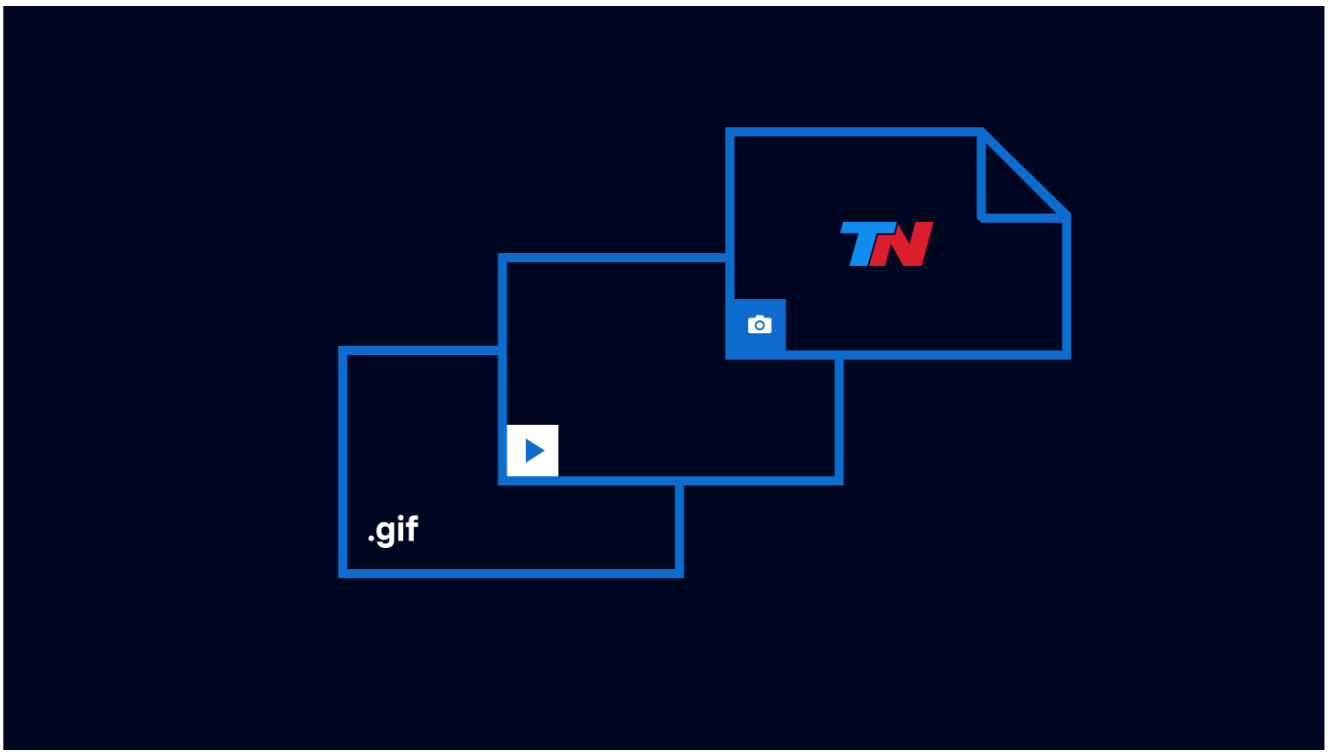
Nuevo intento de estafa por WhatsApp, con una conocida marca de gaseosas

10/03/2020

Una nueva campaña de suplantación de identidad (*phishing*) circula **a través de un mensaje de WhatsApp** con una tentadora oferta, vinculada a la marca Coca Cola. Su objetivo no es regalar heladeras vintage y televisores inteligentes sino **invadir de publicidad no deseada los celulares de las víctimas**.

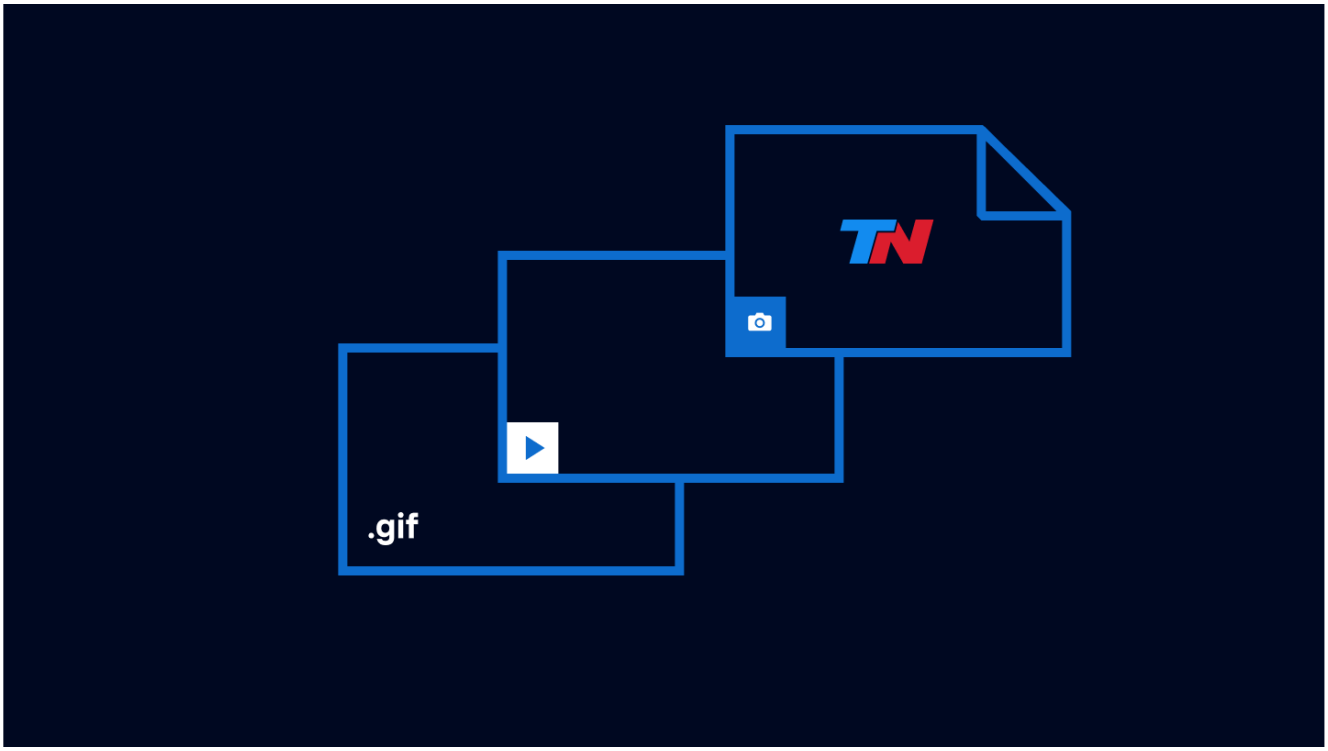
El mensaje que llega a los usuarios intenta hacerles creer que la compañía está regalando productos como parte de la celebración de su 135° aniversario, que en realidad ocurrirá en 2027 según la fecha original de fundación de la marca.



“Lo primero que debería llamar la atención del usuario que recibe este mensaje, en caso de creer que podría tratarse de algo legítimo, es la URL a la cual invita a ingresar, ya que como se puede observar **no corresponde a una dirección oficial**

de la compañía a la que dice representar», explicó Camilo Gutiérrez, Jefe de Laboratorio de ESET Latinoamérica. A pesar de utilizar el nombre de la misma en la URL, el dominio siempre es el que esta inmediatamente a la izquierda de ".com" o, en este caso, de ".live".

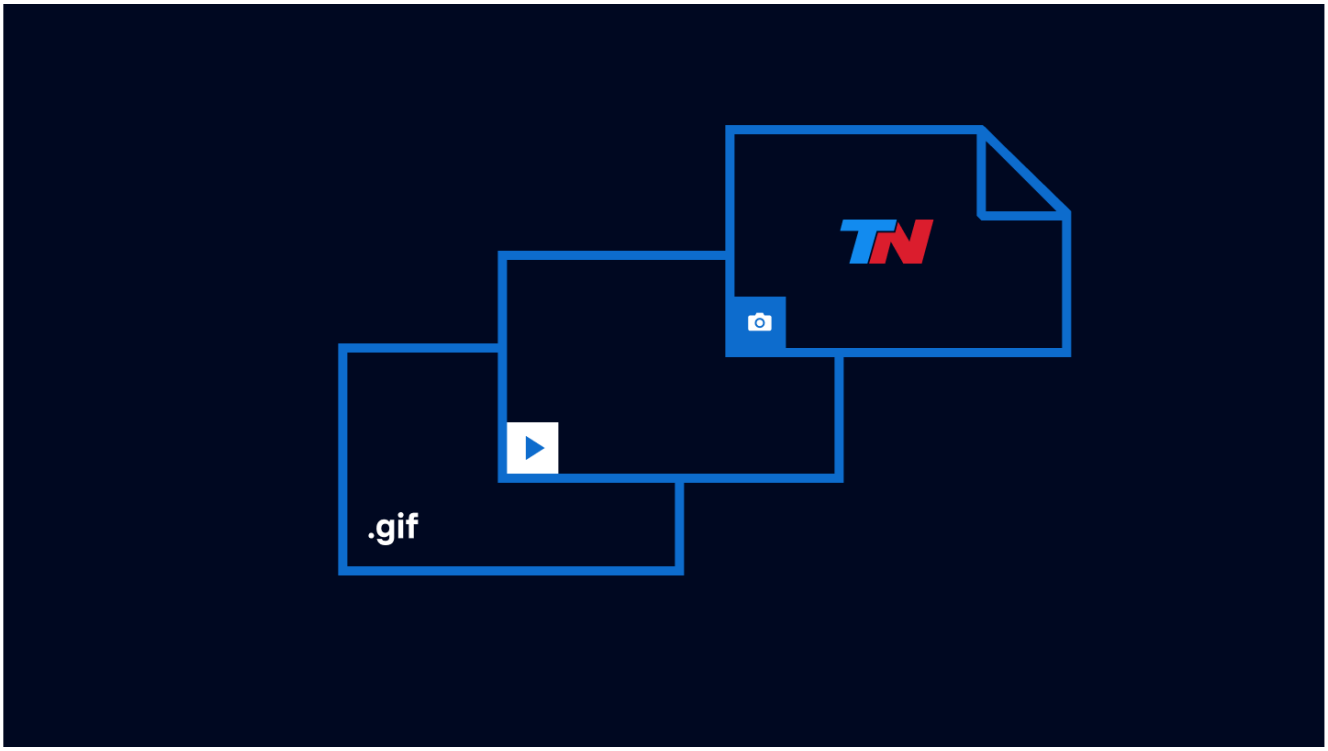
En caso de que el usuario crea en la veracidad del mensaje y acceda al enlace, se encontrará con la siguiente pantalla:



En este punto hay una diferencia entre la información que está en el mensaje que llega a través de WhatsApp y lo que aparece en la pantalla, ya que además de una heladera, se hace referencia a la entrega de un Smart TV.

Esta campaña no solo apunta a usuarios de países de habla hispana, sino que dependiendo desde dónde se haga el acceso al enlace también existe otra versión en inglés, que apunta a usuarios de países angloparlantes.

Por último, tras la verificación de las respuestas, la «campaña» invita a los usuarios a compartir el mensaje con otros 20 contactos, para, supuestamente acceder al beneficio.



La compañía de seguridad informó que **el objetivo de esta campaña es instalar adware** para mostrar publicidad no pedida en los teléfonos de las víctimas.

Consejos de seguridad

– Desconfiar de las promociones que lleguen a través de medios no oficiales. Las empresas suelen divulgar ofertas y concursos **a través de canales oficiales**, ya sea el sitio web o las redes sociales.

– **Evitar hacer click en enlaces sospechosos**, aunque hayan sido enviados por un contacto conocido. En muchas campañas similares, la propagación se hace entre los contactos de la propia víctima.

– Instalar una solución de seguridad confiable en cada uno de los dispositivos conectados a Internet que se utilicen.

– Mantener los dispositivos actualizados.

– No compartir información, enlaces o archivos sin estar seguros de su procedencia.

Fuente: TN