DOMINICALIA

Suplemento dominical. Domingo, 3 de abril de 1988 — HOY — Director: TERESIANO RODRIGUEZ NUÑEZ

LA NUEVA AMENAZA INQUIETA A LOS GOBIERNOS Y A LAS REDES INFORMATICAS

Mi ordenador tiene SIDA

Manuel Calvo Hernando

"Science et Vie" lo ha llamado "el SIDA de los ordenadores". La mayor parte de los otros medios de comunicación de todo el mundo coinciden en hablar de "virus", a pesar de la notoria impropiedad del término, pero alegando sus analogías con la patología del auténtico virus que se instala en una célula para contarminar a las otras. Se trata, en realidad, del último y más grave fenómeno de piratería informática, de algo que de vez en cuando los fabricantes de software incorporan a un programa para presionar a los clientes, pero ahora se ha convertido en una bomba de tiempo (en esta ocasión de carácter lógico), una especie de píldora envenenada capaz de destruir los programas y de saturar las redes.

La gravedad, en función de los objetivos del pirata

La gravedad de este riesgo informático estará en función de los objetivos del pirata. Los daños que pueden producirse son relativamente benignos, como la reducción de la velocidad en la ejecución de programas, o resultar catastróficos y concluir con la destrucción de ficheros y de programas de tratamiento.

Uno de los aspectos más curiosos e inquietantes del fenómeno es que los manipuladores de los programas han incorporado la noción, desgraciadamente actualizada por el SIDA, de portador sano. Así, un disco o una banda magnética son capaces de contaminar a otro ordenador antes de que en el suyo propio se haya observado el daño.

¿Una explosión en Israel el 13 de mayo?

Pero la imaginación de los especialistas no tiene límites, ni para lo positivo ni para lo negativo. Los informáticos temen, pues, nuevas variantes. Se podría sustituir la "bomba" por un envenenamiento progresivo, que ya ha sido detectado, por ejemplo, en la Universidad Hebrea de Jerusalen.

Según "Le Point", este proceso sería rematado por una "explosión" con una fecha concreta: el 13 de mayo de 1988, 40 aniversario de la creación del Estado de Israel, y, por tanto, de la desaparición de Palestina. Entonces, todos los programas contaminados quedarían destruidos.

Hace unos tres años, empezaron a detectarse este tipo de "epidemias" en Estados Unidos, República Federal de Alemania, Israel, Francia y otros países. La que podríamos llamar "contaminación de programas" se basa en la vulnerabilidad de los sistemas informáticos, aún los más protegidos, y consisten en introducir en el programa unas instrucciones caóticas, que permanecen un tiempo sin mostrarse, como la incubación de ciertas enfermedades, y que se multiplican mientras tanto a otros ordenadores, por los habituales intercambios de programas o incluso por vía telefónica.

Preocupación en la Casa Blanca

Hace ya dos años que esta amenaza inquieta a los informáticos y sobre todo al gobierno norteamericano, en cuyas grandes instalaciones se han descubierto ya "virus" que se han multiplicado 300 ó 400 veces, lo que supone un signo de debilidad de estos sistemas, vitales para el país.

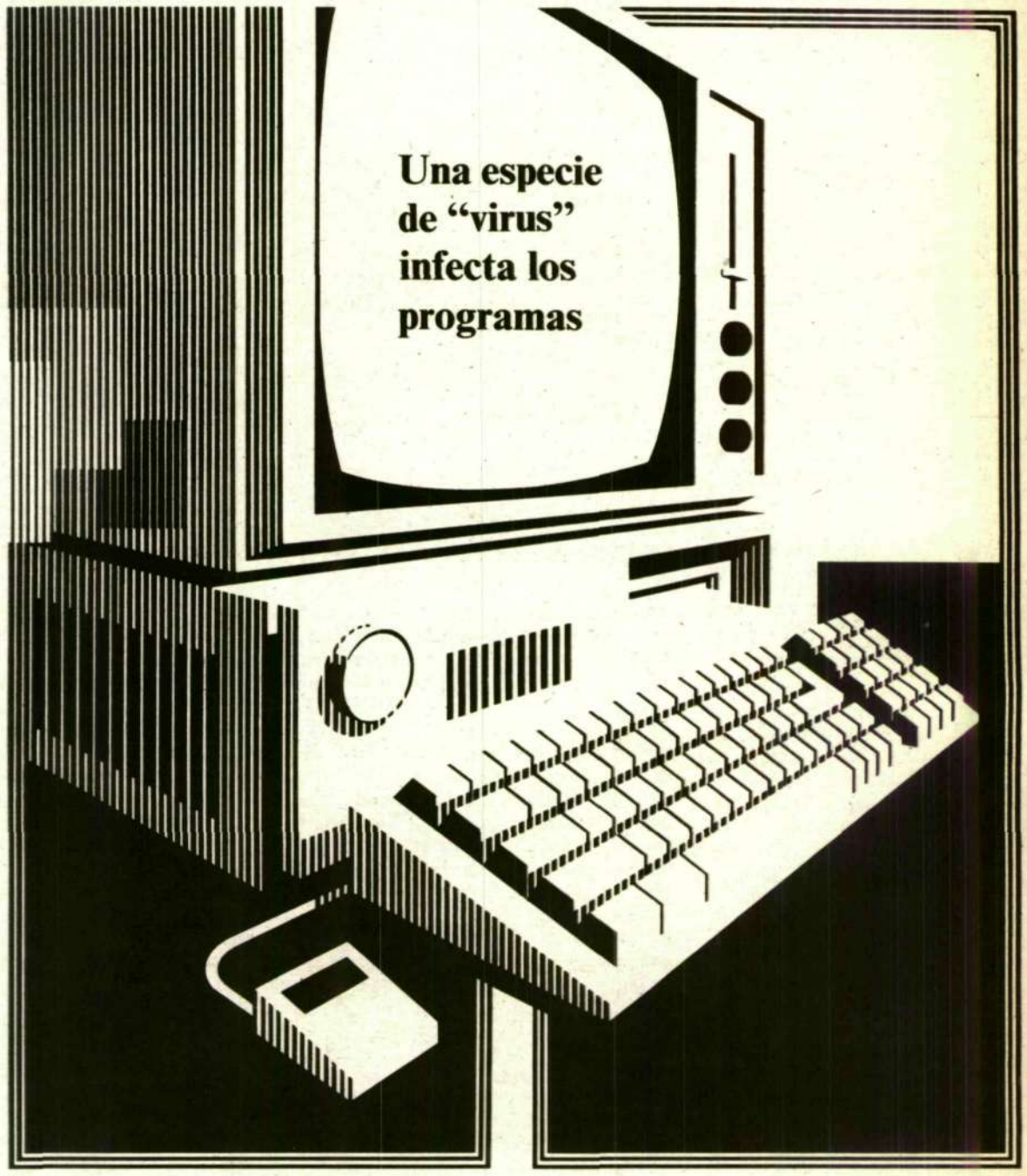
Como dice Henri-Pierre Penel, el problema es internacional, y, teniendo en cuenta el volumen creciente de la comunicación por ordenador, nada se opone por ahora a que una computadora de la Casa Blanca, del Kremlin o de otro despacho de los que gobiernan el mundo, se pueda contagiar con la gripe de..Hong-Kong.

Un club para el caos informático

Son ya numerosos y muy variados los fraudes informáticos y entre nosotros, la Policía Nacional considera la creación de una brigada especializada. El especialista español Luis Camacho anota la sutración de dinero, mercancías, servicios, valores negociables y sofware.

También el robo de información, incluido el espionaje industrial informático.

Otros fraudes se refieren a alterar, borrar, copiar, insertar o utilizar los datos almacenados en un ordenador; establecimiento de "puertas falsas"; recogida de información residual; divulgación no autorizada de datos reservados (la Asociación de Derechos Humanos ha propuesto una ley de protección); el acceso a áreas restringidas; la planificación y simulación de delitos y, por último, los fraudes que ahora alarman a empresas y gobiernos: las "bombas lógicas" (instrucciones no autorizadas para activarse pasado un tiempo) y la introdución de órdenes para que un programa actúe de forma errónea o perturbadora.



Una especie de "virus" infecta los programas

Existen ya casos graves, ocurridos, que nosotros sepamos, en Estados Unidos, Francia y la República Federal de Alemania. En este último país, seis jóvenes penetraron en la red internacional de ordenadores de la NASA y en ocasiones anteriores se han producido ya hechos delictivos.

La mayoría de los autores de estas manipulaciones pertenecen al CCS (Computer Chaos Club), que tiene su sede en Hamburgo, y que presta incluso asistencia jurídica a sus miembros.

Hay que advertir que la mayor parte de las veces estas personas actúan dentro de la ley, teóricamente, y que las autoridades suelen carecer de medios o de experiencia para combatirlos, ya que los autores de los fraudes o de las intromisiones son especialistas muy bien preparados e informados.

¿Soluciones? por ahora, ninguna. Como en el caso de la medicina, se ensayan "programas vacuna" tratar de combatir la nueva piratería informática. Estos programas tienen por objetivo impedir toda nueva carga en la memoria del programa infeccioso, sea cual sea su procedencia. Se piensa también en ensamblar conjuntos de ordenadores, empezando por aquellos que son los más importantes desde el punto de vista estratégico.

Se ensayan «vacunas» para frenar la piratería