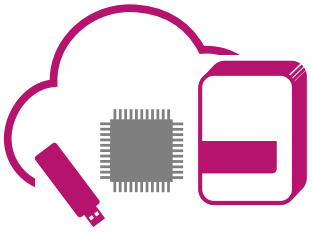
LIVRE BLANC

Défense contre les quatre menaces pour la propriété intellectuelle



Un livre blanc pour les éditeurs de logiciels et les fabricants d'appareils intelligents

Table des matières

Vue d'ensemble

La technologie et l'innovation n'ont jamais évolué aussi rapidement qu'aujourd'hui et incluent dans la majorité des cas un logiciel, sous une forme ou une autre. Qu'il s'agisse de logiciels grand public ou de logiciels SaaS dans le Cloud ou même de périphériques matériels intelligents utilisés dans un centre de données, à votre domicile ou dans votre poche, les logiciels sont aujourd'hui au cœur de toutes nos activités.

Les entreprises qui développent ces produits n'ont pas compté les heures et l'argent investis dans la recherche, le développement et l'écriture du code logiciel. Le code qui alimente ces produits logiciels et ces périphériques matériels intelligents contient des secrets industriels et représente une précieuse propriété intellectuelle. Incorrectement protégée, celle-ci peut facilement être compromise et occasionner des torts irréparables à l'image de marque d'une entreprise, réduire sa capacité à affronter la concurrence, et faire chuter son chiffre d'affaires et la satisfaction de ses clients.

Ce livre blanc aborde les quatre menaces pour la propriété intellectuelle et explique les différentes formes que peuvent prendre les attaques contre la propriété intellectuelle. Il explique également les conséquences d'une protection inadaptée et présente des exemples de meilleures pratiques d'éditeurs utilisant les solutions commerciales de monétisation pour protéger de façon proactive leurs investissements dans la propriété intellectuelle et augmenter leur chiffre d'affaires.

Les quatre menaces pour la propriété intellectuelle

Les attaques contre la propriété intellectuelle peuvent prendre diverses formes :

- Piratage de logiciels
- Ingénierie inversée et vol de secrets industriels
- Manipulation du code
- Activité des marchés parallèles

Chacune d'entre elle constitue une grave menace en matière de chiffre d'affaires et d'innovation future pour les éditeurs de logiciels et les fabricants d'appareils intelligents.

1 Piratage et utilisation illégale de logiciels

Le premier exemple de vol de propriété intellectuelle qui vient à l'esprit est le piratage de logiciels. Le piratage, également appelé utilisation illégale ou vol, consiste à dupliquer et/ou distribuer sans autorisation un logiciel informatique protégé par des droits d'auteur. Il s'agit d'une violation des droits légaux de l'éditeur de logiciels. Selon une étude de la BSA (Business Software Alliance), en 2015, 39 % des logiciels installés sur les ordinateurs à travers le monde n'étaient pas correctement concédés sous licence, représentant une perte mondiale de chiffre d'affaires de 52,2 milliards de dollars.[i]

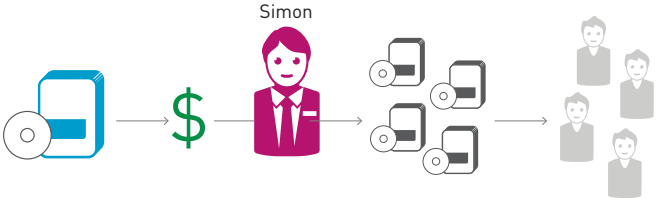
Qu'il s'agisse d'un acte délibéré ou non, les pertes de chiffre d'affaires et celles liées à la propriété intellectuelle sont chaque année considérables et représentent un immense manque à gagner pour les éditeurs de logiciels et les autorités locales. Des recettes qui pourraient être réinvesties dans la Recherche et le Développement pour concevoir et améliorer les programmes informatiques légitimes ne parviennent tout simplement jamais aux éditeurs de logiciels.

Une étude montre que le piratage informatique représente un manque à gagner pour 71 % des éditeurs de logiciels indépendants.[ii]

> Presque la moitié des entreprises participantes (48 %) reconnaissent ne pas être en conformité avec au moins un de leurs contrats de licence de logiciel.

Un scénario simple de piratage de logiciels est illustré ci-dessous. Une personne achète une licence pour utiliser une copie de votre logiciel, puis en fait plusieurs copies qui sont ensuite partagées ou vendues illégalement à d'autres personnes.

PIRATAGE DE LOGICIELS



Simon achète une copie du programme de Jenny, puis en fait des copies illégales.

La majorité des entreprises assimilent le piratage informatique à un acte de vol prémédité. Toutefois, le piratage informatique englobe également l'utilisation abusive intentionnelle ou non d'un logiciel concédé en licence. Une utilisation abusive involontaire peut par exemple avoir lieu lorsqu'une entreprise achète une licence pour l'utiliser sur un nombre limité de postes de travail mais l'utilise sur plus de machines qu'elle n'est autorisée à le faire.

Aujourd'hui, la majorité des utilisateurs finaux savent que l'utilisation non autorisée d'un logiciel est illégale. Toutefois, ils sont encore nombreux à négliger la valeur que représente un logiciel en termes de propriété intellectuelle.

Selon une étude de Vanson Bourne commanditée par Gemalto, presque la moitié des entreprises participantes (48 %) reconnaissent ne pas être en conformité avec au moins un de leurs contrats de licence de logiciel.

Manifestement, l'activité commerciale des éditeurs de logiciels est affectée. En effet, 71 % des personnes interrogées indiquent subir un manque à gagner causé par le piratage de logiciels. Par ailleurs, 79 % déclarent que leur manque à gagner est dû aux clients violant délibérément les contrats de licence. Et 82 % indiquent un manque à gagner supplémentaire causé par les clients violant involontairement les contrats de licence. [ii]

L'étude de la BSA révèle que sur 72 des 116 marchés faisant l'objet de cette étude, plus de 50 % des logiciels installés sur des ordinateurs en 2015 n'avaient aucune licence d'utilisation. Et sur 37 marchés, 75 % ou plus n'avaient aucune licence. [i]

Résultats de l'étude

71 %	des éditeurs de logiciels subissent des pertes de chiffre d'affaires à cause du piratage de logiciels.
79 %	des éditeurs de logiciels subissent un manque à gagner dû aux clients violant délibérément les contrats de licence.
82 %	des éditeurs de logiciels subissent un manque à gagner dû aux clients violant involontairement les contrats de licence.

Les conséquences

Manque à gagner : Le développement d'une application logicielle nécessite un investissement considérable de temps, d'argent et d'efforts. Le piratage de logiciels (notamment, les licences réseau illégales et les mises à niveau non respectées) vous prive de revenus mérités et nuit à vos clients qui, en fin de compte, paient le prix de l'utilisation illégale de vos produits.

Moins d'innovation : Le piratage limite votre compétitivité car il se traduit par des produits plus chers et moins sophistiqués pour vos clients.

Le piratage nuit à vos utilisateurs finaux : La violation des droits d'auteur porte préjudice à l'industrie des logiciels et a également des conséquences néfastes pour l'utilisateur final. Voici quelques raisons évidentes pour lesquelles les utilisateurs devraient éviter d'utiliser des logiciels sans licence :

- Ces logiciels peuvent contenir des programmes malveillants, être défectueux ou corrompus
- Aucun accès à l'assistance technique
- Pas de documentation produit, ni de garantie
- Contenu incorrect ou obsolète
- Difficulté à ou impossibilité de mettre le logiciel à niveau
- Procédures judiciaires coûteuses et/ou lourdes amendes

La solution : protection contre la copie et application des licences

Une stratégie bien pensée et exécutée pour combattre le piratage et l'utilisation illégale de logiciels est une mesure essentielle à mettre en place sur un marché ultra-concurrentiel. Elle devient même vitale dans un contexte économique difficile.

Les éditeurs de logiciels peuvent recourir à des mesures réactives ou préventives afin de lutter contre le piratage et l'utilisation illégale de logiciels :

Mesures réactives

La majorité des éditeurs de logiciels ne protègent pas leurs logiciels contre l'utilisation illégale. Ils se fient plutôt aux contrats de licences logicielles et aux droits d'auteur pour protéger leurs logiciels. Toutefois, ces mécanismes de contrôle n'empêchent pas un utilisateur de copier intentionnellement un logiciel. Ils n'évitent pas non plus l'utilisation abusive délibérée ou involontaire. Si un éditeur estime que son logiciel a été piraté ou utilisé illégalement, les méthodes réactives qu'il peut utiliser reposent sur les armes juridiques mises à disposition pour lutter contre les pirates informatiques.

Les organismes d'intervention FAST (Federation Against Software Theft), SIIA (Software Information Industry Association), BSA, WIPO (World Intellectual Property Office) et bien d'autres encore contribuent à éduquer les utilisateurs et à orienter la loi en faveur de la protection des éditeurs de logiciels. La BSA enquête, poursuit en justice et plaide des cas de piratage informatique. Elle a collaboré avec de nombreux éditeurs de logiciels pour régler des cas de piratage.

Une action en justeice, même si elle porte ses fruits, est néanmoins très coûteuse. Et parce qu'il s'agit d'une mesure intrinsèquement réactive, elle ne permet pas d'éviter le problème.

Mesures préventives

Les éditeurs de logiciels utilisent de nombreuses mesures technologiques préventives pour lutter contre le piratage et l'utilisation illégale de leurs produits.

Certains éditeurs commencent à adopter des pratiques d'écriture de code plus sécurisées.

D'autres écrivent leur propre code de protection et de distribution de licences. Les éditeurs qui demandent à leurs équipes de développeurs d'écrire du code de protection et de distribution de licences ont généralement très peu d'expérience en matière de sécurité, et disposent de ressources limitées pour tenir à jour le code de sécurité et avoir une longueur d'avance sur les pirates informatiques ; ils obtiennent donc des résultats limités.

> Les éditeurs qui demandent à leurs équipes de développeurs d'écrire du code de protection et de distribution de licences ont généralement très peu d'expérience en matière de sécurité, et disposent de ressources limitées pour tenir à jour le code de sécurité et avoir une longueur d'avance sur les pirates informatiques ; ils obtiennent donc des résultats limités.

La majorité des éditeurs de logiciels se fient au savoir-faire ainsi qu'à la sécurité et à l'application robustes des licences des solutions commerciales de monétisation pour lutter contre le piratage et l'utilisation illégale de leurs produits. L'utilisation d'une solution de protection et de distribution de licences peut permettre de commercialiser le produit plus rapidement, d'économiser les coûts de mise en place et de bénéficier d'un coût total de propriété réduit par rapport à une solution de distribution de licences développée en interne.

Les solutions commerciales les plus performantes ont recours à l'application de licences et d'un verrouillage logiciels, matériels ou dans le Cloud. Chacune d'entre elle a ses avantages propres et doit être envisagée en fonction des objectifs et des besoins précis de l'éditeur de logiciels et des demandes de ses clients. Par exemple, si l'éditeur fournit ses logiciels de façon dématérialisée, la protection logicielle et l'activation de produit seront généralement les méthodes les plus indiquées. Si le client souhaite accéder facilement à l'application protégée et pouvoir la transférer d'un ordinateur à un autre, il est fort probable qu'il opte pour la protection matérielle. De même, si le logiciel est acquis par abonnement et livré en tant que service, la distribution de licences dans le Cloud est le meilleur choix.
Il existe de nombreux autres problèmes supplémentaires à prendre en considération lors de la sélection du type de protection logicielle préventive et de distribution de licences à utiliser, notamment le niveau de sécurité requis, les méthodes de distribution, la portabilité, le prix du logiciel et bien plus encore. Les solutions de monétisation logicielle ont fait leur preuve en matière de lutte contre le piratage informatique et comme garantie d'une hausse du chiffre d'affaires.

L'application des licences et la protection contre la copie assurent une hausse du chiffre d'affaires, la protection de votre avantage concurrentiel et une meilleure expérience d'utilisation pour vos clients.

Exemple de meilleure pratique : TAISA

Sentinel HL protège le logiciel de maintenance préventive haut de gamme de TAISA contre le piratage informatique et l'utilisation illégale, tout en dynamisant considérablement ses ventes. Technical Applied International S.A. De C.T (TAISA), fondée en 1974 et basée au Mexique, est le pionnier des logiciels de maintenance préventive déployés dans le monde entier.

> « Nous avons commencé par développer notre propre protection logicielle mais au fil du temps, nous nous sommes rendu compte que notre solution ne suffisait pas pour protéger notre logiciel contre le piratage et les pertes de revenus. » -Pablo Seeliger, TAISA

Le défi commercial

Avec son logiciel de maintenance préventive, TAISA a mis sur le marché une architecture produit unique reposant sur du matériel de maintenance se trouvant sur trois sites différents et sur trois disques : un disque principal et deux disques pour les sauvegardes. Et tout ceci devait être protégé contre le piratage. Face à la demande grandissante du marché pour un logiciel de maintenance préventive et face à la concurrence de plus en plus féroce d'autres entreprises aux États-Unis, la solution de gestion des droits logiciels conçue en interne par TAISA ne suffisait plus à empêcher le piratage. Ils avaient besoin d'une solution plus robuste et plus sûre. « Depuis le développement de notre logiciel de maintenance préventive, il a toujours été nécessaire de le protéger » déclare Pablo Seeliger de TAISA. « Nous avons commencé par développer notre propre protection logicielle. Mais au fil du temps, nous nous sommes rendu compte que notre solution ne suffisait pas pour protéger notre logiciel contre le piratage et les pertes de revenus. » Après avoir réalisé qu'il était préférable d'utiliser une solution plus complète de protection de la propriété intellectuelle, TAISA a testé la compatibilité et les performances de sécurité de plusieurs logiciels de gestion des droits.

La solution

Après avoir testé Sentinel HL, M. Seeliger a été convaincu que ce produit convenait parfaitement pour assurer la sécurité du logiciel de TAISA. Sentinel s'intègre facilement au logiciel de maintenance préventive de TAISA, celui-ci ne fonctionne donc pas sans la clé Sentinel HL. De cette manière, l'utilisation non autorisée est impossible, la protection de la propriété intellectuelle est assurée et de nombreuses options de distribution de licences sont disponibles.

> « Suite à l'installation de Sentinel HL, nos ventes sont montées en flèche et aujourd'hui nous ne concevons pas de développer notre logiciel de maintenance préventive sans la solution Sentinel. »
> -Pablo Seeliger, TAISA

Les résultats

« Sans la solution Sentinel, nos pertes en matière de chiffre d'affaires auraient pu être de 20 ou 30 % » explique Pablo Seeliger. TAISA a désormais la garantie que son logiciel est entièrement protégé. Par ailleurs l'installation des clés de protection HL permet à TAISA de créer deux versions de son logiciel : une version d'utilisation autonome et une version d'utilisation en réseau permettant à plusieurs utilisateurs d'accéder au logiciel. Sentinel HL permet à TAISA de protéger son logiciel instantanément et d'augmenter ses ventes en le proposant à ses clients en plusieurs versions. « Suite à l'installation de Sentinel HL, nos ventes sont montées en flèche et aujourd'hui nous ne concevons pas de développer notre logiciel de maintenance préventive sans la solution Sentinel » affirme Pablo Seeliger.

L'installation de Sentinel HL a également permis à TAISA de conquérir de nouveaux marchés au Venezuela, en Colombie, en Argentine et en Espagne.

2 Activité sur les marchés parallèles

Les marchés parallèles, bien qu'étant moins connus, n'en représentent pas moins une menace potentiellement plus dévastatrice pour les éditeurs de logiciels et les fabricants d'appareils intelligents. Si rien n'est fait, cette pratique peut porter préjudice à votre marque, votre réseau de distribution, voire même votre chiffre d'affaires. Il est donc plus prudent de savoir comment les marchés parallèles peuvent affecter votre activité et quelles mesures vous pouvez prendre pour atténuer ce risque.

Un marché parallèle, tel qu'il est défini par Wikipédia, est un endroit où l'on voit s'échanger des biens par des canaux de distribution qui, bien que légaux, ne sont pas autorisés par le fabricant ou le propriétaire d'origine.

Penchons-nous un peu plus sur le mode de fonctionnement des marchés parallèles.

Il existe des marchés parallèles de nombreux produits fabriqués et vendus à travers le monde. Certains exemples de marchés parallèles les plus populaires auprès du grand public proposent à la vente des marques de montres de luxe, des automobiles, des téléphones portables, des produits de soins capillaires professionnels, des motifs de broderie numériques et des jeux sur PC. Des exemples de commerce B2B (interentreprises) incluent notamment les appareils médicaux, les machines d'automatisation industrielle, les logiciels professionnels et bien d'autres encore. Cette liste n'est pas exhaustive mais vous donnera déjà une idée.

Le marché parallèle des téléphones portables est un bon exemple. La majorité des fabricants de téléphones portables ne proposent pas de téléphones débloqués aux États-Unis. Les clients doivent acheter un téléphone portable associé à un opérateur de téléphonie spécifique (par ex ; T-Mobile, Verizon, AT&T, Sprint).

Comme vous pouvez l'imaginer, cette situation a vu naître un marché parallèle des téléphones cellulaires débloqués. Certains revendeurs d'appareils électroniques portables achètent des téléphones portables neufs (débloqués) hors des États-Unis et les revendent à un prix inférieur à celui des téléphones bloqués via des canaux de distribution autorisés. Bien qu'il ne s'agisse pas d'une pratique illégale, il arrive bien souvent que le client ne soit pas informé et qu'il ne sache pas que :

- les accessoires de chargement CA, s'ils sont inclus, ne sont généralement pas compatibles avec les normes électriques américaines et l'utilisateur devra acheter le chargeur adéquat séparément ;
- les téléphones sont bien souvent configurés par défaut dans une autre langue et doivent être reconfigurés par l'utilisateur ;
- les modes d'emploi, s'ils sont inclus, sont dans la langue du pays où le téléphone était supposé être vendu ; si un manuel d'utilisation est nécessaire, le consommateur devra le rechercher et le consulter en ligne ;
- bien souvent, les téléphones portables vendus sur les marchés parallèles ne sont pas sous garantie et ne peuvent pas être réparés par le fabricant.

Certains consommateurs sont prêts à accepter les inconvénients d'un achat sur les marchés parallèles afin d'obtenir les produits qu'ils veulent à bas prix. Toutefois, lorsqu'ils ont besoin de faire réparer leur produit et qu'ils réalisent que l'appareil qu'ils ont acheté n'est pas sous garantie, la fidélité envers la marque et la réputation de cette dernière peuvent en pâtir.

Les conséquences

Selon une récente étude de KPMG, les « OEM (fabricants d'équipement d'origine) estiment que les marchés parallèles ont un impact considérable sur leur activité, notamment sur leurs profits et leur image de marque. Environ la moitié des personnes interrogées déclarent que les produits issus des marchés parallèles sont en moyenne 25 % moins chers que ceux vendus par les partenaires distributeurs agréés. »[iii]

Les marchés parallèles nuisent aux systèmes de tarification segmentés et affectent les relations avec les canaux de distribution, l'image de marque et la fidélité envers la marque.

Baisse de la satisfaction des clients et dégradation de la fidélité envers la marque
Les produits des marchés parallèles sont souvent vendus à des prix plus bas aux clients peu méfiants qui réalisent, uniquement après coup, que le produit qu'ils ont acheté inclut des garanties non valables, est destiné à la vente dans un autre pays ou pire encore, est obsolète ou non conforme aux réglementations locales en vigueur.

Ces clients ne pourront pas obtenir de services après-ventes, de garantie ni de pièces de rechanges auprès des revendeurs agréés s'ils en ont besoin. Un produit ne répondant pas aux attentes du client a des répercussions sur sa satisfaction et sa fidélité envers la marque.

Relations difficiles avec les canaux de distribution
Bien qu'il soit difficile de contrôler ce paramètre, KPMG estime que jusqu'à 24 % des profits des canaux de distribution tombent entre les mains des vendeurs sur les marchés parallèles.[iii]

Toutefois, l'impact potentiellement le plus coûteux des marchés parallèles réside dans les relations commerciales au sein de votre réseau de distribution agréé. Les partenaires que vous autorisez à fournir des pièces et à assurer les réparations et le service après-vente des clients dans leurs pays font face à la pression croissante d'étendre leurs services aux clients ayant acheté leurs produits sur les marchés parallèles.

Détérioration de votre image de marque et de votre réputation
Vous avez fort probablement investi des millions d'euros en recherche et développement pour votre produit et pour établir une image de marque positive. Lorsque vos produits haut de gamme commencent à s'écouler sur les marchés parallèles à prix réduit, cela peut avoir un effet négatif sur votre image de marque et sur la réputation de votre entreprise.

Perturbation des ventes et de la commercialisation
Les marchés parallèles ont le potentiel de perturber vos prévisions de ventes les plus précises, vos stratégies de tarification, votre positionnement sur le marché et tous vos efforts de commercialisation.

La solution : Différentiation des produits, tarification segmentée, suivi et gestion des licences, distribution et utilisation

Pour préserver l'intégrité des canaux de vente, des produits et du chiffre d'affaires, tout en maintenant la satisfaction des clients, il est important de limiter la présence des logiciels et autres appareils intelligents sur les marchés parallèles. La question est de savoir s'il faut adopter une approche réactive, préventive ou une combinaison des deux.

Approche réactive : Traditionnellement, la défense contre les marchés parallèles est confiée aux avocats et aux tribunaux dans le cadre d'un contentieux. Dans certains des cas les plus médiatisés, les tribunaux ont, pour diverses raisons, tranchés en faveur des fabricants tels que Caterpillar, Kia, Gucci, HP et Intel. Toutefois, de telles mesures peuvent uniquement être prises si vous êtes informé de l'activité parallèle et que vous avez de bonnes raisons pour intenter une action.

En réalité, si vous n'avez pas une équipe entièrement dédiée à la surveillance de l'activité parallèle de vos produits et suffisamment de fonds pour financer la procédure judiciaire, la majorité des cas passent inaperçus ou ne sont pas contestés. En conséquence, vos produits continuent à circuler sur les marchés parallèles.

Même s'il est impossible d'interdire le détournement de produits sur les marchés parallèles, les éditeurs de logiciels et les fabricants de matériels auraient tout intérêt à mettre en place des stratégies proactives afin de limiter les conséquences désastreuses de telles activités.

Approche proactive : Heureusement, il existe des mesures proactives pour vous défendre contre le détournement de vos logiciels et appareils intelligents. Le déploiement d'une technologie de monétisation logicielle avec des fonctions de distribution de licences et de gestion des droits d'accès aux logiciels vous permettra de :

distinguer vos produits sur différents segments de marché.
La technologie de distribution de licences de logiciels vous permettra de développer différentes versions de vos produits afin de répondre aux :

- demandes spécifiques aux différentes régions ;
- normes de santé et de sécurité ;
- conditions requises pour formuler des offres ;
- habitudes de consommation ;
- normes techniques ;
- Niveaux de prix stratégiques.

Lorsque vous utilisez la distribution de licences pour distinguer vos appareils intelligents sur différents segments de marché, vous réduisez les coûts d'exploitation associés à la production et à l'inventaire, limitez l'évaluation par arbitrage et par conséquent, réduisez les ventes sur les marchés parallèles.

Contrôler et gérer les conditions générales d'utilisation de la licence, la distribution et l'utilisation
La gestion des droits d'accès peut être utilisée pour gérer et appliquer la distribution de licences de logiciels, de la distribution à l'activation du produit, en passant par son utilisation. En émettant et en contrôlant vos codes d'activation de manière électronique, vous êtes en mesure de suivre et de gérer tous les produits depuis l'heure de fabrication (sur votre propre site ou chez un sous-traitant) jusqu'à l'activation dans les locaux de l'utilisateur final, en passant par la distribution.

Exemple de meilleure pratique : fournisseur de périphériques réseau

Cette société américaine conçoit et vend des routeurs pour contrôler le trafic réseau des entreprises. Un élément essentiel de sa propriété intellectuelle est son firmware spécialement dédié qui permet de changer de débit et d'optimiser la bande passante.

Le défi : protéger ses routeurs contre l'activité des marchés parallèles

Le fournisseur de routeurs sous-traite la production de ses appareils à un fabricant étranger. La société veut se protéger contre la possibilité que son sous-traitant fabrique plus d'appareils que prévu et vende ces routeurs supplémentaires à des sociétés américaines à un prix largement inférieur à celui pratiqué par ses partenaires distributeurs agréés. En effet, une telle pratique entraînerait une perte de revenus chez le fournisseur de routeurs et détériorerait ses relations avec ses canaux de distribution.

La solution : déployer une solution de monétisation logicielle

Pour réduire la probabilité qu'une activité parallèle ne se mette en place, la société a choisi de déployer une solution de monétisation logicielle. L'utilisation des fonctions de distribution sécurisée de logiciels a permis à la société de distinguer ses produits pour différents segments de marché et de développer différentes versions de ses produits afin de répondre aux niveaux de prix stratégiques. Les fonctions de gestion des droits d'accès ont été utilisées pour gérer et mettre en place la distribution de licences, de la fabrication à la distribution jusqu'à l'activation du produit par l'utilisateur.

Les résultats : activités des marchés parallèles limitées et chiffre d'affaires assuré

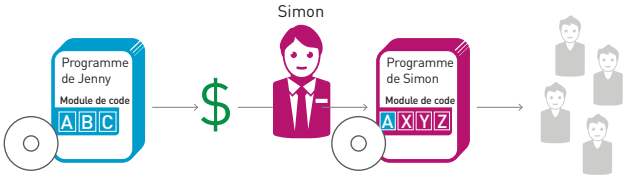
L'utilisation d'une solution de monétisation logicielle a permis à la société de protéger sa propriété intellectuelle. En limitant l'arbitrage par le prix, et en émettant et en suivant l'activation de ses produits de manière électronique, elle est également parvenue à limiter l'activité parallèle.

3 Ingénierie inversée et vol des secrets industriels

Les éditeurs de logiciels font d'énormes investissements en matière de recherche et de développement de leurs produits, d'écriture du code et de création d'une propriété intellectuelle qui représentera un avantage essentiel pour se démarquer de la concurrence sur le marché des logiciels et des appareils intelligents. La propriété intellectuelle est la valeur marchande la plus précieuse pour un éditeur de logiciels ou un fabricant d'appareils intelligents. Proportionnellement, la pression concurrentielle se fait naturellement sentir de plus en plus à l'heure où les entreprises luttent de manière acharnée pour conquérir de nouvelles parts de marché. L'espionnage industriel est de plus en plus courant et la précieuse propriété intellectuelle de votre logiciel (le code, les algorithmes, les fichiers de données d'application et les secrets industriels) est vulnérable aux personnes malveillantes, à l'ingénierie inversée, au vol et à la copie par des concurrents.

Il ne fait aucun doute que l'ingénierie inversée et le vol de secrets industriels ont des conséquences désastreuses sur les éditeurs de logiciels. Dans une étude récente, un pourcentage très élevé (84 %) d'éditeurs de logiciels indépendants à travers le monde ont indiqué être inquiets du risque de voir leur logiciel compromis. Par ailleurs, 81 % d'entre eux estiment que l'ingénierie inversée et le vol représentent un énorme manque à gagner [ii]

INGÉNIERIE INVERSÉE ET VOL



Simon extrait les secrets industriels contenus dans le code du programme de Jenny pour les utiliser dans le code de son programme et le vendre.

Les conséquences

Perte de compétitivité : due à l'ingénierie inversée et au vol de secrets industriels.

Manque à gagner : dû à la prolifération de copies de logiciels et de périphériques matériels intelligents.

Résultats de l'étude

84 %	des éditeurs de logiciels indépendants s'inquiètent du risque de voir leurs logiciels compromis.
81 %	des éditeurs de logiciels indépendants estiment que l'ingénierie inversée et le vol ont un impact négatif sur leur

La solution : protéger la propriété intellectuelle contre l'ingénierie inversée et le vol

Dans le contexte économique actuel, il est plus que jamais fondamental de renforcer votre avantage concurrentiel. Alors que la concurrence est de plus en plus vive, il est primordial de conserver cet avantage en sécurisant vos produits contre l'ingénierie inversée susceptible d'entraîner le vol de vos biens les plus précieux, notamment votre propriété intellectuelle et vos secrets industriels. En protégeant vos secrets industriels et votre code source contre les personnes malveillantes, vous pouvez conquérir de nouvelles parts de marché et continuer à maintenir et à développer votre compétitivité.

Les solutions logicielles sont composées de programmes exécutables et de DLL, mais elles contiennent aussi des fichiers de données d'une valeur encore plus grande que celle des applications logicielles. Dans la majorité des cas, ces fichiers de données contiennent des informations ultraconfidentielles ainsi que la propriété intellectuelle. Tout cela doit être protégé contre le vol et la copie par la concurrence.

Une solution de protection des logiciels et de distribution de licences offrant la technologie d'enveloppement automatique des fichiers (« wrapping ») garantit une protection solide de la propriété intellectuelle contre l'ingénierie inversée. En effet, grâce au chiffrement, à l'obfuscation du code et à l'antidébogage au niveau du système, les algorithmes, les secrets industriels et le savoir-faire professionnel intégrés dans les logiciels sont protégés contre les pirates informatiques.

La protection de la propriété intellectuelle garantit votre compétitivité et une hausse de votre chiffre d'affaires.

Exemple de meilleure pratique : Virtual Surveillance

Sentinel HL neutralise une attaque en cours, en protégeant les systèmes matériels et logiciels de Virtual Surveillance contre l'ingénierie inversée et le vol. Virtual Surveillance conçoit et commercialise des systèmes de surveillance vidéo numériques pour la surveillance et la protection sur plusieurs sites. La société produit également un logiciel d'analyse détectant les mouvements, les dispositifs de pièges numériques, les objets abandonnés ou supprimés, etc. Virtual Surveillance assure l'intégration aux systèmes d'alarme déjà existants et fournit des fonctions de déclenchement de l'alarme en fonction des mouvements détectés sur une vidéo fournie par son logiciel.

> En raison d'une attaque de piratage en cours, il était primordial de mettre en place une solution de protection très rapidement.

Le défi commercial

Virtual Surveillance avait commencé à produire un système de protection anti-copie en interne. Toutefois, leur solution développée en interne n'était pas suffisamment flexible pour permettre le transfert ou la copie de la licence logicielle sur une autre machine. Par exemple, si quelqu'un voulait utiliser les outils à disposition pour usurper les adresses MAC des cartes réseau, il pouvait le faire sans problème en réutilisant toujours la même clé de licence logicielle. Leurs pires craintes se sont matérialisées lorsqu'ils ont découvert une faille de sécurité. Une attaque d'ingénierie inversée était en cours sur leurs produits matériel et logiciel.

> Grâce à la clé Sentinel, Virtual Surveillance est rapidement parvenue à protéger son logiciel avant que la menace ne se transforme en vol manifeste.

La solution

Cette attaque a mené Virtual Surveillance à utiliser Gemalto Sentinel HL. Le logiciel est déployé sur plusieurs applications différentes. Chacune de ces applications dépend du service Web ASP.Net utilisé pour partager du contenu multimédia (vidéos et images instantanées). Cette méthode permet de synchroniser le contenu multimédia sur plusieurs machines et chez différents utilisateurs. Elle exige la saisie d'un code d'accès pour obtenir ces informations.

En raison des exigences de sécurité pour ces applications, il est impératif d'utiliser un réseau fermé. En créant un système utilisant les clés Sentinel pour protéger l'accès au service Web ASP.Net, Virtual Surveillance est en mesure de créer un point unique de défaillance qui rendra toutes les autres applications inutilisables. Ce service Web procède à des vérifications en temps réel de la clé Sentinel à chaque sollicitation. En cas d'absence de la clé, une erreur est envoyée à l'application cliente au lieu de répondre à la demande formulée.

En raison d'une attaque de piratage en cours, il était primordial de mettre en place une solution de protection très rapidement. Gemalto a fourni des instructions simples et concises avec un échantillon de code C# qu'ils ont pu modifier. Grâce à la clé Sentinel, Virtual Surveillance est rapidement parvenue à protéger son logiciel avant que la menace ne se transforme en vol manifeste.

> « Sentinel nous a donné les outils nécessaires pour protéger notre logiciel de façon complète. Ainsi, nous avons pu nous concentrer sur les besoins de nos clients. Le coût total de la protection de nos efforts de développement de plusieurs millions de dollars contre une menace connue s'est élevé à moins de 300 dollars, efforts de développement et frais d'expédition en un jour compris. » -Eric Burcham, Directeur technique chez Virtual Surveillance

Les récompenses

Après moins de deux heures d'efforts de développement et une mise à jour rapide sur site, Virtual Surveillance est parvenue à protéger ses efforts de développement de plusieurs millions de dollars contre une attaque d'ingénierie inversée en cours. Si le pirate était parvenu à ses fins, le coût aurait été incalculable pour la société.

Eric Burcham, directeur technique nous explique « qu'à elles seules, les clés coûtent mille fois moins que le temps et les efforts que nous aurions dû consacrer à coder notre propre protection et à générer et suivre manuellement les clés d'activation pour nos clients. »

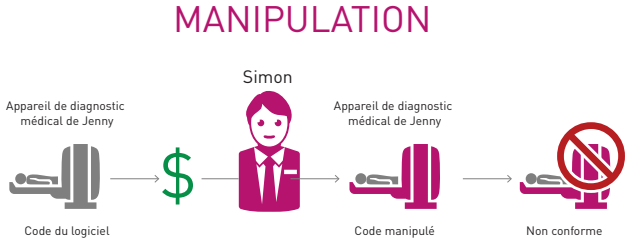
Étant une petite entreprise offrant une solution clé en main très spécialisée à un marché élitiste et en rapide évolution, Virtual Surveillance se devait de protéger ses atouts. Eric Burcham ajoute « Sentinel HL nous a donné les outils nécessaires à la protection intégrale de notre logiciel. Ainsi, nous avons pu nous concentrer sur les besoins de nos clients. Le coût total de la protection de nos efforts de développement de plusieurs millions de dollars contre une menace connue s'est élevé à moins de 300 dollars, efforts de développement et frais d'expédition en un jour compris. »

4 Manipulation

Le vol de secrets industriels est évidemment une catastrophe pour la majorité des éditeurs de logiciels indépendants et fabricants d'appareils intelligents. Mais la manipulation de code peut se révéler tout aussi désastreuse. Ces deux cas de figure peuvent éventuellement porter sérieusement préjudice à la part de marché globale d'une société et donc affecter son chiffre d'affaires potentiel.

On parle de manipulation du code lorsqu'une personne accède au code de votre logiciel et change son mode de fonctionnement. Il est important de noter que la manipulation de code peut être intentionnelle et malveillante, ou accidentelle et de bonne foi. La manipulation de code accidentelle par un utilisateur final est généralement détectée lorsqu'il est déjà trop tard et que le mal est fait.

L'exemple ci-dessous de manipulation de code en toute bonne foi concerne un appareil de diagnostic médical. Le logiciel embarqué est conçu pour contrôler le mode d'exécution des tests de diagnostic. Un utilisateur final estimant que le système est trop lent décide de modifier le code du logiciel de manière suffisante pour accélérer les calculs de 20 %. Mission accomplie ! Il peut désormais tester plus de patients par jour. Il n'y a ici aucune intention malveillante de la part de cet utilisateur.



Simon modifie sans autorisation le code du logiciel qui permet de faire fonctionner l'appareil intelligent de diagnostic médical de Jenny.

Toutefois, ce qu'il ne sait peut-être pas, c'est qu'en accélérant les opérations de calcul, il a également accélérer un processus qui a besoin de temps supplémentaire pour satisfaire à plusieurs normes médicales en vigueur. Les tests suivants effectués sur le matériel se révèleront inexacts. Et à qui sont adressées les critiques débouchant sur une baisse des ventes ? Pas à l'utilisateur qui a faussé l'appareil. Ni à l'hôpital. C'est le fabricant de matériel médical ou l'éditeur de logiciels qui sera blâmé pour avoir fourni un logiciel défectueux.

> Le vol de secrets industriels est évidemment une catastrophe pour la majorité des éditeurs de logiciels indépendants et fabricants d'appareils intelligents. Mais la manipulation de code peut se révéler tout aussi désastreuse. Ces deux cas de figure peuvent éventuellement porter sérieusement préjudice à la part de marché globale d'une société et donc affecter son chiffre d'affaires potentiel.

Les conséquences

La solution risque de ne plus atteindre les objectifs commerciaux : En raison de la manipulation du code, le logiciel et le matériel risquent de ne plus atteindre les objectifs commerciaux pour lesquels ils avaient été conçus.

Résultats inattendus : La manipulation du logiciel incorporé dans un appareil peut altérer le mode de fonctionnement de cet appareil et produire des résultats anormaux au niveau du système.

Manque à gagner : La manipulation du code peut éventuellement permettre aux utilisateurs d'accéder à des fonctions qu'ils n'ont pas payées.

Détérioration de l'image de marque : Les problèmes de conformité avec les réglementations peuvent avoir des conséquences désastreuses et irréversibles pour votre image de marque et pour la réputation de votre produit.

La solution : Protection contre la manipulation du code

Sans les technologies adéquates de chiffrement et d'obfuscation du code, les fournisseurs d'appareils intelligents exposent involontairement leur code à la manipulation.

Les éditeurs de logiciels et les fournisseurs d'appareils intelligents doivent mettre en place un contrôle rigoureux de l'accès au code source de leurs logiciels. Cela leur permettra de protéger leur chiffre d'affaires et d'assurer l'intégrité de leur marque et de leurs produits en empêchant la manipulation du code, l'ingénierie inversée et le vol de la propriété intellectuelle.

> Sans les technologies adéquates de chiffrement et d'obfuscation du code, les fournisseurs d'appareils intelligents exposent involontairement leur code à la manipulation.

Exemple de meilleure pratique : fabricant d'emballages industriels de premier plan

Cette étude de cas concerne l'un des plus grands fabricants d'emballages industriels. Il développe du matériel intelligent piloté par logiciel pour traiter le cycle tout entier de conditionnement de produits alimentaires liquides, tels que le lait et le jus d'orange destinés à la vente aux consommateurs. Le logiciel pilotant leur matériel de conditionnement est programmé pour respecter des dizaines de normes de santé publique et de sécurité.

Les inquiétudes de l'entreprise en matière de protection de la propriété intellectuelle se cristallisent sur le contrôle de l'accès au logiciel pilotant les machines et sur l'accès restreint aux paramètres principaux de contrôle des processus comme la pasteurisation. Ce fabricant de matériel utilise les solutions de monétisation logicielle Sentinel RMS et EMS pour protéger le code de son logiciel contre tout accès et manipulation non autorisés. Ces solutions lui permettent également de contrôler rigoureusement l'identité des personnes autorisées à modifier les paramètres de ses machines de conditionnement.

Conclusion

Les informations issues des études menées indiquent qu'un grand nombre d'éditeurs de logiciels sont inquiets de voir que leur propriété intellectuelle pourrait être compromise.

Si les éditeurs de logiciels s'inquiètent de ce genre de danger et des répercussions pour leur image de marque, leur compétitivité, la satisfaction des clients et leur chiffre d'affaires, pourquoi ne prennent-ils pas des mesures pour s'en protéger ?

Nous pensons que ces éditeurs de logiciels n'ont pas de marge de manœuvre ni le soutien de leur direction ou qu'ils n'ont pas encore vécu les conséquences désastreuses d'un vol de propriété intellectuelle. Les niveaux de préjudice sont variables. Le piratage informatique entraîne un manque à gagner à long terme. Toutefois, les conséquences d'une attaque d'ingénierie inversée ou de la manipulation de code peuvent être désastreuses et affecter une entreprise du jour au lendemain. Et il est en général très difficile de récupérer des pertes de cette envergure.

L'adoption de moyens permettant de réduire et d'empêcher le piratage informatique, l'activité des marchés parallèles, l'ingénierie inversée et la manipulation de la propriété intellectuelle présente dans le code du logiciel a de multiples avantages. L'utilisateur final a la certitude que les programmes dont il se sert fonctionnent comme prévu par l'éditeur et qu'il bénéficiera des services et garanties adéquats. L'industrie du logiciel est payée pour offrir des produits de qualité, dynamiser un marché concurrentiel et développer de nouveaux produits.

Mais la lutte contre le piratage nécessite une alliance des forces entre les consommateurs, les éditeurs de logiciels et les pouvoirs publics. Certaines des plus belles réussites se retrouvent en Amérique du Nord et en Europe où des programmes éducatifs sont associés à des mesures législatives.

En plus de cela, les éditeurs de logiciels doivent adopter une démarche proactive et positive qui se traduit par la mise en place de stratégies de protection des logiciels pour défendre leur propriété intellectuelle contre l'utilisation illégale, la copie, les activités parallèles, le vol et la manipulation.

Les différents exemples de meilleures pratiques l'ont montré : une solution de protection des logiciels et de distribution de licences ayant fait ses preuves sur le terrain est un moyen efficace de se protéger contre les quatre menaces pour la propriété intellectuelle. En effet, elle assure la protection des droits d'auteur, permet de lutter contre le piratage informatique, de maintenir vos prix sur un marché segmenté et de déjouer toutes les tentatives d'espionnage industriel et de falsification.

Par ailleurs, le déploiement d'une technologie de monétisation logicielle peut également être une stratégie d'avant-garde lucrative permettant d'augmenter les ventes, de réduire les coûts, de dynamiser la compétitivité et d'élargir et de conquérir de nouveaux marchés.

À propos de la monétisation logicielle avec Gemalto Sentinel

Gemalto est le leader du marché des solutions de gestion des droits d'accès et de distribution de licences logicielles pour les éditeurs de logiciels sur site, embarqués et dans le cloud. Gemalto Sentinel est la marque la plus fiable de l'industrie des logiciels pour ce qui est des solutions de monétisation logicielle sécurisées, souples et évolutives. Retrouvez plus de renseignements sur www.gemalto.com/france/monetisation-logicielle

Essayez gratuitement les solutions Sentinel !

Participez à la discussion !

- > 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, Étude mondiale de BSA sur les logiciels, Mai 2016, http://globalstudy.bsa.org/2016/downloads/studies/BSA_GSS_US.pdf

ii The State of Software Monetization, Recherche de Vanson Bourne commandée par 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

Nous contacter : Pour obtenir les emplacements et coordonnées de tous les bureaux, veuillez consulter la page www.gemalto.com/france/monetisation-logicielle

Suivez-nous sur : sentinel.gemalto.com/blog

GEMALTO.COM

gemalto
security to be free