入門書

動画関連企業を守る - エンタープライズ、コンテンツ、視聴者の保護

プロットポイント 1：エンタープライズへの攻撃

動画制作は本質的に共同作業です。業界はすでにファイルベースのワークフローに移行し、いくつかの「エンドポイント」からアセットにアクセスできるようになっています。つまり、セキュリティには抜け穴がいくつか生じている可能性があります。

例えば、フリーランサーやポストプロダクション会社はどうでしょうか。多くの場合、こうした外部の協力者は自身が攻撃の標的になるという意識が乏しく、たとえ意識していたとしても、セキュリティチェックを適切に行うためのリソースや専門知識が不足しています。攻撃者にとっては恰好の標的と言えます。

実際、2018 年に発生した『**Orange Is the New Black**』のハッキングでは、大ヒットしたこの Netflix 番組の新シーズンの作業を請け負っていたポストプロダクション会社が、経済的利益を得ようとする攻撃者に狙われ、セキュリティを破られたことが原因でした。攻撃者は、身代金の要求を目的として、完了前の中間品質のファイルを盗み出しました。[1]

また、24 社を超える企業が参加して最近実施された米国の非公開イベント、**Cybersecurity for Broadcasters Retreat** で、最もリクエストの多いトピックは、リモートアクセスのセキュリティとベンダーセキュリティでした。

この問題に役立つ方策を 2 つ挙げてみます。

1. 主要なリソースへのアクセスを求める社員や業務委託先にゼロトラスト・ネットワーク・アクセス・ツールを適用することで、最小権限戦略を強化する
2. セキュア Web ゲートウェイ（SWG）を使用し、ネットワーク内からの悪性トラフィックを検知してブロックする

このようなゼロトラストのアプローチによって、泥棒が金庫に到達できる可能性が軽減し、たとえ到達できたとしても、逃走する能力を制限できます。

プロットポイント 2：動画への攻撃

2013 年、サイコホラー／スリラー TV シリーズの『Hannibal』が「低評価」のため打ち切りになりました。しかし、このシリーズはその年に最も違法ダウンロードされた番組の 5 位になっています。この番組のプロデューサーである Martha De Laurentiis 氏は、『Hannibal』の打ち切りに海賊版の問題が大きく関連していると述べました。[2]

2019 年 6 月には、カタールの放送局、BeIN Media Group が収益の悪化により従業員を 300 人解雇すると発表しました。何が原因でしょうか？ BeIN は、ライバルである beoutQ が BeIN の貴重な有料スポーツコンテンツの著作権侵害を行ったと主張しています。[3]

メディアの海賊版は無声映画の時代からありました。配信がストリーミングに移行し、グローバル化が進むにつれ、海賊行為はより簡単になり、儲けも大きくなりました。海賊版の影響については様々な調査結果がありますが、動画の海賊行為によって米国では年間 10 億ドル以上 [4]、ヨーロッパでも 10 億ユーロ以上 [5] が生み出されているというのがアナリストの一貫した見解です。

海賊行為は多面的なエコシステムであり、ソーシャルメディアで友人にライブストリーミングする素人もいれば、リリースグループを通じて初回放送のコンテンツをリッピングして共有する「インフォアナーキスト」や、経済的利益を目的として高度な動画サービスを運営する攻撃者もいます。さらに国家が情報戦争の一環として海賊版を利用することもあります。

この問題の解決は一筋縄ではいきません。Akamai は世界有数の動画メディア制作企業や配信企業の多くと協力し、「保護、検知、措置」のアプローチを進めてきました。まとめると次のとおりです。

保護：コンテンツと認証情報の窃盗を阻止する

- 動画の制作および保管システムを窃盗から保護する
- 視聴者の詳細情報を窃盗から保護し、再ストリーミングを防ぐ
- 地理的制限や権限を侵害から守る
- 再生権限を侵害から守る

検知：盗まれたファイルの使用者を見つける

- ディープ・ログ・インスペクションによって侵害行為をリアルタイムで把握する
- プロキシ検知で VPN サービスのユーザーを見つける
- 盗まれたファイルをウォーターマークで特定し追跡する

措置：知的財産を盗用する略奪者に対抗措置をとる

- トークンアクセスの取り消しによって、違法な IP アドレスによるストリーミングを阻止する
- ストリームの変更により、著作権侵害を受けたストリームを別のコンテンツに置き換える
- プロキシブロックによって、検知されたユーザーがそのプロキシ IP を使用できないようにする

クライマックス：視聴者への攻撃

2019 年、米国である大規模なサブスクリプションサービスが開始され、大きな成功をおさめました。しかし、24 時間以内に、アカウントがロックされたという新規顧客からの苦情がソーシャルメディアにあふれました。このケースでは、原因はデータ漏えいではなく Credential Stuffing 攻撃でした。

視聴者のアカウントでセキュリティ侵害が生じていることを Over The Top（OTT）サービス側が検知すると、多くの場合、料金を支払っている顧客にアカウントをリセットし、それ以上の窃盗を阻止するよう求めます。この方法では、その企業の知的財産を守ることはできますが、顧客体験が低下してしまいます。

この種の攻撃の多くは自動化された Account Stuffing であるため、ボット管理ツールを使用すれば、アカウントのロックアウトやリセットの必要性が軽減されます。実際の人によるログインをあらかじめ特定できるようにして、同じ人になりすましたボットをブロックできれば理想的です。

アイデンティティは OTT が成功するための基本的な要素です。OTT が視聴者に魅力的な体験を提供し、収益率の高いサブスクリプションベースや広告支援ベースのビジネスモデルを実現するためには、アイデンティティの保護が欠かせません。

結末：英雄の帰還

動画制作企業や配信企業がエコシステムセキュリティを強化しても、攻撃者は傷を癒し、また次の攻撃の準備をするだけです。

Akamai は、動画配信とクラウドセキュリティ両方における重要なパートナーとして、貴社の理想的なサイドキックとなることができます。Akamai はエンタープライズ、アプリケーション、API をどのように保護するのでしょうか。著作権侵害を調査し、これに対抗するために、Akamai はどのように役立つのでしょうか。そして Akamai のボット管理ソリューションはクローンの攻撃をどのように軽減するのでしょうか。

続きは続編をご覧ください。

参考文献

1) ハッカーが Netflix の『Orange Is the New Black』新シリーズの 10 話分をリーク

2)『Hannibal』は海賊に殺された？ | The Hill

3) 海賊版による収益源で BeIN がスタッフを解雇

4) Sandvine ホワイトペーパー ― 動画とテレビ番組の著作権侵害：エコシステムと影響

5) EUIPO レポート：2018 年には約 10 億ユーロの違法な「IPTV」ストリーミングが発生、全体的には海賊行為がわずかに低下