

断ち切る アカウント乗っ取りの キルチェーンを断ち切る

サイバー・キル・チェーンはどのようなものかご存じですか？

アカウント乗っ取りのキルチェーンにおける、サイバー攻撃の各段階を掘り下げ、その阻止方法についてご説明します。

1



予備調査

現象

データ漏えい、認証情報の盗難



防御方法

実装：

- Web Application Firewall
- 暗号化
- 既知の漏えいした情報に対する認証情報の照合
- 強力なセキュリティポリシー



攻撃者による回避策

攻撃者は標的を別のサイトに移すか、ダークウェブで認証情報を購入します。

2



武器の準備

現象

ログイン失敗のわずかな増加



防御方法

確認：

- 正当なユーザーによるログインかどうか
- ボット管理ソフトウェアがチューニングされているか
- ログインエンドポイントが MFA (多要素認証) により保護されているか



攻撃者による回避策

攻撃者は、ボットが検知されたらボットソフトウェアをチューニングします。

3



攻撃

現象

トラフィックの急増、大量のログインリクエスト



防御方法

検証：

- レートコントロール
- MFA
- ユーザーのふるまいの異常
- ボット管理ソフトウェアによる高度な検知



攻撃者による回避策

攻撃は停止し、キルチェーンは断ち切られます。一部のきわめて高度なボットは一時的に検知を逃れる可能性があります。

4



悪用

現象

人の手による単発のリクエスト（わずかなログインの増加）



防御方法

検査：

- ユーザーのふるまいの異常



攻撃者による回避策

攻撃者に大きな回避策はありません。個々の攻撃試行について、犯罪者はアカウント所有者をソーシャルネットワークで検索することができます。

5



アクション

現象

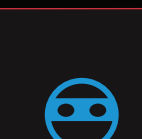
顧客からアカウント乗っ取り被害の報告が急増



防御方法

監視：

- ユーザーがログアウトするまでユーザーのリスクを継続的に監視



攻撃者による回避策

アカウント保護ソフトウェアが攻撃をブロック。攻撃者はあきらめます。

Akamai がアカウントの乗っ取りを阻止するためのサポートをいたします

[詳細はこちら](#)

