

# Estrategia de defensa contra el *malware* dirigido

En los últimos tiempos se viene asistiendo a una proliferación sin precedentes del *malware*. Este hecho resulta preocupante, sobre todo por el creciente grado de especialización y eficiencia del software malicioso. Dentro de esta casuística, y con un impacto económico cada vez mayor, no pocas organizaciones están sobrepasando su umbral de riesgo admisible. Por estos motivos resulta crecientemente necesaria la implantación de una estrategia de defensa contra el fraude y sus daños asociados, causados por este tipo de software malicioso.



José Antonio Lancharro Bervel / Ramón Vicens Lillo

## Aspectos previos y necesarios para establecer la estrategia

Un aspecto crítico de éxito, para llevar a buen puerto la implantación de una estrategia de defensa contra el *malware*, es la integración del mismo dentro de una organización. Para ello, debe analizarse la idiosincrasia de ésta al objeto de engranar los siguientes aspectos:

### 1. Aspectos procedimentales

Resulta necesario contar con la aprobación, por parte de la organización, de una serie de Procedimientos escritos y catalogados en dos categorías:

- Procedimientos orientados a la detección, contención, eliminación y verificación de eliminación de una infección.
- Procedimientos orientados a la restauración de servicios e información corporativa.

### 2. Aspectos humanos

Debe conformarse un equipo de respuesta ante incidentes, pudiendo contemplarse un equipo combinado por personal de la organización y personal de apoyo externo (asesores y especialistas en la lucha contra el *malware*). Dicho equipo debe contar con un mínimo de integrantes para garantizar ciertos niveles de disponibilidad, así como con una clara asignación de roles y responsabilidades, dentro de una cadena de mando bien definida.

Por otro lado, el equipo de respuesta a incidentes debe estar debidamente formado en el uso de las herramientas, así como capacitado en el uso de los procedimientos anteriormente citados.

### 3. Aspectos técnicos

El equipo de defensa contra el *malware* debe contar con:

- Laboratorio de análisis de *malware* equipado, entre otros aspectos, con:
  - Software orientado a la realización de análisis forense.

- Tecnologías de virtualización y/o *sandboxing* para el estudio de comportamientos.
- Disponibilidad de equipos en *standby*.
- Dispositivos de almacenamiento.
- Réplica de las plataformas susceptibles de ser atacadas (servidores, usuarios y clientes fuera de la organización).
- Red de *honeypots* para capturar y estudiar

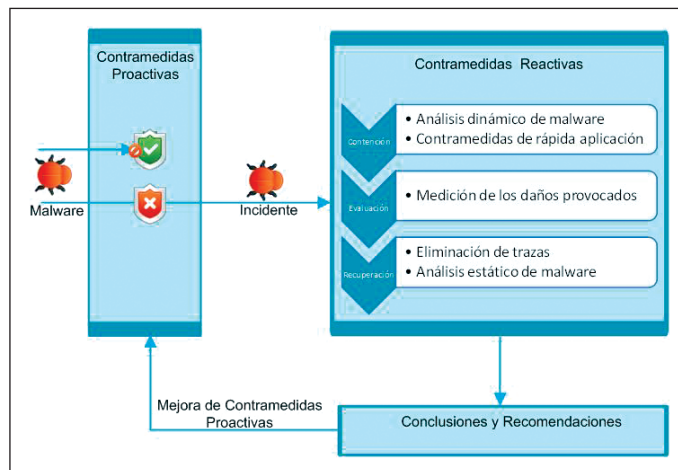


Figura 1.- Mejora continua de la estrategia de defensa contra el *malware*.

**A diferencia del *malware* ‘generalista’, en el que las organizaciones pueden beneficiarse de una detección precoz y contramedidas adoptadas por terceros, el *malware* ‘dirigido’ obliga, en muchos casos, a que sea la propia organización afectada la que inicie el proceso de detección y contención.**

trazas del *malware* existente en la red.

- Mantenimiento de un mapa de la red y una lista actualizada del estado en el que se encuentran los servicios ofrecidos por los sistemas de la red.
- Perfilado de la actividad de red mediante estadísticas, medias, desviaciones típicas y umbrales de normalidad.

Es recomendable la utilización de dos aproximaciones complementarias entre sí, las cuales pueden ser llevadas a cabo para gestionar el riesgo introducido por software malicioso:

• **Aproximación proactiva:** compuesta por mecanismos detectivos y preventivos de seguridad, a nivel de red y de *host*.

• **Aproximación reactiva:** mecanismos correctivos llevados a cabo mediante la puesta en práctica de los procedimientos establecidos tras el descubrimiento de un incidente, como podría ser un caballo de Troya o cualquier otro tipo de *malware*.

## Aproximación proactiva orientada a la defensa contra el *malware*

Las medidas proactivas están orientadas a minimizar la probabilidad de impacto mediante la implementación de controles, focalizados en la prevención y la detección de incidentes de seguridad en los sistemas de información de una organización, como puede ser el parque de servidores y equipos de usuario, tanto dentro de dicha organización como fuera de la misma. En función de las particularidades de cada organización, es recomendable definir una serie de medidas personalizadas, pudiéndose clasificar según las siguientes categorías:

- Definición e implantación de una **política de actualización** de los sistemas de información, ya sea en el nivel de Sistema Operativo o en el de *firmware* para los dispositivos hardware.
  - Implantación de una política fuerte de **segmentación de red**, facilitando de este modo la contención de la propagación del software malicioso que haya podido ser ejecutado.
  - Implantación de una estricta **política de filtrado**, tanto interno como perimetral, para reducir la exposición de los sistemas y, por consiguiente, la probabilidad de infección.
  - En todas aquellas entidades en las que la movilidad de los usuarios sea esencial, se debe disponer de soluciones de **control de acceso a la red** que permitan detectar y aislar

las máquinas de los usuarios potencialmente infectados.

• Disposición de mecanismos de **detección de anomalías**, tanto a nivel de red como de sistema, que generen alertas en función de las anomalías detectadas según:

- Tráfico de red en los diferentes segmentos.
- Perfilado de la actividad de red y de procesos en ejecución, chequeos de integridad, eventos en los sistemas, etc.

• **Configuración segura** de las diferentes máquinas, que permita mantener una ley del **mínimo**

**privilegio en el acceso** al Sistema Operativo por parte de usuarios y aplicaciones.

- **Formación y concienciación** de los usuarios en materia de seguridad, haciendo especial hincapié en los frentes de la ingeniería social asociados al *malware*.

Dado que la correcta implantación de los mecanismos de detección y prevención no son, en muchas ocasiones, triviales, se debe seguir un plan de actuación alineado con una mejora continua, mediante la cual se permita mejorar progresivamente la robustez de la estrategia frente a un ataque (figura 1).

## Aproximación reactiva orientada a la defensa contra el *malware*

Ninguna medida preventiva es infalible, por lo que incluso disponiendo de medidas proactivas sólidas, existe la posibilidad de exposición a ataques, los cuales, aunque con menor probabilidad, podrían tener éxito. Es en esta situación cuando gana protagonismo una aproximación reactiva, orientada a la defensa contra el *malware*, la cual debe contener la infección, erradicar el código malicioso y restablecer la situación de normalidad en sistemas afectados.

En general, la gestión de un incidente relacionado con *malware* se afronta de acuerdo a la siguiente secuencia de pasos:

**1. Contención de daños** provocados por código malicioso.

En el supuesto de que no exista una solución conocida para contener la infección, y que por motivos de negocio no se puedan interrumpir los servicios afectados –como suele suceder en entornos críticos–, blueliv realiza un análisis inicial mediante técnicas de Análisis Dinámico de *Malware*, con el objeto de obtener resultados en el menor tiempo posible. Para ello, deben realizarse las siguientes actividades:

- **Identificar** y extraer un ejemplar del software malicioso.
- **Ejecutar** el ejemplar en un entorno controlado del laboratorio de análisis.
- **Monitorizar** tanto las comunicaciones como los cambios que el *malware* pudiese producir en los sistemas.
- **Analizar** los diferentes comportamientos en un entorno controlado, antes y después de la ejecución, contemplando, entre otros, los siguientes aspectos:

- Actividad de red, con el objeto de trazar un mapa de las comunicaciones realizadas por el código malicioso.
- Procesos de sistema iniciados por el *malware*.
- Cambios producidos en la estructura de ficheros.
- Cambios producidos a nivel de registro (en

entornos Windows).

Estas tareas se realizan dentro de un marco iterativo (figura 2) al objeto de descubrir el mayor número de funcionalidades realizadas por el ejemplar malicioso, mediante la introducción de “cebos” que puedan desencadenar nuevos comportamientos en el mismo, y consecuentemente una mayor comprensión de su comportamiento.

De esta manera, y en un tiempo reducido, se posibilita la definición de las medidas necesarias para contener el impacto producido por el código malicioso analizado, emitiendo una serie de recomendaciones de rápida actuación, que permitan gestionar el incidente de seguridad y mejorar la “aproximación proactiva orientada a la defensa contra el *malware*”, acorde con el Ciclo de Mejora Continua.

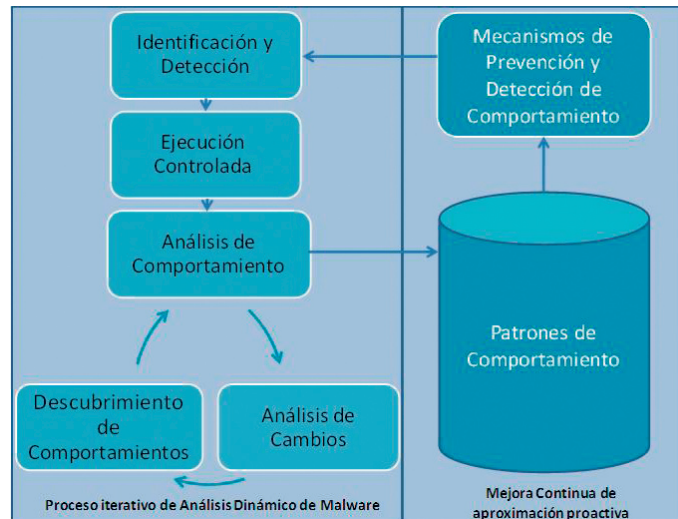


Figura 2.- Sinergias entre aproximación reactiva y proactiva de defensa contra el *malware*.

**2. Evaluación de Daños** producidos en la organización afectada.

Una vez se ha contenido el daño que el *malware* pudiese llegar a ocasionar, y en función del nivel de colaboración que la organización afectada pueda ofrecer, podría evaluarse el daño producido desde distintas perspectivas:

- Impacto económico.
- Impacto reputacional.
- Impacto producido por la no disponibilidad de servicios.
- Impacto producido por la no productividad de personal.
- Impacto ocasionado por la infección en los sistemas de la información afectados.

- Impacto del grado de propagación hacia sistemas externos y/o ajenos a la organización.

## 3. Reparación y Revisión de la infección.

En paralelo a la “Evaluación de Daños”, y en función de la pérdida de disponibilidad e integridad repercutida en los sistemas afectados, se deben aplicar una serie de medidas orientadas al retorno, de forma definitiva, a una situación de normalidad. Estas medidas se fundamentan en revertir todas las alteraciones producidas, en los sistemas afectados por el *malware*. Para ello, se realizan **análisis forenses** sobre los sistemas afectados, así como **análisis estáticos** del *malware*, para obtener un conocimiento detallado, tanto del ejemplar malicioso como del estado de los sistemas afectados. Dichas tareas deben dar respuesta, entre otras, a las siguientes cuestiones:

- ¿Cuál ha sido el vector de entrada del *malware*?
- ¿Cómo se ha comportado?
- ¿Cómo ha afectado a la organización?
- ¿Cómo se ha solucionado?

## Conclusiones

A diferencia del *malware* ‘generalista’, en el que las organizaciones pueden beneficiarse de una precoz detección y contramedidas adoptadas por terceros, el *malware* ‘dirigido’ obliga, en muchos casos, a que sea la propia organización afectada la que inicie el proceso de detección y contención. Sin la estrategia adecuada, es fácil que transcurra un tiempo muy valioso hasta disponer de un conjunto de medidas preventivas eficaces, repercutiendo directamente en un mayor impacto por la incidencia del *malware*.

Aquellas entidades que, sensibilizadas por el riesgo de sufrir ataques dirigidos, pretendan adoptar una estrategia que les permita minimizar el impacto ocasionado, deberán adoptar un modelo de Mejora Continua que les permita evolucionar la estrategia de forma eficiente. ■

**JOSE ANTONIO LANCHARRO BERNEL**

Director Técnico

**BLUELIV**

Joseantonio.lancharro@blueliv.com

**RAMÓN VICENS LILLO**

Consultor de Seguridad

**BLUELIV**

ramon.vicens@blueliv.com

## REFERENCIAS

- <http://blueliv.blogspot.com/>
- <http://www.cert.uy/documentos/pdf/malware-lab.ppt2.pdf>
- [http://zeltser.com/reverse-malware/reverse\\_engineering\\_cheat\\_sheet.pdf](http://zeltser.com/reverse-malware/reverse_engineering_cheat_sheet.pdf)
- [http://www.nebraskacert.org/CSF/CSF-Oct2008\\_example.pdf](http://www.nebraskacert.org/CSF/CSF-Oct2008_example.pdf)
- <http://isc.sans.org/presentations/cookie.pdf>
- [http://www.sans.org/reading\\_room/whitepapers/malicious/malware-analysis-introduction\\_2103](http://www.sans.org/reading_room/whitepapers/malicious/malware-analysis-introduction_2103)