如何保护网络免受 Nimda 病毒攻击

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[规则](#)
[背景信息](#)
[支持的平台](#)
[如何尽量减少损害和降低辐射影响](#)
[相关信息](#)

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。本文档涉及两个主题：

- 网络受到感染，可以采取什么措施？您如何能够最大限度地降低损害和辐射影响？
- 网络尚未感染或仅部分感染。怎样才能最大程度地减少此蠕虫的传播？

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

有关Nimda蠕虫的背景信息，请参阅以下链接：

- 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：

Platform	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)公吨

注意：要使用基于网络的应用识别(NBAR)，您需要启用思科快速转发(CEF)。

从版本12.1E开始，某些Cisco IOS软件平台也支持NBAR。请参阅基于网络的应用识别文档中的“支持的协议”。

以下平台也提供基于类的标记功能和分布式 NBAR (DNBAR)：

Platform	最低 Cisco IOS 软件版本
7500	12.1(6)E
FlexWAN	12.1(6)E

如果要部署NBAR，请注意思科漏洞ID CSCdv06207(仅限注册客户)。 如果遇到此缺陷，可能需要使用CSCdv06207中描述的解决方法。

所有当前版本的Cisco IOS软件都支持访问控制列表(ACL)解决方案。

对于需要使用模块化服务质量(QoS)命令行界面(CLI)（例如用于速率限制ARP流量或使用监察器而不是CAR实施速率限制）的解决方案，需要Cisco IOS软件版本12.0XE、12.1E、12.1T和所有版本12.2中可用的模块化服务质量命令行界面。

要使用承诺访问速率(CAR)，您需要使用Cisco IOS软件版本11.1CC和12.0及更高版本的软件。

如何尽量减少损害和降低辐射影响

本部分概述了能够传播Nimda病毒的感染载体，并提供了减少病毒传播的提示：

- 蠕虫可以通过MIME音频/x-wav类型的邮件附件传播。

  技巧:

  - 在简单邮件传输协议(SMTP)服务器上添加规则，以阻止包含这些附件的任何邮件：
    - readme.exe
    - Admin.dll

- 当您浏览已启用了Javascript执行的受感染的Web服务器，并使用易受攻击的Internet Explorer(IE)版本(如MS01-020,IE 5.0或IE 5.01，不带SP2)时，蠕虫可以传播。

  技巧:

  - 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。
  - 使用思科基于网络的应用识别(NBAR)过滤readme.eml文件以进行下载。以下是配置NBAR的示例：

    <#root>

    ```
    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。完整的实施示例见使用基于网络的应用识别和访问控制列表阻止“红色代码”蠕虫。

- 蠕虫可以以IIS攻击的形式在计算机之间传播(它主要尝试利用由红色代码II的影响创建的漏洞，以及之前通过MS00-078修补的漏洞)。

  技巧:

  - 使用中介绍的Code Red方案：

    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识别和访问控制列表阻止“红色代码”蠕虫

```
<#root>

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。完整的实施示例见使用基于网络的应用识别和访问控制列表阻止“红色代码”蠕虫。

- 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。有关配置示例，请参阅在DOS攻击期间使用CAR的“TCP SYN数据包的速率限制”部分。
- 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。要限制ARP流量的速率，请配置以下命令：

```
<#root>

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：如上文所建议，请使用NBAR过滤下载的readme.eml。

- 蠕虫可以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。

  技巧:

  - 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。

  - 阻止NetBIOS。NetBIOS不应离开局域网(LAN)。 服务提供商应通过阻止端口137、138、139和445过滤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：阻止网络内部部分的端口25(SMTP)。使用邮局协议(POP)3（端口110）或Internet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。仅允许面向网络SMTP服务器的端口25打开。这对使用Eudora、Netscape和Outlook Express等服务的用户来说可能不可行，因为他们有自己的SMTP引擎并且会使用端口25生成出站连接。可能需要对代理服务器或其他机制的可能用途进行一些调查。

- 清理Cisco CallManager/应用服务器

  提示：在其网络中具有Call Manager和Call Manager应用服务器的用户必须执行以下操作来停止病毒传播。他们不能从Call Manager浏览到受感染的计算机，也不能共享Call Manager服务器上的任何驱动器。按照从Cisco CallManager 3.x和CallManager应用服务器清除Nimda病毒中提供的说明进行操作。

- 在CSS 11000上过滤Nimda病毒

  提示：使用CSS 11000的用户必须按照在CSS 11000上过滤Nimda病毒中提供的说明清除NIMDA病毒。

- 思科安全入侵检测系统(CS IDS)对Nimda病毒的响应

  提示：CS IDS有两个不同的组件可用。一个是具有主机传感器的基于主机的IDS(HIDS)和具有网络传感器的基于网络的IDS(NIDS)，两者对Nimda病毒的响应方式不同。有关更详细的说明和推荐的操作过程，请参阅Cisco Secure IDS如何响应Nimda病毒。

相关信息

- 使用基于网络的应用识别和访问控制列表阻止“红色代码”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

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。