



LIBRO BLANCO

El software sin licencia y las amenazas a la seguridad informática

Patrocinado por: BSA | The Software Alliance

John F. Gantz
Thomas Vavra
Victor Lim
Enero de 2015

Pavel Soper
Profesor Lars Smith (Universidad de Louisville)
Stephen Minton

INTRODUCCIÓN

En este documento se analiza la relación entre el uso del software sin licencia y el riesgo de que esté infectado por códigos maliciosos conocidos como “malware”. De este análisis se desprenden tres conclusiones: en primer lugar, que existe una fuerte correlación entre ambas variables; en segundo lugar, que el uso de software ilegal es un fuerte “indicador” de que se encontrará malware y, en tercer lugar, que existen pruebas empíricas de esta relación causa/efecto.

Desde hace tiempo los analistas saben que existe una conexión entre el software sin licencia y las amenazas a la seguridad cibernética. Por ejemplo, cuando el gusano Conficker se diseminó por las computadoras de todo el mundo en 2008 y 2009, los expertos en seguridad advirtieron que descargar software ilegal era una de las principales vías de contagio.¹ Unos años después, al desactivar la red de PC con malware conocido como Citadel (que creó 5 millones de computadoras zombies en 90 países), se descubrió que los delincuentes que la habían creado habían infectado las PC en parte vendiendo versiones ilegales de Microsoft Windows previamente infectadas con ese malware.² Es por eso que en 2013 a nadie sorprendió que el FBI emitiera un alerta al consumidor que advertía que el software ilegal podía contener malware.³

Sin embargo, aún no se ha realizado ningún análisis estadístico exhaustivo de la conexión que existe entre el software ilegal y las amenazas a la seguridad causadas por malware. Por ese motivo, la alianza Business Software Alliance (BSA) solicitó a IDC que examinara la evidencia. Los resultados de ese análisis sugieren que las políticas públicas y las mejores prácticas empresariales que garantizan que el software cuenta con su debida licencia van a mejorar la seguridad de los entornos informáticos.

¹Consulte la publicación en el blog sobre seguridad de Krebs del 20 de junio de 2011 titulado “*Software Cracks: A Great Way to Infect Your PC*”, y comentarios relacionados, en: <http://krebsonsecurity.com/2011/06/software-cracks-a-great-way-to-infect-your-pc/>.

²Se puede leer un breve informe acerca de la desactivación de Citadel en el sitio Web de BBC News en un artículo del 6 de junio de 2013 titulado “*FBI and Microsoft take down \$500m-theft botnet Citadel*”. Consulte también: <http://www.bbc.com/news/technology-22795074>.

³Publicado en agosto de 2013 y disponible en <http://www.fbi.gov/news/stories/2013/august/pirated-software-may-contain-malware>.

CÓMO SE DETERMINA LA CORRELACIÓN

Para analizar la conexión que existe entre el software ilegal y las amenazas a la seguridad, IDC analizó índices de uso de software pirata y de amenazas a la ciberseguridad en 81 países donde existen datos fidedignos sobre ambas variables.

Los índices de software ilegal provienen de la *Encuesta global sobre software*, un estudio bienal que IDC lleva a cabo para BSA,⁴ y la información sobre las amenazas a la seguridad cibernética proviene del *Informe sobre inteligencia de la seguridad* de Microsoft,⁵ que analiza la actividad de 600 millones de computadoras por mes. La métrica elegida para este Libro blanco fue la *tasa de incidencia*, que es el porcentaje de computadoras que ejecutan software de seguridad Microsoft en tiempo real y donde se ha encontrado malware en un trimestre. Para tener una idea, alrededor del 20 % de las PC de todo el mundo denunciaron haber encontrado malware en todos los trimestres de 2013.⁶

La Figura 1 muestra los puntos de datos tanto para el índice de uso de software pirata y la prevalencia del malware encontrado en cada uno de los 81 países para los cuales había datos disponibles sobre ambas variables en 2013.

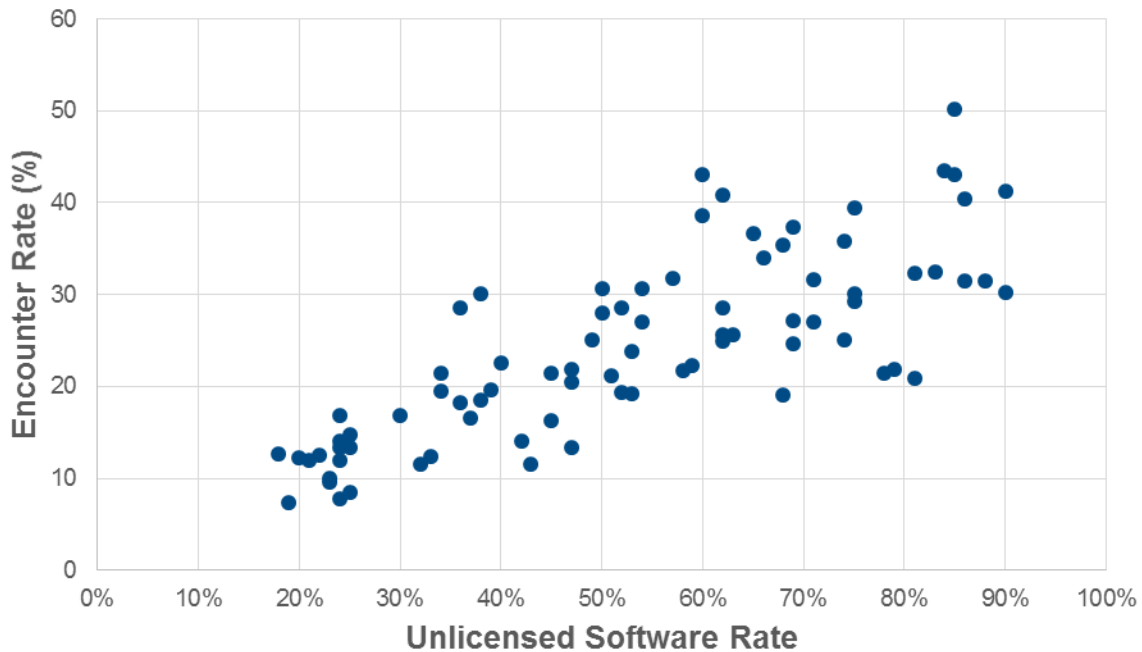
⁴Encuesta global sobre software de BSA: La brecha en el cumplimiento, junio de 2014, disponible en <http://www.bsa.org/studies>.

⁵En los volúmenes 15 y 16 se describen los datos y de la metodología, y se encuentran disponibles en <http://www.microsoft.com/security/sir/default.aspx>.

⁶¿Esta es acaso la mejor medición para las amenazas a la ciberseguridad? Hay otras, publicadas por empresas como Cisco, IBM, Kaspersky, Microsoft, Symantec, Trend Micro y Verizon, además de equipos gubernamentales y de respuesta ante emergencias informáticas, pero la mayoría, si es que tienen información específica del país, analizan los orígenes y no los destinos. Usar una métrica diseñada para PC y empleada en muchos países también resulta interesante para compararla con una métrica basada en el uso de software para PC.

FIGURA 1

Los índices de software ilegal y la incidencia de malware están íntimamente relacionados



Cada punto representa un índice individual de un país del uso de software ilegal y la prevalencia de PCs infectadas con malware (en el Anexo figuran los datos completos). El patrón representa una correlación de fuerte poder estadístico de 0,79 entre ambas variables.

Fuente: IDC, 2015

Ambos valores muestran una clara tendencia ascendente: cuanto más alto es el índice de software pirata en un país, mayor es, por lo general, el número de PC contaminadas con malware en ese país.

Por ejemplo, en 2013, el índice de software pirata para los Estados Unidos fue del 18 % y la tasa de malware encontrado fue del 13 % por trimestre. Para Indonesia, el índice de software pirata fue del 84 % y la tasa de malware encontrado fue del 44 % por trimestre. Brasil, con una tasa de software pirata del 50 %, tuvo una tasa de incidencia de malware del 31 % por trimestre.

El análisis estadístico confirma que los dos conjuntos de variables tienen una fuerte correlación entre sí, lo que significa que suben o bajan al mismo tiempo. El coeficiente de correlación en este caso es de 0,79 (1 representa una correlación perfecta y 0 significa que no hay correlación). A modo de

comparación, la correlación entre el consumo de cigarrillos y el cáncer de pulmón es de 0,72,⁷ la correlación entre la educación y los ingresos es de 0,77,⁸ y la correlación entre las políticas anticorrupción y el crecimiento económico es de 0,77.⁹

Si bien esta correlación no ratifica ni refuta la relación causa/efecto, sí muestra claramente que cuanto más bajos son los índices de software pirata, menos son las PC contaminadas con malware.

LA CONSTRUCCIÓN DE UN MODELO PREDICTIVO

El siguiente paso en el análisis fue desarrollar un modelo para mostrar con qué nivel de exactitud se podrían utilizar los índices de software pirata para *predecir* la incidencia del malware. Para ello, los autores utilizaron una técnica estadística que se llama “análisis de regresión”, por la cual se utilizan los conjuntos de datos para obtener una fórmula en la que una variable (el índice de software pirata utilizado) puede predecir la otra (la tasa de PC infectadas con malware).

La Figura 2 muestra los resultados de ese análisis. Si la fórmula funcionara bien, todos los valores se encontrarían sobre la línea. Si la fórmula no funcionara, los valores quedarían dispersos al azar. En este caso, la mayoría de los valores están agrupados cerca de la línea, con un fuerte valor predictivo desde el punto de vista estadístico (conocido como R cuadrado) de 0,62, lo que significa que el modelo funcionó bastante bien. Se puede interpretar que el 62 % de la variabilidad entre la tasa de malware encontrado en un país y en otro se puede atribuir a la variabilidad en los respectivos índices de software pirata en esos países.

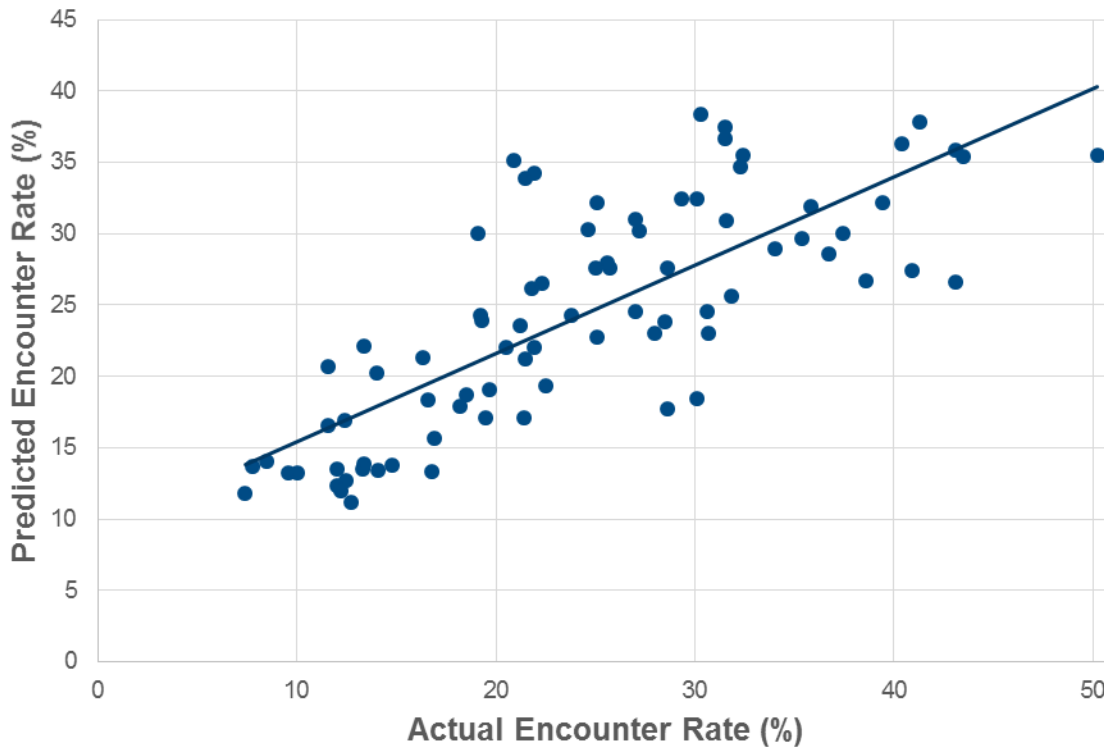
⁷Se trató de un estudio llevado a cabo por el gobierno de Inglaterra que analizó la cantidad de cigarrillos fumados por día en comparación con las tasas de cáncer de pulmón entre miles de hombres pertenecientes a 25 ocupaciones diferentes. Se puede consultar un resumen en <http://www3.nd.edu/~busiforc/handouts/Data%20and%20Stories/correlation/smoking%20and%20cancer/smoking.html>, y un detalle de los cálculos utilizados para obtener el coeficiente de correlación en <http://www.spcforexcel.com/correlation-analysis>.

⁸International Education Statistics, por Friedrich Huebler, agosto de 2008, disponible en <http://huebler.blogspot.com/2005/09/national-wealth-and-school-enrollment.html>. Correlación de Pearson, por IDC.

⁹Consulte el documento de publicaciones de la OECD sobre corrupción y crecimiento económico en <http://www.oecd.org/g20/topics/anti-corruption/issues-paper-on-corruption-and-economic-growth.htm>.

FIGURA 2

El uso de software pirata es un fuerte indicador de PC contaminadas con malware



Cada punto representa el índice de uso de software sin licencia en un país individual y la tasa de incidencia de malware que se predice para ese país (en el Anexo figuran los datos completos). El patrón muestra un fuerte valor predictivo desde el punto de vista estadístico (R cuadrado) de 0,62 entre el uso de software pirata y las PCs infectadas con malware.

Fuente: IDC, 2015

EVIDENCIA DE LA RELACIÓN CAUSA/EFEECTO

No sorprende que el uso del software ilegal y la incidencia del malware estén estrechamente relacionados, ni que un análisis de regresión determine que lo primero sea un fuerte indicador de lo segundo. Sin embargo, estos hallazgos no son suficientes para probar que reducir los índices de software pirata también disminuiría las tasas de incidencia de malware. Para llegar a esta conclusión, hay que considerar el análisis estadístico en el contexto de que existe una fuerte evidencia *empírica* de una relación causa/efecto.

Para comprender bien este concepto, es posible que dos variables tengan un alto valor de correlación pero un bajo valor predictivo en un análisis de regresión. Esto sucede cuando la correlación es una mera coincidencia. Por ejemplo, hace tiempo que se sabe que existe una fuerte correlación entre las

ventas de cremas heladas y las tasas de homicidios en los Estados Unidos, y es obvio que una cosa no es causa de la otra (aunque el calor puede ser causa de ambas).¹⁰ Aquí, sin embargo, lo que hay es evidencia causal.

Por ejemplo, en 2014, IDC llevó a cabo un estudio junto con la Universidad Nacional de Singapur (NUS)¹¹ que descubrió enormes cantidades de malware en software ilegal en más de 800 PC compradas con software ilegal preinstalado, o en DVD piratas, y en software y claves de activación ilegales descargados de Internet. Las pruebas se realizaron en una decena de países en Asia, Europa y las Américas. Conclusión: en promedio, un usuario de un paquete de software sin licencia tiene una probabilidad de uno en tres de encontrar malware.

Esta tasa de contagio multiplicada por la cantidad de paquetes de software ilegales en el mundo sugiere que hay más de 500 millones de paquetes infectados en circulación. (La investigación también reveló que más del 40 % de los consumidores no tenían instalaciones automáticas de de seguridad, lo que también puede facilitar las infecciones de malware en las PC.)

En una encuesta sobre casi 1000 PC localizadas en 15 países, el estudio de IDC-NUS reveló que 1 de cada 5 encuestados dijo que el software ilegal infectó sus PC con un virus; 2 de cada 5 declararon que el software reducía la velocidad de la computadora y debía ser desinstalado (un posible signo de malware oculto), y 1 de cada 10 informó que el software destruía archivos.

A la luz de esta evidencia, no es de extrañar que la *Encuesta global sobre software* de BSA de 2013 revelara que para los usuarios de computadoras en todo el mundo el riesgo de amenazas a la seguridad ocasionadas por malware es el principal motivo para *no* utilizar software ilegal.

CONCLUSIÓN

Este análisis estadístico y la evidencia en el terreno destacan una clara relación entre el software sin licencia y las amenazas a la seguridad informática. No todas las amenazas a la seguridad provienen del malware, y no todo el malware proviene del software sin licencia. Pero es más que evidente que *una parte* del malware *sí* proviene del software sin licencia, y que la *mayoría* del malware constituye una amenaza para la seguridad informática.¹²

¹⁰Justin Peters de *Slate* ha resumido la información sobre esta correlación particular. El artículo se llama: "When Ice Cream Sales Rise, So Do Homicides. Coincidence, or Will Your Next Cone Murder You?" 9 de julio de 2013, en http://www.slate.com/blogs/crime/2013/07/09/warm_weather_homicide_rates_when_ice_cream_sales_rise_homicides_rise_coincidence.html.

¹¹*The Link between Pirated Software and Cybersecurity Breaches*, publicado en marzo de 2014. Disponible en http://news.microsoft.com/download/presskits/dcu/docs/idc_031814.pdf. Este estudio fue precedido de otros estudios de IDC publicados en 2013 y 2007 sobre el malware en el software ilegal.

¹²En su informe llamado "*Data Breach Investigations Report*" de 2013, Verizon reveló que el 40 % de las amenazas tenían que ver con malware y que el 71 % apuntaba a dispositivos de usuarios finales. Ver http://www.secretservice.gov/Verizon_Data_Breach_2013.pdf.

Para empresas, gobiernos y consumidores, la implicancia obvia es que una manera de reducir los riesgos para la seguridad cibernética es reducir el uso de software sin licencia. Para ello es necesario implementar políticas y procedimientos eficaces para la administración de software e invertir recursos para crear conciencia sobre los potenciales peligros asociados al uso de software pirata. Los peligros radican en el malware que puede estar incorporado en el software, en los sitios y las fuentes de los cuales se obtiene el malware, pero también en la reticencia de los usuarios de software pirata a instalar actualizaciones de seguridad. Pero la evidencia muestra que el software pirata está claramente relacionado con las amenazas a la seguridad causadas por malware, y el costo global del problema ronda los cientos de miles de millones de dólares por año.¹³

¹³Consulte "La relación entre el software pirata y las amenazas a la seguridad informática", op. cit.

ANEXO: PAÍSES Y DATOS UTILIZADOS EN ESTE ESTUDIO

En la Tabla 1 se enumeran los países y los datos incluidos en este estudio.

TABLA 1

Índice de software ilegal y tasa de PC infectadas con malware por país, 2013 (%)

País	Índice de software ilegal	Tasa de malware
Moldova	90	30
Georgia	90	41
Venezuela	88	32
Bielorrusia	86	32
Irak	86	40
Argelia	85	43
Pakistán	85	50
Indonesia	84	44
Ucrania	83	32
Nigeria	81	21
Vietnam	81	32
Guatemala	79	22
Kenia	78	22
Albania	75	29
República Dominicana	75	30
Túnez	75	39
China	74	25
Kazajstán	74	36
Líbano	71	27
Tailandia	71	32
Argentina	69	25
Serbia	69	27
Filipinas	69	37
Uruguay	68	19
Ecuador	68	35

TABLA 1

Índice de software ilegal y tasa de PC infectadas con malware por país, 2013 (%)

País	Índice de software ilegal	Tasa de malware
Marruecos	66	34
Perú	65	37
Bulgaria	63	26
Grecia	62	25
Rumania	62	26
Rusia	62	29
Egipto	62	41
India	60	39
Turquía	60	43
Chile	59	22
Kuwait	58	22
Jordania	57	32
Malasia	54	27
México	54	31
Latvia	53	19
Lituania	53	24
Croacia	52	19
Colombia	52	29
Polonia	51	21
Arabia Saudita	50	28
Brasil	50	31
Qatar	49	25
Estonia	47	13
Chipre	47	21
Italia	47	22
Eslovenia	45	16
España	45	22
Hong Kong	43	12
Puerto Rico	42	14

TABLA 1**Índice de software ilegal y tasa de PC infectadas con malware por país, 2013 (%)**

País	Índice de software ilegal	Tasa de malware
Portugal	40	23
Hungría	39	20
Taiwán	38	19
Corea	38	30
Eslovaquia	37	17
Francia	36	18
Emiratos Árabes Unidos	36	29
República Checa	34	20
Sudáfrica	34	21
Irlanda	33	12
Singapur	32	12
Israel	30	17
Noruega	25	9
Canadá	25	13
Países Bajos	25	15
Finlandia	24	8
Suiza	24	12
Alemania	24	13
Reino Unido	24	14
Bélgica	24	17
Suecia	23	10
Dinamarca	23	10
Austria	22	13
Australia	21	12
Nueva Zelandia	20	12
Japón	19	7
Estados Unidos	18	13

Fuente: IDC, 2015

Acerca de IDC

International Data Corporation (IDC) es el principal proveedor global de inteligencia de mercado, servicios de consultoría y eventos para los mercados de tecnología de la información, telecomunicaciones y tecnología del consumidor. IDC ayuda a profesionales de TI, ejecutivos de negocio y a la comunidad de inversores a tomar decisiones basadas en hechos acerca de compras de tecnología y estrategia de negocio. Con más de 1100 analistas, IDC ofrece experiencia y conocimientos globales, regionales y locales sobre oportunidades y tendencias de tecnología y del sector en más de 110 países en todo el mundo. Hace 50 años que IDC proporciona conocimientos estratégicos para ayudar a sus clientes a alcanzar sus objetivos clave de negocio. IDC es una subsidiaria de IDG, la empresa líder de medios tecnológicos, investigación y eventos del mundo.

Casa matriz

5 Speen Street
Framingham, MA 01701
EE.UU.
508.872.8200
Twitter: @IDC
idc-insights-community.com
www.idc.com

Aviso de copyright

Publicación externa de información o datos relacionados con IDC: toda información de IDC que se use en publicidad, comunicados de prensa o material promocional requiere la aprobación previa por escrito del correspondiente vicepresidente o Gerente de país de IDC. Toda solicitud debe venir acompañada de un borrador del documento propuesto. IDC se reserva el derecho de negar la aprobación para uso externo por cualquier motivo.

Copyright 2015 IDC. Está prohibida su reproducción sin permiso escrito.

