01 de Junio de 2005	Universidad de Granada	Granada Hoy

Granada Hoy

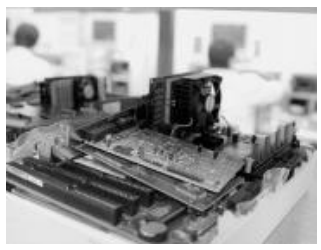
Actualización | miércoles, 01 de junio de 2005, 06:21

CULTURA

nuevas tecnologías

Un informático aplica análisis forense contra la ciberpiratería

Este control en los ordenadores sirve de herramienta para determinar las causas de los ataques informáticos, uno de los grandes problemas actuales de internet



g. h.

A FONDO. El análisis forense aplicado a ordenadores llega hasta las entrañas de los equipos.

■ Los gobiernos, saturados por el correo basura

I. GARCÍA

GRANADA. Los ataques informáticos han dejado de ser exclusivos de expertos programadores y se están popularizando. Una agencia de vigilancia *on–line* contabilizó el año pasado 400.000 ataques a través de internet, un 36 por ciento más que el año anterior. El objetivo de estos *ciberpiratas –crackers–* es hacerse con el control de ordenadores conectados a la red para usarlos según sus intereses.

En muchos casos los usuarios de los equipos afectados no son conscientes de que sus ordenadores son rehenes de los *crackers*. Sin embargo los informáticos están desarrollando herramientas para descubrir estos ataques y localizar a los responsables. Una de ellas es el análisis forense aplicado a los ordenadores, técnica que reproduce lo que hacen los detectives de la policía para resolver un caso y cuyas conclusiones pueden ser utilizadas como prueba en un juicio. Como en la serie de televisión *CSI* pero con ordenadores.

Este tipo de técnicas se aplican a equipos que han sufrido ataques de *ciberpiratas* con el objetivo de determinar "quién lo hizo, cómo y por qué", explica Juan Martín Galeote, ingeniero informático de la **Universidad de Granada** (UGR) que fue recientemente premiado en un concurso internacional de análisis forense informático.

En este concurso realizó la autopsia a un ordenador muerto –desconectado– que la organización había colocado como señuelo. Galeote procedió aplicando el método científico: plantear una hipótesis y demostrarla de varias maneras, como hacen los detectives de verdad. Todo el proceso lo realizó con programas de código abierto, el denominado *sotware* libre.

Mediante una copia del disco duro afectado el informático pudo realizar una réplica del equipo y "desmenuzar los pequeños detalles" del sistema en busca de pistas, como los accesos a los ficheros, su modificación o supresión. El tiempo transcurrido desde el ataque es fundamental, ya que "cuanto más tiempo pase, más difícil es recuperar la información".

Con estos datos se puede reconstruir la vida del ordenador y descubrir las huellas dejadas por los asaltantes, así como los programas que utilizaron para el ataque. "Aunque intentan ocultar sus pasos siempre dejan algún rastro", asegura el informático granadino.

Seguir este rastro para dar con la identidad de los *crackers* puede resultar algo más complicado. Todos los ordenadores conectados a internet tienen un número que los identifica, pero "esto no es un dato seguro, porque lo más probable es que el ordenador desde el que fue atacado también estuviese pirateado", reconoce Galeote. El rastro se pierde así en una maraña de conexiones por todo el mundo.

Sin embargo, en este caso –como en la mayoría de los asaltos que se realizan– los piratas utilizaron programas que están disponibles en la red, por lo que "mediante una orden judicial se puede contactar con el proveedor de la página a la que se conectaron para descargarse estos programas". Esta vía puede llevar hasta los *crackers* que, en el caso investigado por Galeote, eran de nacionalidad rumana.

La finalidad de estos ciberpiratas es tan antigua como la que animaba a sus antecesores marinos: la económica. Utilizaban sus redes de ordenadores esclavos –*zombies*, en la jerga– para alquilarlos a quienes envían correo basura, a precios que pueden llegar a 100 euros la hora. Además intentaron un timo consistente en hacer una copia de la página web del banco del usuario para después pedirle que les recuerde sus datos. Suerte que el equipo era sólo un señuelo. Y que los informáticos están preparándose para convertirse en *ciberpolicías*.La plaga del *spam*, el correo basura que inunda los ordenadores *zombies*, preocupa ya a las autoridades estadounidenses. La Comisión Federal de Comercio ha lanzado recientemente una campaña *anti spam*, que espera poder globalizar a través de la colaboración con otras agencias gubernamentales. Según los datos que manejan, los ordenadores *zombies* son los responsables de al menos el 40 por ciento del correo basura de todo el mundo. El problema es que muchos de los usuarios desconoce que su ordenador está infectado por uno de los tantos virus que proliferan en la red. El consejo, según Galeote, es "actualizarse y no ejecutar ningún programa desconocido".