Nimda ウイルスからネットワークを保護する方法

内容

概要

この文書では、ネットワークに対する Nimda ワームの影響を最小にする方法を説明し、次の 2 つのトピックを扱います。

- ネットワークが感染している。何を実行できるか。被害と影響を最小限に抑える方法。
- ネットワークはまだ感染していないか、または一部のみ感染している。このワームの拡散を最小にするために何ができるか

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの内容は、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。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

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 ワームの背景情報については、次のリンクを参照してください。

- http://www.cert.org/body/advisories/CA200126_FA200126.html
- http://vil.nai.com/vil/content/v_99209.htm
- http://www.sarc.com/avcenter/venc/data/w32.nimda.a@mm.html

対応プラットフォーム

この文書に記載されている Network-Based Application Recognition（NBAR）ソリューションには、Cisco IOS® ソフトウェアのクラスベース マーキング機能が必要です。特に、マッチング機能では、NBAR 内の HTTP サブポートクラシフィケーション機能を使用します。サポートされているプラットフォームおよび IOS ソフトウェア最低必要条件を次に要約します。

Platform	Cisco IOS ソフトウェアの最低バージョン
7200	12.1(5)T
7100	12.1(5)T
3660	12.1(5)T
3640	12.1(5)T
3620	12.1(5)T
2600	12.1(5)T
1700	12.2(5)T

注：Network-Based Application Recognition(NBAR)を使用するには、Cisco Express Forwarding(CEF)を有効にする必要があります。

NBAR はリリース 12.1E 以降の一部の Cisco IOS ソフトウェアのプラットフォームでもサポートされています。Network-Based Application Recognition のドキュメントの「サポート対象プロトコル」を参照してください。

クラスベース マーキングおよび Distributed NBAR（DNBAR）は次のプラットフォームでも使用できます。

Platform	Cisco IOS ソフトウェアの最低バージョン
7500	12.1(6)E
FlexWAN	12.1(6)E

NBAR を導入する場合は、Cisco Bug ID CSCdv06207（登録ユーザ専用）に注意してください。CSCdv06207 に記述されている回避策は、この障害に遭遇した場合に必要になる場合があります。

Cisco IOS ソフトウェアのすべての現行リリースで、Access Control List（ACL; アクセス コントロール リスト）ソリューションがサポートされています。

モジュラー Quality of Service（QoS）コマンドライン インターフェイス（CLI）を使用する必要

があるソリューションの場合は（レート制限 ARP トラフィックの場合または CAR の代わりにポリサーでレート制限を実現する場合など）、Cisco IOS ソフトウェア リリース 12.0XE、12.1E、12.1T、および 12.2 のすべてのリリースで使用できるモジュラー Quality of Service コマンド行インターフェイスが必要です。

専用アクセス レート（CAR）の使用には、Cisco IOS ソフトウェア リリース 11.1CC および 12.0 以降のソフトウェアのすべてのリリースが必要です。

被害を最小限に抑え、影響を制限する方法

このセクションでは、Nimda ウィルスを広める可能性がある感染媒体について概説し、ウィルスの拡散を減らすヒントを示します。

- このワームは、MIME audio/x-wav タイプの E メール添付ファイルによって広がる可能性があります。**ヒント**：次の添付ファイルがある電子メールをブロックするルールを Simple Mail Transfer Protocol（SMTP）サーバに追加します。readme.exeAdmin.dll
- このワームは、Javascriptの実行が有効になっている感染したWebサーバをブラウズし、MS01-020（SP2を使用しないIE 5.0やIE 5.01など）で説明されている脆弱性のあるInternet Explorer(IE)をををを使用するとして感染をするをが発生する可能性があります。**ヒント**：ブラウザとして Netscape を使用するか、IE で Javascript を無効にするか、または IE に SP2 パッチを適用します。シスコ NBAR を使って、readme.eml ファイルがダウンロードされるのを防ぎます。NBAR を設定する例を次に示します。

```
Router(config)#class-map match-any http-hacks
Router(config-cmap)#match protocol http url "*readme.eml*"
```

トラフィックのマッチングを行った後、トラフィックを破棄するか、ポリシーベースのルーティングで感染したホストを監視できます。完全な実装例は、『"Code Red" ワームをブロックするための Network-Based Application Recognition およびアクセス コントロール リストの使用方法』にあります。

- このワームは、IIS攻撃の形でマシンからマシンに広がることができます(主にCode Red IIの影響によって生じた脆弱性を悪用しようとしますが、MS00-078によって以前にパッチされた脆弱性も悪用しようとしま す)。**ヒント**：次の文書に記述された Code Red 対策方式を使用します。"Code Red " に起因する mallocfail と 高 CPU 利用率への対処法"Code Red" ワームをブロックするための Network-Based Application Recognition およびアクセス コントロール リストの使用方法

```
Router(config)#class-map match-any http-hacks
Router(config-cmap)#match protocol http url "*.ida*"
Router(config-cmap)#match protocol http url "*cmd.exe*"
Router(config-cmap)#match protocol http url "*root.exe*"
Router(config-cmap)#match protocol http url "*readme.eml*"
```

トラフィックのマッチングを行った後、トラフィックを破棄するか、ポリシーベースのルーティングで感染したホストを監視できます。完全な実装例は、『"Code Red" ワームをブロックするための Network-Based Application Recognition およびアクセス コントロール リストの使用方法』にあります。TCP synchronize/start（SYN）パケットをレート制限します。これによってホストは保護されませんが、パフォーマンスを下げてネットワークを実行し続けることができます。レート制限 SYN では、一定のレートを超過するパケットを破棄するため、一部の TCP 接続は通過しますが、すべてではありません。設定例については、『DOS 攻撃時の CAR の使用』の「レートリミット TCP Syn パケット」の項を参照してください。ARP スキャンの量が原因でネットワーク上で問題を起こる場合、レート制限 Address Resolution Protocol（ARP）のトラフィックを考慮します。ARP トラフィックのレート制限を行うには、次のように設定します。

```
class-map match-any arp
   match protocol arp
!
!
policy-map ratelimitarp
   class arp
      police 8000 1500 1500 conform-action transmit exceed-action drop violate-action drop
```

この後、このポリシーを該当 LAN インターフェイスに出力ポリシーとして適用する必要があります。ネットワークで許可する 1 秒あたりの ARP の数を考慮して適切な数に変更します。

- ワームは、Active Desktop を有効にした状態で（W2K/ME/W98 デフォルト）Explorer 内で eml または .nws をハイライトさせることによって広がる可能性があります。 これにより、THUMBVW.DLL がファイルを実行し、その中で参照されている README.EML をダウンロードしようとします（IE バージョンおよびゾーン設定によります）。**ヒント：上で**お勧めしたように、NBARを使用してreadme.emlのダウンロードをフィルタリングしてください。
- ワームはマップされたドライブによって広がる可能性があります。マップ済みのネットワーク ドライブを持つ感染したマシンはすべて、マップされたドライブとサブディレクトリ上のファイルをすべて感染させる可能性があります。**ヒント**：感染したコンピュータが TFTP を使用して感染していないホストにファイルを転送できないように、Trivial File Transfer Protocol（TFTP）（ポート 69）をブロックします。ルータの TFTP アクセスは引き続き使用可能にします（コードをアップグレードするための経路が必要になる場合があるため）。 ルータが Cisco IOS ソフトウェア バージョン 12.0 以降を実行している場合、Cisco IOS ソフトウェアを実行しているルータにイメージを転送するために、File Transfer Protocol（FTP）を使用する選択肢が常にあります。NetBIOS をブロックします。NetBIOS はローカル エリア ネットワーク（LAN）に残す必要はありません。 サービス プロバイダは、ポート 137、138、139、および 445 をブロックすることで、NetBIOS をフィルタに掛ける必要があります。
- ワームは、独自の SMTP エンジンを使って、他のシステムを感染させるために E メールを送ります。**ヒント：ネ**ットワークの内部にあるポート25(SMTP)をブロックします。Post Office Protocol (POP) 3 （ポート110）またはInternet Mail Access Protocol (IMAP) （ポート143）を使用して電子メールを取得しているユーザーは、ポート25にアクセスする必要はありません。ポート25のみがネットワークのSMTPサーバーに接続できます。Eudora、Netscape、およびOutlook Expressを使用しているユーザは、独自のSMTPエンジンを持ち、ポート25を使用して発信接続を生成するため、この操作は実行できない可能性があります。プロキシサーバやその他のメカニズムの使用に適用する必要があります。
- Cisco CallManager/Applications サーバをクリーニングします。**ヒント**：ネットワーク内のCall ManagerおよびCall Managerアプリケーションサーバを使用するユーザは、ウイルスの拡散を停止するために次の操作を行う必要があります。感染しているマシンを Call Manager からブラウズすること、および、Call Manager サーバ上のいずれかのドライブを共有することは厳禁です。Nimda ウイルスを除去するには、『Cisco CallManager 3.x および CallManager Applications サーバからの Nimda ウィルスの除去』に示されている指示に従います。
- CSS 11000 で Nimda ウィルスをフィルタ処理します。**ヒント**： CSS 11000を使用するユーザは、「CSS 11000でのNimdaウィルスのフィルター」の指示に従ってNIMDAウィルスをクリーニングする必要があります。
- Nimda ウイルスに対する Cisco Secure Intrusion Detection System（CS IDS）の対応**ヒント**： CS IDSには2つの異なるコンポーネントがあります。1 つはホスト センサーを備えたホストベースの IDS（HIDS）で、もう 1 つはネットワーク センサーを備えたネットワークベー

スの IDS（NIDS）です。どちらも Nimda ウィルスに対して異なる方法で対応します。詳細な説明と推奨される対処法については、『Cisco Secure IDS の Nimda ウィルスへの対応』を参照してください。

関連情報

- "Code Red" ワームをブロックするための Network-Based Application Recognition およびアクセス コントロール リストの使用方法
- "Code Red " に起因する mallocfail と 高 CPU 利用率への対処法
- DoS 攻撃中の CAR の使用
- Cisco セキュリティ アドバイザリとセキュリティ通知
- テクニカル サポートとドキュメント – Cisco Systems