"Code Red"ワームをブロックするためのネットワークベースのアプリケーション認識およびACL の使用方法

目次

概要

この資料は Network-Based Application Recognition （ NBAR ）によってネットワークイングレスポイントで" Code Red " ワームおよび Cisco IOS® ソフトウェア on Cisco ブロックするために方式をルータ内のアクセス コントロール リスト（ ACL ）を提供したものです。 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: この方式は 1600 シリーズ ルータを on Cisco はたらかせません。

注: 一部の P2P トラフィックは、その P2P プロトコルの特性のために完全にブロックされない場合があります。 これらの P2P プロトコルは動的に完全にトラフィックをブロックすることを試みる解像度エンジンをバイパスするためにシグニチャを変更します。 従って、ブロッキングそれらの代りに帯域幅を完全に制限することを推奨します。 このトラフィックのための帯域幅を絞って下さい。 より少ない帯域幅を大いに与えて下さい; ただし、接続が行くようにして下さい。

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。

- モジュラ QoS Command Line Interface （ CLI ）のコマンドを使用する Quality of Service （ QoS ） サービス ポリシー。
- 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。 この資料の設定は Cisco 3640 でテストされました Cisco IOSバージョン 12.2(24a) を実行する

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たものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分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 "を戦うためにする必要がある最初の事柄は Microsoft から加えます利用可能 なパッチをあります（セクション 方式 A のリンクを参照して下さい: 下記の ACL を使用して下さい）。 これは脆弱 なシステムを保護し、感染した システムからワームを取除きます。 ただし、サーバにパッチを加えることはワームがサーバに打撃を与えることからだけサーバを感染させることを、それ停止しない HTTP GET 要求を防ぎます。 今でも感染の試みのフラッドが殺到するサーバのための可能性があります。

このアドバイザリで詳述されるソリューションはマイクロソフトのパッチと共にはたらくようにネットワークイングレスポイントで" Code Red " HTTP GET 要求をブロックするために設計されています。

このソリューションは HTTP GET 要求のコンテンツを分析する唯一の方法が TCP 接続の確立を次ので多数のキャッシュ エントリ、隣接関係および NAT/PAT エントリの集結によって引き起こされた問題を治さないどんなに感染をブロックするように試みます。 次のプロシージャはネットワークのスキャンから保護を助けません。 ただし、それは外部ネットワークからの蔓延からサイトを保護するか、または保守するマシンが必要がある感染の試みの数を減らします。 インバウンドフィルタリングと組み合わせて、アウトバウンドフィルタリングは感染させたクライアントがグローバル インターネットに" Code Red " ワームを広げることを防ぎます。

サポート対象プラットフォーム

この資料に説明があるソリューションは Cisco IOSソフトウェア内のクラスベース マーキング機能を必要とします。 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。

プラットフォーム	**最低限の 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; Cisco エクスプレス転送）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。

プラットフォーム	**最低限の 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 感染試みはターゲット IIS サーバに大きい HTTP GET 要求を送信 します。 オリジナル" Code Red " フットプリントは下記のように示されています:

```
2001-08-04 16:32:23 10.101.17.216 - 10.1.1.75 80 GET /default.ida
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
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 フットプリントは下記のように示されています:

```
2001-08-04 15:57:35 10.7.35.92 - 10.1.1.75 80 GET /default.ida XXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX%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 要求が .ida 拡張を用いるファイルを常に探して いることに注意して下さい。 従ってこれはすべての感染の試みのよくあるストリングで、としてクラスベース マーキングと IOS で一致条件使用することができます。 GET 要求の残りは必ずしもちょうどバッファオーバーフローを作成するように試みているように一貫していません。 これは上記の 2 つのエントリの比較によって見られる場合があります。

これら二つのシグニチャ間の違いが新しい種類がの" Code Red " ワーム、ダビングされた CodeRed.v3 または CodeRed.C.原因であることが今報告されています。 オリジナル" Code Red "種は GET 要求で新しい種類は「」が含まれているが、「NNNNNNNN」ストリングを示します。 Symantec Advisory を詳細については 参照して下さい。

6:24PM EDT 8月6日 2001 で、新しいフットプリントを記録しました。 これが eEye 脆弱性スキャナーによって置き去りになるフットプリントであることをその後学んでいました 。

```
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 -
```

このアドバイザリで提供される" Code Red "をブロックするための手法はまた次の セクションに示すようにクラスマップ定義をきつく締めることによってこれらをスキャン試み単にブロックできます。

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ために、下記の 3 つのメソッドの 1 つを使用して下さい。 3 つのメソッドはすべて 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。 このトラフィックはそれから下記のように廃棄されます。

方式 A: ACLの使用

この方式はマーク付き" Code Red "パケットを廃棄するのにアウトプットインターフェイスの ACL を使用します。 次のネットワークダイアグラムをこの方式のステップを説明するのに使用しよう:

ステップはこの方式の設定にここにあります:

1. 下記に示されているように Cisco IOSソフトウェアのクラスベース マーキング機能が付いている受信 " Code Red "刻み目を、分類して下さい:`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*"` HTTP URL のの中の上記のクラスマップ外観はの特定の文字列一致し。 " Code Red "の default.ida のほかの他のファイル名を含んでいたことに注意して下さい。 同じようなハッキング攻撃を、次に挙げるドキュメントで説明される Sadmindウイルスのようなブロックするこの手法を使用できます :http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS00-078.asphttp://www.sophos.com/virusinfo/analyses/unixsadmind.html
2. ポリシーを構築し、ポリシーマップで受信 " Code Red "刻み目をマークする **set コマンドを**使用して下さい。 この資料は他のどのネットワークトラフィックもこの値を運んでいることはまずないので 1 という DSCP 値を使用します (小数点で) 。ここに「mark-inbound-http-hacks」と指名されるポリシーマップで受信 " Code Red "刻み目をマークします。 `Router(config)#policy-map mark-inbound-http-hacks Router(config-pmap)#class http-hacks Router(config-pmap-c)#set ip dscp 1`
3. 到着" Code Red "パケットをマークするためにインプット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て下さい。`Router(config)#interface serial 0/0 Router(config-if)#service-policy input mark-inbound-http-hacks`
4. 1 という DSCP 値で一致するサービス ポリシーによって ACL を、ように設定 しました設定

して下さい。`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 は NBAR （ CSCdv48172 ）と併用するためのクラスマップの定義の ACL の **log キーワード**のためのサポートを導入します。 以前のリリースを使用している場合、ACL の **log キーワードを**使用しないで下さい。 することはそうすべてのパケットを CEF スイッチの代りにプロセス交換されるために強制し CEF を必要とするので NBAR ははたらきません。

5. ターゲットのWebサーバに接続するアウトプットインターフェイスの ACL 発信を適用して下さい。`Router(config)#interface ethernet 0/1 Router(config-if)#ip access-group 105 out`
6. ソリューションが予想通りはたらくことを確認して下さい。 **show access-list コマンドを**実行し、Deny ステートメントのための" matches " 値が増分していることを確認して下さい。`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)` コンフィギュレーションのステップでは、またルータを余分なリソースを費やすために引き起こすことを避ける **no ip unreachable interface-level コマンド**で IP unreachables メッセージを送信 することをディセーブルにすることができます。この方式は方式 B セクションに記述されているように 0 を無効にするポリシー ルート DSCP=1 トラフィックことができれば推奨されません。

方式 B: ポリシーベース ルーティング (PBR)の使用

この方式はマーク付き" Code Red "パケットをブロックするのにポリシー ベース ルーティングを使用します。 メソッド A か C が既に設定されている場合この方式のコマンドを適用する必要はありません。

ステップはこの方式の設定にここにあります:

1. トラフィックを分類し、それをマークして下さい。 方式 A.で示されている **class-map および policy-map コマンドを**使用して下さい。
2. インプット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到着" Code Red "パケットをマークするために適用する **service-policy コマンドを**使用して下さい。 方式 A.を参照して下さい。
3. マーク付き" Code Red "パケットで一致する拡張 IP ACL を作成して下さい。`Router(config)#access-list 106 permit ip any any dscp 1`
4. ルーティングポリシーを構築する **route-map コマンドを**使用して下さい。`Router(config)#route-map null_policy_route 10 Router(config-route-map)#match ip address 106 Router(config-route-map)#set interface Null0`
5. インプットインターフェイスにルート マップを加えて下さい。`Router(config)#interface serial 0/0 Router(config-if)#ip policy route-map null_policy_route`
6. **show access-list コマンド**をソリューション使用を期待どおりに確認して下さい。 出力 ACL を使用していて、ACLロギングを有効に する場合、また下記に示されているように **show log コマンドを**、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` 各出力 インターフェイスの出力 ACL を作れます必要としますよりもむしろルータの入力 インターフェイスで破棄された決定を。 再度、コマンド **no ip unreachables コマンド**で送信 IP unreachables メッセージをディセーブルにすることを推奨します。

方式 C: クラスベース ポリシングの使用

この方式は一般に PBR か出力 ACL に左右されないので最もスケーラブルです。

1. 方式 A.で示されている **class-map コマンド**を使用してトラフィックを分類して下さい。
2. ポリシーを **policy-map コマンド**を使用して構築し、このトラフィックのためのドロップアクションを規定 する **police コマンドを**使用して下さい。`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. インプット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" Code Red "パケットを廃棄するために適用する **service-policy コマンドを**使用して下さい。
   `Router(config)#`**`interface serial 0/0`** `Router(config-if)#`**`service-policy input drop-inbound-http-hacks`**
4. ソリューションが **show policy-map interface コマンド**を期待どおりに使用することを確認して下さい。 クラスおよび個々の一致条件については値を増分することを見るようにして下さい。`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

NBAR をこの資料でメソッドと使用した場合、次の機能が NBAR によってサポートされないことに注目して下さい:

- 24 同時 URL 以上、ホストまたは MIME 型は一致します
- URL の最初の 400 バイトを越えて一致
- 非IPトラフィック
- マルチキャストおよび他の非 CEF 切り替えモード
- フラグメント化されたパケット
- 導管で送られた耐久性がある HTTP 要求
- セキュア HTTP の URL/HOST/MIME/分類
- ステートフルプロトコルの同期フロー
- から起きるパケットまたは NBAR を実行するルータに予定されて

次の論理インターフェイスの NBAR を設定できません:

- Fast EtherChannel
- トンネリングか暗号化を使用するインターフェイス
- VLAN
- ダイヤラーインターフェイス
- マルチリンク PPP

注: NBAR は Cisco IOS Release 12.1(13)E 現在で VLAN で設定可能、しかしソフトウェア・ スイッチングパスだけでサポートされてです。

NBAR がトンネル伝送するか、または暗号化が使用される WAN リンクのトラフィックを出力するために分類するのに使用することができないので、トラフィックが出力への WAN リンクに切り替えられる前に入力 分類を行うためにルータの他のインターフェイスにそれを、LAN インターフェイスのような、代りに適用して下さい。

より多くの NBAR 情報に関しては、関連情報のリンクを参照して下さい