



La gran sospecha

En los primeros nueve días del pasado mes de octubre, en los 196.259 mensajes procesados por el Centro de Alerta Temprana sobre Virus Informáticos ¹ se detectaron 4.791 mensajes contaminados por virus (2,4%); en tres de

cada cuatro casos, el responsable de la infección era **SirCam** ² y detrás de él aparecieron dos versiones del virus de ficheros Magister y también el gusano suramericano **Hybris** descubierto hace ahora poco más de un año. En el mes anterior, el número de mensajes procesados por el mencionado centro fue de algo más de un millón y medio, y un 3,3% de ellos iban infectados por el virus **SirCam** en el 82 % de los casos.

En el momento de escribir este artículo, las noticias alertan sobre una posible reactivación del temido gusano **Nimda**, ya que el Servicio de Inteligencia y Registro de Ataques (ARIS) estadounidense ha descubierto un segmento de código en el **Nimda** que podría reactivarlo a los diez días de su aparición. Su forma de expansión sería la misma, como en muchos otros casos: (1) vía correo electrónico con mensaje adjunto, (2) a través de ficheros compartidos, (3) afectando a servidores *web* basados en el Internet Information Server (IIS) de Microsoft, (4) accediendo a páginas *web* previamente infectadas, etc.

Aunque nos podemos defender de los gusanos como **Nimda** o **Código Rojo** descargando parches y actualizaciones de programas antivirus, la industria del software debe tomarse este problema muy en serio; especialmente a la hora de diseñar las aplicaciones, aunque ello implique mayores costes y tiempos de desarrollo más largos. Con casi total seguridad me inclino a pensar que el actual mercado capitalista y global no tendrá en cuenta estas recomendaciones. A pesar de ello, no podremos echarle toda la culpa de lo que está pasando porque, afortunadamente, la complejidad de Internet crece más deprisa que la capacidad que tenemos de asegurarla; digo «afortunadamente» porque, qui-

La intensidad y sofisticación de los recientes ataques por virus y gusanos a través de Internet se ha llegado, incluso, a relacionar con cosas tan tremendas como los tristes acontecimientos del 11 de septiembre. Esta situación puede tener su origen en el pánico que algunos pocos ven bien en fomentar y muchos tienden a sentir; sin embargo, la situación no está nada clara y es interesante preguntarse por quién se beneficia directa o lateralmente de todo esto.

zá, las soluciones que se están poniendo en práctica pueden llegar a ser peores que la propia enfermedad.

Es cierto que las redes de todo tipo, gubernamentales o comerciales, son vulnerables a los ataques vía Internet y que, según la actual coyuntura político-militar ³, esta fenomenología podría aumentar en intensidad pero no en su gravedad. Alguna empresa española fabricante de antivirus ha llegado incluso a recomendar, nada más caídas las torres gemelas y por lo que pudiera pasar, reforzar las defensas contra la infección por virus y gusanos, o contra Ataques por Denegación del Servicio (**DoS**) a sitios *web*. ⁴

Hasta ahora, se nos ha dicho en y por todos los medios que los recientes conflictos políticos y sociales han inspirado y justificado a *hackers* de todo el mundo para llevar a cabo ataques que, con el paso del tiempo, aumentan en volumen y sofisticación. Sin embargo algo no cuadra; ¿nos están queriendo decir que este miedo generalizado y lo profesional de los ataques está causado únicamente por las acciones de jovencitos hiper-hormonados con problemas de socialización? o ¿nos están queriendo decir, por el contrario, que estos ataques son ya, hoy en día, armas de guerra «relacionables» con vergonzosas masacres como la de las torres gemelas de Manhattan, y que desde hace tiempo nada tienen de juvenil? No puedo creer ninguno de los dos extremos; simplemente, ambos me parecen una tomadura de pelo que ofende al intelecto. Los ataques en Internet se están utilizando como excusa según convenga en cada caso, y eso indica que, en realidad, no sabemos nada de este fenómeno. Dado que nadie nos da hipótesis más verosímiles, tendremos que seguir la

máxima de «buscad entre los beneficiarios a los posibles culpables».


EXCUSAS

Para identificar a los beneficiarios de la actual «inseguridad en la red» me gustaría llamar la

atención sobre la muy seria y nada discreta campaña que se ha levantado en todo el mundo a raíz de los acontecimientos del World Trade Center. Airadas voces han llamado a los atónitos ciudadanos del «mundo libre», del «mundo occidental», de las «sociedades superiores» ⁵ a que permitan y acepten limitar sus derechos como ciudadanos, a que se relaje o elimine la confidencialidad de las comunicaciones privadas, a que se agilice excesivamente la obtención de permisos judiciales para pinchar todo tipo de redes, a que se prohíba o estigmatice el uso de la criptografía y cualquier otra herramienta que favorezca la confidencialidad, etc. ⁶

Se ha dicho que los pilotos suicidas utilizaron Internet para organizar sus macabros planes; sin embargo, según parece, ninguno de ellos cifró sus mensajes, ninguno utilizó teléfonos o líneas particulares, ya que «para eso estaban los cibercafés», y lo digo con ironía. ¿De qué han servido entonces los carísimos sistemas Echelon y Carnivore? Pues para interceptar millones de conversaciones que nada tienen que ver con el terrorismo y mucho menos con el espionaje industrial o militar. ¿Van a prohibirse

1 <http://www.alertaantivirus.es/>
2 Fecha de su Descubrimiento: 17 JUL 2001, Origen: Desconocido, Tipo: Virus por correo-e
3 *Sudan Bank Hacked, Bin Laden Info Found* por Ned Stafford, en Newsbytes 27 Sep 2001 <http://www.newsbytes.com/news/01/170588.html>
4 A pesar de todo, los atentados en Estados Unidos del 11 de septiembre no estuvieron acompañados de virus; una semana más tarde apareció el gusano Nimda infectando a alrededor de 100.000 ordenadores de todo el mundo, 80.000 de los cuales eran norteamericanos, proporción que es habitual.
5 <http://www.elpais.es/articulo/elPaísImpresoInternacional> Fecha 2001 10 01., y también con Fecha 2001 10 02
6 «Los que cambian su libertad por su seguridad no merecen ni libertad ni seguridad». Benjamín Franklin.



los cibercafés? ¿Se va a impedir el acceso anónimo a Internet?

Sería curioso que después de unos cuantos años cruzando el desierto del Sinaí, quizá ahora la tecnología de las PKIs termine por hacer su agosto, por llegar a la tierra prometida. Ya que se habla en voz alta de posibles documentos nacionales de identificación en USA y de inmensas bases de datos con huellas dactilares alimentadas con los datos obtenidos con lectores biométricos puestos en los puertos de entrada a los EEUU. Con esta propuesta de identificación universal, ya podría permitirse el acceso a Internet sólo «con el DNI en la boca»; gran ilusión de algunos administradores de sistemas informáticos.

Cualesquiera de estas u otras medidas similares lo único que va a conseguir

7 en [IRIS-MAIL] ORBZ, *Filtros de los puertos 25 y 80*, 27 SEP 2001 11:41:34

8 Algunos responsables de seguridad de algunas universidades realmente no saben cómo determinar qué es un ataque y qué no lo es, por lo que interpretan la actividad de las máquinas o que ésta ocurra fuera de las horas de oficina, como un síntoma inequívoco de infección y proceden a filtrarlas desconectándola del resto del mundo.

es cargarse todos los derechos de información, de expresión, de reunión, de aprendizaje, de cooperación y, por que no, de ocio, que ha supuesto Internet desde la segunda mitad de la década de los noventa para una inmensa y pacífica comunidad de usuarios. La reacción censora e inquisitorial, que ahora sopla con furia en todos los medios y tertulias, queda claramente representa-

La complejidad de Internet crece más rápidamente que la capacidad de cualquiera para maniatarla en aras de «su seguridad».

da en una curiosa frase de un mensaje aparecido en una lista de gestores de servidores de correo electrónico dentro de RedIris: «**no hay nada como un buen estado de excepción para que le hagan caso a uno en la toma de medidas expeditivas ;-)**»⁷.

Los que se benefician de verdad de los ataques de todo tipo que se experimentan a través de Internet, son todos aquellos intolerantes censores que desean atar más corto a la ciudadanía o a

sus trabajadores, y que prefieren fragmentar y gestionar «la Red de redes» en una constelación de pequeños, despóticos y mezquinos reinos, en los que «la ausencia de tráfico» sea la mejor muestra de que «las cosas van bien y las infecciones no progresan»⁸. Estas medidas no supondrán ninguna ventaja en la lucha antiterrorista, por lo que son inútiles y, además, esto ocurre, para más humillación nuestra, incluso en las redes públicas, en las redes académicas, pagadas peseta a peseta con el sudor de la frente de todos y cada uno de esos ciudadanos a los que se les niegan las ventajas de Internet.

La única esperanza que nos queda a algunos es que, «afortunadamente», la complejidad de Internet crece más rápidamente que la capacidad de cualquiera para maniatarla en aras de «su seguridad». n

JORGE DAVILA MURO

Director

Laboratorio de Criptografía

LSIIS - Facultad de Informática - UPM

jdavila@fi.upm.es