

# Tendencias del malware para el 2007

Autores:

Ignacio Sbampato, Vicepresidente de ESET para Latinoamérica  
Lic. Cristian Borghello, Technical & Educational Manager de ESET para  
Latinoamérica

Si hace años nos hubiéramos atrevido a decir que los virus informáticos originales tenderían a desaparecer, sin dudas hubiéramos escuchado muchas risas. Sin embargo, esta es la tendencia que continúa marcándose año a año. Todo indica la disminución progresiva de los virus tal y como los conocemos para, lamentablemente, seguir dando lugar a un nuevo tipo de malware más peligroso: aquel que busca el dinero de los afectados.

Los últimos dos años no han sido especialmente novedosos en cuestión de programas dañinos y a menos que algo significativamente importante cambie las bases actuales, todo hace pensar que esta situación se mantendrá: más spam transportando más gusanos y troyanos, más aprovechamiento de la Ingeniería Social y de las redes de intercambio de información, más botnets, más phishing perfeccionando las técnicas actuales, etc.

La cantidad record de vulnerabilidades y bugs corregidos durante el 2006 se debe en gran parte a iniciativas privadas de descubrimiento de agujeros en las aplicaciones más conocidas, como los exploradores, los sistemas operativos y las herramientas ofimáticas.

El aumento de vulnerabilidades 0-day, la irresponsabilidad con que se las maneja y la aparición cada vez más veloz de PoC (Pruebas de Concepto) y exploits para estos agujeros permiten la aparición "espontánea" de gran cantidad de malware debido a que los creadores de los mismos aprovechan las vulnerabilidades y su forma de explotación para aumentar la cantidad de sistemas infectados y por ende sus ganancias económicas.

Esta tendencia ha llegado al tal punto de masificación entre los delincuentes, que actualmente, se venden vulnerabilidades y exploits que se descubren sobre cualquier tipo de sistema como el nuevo Windows Vista de Microsoft.

Por otro lado, la parte social del problema comienza a hacerse relevante y muestra de ello es el aprovechamiento de las comunidades virtuales online, como mySpace, Second Life y juegos como World of Warcraft y Lineage.

Este tipo de comunidades ya se han convertido en lanzadera para nuevos vectores de ataque y han puesto de manifiesto nuevamente que el usuario final es el eslabón más débil de la cadena. Estos ataques ya no aprovechan las vulnerabilidades en los servidores como años atrás, sino de los programas clientes de los usuarios, mucho más numerosos, generalmente más vulnerables y pocas veces parcheados.

Por otro lado, las comunidades virtuales en donde existe la posibilidad de realizar transacciones, pueden ser aprovechadas por programas y personas dañinas para robar estos datos virtuales, venderlos o estafar y lograr dinero real.

En la actualidad, los sistemas operativos Windows de Microsoft son los más utilizados por el común de los usuarios, y por lo tanto, el principal objetivo de los creadores de códigos maliciosos.

A fines del 2006 se lanzó el nuevo sistema operativo Windows Vista, el cual incluye varios cambios en su arquitectura interna que pueden llevar a nuevas técnicas de infección, además de que muchas de

las actuales seguirán vigentes. Cuando este sistema operativo se haga más masivo, seguramente veremos códigos maliciosos que exploten hipotéticas vulnerabilidades.

Además, el crecimiento en la cantidad de usuarios de Linux, Mac OS y otros sistemas operativos llevará a un incremento en la cantidad de malware enfocado a los mismos, dado que se convertirán en objetivos más interesantes para los creadores de códigos maliciosos.

La evolución de la informática lleva a que nuevos vectores de ataque comiencen a ser utilizados para propagar malware. Ante la convergencia actual de tecnologías, se notan las primeras pruebas de concepto para estos nuevos vectores, como pueden ser las plataformas de 64-bit, los teléfonos móviles o la tecnología VoIP.

Siempre que una nueva tecnología global ha aparecido, los responsables del malware han buscado la forma de aprovecharla con fines dañinos y/o criminales.

Por ejemplo, en el caso de VoIP, podremos ver ataques orientadas a grabar las conversaciones con fines de robo de información confidencial y/o suplantación de identidad.

Aunque hasta ahora no se conocen códigos maliciosos de gran proliferación mundial que exploten las amenazas mencionadas, esto es debido a la dispareja implementación de las nuevas tecnologías. A medida que las mismas se conviertan en estándares, veremos un incremento importante en las amenazas informáticas específicas.

A continuación veremos una breve reseña de otras amenazas que podrán verse en los meses sucesivos, muchas de las cuales ya son utilizadas actualmente:

El poder de la distribución de la información ya ha comenzado a dar sus frutos y los creadores de malware no son ajenos a esta realidad. La explotación de la redes P2P para diseminar programas dañinos ya es ampliamente utilizada desde hace años, pero estas técnicas se perfeccionarán con la aplicación de engaños más reales, como es el caso del lanzamiento del "crack universal de Windows Vista" con un troyano.

En el punto anterior notamos que la piratería y el uso de programas ilegales es una de las claves para la propagación de malware, sobre todo en países en donde la tasa de uso de programas ilegales es tan alta como en América Latina. Es fundamental que los usuarios finales y las corporaciones lo analicen y consideren alternativas de solución viables a corto plazo.

El volumen de spam alcanzado parece no tener límites, y eso sucede gracias a las personas inescrupulosas que contratan los servicios de los spammers. La demanda es tal que estos últimos no dudan en usar todas las herramientas disponibles a su alcance para satisfacer las necesidades de sus clientes. Los gusanos y troyanos diseminados mediante spam tienen como objetivo crear grandes redes de sistemas infectados (botnets) para que los mismos sean utilizados para enviar más spam. De no encontrar una solución jurídico-técnica, puede ser uno de los problemas más graves con los que se ha encontrado Internet desde sus inicios.

El perfeccionamiento de técnicas de phishing y vishing será un imperativo para los creadores de este tipo de engaños, pero más lo será la instalación masiva de troyanos bancarios que aprovechen técnicas de modificación de sitios webs, grabación de imágenes y vídeo para poder robar datos confidenciales.

Seguirán prevaleciendo las técnicas de instalación de keyloggers para robo de información que el usuario pueda teclear. A estos se suman el spyware y el adware (generalmente denominados PUP- Potencial Unwanted programs), los cuales seguirán abusando de la confianza del usuario para su instalación y posterior robo de información.

La ya establecida técnica de ocultamiento y modificación de procesos del sistema (generalmente denominada rootkits) se perfeccionará y los programas dañinos comenzarán a aplicar estas técnicas masivamente para dificultar su detección y remoción.

## Conclusión

Como puede verse, la principal preocupación de los próximos años serán las organizaciones delictivas que, cada vez más organizadas, utilizan las redes de información para perpetrar hechos como los descritos para maximizar sus beneficios económicos.

Estas bandas, que trabajan desde distintos países y cumpliendo distintos roles dentro de sus organizaciones delictivas, no dudarán en seguir perfeccionando y agregando nuevas técnicas de ataque a las ya existentes.

Más Información:

<http://www.eset-la.com/>

[http://es.wikipedia.org/wiki/Voz\\_sobre\\_IP](http://es.wikipedia.org/wiki/Voz_sobre_IP)