NBARとACLを使用した「Code Red」ワームのブロック

内容

概要

このドキュメントでは、Ciscoルータ上のCisco IOS®ソフトウェア内のNetwork-Based Application Recognition(NBAR)およびアクセスコントロールリスト(ACL)を介して、ネットワーク入力ポイントで「Code Red」ワームをブロックする方法について説明します。この解決策は、Microsoft 製 IIS サーバ用推奨パッチと一緒に使用する必要があります。

注：この方法は、Cisco 1600シリーズルータでは機能しません。

注：一部のP2Pトラフィックは、そのP2Pプロトコルの特性により完全にブロックできません。これらのP2Pプロトコルは、トラフィックを完全にブロックしようとするすべてのDPIエンジンをバイパスするように、シグニチャを動的に変更します。したがって、帯域幅を完全にブロックするのではなく、帯域幅を制限することを推奨します。このトラフィックの帯域幅を抑制します。帯域幅を大幅に削減ただし、接続は通過します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Quality of Service(QoS)サービスポリシーは、モジュラQoSコマンドラインインターフェイス(CLI)のコマンドを使用します。
- NBAR
- ACL
- ポリシー ベース ルーティング

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設定は、Cisco IOSバージョン12.2(24a)が稼働するCisco 3640でテストされています

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。

Code Red ワームを阻止する方法

「Code Red」と闘うために最初に行うべきことは、Microsoftから入手可能なパッチを適用することです(Method A:次のACLを使用します)。 これにより、脆弱なシステムが保護され、感染したシステムからワームが削除されます。ただし、サーバにパッチを適用しても、ワームによるサーバへの感染が防止されるだけで、HTTP GET要求がサーバに到達するのを停止することはありません。サーバが大量の感染攻撃にさらされる可能性は依然として存在します。

このアドバイザリに記載されているソリューションは、Microsoftパッチと連携して、ネットワーク入力ポイントでの「Code Red」HTTP GET要求をブロックするように設計されています。

このソリューションは感染をブロックしようとしますが、大量のキャッシュエントリ、隣接関係、およびNAT/PATエントリの蓄積による問題は解決しません。HTTP GET要求の内容を分析する唯一の方法はTCP接続の確立後です。次の手順は、ネットワークのスキャンから保護するのに役立ちません。ただし、外部ネットワークからの侵入からサイトを保護したり、マシンがサービスする必要がある感染試行回数を減らしたりします。着信フィルタリングと組み合わせて、発信フィルタリングを使用すると、感染したクライアントが「Code Red」ワームをグローバルインターネットに拡散するのを防止できます。

対応プラットフォーム

このドキュメントで説明するソリューションには、Cisco IOSソフトウェアのクラスベースの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	最小 Cisco IOS ソフトウェア
7200	12.1(5)T

7100	12.1(5)T
3745	12.2(8)T
3725	12.2(8)T
3660	12.1(5)T
3640	12.1(5)T
3620	12.1(5)T
2600	12.1(5)T
1700	12.2(2)T

注：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。

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	最小 Cisco IOS ソフトウェア
7500	12.1(6)E
FlexWAN	12.1(6)E

IIS Web ログでのアタックの形跡の検出

最初の感染試行は、ターゲットIISサーバに大きなHTTP GET要求を送信します。元の「Code Red」機器シンボルを次に示します。

```
2001-08-04 16:32:23 10.101.17.216 - 10.1.1.75 80 GET /default.ida
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNN%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u
7801%u9090%u9090%u8190%u00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a 403
```

「Code Red」IIのフットプリントを次に示します。

```
2001-08-04 15:57:35 10.7.35.92 - 10.1.1.75 80 GET /default.ida XXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX%u9090
%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%
u9090%u8190%u00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a 403 -
```

GET要求は常に.ida拡張子を持つファイルを探していることに注意してください。これは、すべての感染試行で共通の文字列であるため、IOSでクラスベースのマーキングを使用する照合基準として使用できます。GET要求の残りの部分は、バッファオーバーフローを作成しようとしているだけなので、必ずしも一貫性があるとは限りません。これは、上記の2つのエントリを比較することで確認できます。

この2つのシグニチャの違いは、CodeRed.v3またはCodeRed.Cと呼ばれる「Code Red」ワームの新しい系統によるものです。元の「Code Red」系統はGET要求に「NNNNNN」文字列を含み、新しい系統は「XXXXXXXX」を含みます。 詳細については、Symantecのアドバイザリを参照してください。

2001年8月6日午後6時24分に、新しい設置面積を記録しました。私たちは、これがeEye脆弱性ス

キャナによって残されたフットプリントであることを知りました 。

```
2001-08-06 22:24:02 10.30.203.202 - 10.1.1.9 80 GET /x.ida AAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=X 403 HTTP/1.1 -
```

このアドバイザリに記載されている「Code Red」をブロックする技術は、次のセクションに示すようにクラスマップ定義を強化するだけで、これらのスキャン試行をブロックすることもできます。

IOSクラスベース マーキング機能を使った「Code Red」攻撃のマーク

「Code Red」ワームをブロックするには、次の3つの方法のいずれかを使用します。3つの方法はすべて、Cisco IOS MQC機能を使用して悪意のあるトラフィックを分類します。その後、このトラフィックは次のように廃棄されます。

方法A:ACLの使用

この方法では、出力インターフェイス上のACLを使用して、マーキングされた「Code Red」パケットをドロップします。次のネットワークダイアグラムを使用して、この方法の手順を説明します。

この方法を設定する手順を次に示します。

1. 次に示すように、Cisco IOSソフトウェアのクラスベースマーキング機能を使用して、着信「Code Red」ハックを分類します。

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

   上記のクラスマップは、HTTP URLの内部を参照し、指定された文字列のいずれかに一致します。「Code Red」のdefault.ida以外に他のファイル名が含まれていることに注意してください。 このテクニックを使用して、Sadmindウイルスなどの同様のハック試行をブロックできます。この攻撃については、次のドキュメントで説明します。
   http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS00-078.asphttp://www.sophos.com/virusinfo/analyses/unixsadmind.html
2. ポリシーを作成し、**setコマンドを使用**して、インバウンドの「Code Red」ハックにポリシーマップをマークします。このドキュメントでは、DSCP値1（10進数）を使用します。これは、他のネットワークトラフィックがこの値を伝送しているとは限らないためです。ここでは、「Code Red」ハックに「mark-inbound-http-hacks」という名前のポリシーマップをマークします。

```
Router(config)#policy-map mark-inbound-http-hacks
Router(config-pmap)#class http-hacks
Router(config-pmap-c)#set ip dscp 1
```

3. 着信「Code Red」パケットをマークするために、ポリシーを入力インターフェイスの着信ポリシーとして適用します。
```
Router(config)#interface serial 0/0
Router(config-if)#service-policy input mark-inbound-http-hacks
```

4. サービスポリシーで設定されているように、DSCP値1と一致するACLを設定します。
```
Router(config)#access-list 105 deny ip any any dscp 1
Router(config)#access-list 105 permit ip any any
```

   注：Cisco IOSソフトウェアリリース12.2(11)および12.2(11)Tでは、NBARで使用するクラスマップでの定義で**log**キーワードがサポートされています(CSCdv48172)。 以前のリリースを使用している場合は、ACLで**log**キーワードを使用しないでください。これにより、すべてのパケットがCEFスイッチングではなくプロセススイッチングされ、NBARはCEFを必要とするため動作しません。
5. ACLアウトバウンドを、ターゲットWebサーバに接続する出力インターフェイスに適用します。
```
Router(config)#interface ethernet 0/1
Router(config-if)#ip access-group 105 out
```

6. ソリューションが期待どおりに動作することを確認します。**show access-list**コマンドを実行し、deny文の「matches」値が増加していることを確認します。
```
Router#show access-list 105
Extended IP access list 105
 deny ip any any dscp 1 log (2406 matches)
 permit ip any any (731764 matches)
```
   設定手順では、**no ip unreachable** interface-levelコマンドを使用してIP unreachableメッセージの送信を無効にして、ルータが過剰なリソースを消費しないようにすることもできます。この方法は、「方法B」の項で説明されているように、DSCP=1トラフィックをNull 0にポリシールーティングできる場合は推奨されません。

方法B:ポリシーベース ルーティング (PBR)の使用

この方式では、ポリシーベースルーティングを使用して、マークされた「Code Red」パケットをブロックします。メソッドAまたはメソッドCがすでに設定されている場合、このメソッドのコマンドを適用する必要はありません。

この方法を実装する手順を次に示します。

1. トラフィックを分類し、マーキングします。メソッドAに**示すclass-map**コマンド**とpolicy-map**コマンドを使用します。
2. **service-policyコマンド**を使用して、着信する「Code Red」パケットをマークするために、

入力インターフェイスの着信ポリシーとしてポリシーを適用します。方法Aを参照。

3. マークされた「Code Red」パケットと一致する拡張IP ACLを作成します。

```
Router(config)#access-list 106 permit ip any any dscp 1
```

4. route-mapコマンドを使用して、ルーティングポリシーを作成します。

```
Router(config)#route-map null_policy_route 10
Router(config-route-map)#match ip address 106
Router(config-route-map)#set interface Null0
```

5. ルートマップを入力インターフェイスに適用します。

```
Router(config)#interface serial 0/0
Router(config-if)#ip policy route-map null_policy_route
```

6. show access-listコマンドを使用して、ソリューションが期待どおりに動作することを確認します。出力ACLを使用していて、ACLロギングを有効にしている場合は、次に示すようにshow logコマンドも使用できます。

```
Router#show access-list 106
Extended IP access list 106
 permit ip any any dscp 1 (1506 matches)

Router#show log
Aug 4 13:25:20: %SEC-6-IPACCESSLOGP:
 list 105 denied tcp A.B.C.D.(0) -> 10.1.1.75(0), 6 packets
Aug 4 13:26:32: %SEC-6-IPACCESSLOGP:
 list 105 denied tcp A.B.C.D.(0) -> 10.1.1.75(0), 6 packets
```

すべての出力インターフェイスに出力ACLを必要とせずに、ルータの入力インターフェイスで廃棄を決定できます。ここでも、no ip unreachablesコマンドを使用して、IP到達不能メッセージの送信を無効にすることをお勧めします。

方法C:クラスベース ポリシングの使用

この方式は通常、PBRまたは出力ACLに依存しないため、最もスケーラブルです。

1. メソッドAに示すclass-mapコマンドを使用してトラフィックを分類します。
2. policy-mapコマンドを使用してポリシーを構築し、policeコマンドを使用して、このトラフィックの廃棄アクションを指定します。

```
Router(config)#policy-map drop-inbound-http-hacks
Router(config-pmap)#class http-hacks
Router(config-pmap-c)#police 1000000 31250 31250
 conform-action drop exceed-action drop violate-action drop
```

3. service-policyコマンドを使用して、入力インターフェイスのインバウンドポリシーとしてポリシーを適用し、「Code Red」パケットをドロップします。

```
Router(config)#interface serial 0/0
Router(config-if)#service-policy input drop-inbound-http-hacks
```

4. show policy-map interfaceコマンドを使用して、ソリューションが期待どおりに動作することを確認します。クラスの値と個々の一致基準が増加していることを確認します。

```
Router#show policy-map interface serial 0/0

Serial0/0

  Service-policy input: drop-inbound-http-hacks

    Class-map: http-hacks (match-any)
      5 packets, 300 bytes
```

```
    5 minute offered rate 0 bps, drop rate 0 bps
    Match: protocol http url "*default.ida*"
      5 packets, 300 bytes
      5 minute rate 0 bps
    Match: protocol http url "*cmd.exe*"
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: protocol http url "*root.exe*"
      0 packets, 0 bytes
      5 minute rate 0 bps
    police:
      1000000 bps, 31250 limit, 31250 extended limit
      conformed 5 packets, 300 bytes; action: drop
      exceeded 0 packets, 0 bytes; action: drop
      violated 0 packets, 0 bytes; action: drop
      conformed 0 bps, exceed 0 bps, violate 0 bps

  Class-map: class-default (match-any)
    5 packets, 300 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
    Match: any
```

NBARの制約事項

このドキュメントの方法でNBARを使用する場合、NBARでは次の機能がサポートされていないことに注意してください。

- 24を超える同時URL、ホスト、またはMIMEタイプが一致する
- URLの最初の400バイトを超える照合
- 非IPトラフィック
- マルチキャストおよびその他の非CEFスイッチングモード
- 断片化パケット
- パイプライン型の永続的HTTP要求
- セキュアHTTPによるURL/HOST/MIME/分類
- ステートフルプロトコルによる非対称フロー
- NBARを実行しているルータから発信された、またはルータ宛てのパケット

次の論理インターフェイスではNBARを設定できません。

- Fast EtherChannel
- トンネリングまたは暗号化を使用するインターフェイス
- VLAN
- ダイヤラインターフェイス
- マルチリンク PPP

注：NBARはCisco IOSリリース12.1(13)E以降のVLANで設定できますが、ソフトウェアスイッチングパスでのみサポートされます。

トンネリングまたは暗号化が使用されるWANリンクの出力トラフィックの分類にはNBARを使用できないため、LANインターフェイスなどのルータの他のインターフェイスにNBARを適用して、トラフィックがWANリンクに出力される前に入力分類をします。

NBARの詳細については、「関連情報」のリンクを参照してください