Kaspersky identifica un cibergrupo que espiaba a más de 30 países

17/02/2015

Sus ataques estaban coordinados principalmente desde EE.UU. y el Reino Unido. El virus que usaban afectaba al disco duro del ordenador, de donde era casi imposible eliminar.

Según Kaspersky Lab, Equation Group ha estado funcionando durante casi **20 años** y sus acciones han afectado a miles, tal vez decenas de miles, de usuarios. "Lo que los expertos de la compañía han descubierto recientemente supera todos los ataques maliciosos hasta ahora conocidos", dice el informe de Kaspersky Lab.

La infraestructura de Equation Group cuenta con más de 300 dominios y 100 servidores de control y mando que se hallan principalmente en EE.UU., el Reino Unido, Italia, Alemania, Países Bajos, Panamá, Costa Rica, Malasia, Colombia y la República Checa. Kaspersky Lab ahora controla alrededor de 20 servidores del grupo. De acuerdo con la empresa rusa, los 'hackers' **atacaron 12 grandes fabricantes**: Western Digital Technologies, Maxtor, Samsung, Seagate Technology, Micron Technology, Toshiba Corporation y IBM entre otros.

Kaspersky Lab señala que Equation Group interactuaba con otros cibergrupos, sobre todo con los relacionados con los virus **Flame y Stuxnet**. "La principal funcionalidad del programa de Equation Group es robar información, y podemos confirmar que los atacantes intercambiaron información con 'colegas' que están detrás de los ataques de Stuxnet y Flame. Por el momento, no hay evidencia directa de que Equation Group esté vinculado con servicios especiales, así como no hay certeza absoluta de la nacionalidad de sus creadores", resume el informe.