

ation Recognition and Access Control Lists for Blocking the "C

Table of Contents

<u>Using Network-Based Application Recognition and Access Control Lists for Blocking the</u>	1
<u>Contents</u>	1
<u>Introduction</u>	1
<u>How to Block the "Code Red" Worm</u>	1
<u>Supported Platforms</u>	2
<u>Detect the Infection Attempt in the IIS Web Logs</u>	2
<u>Mark Inbound "Code Red" Hacks Using IOS Class-Based Marking Feature</u>	3
<u>Mark Inbound "Code Red" Hacks Using a Policy Map</u>	4
<u>Block Marked Hack Attempts</u>	4
<u>Block Marked Hack Attempts with an ACL</u>	4
<u>Block Marked Hack Attempts with Policy Based Routing</u>	5
<u>Block Marked Hack Attempts Using a Policing Solution</u>	5
<u>Verify Operation</u>	5
<u>Verify the ACL Solution</u>	5
<u>Verify the Policy Based Routing Solution</u>	5
<u>Verify the Policing Solution</u>	6
<u>NBAR Restrictions</u>	7
<u>Known Issues</u>	7
<u>Related Information</u>	8

Using Network–Based Application Recognition and Access Control Lists for Blocking the

Contents

[Introduction](#)

[How to Block the "Code Red" Worm](#)

[Supported Platforms](#)

[Detect the Infection Attempt in the IIS Web Logs](#)

[Mark Inbound "Code Red" Hacks Using IOS Class–Based Marking Feature](#)

[Mark Inbound "Code Red" Hacks Using a Policy Map](#)

[Block Marked Hack Attempts](#)

[Block Marked Hack Attempts with an ACL](#)

[Block Marked Hack Attempts with Policy Based Routing](#)

[Block Marked Hack Attempts Using a Policing Solution](#)

[Verify Operation](#)

[Verify the ACL Solution](#)

[Verify the Policy Based Routing Solution](#)

[Verify the Policing Solution](#)

[NBAR Restrictions](#)

[Known Issues](#)

[Related Information](#)

Introduction

This advisory provides a method for blocking the "Code Red" worm at network ingress points using Network–Based Application Recognition (NBAR) and Access Control Lists (ACLs) within Cisco IOS® Software on Cisco routers. This solution should be used in conjunction with the recommended patches for IIS servers from Microsoft.

Note: This method does not work on Cisco 1600 series routers.

How to Block the "Code Red" Worm

The first thing you should do to combat "Code Red" is apply the patch available from Microsoft (see links below). This protects vulnerable systems and removes the worm from an infected system. However, applying the patch to your servers only prevents the worm from infecting the servers, it does not stop the HTTP GET requests from hitting the servers. There is still the potential for the server to get bombarded with a flood of infection attempts.

The solution detailed in this advisory is designed to work in conjunction with the Microsoft patch to block the "Code Red" HTTP GET requests at a network ingress point.

This solution attempts to block the infection, however it will not cure problems caused by the buildup of large numbers of cache entries, adjacencies, and NAT/PAT entries, since the only way to analyze the contents of the HTTP GET request is following the establishment of a TCP connection. The following procedure will not help protect against a scan of the network. However, it will protect a site from infestation from an external network or reduce the number of infection attempts that a machine must service. In combination with inbound filtering, outbound filtering prevents infected clients from spreading the "Code Red" worm to the global Internet.

Supported Platforms

The solution described in this document requires the class-based marking feature within IOS. Specifically, the ability to match on any part of an HTTP URL uses the HTTP sub-port classification feature within NBAR. The supported platforms and minimum IOS requirements are summarized below.

Platform	Minimum IOS
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(2)T

Note: You need to enable Cisco Express Forwarding (CEF) in order to use NBAR.

Class-based marking and Distributed NBAR (DNBAR) are also available on the following platforms:

Platform	Minimum IOS
7500	12.1(6)E
FlexWAN	12.1(6)E

Detect the Infection Attempt in the IIS Web Logs

The initial infection attempt sends a large HTTP GET request to the target IIS server. The original "Code Red" footprint is shown below:

```
2001-08-04 16:32:23 24.101.17.216 - 10.1.1.75 80 GET /default.ida
```


Mark Inbound "Code Red" Hacks Using a Policy Map

- Mark inbound "Code Red" hacks with a policy map. We'll use the following network diagram as an example:



Traffic coming in on Ethernet 0/0 is going to be classified and discarded accordingly before being passed to Ethernet 0/1. Once the inbound traffic has been classified as a "Code Red" hack, it can be marked with a specific DSCP. In this case, we chose a decimal value of 1 as it is unlikely that any other traffic will be marked with this DSCP.

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

Apply the service policy to the outside interface so inbound traffic will be marked:

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

Block Marked Hack Attempts

Block marked hack attempts using one of the methods described below.

Block Marked Hack Attempts with an ACL

The ACL should match on the DSCP value of 1 that was marked as the hack attempt entered the router, as shown below:

```
Router(config)#access-list 105 deny ip any any dscp 1 log
Router(config)#access-list 105 permit ip any any
```

Apply it outbound on the inside interface where the target web servers are:

```
Router(config)#interface ethernet 0/1
Router(config-if)#ip access-group 105 out
```

Note: If you are running a moderate to large address space, you will not want to use the log keyword in the access list so as to avoid causing the router to spend excessive resources logging this information. You may also wish to turn off **ip unreachable**. If you are going to use the log keyword, disable **console logging**.

Output access lists are not a recommended solution if you can policy route the DSCP=1 traffic to Null 0 as in the next section.

Block Marked Hack Attempts with Policy Based Routing

The example below shows how to block marked hack attempts using policy based routing:

```
Router(config)#access-list 106 permit ip any any dscp 1
Router(config)#route-map null_policy_route 10
Router(config)#match ip address 106
Router(config)#set interface Null0
Router(config)#interface ethernet 0/0
Router(config-if)#ip policy route-map null_policy_route
```

We are able to make the discard decision at the ingress interface of the router, rather than needing an output ACL on every egress interface. Again, we recommend you disable **ip unreachable**s.

Block Marked Hack Attempts Using a Policing Solution

This final solution is probably the most scalable as it does not depend on either policy based routing or output ACLs.

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

Note: Since you are setting both the conform and exceed action to drop, the rate at which you are policing does not matter.

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

With this solution we can match and drop the traffic without having to resort to ACLs or policy based routing.

Verify Operation

Use one of the procedures below to verify that the procedure is working properly.

Verify the ACL Solution

Use the **show access-list** command, as shown below:

```
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)
```

Verify the Policy Based Routing Solution

Use the **show access-list** and **show log** commands, as shown below:

```
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 pa
Aug 4 13:26:32: %SEC-6-IPACCESSLOGP: list 105 denied tcp A.B.C.D.(0) -> 10.1.1.75(0), 6 pa
```

Note: The **show log** command can be used if you are using output ACLs, and you have logging enabled.

Verify the Policing Solution

Use the **show policy map** command, as shown below:

```
Router#show policy-map interface ethernet 0/0
Ethernet0/0

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

    Class-map: http-hacks (match-any)
      3101 packets, 4292566 bytes
      30 second offered rate 2000 bps, drop rate 0 bps
      Match: protocol http url "*default.ida*"
        3101 packets, 4292566 bytes
        30 second rate 2000 bps
      Match: protocol http url "*cmd.exe*"
        0 packets, 0 bytes
        30 second rate 0 bps
      Match: protocol http url "*root.exe*"
        0 packets, 0 bytes 30 second rate 0 bps
      QoS Set
        ip dscp 1
        Packets marked 3101
```

```
Router#show policy-map interface fastEthernet 0/0
Ethernet0/0
```

```
  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
        30 second rate 0 bps
      Match: protocol http url "*root.exe*"
        0 packets, 0 bytes 30 second 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
        conformed 0 bps, exceed 0 bps violate 0 bps
```

NBAR Restrictions

The NBAR feature does not support the following features:

- More than 24 concurrent URLs, HOSTs or MIME type matches
- Matching beyond the first 400 bytes in a URL
- Non-IP traffic
- Multicast and other non-CEF switching modes
- Fragmented packets
- Pipelined persistent HTTP requests
- URL/HOST/MIME/ classification with secure HTTP
- Asymmetric flows with stateful protocols
- Packets originating from or destined to the router running NBAR

You can't configure NBAR on the following logical interfaces:

- Fast EtherChannel
- Interfaces that use tunneling or encryption
- VLANs
- Dialer interfaces
- Multilink PPP

Note: NBAR cannot be used to classify output traffic on a WAN link where tunneling or encryption is used. Therefore, NBAR should be configured on other interfaces on the router (such as a LAN link) to perform input classification before the traffic is switched to the WAN link for output.

For more NBAR information please see the links in the [Related Information](#) section below.

Known Issues

The "Code Red" worm exploits a vulnerability on unpatched servers within IIS that uses the Microsoft Indexing Service. The Internet Data Administration script file (default.ida) is installed by default on all IIS servers. "Code Red" relies on the presence of this file to carry out the exploit. Most systems do not use this service so the blocking method provided in this advisory will be effective. However, some servers may use this service within IIS. In this case, the blocking method proposed here could block legitimate requests to the IIS server.

Related Information

- [Configuring Network-Based Application Recognition \(NBAR\)](#)
 - [Dealing with mallocfail and High CPU Utilization Resulting From the "Code Red" Worm](#)
 - [Using Cisco Secure IDS/NetRanger Custom String Match Signatures for "Code Red" Worm Remote Buffer Overflow in Microsoft Index Server ISAPI Extension in IIS 4.0 and 5.0](#)
 - [Feature Navigator Tool](#)
 - [Bug Toolkit](#)
-

Home	What's New	How to Buy	Login	Profile	Feedback	Search	Map/Help
----------------------	----------------------------	----------------------------	-----------------------	-------------------------	--------------------------	------------------------	--------------------------

All contents are Copyright © 1992--2001 Cisco Systems Inc. All rights reserved. [Important Notices](#) and [Privacy Statement](#).