



El bueno, el feo y el malware 2.0

Artículo de opinión
Fernando de la Cuadra

Octubre 2007

Recientemente se ha estrenado una película en la que un terrorista consigue hacerse con el control absoluto de todos (TODOS) los ordenadores de Estados Unidos gracias a un ciberataque. Aparte de esto, la película es interesante, supone un ensayo social sobre nuestra dependencia de los sistemas informáticos.

Afortunadamente no es más que una película de ciber-ficción, ya que incluso se consigue cortar el agua corriente que llega a las casas. Es posible que la gestión del agua esté muy informatizada, pero por ahora no todas las conducciones se manejan exclusivamente mediante Internet. Alguna tubería más antigua queda, estoy seguro.

El ataque, sin embargo, puede venir de otro lado. La fuerza que pueden desarrollar los ordenadores que en este momento se encuentran infectados es muy, muy grande. Basta recordar que ya en enero de 2004 MyDoom consiguió causar problemas a Santa Cruz Operation, ya que el gusano estaba preparado para lanzar un ataque de denegación de servicios contra el sitio web de esta empresa.

Estamos hablando del año 2004. Ahora, en 2007, la situación ha cambiado radicalmente. El malware es muchísimo más abundante que nunca, y el número de máquinas infectadas es muy superior al de 2004. Y no solo en número, ya que aunque hay más ordenadores que en 2004, el porcentaje de ellos con problemas es mucho mayor. Crece el malware, crece el parque informático, crece el peligro.

Y además, también ha crecido un valor que en muchas ocasiones pasa desapercibido: el ancho de banda disponible para sistemas personales. Hoy en día es muy habitual disponer de ofertas de proveedores que empiezan en un megabit por segundo, cifra que hace unos años era astronómica. Tener 4 Mb de ancho de banda en una casa no es excepcional, y en las empresas medianas eso se queda pequeño. Es decir, estamos proporcionando al malware cada vez más capacidad de comunicación.

Según diversas fuentes, en este momento existen más de 2 millones de ordenadores zombis en Asia. Si cada uno de ellos tiene como poco un megabit por segundo de ancho de banda... en Asia puede llegar a utilizarse para fines maliciosos un ancho de banda impresionante. A esto hay que ir añadiendo los más de 20.000 nuevos zombis nuevos diarios, para ir reponiendo los que son detectados o simplemente, mueren en el intento.

Con esa capacidad de ataque, cualquier servicio que dependa de Internet caerá seguro. No hay manera de resistir tan avalancha de información, por lo que podrían caer servicios uno detrás de otro. Las comunicaciones se ralentizarían de forma monstruosa, los servicios de Internet quedarían colapsados.

Pero en el fondo, hay un error de base en estas ciberficciones. ¿A qué hacker le interesa dejar sin agua una ciudad? ¿Quién tiene interés en que las centrales nucleares dejen de funcionar de golpe? Ni siquiera los ecologistas más radicales podrían estar interesados en eso. Como en las novelas de Agatha Christie, para encontrar al culpable basta con saber quién es el que saca más beneficio, y dejar a una ciudad sin luz no proporcionaría beneficios a un hacker.

Los ciberdelincuentes hoy en día no tienen sueños megalómanos de destrucción. Lex Luthor, el villano de Superman, sí los tenía, pero no es más que un personaje de cómic. Hoy en día, mejor que hacerse con el dominio del mundo entero y gobernarlo bajo una dictadura, los villanos quieren obtener dinero, hacer negocios lo más rápida y silenciosamente posible.

Es mucho más rentable conseguir los datos de las cuentas corrientes de varios usuarios u ordeñar esas cuentas corrientes poco a poco. Para esto no hace falta más que unos cuantos troyanos instalados en los sistemas y empezar a manejarlos adecuadamente. Y quien dice unos cuantos dice cientos o miles de datos de cuentas bancarias o tarjetas de crédito para disfrutar del dinero ajeno.

Y esto no es ciberficción. Los datos de infecciones son cada vez más alarmantes, y lo que es peor: los usuarios no saben que están infectados. Todavía se confía demasiado en soluciones antivirus basadas en tecnologías completamente obsoletas, capaces de detectar muchos códigos, sí, pero únicamente los conocidos.

Cuando aparece un nuevo código y llega a un sistema sin capacidad adecuada de protección, hará que el ordenador pase a engrosar la cifra de nuevos zombies. La transformación de un código malicioso conocido en otro distinto es una tarea sencilla, e incluso puede automatizarse para que cada pocos minutos se cree uno nuevo. ¿Pueden los laboratorios detectarlos y ofrecer soluciones cada 10 minutos? Y si lo hacen, ¿se actualizan los usuarios cada 10 minutos? Y si lo hacen, ¿puede su solución manejar detecciones de decenas de megas de manera ágil?

Evidentemente, la respuesta es no a todas las preguntas. La solución a una nueva situación de seguridad no es la tecnología antigua. Hay que dar un paso adelante y empezar a pensar que la tecnología nos puede ayudar, pero necesitamos más. Un solo ordenador no puede encargarse de analizar y procesar todo lo que se le viene encima.

Cuando hace ya muchos años la capacidad de cálculo de los sistemas era tremendamente pequeña, se recurría a grandes centros de cálculo de manera muy habitual, y aún hoy se emplean superordenadores para cálculos sobre predicciones meteorológicas o para analizar el plegado de proteínas. Se recurre a sitios especializados donde los sistemas están a una escala suficiente para macro procesos de cálculo, en donde el número de operaciones por segundo es increíblemente superior a los sistemas normales.

Este mismo esquema de cálculo sirve para la protección contra malware. Ante una avalancha de códigos maliciosos como la que estamos viviendo, un simple PC no puede tener la capacidad de cálculo y proceso necesarias para detectar en milisegundos más de dos millones de códigos maliciosos. Sin embargo, centros especializados en su análisis y detección sí que pueden hacerlo.

Además, en estos centros se cuenta con la ventaja de tener información on line de millones de ordenadores que están mandando datos sobre códigos maliciosos, por lo que se puede tener en tiempo real información sobre las últimas amenazas, incluso la que hace cinco minutos que ha sido creada y solamente ha tenido tiempo de infectar un par de ordenadores.

Por tanto, ante la realidad de la avalancha de malware, podemos contar con la potencia de detección de centros especializados. Ya están disponibles, y gracias a ellos podemos analizar un sistema y descubrir hasta los más recientes códigos maliciosos sin necesidad de esperar a la actualización de mañana. Ese momento puede resultar demasiado tarde.

Fernando de la Cuadra
Community & Spokerperson Manager
Panda Security (<http://www.pandasecurity.com>)
E-mail: fernando.delacuadra@pandasecurity.com