Cisco Secure IDS の Nimda ウィルスへの対応

目次

概要

この文書では、Cisco Secure Intrusion Detection System（IDS）による Nimda ワーム（コンセプト ウィルスとしても有名）の識別と、Web サーバを攻撃から守る方法について説明します。 ワームの動作に関する複雑で技術的な問題はすでにいろいろな場所で文書化されており、この文書では取り扱っていません。 Nimda ワームに関する最も技術的な説明の 1 つが、「CERT® Advisory CA-2001-26 Nimda Worm」で確認できます。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

Nimda ワームはインターネットで積極的に広がっているハイブリッド ワームおよびウイルスです。 Cisco IDS の Nimda および機能を理解するために拡散を軽減するこれら二つの用語を定義する

ことは重要です:

- ワームとは、人間による操作なしに自動的に拡散する悪質なコードを意味します。
- **ウイルスは** E メールを開くときある種の人間の介入を通って広がる悪意のあるコードをのような、参照するか感染したWebサイトを、または手動で実行します感染したファイルを示します。

Nimda ワームは、実際にはワームとウィルスの両方の性質を持つハイブリッド型です。 Nimda は複数の方法で感染しますが、多くの場合、それは人間にとよる操作を必要とします。 Cisco IDS ホストセンサは Microsoft の Internet Information Server （IIS）の脆弱性によって広がるワームのような感染方式をブロックします。 Cisco IDS はメールの添付データを開くときウイルスのようの、手動による感染理由、のような、参照します感染したWebサイトをブロックしません、または手動で 感染したファイルを実行して下さい。

Cisco IDS Host Sensor による Nimda の防御

Cisco IDS ホストセンサは Nimda ワームが使用するそれらを含むディレクトリ トラバーサル不正侵入を防ぎます。 ワームが Cisco IDS で保護されした Webサーバを危殆化するように試みるとき攻撃は失敗し、サーバは危殆化されません。

これらの Cisco IDS ホストセンサ ルールは Nimda ワームの成功を防ぎます:

- IIS ディレクトリ トラバーサル（4 ルール）
- IIS ディレクトリ トラバーサルとコードの実行（4 ルール）
- IIS Double Hex 符号化ディレクトリ トラバーサル（4 ルール）

Cisco IDS ホストセンサはまた Web コンテンツに不当な変更に対して守ります、従ってワームが他のサーバにそれ自身を広げるために Webページを変えないようにしません。

Cisco IDS は、標準的なセキュリティの最良実施例に基づいて、Web サーバを Nimda から防御しています。 これらの最良 の 方法は E メールを読まないか、または本番 Webサーバからの Web を参照するために定まりません、またネットワーク共有を持たないためにサーバで開いて下さい。 Cisco IDS ホストセンサは Webサーバが HTTP および IIS エクスプロイトによって妥協されることを防ぎます。 前述最良 の 方法は Nimda ワームがいくつかの手動で行う方法によって Webサーバに着かないようにします。

Cisco IDS Network Sensor による Nimda の識別

Cisco IDS ネットワークセンサは Nimda ワームが使用するそれらを含むウェブアプリケーション攻撃を識別します。 ネットワークセンサは不正侵入を識別し、Nimda 感染を隔離するために影響を受けたのかコンプロマイズド ホストについての詳細を提供できます。

起動 されるこれらの Cisco IDS ネットワーク センサ アラーム:

- WWW WinNT cmd.exe Access（SigID 5081）
- IIS CGI Double Decode（SigID 5124）
- WWW IIS Unicode Attack（SigID 5114）
- IIS Dot Dot Execute Attack（SigID 3215）
- IIS Dot Dot Crash Attack（SigID 3216）

オペレータはアラームを参照しません Nimda を名前で識別する。 彼らはターゲットを妥協するために Nimda 試み異なるエクスプロイトとして注意される一連のアラームを参照します。 アラ

ームは危殆化されたネットワークから接続されていなく、きれいになり、修正され、ホストにの送信元アドレスを識別します。

推奨される対処法

Nimda ワームから保護するために次の手順に従って下さい:

1. Microsoft から Microsoft Outlook、Outlook Express、利用可能 な Internet Explorer および IIS のための最新の更新を加えて下さい 。
2. 使用しているウィルス スキャン ソフトウェアを最新パッチでアップデートし、ウィルスの拡散を防ぎます。**注:** 感染から PC を保護するために最新のウイルスパッチをダウンロードできます。 PC が既に感染している場合、このウイルスパッチは手動で PC のハード ドライブをスキャンし、マシンから感染を取除くことを可能にします。
3. Cisco IDS を導入して、脅威を減らし、感染を抑え、サーバを保護してください。

関連情報

- Nimda ウイルスからネットワークを保護する方法
- シスコ製品のセキュリティについての勧告および注意
- Cisco Secure Intrusion Detection のサポートページ
- テクニカルサポート - Cisco Systems