

## **Tendencias actuales en código malicioso: Pronósticos para el año 2003**

Elaborado por *Departamento de medición de resultados de TrendLabs*  
*Trend Micro, Inc.*

Como es habitual al final de cada año, en las empresas se debate la planificación del siguiente, siendo uno de los temas principales a qué merece la pena destinar el presupuesto disponible.

De varios estudios que sobre el gasto empresarial se han realizado recientemente se desprende que, por lo menos, ahora figuran en los presupuestos partidas destinadas a la protección de las redes internas, que comprenden antivirus, cortafuegos y adquisición de otros productos de seguridad. La cuestión que continúa pendiente es dar con un método con el que los administradores de sistemas puedan predecir la solidez de sus defensas informáticas y transmitan su punto de vista a la alta dirección.

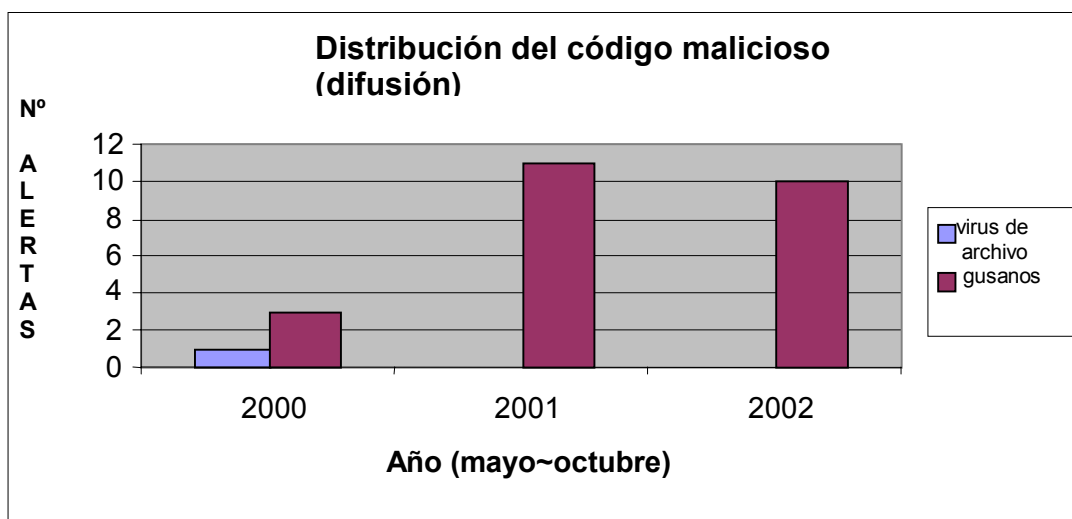
En varias ocasiones se han publicado predicciones relativas a la próxima "bomba" que el código malicioso nos depara para el futuro próximo. Hay que tener en cuenta que la información que se baraja suele pecar de subjetiva por ser incompleta y referida tan sólo a unos meses. Los datos estadísticos referidos a la cantidad de infecciones sufridas en un determinado periodo de tiempo señalarán únicamente hacia dónde se ha extendido efectivamente los virus que han aparecido, pero no qué tendencias se están imponiendo entre quienes los escriben. Para realizar un pronóstico acertado habría que partir además de los brotes víricos reales surgidos en todo el mundo y documentados por los distintos desarrolladores de antivirus, analizando en cada caso cómo se extendió la infección.

Echando un vistazo a los meses con más movimiento en los tres años que van de 2000 a 2002, y en concreto a los meses comprendidos entre mayo y octubre, se observa un gigantesco aumento, del 175%, de los ataques víricos en todo el mundo en 2001 respecto al 2000, volumen que se mantiene en 2002. Sólo esto ya demuestra la necesidad evidente de mejorar en general la capacidad defensiva. La cuestión es cómo.

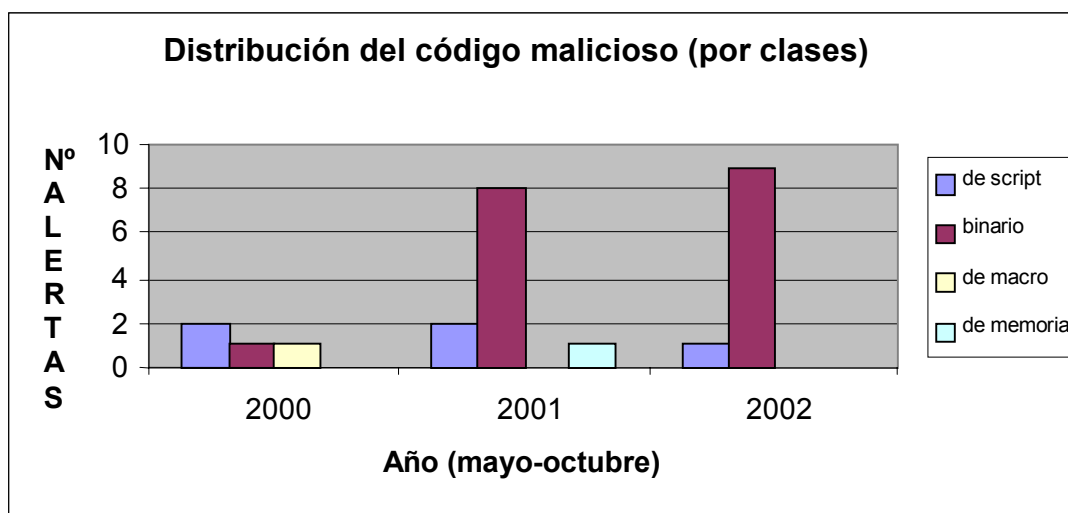
Hasta hace tres años, lo normal era que el código malicioso se expandiese a través de las vías de infección tradicionales: disquetes, ficheros infectados que se enviaban a compañeros y amigos o almacenados en carpetas de acceso común y otras vías similares. Por supuesto, el contagio se producía siempre de forma accidental. Las

infecciones salían a la luz cuando el virus, tras haber ido trasladándose lentamente de un departamento a otro de la empresa infectando archivos a su paso, era detectado en varios puntos al mismo tiempo por un antivirus actualizado, o se daba a conocer presentando ante el usuario su mensaje de presentación.

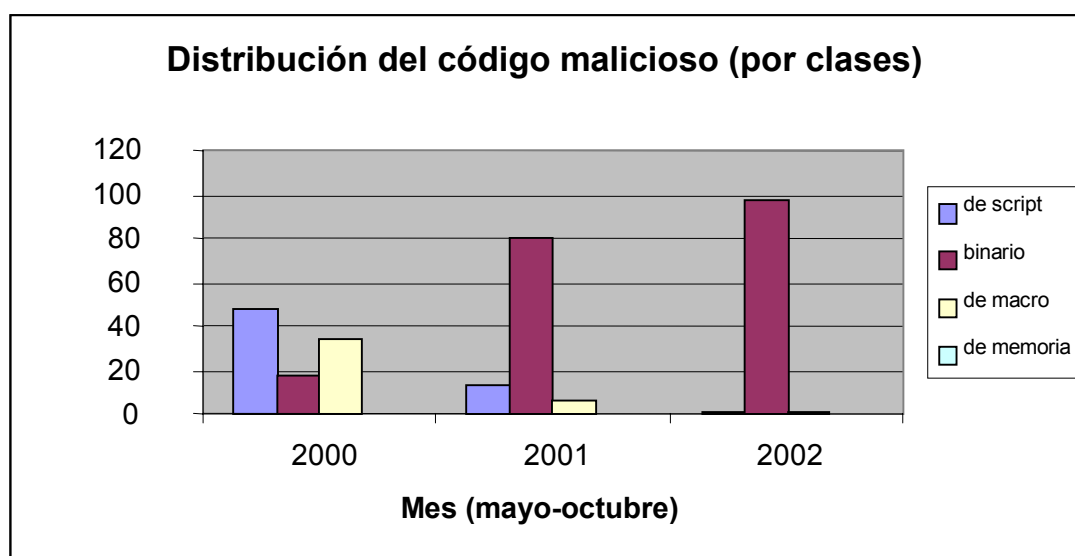
La rápida evolución que han experimentado los gusanos se debe a que los desarrolladores de virus han hallado la manera de propagar sus maliciosas creaciones más rápido y en un mayor número de equipos. Si observamos el mismo periodo de tiempo que teníamos en cuenta hace un momento, veremos que cuatro de cada cinco elementos de código malicioso "en libertad" -in the wild- era un gusano puro. Actualmente, el 100% de los virus detectados presentan rasgos típicos de los gusanos.



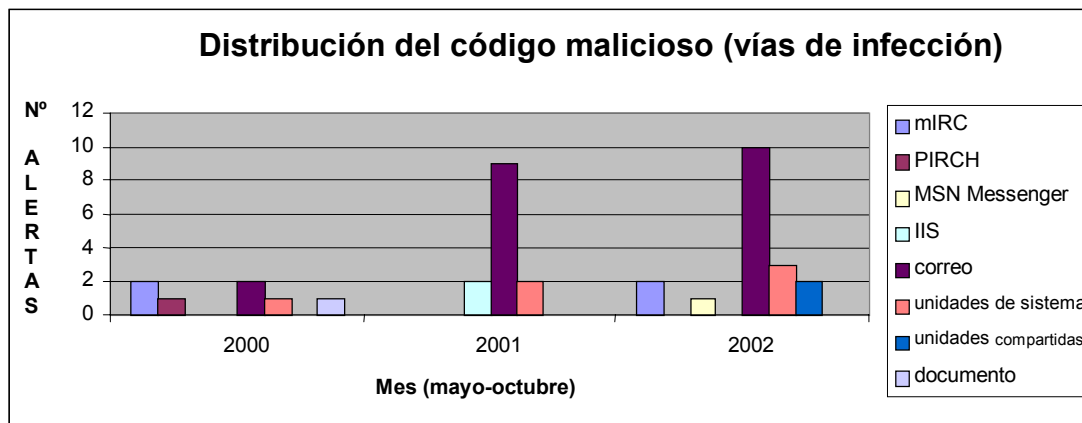
Al examinar más de cerca estos datos, ya desglosados, se advierte que los virus de script y de macro han perdido eficacia, desapareciendo prácticamente de la gráfica a principios del año 2002. La figura siguiente se ha extraído de estadísticas reales elaboradas en TrendLabs, la red de centros de investigación de Trend Micro Inc.



Si expresamos en una gráfica similar datos recogidos por el equipo de la revista Virus Bulletin relativos al mismo periodo de tiempo, se observa que el crecimiento porcentual de código malicioso libre, iequivale en número a las alertas víricas documentadas en los tres años!



El panorama actual del código malicioso informático resulta, por sus características, de lo más variopinto. Por un lado, el IRC resurge en el año 2002 como vía de distribución de código malicioso. Al parecer, hay cada vez más interesados en llevar a cabo la hazaña de aprovecharse de las vulnerabilidades de sistema de servicios de publicación de la red como el IIS de Microsoft o Apache, así como desarrolladores de códigos maliciosos "conceptuales" para el servidor SQL de Microsoft. Otra tendencia muy clara es utilizar como medio de difusión los envíos masivos, las unidades compartidas del sistema y la mensajería instantánea (P2P). El término *amenaza mixta* se ha acuñado para referirse a estos tipos de código malicioso que infectan a través de varias vías al mismo tiempo (ver gráfica siguiente).



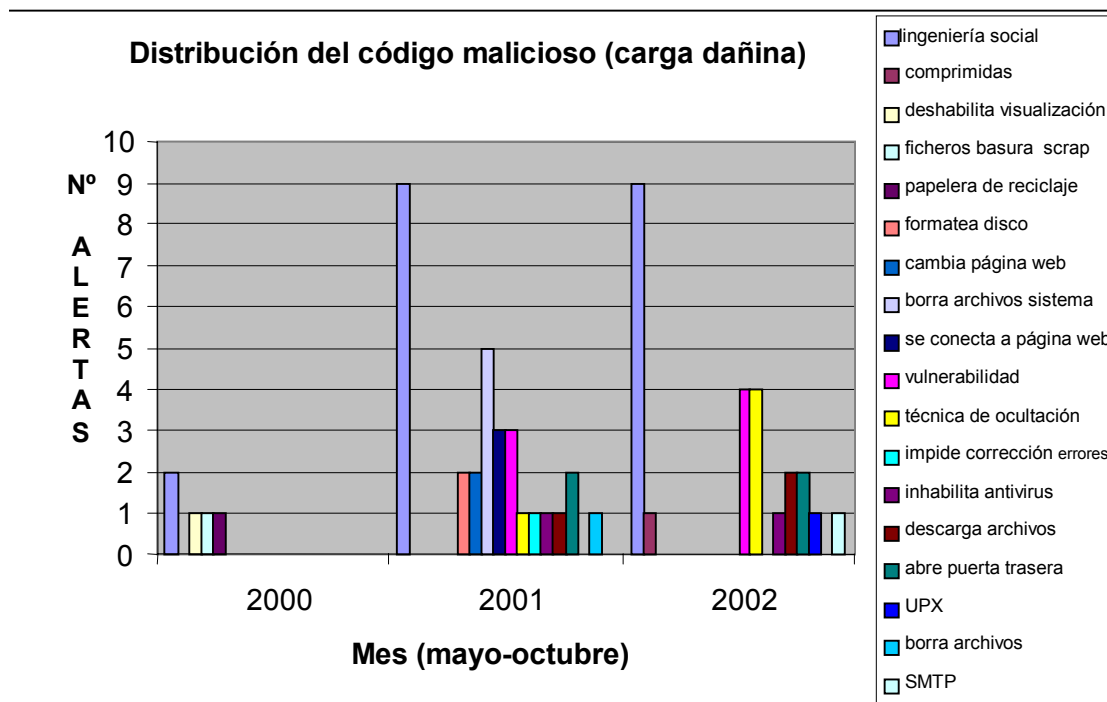
A la hora de concebir estrategias de protección para el futuro, a partir de la información expresada en la gráfica anterior, los administradores deberían tener en cuenta las características particulares que el código malicioso adopta con el fin de sobrevivir cuando penetra en el entorno de una empresa. La mayoría de los gusanos, volviendo a la primera gráfica que presentamos, utilizan mensajes de correo electrónico que simulan venir de amigos o conocidos para convencer a quienes los reciben de que pinchen y ejecuten los archivos que vienen adjuntos.

En el cuadro siguiente se ve que, cada vez más a menudo, la autocompresión y el cifrado complican aún más las cosas, al suponer una dificultad añadida a la hora de analizar los efectos negativos de un elemento de código malicioso. Las vulnerabilidades y errores de programas de uso habitual han demostrado ser el talón de Aquiles de las estrategias de protección, pasando por consiguiente a ocupar un lugar destacado en el arsenal de los hackers o piratas informáticos.

Dependiendo del grado de privilegio que se otorgue a los usuarios en un sistema inseguro, los piratas podrán volver a entrar por puertas traseras para seguir haciendo más daño. Los fabricantes de antivirus o de productos de seguridad poco pueden hacer en estos casos, si los programadores no dan con un parche para el software vulnerable o proporcionan enlaces a soluciones externas.

Otra técnica en auge es la de introducir en los equipos código malicioso autoinstalable que atraiga actualizaciones desde sitios web invadidos por piratas. Un simple enlace unido a código ActiveX puede atravesar tranquilamente el antivirus y el software de filtrado hasta llegar al confiado usuario, que no dudará en hacer doble clic sobre él. Otra característica del código malicioso actual es hacer pruebas de autoconfirmación de su presencia en un sistema, para a continuación deshabilitar y eliminar el antivirus, cortafuegos personal o software antitroyanos que se estén ejecutando en la memoria de la máquina.

Cuando el gran público se estaba acostumbrando a culpar a Outlook y Outlook Express por las infiltraciones que con tanta facilidad sufren, los creadores de virus comienzan a enviar sus desarrollos con su propio protocolo de transporte de correo (SMTP), desvinculándose totalmente de la *interfaz de programación de aplicaciones de mensajería* (MAPI) que emplean los programas de correo de Microsoft. También los escritores de virus aprenden de sus errores y están regresando a los virus en estado puro, eliminando las cargas dañinas. Esta impresión se obtiene al comparar los datos de 2001 con los del 2002, todos en la gráfica siguiente.



Lo importante ahora es saber qué nos espera. De los hechos observados y presentados se infieren claramente los siguientes pronósticos y estrategias, que se irán manifestando a medida que nos adentremos en el 2003:

- La norma seguirá siendo que las redes se vean acechadas por amenazas mixtas.
- El código malicioso actual y el que se cree en el futuro intentará por distintos medios deshabilitar los programas antivirus, cortafuegos personales o incluso antitroyanos que protejan los sistemas.
- Habrá que instalar en las empresas software de filtrado de páginas web o, por lo menos, aplicar medidas que impidan que los usuarios sean redireccionados sin darse cuenta a sitios de Internet que contengan código malicioso.
- Como medida de protección extra seguirán filtrándose los archivos adjuntos a los mensajes de correo. No obstante, los antivirus ubicados en la pasarela de Internet serán más eficaces a la hora de evitar que archivos infectados se cuelen en las redes de las empresas.
- Se recurrirá de cuando en cuando a los tan extendidos canales públicos de mensajería, como el IRC y los P2P, dada la explosión que experimentará la demanda de comunicaciones más rápidas. Sin embargo, la actividad cotidiana en las empresas seguirá lastrada por un sobrecargadísimo volumen de correo electrónico.
- Varios informes de reciente publicación señalan que, al parecer, en menos de cinco años, el 25% del correo electrónico que circulará consistirá en algún tipo de texto promocional no solicitado: dos de cada diez mensajes que entran en los buzones personales.
- Microsoft está apostando fuerte por su plataforma .NET prometiendo que crecerá en muy poco tiempo y que será muy sencilla de integrar en un amplio abanico de dispositivos informáticos. Hasta el momento, ha habido cuatro intentos de crear código malicioso para este nuevo medio, lo que resulta preocupante puesto que, en caso de hacerse realidad, sería código dañino capaz de penetrar en todas las plataformas que admitiesen esta arquitectura.
- Los administradores de sistema deben evaluar cuidadosamente las necesidades de sus redes en términos de software y elegir programas cuyos desarrolladores puedan comprometerse como mínimo a aportar remedios a las vulnerabilidades que puedan

encontrarse antes de que sea demasiado tarde. Ningún fabricante puede afirmar que su software, aunque ha pasado pruebas exhaustivas, funcionará siempre perfectamente.

Por consiguiente, al prepararse para defender mejor las redes que tienen a su cargo, los administradores deberán buscar productos y servicios que ofrezcan, con total seguridad y continuidad en el tiempo, soluciones adecuadas a los problemas que acabamos de plantear.