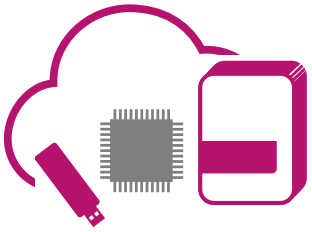
gemalto
security to be free



INFORME TÉCNICO

Protección contra las cuatro amenazas a la propiedad intelectual

Informe técnico dirigido a editores de software y fabricantes de dispositivos inteligentes

Índice

Información general 2

Las cuatro amenazas a la propiedad intelectual 2

Piratería y uso ilegal de software 2

- Las consecuencias 3
- La solución: protección contra copia y cumplimiento de licencia 3
- Ejemplo de prácticas recomendadas: TAISA 4

Actividades en el mercado gris 5

- Las consecuencias 5
- La solución: diferenciación de productos, fijación de precios por segmentos, seguimiento y gestión de los términos de licencia, la distribución y el uso 6
- Ejemplo de prácticas recomendadas: proveedor de dispositivos de red 7

Ingeniería inversa y robo de secretos comerciales 7

- Las consecuencias 7
- La solución: protección contra la ingeniería inversa y el robo 8

Ejemplo de prácticas recomendadas: Virtual Surveillance 8

Manipulación indebida 9

- Las consecuencias 10
- La solución: protección contra manipulaciones indebidas 10
- Ejemplo de prácticas recomendadas: empresa líder dedicada a la fabricación de envases 10

Conclusión 11

Acerca de las soluciones de monetización de software de Sentinel 11

Información general

La tecnología y la innovación nunca antes han evolucionado con tanta rapidez y la mayoría de los cambios involucran al software de una u otra manera. En la actualidad el software lo impulsa todo, desde productos de software empaquetados y listos para ser usados, hasta software ofrecido como un servicio desde la nube, dispositivos inteligentes de hardware en el centro de datos, el hogar o la palma de la mano.

Las empresas que desarrollan estos productos han invertido una enorme cantidad de tiempo y dinero en la investigación y desarrollo, así como en la escritura de códigos de software. El código que permite el funcionamiento de estos productos de software y dispositivos inteligentes de hardware contiene secretos comerciales y constituye una valiosa propiedad intelectual (IP, por sus siglas en inglés). Si no se dispone de la protección adecuada, esta IP puede verse comprometida con bastante facilidad, lo que podría causar un daño irreparable a la marca de una empresa, su capacidad competitiva, sus ingresos y la experiencia ofrecida a sus clientes.

En el presente informe se describen las cuatro amenazas a la propiedad intelectual y se explican las formas que adoptan los ataques a la IP. De igual modo, se explican las consecuencias derivadas de la protección inadecuada y se presentan ejemplos de buenas prácticas que ilustran el modo en que editores exitosos están empleando soluciones de monetización comerciales para proteger de manera proactiva sus inversiones en la propiedad intelectual y aumentar sus ingresos.

Las cuatro amenazas a la propiedad intelectual

Los ataques a la propiedad intelectual adoptan formas diversas:

- Piratería de software
- Ingeniería inversa y robo de secretos comerciales
- Manipulación de código
- Movimiento en el mercado gris

Cada una de estas actividades representa una grave amenaza a los ingresos derivados del software y a la innovación en el futuro prara los editores de software y los fabricantes de dispositivos inteligentes.

1 Piratería y uso ilegal de software

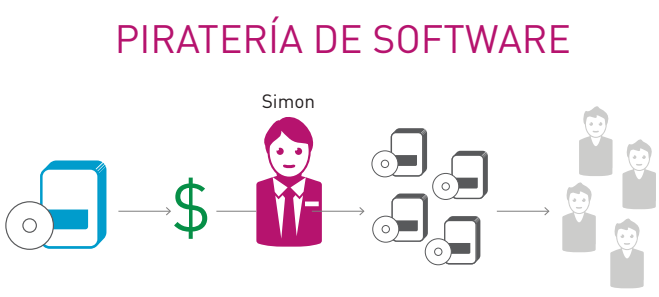
La piratería de software es la situación más obvia en la que la IP puede verse comprometida. La piratería, también conocida bajo el nombre de uso ilegal y robo, consiste en la copia y/o distribución no autorizada de programas de software sujetos a derechos de autor, lo que vulnera los derechos legales de los editores de software. De acuerdo con la Business Software Alliance (también conocida como BSA) en 2015, el 39 % del software instalado en equipos a nivel mundial no contaba con la licencia debida y la pérdida de ingresos en todo el planeta derivada de software sin licencia ascendía a $52,2 miles de millones.[i]

Como resultado de la piratería, sea de manera deliberada o no, cada año se pierde una enorme cantidad de propiedad intelectual y las empresas de software y los gobiernos locales pierden ingresos. Los ingresos que se reinvertirían en I+D para desarrollar y mejorar programas informáticos legítimos simplemente no llegan a las manos de los editores de software.

Las investigaciones demuestran que el 71 % de los proveedores de software independientes (ISV, por sus siglas en inglés) han perdido ingresos como resultado de la piratería de software.[ii]

> Casi la mitad de las empresas encuestadas, el 48 %, admite que su organización ha incumplido las condiciones de al menos uno de sus contratos de licencia de software.

En el gráfico que figura a continuación se describe un caso sencillo de piratería de software. Alguien adquiere una licencia para utilizar una copia del programa de software y hace varias copias que se comparten o venden de manera ilícita a otras personas.



Simón compra una copia del programa Jenny, después hace copias ilegales.

Para la mayoría de las organizaciones la piratería de software equivale a robo intencional, aunque el término también incluye el uso excesivo de software con licencia legal, bien sea deliberado o accidental. Un ejemplo del uso excesivo accidental es cuando una empresa adquiere y licencia un determinado número de puestos, pero en realidad utiliza más de los que tiene derecho a usar.

Aunque en la actualidad la mayoría de los usuarios finales son conscientes de que el uso de software sin licencia es ilegal, muchos hacen caso omiso a la importancia que reviste el considerar al software como propiedad intelectual de alto valor.

De acuerdo con la investigación realizada por Vanson Bourne a petición de Gemalto, casi la mitad de las empresas encuestadas, el 48 %, admite que su organización ha incumplido las condiciones de al menos uno de sus contratos de licencia de software.

Es evidente que los negocios de los editores de software se están viendo afectados ya que el 71 % de los encuestados indicó que está perdiendo ingresos debido a la piratería de software. Además, el 79 % sostiene que la pérdida de ingresos se debe a clientes que incumplen los acuerdos de licenciamiento de manera deliberada y el 82 % declara haber sufrido pérdidas de ingresos adicionales debido a clientes que trasgreden las condiciones estipuladas en dichos acuerdos sin darse cuenta. [ii]

La investigación realizada por BSA concluyó que en 72 de los 116 mercados que fueron objeto de estudio, más del 50 % de todos los software instalados en PC en 2015 carecía de licencia y en 37 de los mercados al menos el 75 % no contaba con licencia. [i]

Resultados de la encuesta

71 % de las empresas de software pierden ingresos debido a la piratería de software.

79 % de las empresas de software pierden ingresos debido a clientes que a sabiendas incumplen los acuerdos de licenciamiento.

82 % de las empresas de software pierden ingresos debido a clientes que trasgreden las condiciones estipuladas en los acuerdos de licenciamiento sin darse cuenta.

Las consecuencias

Pérdida de ingresos: para desarrollar una aplicación de software es necesario invertir una gran cantidad de tiempo, dinero y esfuerzo. La piratería de software (incluyendo licencias de red ilegales y actualizaciones incumplidas) impide el acceso a los ingresos merecidos y perjudica a los clientes que sí pagan por los productos, quienes acaban asumiendo el costo derivado del uso ilegal de los mismos.

Menos innovación: la piratería limita la capacidad de las empresas para ser competitivas, lo que se traduce en productos menos avanzados y a precios más elevados para los clientes.

La piratería afecta a los usuarios finales: la infracción de los derechos de autor no solo perjudica al sector del software, sino que además conlleva consecuencias negativas para el usuario final. A continuación se presentan algunos de los argumentos más sensatos por los que los usuarios deberían evitar software sin licencias:

- El software puede contener malware o estar defectuoso o dañado
- No se dispone de acceso a soporte técnico
- No se cuenta con ningún tipo de documentación o garantía para el producto
- El contenido puede ser incorrecto o estar obsoleto
- La actualización del software resulta sumamente difícil o imposible
- Costosas demandas y/o sanciones significativas

La solución: protección contra copia y cumplimiento de licencia

Una estrategia bien planificada y ejecutada para hacer frente a la piratería y el uso ilegal de software es una práctica comercial clave en un mercado sólido, pero cobra una importancia mucho mayor en entornos económicos difíciles.

Los editores de software pueden adoptar medidas reactivas o preventivas para luchar contra la piratería y el uso ilegal:

Medidas reactivas

Muchos de los editores de software no toman ningún tipo de medidas para proteger su software contra el uso ilegal y dependen únicamente de los contratos de licencia de software y de la ley de derechos de autor. Sin embargo, estos mecanismos de control no impiden que los usuarios copien el software intencionalmente ni tampoco evitan el uso excesivo, bien sea deliberado o accidental. Si un editor considera que su software ha sido pirateado o utilizado de forma ilegal, el alcance de las medidas reactivas radica únicamente en los recursos jurídicos disponibles para proteger a los editores de software contra los piratas informáticos.

Los grupos dedicados a la vigilancia y el control, como la Federación en Contra del Robo de Software (FAST, por sus siglas en inglés), la Asociación de la Industria de Software e Información (SIIA), la BSA, la Organización Mundial de la Propiedad Intelectual (WIPO) y otros, contribuyen con la educación de los usuarios e impulsan leyes que protegen a los editores de software. La BSA también investiga, enjuicia y litiga casos denunciados de piratería y ha colaborado con una gran cantidad de editores de software para resolver casos de piratería.

Si bien es cierto que las acciones legales son valiosas, su costo puede ser bastante elevado. Además, debido a que por naturaleza estas son medidas reactivas, no se puede depender de ellas para evitar el problema.

Medidas proactivas

Existe una gran cantidad de medidas preventivas basadas en tecnología que los editores de software pueden adoptar para hacer frente a la piratería y el uso ilegal.

Algunos editores comienzan por utilizar prácticas de escritura de código más seguras.

Otros optan por escribir su propio código de protección y licenciamiento. Por lo general, los editores que dependen de su personal de desarrollo para escribir su propio código de protección y licenciamiento tienen conocimientos limitados en materia de seguridad, recursos limitados para mantener el código de seguridad y estar siempre un paso adelante de los hackers y resultados limitados.

> Por lo general, los editores que dependen de su personal de desarrollo para escribir su propio código de protección y licenciamiento tienen conocimientos limitados en materia de seguridad, recursos limitados para mantener el código de seguridad y estar siempre un paso adelante de los hackers y resultados limitados.

Para luchar contra la piratería y el uso ilegal, la mayoría de los editores de software confían en los conocimientos especializados, la robusta seguridad y el cumplimiento de licencias que ofrecen las soluciones de monetización disponibles en el mercado. El uso de una solución de licenciamiento y protección comercial se puede traducir en una mayor rapidez para el lanzamiento de productos al mercado, además de un ahorro inicial en gastos de implementación y un costo de propiedad menor en comparación con un sistema de licenciamiento desarrollado internamente.

Las soluciones comerciales más poderosas utilizan bloqueo basado en software, hardware y en la nube y cumplimiento de licencias. Cada una de estas ofrece una serie de ventajas particulares y deben ser tomadas en cuenta en función de las metas y necesidades específicas de cada editor de software y las exigencias de sus clientes. Por ejemplo, si el editor entrega el software de forma electrónica, el mejor método que se puede aplicar suele ser la protección y activación del producto basada en software. Si el cliente usuario final requiere un acceso fácil a la aplicación protegida con portabilidad entre equipos, lo más probable es que opte por una protección basada en hardware. De igual modo, si el software está basado en suscripciones y se ofrece como un servicio, la mejor elección es el licenciamiento basado en la nube.
Hay una serie de factores adicionales que se debe tomar en cuenta al seleccionar el tipo de protección y licenciamiento proactivo de software que se va a utilizar, incluyendo el nivel de seguridad requerido, los métodos de distribución, la portabilidad, el precio del software, entre otros. Las soluciones de monetización de software disponibles en el mercado son métodos comprobados que ayudan a impedir la piratería de software y garantizar los ingresos derivados del mismo.

La protección contra copia y el cumplimiento de licencia asegura ingresos, protege su ventaja competitiva y garantiza una mejor experiencia para sus usuarios finales.

Ejemplo de prácticas recomendadas: TAISA

Sentinel HL protege el valioso software de mantenimiento preventivo de TAISA contra la piratería y el uso ilegal al tiempo que aumenta significativamente las ventas. Técnicos Asociados Informática S.A. (TAISA), fundada en 1974, tiene sede en México y se ha convertido en el líder en la creación de software de mantenimiento preventivo utilizado a escala mundial.

> "Comenzamos con un sistema de protección de software propio, pero con el paso del tiempo nos dimos cuenta de que la solución con la que contábamos era demasiado básica para proteger nuestro software contra la piratería y pérdidas". -Pablo Seeliger, TAISA

El desafío comercial

Con la creación de su software de mantenimiento preventivo (PM, por sus siglas en inglés), TAISA lanzó una arquitectura de producto única que dependía del equipo de mantenimiento instalado en tres ubicaciones y de tres discos: un disco maestro y dos de copia de seguridad; todos estos requerían protección contra la piratería. Con la creciente demanda de Software de PM en el mercado y una competencia cada vez mayor de empresas con sede en los Estados Unidos, la solución desarrollada internamente para gestionar los derechos de software de TAISA ya no era suficiente para impedir la piratería, por lo que necesitaban algo que ofreciera un mayor grado de solidez y seguridad. "Desde que desarrollamos nuestro Software de PM ha existido la necesidad de protegerlo", afirmó Pablo Seeliger de TAISA. "Comenzamos con un sistema de protección de software propio, pero con el paso del tiempo nos dimos cuenta de que la solución con la que contábamos era demasiado básica para proteger nuestro software contra la piratería y pérdidas". Tras percatarse de que necesitaban una protección de IP más completa, TAISA puso a prueba diferentes productos de gestión de derechos de software para evaluar el grado de compatibilidad y seguridad que ofrecían.

La solución

Tras poner a prueba Sentinel HL, Seeliger se convenció de que esta solución ofrecía el nivel de seguridad requerido por el software de TAISA. Sentinel se integra con el Software de PM de TAISA de modo que no se pueda ejecutar el programa sin la llave Sentinel HL, lo cual impide el uso no autorizado y ofrece protección de la propiedad intelectual y diversas opciones de licenciamiento.

> "Tras la implementación de Sentinel HL las ventas aumentaron notablemente, a tal punto que en la actualidad jamás consideraríamos seguir desarrollando nuestro software de PM sin Sentinel". -Pablo Seeliger, TAISA

Los resultados

"Sin Sentinel, las pérdidas en el volumen de ventas podrían haber alcanzado el 20 o 30 por ciento", indicó Seeliger. Ahora TAISA no solo es capaz de proteger su producto de software con absoluta certeza, sino que además la implementación de las llaves de protección HL ha permitido a la empresa crear dos versiones del software: una versión de usuario único y otra en red, la cual permite el acceso de múltiples usuarios al software. Gracias a Sentinel HL, TAISA es capaz de proteger su software una sola vez y ofrecerlo a los clientes en diversos formatos, lo que ha aumentado el volumen de ventas. "Tras la aplicación de Sentinel HL las ventas aumentaron notablemente, a tal punto que en la actualidad jamás consideraríamos seguir desarrollando nuestro software de PM sin Sentinel", sostuvo Seeliger.

La aplicación de Sentinel HL también permitió que TAISA expandiera con confianza su alcance de mercado a países como Venezuela, Colombia, Argentina y España.

2 Movimientos en el mercado gris

El mercado gris representa una amenaza que a pesar de ser menos conocida podría tener efectos devastadores para los desarrolladores de software y los fabricantes de dispositivos inteligentes. Si no se controlan, las actividades en este mercado pueden ser perjudiciales para su marca, su canal e incluso sus ingresos. Por lo tanto, es conveniente entender el modo en que el comercio en el mercado gris puede afectar a su negocio y desarrollar medidas correctivas para mitigar el riesgo.

De acuerdo con la definición de Wikipedia, el mercado gris se refiere a la comercialización de productos a través de canales de distribución que, a pesar de ser legales, son diferentes a los autorizados por el fabricante.

Echemos un vistazo más de cerca a cómo funciona el mercado gris.

El mercado gris es una realidad para muchos productos fabricados y vendidos en el mundo entero. Algunos ejemplos de bienes de mercado gris dirigidos a consumidores incluyen: marcas de relojes lujosos, automóviles, teléfonos móviles, productos profesionales para el cuidado del cabello, patrones de bordado digitales y juegos para PC. Entre los ejemplos de B2B (o negocio a negocio) se encuentran los dispositivos médicos, los equipos industriales de automatización, software empresarial, etc. Esta no es una lista exhaustiva, pero basta para aclarar la idea.

El mercado gris para los teléfonos móviles es un buen ejemplo. Muchos fabricantes de teléfonos móviles no ofrecen teléfonos desbloqueados en los Estados Unidos. Los clientes deben comprar teléfonos que están bloqueados de modo que solo puedan ser utilizados con un proveedor de servicio de telefonía celular específico (por ejemplo, T-Mobile, Verizon, AT&T, Sprint).

Como era de esperarse, esto ha creado un mercado gris para los teléfonos desbloqueados. Algunos comerciantes de equipos electrónicos móviles adquieren teléfonos móviles nuevos (desbloqueados) fuera de los Estados Unidos y los venden en el país por un precio inferior al de los teléfonos bloqueados adquiridos por los canales autorizados. Si bien es cierto que esta no es una práctica ilegal, en la mayoría de los casos no se informa al cliente al respecto y se puede engañar a los compradores que desconozcan la situación debido a que:

- Los cargadores de CA, si vienen incluidos, por lo general no son compatibles con las especificaciones eléctricas de los EE. UU. y el usuario debe comprar el cargador adecuado por separado.
- A menudo los teléfonos vienen configurados por defecto en otro idioma y el usuario debe reconfigurar el equipo.
- Los manuales de instrucciones, si vienen incluidos, están escritos en el idioma hablado en la región a la que el teléfono había sido destinado. Si es necesario consultar las instrucciones, el consumidor debe buscarlo y acceder a este en línea.
- Con bastante frecuencia, estos teléfonos celulares de mercado gris no incluyen ningún tipo de garantía por lo que no pueden ser reparados por el fabricante.

Algunos consumidores están dispuestos a tolerar los inconvenientes derivados de la compra a través de mercados paralelos si esto les permite obtener lo que quieren a un precio más bajo. Aunque cuando el producto requiere mantenimiento, y el cliente se da cuenta de que la compra no incluía garantía, la lealtad a la marca y su reputación pueden verse afectadas.

Las consecuencias

Según una encuesta realizada recientemente por KPMG, "los fabricantes de equipos originales consideran que el mercado gris tiene un gran impacto en sus negocios, especialmente en las ganancias y la reputación de la marca. Cerca de la mitad de los encuestados afirma que los productos de mercado gris a menudo se ofrecen a un precio que está más de un 25 % por debajo del precio medio ofrecido por los socios de canal autorizados". [iii]

El mercado gris socava los planes de precios segmentados y perjudica las relaciones con el socio de canal, así como la reputación y la lealtad de marca.

Reducción del nivel de satisfacción de los clientes y deterioro de la lealtad de marca
Los productos de mercado gris a menudo se venden a un precio más bajo a clientes que no son conscientes de la situación y que solo más adelante se dan cuenta de que el producto que han comprado incluye garantías inválidas, fue diseñado para ser utilizado en países diferentes a aquel en el que se realizó la compra, o lo que es peor aún, está obsoleto o no cumple con los requisitos normativos locales.

A estos clientes se les priva del acceso a servicios, respaldo de garantía y piezas de repuesto de revendedores autorizados, en caso necesario. Además, cuando el producto no cumple con las expectativas del cliente, su satisfacción y lealtad se ven afectadas, lo que acaba por deteriorar la lealtad de marca.

Relaciones de canal tensas
Aunque es difícil hacerle seguimiento, KPMG estima que hasta un 24 % de los ingresos del canal se desvía a los comerciantes del mercado gris.[iii]

Sin embargo, el impacto de mayor costo del comercio en el mercado gris es el que tiene sobre las relaciones entre la red de distribuidores autorizados. Los socios que usted autoriza para vender piezas de repuesto, servicios de reparación y apoyo publicitario a los clientes en sus regiones están bajo una presión cada vez mayor de ampliar sus servicios de apoyo a fin de incluir a clientes que hayan comprado sus productos a través de proveedores que operan en el mercado gris.

Perjuicio para su imagen corporativa y reputación
Es probable que usted haya invertido millones de dólares en la investigación y el desarrollo de productos, junto con la creación de una imagen positiva para su marca. Cuando sus productos más costosos comienzan a aparecer en el mercado gris a precios reducidos, esto puede perjudicar su marca y repercutir negativamente en la reputación de su empresa.

Alteración de operaciones de venta y marketing
Las importaciones del mercado gris podrían dar lugar a alteraciones en la exactitud de las pronósticos de ventas, estrategias de precios, posicionamiento en el mercado y otras operaciones de marketing.

La solución: diferenciación de productos, fijación de precios por segmentos, seguimiento y gestión de las condiciones, la distribución y el uso de la licencia

A fin de preservar la integridad de los canales de venta, los productos y los ingresos, al tiempo que se mantiene a los clientes satisfechos, es importante limitar la exposición del software y los dispositivos inteligentes al mercado gris. La cuestión radica en determinar si se debe adoptar un enfoque reactivo, proactivo o una combinación de ambos.

Enfoque reactivo: Habitualmente, la defensa contra los mercados grises ha sido responsabilidad de los abogados y el sistema judicial en forma de litigios. Ha habido algunos casos clave en los que los jueces han fallado, por diversas razones, a favor de fabricantes de productos como Caterpillar, Kia, Gucci, HP e Intel, pero estas medidas reactivas solo se pueden tomar cuando se tiene conocimiento de la actividad en el mercado gris y se dispone de una base sólida para emprender acciones legales.

Lo cierto es que, a menos de que usted disponga de personal dedicado a identificar cualquier tipo de actividad en el mercado gris que involucre sus productos y cuente con grandes cantidades de dinero para afrontar los costos del litigio, la mayoría de los casos pasan desapercibidos y/o no se impugnan, lo que permite que se continúen desviando sus productos.

Aunque la prohibición de la desviación de productos a través del mercado gris resulta imposible, a los proveedores de software y los fabricantes de dispositivos les conviene poner en práctica estrategias proactivas que les ayuden a reducir el daño cuasdo por tales actividades.

Enfoque proactivo: Afortunadamente, existen algunas medidas proactivas que usted puede adoptar para protegerse contra la desviación de su software y dispositivos inteligentes. El despliegue de una tecnología comercial de monetización de software con capacidades de licenciamiento y gestión de derechos le permite:

Diferenciar sus productos para diversos segmentos de mercado
La tecnología de licenciamiento de software sofisticada le permite desarrollar diferentes versiones de sus productos a fin de que se ajusten a:

- Regiones geográficas específicas
- Normativa de salud y seguridad
- Requisitos de empaquetado
- Hábitos de consumo
- Normas técnicas
- Niveles de precios estratégicos

Al utilizar el licenciamiento de software para diferenciar los dispositivos inteligentes para diversos segmentos del mercado los costos operativos derivados de la producción y gestión de inventario decrecen, se limita el arbitraje de precios y se restringen las ventas en el mercado gris.

Seguimiento y gestión de las condiciones, la distribución y el uso de la licencia
La gestión de derechos se puede utilizar para administrar y hacer cumplir el licenciamiento de software desde la distribución hasta la activación y el uso del producto. Al emitir y controlar códigos de activación por vía electrónica, se puede hacer seguimiento y gestionar todos los productos desde el momento de la fabricación, bien sea en su propia planta o en una planta de manufactura bajo contrato, hasta la distribución y la activación desde las instalaciones del usuario final.

Ejemplo de prácticas recomendadas: proveedor de dispositivos de red

Esta compañía tiene sede en los Estados Unidos y se dedica al diseño y la venta de enrutadores (también conocidos como routers) que controlan el tráfico de red de empresas. Un elemento clave de su valiosa propiedad intelectual (IP) reside en su firmware para uso especial que permite alternar la velocidad de rendimiento y optimizar el tráfico del ancho de banda.

Desafío: protección contra la comercialización de sus routers en el mercado gris

El proveedor de routers contrata a un fabricante extranjero para fabricar sus enrutadores. La empresa quería protegerse contra la posibilidad de que el fabricante contratado produjera unidades de más para venderlas a negocios estadounidenses a un precio más bajo que el ofrecido por sus socios de canal autorizados. Esto desviaría los ingresos del proveedor de routers y perjudicaría las relaciones de canal.

Solución: desplegar una solución comercial de monetización de software

A fin de reducir el potencial de actividad en el mercado gris, la empresa de routers optó por desplegar una solución comercial de monetización de software. El poder utilizar las capacidades de licenciamiento seguro permitió a la empresa diferenciar sus productos para diferentes segmentos de mercado y desarrollar diferentes versiones de los productos para ajustarse a niveles de precios estratégicos. Las capacidades de gestión de derechos se utilizaron para administrar y hacer cumplir el licenciamiento del producto desde el momento de su fabricación, hasta la distribución y la activación por parte del usuario final.

Resultados: restricción de las actividades en el mercado gris y protección de los ingresos

El uso de una solución comercial de monetización de software permitió a este proveedor de routers proteger su IP y, al limitar el arbitraje de precios y emitir y seguir las activaciones de productos por vía electrónica, pudo restringir las actividades en el mercado gris.

3 Ingeniería inversa y robo de secretos comerciales

Los editores de software invierten una importante cantidad de recursos en la investigación y el desarrollo de sus productos, la escritura de códigos y la creación de propiedad intelectual que actúa como una ventaja clave y como diferenciador de los software y dispositivos inteligentes impulsados por software de la competencia. La propiedad intelectual (IP) representa la mayor parte del valor comercial de una empresa de software o un fabricante tradicional de dispositivos inteligentes. En consecuencia, las presiones competitivas aumentan a medida que las empresas adoptan estrategias más agresivas para tratar de incrementar su negocio. El espionaje competitivo es una práctica cada vez más habitual, por lo que su valiosa IP de software –que incluye códigos, algoritmos, archivos de datos de aplicaciones y secretos comerciales– está expuesta a ojos curiosos, ingeniería inversa, robo e imitación por parte de competidores.

No cabe duda de que la ingeniería inversa y el robo de secretos comerciales están teniendo consecuencias negativas para los editores de software. De acuerdo con una encuesta realizada recientemente, una abrumadora mayoría, el 84 %, de los ISV encuestados a nivel mundial admite sentirse preocupado ante la posibilidad de que su software pueda verse afectado y el 81 % considera que la ingeniería inversa y el robo están mermando sus ingresos. [ii]

Simón extrae secretos comerciales del código del programa Jenny

Las consecuencias

Pérdida de la ventaja competitiva: a través de la ingeniería inversa y el robo de secretos comerciales.

Pérdida de ingresos: debido a la proliferación de imitaciones de software y dispositivos de hardware impulsados por software.

Resultados de la encuesta

84 %	de los ISV les preocupa por que su software pueda verse comprometido
81 %	de los ISV considera que la ingeniería inversa y el robo están repercutiendo negativamente en sus ingresos

La solución: protección de la IP de valor contra la ingeniería inversa y el robo

Ante la situación económica actual, hoy más que nunca resulta indispensable asentar la ventaja competitiva. A medida que la competencia aumenta, es importante asegurar esa ventaja mediante la adopción de medidas que protejan sus productos contra la ingeniería inversa que podría dar lugar al robo de la propiedad intelectual y los secretos comerciales de alto valor. Al proteger los secretos comerciales y el código fuente de individuos malintencionados se gana cuota de mercado ya que la ventaja competitiva se mantiene y sigue aumentando.

Las soluciones de software no solo constan de archivos ejecutables y DLL, también incluyen archivos de datos cuyo valor a menudo puede ser muy superior al de las aplicaciones de software. En muchos casos, estos archivos de datos contienen información altamente confidencial y propiedad intelectual que también se debe proteger contra robo e imitación por parte de competidores.

Una solución comercial de protección y licenciamiento que incluye tecnología de envoltorio automático ofrece una robusta protección de la propiedad intelectual contra la ingeniería inversa mediante el cifrado de archivos, la ofuscación de código y la antidepuración a nivel del sistema, lo que garantiza que los algoritmos, secretos comerciales y conocimientos técnicos profesionales integrados en el software estén protegidos contra hackers.

La protección de la propiedad intelectual resguarda la ventaja competitiva y los ingresos.

Ejemplo de prácticas recomendadas: Virtual Surveillance

Sentinel HL detiene los ataques en curso y protege los sistemas de software y hardware de Virtual Surveillance contra la ingeniería inversa y el robo. Virtual Surveillance se dedica al diseño y la comercialización de sistemas de videovigilancia digital utilizados para vigilar y proteger las operaciones en múltiples lugares. La empresa también produce software para el análisis de movimiento incluyendo un sistema digital de detección de intrusiones, detección de movimiento, detección de objetos olvidados o extraídos, etc. Virtual Surveillance ofrece integración con sistemas de alarmas existentes y capacidades de activación de alarma basadas en la detección de cualquier movimiento en las imágenes de video captada por su software.

> Debido a que había una amenaza de ataque cibernético inminente, era indispensable implementar la solución con rapidez.

El desafío comercial

Al principio Virtual Surveillance desarrollaba internamente su protección contra copia, pero su sistema de protección dificultaba la copia de la licencia de software y su traslado de un equipo a otro diferente. Por ejemplo, si alguien utiliza alguna de las herramientas que se pueden obtener con muchísima facilidad para suplantar las direcciones MAC de las tarjetas de red, esta persona podría reutilizar continuamente una clave de licencia de software única. Sus peores temores se volvieron realidad cuando se confirmó una infracción de la seguridad. Alguien estaba intentando realizar ingeniería inversa de sus productos tanto de software como de hardware.

> Con el respaldo de la llave Sentinel, Virtual Surveillance fue capaz de proteger su software con rapidez antes de que la amenaza se convirtiera en un robo consumado.

La solución

Este ataque llevó a Virtual Surveillance a dar con Sentinel HL de Gemalto. El software está repartido entre varias aplicaciones diferentes y cada una de estas depende de un servicio Web ASP.Net que se utiliza para compartir contenidos multimedia, tales como videos e imágenes de instantáneas. Este método permite la sincronización de contenidos multimedia en varios equipos y usuarios y exige un código de acceso para obtener la información.

Debido a los requisitos de seguridad de estas aplicaciones, es absolutamente necesario utilizar una red cerrada. Tras la creación de un sistema que utiliza llaves Sentinel para proteger el acceso al servicio Web ASP.Net, Virtual Surveillance es capaz de crear un punto de falla único que hace que las otras aplicaciones sean inservibles. El servicio Web realiza controles a la llave Sentinel durante cada llamada y en tiempo real. Cuando la llave no está presente esta hace que se produzca un error en la aplicación del cliente, en lugar de dar curso a la solicitud.

Debido a que había una amenaza de ataque cibernético inminente, era indispensable implementar la solución con rapidez. Gemalto ofreció instrucciones rápidas y sencillas, junto con un código C# de muestra que la empresa fue capaz de modificar. Con el respaldo de la llave Sentinel, Virtual Surveillance fue capaz de proteger su software con rapidez antes de que la amenaza se convirtiera en un robo consumado.

> "Sentinel nos facilitó las herramientas necesarias para proteger completamente nuestro software a fin de que pudiéramos dedicar más tiempo a las necesidades de nuestros clientes. El gasto total para proteger nuestra labor de desarrollo –valorada en muchos millones de dólares– contra una amenaza conocida fue de menos de 300 dólares, incluyendo el tiempo de desarrollo y el envío por servicio de mensajería rápida en ambos sentidos". -Eric Burcham, CTO, Virtual Surveillance

La recompensa

Tras un plazo de menos de dos horas dedicado al desarrollo y una rápida actualización en las instalaciones de la empresa, Virtual Surveillance fue capaz de proteger completamente su labor de desarrollo, la cual está valorada en muchos millones de dólares, contra un ataque de ingeniería inversa en curso. Si el hacker hubiera tenido éxito, el costo para la empresa hubiera sido incalculable.

Eric Burcham, director tecnológico, indicó que "las llaves como tales cuestan mil veces menos que el tiempo y esfuerzo que hubiéramos tenido que dedicar a la escritura de código de una solución de protección con el mismo nivel de excelencia y a la generación y el seguimiento manual de llaves de activación para nuestros clientes".

Al tratarse de una empresa pequeña que ofrece una solución llave en mano a un mercado elitista y en rápida evolución, Virtual Surveillance necesitaba proteger sus activos. Burcham señaló además que "Sentinel HL nos facilitó las herramientas necesarias para proteger completamente nuestro software a fin de dedicar más tiempo a las necesidades de nuestros clientes. El gasto total para proteger nuestra labor de desarrollo –valorada en muchos millones de dólares– contra una amenaza conocida fue de menos de 300 dólares, incluyendo el tiempo de desarrollo y el envío por servicio de mensajería rápida en ambos sentidos".

4 Manipulación indebida

Si bien es cierto que el robo de secretos comerciales puede ser catastrófico, para muchos ISV y fabricantes de dispositivos inteligentes, la manipulación de código puede resultar igualmente devastadora. Ambas situaciones conllevan grandes posibilidades de perjudicar la cuota general de mercado y así reducir el potencial de ingresos.

La manipulación indebida ocurre cuando alguien obtiene acceso al código de software y hace cambios al modo en que funciona el producto. Es importante destacar que la manipulación puede ser intencional y maliciosa o accidental y bienintencionada. La manipulación accidental realizada por un usuario final suele pasar desapercibida hasta que el daño ya está hecho y es demasiado tarde.

En el ejemplo de manipulación bienintencionada que se presenta más abajo, nos centramos en un equipo de diagnóstico médico. El software interno ha sido diseñado para controlar el modo en que se realizan las pruebas de diagnóstico. Supongamos ahora que un usuario final considera que el sistema es lento y decide manipular el código de software solo lo necesario para acelerar los cálculos en un 20 %. Misión cumplida: ahora se puede

Simón hace cambios no autorizados al código de software que controla el dispositivo de diagnóstico médico inteligente de Jenny

examinar a más pacientes cada día. No hay ningún tipo de intención maliciosa.

Lo que esta persona no sabe es que al acelerar el proceso de cálculo se acelera un proceso que requiere ese tiempo adicional para cumplir con una serie de normativas del sector médico. Las pruebas posteriores realizadas con ese equipo son inexactas. ¿Quién termina siendo atacado por los medios de comunicación y sufre la caída de ventas consiguiente? No es el usuario que interfirió con el equipo ni tampoco el hospital. El fabricante del equipo médico y/o el proveedor de software es de quien se hablará por ofrecer un software defectuoso.

> Si bien es cierto que el robo de secretos comerciales puede ser catastrófico, para muchos ISV y fabricantes de dispositivos inteligentes, la manipulación de código puede resultar igualmente devastadora. Ambas situaciones conllevan grandes posibilidades de perjudicar la cuota general de mercado y así reducir el potencial de ingresos.

Las consecuencias

Es posible que la solución deje de cumplir con los objetivos comerciales. Como consecuencia de la alteración mediante la manipulación de código, es posible que el software y el equipo dejen de cumplir con los objetivos comerciales para los que fue diseñado.

Resultados inesperados:La manipulación del software integrado en un dispositivo puede alterar el modo en que funciona el equipo y dar lugar a resultados corrompidos.

Pérdida de ingresos: La manipulación de código puede brindar acceso a los usuarios a características por las que no han pagado.

Perjuicio para la reputación de la marca: Los problemas relacionados al cumplimiento normativo pueden causar daños irreversibles a la reputación de la marca y el producto.

La solución: protección contra manipulaciones

Sin saberlo, los proveedores de dispositivos inteligentes dejan su código expuesto a la manipulación si no disponen de las tecnologías de protección mediante cifrado y ofuscación de código adecuadas.

La capacidad de controlar de manera eficaz el acceso al código fuente del software permite a los editores de software y a los proveedores de dispositivos médicos proteger sus ingresos y salvaguardar la integridad de sus marcas y productos al impedir la manipulación del producto, la ingeniería inversa y el robo de la IP.

> Sin saberlo, los proveedores de dispositivos inteligentes dejan su código expuesto a la manipulación si no disponen de las tecnologías de protección mediante cifrado y ofuscación de código adecuadas.

Ejemplo de prácticas recomendadas: empresa líder dedicada a la fabricación de envases

Este ejemplo de caso se trata de una empresa líder dedicada al desarrollo de equipos impulsados por software que se utilizan para procesar de principio a fin el envasado de productos alimenticios líquidos, tales como la leche y el jugo de naranja. El software que permite el funcionamiento de sus equipos de envasado está programado para cumplir con una gran cantidad de normas en materia de salud pública y seguridad.

Las preocupaciones de la empresa en torno a la protección de la IP se centran en controlar el acceso al software que operan a las máquinas y limitar la capacidad para manipular los parámetros clave que controlan procesos como la pasteurización. Este fabricante de equipos utiliza una combinación de soluciones de monetización de software Sentinel RMS y EMS para proteger el código de su software contra el acceso no autorizado y la manipulación indebida, así como para controlar estrictamente quién puede modificar los parámetros que determinan el funcionamiento del equipo de envasado.

Conclusión

Los resultados de las investigaciones indican que a una gran cantidad de editores de software le preocupa que su propiedad intelectual pueda verse comprometida.

Pero si a las empresas de software les preocupa dicho riesgo y las repercusiones que la propiedad intelectual de software afectada pueda tener en su marca, su capacidad para competir, la experiencia del cliente y sus ingresos, entonces ¿por qué no la protegen?

Suponemos que esto se debe a que los editores de software no cuentan con el ancho de banda, el apoyo que necesitan por parte de sus superiores o aún no han vivido una tragedia derivada de la propiedad intelectual. Los niveles de perjuicio varían. Con el paso del tiempo, la piratería de software da lugar a la pérdida de ingresos, pero las consecuencias de la ingeniería inversa y la manipulación indebida pueden ser devastadoras y tienen la capacidad de cambiar un negocio de la noche a la mañana. Recuperarse de tales pérdidas resulta sumamente difícil.

El encontrar la manera de reducir y prevenir la piratería de software, el comercio en el mercado gris, la ingeniería inversa y la manipulación indebida de la propiedad intelectual contenida en el código de software aporta numerosas ventajas. El usuario final tiene la certeza de que los programas que utiliza funcionan según lo previsto por el editor, de modo que incluyen las garantías y soporte adecuados. Al sector del software se le paga para fabricar productos de calidad, lo que estimula un mercado competitivo y el desarrollo subsiguiente de productos.

Pero para poner fin a la piratería es necesario contar con un esfuerzo combinado que involucre a los consumidores, los fabricantes de software y el gobierno. Algunos de los esfuerzos de mayor éxito han implicado la combinación de programas educativos con medidas para garantizar el cumplimiento de las normas, lo que ha arrojado resultados satisfactorios en Norteamérica y Europa.

Más allá de esto, los editores de software deben adoptar medidas proactivas y positivas para implementar estrategias de protección de software tendentes a defender su propiedad intelectual contra el uso ilegal, la realización de copias, el desvío a través de mercados grises, el robo y la manipulación indebida.

Tal y como lo ilustran los ejemplo de prácticas recomendadas, una solución de protección y licenciamiento de software puesta a prueba en el campo es un medio eficaz para hacer frente a las cuatro amenazas que acechan a la IP a fin de proteger los derechos de autor, luchar contra la piratería, mantener el precio por segmento e impedir el espionaje competitivo y la manipulación indebida.

Lo que muchos aún ignoran es que el despliegue de tecnología para la monetización de software también puede ser una estrategia progresista de generación de ingresos que aumente el volumen de ventas, reduzca los costos, impulse la ventaja competitiva y amplíe el alcance de mercado.

Acerca de la monetización de software de Gemalto Sentinel

Gemalto es la empresa líder en el mercado de las soluciones de licenciamiento de software y de gestión de derechos para los proveedores de software local, integrado y basado en la nube. En el sector del software, Gemalto Sentinel es la marca de mayor confianza para soluciones de monetización de software seguras, flexibles y adaptables a cambios tecnológicos futuros. Para más información, visite: www.gemalto.com/latam/monetizacion-de-software

¡Pruebe las soluciones Sentinel de forma gratuita!

Únete a la conversación

> Facebook
https://www.facebook.com/Sentinel-Software-Monetization-1758261374199865/

> LinkedIn
https://www.linkedin.com/showcase/10586190/

> Twitter
https://twitter.com/Sentinel_SM

> Google+
https://plus.google.com/u/2/111213966957422791805

> YouTube
https://www.youtube.com/channel/UCO_hjzzJXm0wE7L1kxZjfcg

> Blog
https://sentinel.gemalto.com/blog

i Seizing Opportunity Through License Compliance, BSA Global Software Survey, May 2016, http://globalstudy.bsa.org/2016/downloads/studies/BSA_GSS_US.pdf

ii The State of Software Monetization, Vanson Bourne research commissioned by Gemalto, http://www2.gemalto.com/software-monetization-trends/

iii Effective Channel Management Is Critical in Combating the Gray Market and Increasing Technology Companies' Bottom Line: KPMG Gray Market Study Update, KPMG, LLP, http://www.agmaglobal.org/cms/uploads/whitePapers/7-10-08KPMGWhitePaperGrayMarketStudy.pdf

Comuníquese: Para todas las oficinas e información de contacto, visite www.gemalto.com/latam/monetizacion-de-software

Síganos en: sentinel.gemalto.com/blog

GEMALTO.COM

gemalto
security to be free