Las máquinas virtuales de VMware, objetivo del troyano Crisis

El malware **Crisis**, un tipo de troyano detectado el pasado mes de julio por **Intego**, es capaz de **infectar máquinas virtuales creadas con el software de VMware**. Así lo confirma la compañía de seguridad **Symantec** tras el análisis exhaustivo de su código.

No es el único objetivo por el que este troyano fue confeccionado. De hecho es capaz de llevar a cabo distintos ataques, como la infección de dispositivos móviles basados en Windows Mobile (que estén conectados al PC), unidades extraíbles USB, la grabación de conversaciones a través de Skype o el robo de los sitios visitados a través de los navegadores Firefox y Safari. No es tampoco un virus exclusivo de Windows, sino que también es capaz de detectar Mac OS y lanzar el código javascript diseñado específicamente para la plataforma de Apple.

En el caso de la infección de máquinas virtuales de VMware, Symantec explica que **podría ser el primer malware capaz de expandirse en este tipo de recursos virtualizados**. “en el momento en que un ordenador es infectado, el troyano busca una imagen de VMware. Si la encuentra, es capaz de montarla y copiarse a sí mismo en ella valiéndose de la herramienta VMware Player”, destacan los investigadores.

A su vez, Kaspersky Lab, que lo detecta con el nombre de **Morcut**, apunta que “esta funcionalidad específica para atacar máquinas virtuales es capaz de buscar información sobre cuentas bancarias o movimientos de comercio electrónico para robar los datos asociados y enviarlos a los creadores del troyano”.

Por el momento no se ha detectado un número muy alto de máquinas infectadas por el troyano Crisis, aunque todas las compañías de seguridad coinciden en que se trata de un importante amenaza en potencia para este tipo de ordenadores virtuales.