Anti-Malware Testing Standards Organization
(Organización de estándares para la evaluación de programas antimalware)

Principios fundamentales para la evaluación

Disclaimer

This document is a translation of the English-language AMTSO document **"Fundamental Principles of Testing" (version 2008-10-31)** at http://www.amtso.org/documents/doc_download/6-amtso-fundamental-principles-of-testing.html. It is provided in good faith in order to make the concepts clearer to a wider audience. However, we cannot guarantee that it reflects the content of the master version with complete accuracy.

In the event of any conflict or divergent interpretation, the authoritative version remains the latest approved version of the English-language master document on the AMTSO web site.

Principios fundamentales para la evaluación

La siguiente lista es un resumen de los principios que los evaluadores, las publicaciones y los vendedores deben aplicar durante la evaluación de programas antivirus. Estos principios se basan en nuestra creencia de que cada una de las personas involucradas en este tipo de evaluación debe actuar con ética, evaluar adecuadamente y comunicarse en forma justa y precisa. Si desea obtener más información, por favor lea los comentarios para cada punto, que comienzan en la página 2, a continuación.

1. **La evaluación no debe poner al público en peligro.**
2. **La evaluación debe ser imparcial.**
3. **La evaluación debe ser razonablemente abierta y transparente.**
4. **La efectividad y el rendimiento de los productos antimalware deben ser medidos de manera equilibrada.**
5. **Los evaluadores deben tomar la precaución de validar si las muestras o los casos de prueba fueron correctamente clasificados como maliciosos, inofensivos o no válidos.**
6. **La metodología para la evaluación debe ser consistente con el propósito de la evaluación.**
7. **Las conclusiones de una evaluación deben estar basadas en los resultados de la evaluación.**
8. **Los resultados de la evaluación deben ser válidos a nivel estadístico.**
9. **Los vendedores, evaluadores y editores deben tener un punto de contacto activo para recibir correspondencia relacionada a las evaluaciones.**

Principio 1: La evaluación no debe poner al público en peligro.

Éste es un principio fundamental para el estatuto de AMTSO, para su objetivo y para cada uno de sus miembros. El público tiene el derecho de esperar que el desarrollo y la venta de productos antimalware, la revisión de dichos productos y la publicación de esas revisiones se realicen, fundamentalmente, para protegerlos. En consecuencia, el principio más importante en la evaluación de productos antimalware es que ni los productos ni la evaluación que conllevan deben poner al público en peligro. De este principio también se desprende que los evaluadores siempre deben seguir procedimientos adecuados para evitar la liberación accidental de muestras. Además, bajo ningún motivo hay que crear nuevos códigos maliciosos con el propósito de evaluar los productos.

P. ¿Cuáles son los procedimientos que se consideran "adecuados"?

> R. Se espera que todos los entornos de evaluación utilicen las mejores prácticas según los estándares de la industria para asegurar que las muestras de códigos maliciosos no se liberen accidentalmente y que se evite todo tipo de riesgo al público.

P. ¿Qué se quiere decir por "creación de nuevos códigos maliciosos"?

> R. Esta referencia históricamente ha tenido que ver con la creación de nuevos virus o variantes de códigos maliciosos. La primera objeción se basa en el principio de que la cantidad de muestras en el mundo real es más que suficiente para todos. Esta declaración se complicó con la introducción de empaquetadores y máquinas virtuales, generando la pregunta de si el hecho de utilizar estos vehículos cambiaban los códigos maliciosos preexistentes hasta el punto tal de ser considerados "nuevos". Hay razones legítimas para modificar las características de códigos maliciosos existentes con el propósito de realizar una evaluación – de hecho, este principio no se incluye para prohibir ese tipo de evaluación. Sin embargo, para ser claros, este principio se incluye aquí para demostrar la desaprobación unánime de AMTSO respecto a la idea de crear nuevos virus u otros tipos de códigos maliciosos y el riesgo al público que esta práctica conlleva. Si desea contactarse con AMTSO sobre este tema, por favor envíe su consulta a principles@amtso.org para obtener información más detallada.

Principio 2: La evaluación debe ser imparcial.

Nosotros creemos que la evaluación de productos antimalware, por su propia naturaleza, debe ser imparcial – todos los productos deben tratarse de la misma manera. Más allá de que la evaluación sea patrocinada por un vendedor para promover un mensaje de marketing o por una revista importante para publicar un artículo sobre la eficacia de un producto, el evaluador siempre está obligado a llevar a cabo la evaluación en forma ética y a presentar resultados veraces e imparciales.

Existen muchas circunstancias por las que los vendedores pueden otorgar incentivos financieros a una publicación o a un evaluador. Estos incentivos no son inusuales ni poco éticos, y se pueden obtener, por ejemplo, a través de comisiones evaluadoras o para obtener rédito publicitario. Aunque en general son inofensivos, para evitar que sean vistos como algo inapropiado, creemos que estas relaciones, cuando son significativas, deben ser divulgadas. Por lo tanto, para cumplir con este principio, alentamos a los evaluadores y editores a divulgar públicamente cualquier tipo de relación financiera significativa con una de las partes evaluadas o uno de sus asociados.

P. ¿Qué conformaría un incentivo financiero significativo?

> R. La intención de este principio es evitar la parcialidad y el conflicto de intereses en la evaluación de productos y en su comunicación al público. Por lo tanto, la divulgación debe incluir cualquier relación establecida que podría llegar a influenciar al evaluador, lo que incluye: (i) si la publicación o el evaluador ha recibido ingresos de un vendedor o asociado para realizar una evaluación en particular y (ii) si la publicación o el evaluador recibe de un vendedor en particular un porcentaje significativo de los ingresos totales. Aunque se les pida a los evaluadores divulgar la fuente de sus muestras en los detalles de las evaluaciones, el suministro de muestras en general no se considera un incentivo financiero.

P. ¿Cómo se debe hacer esta divulgación?

> R. Lo ideal es que cada evaluador y cada publicación suministren estos datos en una nota al pie en cada informe publicado, o mediante un vínculo u otra referencia para que el público pueda acceder a la información.

Principio 3: La evaluación debe ser razonablemente abierta y transparente.

AMTSO reconoce que algunas publicaciones no siempre estarán de acuerdo con la divulgación de la metodología utilizada para las evaluaciones publicadas. No obstante, AMTSO tiene la firme convicción de que realizar evaluaciones abiertas y transparentes es un elemento crítico para el cumplimiento de estos principios fundamentales y para asegurar la confiabilidad y consistencia en las evaluaciones de programas antimalware. En consecuencia, creemos que todos los resultados divulgados al público deben estar acompañados (o hacer referencia a la ubicación) de detalles sobre la evaluación y la metodología utilizada.

Los detalles sobre la evaluación específica deben incluir la siguiente información:

1. ¿Qué soluciones se evaluaron?
2. ¿Cómo se obtuvieron las soluciones y cómo se actualizaron?
3. ¿Cómo se obtuvieron y validaron las muestras o los casos de prueba? (Ver también el principio número 5.)
4. ¿Qué versiones de los productos se utilizaron?
5. ¿Qué configuraciones se usaron y qué ajustes se hicieron?
6. ¿Cuándo se llevó a cabo la evaluación y bajo qué condiciones?

7. ¿En qué entorno se realizó la evaluación? (Por ejemplo, la versión del sistema operativo/entorno operativo, los *Service Pack* instalados, y otros programas activos en ese momento.)

Los detalles sobre la metodología de evaluación específica deben incluir la siguiente información:

1. ¿Cómo se seleccionaron las muestras o los casos de prueba?
2. ¿Cuáles fueron las fuentes de las muestras o los casos de prueba maliciosos e inofensivos?
3. ¿Cómo se aplicaron las muestras o los casos de prueba maliciosos e inofensivos?
4. ¿Cómo fue la respuesta de las soluciones comparadas?
5. ¿La evaluación comparó tipos de productos y funcionalidades similares o comparó tipos de productos y funcionalidades significativamente diferentes?
6. Si la comparación fue de productos diferentes, ¿cómo se compararon las diversas soluciones?
7. ¿Cómo se calcularon e interpretaron los resultados?

P. ¿Dónde se debe divulgar la evaluación y la metodología utilizada?

> R. Lo ideal es que esta información se incluya en el informe publicado, ya sea en el cuerpo del informe o mediante un vínculo a la información relevante. Si las publicaciones no tienen la posibilidad o no desean incluir esta información, los mismos evaluadores pueden dejarla disponible en su sitio Web haciendo referencia a una evaluación específica o general.

P. ¿Es necesario que los evaluadores suministren retroalimentación y/o muestras a los vendedores?

> R. No. Sin embargo, AMTSO prefiere que los evaluadores les suministren a los vendedores una retroalimentación adecuada y constructiva en un lapso de tiempo razonable y aceptable sobre fallas específicas y deficiencias (por ejemplo, colapso del programa, falsos positivos, falsos negativos, etc.). La retroalimentación puede llevarse a cabo enviando detalles técnicos, secuencias de pasos llevados a cabo para su reproducción, archivos de registro, vuelcos de memoria, muestras, etc.

Principio 4: La efectividad y el rendimiento de los productos antimalware deben ser medidos de manera equilibrada.

Es difícil resumir la eficacia de un producto con una única medición – lo que puede inducir al error. Se espera que los evaluadores presenten mediciones múltiples del rendimiento de los productos en diversas áreas para que los usuarios puedan tomar una decisión contando con información suficiente.

Por ejemplo, los evaluadores deben equilibrar en forma apropiada los casos de prueba correspondientes a falsos negativos y falsos positivos. Un producto que detecta con éxito un alto porcentaje de códigos maliciosos pero que lamentablemente tiene una alta

tasa de falsos positivos quizá no sea “mejor” que una solución que detecte menos códigos maliciosos pero que genere menos falsos positivos.

Principio 5: Los evaluadores deben tomar la precaución de validar si las muestras o los casos de prueba fueron correctamente clasificados como maliciosos, inofensivos o no válidos.

Muchas veces ha ocurrido que resultados de evaluaciones que parecían confiables en realidad no eran válidos porque las muestras utilizadas en las evaluaciones no habían sido bien clasificadas. Por ejemplo, si un evaluador determina que un producto tiene una tasa elevada de falsos positivos, ese resultado puede ser erróneo si algunas de las muestras fueron clasificadas como “inofensivos” en forma equivocada. Por lo tanto, nuestra posición es que hay que tener la precaución razonable de categorizar las muestras o los casos de prueba, y en particular alentamos a los evaluadores a revalidar las muestras o los casos de prueba que hayan provocado resultados de falsos negativos o falsos positivos.

De manera similar, hay que tener la precaución de identificar muestras alteradas, que no funcionan, o que sólo son maliciosas en ciertos entornos o bajo condiciones específicas.

Principio 6: La metodología para la evaluación debe ser consistente con el propósito de la evaluación.

Las evaluaciones deben estar orientadas al propósito intencional o explícito del informe o artículo correspondiente publicado. Creemos que los editores deben indicar el objetivo de sus evaluaciones en forma explícita, y que la metodología empleada debe ser consistente con el objetivo indicado. (Por ejemplo, publicar los resultados de una evaluación en una revista orientada al público general sin aclarar que la evaluación se realizó sobre productos corporativos que no se corresponden con la experiencia del usuario general.)

Para más información sobre el tema, David Harley ha publicado un *paper* donde analiza en detalle los problemas que surgieron en una evaluación que demostró tener inconsistencias entre el objetivo de la evaluación y la metodología utilizada.

Ver http://www.smallblue-greenworld.co.uk/AV_comparative_guide.pdf

Principio 7: Las conclusiones de una evaluación deben estar basadas en los resultados de la evaluación.

Este principio alude a un problema serio que consiste en publicar conclusiones junto a datos de la evaluación, pero que no se basan en esos datos. (Por ejemplo, llegar a conclusiones amplias y/o inapropiadas basándose en datos restringidos.)

Principio 8: Los resultados de la evaluación deben ser válidos a nivel estadístico.

Los evaluadores deben usar una cantidad suficiente de muestras, casos de prueba o escenarios para que los resultados sean válidos estadísticamente. Además, el análisis que hace el evaluador sobre los errores en la medición es importante y debe ser publicado. En general, AMTSO recomienda usar la mayor cantidad de escenarios de prueba como sea posible.

Para más información sobre el tema, Igor Muttik ha publicado un *paper* donde analiza en detalle la manera en que el uso de una cantidad insuficiente de muestras o casos de prueba puede generar resultados aleatorios en una evaluación.

Ver: http://www.mcafee.com/common/media/vil/pdf/imuttik_VB_conf_2001.pdf

Principio 9: Los vendedores, evaluadores y editores deben tener un punto de contacto activo para recibir correspondencia relacionada a las evaluaciones.

Un “punto de contacto activo” es un punto de accesibilidad actual y verificado en forma regular (por teléfono, fax o correo electrónico) suministrado por los vendedores, departamentos de relaciones públicas, evaluadores y editores. El vendedor, evaluador o editor debe responder la correspondencia relevante sobre el producto, la evaluación o la metodología utilizada dentro de un lapso razonable de tiempo.