使用基于网络的应用程序识别和ACL阻拦的" Code Red "蠕虫

目录

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： 若干P2P数据流不可以完全地封锁的归结于其P2P协议的本质。这些P2P协议动态地更改他们的签名绕过设法所有DPI的引擎完全地阻塞他们的数据流。所以，推荐限制带宽而不是完全阻拦他们。节流此数据流的带宽。产生较少带宽;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。然而，适用于补丁程序您的服务器只防止蠕虫传染服务器，它从按下服务器不终止HTTP GET请求。仍有在服务器的可能性被轰击与一群感染企图。

在此建议选派的解决方案设计与Microsoft补丁程序一道工作拒绝" Code Red " HTTP GET请求在网络入口点。

此解决方案尝试阻拦传染，然而不会治疗很大数量的缓存条目、邻接和NAT/PAT条目积累引起的问题，因为要分析HTTP GET请求的内容的唯一方法跟随TCP连接的建立。以下过程无法防范网络扫描。然而，它将保护站点免受从一个外部网络的袭击或减少的感染企图的数量机器必须服务。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。特别地，能力匹配在HTTP URL的任何部分使用在NBAR内的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

发现在IIS Web日志的感染企图

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
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
```

“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 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 -
```

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请求的剩下的事不一定一致，尝试创建缓冲区溢出。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。而新的威胁包含“”，原始" Code Red "应变在GET请求包含“NNNNNNNN”字符串。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。我们从那以后获悉这是由eEye弱点扫描程序忘记的覆盖区 。

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

阻拦在此建议提供的" Code Red "的技术能通过加强类映射定义也阻拦这些扫描尝试如下个部分所显示。

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*"
```
   上述类映射查找在HTTP URL里面并且匹配其中任一个指定的字符串。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 Sadmind 病毒。
   http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS00-078.asphttp://www.sophos.com/virusinfo/analyses/unixsadmind.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. 配置ACL在的DSCP值配比为1，和由服务策略设置。
```
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。执行如此强制所有信息包被过程交换而不是经过CEF交换的，并且NBAR不会工作，因为要求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**并且保证Deny语句的" matches "值增加。
```
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。如果已经配置，您不需要适用in命令此方法方法A或C。

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和启用了ACL记录，您能也使用**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
```
我们能做出丢弃决策在路由器的入口接口，而不是需要输出ACL在每个输出接口。再次建议您使用 **no ip unreachables** 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

因为不取决于PBR或输出ACL，此方法通常是最可升级的。

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

当使用NBAR以方法在本文时，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
- 分段的信息包
- 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

您不可以在以下逻辑接口上配置 NBAR：

- 快速以太信道

- 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。

因为NBAR不可能用于分类输出在使用建立隧道或加密的广域网链路的数据流，请适用它于在路由器的其他接口，例如LAN接口，进行输入分类，在数据流换成输出的前广域网链路。

关于更多NBAR信息，请参阅在相关信息的链路