

La Guardia Civil dice que la red de ordenadores 'zombies' es la mayor detectada en todo el mundo

Tres ciudadanos españoles controlaban más de 13 millones de ordenadores infectados

La Guardia Civil, en colaboración con el FBI, ha detenido a tres ciudadanos españoles que controlaban más de 13 millones de ordenadores infectados de los que obtenían datos financieros y personales. El Instituto Armado asegura que es la mayor red de ordenadores 'zombies' detectada en todo el mundo. Los ordenadores infectados estaban repartidos en 190 países y afectaban a instituciones gubernamentales, empresas privadas --entre ellas 40 de los bancos más importantes del mundo-- y ordenadores particulares, según informó el teniente coronel jefe del departamento de Investigación de Delincuencia Económica y Tecnológica de la Benemérita, José Antonio Berrocal, en rueda de prensa.



En los registros practicados en los domicilios de los detenidos se han intervenido PCs, material informático e información personal de más de 800.000 direcciones IP, que pueden incluir a varios o sólo un ordenador bajo la misma dirección. La 'botnet' fue detectada y se bloqueó su control de acceso a los tres implicados. Los datos obtenidos podían utilizarlos los propios detenidos o alquilarlos a bandas organizadas dedicadas al fraude bancario.

De hecho, según informó Berrocal, hay indicios de que la red había sido alquilada durante un tiempo para que terceros pudiesen utilizarla. El máximo responsable de la red, cuya identidad responde a las iniciales F.C.R., de 31 años, se hacía llamar a sí mismo 'Netkairo' o 'Hamlet1917' y fue detenido en Balmaseda (Vizcaya). Otro de los detenidos, J. B. R., de 25 años, se identificaba bajo el nick de 'OsTiaToR' y es de Santiago de Compostela. El tercer detenido, J.P.R. de 30 años, se identificaba como 'Johnyloleante' y residía en Molina de Segura, en Murcia.

Todos ellos fueron puestos a disposición judicial en la Audiencia Nacional. Tras la detención, los responsables de la 'botnet' han sido puestos en libertad con cargos a la espera de la finalización de la instrucción. Según los responsables de la Guardia Civil, todavía se está investigando la "ingente" cantidad de datos que la red había conseguido robar.

Los tres detenidos en España no eran, según se ha extraído de los ordenadores incautados, los creadores del 'malware' que ha extendido la 'botnet' sino que se trata de un 'software' adquirido y que ellos, como administradores, han desarrollado. A su vez, según informó Berrocal, hay indicios de que la

red había sido alquilada por terceros con objetivos aún por determinar pero que pueden desembocar en robo de datos personales, saturación de servicios o envío masivo de 'spam'.

Por el momento, la investigación no está cerrada y los agentes recordaron que todavía podrían producirse nuevas detenciones. "Es lo lamentable de la seguridad en la Red, mientras que hay muy pocas personas que sean capaces de crear un 'software' malicioso cualquiera pueda pagar por estas aplicaciones y utilizarlas", declaró el jefe de delitos telemáticos de la Guardia Civil, el comandante Juan Salom.

Salom también lanzó un mensaje a los ciudadanos advirtiéndole que "ha habido suerte" al haberse producido la detención antes de que los datos fueran explotados masivamente por los responsables de la 'botnet' y advirtió de que aunque la Red "es muy beneficiosa" hay que utilizarla con responsabilidad.

Por su parte el director técnico de PandaLabs, Luis Corrons, aclaró que a pesar de un ordenador haya sido infectado, actualmente, "cualquier programa antivirus" es capaz de eliminar la infección que, en este caso, se ha podido extender a través de las redes P2P, mensajería instantánea e incluso dispositivos USB.

Cronología de la investigación

Los primeros indicios sobre el desarrollo de la red de ordenadores 'zombies' --botnet Mariposa-- los tuvo la empresa de seguridad informática canadiense Defense Intelligence en mayo de 2009. En colaboración con la empresa española Panda se inició un seguimiento que reveló que los administradores o 'botmasters' son españoles o de habla hispana. En octubre y noviembre del pasado año la investigación alcanzó "su punto máximo".

Se descubrió que la red conectaba con dominios españoles y estadounidenses y en ese momento tanto Panda como el FBI informaron a la Guardia Civil de la investigación. La operación de desmantelamiento comenzó el 23 de diciembre del pasado año. "No es una fecha al azar", según Corrons, ya que se intenta realizar estas operaciones en momentos en que la gente está "mas distraída" al igual que hacen los propios delincuentes cuando actúan en la Red. En ese momento, los primeros indicios revelaron el número de ordenadores infectados --13 millones en 190 países-- cantidad que "sorprendió" a los propios responsables al ser la mayor red de ordenadores intervenida hasta la fecha.