Cisco WSAランサムウェア検出機能およびAMP統合の検証

内容

問題

Cisco Secure Web Appliance(WSA)がトリプルXランサムウェアに固有のシグニチャまたは検出機能を提供するかどうかに関して問い合わせがありました。この質問には、高度なマルウェア防御(AMP)とCisco Talos脅威インテリジェンスの統合がWSAプラットフォームで正しく機能しているかどうかを検証する方法について、明確化を求める要求も含まれていました。

環境

- CiscoセキュアWebアプライアンス(WSA)
- 高度なマルウェア防御(AMP)の統合
- Cisco Talos脅威インテリジェンスの統合
- WebレピュテーションとURLフィルタリング(WBRS)
- アンチマルウェアスキャンエンジン(Webroot、McAfee、Sophos)
- Application Visibility and Control（AVC）

解決方法

Cisco Secure Web Applianceは、Triple X Ransomwareという名前の単一の専用シグニチャを利用しません。代わりに、WSAは、さまざまな検出技術を使用してランサムウェアの脅威を特定してブロックする包括的なマルチレイヤセキュリティアーキテクチャを採用しています。これには、Triple X Ransomwareの亜種も含まれます。

WSAの検出方法

WSAプラットフォームは、ランサムウェア保護に次の検出技術を使用します。

- パターンマッチングアルゴリズム
- 発見的分析
- エミュレーション技術
- Cisco Talos脅威インテリジェンスと統合された高度なマルウェア防御(AMP)
- WebレピュテーションとURLフィルタリング(WBRS)
- Webroot、McAfee、Sophosなどの複数のアンチマルウェアスキャンエンジン
- Application Visibility and Control（AVC）

これらの検出機能は、新たな脅威に対する保護を確保するために、数分ごとに導入される新しいルールで継続的に更新されます。

AMPとTalosの統合の検証

高度なマルウェア防御(AMP)とCisco Talos脅威インテリジェンスの統合がWSAで正しく機能していることを確認するために、管理者は次の口グを確認できます。

手順1:WSAアクセスログの確認

WSAアプライアンスのアクセスログを調べて、ダウンロードされたファイルとWeb要求にAMP判定が適用されていることを確認します。

手順2:AMPログを確認する

AMPログを確認して、マルウェア分析の結果と脅威インテリジェンスデータが処理されていることを確認します。

ステップ3:WBRSスコアの確認

Webレピュテーション(WBRS)スコアが入力されており、ログ内のWeb要求に関連付けられてい

ることを確認します。

AMPの判定とWBRSスコアがログに入力され適用されている場合は、AMPとTalosの統合が期待どおりに機能しており、脅威に関するインテリジェンスベースのリアルタイムの判断を提供していることを示しています。

原因

これは、トラブルシューティングを必要とする技術的な問題ではなく、WSAランサムウェア検出機能に関する情報の要求でした。この調査は、WSAが特定のランサムウェアの亜種に対してどのように防御を行うのかを理解し、脅威インテリジェンス統合が適切に機能していることを確認する必要性から行われました。

関連コンテンツ

- Cisco Secure Web Applianceの機能と利点
- Cisco Talos脅威インテリジェンスサービス
- Cisco Secure Web Applianceデータシート
- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。