Cisco Secure IDS 如何应对 Nimda 病毒？

目录

简介

本文解释Cisco安全入侵监测系统(IDS)如何鉴别并且防止Web服务器妥协攻击通过NIMDA蠕虫(亦称概念病毒)。蠕虫病毒的复杂技术工作是超出此公告版的范围之外并且在别处是有大量文件证明的。其中一NIMDA蠕虫的最好的技术说明可以在CERT®资询CA-2001-26 NIMDA蠕虫找到 。

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。

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

NIMDA蠕虫是在互联网积极地传播的混合的蠕虫病毒和病毒。要了解Nimda和Cisco IDS的能力缓和其扩展，定义这两期限是重要的：

- **蠕虫病毒**是指自动扩展，没有人为干预的恶意代码。
- **病毒**是指通过某种人为干预传播的恶意代码，例如，当您打开电子邮件时，浏览感染的网站或

者手工执行染毒的文件。

NIMDA蠕虫实际上是陈列蠕虫病毒和病毒特性的混合。Nimda在多种方式传染，多数要求人为干预。Cisco IDS主机传感器阻塞通过在Microsoft的互联网信息服务器(IIS)的漏洞传播的类似蠕虫的感染方法。Cisco IDS不阻塞类似病毒的，手工传染方法，例如，当您打开电子邮件附件时，浏览感染的网站，或者请手工执行一个染毒的文件。

Cisco IDS 主机传感器保护主机免受 Nimda 蠕虫攻击

Cisco IDS主机传感器防止目录遍历攻击，包括NIMDA蠕虫使用的那些。当蠕虫病毒尝试攻陷思科IDS保护的Web服务器时，攻击发生故障，并且服务器没有被攻陷。

这些Cisco IDS主机传感器规则防止NIMDA蠕虫的成功：

- IIS目录遍历(四个规则)
- IIS目录遍历和编码执行(四个规则)
- IIS加倍十六进制编码目录遍历(四个规则)

Cisco IDS主机传感器也防止对Web内容的未被授权的更改，因此不允许蠕虫病毒修改网页为了传播自己到其他服务器。

Cisco IDS遵守标准安全最佳实践保护Web服务器以防止Nimda。这些最佳实践指明不读电子邮件或浏览从制作Web服务器的Web，以及没有网络共享请打开在服务器。Cisco IDS主机传感器防止Web服务器折衷通过HTTP和IIS检测安全漏洞代码。上述最佳实践保证NIMDA蠕虫在Web服务器不到达通过一些人工方法。

Cisco IDS 网络传感器辨认 Nimda

Cisco IDS网络传感器识别Web应用程序攻击，包括NIMDA蠕虫使用的那些。网络传感器能识别攻击和提供关于受影响的细节或受影响的主机隔离NIMDA传染。

这些Cisco IDS网络传感器告警火：

- WWW WinNT cmd.exe访问(SigID 5081)
- IIS CGI双解码(SigID 5124)
- WWW IIS Unicode攻击(SigID 5114)
- IIS点点执行攻击(SigID 3215)
- IIS点点失败攻击(SigID 3216)

操作员看不到按名称标识Nimda的报警。他们看到作为Nimda尝试不同的检测安全漏洞代码注释的一系列的报警减弱目标。报警识别应该从网络隔离，清洗和修补被攻陷了，并且主机的源地址。

推荐行动过程

遵从这些步骤防止受到NIMDA蠕虫：

1. 申请最新的更新Microsoft Outlook、奥特卢克Express、Internet Explorer和IIS可得到从Microsoft 。
2. 更新您的病毒扫描软件以最新的补丁程序缓和病毒的扩展。**注意：** 您能下载最新的病毒补丁保护您的从传染的PC。如果您的PC已经被传染了，此病毒补丁允许您手工扫描您的PC硬盘驱动器和从计算机清洗传染。

3. 部署Cisco IDS缓和威胁，包含传染，并且保护服务器。

相关信息

- 如何保护网络以免受 NIMDA 病毒
- Cisco 产品安全建议和通知
- Cisco安全入侵检测支持页
- 技术支持 - Cisco Systems