입문서

비디오 사업자, 콘텐츠, 시청자를 안전하게 보호하는 방법

발단: 기업에 대한 공격

비디오 제작은 본질적으로 협업입니다. 그런데 비디오 제작 산업이 파일 기반의 워크플로우로 이전함에 따라 자산에 접속 또는 터치할 수 있는 '엔드포인트'의 수가 증가했습니다. 이는 보안 방어 체계의 잠재적인 허점 역시 증가했다는 것을 의미합니다.

프리랜서와 포스트 프로덕션 기업을 예로 들겠습니다. 이들은 자신이 공격의 표적이 될 거라고 생각하지 않습니다. 만약 표적이 된다 하더라도 적절한 보안 체계를 확립하는데 필요한 리소스와 전문성을 갖고 있지 않습니다. 바로 이런 점 때문에 이들은 이상적인 표적이 됩니다.

예를 들어 2018년 발생한 '오렌지 이즈 더 뉴 블랙(Orange Is the New Black)' 해킹 사건은 유명 넷플릭스 드라마의 새 시즌을 제작하던 포스트 프로덕션 기업을 감염시켜 금전적인 이득을 취하려던 공격자들의 소행이었습니다. 공격자는 메자닌 품질의 파일을 훔친 뒤 돈을 요구했습니다.[1]

최근 미국에서 20여개의 기업이 참여해 비공개로 진행된 방송사를 위한 사이버보안(Cybersecurity for Broadcasters) 모임에서도 원격 접속 및 벤더 보안에 대한 요청이 가장 많았습니다.

다음과 같은 방법이 도움이 될 수 있습니다.

1. 제로 트러스트 네트워크 접속 툴을 이용하여 핵심 리소스에 접속하는 직원 및 협력업체 직원에게 최소 권한을 부여하는 전략 실행
2. 보안 웹 게이트웨이(SWG)를 사용하여 네트워크 내부에서 발생하는 악성 트래픽 탐지 및 차단

이러한 제로 트러스트 접근 방식을 통해 공격자가 내부로 침입할 가능성을 낮추고 침입하더라도 도주하지 못하도록 제한할 수 있습니다.

전개: 비디오에 대한 공격

2013년 심리 공포 스릴러 TV 드라마인 '한니발(Hannibal)'이 '저조한 시청률' 때문에 종영되었습니다. 하지만 이 드라마는 그해 가장 많이 불법 다운로드된 TV 시리즈 5위에 올랐습니다. 프로듀서인 마사 드 로렌티스(Martha De Laurentiis)는 불법 복제가 '한니발'의 종영에 큰 영향을 끼쳤다고 밝혔습니다.[2]

2019년 6월 카타르 방송사인 BeIN Media Group은 매출 감소로 인해 300명의 인원을 감축한다고 밝혔습니다. 이유는 무엇이었을까요? BeIN은 경쟁사인 beoutQ가 자사 울트라 프리미엄 스포츠 콘텐츠를 불법으로 복제한다고 주장합니다.[3]

미디어 불법 복제는 무성영화를 제작하던 시대부터 존재해 왔습니다. 미디어 배포 방식이 스트리밍 방식으로 전환되고 세계화됨에 따라 공격자는 더 간편한 방법으로 높은 범죄 수익을 올릴 수 있게 되었습니다. 불법 복제의 영향에 대한 연구는 매우 다양합니다. 하지만 분석가들은 비디오 불법 복제 시장 규모가 미국의 경우 연간 최소 10억 달러[4], 유럽은 연간 10억 유로[5]가 넘는 것으로 파악하고 있습니다.

또한 불법 복제 생태계는 다양합니다. 아마추어들은 소셜 미디어를 통해 친구들에게 라이브로 스트리밍하고, '정보 무정부주의자(anarchists)'들은 릴리스 그룹을 통해 미개봉 콘텐츠를 탈취해 공유하며, 금전적 이득을 노리는 공격자들은 정교한 비디오 서비스를 운영합니다. 국가 차원에서 불법 복제를 정보전의 일환으로 사용하는 경우도 있습니다.

미디어 불법 복제는 까다로운 문제입니다. Akamai는 세계 최대 비디오 미디어 제작사 및 유통사와 협업하여 '보호, 탐지, 실행' 접근 방식을 적용하고 있습니다. 이를 요약하면 다음과 같습니다.

보호: 콘텐츠 및 인증정보 도난 방지

- 비디오 제작 및 스토리지 시스템의 도난 방지
- 재스트리밍을 예방하기 위해 시청자 세부 정보의 도난 방지
- 지역 및 권리 침해 방지
- 플레이백 위반 행위 차단

탐지: 도난당한 파일의 사용자 식별

- 심층 로그 검사로 침해 행위에 대한 실시간 상황 파악
- 프록시 탐지를 통한 VPN 서비스 사용자 식별
- 워터마킹을 이용하여 도난당한 파일 식별 및 추적

실행: 지적 재산을 불법으로 사용하는 공격자 차단

- 토큰 접속을 철회하여 문제를 일으키는 IP 주소의 스트리밍 차단
- 스트리밍 수정을 통해 불법 복제된 스트리밍을 대체 콘텐츠로 전환
- 탐지된 사용자가 해당 프록시 IP를 사용하지 못하게 차단

절정: 시청자에 대한 공격

2019년 미국에서는 대규모의 새로운 구독 서비스가 출시되어 큰 성공을 거두었습니다. 하지만 24시간이 지나기도 전에 일부 고객은 자신의 계정이 잠겼다며 소셜 미디어에 불만을 표출하기 시작했습니다. 이 사건은 데이터 유출이 아닌 크리덴셜 스터핑 공격이었습니다.

OTT(Over the Top) 서비스에서 시청자의 계정이 유출되었다는 것을 확인하면 대부분의 기업들은 추가 유출을 방지하기 위해 유료 고객에게 계정 재설정을 요청합니다. 기업의 지적 재산을 보호하는 데는 도움이 되지만 고객 경험의 불편을 초래할 수 있습니다.

이러한 공격의 대부분은 자동화된 '계정 스터핑' 방식을 사용합니다. 계정 잠금 및 재설정의 필요성을 줄일 수 있는 한 가지 방법은 봇을 관리하는 것입니다. 우수한 봇 관리 툴은 로그인 주체가 사람인지를 선제적으로 파악하고 사람인 척 행동하는 봇을 차단할 수 있습니다.

ID는 OTT 혁신의 핵심 구성요소입니다. 우수한 시청자 경험을 가능하게 하고 수익성 높은 구독 기반 및 광고 기반의 비즈니스 모델을 구현하기 때문에 ID를 보호하는 것이 무엇보다 중요합니다.

결말: 영웅의 귀환

비디오 제작사와 유통사가 더 안전한 생태계를 향한 여정을 마무리하는 가운데 공격자들은 상처를 치료하며 다음 공격을 준비하고 있습니다.

Akamai는 비디오 전송 및 클라우드 보안 분야에서 핵심 파트너 역할을 할 수 있는 든든한 지원자입니다. Akamai가 기업, 앱, API 보안을 지원하고 불법 복제 관련 문제를 파악 및 해결하는 방법, 봇 관리 솔루션을 통해 클론 공격을 줄이는 방법을 확인하시기 바랍니다.

속편에서 뵙겠습니다.

참조

1) 넷플릭스 해킹으로 '오렌지 이즈 더 뉴 블랙' 신규 에피소드 10편 유출(Netflix hacked, 10 new Orange Is the New Black episodes leaked)

2) 해적들이 '한니발'을 죽였나?(Did pirates kill 'Hannibal'?) | The Hill

3) BeIN, 불법 복제로 인한 매출 감소로 제작 인력 감축(BeIN axes staff claiming profits hit by piracy)

4) 샌드바인 백서 — 비디오 및 텔레비전 불법 복제: 생태계와 영향(Sandvine White Paper — Video and Television Piracy: Ecosystem and Impact)

5) EUIPO 리포트: 2018년 10억 유로 상당의 불법 'IPTV' 스트리밍 발생: 전체 불법 복제는 일부 감소(EUIPO Reports: Nearly €1B in illegal 'IPTV' streaming in 2018; overall piracy down slightly)

Akamai Experience the Edge