如何解决“红色代码”蠕虫引起的 mallocfail 和 CPU 使用率过高的问题

目录

简介

本文档介绍“红色代码”蠕虫以及蠕虫在思科路由环境中可能引起的问题。本文档还介绍防止蠕虫感染的技术，并提供指向相关建议的链接，这些建议描述了蠕虫相关问题的解决方案。

“红色代码”蠕虫利用Microsoft Internet Information Server(IIS)5.0版的索引服务中的漏洞。当“红色代码”蠕虫感染主机时，它会导致主机探测并感染随机的IP地址系列，从而导致网络流量急剧增加。如

果网络中存在冗余链路，且/或思科快速转发(CEF)不用于交换数据包，则此问题尤其严重。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文件规则的更多信息请参见“ Cisco技术提示规则”。

“红色代码”蠕虫如何感染其他系统

"""Code Red""蠕虫试图连接到随机生成的IP地址。"每个受感染的IIS服务器都可能尝试感染同一组设备。可以跟踪蠕虫的源IP地址和TCP端口，因为它不是欺骗的。单播反向路径转发(URPF)无法抑制蠕虫攻击，因为源地址合法。

有关“红色代码”蠕虫的建议

以下建议描述“红色代码”蠕虫，并说明如何修补受该蠕虫影响的软件：

- Cisco安全建议:“红色代码”蠕虫 — 客户影响
- 远程IIS索引服务器ISAPI扩展缓冲区溢出
- .ida "红色代码"蠕虫
- CERT?建议CA-2001-19 “红色代码”蠕虫利用IIS索引服务DLL中的缓冲区溢出

症状

以下是指示思科路由器受“红色代码”蠕虫影响的一些症状：

- NAT或PAT表中的大量流（如果使用NAT或PAT）。
- 网络中大量ARP请求或ARP风暴（由IP地址扫描引起）。
- IP输入、ARP输入、IP Cache Ager和CEF处理过程使用过多内存。
- ARP、IP输入、CEF和IPC中CPU利用率过高。
- 如果使用NAT，则中断级别CPU利用率高，流量速率低，或IP输入进程级别CPU利用率高。

内存低或中断级别持续高CPU利用率(100%)可能导致Cisco IOS®路由器重新加载。重新加载是由于应力条件导致进程行为错误引起的。

如果您不怀疑站点中的设备受到“红色代码”蠕虫的感染或是该蠕虫的目标，请参阅相关信息部分，了解有关如何排除您遇到的任何问题的其他URL。

识别受感染的设备

使用流交换确定受影响设备的源IP地址。在所有接口上配置ip route-cache flow，记录路由器交换的所有数据流。

几分钟后，发出show ip cache flow命令查看记录的条目。在“红色代码”蠕虫感染的初始阶段，蠕虫会尝试自我复制。当蠕虫向随机IP地址发送HT请求时，会发生复制。因此，您必须查找目标端口为80（HT，十六进制为0050）的缓存流条目。

show **ip cache flow | include 0050**命令显示TCP端口80（十六进制0050）的所有缓存条目：

```
Router#show ip cache flow | include 0050
...

scram        scrappers    dative      DstIPaddress   Pr SrcP  DstP  Pkts
Vl1       193.23.45.35      Vl3        2.34.56.12    06 0F9F  0050     2
Vl1    211.101.189.208     Null     158.36.179.59    06 0457  0050     1
Vl1       193.23.45.35      Vl3     34.56.233.233    06 3000  0050     1
Vl1     61.146.138.212     Null     158.36.175.45    06 B301  0050     1
Vl1       193.23.45.35      Vl3     98.64.167.174    06 0EED  0050     1
Vl1     202.96.242.110     Null     158.36.171.82    06 0E71  0050     1
Vl1       193.23.45.35      Vl3     123.231.23.45    06 121F  0050     1
Vl1       193.23.45.35      Vl3       9.54.33.121    06 1000  0050     1
Vl1       193.23.45.35      Vl3      78.124.65.32    06 09B6  0050     1
Vl1      24.180.26.253     Null    158.36.179.166    06 1132  0050     1
```

如果发现具有相同源IP地址、随机目标IP地址[1]、DstP = 0050(HTTP)和Pr = 06(TCP)的条目数量异常高，则可能已找到受感染的设备。在本输出示例中，源IP地址为193.23.45.35，来自VLAN1。

[1] 另一个版本的“红色代码”蠕虫（称为“红色代码II”）不会选择完全随机的目的IP地址。相反，“红色代码II”保留IP地址的网络部分，并选择IP地址的随机主机部分以便传播。通过这种方式，它可以在同一网络范围内更快地传播。

“红色代码II”使用以下网络和掩码：

```
Mask          Probability of Infection
0.0.0.0         12.5% (random)
255.0.0.0       50.0% (same class A)
255.255.0.0     37.5% (same class B)
```

排除的目标IP地址是127.X.X.X和224.X.X.X，不允许使用0或255的二进制八位数。此外，主机不会尝试重新感染自己。

有关详细信息，请参阅红色代码(II)。

有时，您无法运行netflow来检测“红色代码”感染尝试。这可能是因为您运行的代码版本不支持netflow，或者路由器的内存不足或过分碎片，无法启用netflow。思科建议在路由器上有多个入口接口且只有一个出口接口时不要启用netflow，因为netflow记帐在入口路径上执行。在这种情况下，最好在独立的出口接口上启用IP记帐功能。

注意：ip accounting命令禁用DCEF。请勿在要使用DCEF交换的任何平台上启用IP记帐。

```
Router(config)#interface vlan 1000
Router(config-if)#ip accounting

Router#show ip accounting
  Source           Destination           Packets               Bytes
20.1.145.49      75.246.253.88             2                    96
20.1.145.43      17.152.178.57             1                    48
20.1.145.49      20.1.49.132               1                    48
20.1.104.194     169.187.190.170           2                    96
20.1.196.207     20.1.1.11                 3                   213
20.1.145.43      43.129.220.118            1                    48
20.1.25.73       43.209.226.231            1                    48
20.1.104.194     169.45.103.230            2                    96
20.1.25.73       223.179.8.154             2                    96
20.1.104.194     169.85.92.164             2                    96
20.1.81.88       20.1.1.11                 3                   204
20.1.104.194     169.252.106.60            2                    96
20.1.145.43      126.60.86.19              2                    96
20.1.145.49      43.134.116.199            2                    96
20.1.104.194     169.234.36.102            2                    96
20.1.145.49      15.159.146.29             2                    96
```

在show ip accounting命令输出中，查找尝试将数据包发送到多个目标地址的源地址。如果受感染的主机处于扫描阶段，它会尝试建立到其他路由器的HTTP连接。因此，您将看到尝试访问多个IP地址。这些连接尝试大多数通常失败。因此，您只看到传输的少量数据包，每个数据包的字节计数较小。在本例中，20.1.145.49和20.1.104.194可能已感染。

在Catalyst 5000系列和Catalyst 6000系列上运行多层交换(MLS)时，必须采取不同步骤来启用网络流记帐并跟踪感染。在配备Supervisor 1多层交换功能卡(MSFC1)或SUP I/MSFC2的Cat6000交换机中，默认情况下启用基于NetFlow的MLS，但流模式仅用于目的。因此，源IP地址不会缓存。在Supervisor上使用set mls flow full命令，可以启用“full-flow”模式来跟踪受感染的主机。

对于混合模式，请使用**set mls flow full**命令：

```
6500-sup(enable)set mls flow full
Configured IP flowmask is set to full flow.
Warning: Configuring more specific flow mask may dramatically
increase the number of MLS entries.
```

对于本地IOS模式，请使用mls flow ip full命令：

```
Router(config)#mls flow ip full
```

启用“全流”模式时，系统会显示警告，指示MLS条目显着增加。如果您的网络已经感染了“红色代码”蠕虫，增加的MLS条目的影响是可以在短时间内得到证实的。蠕虫会导致MLS条目过多且呈上升趋势。

要查看收集的信息，请使用以下命令：

对于混合模式，请使用**set mls flow full**命令：

```
6500-sup(enable)set mls flow full
Configured IP flowmask is set to full flow.
Warning: Configuring more specific flow mask may dramatically
increase the number of MLS entries.
```

对于本地IOS模式，请使用**mls flow ip full命**令：

```
Router(config)#mls flow ip full
```

启用“全流”模式时，系统会显示警告，指示MLS条目显着增加。如果您的网络已经感染了“红色代码”蠕虫，增加的MLS条目的影响是可以在短时间内得到证实的。蠕虫会导致MLS条目过多且呈上升趋势。

要查看收集的信息，请使用以下命令：

对于混合模式，请使用[show mls ent命](#)令：

```
6500-sup(enable)show mls ent
Destination-IP  Source-IP     Prot  DstPrt SrcPrt Destination-Mac   Vlan EDst
ESrc DPort     SPort     Stat-Pkts  Stat-Bytes  Uptime   Age
-------------- --------------- ----- ------ ------ ----------------- ---- ----
---- --------- --------- ---------- ----------- -------- --------
```

注意：当这些字段处于“全流”模式时，将填入这些字段。

对于本地IOS模式，请使用**show mls ip命**令：

```
Router#show mls ip
DstIP           SrcIP           Prot:SrcPort:DstPort  Dst i/f:DstMAC
---------------------------------------------------------------------
Pkts         Bytes       SrcDstPorts    SrcDstEncap Age   LastSeen
---------------------------------------------------------------------
```

当您确定攻击涉及的源IP地址和目标端口时，可以将MLS设置回“仅目标”模式。

对于混合模式，请使[用set mls flow destination命](#)令：

```
6500-sup(enable) set mls flow destination
Usage: set mls flow <destination|destination-source|full>
```

对于本地IOS模式，请使[用mls flow](#) **ip destination**命令：

```
Router(config)#mls flow ip destination
```

Supervisor(SUP)II/MSFC2组合可防止攻击，因为CEF交换在硬件中执行，并且网络流统计信息得到维护。因此，即使在“红色代码”攻击中，如果启用全流模式，由于交换机速度更快，路由器也不会被淹没。在SUP I/MFSC1和SUP II/MSFC2上，用于启用全流模式和显示统计信息的命令相同。

[预防技术](#)

使用本节中列出的技术，将“红色代码”蠕虫对路由器的影响降至最低。

[阻止到端口80的流量](#)

如果它在您的网络中可行，防止“红色代码”攻击的最简单方法是阻止所有流向端口80的流量，端口80是WWW的公认端口。构建访问列表以拒绝发往端口80的IP数据包，并将其应用于面对感染源的

接口的入站流量。

减少ARP输入内存的使用

当静态路由指向广播接口时，ARP输入会耗用大量内存，如下所示：

```
ip route 0.0.0.0 0.0.0.0 Vlan3
```

默认路由的每个数据包都会发送到VLAN3。但是，没有指定下一跳IP地址，因此路由器会发送目的IP地址的ARP请求。除非禁用代理ARP，否则该目标的下一跳路由器会使用其自己的MAC地址进行应答。来自路由器的应答在ARP表中创建一个附加条目，数据包的目的IP地址将映射到下一跳MAC地址。“红色代码”蠕虫将数据包发送到随机IP地址，这会为每个随机目标地址添加一个新的ARP条目。每个新ARP条目在ARP输入过程中消耗的内存越来越多。

请勿创建到接口的静态默认路由，尤其是当接口是广播（以太网/快速以太网/GE/SMDS）或多点（帧中继/ATM）时。 任何静态默认路由都必须指向下一跳路由器的IP地址。在您更改了指向下一跳IP地址的默认路由之后，请使用clear arp-cache命令，以清除所有ARP条目。此命令可解决内存使用问题。

使用思科快速转发(CEF)交换

为了降低IOS路由器的CPU利用率，请从Fast/Optimum/Netflow交换更改为CEF交换。启用CEF需要注意几点。下一节讨论CEF和快速交换之间的区别，并说明启用CEF时的含义。

Cisco 快速转发对快速交换

启用CEF以减轻“红色代码”蠕虫导致的流量负载增加。Cisco IOS®软件版本11.1()CC、12.0及更高版本在Cisco 7200/7500/GSR平台上支持CEF。在Cisco IOS软件版本12.0或更高版本中提供对其他平台上CEF的支持。可以使用“软件顾问”工具进一步调查。

有时，由于以下原因之一，您无法在所有路由器上启用CEF:

- 内存不足
- 平台结构不受支持
- 接口封装不受支持

快速交换行为及其意义

以下是使用快速交换时的影响：

- 流量驱动缓存 — 在路由器交换数据包并填充缓存之前，缓存为空。
- 第一个数据包是进程交换的 — 第一个数据包是进程交换的，因为缓存最初是空的。
- 精细缓存 — 缓存是在主网中最具体的路由信息库(RIB)条目部分的粒度构建的。如果RIB对主网131.108.0.0具有/24s，则此主网的缓存是使用/24s构建的。
- /32缓存用于 — /32缓存用于平衡每个目标的负载。当缓存平衡负载时，该主网的缓存使用/32s构建。**注意：**最后两个问题可能导致占用所有内存的大型缓存。
- 在主网边界缓存 — 使用默认路由，在主网边界执行缓存。
- 缓存管理器 — 缓存器管理器每分钟运行一次，在正常内存条件下检查缓存的1/20(5%)的未使用条目，在低内存条件(200k)下检查缓存的1/4(25%)。

要更改上述值，请使用**ip cache-ager-interval X Y Z**命令，其中：

- X是ager运行之间的秒数<0-2147483>。默认值为60秒。
- Y是每次运行时缓存的<2-50> 1/(Y+1)到老化时间（低内存）。 默认值为4。
- Z是每次运行时缓存的<3-100> 1/(Z+1)到老化时间（正常）。 默认值为20。

以下是使用**ip cache-ager 60 5 25**的示例配置。

```
Router#show ip cache
IP routing cache 2 entries, 332 bytes
   27 adds, 25 invalidates, 0 refcounts
Cache aged by 1/25 every 60 seconds (1/5 when memory is low).
Minimum invalidation interval 2 seconds, maximum interval 5 seconds,
quiet interval 3 seconds, threshold 0 requests
Invalidation rate 0 in last second, 0 in last 3 seconds
Last full cache invalidation occurred 03:55:12 ago

Prefix/Length          Age    Interface     Next Hop
4.4.4.1/32        03:44:53    Serial1       4.4.4.1
192.168.9.0/24    00:03:15    Ethernet1    20.4.4.1

Router#show ip cache verbose
IP routing cache 2 entries, 332 bytes
   27 adds, 25 invalidates, 0 refcounts
Cache aged by 1/25 every 60 seconds (1/5 when memory is low).
Minimum invalidation interval 2 seconds, maximum interval 5 seconds,
   quiet interval 3 seconds, threshold 0 requests
Invalidation rate 0 in last second, 0 in last 3 seconds
Last full cache invalidation occurred 03:57:31 ago
Prefix/Length       Age       Interface       Next Hop
4.4.4.1/32-24           03:47:13  Serial1         4.4.4.1
                    4   0F000800
192.168.9.0/24-0        00:05:35  Ethernet1       20.4.4.1
                    14  00000C34A7FC00000C13DBA90800
```

根据缓存器的设置，缓存条目中的某些百分比会过期，超出快速缓存表。当条目快速老化时，快速缓存表老化的百分比越大，缓存表就越小。因此，路由器的内存消耗会减少。缺点是，老化的条目在缓存表中继续传输流量。初始数据包是进程交换的，这会导致IP输入中CPU消耗的**短峰**值，直到为流构建新的缓存条目。

从Cisco IOS软件版本10.3(8)、11.0(3)及更高版本中，IP缓存器的处理方式不同，如下所述：

- **ip cache-ager-interval**和**ip cache-invalidate-delay**命令仅在配置中定义了service internal命令时才可用。
- 如果在老化无效运行之间的周期设置为0，那么这个老化进程则被完全禁用。
- 时间单位是秒。

注意：当您执行这些命令时，路由器的CPU利用率会增加。仅在绝对必要时使用这些命令。

```
Router#clear ip cache ?
A.B.C.D Address prefix
<CR>--> will clear the entire cache and free the memory used by it!

Router#debug ip cache
IP cache debugging is on
```

CEF的优势

- 转发信息库(FIB)表基于路由表构建。因此，在转发第一个数据包之前，会存在转发信息。FIB还包含与直接相连LAN主机相关的/32条目。
- 邻接(ADJ)表包含下一跳和直连主机的第2层重写信息（ARP条目创建CEF邻接）。
- CEF中不存在使CPU利用率突增的缓存器老化器这一概念。若删除某个路由表条目，则同时会删除FIB条目。

注意：同样，指向广播或多点接口的默认路由意味着路由器会为每个新目标发送ARP请求。来自路由器的ARP请求可能会创建一个巨大的邻接表，直到路由器内存不足。如果CEF无法分配内存，CEF/DCEF会禁用自身。您需要再次手动启用CEF/DCEF。

输出示例：CEF

以下是show ip cef summary命令的一些输出示例，显示内存使用情况。此输出是来自Cisco 7200路由服务器的快照，Cisco IOS软件版本12.0。

```
Router>show ip cef summary
IP CEF with switching (Table Version 2620746)
  109212 routes, 0 reresolve, 0 unresolved (0 old, 0 new), peak 84625
  109212 leaves, 8000 nodes, 22299136 bytes, 2620745 inserts, 2511533
  invalidations
  17 load sharing elements, 5712 bytes, 109202 references
  universal per-destination load sharing algorithm, id 6886D006
  1 CEF resets, 1 revisions of existing leaves
  1 in-place/0 aborted modifications
  Resolution Timer: Exponential (currently 1s, peak 16s)
  refcounts:  2258679 leaf, 2048256 node

Adjacency Table has 16 adjacencies


Router>show processes memory | include CEF
 PID TTY  Allocated      Freed    Holding    Getbufs    Retbufs Process
  73   0     147300       1700     146708          0          0 CEF process
  84   0        608          0       7404          0          0 CEF Scanner


Router>show processes memory | include BGP

   2   0    6891444    6891444       6864          0          0 BGP Open
  80   0       3444       2296       8028          0          0 BGP Open
  86   0     477568     476420       7944          0          0 BGP Open
  87   0 2969013892  102734200  338145696          0          0 BGP Router
  88   0   56693560 2517286276       7440     131160    4954624 BGP I/O
  89   0      69280   68633812      75308          0          0 BGP Scanner
  91   0    6564264    6564264       6876          0          0 BGP Open
 101   0    7635944    7633052       6796        780          0 BGP Open
 104   0    7591724    7591724       6796          0          0 BGP Open
 105   0    7269732    7266840       6796        780          0 BGP Open
 109   0    7600908    7600908       6796          0          0 BGP Open
 110   0    7268584    7265692       6796        780          0 BGP Open


Router>show memory summary | include FIB

Alloc PC        Size     Blocks      Bytes    What
0x60B8821C       448          7       3136    FIB: FIBIDB
0x60B88610     12000          1      12000    FIB: HWIDB MAP TABLE
0x60B88780       472          6       2832    FIB: FIBHWIDB
0x60B88780       508          1        508    FIB: FIBHWIDB
```

```
0x60B8CF9C       1904          1       1904    FIB 1 path chunk pool
0x60B8CF9C      65540          1      65540    FIB 1 path chunk pool
0x60BAC004       1904        252     479808    FIB 1 path chun
0x60BAC004      65540        252   16516080    FIB 1 path chun
```

```
Router>show memory summary | include CEF

0x60B8CD84       4884          1       4884    CEF traffic info
0x60B8CF7C         44          1         44    CEF process
0x60B9D12C      14084          1      14084    CEF arp throttle chunk
0x60B9D158        828          1        828    CEF loadinfo chunk
0x60B9D158      65540          1      65540    CEF loadinfo chunk
0x60B9D180        128          1        128    CEF walker chunk
0x60B9D180        368          1        368    CEF walker chunk
0x60BA139C         24          5        120    CEF process
0x60BA139C         40          1         40    CEF process
0x60BA13A8         24          4         96    CEF process
0x60BA13A8         40          1         40    CEF process
0x60BA13A8         72          1         72    CEF process
0x60BA245C         80          1         80    CEF process
0x60BA2468         60          1         60    CEF process
0x60BA65A8      65488          1      65488    CEF up event chunk
```

```
Router>show memory summary | include adj

0x60B9F6C0        280          1        280    NULL adjacency
0x60B9F734        280          1        280    PUNT adjacency
0x60B9F7A4        280          1        280    DROP adjacency
0x60B9F814        280          1        280    Glean adjacency
0x60B9F884        280          1        280    Discard adjacency
0x60B9F9F8      65488          1      65488    Protocol adjacency chunk
```

注意事项

当流数量较大时，CEF通常比快速交换消耗的内存更少。如果快速交换缓存已消耗内存，则必须先清除ARP缓存(通过**clear ip arp**命令)，然后才能启用CEF。

注意：清除缓存时，路由器的CPU使用率会出现峰值。

"红色代码"常见问题及解答

问：我使用NAT，在IP输入中体验100%的CPU利用率。当我执行show proc cpu时，我的CPU利用率在中断级别为100/99或99/98。这是否与"红色代码"相关？

答：最近修复了NAT Cisco漏洞(CSCdu63623(仅注册客户))，涉及可扩展性。当有数万个NAT流（基于平台类型）时，该漏洞会在进程或中断级别导致100%的CPU利用率。

要确定此错误是否是原因，请发出**show align**命令，并验证路由器是否遇到对齐错误。如果您确实看到校准错误或虚假内存访问，请发出**show align**命令几次，并查看错误是否上升。如果错误数增加，则调整错误可能是中断级别CPU使用率较高的原因，而不是Cisco Bug CSCdu63623(仅限注册客户)。 有关详细信息，请参阅排除欺骗访问和校准错误。

show ip nat translation命令可显示活动转换的数量。NPE-300类处理器的熔毁点约为20,000到40,000个转换。此数字因平台而异。

此熔毁问题之前曾由几位客户观察到，但在“红色代码”之后，有更多客户遇到过此问题。唯一的解决方法是运行NAT（而非PAT），以便减少活动转换。如果有7200，请使用NSE-1并降低NAT超时值。

问：我运行IRB，在HyBridge输入进程中遇到CPU使用率较高的情况。为什么会发生这种情况？是否与“红色代码”相关？

A. HyBridge输入进程处理IRB进程无法快速交换的任何数据包。IRB进程无法快速交换数据包的原因可能是：

- 数据包是广播数据包。
- 数据包是组播数据包。
- 目标未知，需要触发ARP。
- 有生成树BPDU。

如果同一网桥组中有数千个点对点接口，HyBridge输入会遇到问题。如果同一多点接口中有数千个VS，HyBridge输入也会遇到问题（但程度较轻）。

IRB问题的可能原因是什么？假设受“红色代码”感染的设备扫描IP地址。

- 路由器需要为每个目的IP地址发送ARP请求。网桥组中每条虚电路上都会针对扫描的每个地址产生大量ARP请求。正常的ARP进程不会导致CPU问题。但是，如果有没有网桥条目的ARP条目，路由器会泛洪发往已存在ARP条目的地址的数据包。因为数据流是由程序交换的，所以可能会导致高CPU利用率。为避免此问题，请增加网桥老化时间（默认为300秒或5分钟）以匹配或超过ARP超时（默认为4小时），以便同步两个计时器。
- 终端主机尝试感染的地址是广播地址。路由器进行等同于子网广播的工作，这种工作需要HyBridge输入程序重复。如果配置了no ip directed-broadcast**命令，则不**会发生这种情况。在Cisco IOS软件版本12.0中，**ip directed-broadcast**命令默认为禁用，这会导致所有IP定向广播被丢弃。
- 以下是与“红色代码”无关的附注，与IRB架构相关：需要复制第2层组播和广播数据包。因此，在广播网段上运行的IPX服务器出现问题会导致链路断开。您可通过用户策略来避免这种问题。有关详细信息，请参阅x数字用户线(xDSL)网桥支持。您还必须考虑网桥访问列表，该列表限制允许通过路由器的流量类型。
- 为了缓解此IRB问题，您可以使用多个网桥组，并确保BVI、子接口和VC存在一对一映射。
- 因为RBE完全避免了桥接堆栈，所以要优于IRB。您可以从IRB迁移到RBE。这些思科漏洞激发了此类迁移：CSCdr11146(仅限注册客户)CSCdp18572(仅限注册客户)CSCds40806(仅限注册客户)

问：我的CPU使用率在中断级别较高，如果我尝试显示日志，我会收到刷新。流量速率也只比正常情况稍高。此问题的原因是什么？

A.以下是show logging命令输**出的**示例：

```
Router#show logging
     Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
                                                ^
                                              this value is non-zero
         Console logging: level debugging, 9 messages logged
```

检查您是否登录到控制台。如果是，请检查是否存在流量HTTP请求。接下来，检查是否存在任何

带有log关键字或调试的访问列表，以观察特定IP流。如果刷新数量增加，可能是因为控制台（通常为9600波特设备）无法处理收到的信息量。在这种情况下，路由器会禁用中断，并只处理控制台消息。解决方案是禁用控制台日志记录或删除您执行的任何类型的日志记录。

问：我可以在运行ip http-server的IOS路由器上看到许多HTTP连接尝试。这是因为“红色代码”蠕虫扫描吗？

A."红色代码"可能是原因。Cisco建议您在IOS路由器上禁用**ip http server**命令，以便它无需处理来自受感染主机的多次连接尝试。

解决方法

有关“红色代码”，蠕虫的建议 章节介绍了各种临时解决方法。有关解决方法，请参阅建议。

在网络入口点阻止“红色代码”蠕虫的另一种方法是在思科路由器的IOS软件中使用基于网络的应用识别(NBAR)和访问控制列表(ACL)。将此方法与推荐的Microsoft IIS服务器修补程序结合使用。有关此方法的详细信息，请参阅在网络入口点使用NBAR和ACL阻止“红色代码”蠕虫。

相关信息

- **排除内存问题**
- **缓冲泄漏故障排除**
- **对 Cisco 路由器上的 CPU 使用率过高进行故障排除**
- **路由器崩溃故障排除**
- **技术说明故障排除 — 路由器**
- **排除路由器故障**
- **技术支持和文档 - Cisco Systems**