

# Los mitos en la seguridad



El mundo de la informática está lleno de mitos y de leyendas difundidas por correo electrónico o simplemente comentadas boca a boca. Estas leyendas no son solo los famosos hoaxes o las cartas en cadena, sino que se dan por hecho una serie de cosas que no suelen ser ciertas, pero son tan difíciles de probar que se dan por ciertas sin comprobación ninguna.

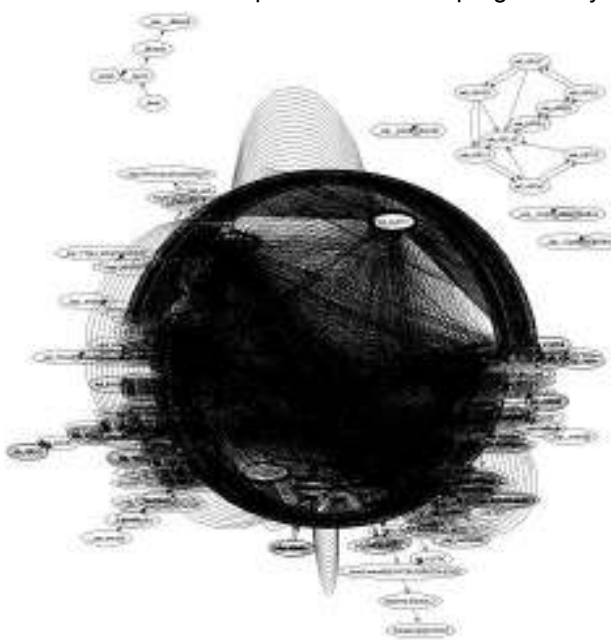
Y dentro del mundo de la seguridad informática, existen también esos extraños mitos. Uno de ellos, con un fundamento real, está cada vez más desvirtuado: los creadores de códigos maliciosos son buenos programadores. Hace tiempo, cuando los virus estaban en su prehistoria, era cierta.

Para que un programa pudiera multiplicarse automáticamente sin que un usuario pudiera darse cuenta y sin que los también prehistóricos programas de seguridad lo detectaran, debía haber sido creado por un buen programador. Era necesario un gran conocimiento de los sistemas, de las posibilidades que brindaban, y tener una gran capacidad de innovación.

Sin embargo, hoy en día estos programadores han dejado de ser esas “estrellas” de la codificación informática. Los códigos maliciosos son cada vez más burdos, con menos innovación y más “chapuceros”.

## El caso de Gaobot.AAF

La afirmación de que los creadores de código malicioso son malos programadores (o por lo menos mucho menos buenos de lo que se piensa) no es gratuita, ya que existen métodos para analizar los programas y ver cómo han sido construidos. Uno



de ellos, muy utilizado por su resultado visual, es la representación de los distintos elementos de un programa mediante grafos. Estos grafos son líneas que relacionan cada subrutina del código, de manera que un programa sencillo y bien construido tendría un grafo simple y claro, mientras que un programa sin organización interna y sin una adecuada sistematización ofrecerá un grafo muy complejo y desordenado.

Además, dos programas similares ofrecerán grafos también similares, lo que ha llevado a PandaLabs, el laboratorio de detección de malware de Panda Software, a utilizarlos para establecer

# Los mitos en la seguridad



similitudes entre distintas variantes de un mismo código malicioso, ya que las llamadas a una misma función dentro de distintos programas se muestran gráficamente en los grafos.

Cuando PandaLabs hizo el análisis de un “bot” (Gaobot.AAF), se sorprendieron con su grafo: no solo por su espectacularidad (le llamaron “La Estrella de la Muerte”, por su parecido a la de “La Guerra de las Galaxias”) sino por su extraña complejidad.

¿Por qué se obtiene este extraño y complejo dibujo? Sencillamente, porque el código fuente original de la familia de bots Gaobot fue puesto a disposición de los creadores de código malicioso, y cada uno de ellos hizo nuevas variantes. Pero esas variantes no estaban optimizadas, por lo que la complejidad iba creciendo en cada variante.

En lugar de demostrar su capacidad como buenos programadores, los creadores de variantes de Gaobot únicamente demuestran que, efectivamente, el mito del gran conocimiento que tienen, son únicamente aprendices de ladrón mediante copias de código ajeno.

## Los virus “indetectables”

Otro mito muy difundido, y alimentado por numerosos correos electrónicos falsos es que existen virus (o gusanos, o troyanos, etc) que no pueden ser detectado por ninguna solución de seguridad. Y desgraciadamente, aunque sea mentira, en ocasiones se airea este mito.

Hace poco apareció la noticia de que un estudiante había creado un troyano con el cual grababa imágenes de las webcam de compañeros de instituto y luego les chantajeaba con el material grabado. Se decía que el troyano creado era “indetectable”.

La afirmación de que un troyano es indetectable contradice esa información, en la que las autoridades crearon un sistema para detectar y eliminar ese código. ¿Es indetectable o no?

El problema radica en la dificultad para detectar un ejemplar determinado de troyano. La mayoría de los fabricantes de soluciones antivirus dependen de las muestras de los códigos maliciosos para poder elaborar una rutina de detección y eliminación, por lo que es necesario que se den dos circunstancias:

1. El código malicioso debe despertar sospechas en un usuario. Si no se muestra un mensaje, o si no se lleva a cabo alguna acción especial en el ordenador que haga al usuario darse cuenta de que algo extraño pasa, el sistema permanecerá infectado ya que no podrá mandarse una muestra a los laboratorios para su análisis.
2. El código malicioso debe tener una cierta propagación. De esta manera aumenta la probabilidad de que alguno de los usuarios afectados notifique a los laboratorios la aparición del código.

# Los mitos en la seguridad



En el caso de este troyano, no se dieron ninguna de las dos, ya que el troyano no mostraba absolutamente ningún mensaje ni daba pistas que pudieran delatarle, prácticamente tal y como hacen todos los caballos de Troya. Y al estar distribuido en muy pocos sistemas (únicamente los de los compañeros de clase del hacker), tampoco se pudo sospechar de él.

Por lo tanto, estamos enfrente de una muestra de la situación del malware hoy en día: ejemplares reducidos y escondidos. Así las empresas antivirus no lo detectarán, tal y como reza la noticia. Sin embargo, esa afirmación no es completa: no lo detectarán hasta que no se conozca.

A pesar de todo, este problema surge únicamente con los sistemas antiguos de detección de códigos maliciosos. Estos sistemas confían ciegamente en los datos almacenados sobre programas maliciosos, sin tener otros sistemas de detección. Así, todo aquello que no esté en su base de datos de firmas de programas, será considerado adecuado.

La tecnología más moderna contra códigos maliciosos evita estos problemas, ya que en lugar de ceñirse exclusivamente en el conocimiento previo de los códigos maliciosos, los busca en función de su comportamiento. Así, un programa que quiera llevar a cabo alguna acción maliciosa en un ordenador, será detenido no porque se le conozca, sino porque las acciones que iba a llevar a cabo.

Mientras que los usuarios sigan confiando en soluciones parciales y anticuadas para la detección de virus y otros programas malignos, no podrán protegerse adecuadamente ya que para ellos seguirán existiendo “códigos indetectables”, en lugar de simplemente “programas peligrosos no conocidos hasta el momento”.

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