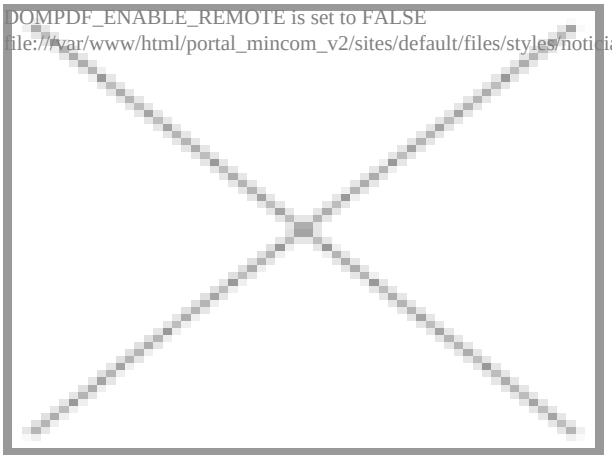

Fuente:
Fayer Wayer

Brasil, México, Chile, Colombia y Argentina están entre los países afectados.
Analistas de Kaspersky Lab, encontraron un foro, llamado xDedic, que es usado para vender sevidores hackeados del tipo Protocolo de Escritorio Remoto (RDP por sus siglas en inglés) por la módica cantidad de USD $6 cada uno.

El problema, aparte del aparente hackeo para obtener acceso a estos servidores, es la información que contienen y que incluye acceso a sitios web y servicios de consumo populares, software instalado para correo directo (del que usan las listas de correo), contabilidad financiera y procesamiento de Punto de Venta o PoS. Además, entre los propietarios de estos datos, están entidades gubernamentales, corporaciones y hasta universidades.

De acuerdo al comunicado de Kaspersky, el proceso que realizan los hackers para irrumpir en los servidores incluye ataques de fuerza bruta, para lograr obtener el modelo del servidor RDP, así como la información contenida; que se pone en un inventario que es ofrecido en el foro antes mencionado.

Con los USD $6 dólares, o más, que pagan los compradores, se ingresa a la información almacenada o al servidor para realizar ataques dirigidos, malware, DDoS, phishing, ataques de ingeniería social, adware, o lo que el cliente requiera. Mientras tanto, los dueños de estos servidores, no están enterados de lo que sucede tras bambalinas.

En mayo de 2016, Kaspersky contabilizó una lista de 70.624 servidores hackeados, distribuidos en 173 países. Entre los 10 más afectados se encuentran Brasil, China, Rusia, India, España, Italia, Francia, Australia, Sudáfrica y Malasia. Mientras que México figura en el doceavo lugar, seguido de Colombia. Argentina se encuentra en el 19, y Chile en el 62.

Costin Raiu, Director del Equipo de Análisis e Investigación Global de Kaspersky Lab, dijo:
XDedic es una confirmación más de que el delito cibernético como servicio se está expandiendo a través de la adición de ecosistemas comerciales y plataformas de negocios. Su existencia hace que sea más fácil que nunca para todo el mundo, desde atacantes maliciosos con poca experiencia hasta APTs respaldadas por estados nación que participan en ataques potencialmente devastadores de una manera barata, rápida y eficaz. Las víctimas finales no son sólo los consumidores u organizaciones específicas en un ataque, sino también los propietarios desprevenidos de los servidores: es muy probable que ignoren completamente que sus servidores han sido secuestrados una y otra vez para diferentes ataques, todos realizados justo debajo de sus narices.

Disponible en:

https://www.fayerwayer.com/2016/06/kaspersky-descubre-mercado-clandestino-con-mas-de-70-000-servidores-hackeados/ [1]

Links
[1] https://www.fayerwayer.com/2016/06/kaspersky-descubre-mercado-clandestino-con-mas-de-70-000-servidores-hackeados/