

使用基于网络的应用识别和 ACL 阻拦“红色代码”蠕虫

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[如何阻拦“红色代码”蠕虫](#)

[支持的平台](#)

[通过 IIS Web 日志检测感染攻击](#)

[使用 IOS 基于类的标记功能对入站“红色代码”黑客进行标记](#)

[方法 A：使用 ACL](#)

[方法 B：使用基于策略的路由 \(PBR\)](#)

[方法 C：使用基于类的策略](#)

[NBAR 限制](#)

[已知问题](#)

[相关信息](#)

简介

本文档提供了在网络入口点阻止“红色代码”蠕虫的一种方法，即通过 Cisco 路由器上 Cisco IOS 软件内的基于网络的应用程序识别 (NBAR) 和访问控制列表 (ACL)。本解决方案应与推荐的 Microsoft IIS 服务器修补程序一起使用。

注意：此方法不适用于 Cisco 1600 系列路由器。

注意：某些 P2P 流量因其 P2P 协议特性而无法完全阻止。这些 P2P 协议动态地更改他们的签名绕过尝试所有 DPI 的引擎完全阻塞他们的流量。所以，推荐限制带宽而不是完全阻塞他们。节流此流量的带宽。给较少带宽;然而，请让连接经历。

先决条件

要求

Cisco 建议您了解以下主题：

- 使用[模块化 QoS 命令行界面 \(CLI\)](#) 命令的服务质量 (QoS) 服务策略。
- NBAR
- ACL

- 基于策略的路由

使用的组件

本文档不限于特定的软件和硬件版本。本文档中的配置已在运行 Cisco IOS 版本 12.2(24a) 的 Cisco 3640 上经过测试。

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

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

如何阻拦“红色代码”蠕虫

要抵御“红色代码”，首先应使用 Microsoft 的可用修补程序（请参见下文[方法 A：使用 ACL](#) 部分的链接）。这可以保护易受攻击的系统并从已感染的系统中删除蠕虫。但是，在服务器上应用修补程序只能防止蠕虫感染服务器，而无法防止 HTTP GET 请求攻击服务器。服务器仍有可能遭受大规模感染攻击。

此建议中详细说明了的解决方案旨在与 Microsoft 修补程序协同工作，在网络入口点阻拦“红色代码”HTTP GET 请求。

此解决方案试图对感染进行阻拦，但无法彻底解决由于大量缓存条目、邻接和 NAT/PAT 条目累积而导致的问题，这是因为分析 HTTP GET 请求内容的唯一方法是跟踪 TCP 连接的建立过程。以下过程无法防范网络扫描。但它保护站点免受外部网络的群攻，或减少计算机必须为其提供服务的感染攻击数目。出站过滤与入站过滤结合起来可以防止受感染的客户机将“红色代码”蠕虫传播到全球 Internet。

支持的平台

本文档所述的解决方案要求使用 Cisco IOS 软件内部基于类的标记功能。具体来说，为能够对 HTTP URL 的任何部分进行检查匹配，需要使用 NBAR 内部的 HTTP 子端口分类功能。支持的平台和最低 Cisco IOS 软件要求汇总如下：

| 平台 | 最低 Cisco IOS 软件要求 |
|------|-------------------|
| 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 |

注意：需要启用 Cisco 快速转发 (CEF) 才能使用 NBAR。

以下平台也提供基于类的标记功能和分布式 NBAR (DNBAR)：

| 平台 | 最低 Cisco IOS 软件要求 |
|---------|-------------------|
| 7500 | 12.1(6)E |
| FlexWan | 12.1(6)E |

通过 IIS Web 日志检测感染攻击

初始感染攻击会向目标 IIS 服务器发送大量 HTTP GET 请求。第一代“红色代码”的攻击痕迹如下所示：

```
2001-08-04 16:32:23 10.101.17.216 - 10.1.1.75 80 GET /default.ida
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNN%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
```

“红色代码”II 的攻击痕迹如下所示：

```
2001-08-04 15:57:35 10.7.35.92 - 10.1.1.75 80 GET /default.ida XXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX%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 -
```

请注意，GET 请求总是查找扩展名为 .ida 的文件。这是所有感染攻击的通用字符串，因此可用作 IOS 中基于类标记的匹配条件。GET 请求的剩余部分不一定会持续，因为它只是为了引起缓冲溢出。比较上面两个条目即可看出这一点。

据目前报道，造成这两个签名不同的原因是由于“红色代码”蠕虫的新变种，别名 CodeRed.v3 或 CodeRed.C。在 GET 请求中，第一代“红色代码”变种包括“NNNNNNNN”字符串，而新变种包括“XXXXXXXX”。有关详细信息，请参阅 [Symantec 建议](#)。

东部夏令时间 2001 年 8 月 6 日下午 6:24，我们记录了一个新的攻击痕迹。此后我们才意识到，这是 [eEye 漏洞扫描工具](#) 所遗漏的攻击痕迹。

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

如下一部分所示，通过加强类映射定义，本建议中所提供的“红色代码”阻拦方法还可阻拦扫描攻击。

使用 IOS 基于类的标记功能对入站“红色代码”黑客进行标记

要阻拦“红色代码”蠕虫，请使用下述三种方法之一。三种方法都使用 Cisco IOS MQC 功能对恶意数据流进行分类。然后，会按下述方法将此类数据流丢弃。

方法 A：使用 ACL

此方法使用输出接口上的 ACL 将标记为“红色代码”的数据包丢弃。使用以下网络图可说明此方法的步骤：



配置此方法的步骤如下：

1. 使用 Cisco IOS 软件基于类的标记功能对入站“红色代码”黑客进行分类，如下所示

```
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*"
```

上述类映射会仔细检查 HTTP URL，并对所有指定字符串进行检查匹配。请注意，除了“红色代码”default.ida 之外，我们还包括了其他文件名。使用此方法可以阻拦类似的黑客攻击，例如以下文档中所描述的 Sadmin 病毒。

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS00-078.asp><http://www.sophos.com/virusinfo/analyses/unixsadmin.html>

2. 建立策略并用 **set** 命令以使用策略映射标记入站“红色代码”黑客。本文档使用的 DSCP 值为 1 (十进制)，这是因为其他任何网络数据流都不大可能携带此值。这里，我们用名为“mark-inbound-http-hacks”的策略映射来标记入站“红色代码”黑客。Router(config)#policy-map mark-inbound-http-hacks

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

3. 将该策略作为入站策略应用到输入接口上，以标记到达的“红色代码”数据包。

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

4. 按照服务策略所设置的，配置一个 ACL，使其与 DSCP 值 1 相匹配。Router(config)#access-list 105 deny ip any any dscp 1

```
Router(config)#access-list 105 permit ip any any
```

注意： Cisco IOS 软件版本 12.2(11) 和 12.2(11)T 在类映射定义中引入了对 ACL 中 **log** 关键字的支持，以使其与 NBAR (CSCdv48172) 配合使用。如果使用早期版本，请勿在 ACL 中使用 **log** 关键字。这样做会迫使所有数据包都进行进程交换，而不是 CEF 交换，从而导致 NBAR 不工作，因为它需要 CEF。

5. 在与目标 Web 服务器相连的输出接口上应用出站 ACL。Router(config)#interface ethernet 0/1

```
Router(config-if)#ip access-group 105 out
```

6. 验证解决方案能否如预期运作。执行 **show access-list** 命令，确保与拒绝语句相匹配的值不断增加。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)
```

也可以在配置步骤中使用 **no ip unreachable** 接口级别命令禁止发送无法到达目标 IP 的消息，以避免路由器消耗过多资源。如果能够如“方法 B”部分所述，将 DSCP=1 的数据流策略路由至 NULL 0，则不建议使用此方法。

方法 B：使用基于策略的路由 (PBR)

此方法使用基于策略的路由对标记为“红色代码”的数据包进行阻拦。如果已配置了方法 A 或 C，则无需应用此方法中的命令。

实施此方法的步骤如下：



1. 对数据流进行分类和标记。使用方法 A 中所示的 **class-map** 和 **policy-map** 命令。
2. 使用 **service-policy** 命令将此策略作为入站策略应用到输入接口上，以标记到达的“红色代码”数据包。请参阅方法 A。
3. 创建一个扩展 IP ACL，使其与标记为“红色代码”的数据包相匹配。Router(config)#**access-list 106 permit ip any any dscp 1**
4. 使用 **route-map** 命令建立路由策略。Router(config)#**route-map null_policy_route 10**
Router(config-route-map)#**match ip address 106**
Router(config-route-map)#**set interface Null0**
5. 将路由映射应用到输入接口。Router(config)#**interface serial 0/0**
Router(config-if)#**ip policy route-map null_policy_route**
6. 使用 **show access-list** 命令验证解决方案能否如预期运作。如果使用输出 ACL 并启用了 ACL 日志记录，则也可以使用 **show log** 命令，如下所示：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
```

可以在路由器的输入接口上做出丢弃决策，而无需使每个输出接口都有一个输出 ACL。再次建议您使用 **no ip unreachable** 命令禁止发送无法到达目标 IP 的消息。

方法 C：使用基于类的策略

通常情况下，此方法最具扩展性，因为它不需依靠 PBR 或输出 ACL。

1. 使用方法 A 中所示的 **class-map** 命令对数据流进行分类。
2. 使用 **policy-map** 命令建立策略，并使用 **police** 命令为该数据流指定丢弃操作。
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. 使用 **service-policy** 命令将此策略作为入站策略应用到输入接口上，以丢弃“红色代码”数据包。
Router(config)#**interface serial 0/0**
Router(config-if)#**service-policy input drop-inbound-http-hacks**
4. 使用 **show policy-map interface** 命令验证解决方案能否如预期运作。确保类别及单个匹配条件不断增加。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 限制

按照本文档中的方法使用 NBAR 时，请注意 NBAR 不支持以下功能：

- 对超过 24 个并发 URL、HOST 或 MIME 类型进行检查匹配
- 对 URL 前 400 及更多个字节进行检查匹配
- 非 IP 数据流
- 多播和其他非 CEF 交换模式
- 分段的数据包
- 通过管道传输的持续 HTTP 请求
- 安全 HTTP 的 URL/HOST/MIME/ 分类
- 使用状态协议的非对称流
- 运行 NBAR 的路由器发送或接收的数据包

您不能在以下逻辑接口上配置 NBAR：

- Fast EtherChannel
- 使用隧道或加密的接口
- VLAN
- 拨号接口
- 多链路 PPP

注意：从 Cisco IOS 版本 12.1(13)E 起可在 VLAN 上配置 NBAR，但仅在软件交换路径中支持。

由于无法使用 NBAR 对使用了隧道或加密的 WAN 链路上的输出数据流进行分类，因此请将其应用于路由器上的其他接口（例如 LAN 接口），这样便可在数据流交换到 WAN 链路进行输出之前执行输入分类。

关于更多 NBAR 信息，请参阅在[相关信息的](#)链路