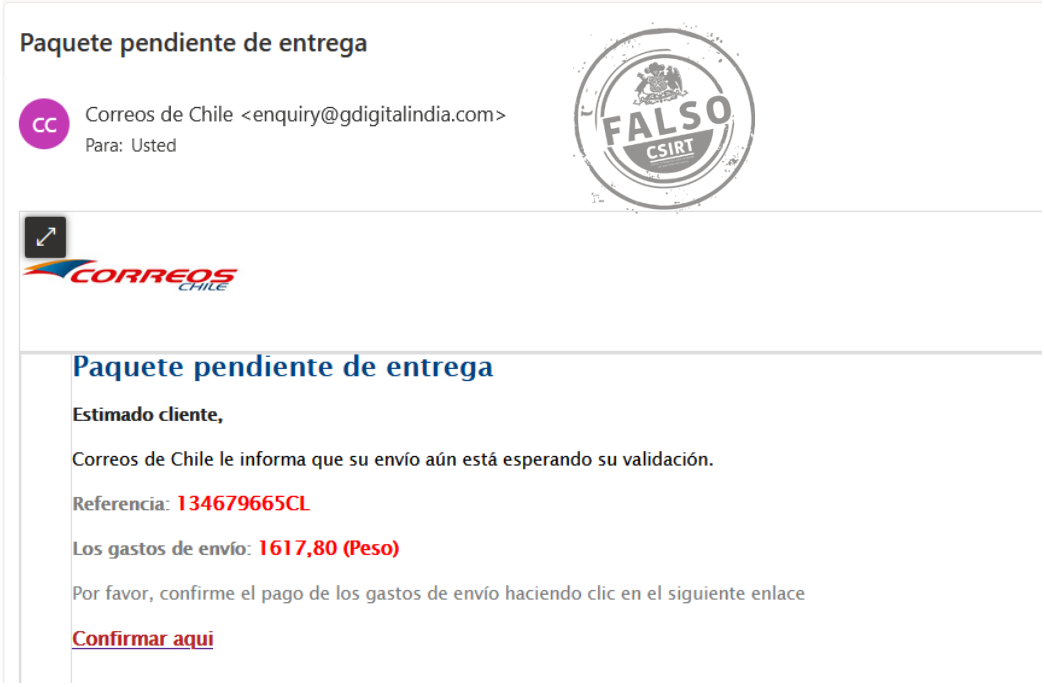
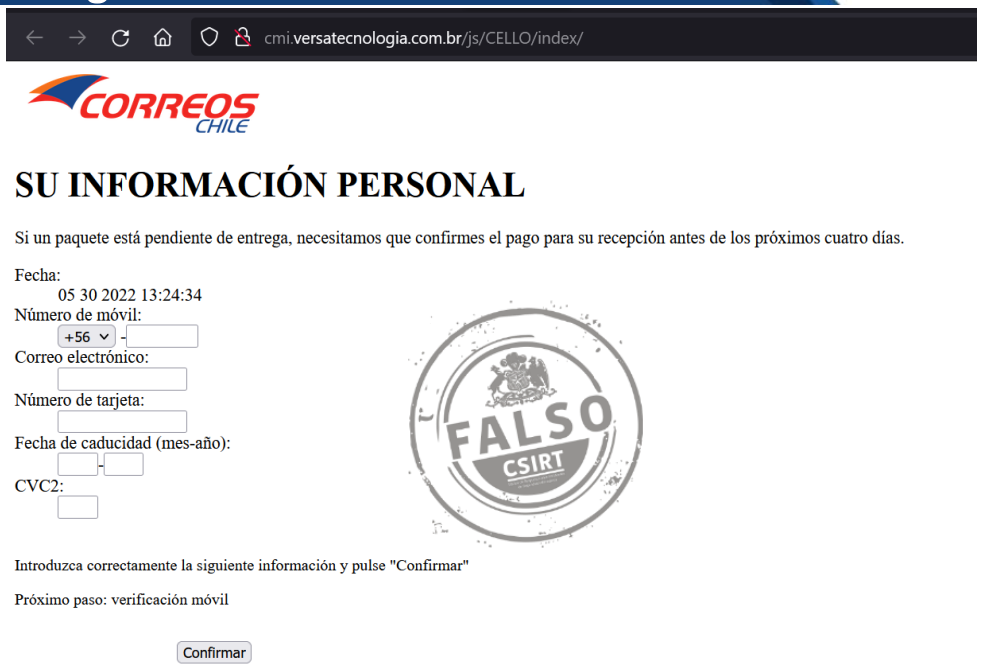


Imagen del sitio



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: 2022.05.30 14:07:37 -04'00'