

# Sistema Anticopia Cd Audio

Scritta da Echelon il 30-05-2003

**Eccovi un elenco delle maggiori protezioni anticopia per i cd, in uso dalle case piu` importanti produttrici di giochi e software e musica.**

---

Scritta in origine da Echelon il 30/5/2003

## Sistemi Anticopia Cd Audio

By Echelon

### Part 1.

Tutti i sistemi anticopia si basano sull'introduzione di errori intenzionali nei dati presenti sul CD, che mandano in tilt i lettori di CD-ROM dei personal computer ma non hanno effetto su un normale lettore di CD (quello dell'impianto stereo).

Quando un qualsiasi lettore di CD (di un impianto stereo o di computer) legge un CD musicale, è in grado di correggere piccoli errori di lettura causati ad esempio da sporco, graffi, difetti di tracciamento del drive, difetti di produzione del disco e via dicendo. Se il lettore non riesce a leggere correttamente un tratto breve del CD, esegue un'interpolazione: semplificando, guarda com'era l'audio appena prima, guarda com'è subito dopo, e poi "crea" l'audio del tratto che non riesce a leggere. Grazie anche all'aiuto di codici di correzione registrati sul CD insieme alla musica, il lettore riesce a compensare questi piccoli difetti in modo così efficace che in genere non ce ne accorgiamo neppure (salvo quando il tratto difettoso è esageratamente lungo).

Questo è quello che avviene durante la normale riproduzione di un CD audio da parte di un computer o di un impianto hifi. Quando invece un computer legge un CD per farne una copia (masterizzarlo) o per eseguire il ripping, cioè estrarne le tracce e poi convertirle in formato MP3 o Wav, il lettore usa un procedimento diverso: legge il CD esattamente com'è, senza interpolazioni, come se fosse un CD-ROM contenente dati. Se c'è un punto illeggibile, il lettore non "crea" i dati mancanti: si limita a dare errore, punto e basta.

Eccovi un elenco delle maggiori protezioni anticopia per i cd, in uso dalle case piu` importanti produttrici di giochi e software e musica.

**Disc Guard** - Ha un funzionamento simile alla tecnologia CD-Cops: questa volta durante la

masterizzazione del CD originale viene inserita una «firma», che non può essere riprodotta dai normali lettori CD presenti sul mercato, ne tantomeno copiata dai masterizzatori. Se il programma di verifica si accorgerà che la firma manca, impedirà all'applicazione di funzionare. Riconoscibile per i files IOSLINK.VXD e IOSLINK.SYS.

**Laserlock** - Nel CD sono stati volontariamente inseriti dei «blocchi danneggiati». Durante la copia il masterizzatore interpreta questi blocchi di dati come errori di lettura e si ferma, Per verificare se è presente la protezione Laserlock. controllate a vista se nel CD è presente L'omonima scritta o DADC, o se c'è una cartella Laserlock all'interno del CD stesso.

**Presenza di falsi file (Dummy files)** - All'interno del contenuto del CD-ROM sono presenti file piuttosto grandi (dai 600 ai 700 Mb) con estensione \*.afp nella cartella principale. Sono file che non servono a niente.

**SecuROM** - È il sistema di protezione sviluppato da Sony: i CD nascono con al loro interno un file non copiabile; una volta installato il contenuto del CD nel vostro PC. avrete sempre bisogno del medesimo CD nel lettore per far funzionare il programma. Il software in questione, infatti, ricerca ogni volta il file nel CD: se non lo trova si interrompe e l' applicazione si chiude. Potete identificare. infatti, la protezione SecuROM dalla presenza di uno o più di questi file: cms16.dll cms95.dll, cms\_nt.dll.

**SecuROM new** ? Quando il gioco viene installato vengono creati i files SINTF16.DLL, SINTF32.DLL e SINTFNT.DLL all'interno della cartella Windows\System.

**SafeDisc** - Tecnologia con funzionamento simile a quella SecuROM: i CD sono scritti originariamente con una cifratura che i masterizzatori non riescono a leggere. Si identifica tramite la presenza dei file 00000001.tmp, clcd16.dll, clcd32.dll, clockspl.exe e, nel caso di giochi, con «nomegioco.exe» insieme a «nomegioco.ico». La protezione include anche una tecnologia anti-hacking, che previene attacchi alla sua sicurezza. La tecnologia anti-hacking è realizzata non solo per rilevare copie illegali, ma anche per fermare cracker distruttivi e pirati commerciali. Esistono quattro varianti di questa protezione.

**SafeDisc v2** ? In questa versione di safedisc sono presenti ancora i file che permettono il facile riconoscimento della protezione: 00000001.tmp, 00000002.tmp, e file con estensione .256 o .016.

**Settori difettosi** - Se date un'occhiata alla superficie dati del CD, potrete riscontrare dei settori difettosi, sono di un colore diverso, un po' più chiaro del resto della superficie e più «lisci». Sono naturalmente «errori volontari», che non impediscono il normale funzionamento del CD, ma ne impediscono la copia perché il masterizzatore le interpreta come errori di lettura.

**TOC errata (illegal TOC)** - La sigla TOC indica la «tabella del contenuto». Quando controllate le dimensioni del CD, vi accorgete che il sistema vi indica che il CD in questione contiene una quantità esosa di dati (1 Giga o più), cosa impossibile perché il supporto ottico non può memorizzare così tanti dati.

**Cd-Cops** - Questa protezione legge il CD e misura la velocità di lettura. Questo valore è un numero (il codice) che è la CHIAVE DEL CD (detto anche "CD key"). Se il CD inserito ha una differente velocità di

lettura (confrontata con il numero memorizzato), il CD non funzionerà dato che la chiave è differente.

**ProtectCD-Vob** ? Il CD contenenti questo tipo di protezione non rispettano le norme ISO per il formato dei dati, precisamente il file di sistema, sul CD. Vi sono, per esempio, alternanze di sessioni di tracce dati e audio. Queste ultime possono essere più brevi di quattro secondi.

**Cactus Data Shield 100** ? Questa tecnica di protezione prodotta da Midbar scrive un dato di Lead-Out errato nella TOC e genera il mancato riconoscimento del CD da parte di molte unità. La prima traccia audio è sovradimensionata, solitamente ci sono molte tracce dati dopo le tracce audio. I CD così protetti potevano comunque essere riprodotti nell'unità CD del computer per 28 secondi.

**Cactus Data Shield 200** ? Anche questa protezione presenta la TOC modificata, come Cactus Data Shield 100, ma solo nella prima traccia. Tutte le altre sono tranquillamente leggibili. I lettori dei normali impianti stereo chiaramente restano esclusi da qualsiasi effetto secondario della protezione. La si riconosce poiché all'interno del Cd è contenuto i files YUCCA.CDS e CACTUSPJ.EXE, quest'ultimo è il player con il quale è possibile ascoltare le tracce del CD sul computer. In questo modo i CD possono essere ascoltati anche sui computer.

**Cactus Data Shield 300** ? L'ultima creazione di Midbar dovrebbe fare presto il proprio debutto sul mercato. Oltre a essere basata su cactus Data Shield 200, essa sfrutta la tecnologica DRM (Digital Rights Management), un metodo sviluppato da Microsoft grazie al quale il produttore dovrebbe riuscire a individuare cosa esattamente viene fatto dei dati presenti sul CD, per esempio quali tracce possono essere copiate e con che frequenza.

**Mediacloq** ? Utilizzata per la prima volta nell'aprile 2001 negli USA, la prima variante della protezione di casa Sunncomm, Mediacloq 1.0, si basa sulla manipolazione della TOC e non consente la riproduzione dal PC, a differenza della versione 2.0, che ha superato la fase dei test e dovrebbe a breve essere utilizzata anche dalla casa discografica BMG. Per compromettere la qualità del sonoro di eventuali copie, pare che il segnale audio venga manipolato da un jitter artificiale.

**Musicguard** ? Frutto del lavoro congiunto di Macrovision e TTR Technologies, viene utilizzata negli USA e prevede l'inserimento di informazioni aggiuntive nel flusso dei dati che, senza compromettere la qualità audio nè impedire di ascoltare il CD al PC, impediscono di copiare il CD causando continuamente l'interruzione del processo di scrittura o riducendo notevolmente la qualità del sonoro. Nel frattempo Musicguard è stata soppiantata dal successore Safeaudio.

**Safeaudio** ? Anch'essa creata da Macrovision e TTR Technologies e finora usata solo negli USA, la tecnica funziona con errori nel materiale audio e mescolando dati di correzione degli errori in modo da simulare disturbi non sopprimibili. I CD con questa protezione dovrebbero essere riproducibili sia con l'impianto stereo sia col PC. La protezione interviene solo quando i dati vengono letti per via digitale causando messaggi di errore che rendono impossibile la copia.

Nella prossima guida prenderemo in esame i vari metodi di sistemi per scavalcare le suddette protezioni e come restare nella legalità dopo tale operazione.

**End of Part 1.**

