

OTT 은행 보호



서론

비디오 불법 복제는 새로운 문제가 아닙니다. 전문 영화 제작의 초창기부터 '사유 재산의 저작권 침해'를 통해 악용함으로써 빠르게 돈을 벌려는 사람들이 있었습니다. 무성 영화 시대에는 극장에서 무단으로 영화 상영시간을 연장하는 소위 '바이시클링' 행위가 지나치게 만연하여 이렇게 양심 없는 행위를 저지르는 극장 주인을 현장에서 포착하기 위해 할리우드에서 '검사원'을 보내곤 했습니다. 그러나 인터넷을 통한 '공유'를 통해 수백만 명의 시청자에게 수천 개의 불법 복사본을 즉시 배포하는 있는 가장 손쉽고 효과적인 디지털 배포가 이루어지기 시작했습니다.

현재 불법 복제자는 다양한 공격 기법을 사용하여 콘텐츠를 검색하고 배포합니다. 흔한 전술로는 크리덴셜 스테핑(시청자 세부 정보를 캡처하고 합법적인 계정을 하이재킹) 또는 TV와 구분하기 어려운 경험의 리니어 채널을 재스트리밍하는 것 등이 있습니다. 불법 복제 기업은 심지어 고객에게 간편한 UX, 고객 서비스, 다양하고 유연한 비즈니스 모델을 제공합니다.

이러한 배경을 염두에 두고 불법 복제의 도전을 파악하고 전략적인 프레임워크를 통해 이를 반격할 수 있는 방안을 알아봅니다.

EU 국가 전역에서 1,370만 명이 주기적으로 불법 복제 서비스를 이용하는 것으로 추산(EUIPO 2019 기준)되며, 단일 국가로는 영국(240만)과 프랑스(230만)에서 불법 사용 인구가 가장 많습니다. EU에서 불법 복제로 창출된 연 매출은 10억 유로로 추산됩니다(EUIPO 2019). 북미 지역에서는 미국의 1,250만 이상 가구에서 불법 복제 비디오에 접속(Parks Associates 2019)한 것으로 추산되며 아시아 태평양 지역에서 이 문제는 더욱 널리 퍼져 있을 수 있습니다. 예를 들어 2019년 AVA 연구에 따르면 홍콩에서는 24%의 소비자가 불법 복제 채널에 접속하기 위해 인터넷 스트리밍 기기에 접속합니다. 필리핀 소비자는 28%, 대만은 34%, 태국은 45%로 증가했습니다. 업계 전반의 노력에도 불구하고 비디오 불법 복제는 여전히 전 세계적으로 심각한 문제라고 볼 수 있습니다. 이로 인한 영향은 업계 전반에서 확인할 수 있으며 재정적 손실과 실업의 원인이 되고 있습니다. 또한 이 문제가 라이선싱에도 영향을 미치는 징후를 보이기 시작했습니다.

주제의 복잡성때문에 정확한 수치를 설정할 수는 없으나 미국 상공회의소에서 의뢰한 보고서에 따르면 영화 업계의 재정적 손실은 400억 달러에서 971억 달러 사이, 그리고 TV 산업의 경우 393억 달러에서 954억 달러 사이로 추산됩니다(NERA Consulting 2019). 여기에서 정부의 과세로 인한 수입 손실은 제외됩니다.

TV 및 영화 업계는 세트 디자이너, 메이크업 아티스트, 음악가부터 제작자와 감독까지 수백만 개의 일자리를 지원하고 있습니다. 즉, 불법 복제로 인해 이러한 사람들의 일자리까지 위협을 받고 있는 셈입니다. 디지털 불법 복제가 미국 경제에 미치는 영향에 관한 2019년 보고서에서 Blackburn, Eisenach, Harrison은 해당 년도에 불법 복제 활동으로 인해 미국에서 23만에서 56만 개의 일자리가 사라진 것으로 추정했습니다.

OTT 은행 보호

**400억 ~ 971억
달러**

불법 복제 비디오로
인한 영화 업계의 추정
손실

**393억 ~ 954억
달러**

불법 복제 비디오로
인한 TV 업계의 추정
손실

게다가 불법 복제가 라이선스에 영향을 미치고 있다는 징후가 나타나기 시작했습니다. 라이선스는 크리에이티브 업계의 생명선이며 이것은 더욱 위험한 전략적 문제입니다. 간단히 말해, 불법 복제 사이트를 통해 콘텐츠를 무료로 이용할 수 있는 경우 잠재적 배포사에서 판권에 상당한 금액을 지불할 이유가 있을까요? 세계에서 가장 큰 스포츠 저작권 구매자 중 하나인 beIN의 CEO 유서프 알 오베이들리(Yousef Al-Obaidly)는 “전 세계적 불법 복제로 인해 스포츠 저작권 거품이 터질 것이며 비즈니스 모델은 재검토되어야 할 것”이라고 말했습니다. 그는 자신의 기업에 대한 권리의 가치가 독점성의 수준을 기반으로 할 것이라는 뜻을 내비쳤습니다. 오스카상 후보에 올랐으며 에미상을 수상한 제작자 제이슨 블룸(Jason Blum)은 혁신적이고 모험적인 영화를 위한 투자금에 불법 복제가 직접적으로 어떤 영향을 미치고 있는지 설명했습니다. 그는 그리 머지 않은 미래의 언젠가는 그 금액을 유지할 수 없게 될 것이며 스튜디오에서 영화 제작을 줄여야 할 것이라 말했습니다.

불법 복제 업계는 어떻게 작동하나요?

어떤 전투에서나 적을 이해하는 것이 중요합니다. 그래야 적의 동기, 전술, 강점, 약점을 파악할 수 있습니다. 인사이트는 이해하기 어렵지만 우리는 아래에 요약된 것처럼 각각의 동기, 정교함의 수준 등 복잡한 일련의 그룹 및 하위 그룹이 있다는 것을 알고 있습니다.

릴리스 그룹

대기업에 대한 투쟁에서 직원들은 자신을 혁명가로 봅니다. 가치 있고 신뢰할 수 있는 사람만이 업로드 사이트의 직원 자격을 얻게 됩니다. 다양한 그룹 및 개인이 특정 장르를 전문으로 하고 새로운 자료를 수집하기 위해 경쟁하며, 인정을 통해 보상받습니다. FACT는 이 구조를 “복잡하고 정교하며 조직화된 해커 스타일의 그룹으로 다른 형태의 사이버 범죄에도 연루된 것으로 의심된다”고 설명했습니다.

사이트 운영자

이들은 Pirate Bay와 같은 토렌트 사이트와 TeaTV같은 스트리밍 스타일 사이트 등의 불법 복제 비디오 사이트를 관리합니다. 릴리스 그룹 및 사이트 운영자들이 동일한지는 알 수 없지만, 많은 연구에서 두 그룹 간에 상당히 중복되는 요소가 있는 것으로 나타났습니다. 운영자는 이 과정에서 수익을 올리며 종종 여러 개의 ‘미러’ 사이트를 실행하여 당국에 의해 중단되더라도 온라인 상태를 유지하고 수익을 올릴 수 있습니다.

인터넷 스트리밍 디바이스 도매상

특히 Kodi를 활용하는 디바이스의 성장은 기회를 노리고 있는 범죄자들에게 상대적으로 안정적이고 예측 가능한 매출 흐름을 제공합니다. 도매상은 완전히 합법적인 채널 또는 범죄 네트워크를 통해 박스를 수입하고 집에서 불법 소프트웨어를 통해 개조하여 온라인으로 판매합니다.



소셜 불법 복제

종종 소셜 미디어를 통하여 콘텐츠를 배포하는 경우로 이 그룹의 사람들은 불법 복제가 불법이라는 사실을 잘 모르거나 양면적인 태도를 보이며 특정 콘텐츠 장르의 비용 또는 구독 피로감에 대응합니다.

불법 복제자가 콘텐츠를 수집하는 방법

불법 복제자가 콘텐츠를 복제하는 방법으로는 여러 가지가 있으며 이는 가치 사슬 전반에서 악용될 수 있는 약점 때문입니다. 사용 사례에 따라 가장 보편적인 기법을 그룹화할 수 있습니다.



TV 채널과 라이브 이벤트의 동시 방송

가장 빠르게 성장하고 있는 불법 복제 행위 중 하나는 TV 채널이나 라이브 이벤트를 캡처하고 재배포하는 것입니다. 이는 다음을 통해 얻을 수 있습니다.

- 비디오 재생 소프트웨어 또는 Android OS 조작
- 모바일 디바이스를 사용해 재생 중에 화면 녹화
- 셋톱 박스에 연결된 HDCP 스트리퍼를 사용하여 암호화 해제된 비디오 가로채기
- 크리덴셜 스테핑 공격을 통해 정상적 시청자 정보에 접속 및 사용
- VPN을 사용하여 시장에서 비디오 전송



온디맨드 콘텐츠

릴리스 그룹은 발매 전 TV 프로그램 및 영화를 시상합니다. 미디어 업계의 구조는 제작 과정에 참여하는 많은 조직과 개인에게 다양한 기회를 제공합니다. 비디오를 수집하기 위해 사용하는 일반적인 방법은 다음과 같습니다.

- 데이터 센터 침해를 통한 사용자 인증정보 또는 비디오 콘텐츠 도난
- 여러 제작 시스템을 통한 비디오 콘텐츠에 대한 접속을 제공하는 사용자 ID 도난
- 물리적 자산을 녹화(현재는 감소함)하여 공유 및 배포
- 다양한 제작 시스템에 대한 시스템 해킹을 통해 비디오 자산에 직접 접속
- iTunes와 같은 정상적인 출처에서 콘텐츠 리핑
- 영화 촬영 시스템
- 중간자 공격을 통한 직접 도난

OTT 은행 보호

불법 복제자가 콘텐츠를 배포하는 방법

불법 복제자는 콘텐츠를 배포하기 위해 다음과 같이 가능한 모든 채널과 사용할 수 있는 기술적 혁신을 사용합니다.

- 사전 녹화된 TV 스트림에 접속하는 직접 제작된 IP 셋톱 박스
- 스트리밍 장치에서 실행되는 소프트웨어 및 불법 복제 배포를 가능하게 하는 PC(예: Kodi)
- 인기 있는 리테일 스트리밍 디바이스에 사이드로딩된 앱
- YouTube와 같이 사용자가 만든 콘텐츠를 호스팅하는 웹사이트 및 소셜 미디어 서비스
- 검색 또는 소셜 미디어에서 찾을 수 있는 링크를 통해 불법 복제 콘텐츠를 스트리밍하는 웹사이트
- 항상 존재하는 다운로드, 파일 호스팅, 사이버랙커, 토렌트 사이트

다양한 불법 복제 페르소나의 배포 전략은 잘 이해되지 않지만, 릴리스 그룹은 보편화와 이타주의를 기본적으로 지원하기 때문에 사이버랙커와 토렌트 사이트 같은 자산 할당 모델을 선호할 가능성이 있다는 것을 알 수 있습니다. 반대로, 금전적 이득을 노리는 사이트 운영자는 정상적인 서비스를 모방하기 위한 ISD/스트리밍 전략과 여러 매출 모델을 장려하는 능력을 선호할 것입니다.

summary

사람들이 불법 복제 사이트를 찾는 데에는 많은 이유가 있습니다. 여기에는 금전적인 이유, 광범위한 영향에 대한 무지, 독점 제한 없이 콘텐츠에 접속할 수 있는 기본적인 능력이 포함됩니다. 불법 복제 시청자에 대해 VFT Solutions, Inc.에서 작성한 2019년 보고서에는 다양한 정체성이 간략하게 설명되어 있으며 그 내용이 여기에 요약되어 있습니다.

- **‘콘텐츠 무정부주의자’**는 온라인 콘텐츠에 대한 공동의 제한 없는 접속을 주장합니다. 이들은 콘텐츠에 대한 모든 비용이 과하다고 보고 있으며 불법 복제가 비도덕적이거나 불법이라고 생각하지 않습니다.
- **‘콘텐츠 로빈 후드’**는 덜 극단적인 관점에서 생각하며 대체 가능한 제안에 대해 열려있습니다. 페르소나는 라이브 스트리밍의 사용자가 아닌 공유된 토렌트 파일을 배포하는 이들입니다.
- **‘실용주의자’**는 대부분 콘텐츠의 가치는 잠깐 동안만 유지되기 때문에 광범위한 콘텐츠 소비가 권리 소유자의 손해 또는 피해를 능가한다고 주장하며 그들의 행동을 정당화합니다.
- **‘게으른 불법 복제자’**는 불법 복제가 불법이라는 사실을 모르거나 모른다고 주장하는 경우가 많습니다. 이들은 비용 절감, 광범위한 가용성, 그리고 접근 용이성의 영향을 받습니다.

VFT는 게으른 불법 복제자와 실용주의자의 정체성이 전체 커뮤니티의 70%를 차지한다고 추산하며, 이러한 그룹을 교육, 전환, 처벌하는 노력이 불법 복제에 가장 큰 영향을 미칠 것이라고 말합니다.

차단할 수 있는가?

답하자면 완전한 차단은 불가능합니다. 역사는 콘텐츠를 악용하려는 불법 복제자가 이타주의적 또는 상업적 이유로 항상 존재한다는 것을 보여줍니다. 그러나 아직 희망은 있습니다. 문제가 가치 사슬 전반에서 전략적으로 해결된다면 이를 최소화할 수 있습니다. 실천의 측면에서는 아래에 명시된 전략적 분야에서 업계 전반에 걸친 협력 강화가 지속적인 영향을 미칠 것입니다.

데이터

명백하게 필요한 한 가지는 전 세계에서 불법 복제의 규모와 영향을 측정하기 위한 표준 방법입니다. 서로 다른 방법과 기술로는 지속적이고 맥락에 기반한 분석을 할 수 없으며 활동 우선순위를 정하거나 반 불법 복제 시책의 반환을 이해하는 데 혼란을 줄 수 있습니다. 이는 ACE(Alliance for Creativity and Entertainment)와 같은 곳이 데이터 수집에서 주도적인 역할을 맡는 등 업계의 단체를 통해 해결할 수 있습니다.

교육

수많은 사람에게 불법 복제란 '누구나' 하는 행위이기 때문에 정상적인 행동으로 보이므로 불법이라고 인식하지 않습니다. 불법 복제는 범죄이며 생계에도 실질적인 영향을 미친다는 사실을 사람들에게 교육하는 노력을 계속해야 합니다.

법률 및 규제

이탈리아의 FAPAV와 같은 업계 단체 또는 정부 이니셔티브를 통해 비디오 불법 복제자를 기소하고 전 세계의 법적 허점을 없애는 몇 가지 훌륭한 계획이 있습니다. 이러한 노력을 위해 협조하고 관련 데이터에 대한 접근이 필요합니다.

기술 및 운영

콘텐츠가 보호받지 못하게 하는 시대는 지났습니다. 그러나 이것이 실제로 의미하는 것은 운영을 전략적으로 검토하고 제작부터 배포에 이르는 워크플로의 취약한 영역을 식별하며 적절한 조치를 적용하는 것입니다. 우리는 이를 360° 체계로 설명합니다.



문제가 가치 사슬 전반에서 전략적으로 해결된다면 이를 최소화할 수 있습니다.

360° 체계

Akamai는 지금까지 불법 복제 그룹이 비디오를 수집 및 배포하는 방법을 검토한 후 세 가지 핵심 원칙에 기반한 프레임워크를 구축하였습니다. 바로 보호, 탐지, 단속입니다. 이 프레임워크를 사용해 조직은 업계에서의 역할을 기반으로 위협 양상을 전략적으로 검토하고 적절한 운영 및 기술적 계획을 실행해 영향을 최소화할 수 있습니다.

보호



크리덴셜 스테핑 차단

앞에서 설명한 것처럼 크리덴셜 스테핑은 불법 복제자가 시청자의 세부 정보를 수집하기 위해 주로 자동화된 봇을 통해 자주 사용하는 공격 기법입니다. 주요 권장 사항은 다음과 같습니다.

- OWASP로 로그인 페이지/API를 코딩합니다. OWASP 모범 사례에 따라 보안 코드를 작성하고 로그인 엔드포인트에 정기적인 해킹 테스트를 수행합니다.
- DDoS 방어 솔루션을 구축합니다. 증폭 봇넷이 인프라에 도달하여 자산을 손상시키는 것을 방지할 수 있습니다.
- Akamai의 Bot Manager Premier와 같은 봇 관리 솔루션을 사용해 사용자 행동과 디바이스 텔레메트리를 확인하여 정교한 인증정보 도용 공격을 방지할 수 있습니다.



시스템 도난 방지

내부 프로덕션 시스템, 디지털 스토리지 또는 퍼블릭 클라우드로부터의 도난은 불법 복제물의 중요한 소스입니다. 광범위하게 말하면 비디오 자산 도난의 몇 가지 형태를 볼 수 있습니다.

- 불법 복제자의 직접 해킹 또는 중간자 공격
- 암호와 같은 고유한 시스템 ID 캡처
- 직원 또는 프리랜서의 도난 행위

위기를 최소화하기 위해 기업에서 활용할 수 있는 여러 기술이 있습니다. 이들은 근본적으로 기업이 기술에 대한 접근을 변화시키기 위해 사용하는 프레임워크인 제로 트러스트 개념을 중심으로 합니다. 프레임워크의 핵심 구성 요소는 위치 또는 호스팅 모델과 관계없이 리소스에 대한 접속을 보호하고, 최소 권한을 기반으로 접속 제어 전략을 적용하고, 모든 트래픽에 의심스러운 활동이 있는지 검사하고 로깅하는 것입니다. 이 프레임워크는 인증된 사용자와 디바이스만 애플리케이션 및 데이터에 접속하도록 허용합니다. 또한, 인터넷의 최신 위협으로부터 애플리케이션과 사용자를 보호합니다.

OTT 은행 보호

제로 트러스트 프레임워크를 구현하는 데 기업이 사용할 수 있는 몇 가지 구성 요소가 있지만, 핵심 프로덕션 및 스토리지 시스템에 대한 직원/프리랜서 접속을 보호하는 것이 핵심 측면입니다. 미디어 기업은 일시적인 인력을 활용하는 업계 특성으로 인해, 때로는 매일 발생하기도 하는 시스템 접속을 구현하고 취소하는 문제에 직면합니다. Akamai의 Enterprise Application Access와 같은 서비스를 사용하면 비디오 유출이 일어날 수 있는 곳에서 사용자에게 기업 네트워크 접속을 허용하지 않고도 특정 애플리케이션에 대한 허용이 사용자와 디바이스의 ID 및 보안 컨텍스트를 기반으로 신속하게 주어집니다.

제로 트러스트의 또 다른 핵심 측면은 불법 복제자가 중간자 공격에 사용하는 톨인 멀웨어, 랜섬웨어, 피싱과 같은 표적 위협을 선제적으로 식별하고 차단하는 시스템을 구현하는 것입니다. 예를 들어 Akamai의 Enterprise Threat Protector는 실시간 보안 인텔리전스를 사용하여 멀웨어, 랜섬웨어, 피싱, DNS 기반 데이터 유출과 같은 표적 위협을 선제적으로 식별하고 차단하는 보안 웹 게이트웨이입니다.

지역 및 IP 권리 침해 방지: 불법 복제자는 콘텐츠를 재스트리밍하기 위해 합법적인 구독자의 세부정보를 성공적으로 획득한 후 그들의 발원 국가와 IP 주소를 가리기 위해 종종 VPN 기술을 사용합니다. Akamai의 강화된 프록시 탐지와 같은 프록시 감지 기술은 익명 프록시 또는 VPN 서비스와 관련된 요청을 엿지에서 지능적으로 차단하여 이러한 사용 사례를 방지합니다.

재생 위반 차단: 불법 복제 방지에서 가장 인기 있는 전술이며, 다양한 방법으로 구현할 수 있습니다. 가장 널리 사용되는 방법은 DRM(디지털 권한 관리)입니다. DRM은 저작권 보호를 받는 자료를 제한하고 무단 배포를 방지하는 톨, 표준 및 시스템을 의미합니다. 그 자체가 하나의 기술은 아닙니다.

보호하려는 자산의 중요도에 따라 일부 배포사는 간단한 암호화(즉, 코드를 잠금 해제하는 키를 가진 디바이스 또는 소프트웨어에서만 읽을 수 있는 코드로 콘텐츠를 작성하는 것)에 만족합니다. 형식적인 보호 기능이 "키"를 통해 제공되며 이는 일반적인 불법 복제에는 불리한 것입니다. 그러나 키는 일반적으로 HTTP 서버에 의해 전달되며 복사 및 공유할 수 있으므로, 때때로 가치가 높은 콘텐츠를 보호하기에 충분하지 않을 수 있습니다.

암호화를 강화하기 위해 고급 DRM 기술은 챌린지/응답 시스템을 사용하여 콘텐츠 암호화 해제 모듈을 통해 키 통신을 처리합니다. 이러한 통신은 암호화되므로 암호화 해제 키가 해킹될 수 있는 위치에 있지 않습니다. 최신 DRM 기술은 또한 위치 또는 시간 기반 규칙과 같은 다양한 디바이스에서 키를 사용할 수 있는 시기와 방법을 정의하는 비즈니스 규칙을 사용합니다.

패키징 과정에서 DRM을 구현하려는 배포사의 경우 복잡성을 관리할 수 있는 클라우드 사업자와 교류하는 것이 유용한 경우가 많습니다. 일례로 Akamai는 온디맨드 콘텐츠를 위한 오리진 스토리지를 Bitmovin, Encoding.com과 같은 여러 공급업체의 처리 기능과 통합하여 암호화를 거의 실시간으로 구현할 수 있도록 했습니다.

탐지

모든 형태의 도난과 마찬가지로, 보호 기능이 항상 성공적인 것은 아니며, 따라서 모든 침해 행위 탐지가 필수적입니다. 거의 실시간으로 불법 복제 활동을 탐지하는 몇 가지 방법이 있습니다.

핑거프린팅

이 방법은 원본 미디어를 수정하지 않고 비디오 콘텐츠를 식별하는 기능을 제공합니다. 틀은 비디오 파일의 속성을 식별, 추출, 나타내는 데 사용되므로 파일 공유 네트워크와 같은 고유한 "핑거프린트"로 모든 비디오를 식별할 수 있습니다. 원본 미디어는 어떤 방법으로는 수정할 필요가 없는 것이 장점입니다. 그러나 핑거프린트는 동일한 제목의 다른 복사본, 즉 첫 번째 인스턴스에서 추출된 복사본을 구분할 수 없습니다.

워터마크

워터마크가 불법 복제를 막을 수는 없지만 서비스 제공업체는 이를 통해 불법 복제를 탐지하고 불법 행위를 하는 사람들을 식별하며, 이에 대해 조치할 수 있습니다. 비디오 워터마킹은 눈에 잘 띄지 않고 제거할 수 없는 "비트" 패턴을 비디오 파일에 추가하는 것으로 구성됩니다. 이 데이터를 시청자 ID에 연결하면 콘텐츠를 암호화 해제하고 복사해 불법 배포한 불법 복제자를 추적할 수 있습니다. 현재 사용되는 비디오 워터마킹에는 세 가지 방법이 있습니다.

- **비트스트림 수정:** 비디오 품질을 유지하는 방식으로 사진이 선택된 영역을 수정하는 것이며 이를 통해 시청자와 세션을 식별할 수 있습니다. 강력한 방법이지만, 상당한 컴퓨팅 오버헤드가 필요하고 시스템에 지연 시간이 더해져 라이브 콘텐츠에 적합하지 않습니다.
- **클라이언트 측 워터마킹:** 신속한 워터마크 추출에 잘 작동하며 셋톱 박스와 같은 기존 플랫폼에 배포할 수 있는 능력이 있습니다. 그래픽 오버레이가 클라이언트 디바이스의 비디오 스트림에 합성되어 보이거나 보이지 않게 할 수 있습니다. 워터마크는 클라이언트 디바이스에 도달할 때까지 적용되지 않으므로 비디오 스트림에 추가 보호가 필요합니다. 사용자 측 기술 또한 OTT 환경에서는 복잡할 수 있는 SDK 배포가 필요합니다.
- **A/B 변형 워터마킹:** OTT 분야를 목표로 두 개의 동일한 비디오 스트림이 생성되고 워터마크가 적용된 후 클라이언트 측 또는 CDN 엣지 처리를 통해 서로 이어지거나 인터레이싱되어 고유 식별자를 제공합니다. 강력하고 비용 효율적인 방법이지만 식별 시퀀스가 길 수 있으므로 빠른 워터마크 추출이 필요한 상황에서는 적합하지 않습니다.

OTT 은행 보호

모든 워터마킹 전략의 핵심 구성요소는 기술로 불법 복제자를 단속하도록 적절한 모니터링을 실시하는 것입니다. 관리형 모니터링 서비스를 사용하거나 사내 역량을 개발하기 위한 조언을 구할 수 있습니다. Akamai는 모든 주요 워터마킹 제공업체와 협력하여 실행 가능한 솔루션을 전반적인 비디오 불법 복제 전략에 통합하고 활용할 수 있도록 보장합니다.

스트림 로그 식별

다른 탐지 형태로는 전송 로그 실시간 조사를 통하는 것입니다. 이 경우, 철저한 로그 검사는 승인된 IP 주소와 무단 IP 주소를 기반으로 하는 침해 행위의 실시간 상황을 제공합니다. Akamai의 Stream Protector와 같은 이러한 솔루션의 장점은 상황에 따라 기능을 설정 또는 설정 해제하는 것으로 이는 스포츠와 같이 시간 제한적인 권리를 보호하는 데 이상적입니다.

단속

불법 복제 활동이 탐지되면 적절한 방식으로 조치를 취해야 합니다. 전략에 따라 방향을 정하면 됩니다.

- **접속 취소:** 스포츠 이벤트와 같이 비디오 자산이 시간에 민감한 경우 불법 스트림의 발신자에 대한 접속을 즉시 취소해야 합니다. 이러한 방법에는 여러 가지가 있습니다. 일반적인 방법은 배포 서비스 공급업체와 함께 협력하여 관련 세부 정보를 교환하고, 문제를 일으키는 IP 주소에서 스트리밍 활동을 중지하는 것입니다. 이는 시간이 소요될 수 있습니다. Akamai는 불필요한 개입 없이 실시간으로 스트림을 취소하는 서비스를 제공합니다. 이는 워터마킹 또는 스트림 로그 식별을 통해 불법 복제 모니터링이 진행되는 경우 뛰어난 효과를 보여주었습니다.
- **스트림 수정:** 시간이 덜 민감한 상황에서 배포사는 이를 대체 콘텐츠(Big Buck Bunny가 인기 있음)로 바꾸거나 스트림 품질을 저하하여 불법 복제 스트림을 수정할 수 있습니다. 이 접근법은 불법 복제자로부터 탐지 사실을 숨기고 다른 스트림 소스로 옮기는 것을 방지합니다.
- **실시간 메시징:** 불법 복제 주체 섹션에서 설명한 것처럼, 게으른 불법 복제자는 인터넷의 익명성 뒤에 숨어 있습니다. VFT와 같은 조직은 소셜 미디어 플랫폼에서 불법 스트리밍 시청자를 식별하고 위반자에게 직접 메시지를 보낼 수 있습니다. 배포사는 이러한 형태의 단속으로 처음에 정상적인 스트림 접속 권한을 제공하는 등의 다른 단속 방식을 취합니다. 만약 침해가 계속된다면 법적 고지를 보냅니다.

결론

지적 재산을 둘러싼 비디오 불법 복제는 복잡하고 미묘한 주제이지만, 미디어 업계 전체의 장기적인 생존 가능성을 위협할 잠재력이 있습니다. 상당한 재정적 손실을 지적하는 확실한 증거가 있지만, 무엇보다도 불법 복제가 글로벌 라이선스 모델을 근본적으로 훼손하거나 영향을 끼칠 가능성이 있다는 점이 중요합니다.

현재까지 업계의 대응은 비교적 잠잠했습니다. 한 분석가는 "지금만 초기 단계이며 앞으로 해야 할 일이 많다"고 설명했습니다. 위협을 인식하기 시작한 배포사가 점차 증가하고 있으며, 대부분의 "티어1" 비디오 제작자와 운영자들은 이제 전담팀을 구성하여 불법 복제를 보다 잘 이해하고, 상황을 평가하고, 관련 불법 복제 방지 전략을 구현합니다.

이 문서에서는 업계에서 대응하는 데 도움이 되는 몇 가지 시급한 요구사항을 설명합니다. 여기에는 불법 복제 데이터 포인트, 일반 대중에 대한 개선되고 지속적인 교육, 업계 전반의 더 나은 협력, 마지막으로 모든 장르의 저작권자로부터 리더십을 통해 저작권 취급 및 배포 시 업계 전반에 걸친 보편성 구축이 포함됩니다.

다행히도 대부분의 사항이 동원되고 있습니다. 이 주제에 대한 연구가 점점 더 고려되고 있으며 더욱 엄격한 법률이 등장하기 시작했습니다. 또한, 벤더사는 잠재력을 극대화하기 위해 능력을 결합하고 있습니다. 일례로 Akamai는 사이버 보안 전문 지식을 갖추고 있을 뿐만 아니라 불법 복제자가 탐지되면 이들의 활동을 즉시 중단시키기 위해 모든 주요 워터마킹 기업과 협력하고 있습니다. 마지막으로, 저작권자들이 기술 워크플로우 전반에 걸쳐 최소한의 콘텐츠 보호 표준을 강력하게 요구한다는 징후가 나타나고 있습니다. 현재 이들은 고립된 인스턴스 또는 MPAA의 경우 "제안"이지만, 앞으로 이러한 사례가 비즈니스를 수행하는 데 필수적인 기능이 될 것으로 보입니다.

이러한 이니셔티브를 통해 문제를 최소화함으로써 재정적 손실을 줄이고, 고용 기회를 보호하고, 글로벌 시장에서 라이선싱이 계속해서 성장할 수 있습니다.

참조

Asia Video Industry Association. 아시아 비디오 업계 보고서. 2019년.

Bevir. 520억 달러에 달하는 온라인 불법 복제 비용. 2017년. 출처 <https://www.ibt.org/publish/cost-of-online-piracy-to-hit52bn/2509.article>

Blackburn 외. 디지털 비디오 불법 복제가 미국 경제에 미치는 영향. 2019년.

Coberly. 불법 복제를 '죽이는' 스트리밍 서비스. 출처 <https://www.techspot.com/news/78977-streaming-services-killing-piracy-new-zealand-study-claims.html>

CustosTech. 디지털 불법 복제의 경제. 2014년.

Daly. 멀티플렉스의 불법 복제. 출처 <https://www.vanityfair.com/news/2007/03/piratebay200703>

Decary, Morselli, Langlois. 와레즈 해커 간의 사회 조직 및 인식에 관한 연구 2012년.

Digital Citizens Alliance. 불법 복제 스트리밍의 위험성. 출처 https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/DCA_Fishing_in_the_Piracy_Stream_v6.pdf

EnigmaX. 와레즈 씬 릴리스 그룹 조직원과의 인터뷰. 2007년. 출처 <https://torrentfreak.com/interview-with-a-warez-scene-releaser/>

European Commission. EU 내 저작권 보호 콘텐츠의 변위율 추정. 2015년 5월.

European Union Intellectual Property Office. 유럽 연합 내 디지털 저작권 침해의 추세. 2018년.

European Union Intellectual Property Office. 유럽 연합 내 불법 IPTV. 2019년.

FACT. 디지털 불법 복제에 관한 보고서. 2017년.

Feldman. 약 5백만 명의 영국인이 불법 TV 스트리밍 서비스 이용 2017년. 출처 <https://yougov.co.uk/topics/politics/articles-reports/2017/04/20/almost-five-million-britons-use-illegal-tv-streami>

FriendsMTS. 프리미엄 유료 TV 콘텐츠에 대한 가입자 워터마크 기술 비교. 2019년.

Frontier Economics. 위조 및 불법 복제의 경제적 영향. BASCAP 및 INTA에서 의뢰. 2017년.

Granados. 보고서: 수백만 명이 불법 라이브 스트리밍한 엘 클라시코. 2015년. 출처 <https://www.forbes.com/sites/nelsongranados/2016/12/05/sports-industry-alert-millions-illegally-live-streamed-biggest-spanish-soccer-rivalry/#3544c3f37147>

Greenburg. 비디오 불법 복제의 경제. 2015년. <https://pitjournal.unc.edu/article/economics-video-piracy>

Ibosiola D., Steery B., Garcia-Recueroy A., Stringhiniz G., Uhligy S., and Tysony G. 영화 캐리비안의 해적: 불법 스트리밍 사이버락커 탐구. 2018년.

Intellectual Property Office. 온라인 저작권 침해 추적기. 2018년.

Jarnikov 외. 적응형 스트리밍을 위한 워터마킹 시스템 2014년.

Jones, Foo. 최신 OTT 불법 복제 비디오 생태계 분석. SCTE•ISBE. 2018년

Joost Poort 외. 글로벌 온라인 불법 복제 연구, 암스테르담 대학교 정보법 연구소. 2018년 7월.

Kan. '왕좌의 게임'을 불법 다운로드하세요? 그 파일은 아마도 멀웨어일 수 있습니다. 2019년. 출처 <https://mashable.com/article/pirating-game-of-thrones-malware?euore>

Lee, T. 텍사스 규모의 궤변. 2006년. 출처 <http://techliberation.com/2006/10/01/texas-size-sophistry/>

리보위츠 S. "인터넷 불법 복제가 저작권자의 판매와 매출에 미치는 영향", Ruth Towse, Christian Handke, Edward Elgar가 편집한 Handbook on the Digital Creative Economy의 "인터넷 불법 복제: 판매에 미치는 예상 영향"이 요약본. 2013년.

Mick, J. 미국 인구의 거의 절반이 불법 복제 행위를 저지르지만, 불법 복제자가 더 많은 합법적 콘텐츠 구매. 2013년 1월 21일. 출처 <http://www.dailytech.com/Nearly+Half+of+Americans+Pirate+Casually+But+Pirates+Purchase+More+Legal+Content/article29702.htm>

Motion Picture Association of America. 미국 영화 및 방송 업계의 경제적 기여. 2018년 11월.

MPA Content Security Program. 콘텐츠 보안 모범 사례 공통 지침. Motion Picture Association. 2019년.

MUSO. 콘텐츠 보호의 ROI 측정. 2020년.

Nordic Content Protection Group. 연간 보고서, 2020년.

Parks Associates. 비디오 불법 복제: 생태계, 위험성 및 영향. 2019년.

Tassi, P. 2014년 4월 15일. "왕좌의 게임" 불법 복제 건수가 세계 기록을 세웠지만, HBO는 관심이 있는가? 출처 <http://www.forbes.com/sites/insertcoin/2014/04/15/game-of-thrones-sets-piracy-world-record-but-does-hbo-care>

Sanchez, J. 2012년 1월 3일 저작권 업계에서 의회를 기만하는 방법. 출처 <http://www.cato.org/blog/how-copyright-industries-congress>

Sandvine. 비디오 및 방송 불법 복제. 2019년.

Schonfeld. 4백만 달러의 연간 매출을 올리는 Pirate Bay. 2008년. 출처 <https://techcrunch.com/2008/01/31/the-pirate-bay-makes-4-million-a-year-on-illegal-p2p-file-sharing-says-prosecutor/>

Sulleyman. 보물 같은 불법 복제: 범죄자들이 불법 스트리밍으로 수백만 달러를 버는 방법. 2017년. 출처 <https://www.independent.co.uk/life-style/gadgets-and-tech/news/piracy-streaming-illegal-feeds-how-criminals-make-money-a7954026.html>



Akamai는 전 세계 주요 기업들에게 안전하고 쾌적한 디지털 경험을 제공합니다. Akamai의 Intelligent Edge Platform은 기업과 클라우드 등 모든 곳으로 확장하고 있고 고객의 비즈니스가 빠르고, 스마트하며, 안전하게 운영될 수 있도록 지원합니다. 대표적인 글로벌 기업들은 Akamai 솔루션을 통해 멀티 클라우드 아키텍처를 강화하고 경쟁 우위를 확보하고 있습니다. Akamai는 가장 가까운 곳에서 사용자에게 의사 결정, 앱, 경험을 제공하고 공격과 위협을 먼 곳에서 차단합니다. Akamai 포트폴리오는 엣지 보안, 웹·모바일 성능, 엔터프라이즈 접속, 비디오 전송 솔루션으로 구성되어 있고 우수한 고객 서비스, 애널리틱스, 24시간 연중무휴 모니터링 서비스를 제공합니다. 대표적인 기업과 기관에서 Akamai를 신뢰하는 이유를 알아보려면 Akamai 홈페이지(www.akamai.com) 또는 블로그(blogs.akamai.com)를 방문하거나 Twitter에서 @Akamai를 팔로우하시기 바랍니다. 전 세계 Akamai 연락처 정보는 www.akamai.com/locations에서 확인할 수 있습니다. Akamai 코리아는 서울시 강남구 강남대로 382 메리츠타워 21층에 위치해 있으며 대표전화는 02-2193-7200입니다. 2020년 07월 발행.