MINE2 FOR VIDEO INDUSTRY

Cyber Deception for Video DRM, OTT Platforms & Studios

A Mine2 Industry Whitepaper

Mine2 Cyber Deception Platform

Honeytokens	MineField	Cloud Mines	Fortify
Fake Screener Files	Fake Media Servers	Fake S3 Buckets	Misconfiguration Scan
Decoy Master Copies	Decoy CMS Portals	Decoy IAM Users	Credential Audit
Bogus CDN Creds	Fake FTP/S3 Stores	Fake Secrets	CVE Detection
Fake DRM License Keys	Decoy API Endpoints	Access Tracking	Hardening Guide

Key Benefits for Content & Media Companies

- Pre-Exfiltration Detection
- Zero False Positives
- Insider Threat Detection

Pre-Release Protection | OTT Security | Studio Pipeline Defense | Copyright Act 1957 Aligned

www.mine2.io | info@mine2.io

A Rs 22,400 Crore Problem Called Piracy

India's entertainment industry lost Rs 22,400 Crore to piracy in 2023 alone -- Rs 13,700 Crore from theatrical releases and Rs 8,700 Crore from OTT platforms, according to the EY-IAMAI 'Rob Report'. India ranks 2nd globally in online piracy with 1,756 Crore visits to pirated websites in 2024 (MUSO). 51% of Indian media consumers access pirated content. OTT piracy now accounts for 63% of all illegal content access, causing Rs 8,000-11,000 Crore in annual losses for the streaming market.

The Real Incidents That Should Alarm You

Netflix/Iyuno Breach (Aug 2024): A post-production partner's internal CMS was compromised through an insecure API in the registration process. Full episodes of Arcane Season 2, Terminator Zero, Heartstopper S3, Dandadan, Spellbound, and Plankton: The Movie leaked to 4Chan and X. Called one of the worst streaming leaks in history. The vulnerability: any public email could register an account on Iyuno's internal content management system.

Indian Pre-Release Leaks (2024-25): Films including Pushpa 2, Kalki 2898 AD, and multiple Tamil releases leaked within hours or even before theatrical release. Analysts point to insiders at post-production studios, content delivery services, and cinema exhibition companies as likely culprits. Kerala police arrested a key Tamilrockers administrator in July 2024.

HBO House of the Dragon (2024): Season 2 finale leaked via a third-party international distributor. HBO was forced to release early press screeners to counter spoiler damage.

Vimeo/Post-Production Leaks (2024): Pre-release films were found on a post-production studio's Vimeo account -- uploaded months before appearing on pirate sites. The studio had 1,000+ videos exposed, with 'for internal use' watermarks, confirming insider access as the origin.

Rs 22,400 Cr	51%	90M
annual piracy losses in India (EY-IAMAI 2023)	of Indian consumers access pirated content	users accessed pirated video in India in 2024

Where Leaks Actually Originate

Understanding the content pipeline reveals why DRM alone cannot solve this problem. Content passes through dozens of hands before reaching the consumer, and each touchpoint is a potential leak source:

- **Production & Post-Production:** Editors, VFX artists, colorists, sound engineers with access to unencrypted master files
- **Localization Partners:** Dubbing studios, subtitle translators (Iyuno had 1,000+ videos accessible via a single API flaw)
- **Screener Distribution:** Review copies sent to press, awards voters, and partners -- often with only a visible watermark
- **CDN & Delivery Systems:** Content engineers with access to origin servers, encryption keys, and CDN purge controls
- **Exhibition & DTH:** Theater projection systems, DTH signal feeds, cable headends -- each with insider access

The Gap: What DRM and Watermarking Cannot Do

DRM and forensic watermarking are essential technologies. But they solve a different problem than what Mine2 addresses. Understanding this gap is critical:

DRM (Widevine, FairPlay, PlayReady)

Protects content during playback -- encrypts the stream so only authorized devices can decode it. But DRM only works at the consumer endpoint. It does nothing to protect content inside your production pipeline, post-production studio, localization partner, or CDN origin server. The Netflix/Iyuno breach happened entirely upstream of DRM.

Forensic Watermarking

Embeds invisible identifiers to trace a leak back to its source after it appears online. Essential for attribution, but fundamentally reactive -- it tells you WHO leaked after the damage is done. By the time a watermark is detected on a torrent site, millions may have already downloaded the content. For a Rs 100 Crore film, 'after the fact' is too late.

The Missing Layer: Pre-Leak Detection

> *DRM protects the stream. Watermarking traces the leak after it happens. Neither detects the attacker or insider while they are still inside your systems, before they exfiltrate content. Mine2 fills this critical gap -- detecting unauthorized access to content assets in real time, before a single frame reaches a pirate site or Telegram channel.*

How Cyber Deception Protects Content

Mine2 deploys realistic-looking fake content assets throughout your infrastructure. These decoys look indistinguishable from real assets to an attacker or malicious insider, but no legitimate workflow should ever access them. When someone does, it is a confirmed threat.

Honeytokens

Fake content files planted alongside real assets: decoy screener copies (Final_Cut_Screener_v3.mov), fake DRM license server credentials, bogus CDN API keys, decoy master copy directories, fake subtitle/dubbing project files, and dummy AWS/S3 credentials for content storage. Any access triggers immediate high-confidence alerts.

MineField

Transforms systems into decoys by running fake services: fake media asset management portals, decoy FTP/SFTP servers appearing to host content libraries, fake CMS interfaces resembling internal content management systems (like the one Iyuno exposed), and fake API endpoints.

Cloud Mines

Scans your AWS environment, suggests and deploys fake S3 buckets appearing to contain content masters, fake IAM roles with content-admin permissions, and fake Secrets Manager entries with CDN/DRM credentials. Tracks all access with full attribution.

Fortify

Proactive hardening: scans for the exact misconfigurations that enabled the Iyuno breach -- insecure APIs, default credentials, open registration endpoints, unpatched CMS software, and exposed storage services.

Content Pipeline Use Cases

1. Pre-Release Content Vaults

The Risk: Master files, rough cuts, and final exports sit on shared storage (NAS, SAN, S3) accessible to editors, VFX teams, and producers. Anyone with access can copy a pre-release film to a USB drive or personal cloud. This is the #1 source of pre-release leaks.
Mine2 Approach: Honeytoken files planted in content vaults: Final_Master_4K_HDR.mxf, Screener_Awards_2024.mov, Pre_Release_Copy.mp4. Any access outside the legitimate editing workflow triggers immediate alerts with user identity, workstation, and timestamp.

2. Post-Production & Localization Partners

The Risk: The Iyuno breach proved that third-party localization and post-production studios are the weakest link. Their internal systems held content from Netflix, Sony/Crunchyroll, and others -- all accessible through a single insecure API. Indian dubbing studios handling multi-language releases face identical risks.
Mine2 Approach: Mandate Mine2 deployment at partner studios as a contractual security requirement. MineField decoy CMS portals detect unauthorized logins. Honeytoken project files (Hindi_Dub_Final_v2.wav, Tamil_Subtitle_Review.srt) detect insider browsing. Fortify audits partner infrastructure for the exact API exposure that enabled Iyuno.

3. CDN & Streaming Infrastructure

The Risk: Content engineers managing CDN origin servers, DRM license servers, and encoding pipelines have privileged access to unencrypted content. Compromised CDN credentials can expose entire content libraries.
Mine2 Approach: Honeytoken CDN API keys and DRM license server credentials planted in engineering environments. Cloud Mines deploy fake S3 origin buckets. MineField creates decoy DRM key management interfaces. Any interaction = confirmed compromise.

4. Screener & Review Copy Distribution

The Risk: Pre-release screeners sent to press, awards voters, and distribution partners are historically the most common source of high-quality leaks. Visible watermarks can be cropped; forensic watermarks only help after the leak.
Mine2 Approach: Screener distribution portals protected by honeytoken tracking links. Decoy screener files with unique identifiers in the download directory. If a recipient shares access credentials or downloads unauthorized content, alerts fire immediately.

5. Exhibition & DTH Signal Protection

The Risk: Theater projection operators, DTH signal engineers, and cable headend technicians have access to decrypted content feeds. With Rs 22,400 Crore in piracy losses, the MIB has mandated forensic watermarking -- but this only traces after the fact.
Mine2 Approach: Honeytoken content files in projection server directories. MineField decoy services mimicking content delivery APIs at exhibition endpoints. Fortify scanning exhibition and headend systems for unauthorized recording devices or exfiltration tools.

6. Insider Threat Across the Pipeline

The Risk: Analysts point to insiders at post-production studios, delivery services, and exhibition companies as the likely source of pre-release leaks. The motivation ranges from financial gain (piracy networks pay for early copies) to disgruntlement or simple negligence.
Mine2 Approach: Deception works equally well against insiders and external attackers. A malicious insider browsing directories they shouldn't access will inevitably touch a decoy file. Unlike behavioral analytics (which generate false positives), deception produces confirmed evidence of unauthorized access -- usable in HR proceedings and legal action.

Where Mine2 Fits in the Content Security Stack

Mine2 is not a replacement for DRM or watermarking -- it is the missing detection layer that completes the content security stack:

DRM — *Protects consumer playback*
Widevine/FairPlay/PlayReady

Forensic Watermark — *Traces leak source after the fact*
Invisible identifiers

Mine2 Deception — *Detects attacker BEFORE exfiltration*
Honeytokens + MineField

Fortify Hardening — *Prevents initial compromise*
Misconfig scan + CVE audit

Regulatory & Industry Compliance

Copyright Act, 1957 & IT Act, 2000

Copyright infringement carries criminal penalties including imprisonment up to 3 years and fines up to Rs 2 Lakh. The IT Act addresses unauthorized access to computer systems. For studios pursuing legal action against insiders, Mine2's forensic-grade evidence trail -- timestamped alerts with user identity, IP address, file accessed -- strengthens prosecution.

MIB Forensic Watermarking Mandate

The Ministry of Information & Broadcasting established a task force mandating forensic watermarking for broadcast and exhibition. Mine2 complements this by catching unauthorized access to content BEFORE it is watermarked, exported, or distributed -- plugging the gap between content creation and watermark application.

DPDP Act, 2023 (Subscriber Data)

OTT platforms are Data Fiduciaries processing subscriber PII, payment data, and viewing preferences for 547 million+ video streamers in India. Beyond content protection, Mine2 honeytokens also guard subscriber databases against breach.

Studio Security Mandits (TPN/MPAA)

The Trusted Partner Network (TPN) assessment, backed by the MPA (formerly MPAA), requires post-production facilities to demonstrate active security controls protecting content. Mine2 provides demonstrable detection capabilities that satisfy TPN assessment requirements for content security monitoring and insider threat detection.

CERT-In Incident Reporting

The 6-hour CERT-In reporting mandate applies to content platforms handling sensitive data. Mine2's immediate, context-rich alerts enable compliance without lengthy manual investigation.

How Mine2 Would Have Changed the Outcome

Scenario 1: The Iyuno-Style Partner Breach

Without Mine2: Attacker discovers an insecure registration API on a localization partner's content management system. Creates an account with a public email. Gains access to the internal CMS hosting unreleased content from multiple studios. Downloads full seasons and films. Content appears on 4Chan within days. Netflix calls it 'one of the worst streaming leaks in history.'

With Mine2: Same API exploitation. But the CMS also contains Mine2 honeytoken project files -- a decoy Arcane_S2_Final_Mix.mxf and fake subtitle project Hindi_Dub_v3.srt. The attacker downloads these alongside real files. Mine2 alerts fire within seconds with the new account's email, IP, and exact files accessed. Security team locks the account and patches the API. Zero content reaches 4Chan.

Scenario 2: Insider Leak of a Rs 200 Crore Film

Without Mine2: A post-production editor, approached by a piracy syndicate offering Rs 5 Lakh, copies the pre-release master of a major Bollywood film to a personal drive. The film appears on Tamilrockers within hours of theatrical release. Opening weekend collections drop 20-30%. The forensic watermark eventually identifies the editor -- but only after Rs 50 Crore in box office damage.

With Mine2: Same insider temptation. But while browsing the post-production NAS to locate the master file, the editor opens a directory containing Mine2 honeytoken: Master_Final_4K_v7.mxf. Mine2 alerts the security team with user identity, workstation, and timestamp -- three days before release. The editor is confronted with evidence. The film opens as planned.

Scenario 3: OTT Platform Subscriber Data Breach

Without Mine2: An attacker compromises an OTT platform's backend through a vulnerable API. Accesses subscriber database with 10 Crore+ user records including payment details, viewing history, and Aadhaar-linked KYC. Exfiltrates data over weeks. Discovery: 4 months later via CERT-In.

With Mine2: Same API compromise. But during reconnaissance, the attacker queries a MineField fake subscriber database that appears alongside real data stores. Alert fires immediately. Security team isolates the compromised API endpoint. Zero subscriber records exfiltrated.

Getting Started

1. Map Identify content touchpoints: production storage, post-production NAS, partner access, CDN origins, DRM key servers, exhibition endpoints, and cloud infrastructure.

2. Plan Strategic placement of deception assets along the content pipeline -- at every point where unencrypted or pre-DRM content is accessible.

3. Deploy Days, not months. Zero impact on content workflows, encoding pipelines, or playback quality. No agents on editing workstations.

4. Extend Deploy Mine2 at partner studios as a contractual requirement. Integrate alerts with your anti-piracy operations team.

5. Evolve As content pipelines change -- new OTT launches, new partners, cloud migrations -- Mine2 coverage evolves with your workflows.

Business Value for Content Companies

Protect Opening Weekend Revenue

A single pre-release leak can cost a Rs 200 Crore film 20-30% of opening weekend collections. Mine2 detects unauthorized content access during the critical window between post-production and release -- when the content is most valuable and most vulnerable.

Convert Piracy Loss to Revenue

The MPA/IP House report projects that effective anti-piracy measures could migrate 45% of piracy users to legal services by 2029. Detecting and stopping leaks at source is the most effective anti-piracy measure available -- it prevents content from entering the piracy ecosystem at all.

Insider Threat Evidence for Legal Action

Mine2 provides forensic-grade evidence: timestamped alerts with user identity, IP address, file accessed, and method of access. This evidence is admissible and actionable -- for HR proceedings, contract termination with partners, or prosecution under the Copyright Act and IT Act.

Partner Security Verification

After Iyuno, studios need to verify partner security, not just trust it. Deploying Mine2 at partner facilities provides real-time visibility into unauthorized content access across your entire distribution chain -- not just annual security audits.

Subscriber Data Protection

OTT platforms with 547 million+ video streamers hold massive subscriber data. Mine2 protects both content assets AND subscriber databases simultaneously, addressing content piracy and data breach risk with one deployment.

Minimal Workflow Impact

No agents on editing workstations. No encoding pipeline changes. No playback latency. No DRM integration complexity. Mine2 operates alongside your existing content security stack without touching production workflows.

Why Mine2 for Content Protection:

- Catches leakers BEFORE content leaves the building
- Near-zero false positives: every alert is a confirmed threat
- Works equally against external attackers AND malicious insiders
- Complements DRM and watermarking -- fills the detection gap
- Forensic evidence trail for legal action and partner accountability

Conclusion

India's Rs 22,400 Crore piracy crisis will not be solved by DRM and watermarking alone. The Iyuno breach proved that content leaks originate upstream -- from post-production partners, insider threats, and compromised internal systems that DRM never touches.

Every leaked frame is a frame that DRM failed to protect -- because DRM was never designed to protect content inside your pipeline. Mine2 is. Detect the threat before the leak. Protect the content before it reaches a pirate site. Preserve the revenue before opening weekend.

Contact Mine2 Today

www.mine2.io | info@mine2.io