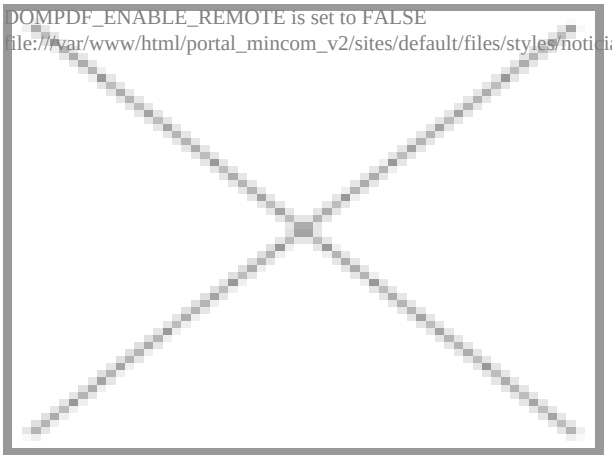

Fuente:
siliconnews

Aunque los objetivos están ubicados principalmente en Brasil, también se han identificado empresas víctimas en EEUU, Francia, Kazajstán, Emiratos Árabes Unidos, India y Rusia.

Kaspersky Lab ha anunciado el descubrimiento del Grupo Poseidón, un actor de amenazas avanzadas activas que lleva operando a nivel global desde 2005.

El malware está diseñado para funcionar específicamente en equipos Windows en portugués brasileño e inglés. Una de las características del Grupo Poseidón es la exploración activa de las redes corporativas basadas en el dominio.

Una vez que un equipo está infectado, el malware informa a los servidores de comando y control antes de comenzar una fase compleja de movimiento lateral. En esta fase interviene una herramienta especializada que recoge de forma automática un gran flujo de información: credenciales, políticas de gestión de grupos e incluso los logs del sistema para perfeccionar futuros ataques y asegurar la ejecución de los programas maliciosos.

“El Grupo Poseidón es un equipo sólido con muchos años de trayectoria en todos los dominios: tierra, aire y mar. Algunos de sus centros de mando y control se han encontrado en el interior de los ISP que ofrecen servicios de Internet a los barcos en alta mar, en las conexiones inalámbricas, así como los operadores tradicionales. Además, la vida útil de sus implants es muy corta, lo que les ha ayudado a operar mucho tiempo sin ser detectados“, ha explicado Dmitry Bestúzhev, director de investigación global de Kaspersky Lab América Latina.

Se han identificado al menos 35 empresas víctimas, entre las que se incluyen instituciones financieras y gubernamentales, telecomunicaciones, energía, empresas de servicios públicos, medios de comunicación y empresas de relaciones públicas.

Aunque los objetivos están ubicados principalmente en Brasil, también se han encontrado víctimas en EEUU, Francia, Kazajstán, Emiratos Árabes Unidos, India y Rusia.

Disponible en: http://www.siliconnews.es/2016/02/10/se-descubre-el-malware-poseidon-en-equipos-windows/ [1]

Links
[1] http://www.siliconnews.es/2016/02/10/se-descubre-el-malware-poseidon-en-equipos-windows/