Как система обнаружения вторжений Cisco реагирует на вирус Nimda

Содержание

Введение

В этом документе объясняется, как система обнаружения несанкционированного доступа Cisco (IDS) определяет и предотвращает опасность атаки на веб-сервер червя Nimda (также известного под названием вируса Concept). В данном документе не рассматривается сложная техническая работа червя, она описана в других документах. Одно из лучших технических описаний Червя nimda может быть найдено в CERT® Advisory CA-2001-26 Nimda Worm.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.

Общие сведения

Червь nimda является гибридным червем и вирусом, который распространяется настойчиво в Интернете. Для понимания Nimda и способностей Cisco IDS смягчить его распространение важно определить эти два срока:

- **Червь представляет собой вредоносный код, который распространяется автоматически без вмешательства человека.**
- **Вирус** обращается к вредоносной программе, которая распространяется через некоторый тип ручного вмешательства, такой как тогда, когда вы открываете электронную почту, просматриваете зараженный вебсайт, или вручную выполняете зараженный файл.

Червь nimda является фактически гибридом, который показывает характеристики и червя и вируса. Заражение вирусом Nimda происходит несколькими путями, но почти все они требуют человеческого вмешательства. Хост-сенсор Cisco IDS блокирует методы инфицирования наподобие червя, которые распространяются через уязвимости в информационном сервере интернета (IIS) Microsoft. Cisco IDS не блокирует подобное вирусу, способы заражения вручную, такой как тогда, когда вы открываете вложение электронной почты, просматриваете зараженный вебсайт, или вручную выполняете зараженный файл.

Хост-сенсор системы обнаружения сетевых атак Cisco обеспечивает защиту от вируса Nimda

Хост-сенсор Cisco IDS предотвращает атаки Обхода каталогов, которые включают используемых Червем nimda. Когда червь пытается поставить под угрозу защищенный от Cisco IDS Web-сервер, сбои атаки и сервер не поставился под угрозу.

Эти правила хост-сенсора Cisco IDS предотвращают успех Червя nimda:

- Обход каталогов IIS (четыре правила)
- Обход каталогов и выполнение программ IIS (четыре правила)
- Обход каталога IIS с двойным шестнадцатеричным кодированием (четыре правила)

Хост-сенсор Cisco IDS также защищает от неавторизованное изменений к вебу - контенту, таким образом, это не позволяет червю изменять веб-страницы для распространения к другим серверам.

Система Cisco IDS соответствует лучшим стандартам безопасности и обеспечивает защиту веб-серверов от сетевого червя Nimda. Эти оптимальные методы диктуют, чтобы не считать электронную почту или просмотреть веб-сайты от производственного Web-сервера, а также не иметь сетевые ресурсы, открытые на сервере. Хост-сенсор Cisco IDS препятствует тому, чтобы Web-сервер поставился под угрозу посредством использования IIS и HTTP. Вышеупомянутые оптимальные методы гарантируют, что Червь nimda не поступает в Web-сервер некоторыми ручными средствами.

Сетевой сенсор Cisco IDS идентифицирует вирус Nimda

Сетевой датчик Cisco IDS определяет атаки веб - приложения, которые включают

используемых Червем nimda. Сетевой датчик в состоянии определить атаки и предоставить подробную информацию о влияемом или скомпрометированных хостах для изоляции Вируса Nimda.

Эти Сигналы сетевого датчика Cisco IDS огонь:

- Доступ WWW WinNT cmd.exe (SigID 5081)
- CGI IIS дважды декодирует (SigID 5124)
- WWW IIS Unicode Attack (SigID 5114)
- Атака выполнения "точка точка" информационного сервера Internet (SigID 3215)
- Атака "точка-точка" на отказ сервера IIS (SigID 3216)

Операторы не видят сигнал тревоги, который определяет Nimda по имени. Они видят серию сигналов тревоги, на которые обращают внимание, поскольку Nimda пробует другое использование, чтобы поставить под угрозу цель. Сигналы тревоги определяют адрес источника хостов, которые поставились под угрозу, и это должно быть изолировано от сети, убрало и исправило.

Рекомендуемый порядок действий

Выполните эти действия для защиты против Червя nimda:

1. Примените последние обновления для Microsoft Outlook, Outlook Express, Internet Explorer и IIS, доступного от Microsoft.
2. Обновите антивирусное программное обеспечение с помощью последних обновлений, чтобы снизить распространение вирусов.**Примечание:** Можно загрузить последнее исправление для удаления вируса для защиты ПК от заражения. Если ваш ПК был уже заражен, это исправление для удаления вируса позволяет вам вручную просматривать жесткий диск своего ПК и чистить заражение от машины.
3. Разверните Cisco IDS, чтобы смягчить угрозу, содержать заражение и защитить серверы.

Дополнительные сведения

- Защита сети от вируса Nimda
- Сообщения и примечания по безопасности продуктов Cisco
- Страница поддержки системы обнаружения несанкционированного доступа Cisco
- Техническая поддержка - Cisco Systems