Alerta de seguridad cibernética	8FPH20-00245-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Junio de 2020
Última revisión	11 de Junio 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 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), advierte sobre una campaña de phishing que se está difundiendo a través de WhatsApp supuestamente proveniente de la marca de cerveza Heineken.

El atacante busca persuadir a las personas para utilizar el enlace adjunto al mensaje.

El mensaje promociona a una marca de cerveza ofreciendo un premio equivalente a una Hielera llena de Cerveza Gratis.

Si la víctima selecciona el enlace, es dirigida a una encuesta que debe completar para recibir el supuesto beneficio. Al terminar la encuesta aparece un supuesto proceso de verificación, donde se le solicita compartir el mensaje de la promoción con al menos 20 contactos de WhatsApp. De esta manera, el atacante expande su atácate abarcando más usuarios para ser afectados.

Al realizar el proceso de verificación de las ulrs que aparecen en la falsa promoción, se pudo identificar el direccionamiento a publicidad no deseada y a sitios de baja reputación

Observación

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

Indicadores de compromiso

Urls sitio falso:

hxxps://heineken.regalo[.]top/

Urls Redirecciones:

Body SHA-256 sitio falso

8afbc024932eab93a3c1f4e26345adacfe56134bed04cf5ed84f69d7951a3066

Certificado Digital

Fecha Valido	:	09/09/2019
Fecha Termino	:	09/09/2020
Emitido	:	CloudFlare Inc ECC CA-2

Datos Alojamiento

Red	:	172.64.163.28
IP	:	172.64.0.0/15
Número de sistema autónomo (AS)	:	13335
Etiqueta del sistema autónomo	:	Cloudflare Inc
País	:	Estados Unidos
Registrador	:	ARIN

Datos del Dominio

Nombre de dominio	:	regalo[.]top
Estado del dominio	:	clientTransferProhibited addPeriod
Creado	:	14 de Abril de 2020
Expira	:	14 de Abril de 2021
Información del registrador	:	NameSilo
ID IANA	:	1479
Correo electrónico	:	abuse@namesilo.com
Servidores de nombres	:	nick.ns.cloudflare.com, pam.ns.cloudflare.com

Imagen del mensaje

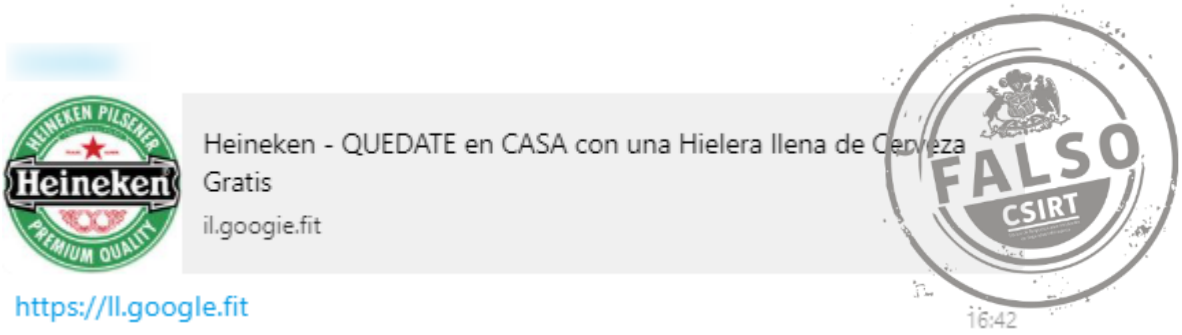
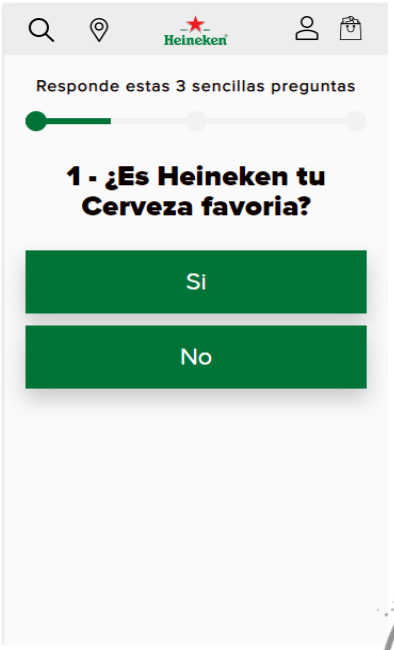
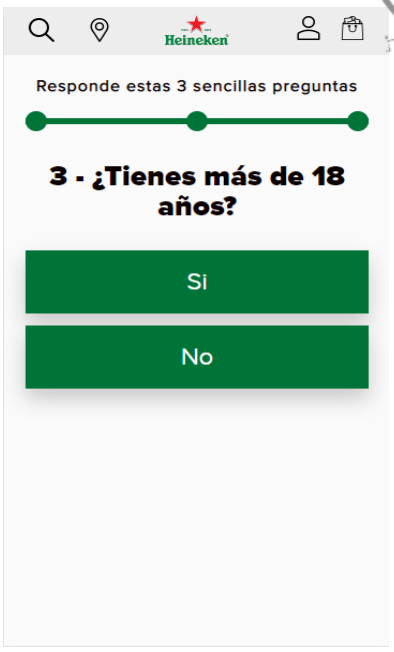


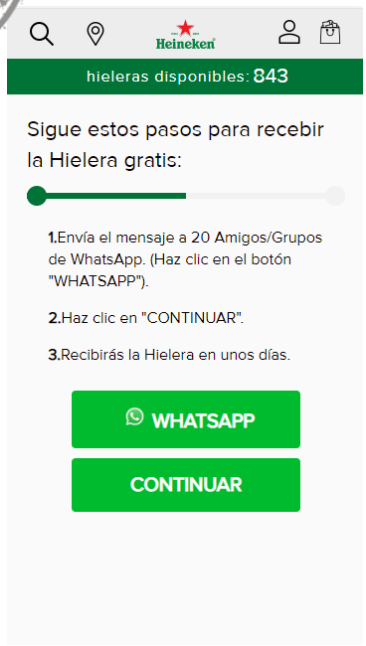
Imagen del sitio


Heineken
Responde estas 3 sencillas preguntas
1 - ¿Es Heineken tu Cerveza favoria?
Si
No


Heineken
Responde estas 3 sencillas preguntas
2 - ¿Cómo te enteraste de nuestra oferta?
Google
Whatsapp
Facebook


FALSO
CSIRT


Heineken
Responde estas 3 sencillas preguntas
3 - ¿Tienes más de 18 años?
Si
No


Heineken
hieleras disponibles: 843
Sigue estos pasos para recebir la Hielera gratis:
1.Envía el mensaje a 20 Amigos/Grupos de WhatsApp. (Haz clic en el botón "WHATSAPP").
2.Haz clic en "CONTINUAR".
3.Recibirás la Hielera en unos días.
WHATSAPP
CONTINUAR

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.