如何保护网络以免受 NIMDA 病毒

目录

简介

本文描述了最大限度减少NIMDA蠕虫对您的网络的影响的方式。本文讨论两个主题：

- 网络被传染，什么可以执行？如何能最小化损伤和余波？
- 网络没有被传染，也不部分地只被传染。什么可以执行最小化传播此蠕虫病毒？

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

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

关于NIMDA蠕虫的背景信息，参考这些链路：

- http://www.cert.org/body/advisories/CA200126_FA200126.html
- http://vil.nai.com/vil/content/v_99209.htm
- http://www.sarc.com/avcenter/venc/data/w32.nimda.a@mm.html

支持的平台

本文描述的基于网络的应用程序识别(NBAR)解决方案，需要Cisco IOS®软件中的基于级别的标记功能。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 软件版本
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(5)T

注意： 您需要使思科快速转发(CEF)为了使用基于网络应用的识别(NBAR)。

开始用版本12.1E的一些Cisco IOS软件平台也支持NBAR。请参阅“支持的协议”在基于网络的应用程序识别文档。

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 软件版本
7500	12.1(6)E
FlexWan	12.1(6)E

如果部署NBAR，请注意Cisco Bug ID CSCdv06207 (仅限注册用户)。如果遇到此缺陷，在CSCdv06207描述的应急方案可能是需要的。

Cisco IOS软件所有当前版本支持访问控制表(ACL)解决方案。

对于您需要使用模块化服务质量的解决方案(QoS)命令行界面(CLI) (例如速率限制ARP流量或实现限制与策略器的速率而不是CAR)，是可用的在Cisco IOS软件版本12.0XE、12.1E、12.1T和所有版本12.2的您需要模块化服务质量命令行接口。

对于承诺比特率使用(CAR)，您需要Cisco IOS软件release11.1CC和12.0及以上版本软件所有版本。

如何最小化损伤和限制余波

此部分概述能传播NIMDA病毒的传染向量，并且提供提示减少病毒的扩展：

- 蠕虫病毒能通过MIME audio/x-wav类型的电子邮件附件传播。**提示：**增加在您的简单邮件传输

协议(SMTP)服务器的规则阻塞有这些附件的所有电子邮件：readme.exeAdmin.dll

- 蠕虫病毒能传播，当您浏览有启用和用例如是易受攻击对在MS01-020讨论的检测安全漏洞代码的Internet Explorer版本时(IE)的Javascript执行的一被传染的 Web服务器(没有SP2的IE 5.0或IE 5.01)。**提示：**使用netscape作为浏览器，或者在IE上禁用Javascript，或者安装SP II的IE补丁。请使用Cisco基于网络的应用识别(NBAR)过滤从下载的readme.eml文件。这是配置NBAR的示例：`Router(config)#class-map match-any http-hacks`
  `Router(config-cmap)#match protocol http url "*readme.eml*"` 一旦您匹配了数据流，您便可以选择丢弃或根据策略路由数据流，以监控被感染的主机。完整实施的示例在使用被找到基于网络的应用程序识别，并且" Code Red "蠕虫的阻塞的访问控制列表。
- 蠕虫病毒能从计算机传播到计算机以IIS攻击(的形式主要尝试利用红色代码影响创建的MS00-078以前修补的漏洞II，而且漏洞)。**提示：**请使用描述的红色代码计划在：如何解决“红色代码”蠕虫引起的 mallocfail 和 CPU 使用率过高的问题使用基于网络的应用程序识别和访问控制列表阻塞的" Code Red "蠕虫病毒
```
Router(config)#class-map match-any http-hacks
Router(config-cmap)#match protocol http url "*.ida*"
Router(config-cmap)#match protocol http url "*cmd.exe*"
Router(config-cmap)#match protocol http url "*root.exe*"
Router(config-cmap)#match protocol http url "*readme.eml*"
```
  一旦您匹配了数据流，您便可以选择丢弃或根据策略路由数据流，以监控被感染的主机。完整实施的示例在使用被找到基于网络的应用程序识别，并且" Code Red "蠕虫的阻塞的访问控制列表。速率限制TCP同步/启动(SYN)数据包。这不能保护主机，但是允许您的网络在低性能方式下运行还仍然保持连接。对SYN进行速率限制，您会丢弃超出一定速率的信息包，部分(但不是所有)TCP连接将会畅通。对于配置示例，参考使用CAR的“限制为TCP SYN数据包的速率”部分在DOS攻击期间。如果大量ARP扫瞄导致了网络中的问题，就应考虑对地址解析协议(ARP)数据流进行速率限制。对速率限制ARP流量，请配置以下：
```
class-map match-any arp
   match protocol arp
!
!
policy-map ratelimitarp
   class arp
      police 8000 1500 1500 conform-action transmit exceed-action drop violate-action drop
```
  此策略需要运用到相关LAN接口，作为输出策略。修改该数字，使其与您将在网络上允许的每秒ARP的数量相适应。
- 蠕虫可能通过标记被启用活动桌面(默认为W2K/ME/W98)的Explorer中的.eml或.nws来传播。这造成THUMBVW.DLL执行文件，并尝试下载README.EML (根据您的IE版本和区域设置而定)。**提示**： 如上所推荐，使用NBAR过滤从下载的readme.eml。
- 蠕虫病毒能通过映射的驱动器传播。任何带映射网络驱动器的受感染的机器，将可能感染映射驱动器和其子目录上的所有文件。**提示：**拦截普通文件传输协议(TFTP) (端口69) ，使受感染的机器不能使用TFTP，将文件传输到未受感染的主机上。保证路由器的TFTP访问仍然可用(因为您可能需要路径升级代码)。如果路由器正在运行Cisco IOS软件版本12.0或更新版本，您永远有使用文件传输协议(FTP)的选项，将镜像传输到运行Cisco IOS软件的路由器。块NetBIOS。NetBIOS不应该必须留下局域网。服务提供商应该由阻塞端口137， 138， 139和445过滤掉NetBIOS。
- 蠕虫利用它自己的SMTP引擎，发出电子邮件，传染其他系统。**提示**： 阻塞您的网络内部的端口25 (SMTP)。使用邮政协议(POP) 3(端口110)或互联网邮件访问协议(IMAP) (端口143)检索电子邮件的用户不需要访问端口25。只允许端口25对网络的SMTP服务器开放。这对使用Eudora、Netscape和Outlook Express或其他程序的用户可能不适用，因为它们有自己的SMTP引擎并且使用端口25生成出站连接。可能需要进行某些调查，查看是否可以使用代理服务器或其他某些机制。
- 清洗Cisco CallManager/应用服务器**提示**： 用户用在他们的网络的Call Managers和

CallManager应用服务器必须执行以下终止传播病毒。他们不能浏览到从CallManager的受感染的机器并且他们不能共享在CallManager服务器的任何驱动。遵从在从Cisco CallManager 3.x和CallManager应用服务器的清洗NIMDA病毒提供的说明为清洗NIMDA病毒。

- 过滤在CSS 11000的NIMDA病毒**提示**： 用户用CSS 11000必须遵从在过滤NIMDA病毒提供的说明在CSS 11000为清洗NIMDA病毒。
- 对NIMDA病毒的Cisco安全入侵监测系统(CS IDS)答复**提示**： CS IDS有可用两个不同的组件。有一主机传感器和基于网络IDS的一个是基于主机的IDS (HIDS) (NIDS)有一个网络传感器，其中之二以不同的方式响应对NIMDA病毒。更多详细说明和推荐的行动，参考Cisco Secure IDS如何响应对NIMDA病毒。

相关信息

- **使用基于网络的应用程序识别和访问控制列表阻塞的" Code Red "蠕虫**
- **如何解决“红色代码”蠕虫引起的 mallocfail 和 CPU 使用率过高的问题**
- **在 DOS 攻击期间使用 CAR**
- **Cisco 安全建议和通知**
- **技术支持和文档 - Cisco Systems**