Cisco Secure IDS如何響應Nimda病毒

目錄

簡介

本文檔介紹思科安全入侵檢測系統(IDS)如何識別和防止Nimda蠕蟲（也稱為概念病毒）對Web伺服器的攻擊。 蠕蟲的複雜技術功能超出本公告的範圍，並且已在其他位置進行了詳細記錄。有關Nimda蠕蟲的最佳技術說明之一，請參閱CERT® Advisory CA-2001-26 Nimda Worm 。

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。

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

Nimda蠕蟲是一種混合蠕蟲和病毒，正在網際網路上大肆傳播。要瞭解Nimda和Cisco IDS緩解其傳播的能力，必須定義以下兩個術語：

- **蠕蟲**是指無需人工干預即可自動傳播的惡意代碼。
- **病毒**是指通過某種型別的人類干預（例如開啟電子郵件、瀏覽受感染網站或手動執行受感染檔

案）傳播的惡意代碼。

Nimda蠕蟲實際上是一個混合體，具有蠕蟲和病毒的特徵。尼姆達感染的方式多種多樣，其中大多數都需要人工干預。Cisco IDS主機感測器阻止通過Microsoft Internet Information Server(IIS)中的漏洞傳播的蠕蟲狀病毒感染方法。 Cisco IDS不會阻止類似病毒的手動感染方法，例如當您開啟電子郵件附件、瀏覽受感染網站或手動執行受感染檔案時。

Cisco IDS主機感應器防禦Nimda

Cisco IDS Host Sensor（Cisco IDS主機感測器）可防止目錄遍歷攻擊，包括Nimda蠕蟲所使用的攻擊。當蠕蟲試圖危害受Cisco IDS保護的Web伺服器時，攻擊會失敗，伺服器不會受到危害。

以下Cisco IDS主機感測器規則會阻止Nimda蠕蟲成功：

- IIS目錄遍歷（四個規則）
- IIS目錄遍歷和代碼執行（四個規則）
- IIS Double Hex Encoding Directory Traversal（四個規則）

Cisco IDS Host Sensor（Cisco IDS主機感測器）還能防止未經授權的Web內容更改，因此它不允許蠕蟲為了將自身傳播到其他伺服器而更改網頁。

Cisco IDS符合標準安全最佳實踐，可保護Web伺服器免受Nimda攻擊。這些最佳做法要求不要從生產Web伺服器讀取電子郵件或瀏覽Web，也不要在伺服器上開啟網路共用。Cisco IDS Host Sensor（Cisco IDS主機感測器）可防止Web伺服器通過HTTP和IIS漏洞被破壞。上述最佳實踐確保Nimda蠕蟲不會通過某種手動方式到達Web伺服器。

Cisco IDS網路感測器識別Nimda

Cisco IDS Network Sensor（Cisco IDS網路感測器）可識別Web應用攻擊，包括Nimda蠕蟲所使用的攻擊。網路感測器能夠識別攻擊，並提供受影響或受影響主機的詳細資訊，以隔離Nimda感染。

以下Cisco IDS網路感測器警報觸發：

- WWW WinNT cmd.exe訪問(SigID 5081)
- IIS CGI雙重解碼(SigID 5124)
- WWW IIS Unicode攻擊(SigID 5114)
- IIS Dot Execute Attack(SigID 3215)
- IIS Dot Crash Attack(SigID 3216)

操作人員看不到按名稱標識Nimda的警報。他們看到一系列警報，在尼姆達試圖利用不同的漏洞來攻擊目標時。警報標識已受到危害的主機的源地址，這些主機應與網路隔離、清除和修補。

建議的行動方針

按照以下步驟防止Nimda蠕蟲的傳播：

1. 應用Microsoft提供的Microsoft Outlook、Outlook Express、Internet Explorer和IIS的最新更新。
2. 使用最新補丁更新您的病毒掃描軟體，以緩解病毒的傳播。**注意：您**可以下載最新的病毒補丁，保護您的電腦免受感染。如果您的電腦已被感染，此病毒補丁允許您手動掃描電腦的硬碟並從電腦中清除感染病毒。

3. 部署思科IDS以緩解威脅、遏制感染並保護伺服器。

相關資訊

- 如何保護您的網路免受Nimda病毒的侵擾
- 思科產品安全建議和通知
- 思科安全入侵偵測支援頁面
- 技術支援 - Cisco Systems