如何保護您的網路免受Nimda病毒的侵擾

目錄

簡介

本文檔介紹如何將Nimda蠕蟲對網路的影響降至最低。本文討論兩個主題：

- 網路受到感染，可以採取什麼措施？如何才能將破壞和輻射塵埃降到最低？
- 網路尚未感染或僅部分感染。如何將此蠕蟲的傳播降至最低？

必要條件

需求

本文件沒有特定需求。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

背景資訊

有關Nimda蠕蟲的背景資訊，請參閱以下連結：

- 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

支援的平台

本文所述的網路型應用程式辨識(NBAR)解決方案需要Cisco IOS®軟體中的類別型標記功能。具體而言，在HTTP URL的任何部分上進行匹配的功能會使用NBAR中的HTTP子埠分類功能。支援的平台和最低Cisco IOS軟體要求概述如下：

平台	最低Cisco IOS軟體版本
7200	12.1(5)公噸
7100	12.1(5)公噸
3660	12.1(5)公噸
3640	12.1(5)公噸
3620	12.1(5)公噸
2600	12.1(5)公噸
1700	12.2(5)公噸

注意：您需要啟用Cisco Express Forwarding(CEF)才能使用基於網路的應用識別(NBAR)。

從版本12.1E開始的一些Cisco IOS軟體平台也支援NBAR。請參閱基於網路的應用識別文檔中的「支援的協定」。

以下平台上還提供了基於類的標籤和分散式NBAR(DNBAR):

平台	最低Cisco IOS軟體版本
7500	12.1(6)E
FlexWAN	12.1(6)E

如果要部署NBAR，請注意思科錯誤ID CSCdv06207(僅限註冊客戶)。 如果遇到此缺陷，可能需要使用CSCdv06207中描述的解決方法。

所有目前版本的Cisco IOS軟體都支援存取控制清單(ACL)解決方案。

對於需要使用模組化服務品質(QoS)指令行介面(CLI)的解決方案（例如用於速率限制ARP流量或使用管制器而不是CAR實作速率限制），您需要Cisco IOS軟體版本12.0XE、12.1E、12.1T和所有12.2版本中提供的模組化服務品質指令行介面。

若要使用承諾存取速率(CAR)，您需要Cisco IOS軟體版本11.1CC和所有版本的12.0和更新軟體。

如何減輕損失與限制輻射

本節概述了可以傳播Nimda病毒的感染載體，並提供了減少病毒傳播的提示：

- 蠕蟲可以通過MIME音訊/x-wav型別的郵件附件傳播。**提示**：在簡單郵件傳輸協定(SMTP)伺服器上新增規則，以阻止包含這些附件的任何電子郵件：readme.exeAdmin.dll

- 當您瀏覽已啟用Javascript執行的受感染Web伺服器並使用易受在MS01-020 （例如，IE 5.0或沒有SP2的IE 5.01）中討論的漏洞攻擊的Internet Explorer(IE)版本時，蠕蟲會傳播。**提示：**使用Netscape作為瀏覽器，或者禁用IE上的Javascript，或者將IE修補到SP II。使用思科基於網路的應用識別(NBAR)過濾readme.eml檔案不被下載。以下是設定NBAR的範例：

```
Router(config)#class-map match-any http-hacks
Router(config-cmap)#match protocol http url "*readme.eml*"
```

匹配流量後，您可以選擇丟棄或基於策略路由流量以監控受感染的主機。完整的實施示例可在使用基於網路的應用識別和訪問控制清單阻止「紅色代碼」蠕蟲中找到。

- 蠕蟲可以以IIS攻擊的形式在機器之間傳播(它主要嘗試利用由Code Red II產生的漏洞，以及之前由MS00-078 修補的漏洞)。**提示：**使用中介紹的紅色代碼方案：處理「紅色代碼」蠕蟲引起的mallocfail和CPU使用率高的問題使用基於網路的應用識別和訪問控制清單阻止「紅色代碼」蠕蟲

```
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*"
```

匹配流量後，您可以選擇丟棄或基於策略路由流量以監控受感染的主機。完整的實施示例可在使用基於網路的應用識別和訪問控制清單阻止「紅色代碼」蠕蟲中找到。速率限制TCP同步/啟動(SYN)封包。這不會保護主機，但允許網路以降級方式運行並保持運行。通過速率限制SYN，您會丟棄超過特定速率的資料包，因此某些TCP連線會通過，但並非全部。有關配置示例，請參閱在DOS攻擊期間使用CAR的「TCP SYN資料包的速率限制」部分。如果ARP掃描量導致網路出現問題，請考慮速率限制地址解析協定(ARP)流量。要限制ARP流量的速率，請配置以下內容：

```
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
```

然後，需要將此策略作為輸出策略應用到相關的LAN介面。根據需要修改此圖，以便滿足網路上每秒允許的ARP數量。

- 蠕蟲可通過在已啟用Active Desktop（預設為W2K/ME/W98）的Explorer中突出顯示.eml或.nws來傳播。 這會導致THUMBVW.DLL執行檔案並嘗試下載其中引用的README.EML（取決於您的IE版本和區域設定）。**提示：**按照上述建議，使用NBAR過濾要下載的readme.eml。
- 蠕蟲可以通過對映的驅動器傳播。任何已對映網路驅動器的受感染電腦都可能會感染對映驅動器及其子目錄上的所有檔案**提示：**阻止簡單式檔案傳輸協定(TFTP)（埠69），使受感染的電腦無法使用TFTP將檔案傳輸到未感染的主機。確保路由器的TFTP訪問仍然可用（因為可能需要路徑來升級代碼）。 如果路由器正在運行Cisco IOS軟體版本12.0或更高版本，則始終可以選擇使用檔案傳輸協定(FTP)將映像傳輸到運行Cisco IOS軟體的路由器。阻止NetBIOS。NetBIOS不應離開區域網(LAN)。 服務提供商應通過阻止埠137、138、139和445過濾NetBIOS。
- 該蠕蟲利用自己的SMTP引擎傳送電子郵件以感染其他系統。**提示：**阻止網路內部部分的埠25(SMTP)。使用郵局協定(POP)3（埠110）或Internet郵件訪問協定(IMAP)（埠143）檢索電子郵件的使用者不需要訪問埠25。僅允許面向網路SMTP伺服器的埠25開啟。這對使用Eudora、Netscape和Outlook Express等服務的使用者來說可能不可行，因為他們有自己的SMTP引擎並使用埠25生成出站連線。可能需要對代理伺服器或其他機制的可能用途進行一些調查。

- 清理Cisco CallManager/應用伺服器**提示**：在其網路中具有Call Manager和Call Manager應用程式伺服器的使用者必須執行以下操作來停止病毒的傳播。他們不能從Call Manager瀏覽到受感染的電腦，而且他們不能共用Call Manager伺服器上的任何驅動器。按照從Cisco CallManager 3.x和CallManager應用伺服器清除Nimda病毒中提供的說明清除Nimda病毒。
- 在CSS 11000上過濾Nimda病毒**提示**：使用CSS 11000的使用者必須按照在CSS 11000上過濾Nimda病毒中提供的說明清除NIMDA病毒。
- 思科安全入侵檢測系統(CS IDS)對Nimda病毒的響應**提示**：CS IDS有兩個不同的元件可用。一個是基於主機的入侵檢測系統(HIDS)具有一個主機感測器，另一個是基於網路的入侵檢測系統(NIDS)具有一個網路感測器，兩者對尼姆達病毒的反應方式不同。有關更詳細的說明和推薦的操作過程，請參閱Cisco Secure IDS如何響應Nimda病毒。

相關資訊

- **使用基於網路的應用識別和訪問控制清單阻止「紅色代碼」蠕蟲**
- **處理「紅色代碼」蠕蟲引起的mallocfail和CPU使用率高的問題**
- **在DOS攻擊期間使用CAR**
- **思科資安顧問和通知**
- **技術支援與文件 - Cisco Systems**