Ciberdelincuentes roban al menos 265 millones de bancos de todo el mundo

15/02/2015

Este sábado el diario The New York Times desvelaba que un grupo de ciberdelincuentes habrían robado al menos 300 millones de dólares (unos 263 millones de euros) de bancos de todo el mundo desde finales de 2013.

La cifra podría llegar a ser el triple, de 900 millones, añaden. Según este diario, la mayor parte de las víctimas estarían en Rusia (aunque también se han atacado a bancos de EE UU, Japón y países de Europa). En total, serían más de 100 bancos e instituciones financieras de un total de 30 países, lo que podría convertirse en el mayor robo bancario de la historia. Los datos, adelantados este sábado por el periódico estadounidense, forman parte de un informe de la empresa de ciberseguridad rusa Kaspersky Lab que se hará público este lunes.

Esta empresa descubrió que en los ordenadores internos de estos bancos, utilizados por empleados que procesan a diario transferencias, se había introducido malware que permitía a los ciberdelincuentes registrar cada movimiento. El software malicioso se ocultaba durante meses, enviando vídeos e imágenes que informaban a este grupo cuál era la rutina diaria del banco, según Kaspersky.

'Modus operandi'

Según los investigadores de Kaspersky, la técnica empleada por los ciberdelincuentes ha sido la clave para que durante estos años ni los bancos ni la justicia se percataran de un robo de tal magnitud.

Como en cualquier otro ciberataque, el grupo enviaba a sus víctimas emails infectados (con mensajes que parecían provenir de algún amigo) como cebo. En cuanto los empleados del banco abrían el correo electrónico, estaban descargando inconscientemente un código malicioso que permitió a los ciberdelincuentes rastrear la red del banco hasta localizar a los empleados que administraban los sistemas de transferencias bancarias o que tenían acceso a cajeros automáticos. A continuación, instalaban en esos ordenadores una herramienta de control remoto que capturaba vídeo e imágenes de la pantalla. La finalidad era "imitar sus actividades", según ha revelado Sergey Golovanov, encargado de la investigación en Kaspersky Lab. "De este modo, todo parecería normal, como si fuera una transacción rutinaria".

En cuanto a las cantidades sustraídas, Kaspersky tiene pruebas del robo a clientes de unos 300 millones de dólares, aunque reconoce que podría llegar a ser el triple. Además, indican que el cálculo es imposible de verificar porque los robos se limitaban a 10 millones de dólares por cada transacción, aunque algunos bancos fueron atacados en varias ocasiones.

Según señala The New York Times, el silencio en torno a la investigación parece estar motivado en parte por la reticencia de los bancos atacados a reconocer que sus sistemas fueron burlados con facilidad, y en parte por el hecho de que estos ataques todavía continúan.

"Probablemente este sea el ataque más sofisticado visto hasta la fecha en cuanto a las tácticas y métodos utilizados por los cibercriminales para mantenerse en secreto", ha calificado el director de la oficina que Kaspersky tiene en EE UU, Chris Doggett.