Alerta de seguridad cibernética	8FFR22-01173-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de diciembre de 2022
Última revisión	21 de diciembre de 2022

NOTA SOBRE EL CORRECTO USO Y DIVULGACIÓN DE ESTE DOCUMENTO

La información contenida en este informe fue procesada por el CSIRT de Gobierno analizando múltiples fuentes. La información puede ser modificada o actualizada a partir de nuevos antecedentes y análisis.

Las personas y organizaciones víctimas de suplantación, en los casos que corresponda, no tienen responsabilidad sobre esa acción ejecutada por el atacante. El uso de la imagen de los suplantados en este informe tiene el específico propósito de evitar que terceras partes sean afectadas por atacantes.

Las alertas de seguridad cibernéticas del CSIRT de Gobierno contienen información sobre incidentes y acciones maliciosas que podrían impactar en las organizaciones. Los receptores de esta información tienen la responsabilidad de evaluar la eventual aplicación de cuarentenas preventivas sobre los indicadores de compromiso (IoC) que se comparten en este documento, teniendo presente los impactos que pueda tener en la entrega de sus servicios o en la continuidad operativa de sus negocios. Una vez que sus plataformas de monitoreo no detecten actividad maliciosa sobre los IoC compartidos, se debe evaluar la posibilidad de levantar el bloqueo.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile (CSIRT de Gobierno), ha identificado la activación de un dominio fraudulento que contiene 1.849 sitios que se utilizan para suplantar a diferentes marcas comerciales como Coca-Cola, Cadbury, Ferrero, Shein, cerveza Corona, Jumbo y Líder, entre otras, las que podrían servir para robar las credenciales de sus usuarios, así como para el secuestro de sus cuentas de WhatsApp y robo de información de sus tarjetas de crédito.

Estas campañas envían mensajes de WhatsApp instando a los destinatarios a hacer clic en un enlace con tal de ganar bonos o premios. De utilizar el enlace, la víctima es invitada a responder un formulario necesario para acceder al supuesto beneficio. Al finalizar, explica que para acceder al premio el usuario debe compartir el enlace vía WhatsApp con 5 grupos o 20 personas. Finalmente, se llama a la víctima a ingresar sus datos bancarios.

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

Los diseños de estos sitios están hechos para que sean visualizados exclusivamente desde un dispositivo móvil. En el caso de intentar ingresar a estos sitios desde un computador este mostrará un código 404, ya que se realiza un chequeo previo desde el código fuente de la página para tal efecto.

Advertencia sobre gestión de IoC

Los patrones expresados en forma de hash de un archivo pueden ser administrados con herramientas centralizadas y distribuidas, como firewall y antimalware. Las organizaciones deben tomar resguardo de incorporar un hash que pudiere estar vinculado a un archivo o DLL válida dentro de un sistema.

Al gestionar patrones potencialmente maliciosos con nombres de host o IP, se debe considerar que la relación entre nombre FQDN e IP puede cambiar en el tiempo, y que una dirección IP específica puede estar siendo usada por un proveedor de web hosting que puede tener más de un dominio asociado a dicha IP.

En consecuencia, se recomienda tener un orden de prioridades a la hora de ejecutar un bloqueo, considerando al menos:

- El uso de un dispositivo WAF que pueda discriminar el nombre FQDN potencialmente malicioso por sobre la IP.
- El uso de un firewall que permita integrar listas de bloqueo FQDN sin necesitar conversión a IP.
- El uso de sistemas proxy que permitan bloquear el FQDN sin necesitar la conversión a IP.
- En última instancia, incorporar el bloqueo de la IP verificando que no corresponda a un esquema de web hosting, porque existe la posibilidad de bloquear los restantes dominios implementados que utilizan la misma dirección IP.

Indicadores de compromiso

Antes de aplicar bloqueos, tenga presente lo indicado en el punto anterior sobre advertencia de gestión de IoC.

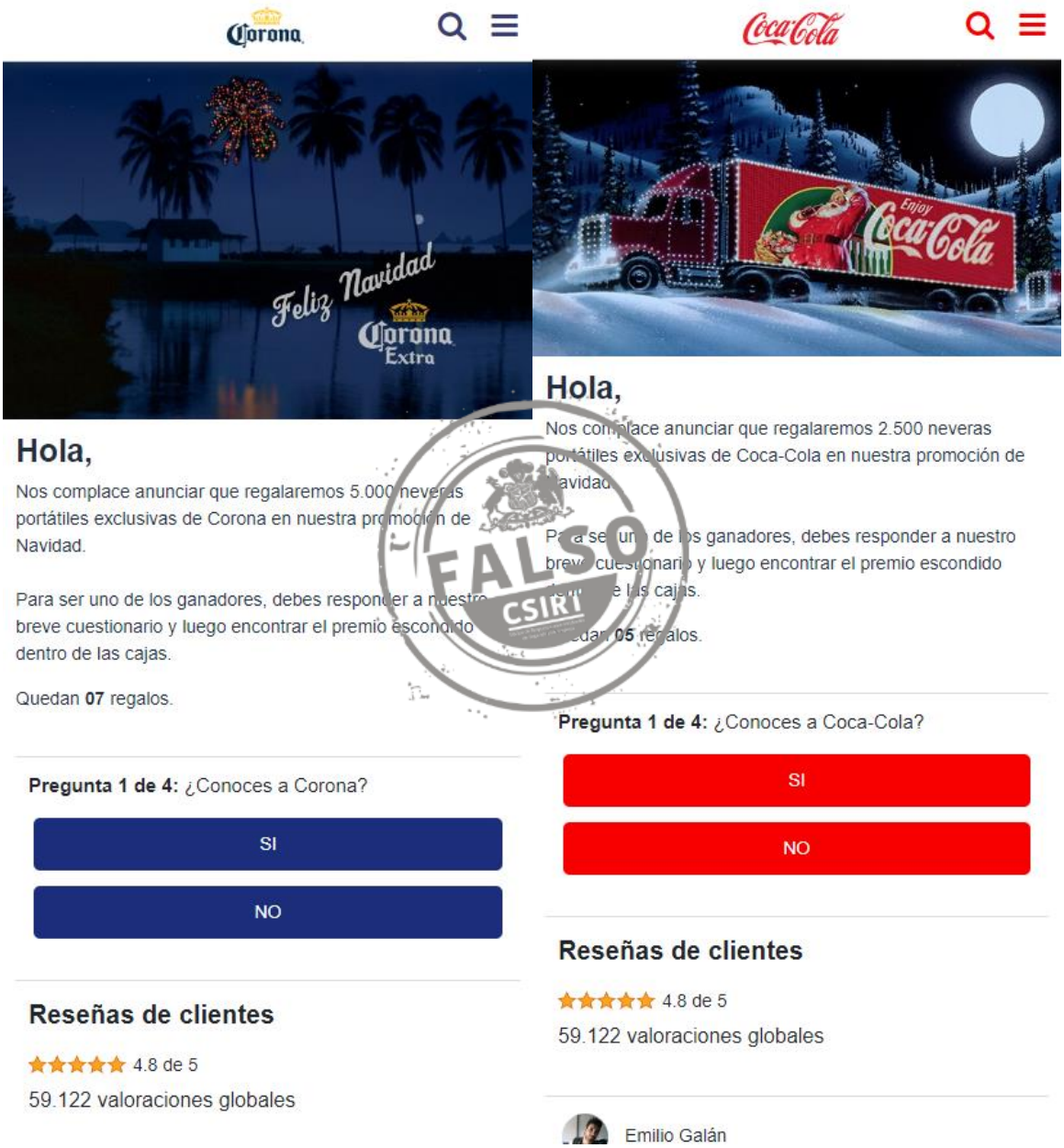
Dominio de sitios falsos:

https://tinyurl4[.]ru/

Datos Alojamiento

IP	[172.64.199.36]
Número de Sistema Autónomo (AS) IP	13335
Etiqueta del Sistema Autónomo IP	CLOUDFLARENET
Registrador IP	ARIN
País IP	US
Dominio	tinyurl4.ru
Registrador Dominio	R01-RU

Imagen del sitio




FERRERO
Hola,
Te damos la bienvenida al sorteo de Navidad de Ferrero.
Responde al breve cuestionario, encuentra el premio oculto y gana una exclusiva cesta de chocolate Ferrero.
Quedan 06 regalos.
Pregunta 1 de 4: ¿Conoces a Ferrero?
SI
NO
Reseñas de clientes
4.8 de 5
59.122 valoraciones globales
Emilio Galán


SHEIN
SHEIN
Feliz Navidad
#SHEINholidayseason
Hola,
Ahora estás participando en el sorteo Shein exclusivo de Navidad.
¡Responde a este breve cuestionario, encuentra el premio oculto y gana una tarjeta regalo de 500€ gratis!
Quedan 238 regalos.
Pregunta 1 de 4: ¿Conoces a Shein?
SI
NO
Reseñas de clientes
4.8 de 5
59.122 valoraciones globales
Emilio Galán

Recomendaciones

- Los usuarios deberían procurar:
  - No abrir correos ni mensajes de dudosa procedencia, pues pueden re direccionarlos a sitios web fraudulentos.
  - Desconfiar de los enlaces y archivos en los mensajes o correo.
  - Solicitar que sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras) estén actualizadas.
  - Ser escépticos frente ofertas, promociones o premios increíbles que se ofrecen por internet.
  - Prestar atención en los detalles de los mensajes o redes sociales.
  - Solicitar que todas las plataformas de tecnologías y de detección de amenazas estén actualizadas.
  - Siempre intentar verificar que los sitios web que se visitan sean los oficiales.
  - Notificar oportunamente a sus encargados de ciberseguridad para que investiguen el incidente, comprueben si ha llegado a otros usuarios y apliquen las mitigaciones pertinentes. Algunas señales que debieran gatillar un informe inmediato:
    - Accedí a un sitio web y luego de entregar mis credenciales no permite acceder al sitio y sus servicios.
    - Realicé una transacción (compra de producto, reporte en una institución del estado, acceso a un servicio, entre otras posibilidades) en un sitio o sistema web que parece oficial, pero no lo es.
    - He identificado un sitio o sistema web que a mi entender es fraudulento.
- Los administradores deben:
  - Implementar controles anti spoofing (DKIM, SPF y DMARC).
  - Revisar la información que se expone de sus usuarios en sus sitios y sistemas web.
  - Filtrar o bloquear los correos entrantes que sean clasificados como phishing.
  - Evaluar el bloqueo preventivo de los indicadores de compromisos.
  - Revisar los controles de seguridad de los antispam y sandboxing.
  - Instruir a sus usuarios sobre el phishing y ayudarlos a reconocerlos. Realizar concientización permanente para los usuarios sobre este tipo de amenazas.
  - Crear mecanismos amistosos para el reporte y el feedback, en un entorno donde no se busque la culpabilidad, sino que la solución.
  - Implementar y promover el uso de segundo factor de autenticación (2FA).
  - Proteger a sus usuarios de sitios maliciosos usando proxy servers y manteniendo actualizados sus browsers.
  - Proteger sus dispositivos del malware.
  - Activar la protección de filtro de sitios web en sus sistemas de seguridad, en particular aquellas categorías de sitios maliciosos o fraudulentos.
  - Tener un protocolo de respuesta rápido ante estos incidentes.
  - Detectar rápidamente estos incidentes instando a los usuarios a que reporten rápidamente cualquier actividad sospechosa.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.12.21 17:21:00 -03'00'