EXCELSIOR
EL PERIÓDICO DE LA VIDA NACIONAL

Fecha	Sección	Página
03.12.2014	Dinero	1-14

ALERTAN DE *HACKERS* IRANÍES

EMPRESAS BAJO ATAQUE

excelsior.com.mx
cobertura

La firma Cylance reporta que ciberdelincuentes han vulnerado la seguridad informática y extraído materiales sensibles de corporativos y gobiernos de países como México y EU

Impactos críticos

2010
Stuxnet

2011
Comodo
Duqu
DigiNotar

2012
Flame
Shamoon
Gauss
Operation ababil

2013
NMCI

2014
Saffron Rose
Newscaster

Imagen tomada de: Estudio de Cylance / FUENTE: Cylance


DINERO
EMPRESAS BAJO ATAQUE
Alcanza el dólar $14.40 en bancos
Los Ramones está operando

Continúa en siguiente hoja

EXCELSIOR
EL PERIÓDICO DE LA VIDA NACIONAL

Fecha	Sección	Página
03.12.2014	Dinero	1-14

Cibercriminales iraníes atacan a México

UN INFORME DE LA EMPRESA CYLANCE, DE EU, ASEGURA QUE FIRMAS DE PETRÓLEO Y GAS EN TERRITORIO MEXICANO FUERON AFECTADAS; PEMEX LO NIEGA

POR AURA HERNÁNDEZ Y NAYELI GONZÁLEZ
dinero@gimm.com.mx

Un grupo de cibercriminales iraníes se introdujo en los sistemas de varias empresas de sectores clave en México y otros 15 países por medio de una campaña llamada Cleaver, que lleva activa al menos dos años y que si no es detenida podría tener repercusiones en el mundo físico, advirtió Stuart McClure, presidente de la empresa Cylance.

La firma de seguridad informática siguió los pasos del grupo, cuyo origen ubicó en Irán, tras analizar las direcciones IP y los sobrenombres que utilizan, aunque también opera en Holanda, Canadá y Reino Unido.

Dicho grupo se encargó de atacar y extraer información sensible de 50 empresas y también tiene entre sus objetivos a instituciones gubernamentales, ya que estuvieron detrás de un ciberataque realizado a la red interna de la Marina de Estados Unidos en 2013.

Rechazan ataque

De acuerdo con el reporte de 86 páginas de Cylance, México fue uno de los países atacados centrándose los esfuerzos de los cibercriminales en la industria petrolera y de gas que tiene operaciones en el Distrito Federal.

"De hecho, el petróleo y gas fue uno de los puntos en los que se enfocó el equipo de Cleaver, yendo tras al menos nueve de estas compañías alrededor del mundo", destacó McClure.

Petróleos Mexicanos que es la empresa encargada de dichos sectores en el país negó de "manera categórica" que sus sistemas informáticos hayan sido vulnerados.

El área de Comunicación social dijo a **Excélsior** que no han tenido ninguna afectación que pudiera poner en riesgo los datos o la operación de la compañía.

México no fue la única víctima de estos cibercriminales, el equipo de seguridad de Cylance informó que en total el número de atacados asciende a cerca de 50 empresas.

Una decena de ellas tiene su sede en Estados Unidos, entre las que destacan una aerolínea, una universidad de medicina, una compañía especializada en la producción de gas natural, otra que se encarga de la manufactura de automóviles e incluso está una instalación militar.

Preocupa el sector aéreo

"Quizás la evidencia más escalofriante que recogimos de esta campaña fue que se centró y comprometió las redes y sistemas de transportes como aerolíneas y aeropuertos en Corea del Sur, Arabia Saudita y Paquistán", declararon los especialistas en el reporte.

Y es que los cibercriminales lograron tener el acceso completo a las puertas de la central aérea de Seúl y sus sistemas de control de seguridad, lo que podría permitir que cualquiera pueda entrar a zonas restringidas, y también lograron hacer compras fraudulentas en las aerolíneas.

Los expertos de la firma no descartan la posibilidad de que la seguridad de los pasajeros de las aerolíneas se vea afectada en un futuro por esta campaña.

Pese a la investigación de dos años, Cylance desconoce el verdadero objetivo que persigue esta campaña de espionaje, infiltración y robo de información.

Las razones

Ante ello los expertos creen que se trata de una campaña patrocinada por el gobierno de Irán.

Esto no resulta sorprendente si se recuerda que dicho gobierno fue atacado por medio de un gusano informático llamado Stuxtnet que se dice pudo ser creado con el apoyo de Estados Unidos para retrasar su programa nuclear.

De hecho, McClure y su equipo consideran que la sofisticación de los cibercriminales de Irán creció rápidamente desde que se descubrió dicho gusano y han tomado algunas represalias, como un ataque de denegación de servicios contra bancos estadunidenses.

"Con plazos a vencer en torno a las discusiones nucleares iraníes en 2015, los ataques pueden estar vinculados a la capacidad de negociación cuando se habla de un pacto con las superpotencias nucleares de Estados Unidos, Gran Bretaña, Francia, Alemania, Rusia y China", supone Cylance.

El método de ataque

Los cibercriminales hicieron uso de diversos métodos. Durante la investigación se pudo observar técnicas de ataque *web*, engaño de los usuarios, programas maliciosos (*malware)* en el código SQL, el uso de equipos de explotación para propagar gusanos, la personalización de herramientas para saltarse credenciales, encriptación o instalar puertas traseras.

Además, algunos sistemas comprometidos incluyen los servidores *web* de Windows que corren con sistemas como ISS y ColdFusion, servidores Linux y de Cisco sus redes privadas virtuales, los *switches* y *routers*.

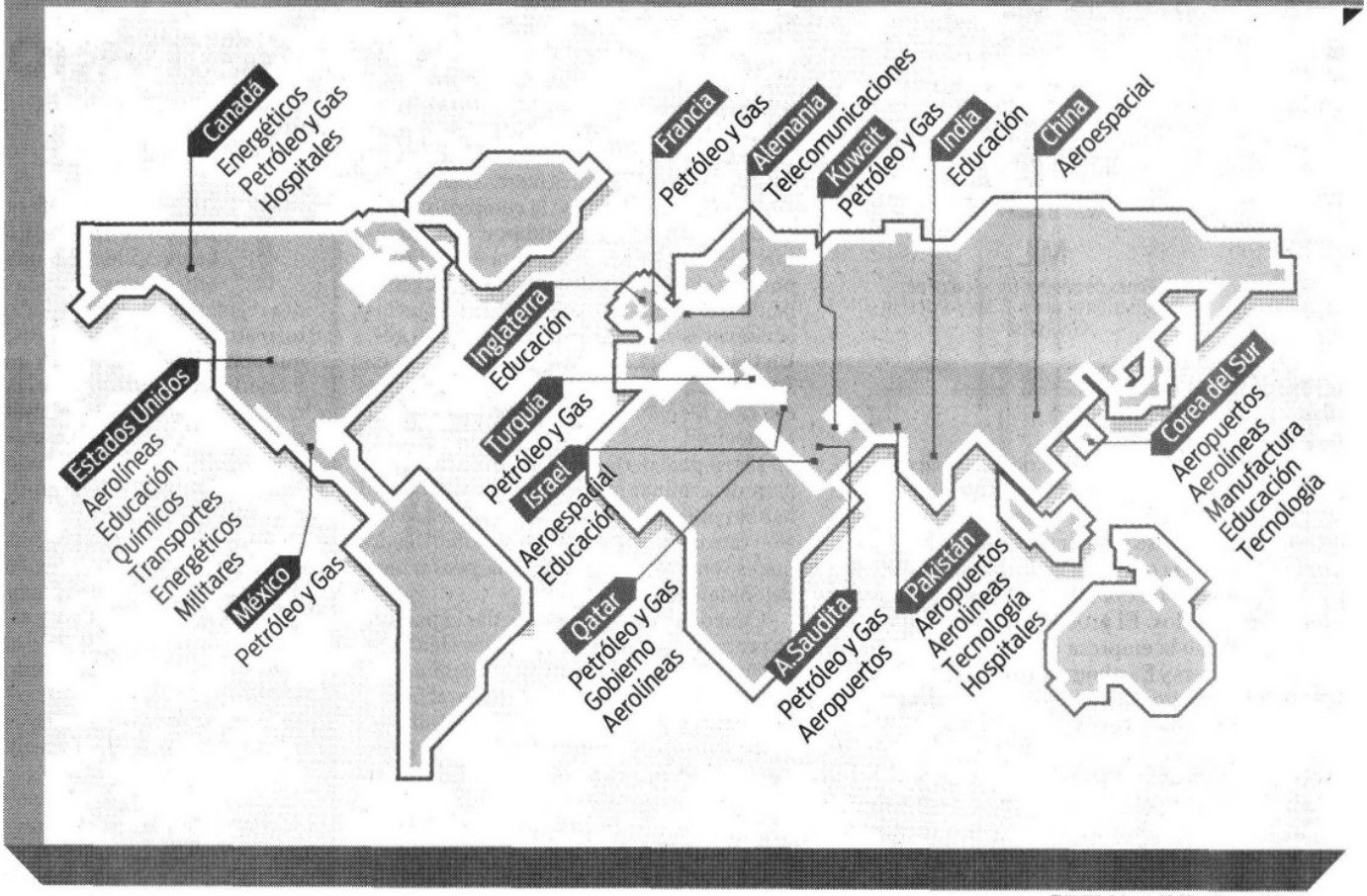
El gerente *senior* de Comunicaciones Corporativas globales de Cisco, Nigel Glennie, aseguró a **Excélsior** que los productos de la compañía no sufren de ninguna vulnerabilidad o problemas en su seguridad.

"Mi valoración es que no estamos hablando de un problema con un producto de Cisco, sino que los atacantes robaron la cuenta de usuario y clave de acceso", resaltó. Agregó que nadie de Cylance se ha contactado con el equipo de respuestas a incidentes de seguridad de los productos de Cisco para avisar de alguna vulnerabilidad.

En lo que respecta a Microsoft, hasta el momento los ejecutivos de la empresa no se han pronunciado acerca de la posibilidad de que sus servicios y productos hayan sido comprometidos.

Países atacados

Las pesquisas de Cylance determinaron que el grupo de ciberdelincuentes que, asegura, opera desde Irán, afectó todo tipo de compañías públicas y privadas en 16 países, sin que se conozca cuál es su objetivo.



FUENTE: Cylance / Gráfico: Fernando Fraga

Continúa en siguiente hoja

EXCELSIOR
EL PERIÓDICO DE LA VIDA NACIONAL

Fecha	Sección	Página
03.12.2014	Dinero	1-14