



María Alicia Pinzón Montenegro es acusada por la Fiscalía española por ser la persona que creó el software utilizado por la red de interceptaciones ilegales que ya ha dejado hasta ahora ocho detenidos, entre ellos, el general Humberto Guatibonza. La hacker confesó a los investigadores cómo inició su trabajo en la organización.

La experta en informática le ofreció a la Fiscalía colaborar para entregar información sobre sus socios y de cómo creó el sistema. Les advirtió que no ingresen sus claves porque dejó seguros que eliminaban toda la información contenida en los equipos.

Montenegro es madre soltera y vivía con sus padres en Ipiales, afirmó que comenzó a trabajar en la creación del sistema de interceptaciones ilegales en 2006, cuando decidió nombrarlo como Fénix.

Dijo a la Fiscalía que lo hizo porque se dio cuenta de que la información era muy solicitada por integrantes de la Fuerza Pública con los que ya había trabajado entregando archivos obtenidos de equipos informáticos.

Al principio, Fénix permitía verificar cuentas de correo y lograr obtener la ubicación asociada a dichos correos, sin embargo, al poco tiempo la hacker logró perfeccionarlo.

Calificada como genio por el Coronel del Ejército, Jorge Humberto Salinas, detenido y testigo de la fiscalía, la hacker logró en muy poco tiempo perfeccionar sus sistema y conseguir otro tipo de accesos a redes telefónicas y equipos de cómputo.

Montenegro informó a los investigadores que el sistema fue creado por ella con información empírica y con datos básicos que supuestamente le suministró un profesor de una Universidad, quien «le dio información sobre cómo desarrollar aplicaciones en cuestiones de redes».

Fénix logró después recuperar mensajes privados de WhatsApp, ubicación de teléfonos celulares, ubicación de teléfonos satelitales, entre otros.



Según el expediente, el primer caso fue el de Ferrocarriles del Pacífico, y a partir de entonces, se empezaron a realizar pruebas en la interceptación de mensajes que resultaron ser efectivas.

La Fiscalía asegura que dichas capacidades son reales. La hacker explicó que ella no estaba cometiendo acciones ilegales ya que estaba entregando información solicitada por exintegrantes de las Fuerzas Militares que estaba siendo utilizada en investigaciones contra redes que estaban robando, amenazando o extorsionando a algunas empresas.

El coronel Salinas admitió haber contactado a la hacker en 2006, y asegura que la conocía porque ya había trabajado en el ejército y le preguntó que si ella podía interceptar audios y comunicaciones de WhatsApp. Ella lo hizo porque había sospechas sobre robos internos en la empresa Ferrocarriles del Pacífico, donde fue contratado el coronel como jefe de seguridad.

A partir de ese momento, la hacker crea su empresa criminal, ya que la Fiscalía asegura que llegaron a tener más de 170 casos activos en los que se hicieron interceptaciones ilegales.

La Fiscalía también dijo que los integrantes de la red consideraron que Fénix podría ser clave en la aplicación de la figura del acusador privado que entró en vigencia a mediados del año pasado, mismo que permitía a particulares realizar sus propias investigaciones y llevarlas a juicio.

Según los investigadores, la hacker desplegó toda una ofensiva comercial para ofrecer los servicios de Fénix a particulares que necesitaban realizar investigaciones privadas.

Dicho software resultó tan efectivo que hasta se hicieron contactos a nivel internacional para ofrecer los servicios a clientes potenciales.