Alerta de seguridad informática	8FPH22-00566-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de julio de 2022
Última revisión	26 de julio de 2022

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 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, del WEB Admin. En esta campaña, los delincuentes indican falsamente a la víctima que la cuenta de correo electrónico se actualizará a una nueva interfaz de usuario web mejorada. El atacante disponibiliza un enlace para que se realice el cambio. Al ingresar, la persona es dirigida a un sitio falso, semejante a una interfaz de correo, donde se expone al robo de su usuario y contraseña (credenciales).

Observación

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

Indicadores de compromiso

Urls sitio falso:
https://webmenimastesa.wapka.co/

Asunto:
Aviso de seguridad

Correo de salida:
regionaloccidente@dinaf.gob[.]hn

SMTP Host:
[181.210.30.114]

Otros antecedentes

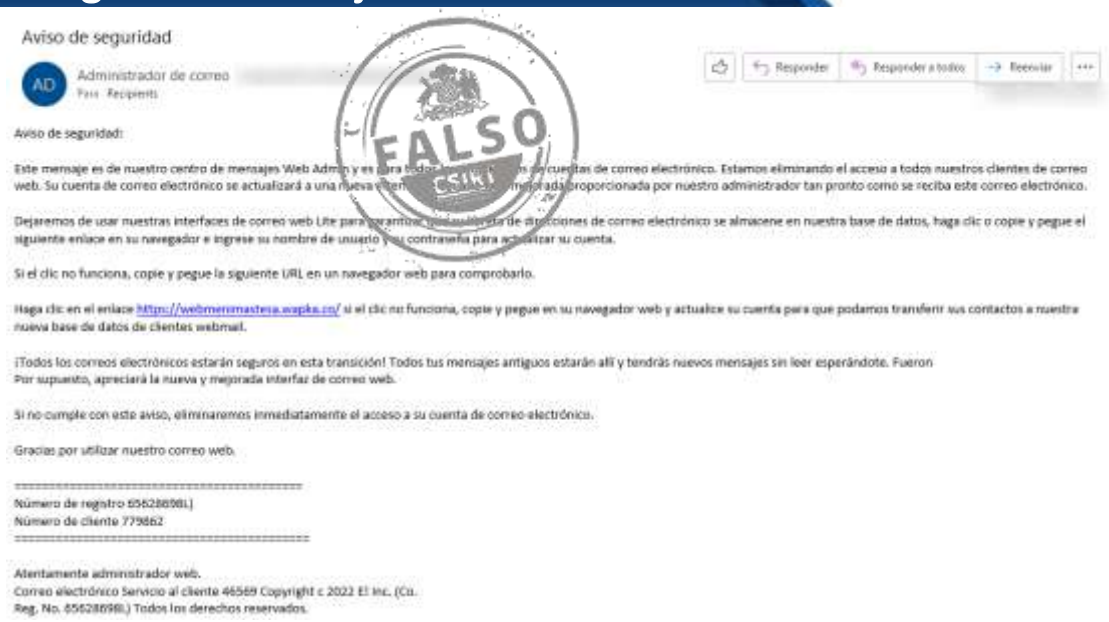
Certificado Digital

Fecha Válido	:	18-03-2022
Fecha Término	:	19-03-2022
Emitido	:	Cloudflare Inc ECC CA-3

Datos Alojamiento y Dominio

IP	:	[104.21.18.179]
Número de sistema autónomo (AS) IP	:	13335
Etiqueta del sistema autónomo IP	:	CLOUDFLARENET
Registrador IP	:	ARIN
País IP	:	US
Dominio	:	wapka[.]co
Registrador Dominio	:	NAMECHEAP INC

Imagen del mensaje



Aviso de seguridad

AD Administrador de correo
Para Recipients

Responder | Responder a todos | Reenviar | ...

Aviso de seguridad:

Este mensaje es de nuestro centro de mensajes Web Admin y es para todos los usuarios de cuentas de correo electrónico. Estamos eliminando el acceso a todos nuestros clientes de correo web. Su cuenta de correo electrónico se actualizará a una nueva versión mejorada proporcionada por nuestro administrador tan pronto como se reciba este correo electrónico.

Dejaremos de usar nuestras interfaces de correo web Lite para garantizar que nuestra lista de direcciones de correo electrónico se almacene en nuestra base de datos, haga clic o copie y pegue el siguiente enlace en su navegador e ingrese su nombre de usuario y su contraseña para actualizar su cuenta.

Si el clic no funciona, copie y pegue la siguiente URL en un navegador web para comprobarlo.

Haga clic en el enlace https://webmenmasteva.wapka.co/ si el clic no funciona, copie y pegue en su navegador web y actualice su cuenta para que podamos transferir sus contactos a nuestra nueva base de datos de clientes webmail.

¡Todos los correos electrónicos estarán seguros en esta transición! Todos tus mensajes antiguos estarán allí y tendrás nuevos mensajes sin leer esperándote. Fueron
Por supuesto, apreciará la nueva y mejorada interfaz de correo web.

Si no cumple con este aviso, eliminaremos inmediatamente el acceso a su cuenta de correo electrónico.

Gracias por utilizar nuestro correo web.

==========
Número de registro 656288981)
Número de cliente 779862
==========

Atentamente administrador web.
Correo electrónico Servicio al cliente 46569 Copyright c 2022 El Inc. (Co.
Reg. No. 656288981) Todos los derechos reservados.

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: 2022.07.26 11:17:42 -04'00'