

# Predicciones para el año 2007



El problema de hacer una predicción sobre la seguridad para el año 2007 es que por muy básica y o muy extravagante que fuera, podría verse cumplida. ¿Quién hubiera dicho en 1999 que un virus iba a colapsar Internet y sería portada en todos los periódicos? Loveletter lo consiguió en el 2000. ¿Quién no se hubiera sorprendido si en 2002 hubiera dicho que un gusano iba a colapsar cientos de servidores en menos de un minuto? SQLSlammer lo hizo en Enero de 2003.

Podemos ponernos a intentar imaginar una catástrofe. Conseguir que Internet se detenga es muy complicado, pero es una meta para los hackers. Y podría llevarse a cabo, simplemente con un gusano “silencioso”, que pudiera introducirse en muchos sistemas y a partir de ahí lanzar un ataque en un momento dado.

Pero claro, Internet no es tan fácil de tirar. Sería más factible intentar un ataque de denegación de servicios contra algún servicio vital en Internet. Por ejemplo, un gusano suficientemente extendido que en un momento dado intentara validarse en los servidores de la seguridad social de un determinado país. Simplemente lanzando solicitudes de ingreso a una página de consulta de pensiones el sistema pronto dejaría de poder funcionar hacia el público por la imposibilidad de abarcar tantas peticiones.

En caso de que los servidores estuvieran tan dimensionados como para poder evitar ese ataque, bastaría con encontrar un número adecuado de máquinas que hicieran esa tarea. Simplemente con un par de docenas de redes de bots lanzando varias peticiones por segundo estaría el trabajo conseguido.

Pero evidentemente, esto no va a pasar. Los creadores del código malicioso, los hackers y demás especies no buscan ya otra cosa que dinero por sus fechorías. ¿Para qué se iban a molestar en hacer algo que no les reportara ningún beneficio económico? Si queremos ser realistas, el problema que tendremos el año que viene será el mismo que este: los robos de datos confidenciales de los usuarios para poder operar en los bancos con identidades robadas. Ese sí será el problema, y no una fantasía.

Las técnicas que utilizarán los hackers para el robo de datos confidenciales se refinarán aún más. Por un lado, las técnicas de diseño y programación deberán verse mejoradas, puesto que los sistemas automáticos de detección de phishing son cada vez más potentes, e incluso los navegadores ya contemplan la posibilidad de detectar páginas fraudulentas.

Y por otro lado, lo que deberán mejorar, y mucho, son las técnicas de ingeniería social. Los correos anunciando que nos ha tocado la lotería, o que la viuda de un ex presidente centroafricano nos necesita para evadir capitales están ya muy vistos (aunque parece que son efectivos, dada su proliferación), por lo que aparecerán nuevos intentos de timos. ¿Cuáles? ¡Si lo supiera!

Las empresas deberán extremar las precauciones ante un nuevo tipo de amenaza: los “troyanos únicos”. Los fabricantes de soluciones antivirus clásicas dependen de las muestras de código malicioso que encuentran para poder elaborar una rutina de

# Predicciones para el año 2007



desinfección contra el código malicioso. Pero ¿y si únicamente existe un ejemplar de ese código? ¿Y si un hacker ha enviado al director de una empresa un troyano espía y no lo distribuye más?

La información conseguida en ese ordenador vale su peso en oro (por muy poco que pesen los bits), y las posibilidades de que ese troyano llegue a manos de los investigadores antimalware es muy pequeña, por no decir nula. Permanecerá en ese sistema hasta que el creador se aburra de ese equipo y decida trasladarlo a otro para proseguir su maliciosa tarea.

Mención aparte merecen las vulnerabilidades de los sistemas operativos y de las aplicaciones. Cada nuevo sistema operativo, al igual que un coche nuevo, necesita un cierto tiempo de rodaje (por mucho tiempo en fase beta que haya pasado) en el que sin duda se encontrarán vulnerabilidades. 2007 será el año de Windows Vista, y aunque se anuncie como un sistema seguro, algún problema tendrá. También Windows NT se anunciaba con un nivel de seguridad muy elevado cuando se anunció a primeros de los 90 del siglo pasado.

Poco a poco, irán apareciendo errores, lógicamente, y se irán arreglando con el tiempo. Pero el problema que existirá es el tiempo que pase entre el descubrimiento de un determinado error y el exploit que se aproveche de ese error. Ese tiempo es crítico, y en muchos casos tan pequeño que queda reducido a cero días, en el caso de los “zero day exploits”. Aquí la capacidad de reacción es fundamental, y los sistemas de defensa contra vulnerabilidades se convertirán en piezas fundamentales de la política de seguridad de cualquier empresa mínimamente preocupada.

El spam, los incómodos correos no solicitados, también evolucionará hacia nuevos derroteros. Yo no se tratará de vender dudosas pastillas milagrosas, créditos a bajo precio o ridículas copias de relojes de marca, sino que su finalidad tenderá a hacer rentables otros negocios. Se ha visto ya en el 2006 la efectividad del spam como herramienta para alterar precios de acciones bursátiles, por lo que en el 2007 continuará la tendencia e incluso veremos más sistemas de conseguir dinero fraudulentamente.

Y dirigiéndonos a un terreno más “mundano”, podemos aventurar que continuarán propagándose códigos protegidos con rootkits, que se intentarán crear virus para teléfonos móviles (presumiblemente con el mismo efecto que los conocidos hasta ahora, es decir, casi nulo), que los directivos con portátiles conectados a redes WiFi lo van a pasar mal por las intrusiones cuando se conectan a redes extrañas (en aeropuertos, por ejemplo), que los dialers culminarán su desaparición...

Sin embargo, para todos estos problemas existen soluciones. Si los virus como el “Viernes 13” han conseguido pasar a la historia gracias a soluciones de seguridad antivirus, todos los problemas nuevos que puedan surgir en 2007 también tienen ya sistemas de prevención. Son las tecnologías inteligentes de detección de código malicioso. Son sistemas que simplemente basándose en qué está haciendo un determinado programa lo podrán catalogar como peligroso y detenerlo.

# Predicciones para el año 2007



De esta manera, un troyano único en el equipo del director de la empresa, una intrusión por WiFi aprovechando un exploit “zero day”, un nuevo rootkit intentando llevar a cabo una tarea peligrosa... todos ellos serán detenidos antes de que puedan realmente causar daños.

Para el 2007 se avecinan peligros a escala 2007, ¿por qué no utilizar tecnologías de prevención a escala 2007? Seguir empleando los mismos sistemas de protección que en el año 2000 únicamente nos protegerá de las amenazas que utilicen la tecnología del año 2000.

**Fernando de la Cuadra**  
**Editor Técnico Internacional**  
Panda Software (<http://www.pandasoftware.com>)  
E-mail: [Fdelacuadra@pandasoftware.com](mailto:Fdelacuadra@pandasoftware.com)