



# Los virus informáticos y las rutinas de doble uso

La empresa Computer Economics<sup>1</sup>, con sede en California y dedicada a la investigación de los efectos económicos de los ordenadores y de la informática en general, ha publicado que en el año 2000 las pérdidas causadas por virus informáticos en todo el mundo fueron de 17,1 miles de millones de dólares.

Con la aparición de los códigos Nimda, Sir Cam y Code Red, en el año 2001 se alcanzó un máximo sin precedentes en este tipo de fenómeno informático. Se estima que la contención del Nimda costó 635 millones de dólares en pérdidas de productividad y en los costes asociados a la restauración de los sistemas afectados. En el caso de las distintas versiones del Code Red, el coste estimado fue de 2.620 millones, el Sir Can de 1.150 millones y fueron necesarios otros 875 millones de dólares para detener la expansión del sencillísimo «I Love You».

Las estadísticas publicadas por el CERT indican que en el año 2001 fueron 52.658 los casos denunciados mientras que en el año anterior sólo fueron 21.756, lo que supone un espectacular crecimiento del 242%. Este incremento quizá deba verse desde la incómoda perspectiva de los que tienen que luchar alguna vez con una de estas infecciones<sup>2</sup>, o desde el punto de vista económico pensando en un crecimiento análogo en las pérdidas ocasionadas. Sea el uno o el otro, el caso es que este tipo de «presentaciones apocalípticas» y un tanto «mileneristas» son frecuentes y sistemáticas hoy en día, como si el problema de los virus informáticos fuese algo consustancial a Internet y a la informática civil y democrática.

A pesar de que esté de moda el «alarmismo» en este tipo de temas, hay

**El número de incidentes causados por virus informáticos aumenta con una tasa de crecimiento que ya la quisieran para sus beneficios las cada día más numerosas empresas a las que logra afligir daños de importancia creciente. El ambiente está muy enrarecido con el falso enfrentamiento entre fabricantes de virus y los de anti-virus que sacan sus beneficios del mismo campo de cultivo. El carácter «malévolo» de ciertos códigos no está escrito en ellos sino en la apreciación que de sus acciones tenemos los usuarios, por lo que no es posible distinguir buenos y malos en este escenario de códigos ejecutables. A pesar de todo, el problema de los virus (biológicos) no es nuevo y su solución ya existe, por lo que la informática tiene todavía mucho que aprender de los seres vivos en general, y de sus sistemas inmunológicos en particular.**

algunos especialistas<sup>3</sup> que ponen en seria cuarentena dichos valores ya que las empresas de consultoría dedicadas a producir este tipo de resultados no son muy dadas a contar cuáles han sido los datos y procedimientos seguidos para confeccionar sus informes, lo que deja fuera del método científico a este

*Los sistemas informáticos actuales son un ejemplo planetario de un gran organismo único que carece de cualquier tipo de defensa.*

tipo de «revelaciones» econométricas.

Si no podemos conocer realmente el impacto de los virus o códigos malignos, no debemos enfrentar el fenómeno desde sus aspectos económicos; sin embargo esto es lo que se hace cada vez con más frecuencia.

Las fuentes de este tipo de estudios suelen ser los clientes y usuarios de sistemas informáticos (víctimas), los proveedores de aplicaciones antivirus y los administradores de sistemas. Los clientes, como gente interesada en que funcionen las máquinas y su negocio no se detenga, sólo les importa que los sistemas funcionen y poco más. Los administradores de sistemas son los responsables, dentro de las empresas, de que todo vaya como la seda y, consecuentemente, la cuantía y seguridad de sus salarios dependen de que si algo

va mal sean capaces de arreglarlo eficazmente. Como tercera pata del banco tenemos a las empresas proveedoras de antivirus que, al igual que el flautista de Hamelin necesitaba a las ratas para ganarse la vida, aquellas necesitan la amenaza de los virus para su propia existencia.

Según todo esto, el problema de los virus informáticos es algo bastante serio y resbaladizo. La situación actual beneficia a las compañías de anti-virus y a las exigencias salariales de aquellos nuevos «flautistas» que alquilan a las empresas su experiencia en la retención y erradicación de esas sofisticadas plagas. Sin embargo el problema no alcanza un punto estable y la amenaza aumenta año tras año, lo cual demuestra que el problema sigue abierto y no se puede aceptar que las cosas sigan así; ahora bien, ¿qué se puede hacer?

## La carta de naturaleza de los virus informáticos

El fenómeno de los virus informáticos nace de las mismas raíces que el resto de las aplicaciones informáticas. Los virus de macros en las aplicaciones de Windows Office<sup>4</sup> no se distinguen en

1 <http://www.computereconomics.com/>

2 Narración del ataque mediante virus a CIO <http://www.cio.com/archive/060101/outbreak.html>

3 Ver Michelle Dello: «El verdadero costo de los Virus», por ejemplo en <http://www.wired.com/news/infrastructure/0,1377,49681,00.html> o la lista de promotores al pánico vírico de Rob Rosenberger en Internet <http://vmyths.com/resource.cfm?id=57&page=1>

4 Tomamos este ejemplo no para el escarnio de Microsoft en su proceder a la hora de diseñar y desarrollar sus sistemas operativos o aplicaciones, sino como reconocimiento de su absoluta supremacía en la ofimática planetaria actual.

nada de cualesquiera otros macros que ese sistema permite y que son consideradas provechosas para el usuario de los mismos. Los códigos maliciosos no son en nada diferentes de los que se puedan considerar «*beneficiosos*» por lo que es imposible imaginar, *a priori*, cuales son unos y cuales son los otros. El carácter de un código que ejecuta en los ordenadores actuales es algo subjetivo, por lo que es imposible dar una solución que erradique a los virus informáticos que no sea eliminar las funcionalidades que utilizan y los cobijan. Esta posibilidad no es aceptable ya que, de recurrir a una limitación funcional de los ejecutables actuales (aplicaciones y sistemas operativos), lo que estaríamos haciendo es retrotraer hasta etapas mucho más primitivas a la informática actual.

Si no se puede limitar el software presente y futuro, y no podemos adelantarnos de ningún modo a la imaginación y experiencia de los fabricantes de códigos maliciosos, el problema de los virus informáticos puede parecerse una barrera insalvable; sin embargo no tiene por qué ser así.

Además de la característica destructora o insidiosa que tienen los virus actuales, otra quizá más importante es su **capacidad de difusión** antes de que se pueda desarrollar, distribuir y aplicar el antídoto específico adecuado. En cualquier incidente que estudiemos podremos ver que el problema nace realmente en la capacidad de infección de muchos ordenadores en periodos de tiempo muy cortos.

Con una buena política de salvaguardias, la infección e incluso destrucción de un equipo no llega a ser más importante que la destrucción de un disco duro o de cualquier otro fallo severo del software o del hardware.

Lo que da carta de naturaleza a un virus informático en la sociedad actual es su capacidad de paralizar y/o destruir todo el sistema informático de una empresa y ponerla fuera de juego durante días o semanas. Según esto, el flanco que habría que atacar sería el de la propagación de los virus y de ahí las (incorrectas) campañas para el control del correo electrónico y otros tipos de difusión de ejecutables menos eficientes.

El problema esencial de los sistemas informáticos es que no son tales, sino

que estamos hablando de un mismo y único «organismo» informático. Cualquiera aplicación ampliamente utilizada es exactamente la misma en cualesquiera ordenadores en los que se ejecuta. Una macro de *Windows Office* no distingue en qué ordenador se ejecuta, por lo que el proceso de infección es la misma migración de código de una máquina a otra.

En la evolución de los sistemas vivos hubo que esperar muchos millones de años a que aparecieran los primeros sistemas inmunitarios. En un organismo biológico las reglas de funcionamiento son las mismas, sin embargo, cada uno de ellos es esencialmente distinto gracias a sus defensas inmunitarias. Estamos hartos de oír hablar de la dramática situación de aquellos que necesitan el transplante de un órgano

*Los sistemas operativos actuales tienen mucha responsabilidad en lo que está ocurriendo y sólo en ellos se puede implantar un nuevo modo de hacer las cosas para evitar no a los virus, sino a su capacidad de infectar.*

para seguir vivos.

La compatibilidad inmunológica es una de las cosas que nos hace más individuos y más irrepetibles como seres vivos. Ya es habitual en nuestras vidas conocer lo irremediable de las consecuencias de las «*Inmunodeficiencias adquiridas*» para aquellos organismos que estamos condenados a vivir en un entorno plagado de virus (biológicos). Pues bien, los sistemas informáticos actuales se encuentran, en este sentido, en las mismas fases que la vida cuando no se habían desarrollado los sistemas inmunitarios. Los sistemas informáticos actuales son un ejemplo planetario de un gran organismo único que carece de cualquier tipo de defensa.

### La solución de la naturaleza

La solución que se dio en la naturaleza después de miles de millones de años de selección natural ciega fue hacer de cada ser vivo un compartimento prácticamente estanco en el que sólo podían progresar (ejecutarse) aquellas operaciones que son propias de ese organismo y de ningún otro.

Mientras los ejecutables informáticos no sean, de algún modo, específicos a la máquina en la que están instalados y a la que pertenecen, la migración de los virus, los procesos de infección serán tan rápidos como rápidas sean las líneas de comunicación entre ordenadores, y las consecuencias de los códigos malignos tendrán las magnitudes que hoy empezamos a vislumbrar.

La encrucijada que plantean los virus o códigos maliciosos puede ser la que dé paso a una nueva informática cualitativamente distinta a la que hoy conocemos y somos capaces de imaginar.

Hay que huir de la estéril e interesante dualidad entre fabricantes de virus y fabricantes de anti-virus, ya que en ella el usuario de los sistemas informáticos sólo puede perder tiempo, dinero y toda su información y patrimonio. Hay que huir o, al menos no limitarse, a los enfoques que tienen del problema los nuevos flautistas de Hamelin, y buscar otros procedimientos que pasan por rediseñar la esencia de los sistemas actuales desde el mismo momento en el que se diseñan. Los sistemas operativos actuales tienen mucha responsabilidad en lo que está ocurriendo y sólo en ellos se puede implantar un nuevo modo de hacer las cosas para evitar no a los virus, sino a su capacidad de infectar.

Todos aquellos que en estas recomendaciones vean una excusa óptima para limitar en el futuro las capacidades del software y de los equipos, la universalidad de Internet, o el libre tránsito de códigos o cualesquiera objetos digitales entre ordenadores, que sepan que no han entendido nada y que sus actitudes son el peor de los virus informáticos.

Creo que el problema de los virus informáticos no es la primera vez que se plantea (quizá sí a nosotros como artífices de lo que llamamos informática) y que ha sido magistralmente resuelto por la naturaleza. Tan sólo tenemos que saber leer en lo que ya ocurre a nuestro lado. |

---

JORGE DÁVILA MUÑOZ  
Director  
Laboratorio de Criptografía  
LSIIS - Facultad de Informática - UPM  
jdavila@fi.upm.es