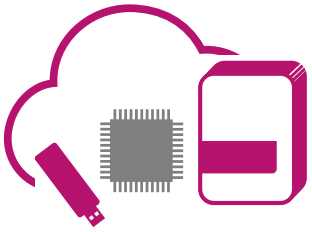
gemalto
security to be free



WHITE PAPER

# Come difendersi dalle quattro minacce alla proprietà intellettuale

## Un white paper per i produttori di software e i fabbricanti di dispositivi intelligenti

### Indice

## Panoramica

La tecnologia e l'innovazione avanzano a ritmo sempre più rapido e il software gioca un ruolo fondamentale in questo contesto. Il software è dappertutto: esistono prodotti software confezionati, software offerto come servizio su cloud o dispositivi hardware intelligenti, in data center, direttamente a casa tua o nel palmo della tua mano.

Le aziende che sviluppano questi prodotti hanno investito una quantità considerevole di tempo e denaro in ricerca e sviluppo, nonché nella scrittura del codice software. Il codice che fa funzionare questi prodotti software e dispositivi hardware intelligenti contiene segreti industriali ed è una proprietà intellettuale molto preziosa. Se non viene protetta adeguatamente, questa proprietà intellettuale può essere facilmente attaccata; ciò, a sua volta, può causare danni irreparabili al marchio di un'azienda, alla sua competitività, ai suoi profitti e all'esperienza d'uso offerta ai clienti.

Questo paper esamina le quattro minacce alla proprietà intellettuale e spiega come vengono effettuati i relativi attacchi. Descrive inoltre le conseguenze di una protezione inadeguata e presenta esempi di best practice adottate da produttori di successo: vedremo come questi ultimi stanno utilizzando soluzioni commerciali per la monetizzazione al fine di proteggere proattivamente i loro investimenti nella proprietà intellettuale e aumentare i profitti.

## Le quattro minacce alla proprietà intellettuale

Esistono diversi tipi di attacchi alla proprietà intellettuale:

- Pirateria informatica
- Reverse engineering e furto di segreti industriali
- Manomissione del codice
- Attività sul mercato grigio

Ognuna di queste minacce mette a repentaglio sia i profitti derivati dal software che l'innovazione futura di produttori di software e dispositivi intelligenti.

### 1 Pirateria informatica e uso illegale

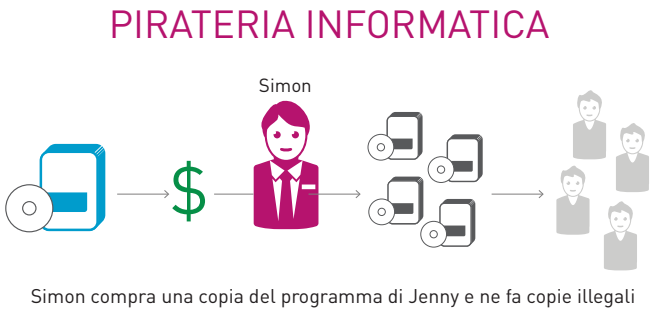
L'esempio più ovvio di danni alla proprietà intellettuale è la pirateria informatica. Si tratta di uso illegale e furto di software, più specificamente di copia e/o distribuzione non autorizzata di software informatico protetto da copyright, un atto che viola i diritti del produttore di software. Secondo la Business Software Alliance (BSA), nel 2015 il 39% del software installato sui computer di tutto il mondo non era autorizzato da un accordo di licenza, e la conseguente perdita di profitti a livello globale ammontava a 52,2 miliardi di dollari.[i]

A causa della pirateria, intenzionale o meno, ogni anno si registrano perdite elevate in termini di proprietà intellettuale e di profitti a scapito di aziende produttrici di software e amministrazioni locali. Tali profitti potrebbero essere reinvestiti in ricerca e sviluppo per creare e migliorare programmi software legittimi, ma purtroppo è denaro che non arriva mai ai produttori.

Dalle ricerche emerge che il 71% degli ISV ha perso profitti a causa della pirateria informatica.[ii]

> Quasi la metà delle imprese contattate (48%) ammette di non rispettare almeno uno dei rispettivi accordi di licenza software.

Qui di seguito descriveremo un semplice caso di pirateria informatica. Qualcuno acquista una licenza per utilizzare una copia di un programma software e crea poi diverse copie che vengono condivise o vendute ad altri illegalmente.




Simon compra una copia del programma di Jenny e ne fa copie illegali

La maggior parte delle organizzazioni associa la pirateria informatica al furto intenzionale; tuttavia, essa include anche casi di utilizzo eccessivo, sia intenzionale che involontario, di software concesso in licenza legalmente. Un esempio di utilizzo eccessivo involontario è il caso dell'azienda che acquista una licenza per utilizzare un determinato numero di postazioni, ma in realtà ne usa più di quante potrebbe.

Sebbene oggi la maggior parte degli utenti finali sappia che l'uso non autorizzato di software è illegale, molti sembrano non considerare il software come proprietà intellettuale con un proprio valore.

Secondo la ricerca condotta da Vanson Bourne su richiesta di Gemalto, quasi la metà delle imprese contattate (48%) ammette di non rispettare almeno uno dei rispettivi accordi di licenza software.

Il 71% dei produttori di software intervistati sostiene di aver perso profitti a causa della pirateria informatica: è evidente che il problema ha un impatto negativo sul settore. Inoltre, il 79% afferma di aver perso profitti a causa di clienti che violano intenzionalmente accordi di licenza. Infine, l'82% dichiara di subire perdite aggiuntive a causa di clienti che violano tali accordi involontariamente. [ii]

Secondo lo studio condotto dalla BSA, in 72 dei 116 mercati indagati, oltre il 50% del software per PC fornito nel 2015 non era autorizzato da licenza. Inoltre, più del 75% del software non era autorizzato in 37 di questi mercati.[i]

## Risultati del sondaggio

| | |
|---|---|
| **71%** | dei produttori di software sta perdendo profitti a causa della pirateria informatica |
| **79%** | dei produttori di software sta perdendo profitti a causa di clienti che violano intenzionalmente accordi di licenza |
| **82%** | dei produttori di software sta perdendo profitti a causa di clienti che violano involontariamente accordi di licenza |

### L'impatto

Profitti perduti - Sviluppare un'applicazione software implica ingenti investimenti in termini di tempo, denaro e sforzi. La pirateria informatica (incluse licenze di rete illegali e upgrade non ufficiali) ti priva dei profitti che ti spettano e danneggia i tuoi clienti paganti: sono loro che, in definitiva, pagano per l'uso illegale dei tuoi prodotti.

Meno innovazione - La pirateria limita la tua competitività e porta a prodotti più cari e meno innovativi per i tuoi clienti.

La pirateria danneggia i tuoi clienti finali - La violazione del copyright danneggia non solo il settore del software, ma anche il cliente finale. Esistono vari motivi per cui gli utenti devono evitare il software non autorizzato.

- Il software può contenere malware, essere difettoso o corrotto
- Non è possibile accedere all'assistenza tecnica
- Mancano la documentazione e le garanzie relative al prodotto
- Il contenuto può essere errato o datato
- È difficile o impossibile eseguire l'upgrade
- Cause legali costose e/o penali significative

### La soluzione: protezione da copia e implementazione di licenze

Una strategia ben programmata ed eseguita per combattere la pirateria e l'uso illegale di software è una pratica fondamentale in un mercato forte, e diventa ancora più importante in un ambiente economico difficile.

I produttori di software possono adottare misure reattive o preventive per far fronte alla pirateria e all'uso illegale:

**Misure reattive**

Molti produttori di software non fanno nulla per tutelare il proprio software dall'uso illegale. Si affidano semplicemente agli accordi di licenza software e alle leggi vigenti sul copyright. Tuttavia, questi meccanismi di controllo non impediscono ad un utente di copiare il software intenzionalmente. Inoltre, non prevengono l'utilizzo eccessivo intenzionale o involontario. Se un produttore crede che il suo software sia stato piratato o usato illegalmente, l'efficacia dei metodi reattivi si riduce ai rimedi legali a sua disposizione per contrastare i pirati informatici.

Organizzazioni di vigilanza come la Federation Against Software Theft (FAST), la Software Information Industry Association (SIIA), la BSA, l'Organizzazione mondiale per la proprietà intellettuale (WIPO) e altre si stanno adoperando per educare gli utenti e promuovere normative a tutela dei produttori di software. La BSA inoltre investiga, persegue e avvia cause per casi di pirateria informatica segnalati e collabora con molti produttori di software nella risoluzione di casi di questo genere.

Sicuramente, le azioni legali sono importanti, ma possono essere molto costose. In più, sono essenzialmente reattive, quindi non possono prevenire il problema.

**Misure proattive**

Esistono numerose misure preventive di natura tecnologica che vengono adottate dai produttori di software per combattere la pirateria e l'uso illegale.

Alcuni produttori adottano pratiche di scrittura di codice più sicure.

Altri scrivono un proprio codice per la protezione e il licensing. I produttori che si affidano al proprio team di sviluppo per scrivere un codice per la protezione e il licensing in-house hanno solitamente meno esperienza nel campo della sicurezza, risorse limitate per il mantenimento di tale codice e la lotta contro gli hacker, e ottengono quindi risultati limitati.

> I produttori che si affidano al proprio team di sviluppo per scrivere un codice per la protezione e il licensing in-house hanno solitamente meno esperienza nel campo della sicurezza, risorse limitate per il mantenimento di tale codice e la lotta contro gli hacker, e ottengono quindi risultati limitati.

Per far fronte a pirateria e uso illegale, molti produttori di software preferiscono l'esperienza, la sicurezza e l'implementazione di licenze garantite dalle soluzioni per la monetizzazione disponibili sul mercato. Avvalersi di una soluzione commerciale per la protezione e il licensing può risultare in un tempo di commercializzazione più rapido, risparmi nell'implementazione e un minor costo di proprietà in confronto al licensing sviluppato in-house.

Le soluzioni commerciali più potenti implementano il licensing e vincolano le licenze con software, hardware o su cloud. Ognuna di queste opzioni ha i suoi vantaggi e deve essere valutata alla luce degli obiettivi specifici e delle esigenze del produttore di software, nonché dei bisogni dei suoi clienti. Ad esempio, se il produttore fornisce il software in forma elettronica, una protezione e un'attivazione del prodotto tramite software è generalmente l'opzione migliore. Se il cliente utente finale richiede un accesso facile all'applicazione protetta e una portabilità tra diversi computer, verrà probabilmente scelta la protezione hardware. Se il software è concesso via abbonamento e fornito come servizio, il licensing basato su cloud è la scelta ottimale.
La scelta di un'opzione proattiva per il licensing e la protezione di software deve tener conto di diversi altri fattori, come il livello di sicurezza richiesto, i metodi di distribuzione, la portabilità, il prezzo del software e altri ancora. Le soluzioni commerciali per la monetizzazione del software sono un metodo di comprovata efficacia per la prevenzione della pirateria informatica e la tutela dei profitti derivati dal software.

La protezione da copia e l'implementazione di licenze assicurano profitti, proteggono il tuo vantaggio competitivo e garantiscono ai tuoi utenti finali una migliore esperienza d'uso.

## Caso di best practice: TAISA

Sentinel HL protegge il software di manutenzione preventiva ad alto valore di TAISA dalla pirateria e dall'uso illegale, aumentando significativamente le vendite. Technical Applied International S.A. De C.T. (TAISA) è stata fondata nel 1974 e ha sede in Messico; si tratta di un fornitore leader sul mercato internazionale di software di manutenzione preventiva.

> "Inizialmente abbiamo sviluppato in-house una soluzione per la protezione del software, ma poi abbiamo capito che era troppo semplice per proteggere il nostro software da pirateria e perdite." -Pablo Seeliger, TAISA

### La sfida

Il software prodotto da TAISA presenta un'architettura speciale che si basa su strumenti di manutenzione presso tre impianti e su tre dischi, un disco master e altri due di backup; tutti e tre necessitano di protezione anti-pirateria. Col tempo, la richiesta di questo tipo di software è aumentata e la concorrenza da parte di altre aziende americane si è fatta più agguerrita: la soluzione di TAISA non era più sufficiente per far fronte alla pirateria. Era necessaria una soluzione più solida e affidabile. "Fin da quando abbiamo sviluppato il nostro software, c'è sempre stato il bisogno di proteggerlo," ha detto Pablo Seeliger di TAISA. "Inizialmente abbiamo sviluppato in-house una soluzione per la protezione del software, ma poi abbiamo capito che era troppo semplice per proteggere il nostro software da pirateria e perdite." Quando ha capito di aver bisogno di una protezione della proprietà intellettuale più completa, TAISA ha testato la compatibilità e la sicurezza offerte da diversi prodotti per la gestione di diritti software.

### La soluzione

Una volta testata la soluzione Sentinel HL, Seeliger ha capito che avrebbe potuto offrire a TAISA la sicurezza necessaria per il suo software. Sentinel si integra perfettamente al software prodotto da TAISA: questo software non può essere eseguito senza la chiave Sentinel SL, al fine di prevenire l'uso non autorizzato, proteggere la proprietà intellettuale e offrire varie opzioni di licensing.

> "A seguito dell'implementazione di Sentinel HL, le vendite sono aumentate considerevolmente: oggi sappiamo che sarebbe impossibile sviluppare ulteriormente il nostro software senza Sentinel." -Pablo Seeliger, TAISA

## I risultati

"Senza Sentinel, le nostre perdite in termini di vendite sarebbero state del 20% o 30%," ha spiegato Seeliger. TAISA è ora in grado di proteggere il suo prodotto con la massima sicurezza; inoltre, le chiavi di protezione HL permettono di creare due versioni del software: una versione per un singolo utente e una versione di rete che consente a più utenti di accedere al software. Con Sentinel HL, TAISA è in grado di proteggere il suo software con un'unica soluzione e fornirlo ai clienti in diversi formati, con un conseguente aumento delle vendite. "A seguito dell'implementazione di Sentinel HL, le vendite sono aumentate considerevolmente: oggi sappiamo che sarebbe impossibile sviluppare ulteriormente il nostro software senza Sentinel," ha detto Seeliger.

Grazie a Sentinel HL, TAISA ha potuto espandersi con sicurezza su mercati come Venezuela, Colombia, Argentina e Spagna.

## 2 Vendite sul mercato grigio

Le vendite sul mercato grigio sono una minaccia meno conosciuta ma non meno devastante, che mette in pericolo produttori di software e dispositivi intelligenti. Se ignorata, questa pratica può danneggiare il tuo marchio, il tuo canale e perfino i tuoi profitti. Pertanto, è importante capire come le vendite sul mercato grigio possono avere un impatto sulla tua attività e sviluppare contromisure per mitigare i rischi.

Un mercato grigio, così come definito da Wikipedia, è il commercio di un prodotto tramite canali di distribuzione legali ma non destinati a quello scopo dal produttore originale.

Diamo uno sguardo più approfondito a questo tipo di mercati.

I mercati grigi esistono per diversi tipi di prodotti venduti in tutto il mondo. Alcuni esempi di prodotti sul mercato grigio destinati ai consumatori sono marche di orologi di lusso, automobili, cellulari, prodotti professionali per capelli, schemi digitali per ricami e videogiochi per PC. Tra gli esempi B2B troviamo dispositivi medici, macchine per l'automatizzazione industriale, software aziendale e così via. Questo elenco non è esaustivo, ma sicuramente rende l'idea.

Il mercato grigio dei cellulari è un buon esempio. Negli Stati Uniti, molti produttori di cellulari non offrono telefoni sbloccati. I clienti devono acquistare cellulari bloccati da un fornitore di servizi di telefonia cellulare specifico (ad esempio T-Mobile, Verizon, AT&T o Sprint).

Come ci si può aspettare, ciò ha creato un mercato grigio di cellulari sbloccati. Alcuni rivenditori di dispositivi elettronici mobili acquistano all'estero cellulari nuovi (sbloccati) e li rivendono negli Stati Uniti a un prezzo inferiore rispetto ai cellulari bloccati attraverso canali autorizzati. Questa non è una pratica illegale, ma spesso il cliente non è al corrente della situazione e può essere fuorviato nei modi seguenti:

- il caricabatterie, se incluso, di solito è incompatibile con le specifiche di corrente statunitensi e l'utente deve quindi acquistare il caricabatterie appropriato separatamente;
- spesso, il cellulare stesso è impostato su un'altra lingua e deve essere resettato dall'utente;
- il manuale di istruzioni, se incluso, è scritto nella lingua della regione a cui era destinato il cellulare. Se al cliente serve un manuale, dovrà cercarlo online;
- spesso, i cellulari disponibili sul mercato grigio non includono una garanzia, quindi non possono essere inviati al produttore per ricevere assistenza.

Alcuni consumatori non si preoccupano di questi inconvenienti e preferiscono comprare quello che vogliono ad un prezzo ridotto su questi mercati paralleli. Ma quando avranno bisogno di assistenza e si accorgeranno che il prodotto acquistato non è coperto da garanzia, la fedeltà al marchio e la reputazione di quest'ultimo potrebbero risentirne.

### L'impatto

Secondo un recente sondaggio di KPMG, "gli OEM sentono l'impatto che ha il mercato grigio sulle loro attività, soprattutto in termini di profitti e reputazione del marchio. Circa la metà degli intervistati dichiara che i prodotti sul mercato grigio sono spesso scontati del 25% rispetto al prezzo medio autorizzato per i channel partner." [iii]

I mercati grigi danneggiano le politiche sui prezzi in base ai segmenti e quindi le relazioni con i partner di canale, la reputazione e la fedeltà al marchio.

#### Danni alla soddisfazione del cliente e alla fedeltà al marchio

I prodotti sul mercato grigio sono spesso venduti ad un prezzo ribassato a clienti ignari, che scoprono solo successivamente che il prodotto acquistato include garanzie non valide, era destinato all'uso in altri paesi o - peggio ancora - è obsoleto o non è conforme ai requisiti di legge locali.

Questi clienti non possono usufruire di servizi, assistenza durante il periodo di garanzia e parti di ricambio fornite dai rivenditori autorizzati. E se il prodotto non soddisfa le aspettative del cliente, la sua soddisfazione e la sua fedeltà ne risentiranno, con conseguente danno alla fedeltà al marchio.

**Relazioni di canale indebolite**
Anche se è difficile da monitorare, KPGM stima che fino al 24% dei profitti di un determinato canale possono finire nelle tasche di commercianti sul mercato grigio.[iii]

Tuttavia, l'impatto potenzialmente più fatale delle vendite sul mercato grigio si ha sulle relazioni con la rete di distribuzione autorizzata. I partner che hai autorizzato a fornire parti di ricambio, riparazioni e assistenza promozionale ai clienti nelle loro regioni sono sempre più sotto pressione, a causa delle richieste di supporto da parte di clienti che hanno acquistato i tuoi prodotti sul mercato grigio.

**Danni all'immagine e alla reputazione della tua azienda**
Probabilmente avrai investito milioni in ricerca e sviluppo di prodotti e nella creazione di un'immagine positiva per il tuo marchio. Quando i prodotti che normalmente vendi a un prezzo elevato iniziano ad arrivare sul mercato grigio a prezzi ribassati, il tuo marchio ne può risentire, così come la reputazione della tua azienda.

**Danni al marketing di vendite e prodotti**
L'attività sul mercato grigio può compromettere l'accuratezza delle previsioni di vendita, le strategie relative ai prezzi, il posizionamento sul mercato e altri aspetti del marketing.

## La soluzione: differenziare i prodotti, definire i prezzi in base ai segmenti, monitorare e gestire i termini di licenza, distribuzione e utilizzo

Per preservare l'integrità di canali di vendita, prodotti e profitti, e allo stesso tempo accontentare i clienti, è importante limitare l'esposizione di software e dispositivi intelligenti al mercato grigio. L'azienda dovrà decidere se adottare un approccio reattivo, un approccio proattivo o una combinazione dei due.

Approccio reattivo - Di norma, la protezione dal mercato grigio tramite le vie legali è compito degli avvocati e del sistema giudiziario. In alcuni casi emblematici, in tribunale hanno vinto, per vari motivi, produttori come Caterpillar, Kia, Gucci, HP e Intel.Ma queste sono misure reazionarie che possono essere adottate solo se si è a conoscenza delle vendite sul mercato grigio e se l'accusa ha un fondamento concreto.

In realtà, a meno di non avere personale specificamente addetto al mercato grigio e di non disporre di ingenti fondi, la maggior parte dei casi non viene rilevata e/o non viene contestata, per cui i prodotti continuano ad essere deviati su questo mercato.

Anche se è impossibile bandire la vendita di prodotti sul mercato grigio, i fornitori di software e i produttori di dispositivi dovrebbero implementare strategie proattive per limitare i danni.

Approccio proattivo - Fortunatamente, esistono modi proattivi di difendersi dalla deviazione sul mercato grigio del tuo software e dei tuoi dispositivi intelligenti.L'impiego di una tecnologia disponibile sul mercato per la monetizzazione del software che prevede software licensing e gestione delle autorizzazioni ti consente di:

**Differenziare il tuo prodotto per vari segmenti di mercato**
Una tecnologia sofisticata per il software licensing ti consente di sviluppare più versioni dei tuoi prodotti per soddisfare:

- diverse regioni geografiche
- normative sanitarie e di sicurezza
- requisiti di imballaggio
- abitudini di consumo
- Standard tecnologici
- fasce di prezzo strategiche

Utilizzando il software licensing per differenziare i tuoi dispositivi intelligenti per diversi segmenti di mercato, puoi ridurre i costi operativi associati alla produzione e all'inventario, limitare l'arbitraggio dei prezzi e quindi le vendite sul mercato grigio.

**Monitorare e gestire i termini, la distribuzione e l'uso delle licenze**
La gestione di autorizzazioni può essere utilizzata per organizzare e implementare il software licensing, dalla distribuzione fino all'attivazione del prodotto e all'uso effettivo. Grazie all'emissione e al controllo elettronico di codici di attivazione, puoi monitorare e gestire tutti i prodotti dal momento della produzione - nel tuo stabilimento o in un altro in outsourcing - alla distribuzione, fino poi all'attivazione e all'utilizzo da parte dell'utente finale.

### Caso di best practice: rivenditore di dispositivi di rete

Quest'impresa americana progetta e vende router per il controllo del traffico di rete delle aziende. Un componente fondamentale della sua preziosa proprietà intellettuale risiede nel suo speciale firmware che permette di regolare la velocità di elaborazione e l'ottimizzazione del traffico su Internet.

### Sfida: evitare la vendita dei router sul mercato grigio

Il rivenditore di router affida ad un produttore terzo all'estero la produzione dei suoi router. L'azienda vuole evitare che quest'ultimo produca un surplus di unità per poi rivenderlo ad altre aziende statunitensi a un prezzo molto inferiore rispetto a quello dei suoi channel partner autorizzati. Quest'attività, infatti, sottrarrebbe profitti dal rivenditore di router e danneggerebbe le relazioni con i partner di canale.

### Soluzione: implementazione di una soluzione commerciale per la monetizzazione del software

Per ridurre il rischio di vendite sul mercato grigio, l'azienda produttrice di router ha scelto di implementare una soluzione commerciale per la monetizzazione del software. Grazie all'impiego di un licensing sicuro, l'azienda ha potuto differenziare i suoi prodotti per diversi segmenti di mercato e sviluppare più versioni di ogni prodotto, adatte alle diverse fasce di prezzo. Grazie alla gestione di autorizzazioni, è stato possibile gestire e implementare il licensing a partire dal momento della produzione fino alla distribuzione tramite canali e all'attivazione da parte dell'utente finale.

### Risultati: attività sul mercato grigio limitata e profitti assicurati

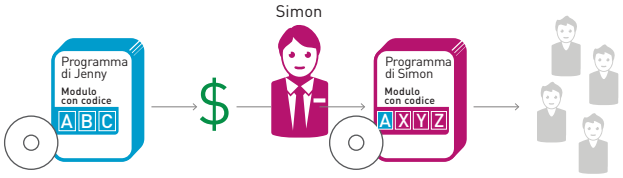
Il ricorso ad una soluzione commerciale per la monetizzazione del software ha permesso a questo rivenditore di router di proteggere la sua proprietà intellettuale, limitare l'arbitraggio dei prezzi ed emettere e monitorare elettronicamente le attivazioni dei prodotti, al fine di limitare le attività sul mercato grigio.

## 3 Reverse engineering e furto di segreti industriali

I produttori di software investono ingenti risorse in ricerca e sviluppo per i loro prodotti, nella scrittura di codice e nella creazione di proprietà intellettuale. Quest'ultima infatti costituisce un vantaggio chiave e consente di differenziare i propri prodotti rispetto al software dei concorrenti e ai dispositivi intelligenti su base software. La proprietà intellettuale costituisce la quota principale del valore sul mercato di una tipica azienda produttrice di software o di dispositivi intelligenti. Allo stesso tempo, la competizione aumenta naturalmente a mano a mano che le aziende tentano di imporsi sul mercato in modo più aggressivo. Lo spionaggio industriale è sempre più comune e la proprietà intellettuale nel tuo software - contenente codice, algoritmi, file di dati di applicazioni e segreti industriali - è esposta a sguardi indiscreti, reverse engineering, furto ed imitazione da parte della concorrenza.

Non c'è dubbio: il reverse engineering e il furto di segreti industriali stanno danneggiando i produttori di software. Secondo un recente sondaggio, ben l'84% degli ISV intervistati a livello globale afferma di essere preoccupato per la vulnerabilità del proprio software. Inoltre, l'81% crede che il reverse engineering e il furto stia costando loro profitti. [ii]

REVERSE ENGINEERING E FURTO




Simon estrae segreti industriali dal codice del programma di Jenny, li usa nel proprio codice e poi vende il programma

### L'impatto

Perdita di vantaggio competitivo: a causa del reverse engineering e del furto di segreti industriali.

Perdita di profitti: a causa della proliferazione di imitazioni di software e dispositivi hardware su base software.

### Risultati del sondaggio

| | |
|---|---|
| **84%** | degli ISV è preoccupato per la vulnerabilità del proprio software |
| **81%** | degli ISV crede che il reverse engineering e il furto stiano danneggiando i suoi profitti |

## La soluzione: protezione da reverse engineering e furto

Nell'attuale situazione economica è più essenziale che mai consolidare il tuo vantaggio competitivo. Quando la concorrenza si fa più agguerrita, è importante conservare quel vantaggio proteggendo i tuoi prodotti dal reverse engineering, l'attività che favorisce il furto di proprietà intellettuale e segreti industriali. È proteggendo i tuoi segreti industriali e il tuo codice sorgente da sguardi indiscreti che puoi mantenere la tua quota di mercato e incrementare il tuo vantaggio competitivo.

I prodotti software non consistono solo in file eseguibili e DLL, bensì anche in file dati che potrebbero essere ancora più preziosi delle applicazioni stesse. In molti casi, questi dati contengono proprietà intellettuale e informazioni particolarmente sensibili che devono essere protette dal furto e dall'imitazione da parte della concorrenza.

Una soluzione commerciale per il licensing e la protezione del software, dotata di una tecnologia di file wrapping automatica, protegge in modo sicuro la tua proprietà intellettuale dal reverse engineering tramite la crittografia di file, l'offuscamento di codice e l'anti-debugging a livello di sistema, di modo che gli algoritmi, i segreti industriali e il know-how professionale nel software siano al sicuro dagli hacker.

La difesa della tua proprietà intellettuale protegge il tuo vantaggio competitivo e i tuoi profitti.

## Caso di best practice: Virtual Surveillance

Sentinel HL è in grado di sventare un attacco in corso e protegge i sistemi hardware e software di Virtual Surveillance da furto e reverse engineering. Virtual Surveillance progetta e vende sistemi di videosorveglianza digitali per la protezione e la sorveglianza di attività in più siti. L'azienda produce inoltre software per l'analisi di movimenti, inclusi rilevamento di movimenti, linee virtuali, rilevamento oggetti abbandonati o rimossi ecc. I prodotti di Virtual Surveillance si integrano nei sistemi di allarme già installati ed è possibile attivare l'allarme sulla base di qualsiasi movimento rilevato dal software nel segnale video.

> L'azienda aveva percepito una minaccia di attacco informatico ed era essenziale agire immediatamente.

### La sfida

In origine, Virtual Surveillance aveva sviluppato in-house la sua protezione da copia. Tuttavia, con questa soluzione risultava difficile copiare la licenza software o trasferirla su un'altra macchina. Ad esempio, se qualcuno avesse utilizzato uno degli strumenti disponibili per lo spoofing degli indirizzi MAC delle schede di rete, avrebbe potuto continuare a riutilizzare un'unica chiave di licenza software. Questo timore si è trasformato in realtà quando è stata scoperta una violazione della sicurezza. Qualcuno stava tentando di eseguire il reverse engineering dei loro prodotti hardware e software.

> Grazie alla chiave Sentinel, Virtual Surveillance è stata in grado di proteggere il suo software prima che la minaccia potesse concretizzarsi in un furto vero e proprio.

### La soluzione

Dopo l'attacco, Virtual Surveillance ha scelto di usare Sentinel HL di Gemalto. Il software è ripartito su diverse applicazioni, ognuna dipendente da un servizio web ASP.Net utilizzato per condividere media, come video o screenshot. Questo metodo consente la sincronizzazione dei media tra più macchine e utenti e richiede un codice d'accesso per ottenere le informazioni.

Visti i requisiti di sicurezza di queste applicazioni, è assolutamente necessario avere una rete chiusa. Grazie a un sistema che utilizza chiavi Sentinel per proteggere l'accesso al servizio web ASP.Net, Virtual Surveillance può creare un single point of failure, rendendo inutili le altre applicazioni. Il servizio web controlla in tempo reale la chiave Sentinel durante ogni chiamata. Se la chiave non fosse presente, invierebbe un segnale di errore all'applicazione client, invece di soddisfare la richiesta.

L'azienda aveva percepito una minaccia di attacco informatico ed era essenziale agire immediatamente. Gemalto ha fornito istruzioni veloci e semplici e un codice campione C# da modificare. Grazie alla chiave Sentinel, Virtual Surveillance è stata in grado di proteggere il suo software prima che la minaccia potesse concretizzarsi in un furto vero e proprio.

> "Sentinel ci ha dato gli strumenti necessari per proteggere al meglio il nostro software: adesso possiamo concentrarci sulle esigenze dei nostri clienti. Il costo totale della protezione del nostro investimento plurimilionario da una minaccia conosciuta è stato inferiore a 300 dollari, incluso il tempo di sviluppo e la spedizione nei due sensi da un giorno all'altro." -Eric Burcham, CTO, Virtual Surveillance

### Le ricompense

Dopo meno di due ore di sviluppo e un rapido aggiornamento in loco, Virtual Surveillance ha messo in salvo il suo investimento plurimilionario da un attacco in corso di reverse engineering. Se quest'ultimo fosse andato a segno, i costi sarebbero stati incalcolabili.

"Le chiavi stesse," ha notato il CTO Eric Burcham, "sono costate il mille per cento in meno rispetto al tempo e al lavoro che avremmo dovuto impiegare per creare una soluzione e generare e monitorare manualmente le chiavi di attivazione per i clienti."

Virtual Surveillance è un'azienda di dimensioni ridotte che offre una soluzione chiavi in mano altamente specializzata per un mercato d'élite in rapido cambiamento, e che quindi aveva bisogno di proteggere le sue risorse. Burcham ha aggiunto: "Sentinel HL ci ha dato gli strumenti necessari per proteggere al meglio il nostro software, così abbiamo potuto concentrarci sulle esigenze dei nostri clienti. Il costo totale della protezione del nostro investimento plurimilionario da una minaccia conosciuta è stato inferiore a 300 dollari, incluso il tempo di sviluppo e la spedizione nei due sensi da un giorno all'altro."

## 4 Manomissione

Il furto di segreti industriali può risultare catastrofico, ma per molti ISV e produttori di dispositivi intelligenti la manomissione del codice può essere altrettanto devastante. Entrambe le minacce possono danneggiare significativamente la quota di mercato e quindi diminuire il potenziale di profitto.

La manomissione si verifica quando qualcuno accede al codice del tuo software e modifica il funzionamento del tuo prodotto. È importante capire che la manomissione può essere intenzionalmente dannosa, oppure involontaria e con buone intenzioni. La manomissione involontaria ad opera di un utente finale solitamente non viene rilevata finché il danno è fatto ed è troppo tardi.

Nell'esempio qui sotto, consideriamo un dispositivo di diagnosi medica. Il software interno è stato progettato per controllare l'esecuzione di test diagnostici. Immaginiamo un utente finale che crede che il sistema sia troppo lento e decide di modificare il codice del software per velocizzare i calcoli del 20%. Missione compiuta: adesso può esaminare più pazienti al giorno. L'intenzione non è quella di danneggiare il produttore.

Quello che l'utente non sa è che in questo modo ha velocizzato un processo che usa il tempo in più per rispettare diverse normative del settore medico. I test


Simon apporta modifiche non autorizzate al codice del software all'interno del dispositivo medico-diagnostico intelligente di Jenny

eseguiti successivamente con il dispositivo non sono precisi. Chi riceve recensioni negative e vede le proprie vendite diminuire? Non l'utente che ha interferito con il dispositivo. Non l'ospedale. È il produttore del dispositivo e/o il fornitore di software che verrà citato per aver venduto software difettoso.

> Il furto di segreti industriali può risultare catastrofico, ma per molti ISV e produttori di dispositivi intelligenti la manomissione del codice può essere altrettanto devastante. Entrambe le minacce possono danneggiare significativamente la quota di mercato e quindi diminuire il potenziale di profitto.

## L'impatto

La soluzione può non essere più adatta per raggiungere gli obiettivi commerciali: in conseguenza della manomissione tramite manipolazione del codice, il software e i dispositivi potrebbero non essere più adatti per raggiungere gli obiettivi commerciali per cui erano stati creati.

Risultati inattesi:la manomissione del software embedded in un dispositivo può modificare il funzionamento del dispositivo stesso e produrre risultati errati.

Perdita di profitti: la manomissione del codice potrebbe potenzialmente consentire agli utenti l'accesso a funzionalità per le quali non hanno pagato.

Danni alla reputazione del marchio: problemi di conformità a normative possono danneggiare irrimediabilmente la reputazione del tuo marchio e dei tuoi prodotti.

## La soluzione: protezione da manomissione

Senza le tecnologie di crittografia adatte e la protezione dall'offuscamento di codice, i rivenditori di dispositivi intelligenti rendono inconsapevolmente il loro codice vulnerabile alla manomissione.

Tramite un controllo efficace del codice sorgente e la prevenzione di manomissione, reverse engineering e furto di proprietà intellettuale, è possibile proteggere i profitti e salvaguardare l'integrità di marchi e prodotti.

> Senza le tecnologie di crittografia adatte e la protezione dall'offuscamento di codice, i rivenditori di dispositivi intelligenti rendono inconsapevolmente il loro codice vulnerabile alla manomissione.

## Caso di best practice: produttore leader nel settore degli imballaggi

Prendiamo l'esempio di un produttore leader del settore che sviluppa macchinari su base software per elaborare il confezionamento end-to-end di prodotti alimentari liquidi come latte e succo di frutta. Il software nel macchinario è programmato per essere conforme a molteplici normative di salute e sicurezza pubblica.

In termini di protezione della proprietà intellettuale, l'azienda vuole controllare l'accesso al software e limitare il rischio di manomissione di parametri chiave che controllano processi come la pastorizzazione. Questo produttore di dispositivi utilizza le soluzioni per la monetizzazione del software Sentinel RMS ed EMS allo scopo di proteggere il suo codice dall'accesso non autorizzato e dalla manomissione, e per controllare chi può modificare i parametri che controllano il macchinario di imballaggio.

## Conclusione

Dalle ricerche emerge che molti produttori di software sono preoccupati per la vulnerabilità della loro proprietà intellettuale.

Se tali aziende temono che le minacce alla proprietà intellettuale possano danneggiare il loro marchio, la loro competitività, l'esperienza dei loro clienti e i loro profitti, perché non fanno di più per proteggerla?

Sospettiamo che non dispongano della capacità necessaria o del supporto dei dirigenti, oppure che non abbiano ancora subito un attacco alla loro proprietà intellettuale. Ci sono diversi livelli di danno. Mentre la pirateria informatica può risultare in perdite di profitti a lungo termine, il reverse engineering e la manomissione possono essere catastrofici e cambiare un'attività da un giorno all'altro. È molto difficile far fronte a simili danni.

Trovare soluzioni per ridurre e prevenire la pirateria informatica, le vendite sul mercato grigio, il reverse engineering e la manomissione della proprietà intellettuale insita nel codice software offre numerosi vantaggi. L'utente finale ha la certezza che i programmi che utilizza sono esattamente come li aveva progettati il produttore e può usufruire di servizi di assistenza grazie alla garanzia. Il settore del software è pagato per creare prodotti di qualità, stimolare un mercato competitivo e continuare a sviluppare prodotti.

Ma lo stop alla pirateria richiede uno sforzo congiunto da parte di consumatori, produttori di software e governi. Sia in America del Nord sia in Europa sono stati lanciati programmi educativi di successo, seguiti a loro volta da un'implementazione efficace.

Ma, oltre a questo, i produttori di software devono adottare misure proattive e positive, sotto forma di strategie per la protezione del software, per difendere la proprietà intellettuale da uso illegale, copia non autorizzata, vendite su mercati grigi, furto e manomissione.

Come illustrato dagli esempi di best practice, una soluzione collaudata per il licensing e la protezione del software è un modo efficace per far fronte alle quattro minacce alla proprietà intellettuale, proteggere i copyright, combattere la pirateria, definire prezzi adeguati per ciascun segmento, sventare lo spionaggio industriale e la manomissione.

È fondamentale capire che l'utilizzo di una tecnologia per la monetizzazione del software può essere anche una strategia di profitto a lungo termine per aumentare le vendite, tagliare i costi, aumentare il vantaggio competitivo ed espandere la propria presenza sul mercato.

## Informazioni sulla monetizzazione del software Gemalto Sentinel

Gemalto è leader di mercato in soluzioni di software licensing e gestione delle autorizzazioni per fornitori di software on-premises, embedded o basato su cloud. Gemalto Sentinel è la marca più stimata nel settore da chi cerca soluzioni sicure, flessibili e scalabili per la monetizzazione del software. Per ulteriori informazioni, visita la seguente pagina web: https://www.gemalto.com/software-monetization/

**Prova le soluzioni Sentinel gratuitamente!**

## Partecipa alla discussione

> 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, Sondaggio Globale sul Software di BSA, Maggio 2016, http://globalstudy.bsa.org/2016/downloads/studies/BSA_GSS_US.pdf

ii The State of Software Monetization, Ricerca di Vanson Bourne su Incarico di 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: Aggiornamento dello Studio sul Mercato Grigio di KPMG LLP, http://www.agmaglobal.org/cms/uploads/whitePapers/7-10-08KPMGWhitePaperGrayMarketStudy.pdf

**Contattaci:** per informazioni e i contatti di tutte le sedi, visita www.gemalto.com/software-monetization

**Seguici:** sentinel.gemalto.com/blog

GEMALTO.COM

gemalto
security to be free