
NEWSLETTER
totalsec
Expertos en Ciberseguridad
No. 295 | Oct 25 - Oct 29

CIBERATAQUE GOLPEA A GASOLINERAS DE IRÁN

OCTUBRE 26, 2021/FUENTE: EL FINANCIERO[1]

Un ciberataque a las gasolineras de Irán este martes paralizó un sistema del gobierno que maneja subsidios de combustibles y obligó a los conductores a hacer largas filas.

Ningún grupo se atribuyó el ataque, que fue similar a otro ocurrido semanas atrás, que pareció apuntar directamente al líder supremo, ayatolá Alí Jamenei, cuando la economía del país colapsa bajo las sanciones estadounidenses.

Según la televisión estatal, un funcionario anónimo del Consejo de Seguridad Nacional reconoció el ciberataque horas después de mostrar largas filas de autos que esperaban recibir gasolina. Un periodista de la Associated Press vio filas de autos en una gasolinera cerrada y con las bombas apagadas.

La TV estatal informó que funcionarios del Ministerio de Petróleo realizaban una "reunión de emergencia" para tratar de resolver el problema.

La agencia noticiosa semioficial ISNA, la primera en calificar al incidente de ciberataque, dijo que quienes intentaban comprar combustible por medio de una tarjeta emitida por el gobierno recibían el mensaje "ciberataque 64411. La mayoría de los iraníes dependen de esos subsidios para cargar sus vehículos, sobre todo en medio de los problemas económicos del país.

Este ataque paralizó el sistema de subsidios en combustibles y provocó largas filas

Si bien ISNA no aludió al significado del número, éste está asociado con una línea telefónica manejada por la oficina de Jamenei que responde a preguntas sobre el derecho islámico. ISNA luego retiró el informe y dijo que la habían hackeado. Este es un argumento empleado frecuentemente por los medios iraníes cuando publican noticias que pueden provocar las iras de la teocracia.

Canales satelitales extranjeros en lengua farsi publicaron videos aparentemente tomados por conductores en la importante ciudad de Isfahan donde tableros electrónicos mostraban leyendas como "¡Jamenei! ¿Dónde está nuestra gasolina?" o "Gasolina gratis en la gasolinera Jamaran", una alusión a la casa del difunto líder supremo, ayatolá Ruhola Jomeini.

[1]Fuente: https://www.elfinanciero.com.mx/mundo/2021/10/26/ciberataque-golpea-a-gasolineras-de-iran/

MEXICANOS, LOS MÁS PREOCUPADOS POR LOS CIBERATAQUES EN EL MUNDO

OCTUBRE 27, 2021/FUENTE: FORBES[2]

La pandemia de Covid-19 le abrió la puerta a los riesgos cibernéticos al pausar las interacciones físicas y priorizar el mundo digital para uso personal y profesional, ante esto, la compañía tecnológica Unisys reveló a través de su Índice de Seguridad que los mexicanos, sobre todo con grados universitarios, son los más preocupados, hasta 13% más, por los ciberataques en el mundo.

"En México saltó la preocupación de tercer lugar al primer lugar en comparación con el año pasado, sobre todo en mexicanos con grados universitarios. Es necesaria la inversión del gobierno para aprobar leyes de protección de datos personales, hay que tener inversiones de las empresas y todas las verticales de la industria, además de promover programas de cómo usar internet", explicó Alexis Aguirre, Director de Ciberseguridad de Unisys en entrevista para Forbes México.

La compañía tecnológica Unisys reveló que el robo de identidad y el fraude de tarjetas bancarias son las principales preocupaciones de los mexicanos

En tanto, el índice reveló también que el robo de identidad y el fraude de tarjetas bancarias son las principales preocupaciones de los mexicanos en temas de ciberseguridad.

"Las personas están mucho más expuestas a los riesgos cibernéticos a causa de la pandemia y están más preocupadas porque de un día para el otro se dieron cuenta que el riesgo incrementó porque el volumen de transacciones que hacemos con nuestras compras aumentó y por otro lado, el número de ataques cibernéticos se intensificó", explicó Mauricio Cataneo, Vicepresidente de Unisys en Latinoamérica.

Los países más preocupados por el riesgo que significan los ciberataques a nivel mundial son: México, Colombia, Brasil, Estados Unidos, Australia, Francia, Reino Unido, Nueva Zelanda, Bélgica, Alemania y Países Bajos, donde seis de estas naciones vieron un aumento en las preocupaciones de seguridad durante 2020.

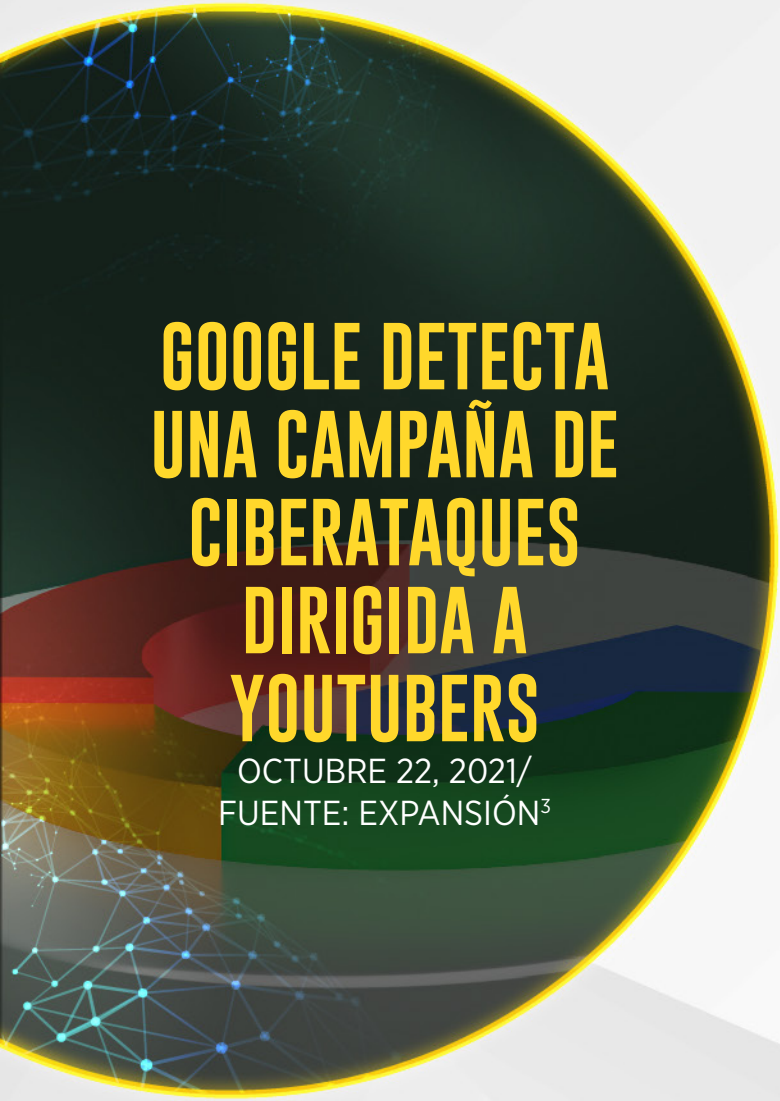
"Los riesgos cibernéticos aumentan en 2021 entre las preocupaciones de los consumidores, pero esta sigue siendo una preocupación menor que la seguridad personal y financiera en México".

Si bien el 66% de los encuestados aseguró que desconfía de hacer clic en enlaces sospechosos, solo el 29% conocía las estafas sofisticadas como el secuestro SIM y únicamente un 22% conoce las organizaciones adecuadas para denunciar los ciberataques.

Ante esto, ambos expertos aseguraron que la adopción de datos biométricos es necesaria para aumentar la seguridad de los usuarios y evitar ataques o filtraciones de datos.

Este índice de seguridad de Unisys se basó en encuestas nacionales e internacionales de muestras representativas de 11,000 adultos de 18 a 64 años en 11 mercados: Alemania, Australia, Bélgica, Brasil, Colombia, Estados Unidos, Francia, México, Países Bajos y Nueva Zelanda.

[2]Fuente: https://www.forbes.com.mx/tecnologia-mexicanos-los-mas-preocupados-por-los-ciberataques-en-el-mundo/



GOOGLE DETECTA UNA CAMPAÑA DE CIBERATAQUES DIRIGIDA A YOUTUBERS

OCTUBRE 22, 2021/
FUENTE: EXPANSIÓN[3]

Las campañas de phishing son un problema conocido en el mundo empresarial y han escalado de tal manera que ya llegó hasta los youtubers, según un informe de Google se detectaron alrededor de 15,000 cuentas falsas y más de un millón de mensajes maliciosos dirigidos a estos creadores de contenido.

El informe señala que los intentos de phishing fueron ejecutados por piratas informáticos de habla rusa y si bien han recuperado cerca de 4,000 cuentas desde finales de 2019, la compañía detalló que los ciberdelincuentes primero buscaban que los youtubers entregaran sus datos de acceso por medio de sitios web falsos.

También destacó que los atacantes intentaban infectar sus equipos con un malware para robar sus cookies de inicios de sesión y tener una forma más sencilla de acceder a diversos niveles de su información.

El Grupo de análisis de amenazas de Google (TAG, por sus siglas en inglés) detalló que el engaño a los creadores se basó en ofrecer colaboraciones publicitarias con compañías como Cisco o Steam. Algunos casos estuvieron relacionados con un "software de noticias COVID-19" y si los creadores estaban de acuerdo en participar, recibían un enlace que infectaba su equipo.

La atracción de los ciberdelincuentes por las cookies de los creadores de contenido en YouTube se debe a que estos archivos almacenan los datos de inicio de sesión de un usuario y, de hecho, son los responsables de que las personas no deban ingresar sus datos una y otra vez.

No obstante, si los piratas informáticos obtuvieron las cookies de los youtubers y las usaron antes de que caducarán, es posible que hayan tomado el control de su canal, cambiar contraseñas para bloquear a los dueños legítimos e incluso les habrían dado acceso a Gmail, Drive u otros servicios vinculados.

Este tipo de campañas demuestran que si bien las campañas de ataques informáticos se han dirigido en mayor medida a las empresas , pues dejan más ganancias, los influencers o creadores de contenido también son un blanco atractivo debido a las grandes audiencias que pueden llegar a tener.

Las ofensivas contra los creadores estuvieron basadas en estafas para obtener su información o para instalar malwares en sus equipos

En el reporte se detalla que después de conseguir las cuentas, los atacantes las vendieron entre tres y 4,000 dólares. El precio se determinó a partir del número de suscriptores con el que contaba el canal.

Otra de las acciones que ejecutaron los cibercriminales en torno a las cuentas robadas fue transformarlas en su totalidad para hacerlas pasar "por grandes empresas de intercambio de tecnología o de criptomonedas". A través de esta modalidad, los atacantes transmitían videos en vivo a grandes audiencias donde prometían obsequios o criptomonedas a cambio de contribuciones.

¿Qué hace Google para proteger a sus youtubers?
Ante este tipo de dinámicas, Google ha instado a sus creadores a ejecutar algunas acciones para protegerse, como activar la verificación en dos pasos, con el objetivo de contar con una segunda llave de seguridad y ralentizar las ofensivas. Incluso esta opción ya es una forma predeterminada de cuidar a los usuarios.

Asimismo, el TAG confirmó hace una semana que ha enviado más de 50,000 advertencias por ataques de malware o phishing a sus usuarios que podrían estar en riesgo. Esto representa un aumento del 33% en comparación con el 2020.

"Cada mes se envían miles de advertencias, incluso en los casos en lo que se bloquea el ataque correspondiente. Si recibes una alerta, no significa que tu cuenta haya sido comprometida, sino que has sido identificado como un objetivo", menciona la empresa.

[3]Fuente: https://expansion.mx/tecnologia/2021/10/22/google-detecta-una-campana-de-ciberataques-dirigida-a-youtubers


NEWSLETTER
totalsec
Expertos en Ciberseguridad