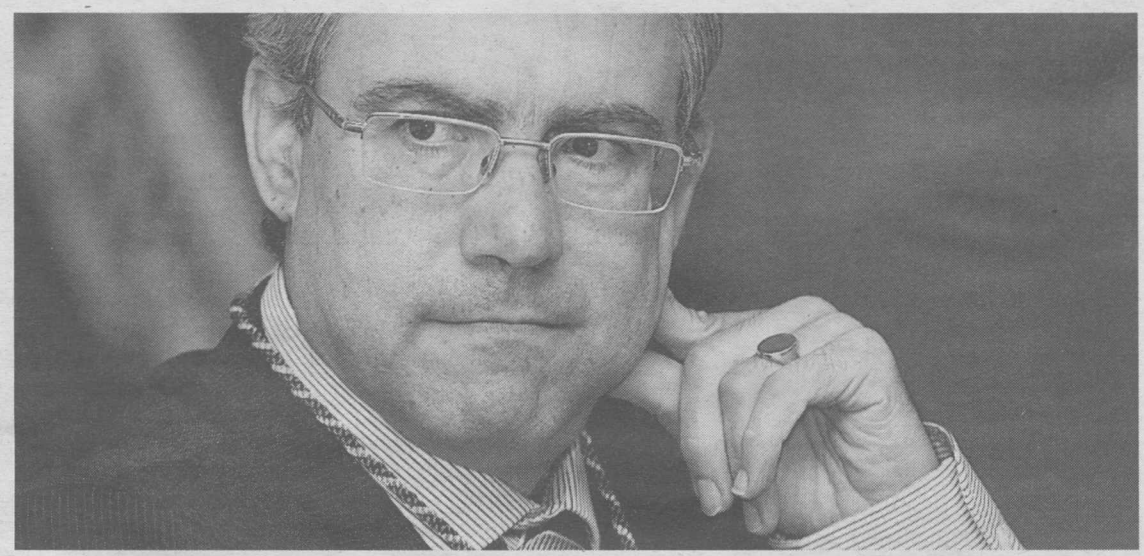
da más que mos 'pa' lo malo as noticias»

salimos en las noticias 'pa' malas», comentaba ayer e un vecino de Molina de a las pocas horas de tras- r que el tercer detenido de Mariposa reside en esta lo- l. Los molinenses aún tie- esente que el pasado fin ana fueron portada dos vecinos 'cazados' por un 237 y 233 kilómetros por odo un récord. Ayer le to- turno al tal Jonhy Lo- , un 'nick' tras el que está e 30 años. «¡Menudo apo- legido el liante éste!», se- otro vecino. ¿Pero quién a Loleante? Parece que A algunos gerentes de s de informática les sona- ombre, pero en realidad a podido identificarlo, ni a las fuentes policiales tadas en el municipio. Lo tienen claro es que Lo- es «un verdadero hacker, que lo es realmente no lo endo», señala un informá- n embargo, no se trata de n experto porque, según cia, Johny y sus dos socios eñaron la red, sino que la aron. Los vecinos mani- an gran sorpresa confor- n conociendo más deta- bre todo por el alcance in- ional de la red. «Parece a que un zagal del pueblo a en esos berenjenales», n hombre mayor del Lla- sí, la gente también tie- o que quien la hace, la unque sea del pueblo. «Lo tenían mis datos», co- ba el regente de una tien- nformática.

nte el registro. :: G. CIVIL



El decano de Informática, José Manuel García, el día de su toma de posesión. :: EDU BOTELLA / AGM

«Cualquiera puede tener un 'hacker' cerca de su casa»

José Manuel García Decano de la Facultad de Informática de la UMU

:: D. VIDAL

MURCIA. José Manuel García Carrasco (Valencia, 1962) es uno de los referentes en la Región si preguntamos por un experto en ordenadores. Su condición de decano de la Facultad de Informática de la UMU es idónea para responder a todas las preguntas que surgen cuando se habla de 'hackers', 'botnet' o cosas similares. El nombre lo dice casi todo, pero mejor que lo explique él.

–Zombis... El nombre da miedo.

–Con eso se quiere decir que el ordenador no se mueve por voluntad propia, sino que están 'poseídos'. No funcionan de manera autónoma, ya que obedecen las órdenes de aquellos que los 'poseen'. Al tener varios ordenadores controlados, se puede crear esa 'botnet' (red de robots).

–Lo estamos mejorando... Pero ¿le puede pasar a cualquiera?

–Claro. A cualquiera que tenga un ordenador conectado a Internet.

–¿Y cómo llega un ordenador personal a ser el zombi de otro?

–La palabra más conocida es virus, aunque también se conocen como troyanos. Vienen con programas que nos descargamos o con propaganda que nos llega al ordenador y que es 'aceptada' por el usuario. Es decir, se accede a un contenido que viene con un correo de remitente desconocido o se 'pincha' en una web maliciosa. Así entra el virus que da acceso a todos los contenidos del ordenador a esa tercera persona.

–Bien –o mal, mejor dicho–, el ordenador ya es un zombi. ¿Qué pueden hacer con él?

–Se puede acceder a los archivos de tu ordenador y a tu cuenta corriente. Las transacciones comerciales por Internet son seguras porque utilizan claves cifradas, pero cuando el ordenador se infecta, esas claves ya son accesibles para terceros... Pero lo normal es que tu ordenador, como el de miles, se utilice para atacar a otros servidores más potentes...

–¿Está diciendo que nos 'utilizan' para conseguir otros objetivos?

–Claro. Utilizan esos ordenadores para colapsar por ejemplo la web de la Casa Blanca... Programan a todos los zombis a una hora determinada para conectarse a un servidor, y entonces el colapso inutiliza el servicio. Pero eso no es lo más preocupante. Me preocupa mucho más que 'fisguen'. Que puedan tener acceso a todos los archivos de tu ordenador, sacar información y chantajearte.

–¿Qué se puede hacer para evitar esta intromisión?

–Lo principal es tener un buen antivirus y al día. No tiene por qué ser caro, hay muchos gratuitos en Internet; también es bueno tener adaptado el antivirus para los puertos USB, que pueden ser 'portadores'.

–¿Podemos saber que el ordenador responde a otra persona?

–Cuando la luz de actividad del disco duro –de 'pensar'– parpadea demasiado y con intensidad cuando tú estás haciendo un trabajo que no requiere demasiado esfuerzo al ordenador, como escribir o ver el correo, es para empezar a sospechar...

–Siguiente paso. ¿Cómo nos libramos de este 'secuestro'?

–Actualizar el antivirus y hacer un análisis. En caso de que no detecte nada, si tenemos sospechas fundadas, hay que llamar a un técnico.

–¿Es tan fácil tener 13 millones de ordenadores a tu disposición?

–Si los ordenadores no tienen las defensas adecuadas, se puede tardar una o dos tardes.

–Resulta que había un 'hacker' en Molina... ¿Es fácil que podamos vivir al lado de uno de ellos?

–Pues sí, cualquiera de nosotros puede tener un 'hacker' cerca de su casa. Pero hay que aclarar que un 'hacker' es aquel que es capaz de saltarse la seguridad de un ordenador. Hay buenos y malos. De todas maneras, para ser 'hacker' hace falta tener unos conocimientos avanzados. Algunos sólo son 'hackers' para demostrar lo listos que son. Otros causan daño.

Si el ordenador 'piensa' mucho cuando se está leyendo el correo, hay que empezar a sospechar