Mythosレベルの攻撃に対応するZscaler Deception

ZPAとDeceptionによる多層型防御

概要

Cloud Security Alliance (CSA)は、デセプションの機能を90日以内に構築するよう推奨しています。ZPAのお客様であればわずか数分で完了します。

Mythos対応の脅威検出

MythosレベルのAIによる攻撃、およびCSAが提唱する90日以内のデセプション導入要件に対応するため、Zscaler Deceptionはワンクリックの展開を実現します。新たなエージェントやハードウェア、ネットワークの再設定なしに、ゼロトラスト環境全体で包括的なデセプション戦略が有効になります。Deceptionは既存のインフラを通じて有効化され、ユーザーへの変更も一切なく以下を実現できます。

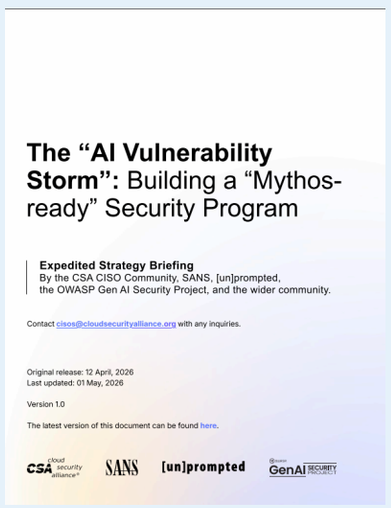
- **ラテラル ムーブメントの阻止：**デコイ アプリケーションは、Zscaler Private Accessの実際のプライベート アプリと並んで表示されます。攻撃者が水平移動を試みても、実際のリソースではなくデコイにアクセスすることになります。
- **エンドポイント ルアーによる攻撃者のリダイレクト：**Zscaler Client Connectorを通じて展開されるデコイの認証情報やブックマークにより、侵害されたアイデンティティーは実際のリソースから遠ざかり、直接デコイに誘導されます。
- **許可されていないサービスを探索する攻撃者の捕捉：**実際のアプリ上に配置されたデコイ サービスにより、正規ユーザーが決してアクセスしないポートをスキャンする攻撃者を捕捉します。

AIに対する確定的なアラート

AIによる攻撃は、正規のツールを用いて数分でキル チェーンを進行し、EDRのような従来の制御では検知されません。Deceptionはシグネチャーや行動検出の問題を完全に回避します。正規ユーザーがデコイにアクセスする理由はないため、すべてのやり取りは疑いの余地なく悪意のあるものと確定されます。エージェント型AIの攻撃者であっても、侵害された内部者であっても、シグナルは同じであり、侵害の決定的な証拠となります。

ZPAによる自動封じ込め

デコイが起動した瞬間、DeceptionはZPAを通じて、侵害されたユーザーのプライベート アプリケーションへのアクセスを、サインインしているすべてのデバイスで自動的に取り消します。事前承認された対応により、アナリストが手動でブロックを承認する必要はなく、攻撃者は水平移動する前に遮断されます。これにより、SOCキューの速度ではなく攻撃の速度でラテラル ムーブメントを排除できます。



Cloud Security Allianceは、企業がMythosを悪用した攻撃に備えられるよう、米CISA、NSA、およびホワイトハウスの元サイバー政策責任者らをはじめとする、250名以上のCISOとセキュリティ リーダーを招集しました。

結果：緊急戦略ブリーフィングが作成され、Mythosに対応できるセキュリティ プログラムのための**11の優先アクション**が示されました。

9：デセプション能力を構築する

今後90日以内の実装義務化を伴う「HIGH」リスクの分類。

「デセプションは攻撃ツールや脆弱性に依存せず、*TTP*に基づいて攻撃と攻撃者を特定します。」

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com/jp

Zero Trust Everywhere