如何保护您的网络以防止NIMDA病毒

Contents

Introduction

本文描述方式使NIMDA蠕虫减到最小的影响对您的网络。本文讨论两个题目：

- 网络被传染，什么可以执行？如何能使损伤和余波减到最小？
- 网络没有被传染，也不部分地只被传染。什么可以执行使传播此蠕虫减到最小？

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment.All of the devices used in this document started with a cleared (default) configuration.If your network is live, make sure that you understand the potential impact of any command.

Conventions

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，请参见这些链路：

- 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

在本文描述的基于网络应用的识别(NBAR)解决方案要求在Cisco IOS软件内的基于类别的标记功能。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

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

开始从版本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

如果配置NBAR，请注意Cisco Bug ID CSCdv06207 (仅限注册用户)。如果遇到此缺陷，在CSCdv06207描述的解决方法可能是需要的。

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(QoS)命令行界面(CLI)的解决方案(例如速率限制ARP数据流或实现限制与策略器的费率而不是CAR)，您需要是可用的在Cisco IOS软件版本12.0XE、12.1E、12.1T和所有版本12.2的模块化服务质量命令行界面。

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。

如何使损伤减到最小和限制余波

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)服务器的规则阻拦有这些附件的所有电子邮件：readme.exeAdmin.dll

- 蠕虫能传播，当您访问有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执行功能的一被传染的 Web服务器(没有SP2的IE 5.0或IE 5.01)。**提示：**用Netscape作为您的浏览器或者禁用在IE的Javascript或者获得IE被修补对SP II。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*"
```

一旦匹配了数据流，您能选择丢弃或策略基于路由监控感染的主机的数据流。完整实施的示例在使用被找到基于网络的应用程序识别和访问控制列表阻拦" Code Red "蠕虫。

- 蠕虫能从机器传播到机器以IIS攻击(的形式主要尝试利用红色代码II的作用创建的MS00-078以前修补的弱点，而且弱点)。**提示：**请使用红色代码计划描述在：处理起因于" Code Red "蠕虫的mallocfail和高CPU利用率使用基于网络的应用程序识别和访问控制列表阻拦的" Code Red "蠕虫

```
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*"
```

一旦匹配了数据流，您能选择丢弃或策略基于路由监控感染的主机的数据流。完整实施的示例在使用被找到基于网络的应用程序识别和访问控制列表阻拦" Code Red "蠕虫。费率限制TCP同步/启动(SYN)信息包。这不保护主机，但是允许您的网络以一个降低方式运行和仍然保持。由速率限制SYN，您丢掉超出特定速率的信息包，因此一些TCP连接将通过，但是不是所有。关于配置示例，请参见使用CAR的“限制为TCP Syn信息包的费率”部分在DOS攻击期间。考虑速率限制地址解析协议(ARP)数据流，如果相当数量ARP扫瞄的网络引起问题。对费率限制ARP数据流，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
```

此策略然后需要被运用于相关LAN接口作为输出策略。修改图如适当顾及ARPs的编号每您在网络要允许的秒。

- 蠕虫能通过突出显示.eml或.nws传播在Explorer有活动桌面功能(W2K/ME/W98默认情况下)。这造成THUMBVW.DLL执行文件和尝试下载它参考的README.EML (根据您的IE版本和区域设置)。**提示**： 如上所推荐，使用NBAR过滤从下载的readme.eml。
- 蠕虫能通过映射的驱动器传播。映射网络驱动器的所有受感染的机器可能将传染所有在映射的驱动器和其子目录的文件**提示：**阻拦简单文件传输协议(TFTP) (端口69)，以便受感染的机器不能使用TFTP调用文件到没被感染的主机。保证路由器的TFTP访问是可用的(因为您可能需要路径到升级代码)。如果路由器运行Cisco IOS软件版本12.0或以上，您总是有使用文件传输协议(FTP)的选项转交镜像运行Cisco IOS软件的路由器。块NetBIOS。NetBIOS不应该必须留下一个区域网(LAN)。服务提供商应该由阻塞端口137， 138， 139和445过滤掉NetBIOS。
- 蠕虫利用其自己的SMTP引擎发送电子邮件传染其他系统。**提示**： 阻拦在您的网络的内部的端口25 (SMTP)。检索他们的电子邮件使用邮政协议的用户(POP) 3 (端口110)或互联网邮件访问协议(IMAP) (端口143)不需要对端口25的访问。只请允许端口25是开放的面对网络的SMTP服务器。使用端口25，因为他们有他们自己的SMTP引擎，并且生成出局连接这可能不是可行的为用户使用Eudora、Netscape和奥特卢克Express，除了别的以外。若干调查也许需要适用于

可能的用途代理服务器或某个其他机制。

- 清洗Cisco CallManager/应用服务器**提示**： 有Call Managers的用户和在他们的网络的呼叫管理器应用服务器必须执行以下终止传播病毒。他们不能访问到从呼叫管理器的受感染的机器并且他们不能共享在呼叫管理器服务器的任何驱动。遵从在清洁从Cisco CallManager 3.x和呼叫管理器应用服务器的NIMDA病毒提供的指令为清洗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病毒提供的指令在CSS 11000为清洗NIMDA病毒。
- 对NIMDA病毒的Cisco安全入侵监测系统(CS IDS)回应**提示**： CS IDS有可用两个不同的组件。有有一个网络传感器，其中之二以不同的方式回应NIMDA病毒。的一个主机传感器和基于网络IDS的一个是招待基础的IDS (HIDS) (NIDS)关于一个详细说明和推荐的行动，请参见Cisco Secure IDS如何回应NIMDA病毒。

Related Information

- **使用基于网络的应用程序识别和访问控制列表阻拦的" Code Red "蠕虫**
- **处理起因于" Code Red "蠕虫的mallocfail和高CPU利用率**
- **使用在DOS攻击期间的CAR**
- **Cisco 安全建议和通知**
- Technical Support & Documentation - Cisco Systems