Ciberterrorismo. Algunas reflexiones personales

Carlos Jiménez, Presidente de Secuware

Siempre que se escribe sobre ciberterrorismo se tiene la sensación de estar en el filo de una navaja. Describir las debilidades de los sistemas, o las futuras consecuencias de las mismas es convertirse en un mensajero de futuras calamidades. Lo que los siguientes párrafos pretenden es todo lo contrario: evitar que se puedan producir.

El crecimiento de la informática personal en los últimos 25 años ha permitido que los ordenadores se utilicen para todo. Cada día dependemos más de ellos. Y para evitar una interrupción en los sistemas, se utiliza la redundancia. Un centro alternativo que pueda ponerse en marcha si fallan los sistemas principales. Pero esta aproximación tiene un problema: ¿Qué es un fallo de un sistema?. Si es fortuito, es fácil de identificar: si un ordenador se apaga, si un programa no funciona, cualquiera puede darse cuenta de que algo va mal. Pero si es un fallo intencionado, como que un ordenador cambie un digito en un programa de contabilidad una vez cada 10.000 es un fallo prácticamente imposible de detectar. Si un programa le dice al ordenador que haga las cosas mal, las hará mal con mucha eficacia.

Durante los últimos 18 años se han creado unos 150.000 programas maliciosos (virus informáticos, troyanos, spyware, y otra clase de malware), algunos para demostrar vulnerabilidades, muchos con un fin lucrativo, otros simplemente por ego, pero todos tenían algo en común: atacaban los sistemas aprovechando que los ordenadores permiten ejecutar cualquier programa. Si en la vida real, yo obedeciera ciegamente las instrucciones que me diera cada persona con la que me cruzo por la calle, tendría todas las papeletas para ser víctima de un gracioso o de un sinvergüenza.

Pero ahora están todos los ordenadores interconectados a través de Internet, la probabilidad de encontrarse con un sinvergüenza ha aumentado muchísimo. En el mundo real, las amenazas están limitadas por la proximidad física y esto disminuye el riesgo. Pero en un mundo digital hiperconectado, las amenazas pueden venir desde cualquier lugar, y el riesgo se dispara. Afortunadamente las redes de mando y control que se encargan de la seguridad de sistemas militares, por ejemplo, están aisla-

> **"El punto más vulnerable es el ordenador personal. Uno de los cambios, tras el 11-S, es considerar que el ordenador debe dejar de ser personal, y empezar a ser corporativo"**

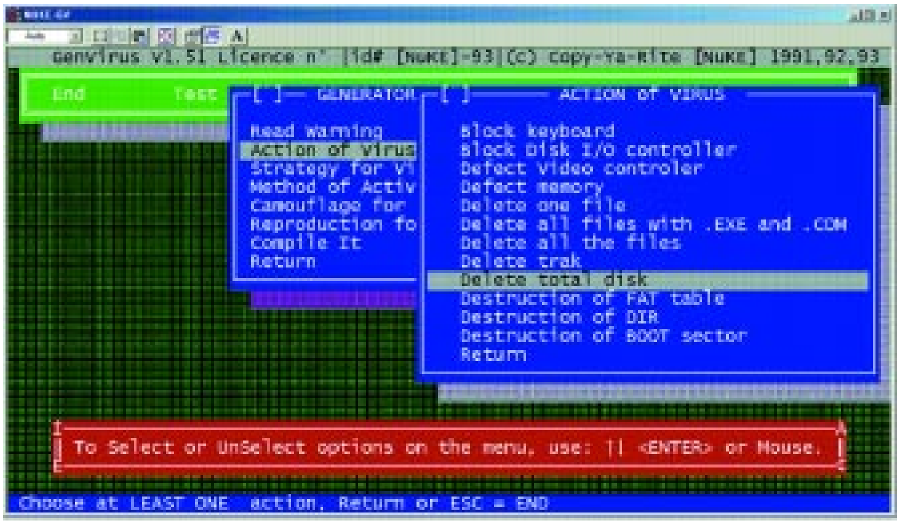
das de Internet lo que imposibilita el ataque externo. Pero otros sistemas críticos, como las centrales nucleares por ejemplo, utilizan ordenadores personales que si están conectados a Internet. Primera recomendación: si tu sistema es crítico, aíslalo de Internet. No sigas la moda de que todo tiene que estar conectado con Internet. Y navega o ten el correo en un ordenador o red aparte que puedas asumir que se puede comprometer. Y haz copias de seguridad, lo más probable es que acabes teniendo problemas.

El problema de un mundo interconectado con ordenadores que ejecutan cualquier cosa es que es una infraestructura atacable desde un lugar remoto y con un ataque generalizado. Mas que un ataque ciberterrorista a la OTAN, si se puede producir un ataque a la economía de un país atacando coordinadamente a miles de ordenadores de empresas de ese país. Los intentos hasta ahora son tímidos, en forma de virus informáticos, que no han perseguido una destrucción indiscriminada. Es más rentable el control remoto del ordenador. Se calcula que más del 80% de los ordenadores contienen software espía. Si tu ordenador contiene algún programa de este tipo, y tiene programado alguna característica destructiva por ejemplo el borrado de la Flash de la BIOS, puede estar esperando a que el atacante remoto simplemente de la orden de activación. ¿Es esto utilizable por el terrorismo internacional?

Creo que la respuesta hoy en día es no. Existe todavía una brecha digital en el terrorismo tradicional, pero es brecha es artificial, existe demasiada gente con el conocimiento para atacar sistemas. Seria relativamente sencillo amenazar o extorsionar a gente con el conocimiento para atacar.

Hace 17 años el autor de este artículo creó el primer antivirus de ordenador, cuando acababa sus estudios de Ingeniero de Telecomunicación. Mi aportación fue crear un sistema en tiempo real que evitaba la ejecución de programas infectados, en lugar de tener un escáner que rastreaba el disco duro buscando virus. Era más eficiente detectar sólo en el momento del riesgo (antes de ejecutar) que perder decenas de minutos esperando a explorar el disco duro. Pero en 1998 vendí Anyware a McAfee porque estaba convencido que el problema que crecía exponencialmente necesitaba otro tipo de solución. Y funde Secuware y creamos el único sistema operativo de seguridad del mundo: SSF. En lugar de detectar 150.000 virus (y creciendo) tiene mucho mas sentido detectar el software confiable, que en una empresa como Time Warner, no llega a 1.000 programas. ¡Es cien veces menos trabajo detectar un programa entre mil que un virus entre 150.000!, pero y más importante, es infinitamente más seguro: sabemos que hacer con cada nuevo programa: aislarlo. Los ordenadores solo ejecutan los programas conocidos. Así funcionamos en la vida real, yo dejo entrar en mi casa a las personas que conozco pero no a cualquier persona, desde pequeños nos enseñan a no hablar con desconocidos. Por si acaso.

El problema es que el sistema más débil será el punto más vulnerable y por el que nos querrán atacar. Hoy en día, el punto más vulnerable es el ordenador personal. Uno de los cambios tras el 11-S, es considerar que el ordenador debe dejar de ser personal, y empezar a ser corporativo. Es decir, es la organización la que controla como debe utilizarse (al fin y al cabo lo ha pagado ella) y no el usuario. Según Microsoft, menos del 10% de los ordenadores se utilizan más allá de aplicaciones puramente ofimáticas. Si consiguiéramos que ese 10% estuviera mejor protegido (en cuanto a manipulación, interferencia en sus datos) por su criticidad y el resto no se pudiera estropear (como nunca se le estropeó a mi padre su maquina de escribir durante 30 años), conseguiríamos reducir muchísimo las posibilidades de un ataque económico.◆



```
Genvirus V1.51 Licence n° [id# [NUKE]-93](c) copy-Ya-Rite [NUKE] 1991,92,93
To Select or UnSelect options on the menu, use: ↑↓ <ENTER> or Mouse.
Choose at LEAST ONE  action, Return or ESC = END
```

Un programa generador de virus puede crear un virus en menos de 3 minutos.