Come proteggere la rete dal virus Nimda

Sommario

Introduzione

Questo documento descrive come ridurre al minimo l'impatto del worm Nimda sulla rete. Questo documento tratta due argomenti:

- La rete è infetta, cosa si può fare? Come ridurre al minimo i danni e le ricadute?
- La rete non è ancora infetta, o lo è solo parzialmente. Cosa si può fare per ridurre al minimo la diffusione di questo verme?

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Premesse

Per informazioni di base sul verme Nimda, fare riferimento a questi collegamenti:

- 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

Piattaforme supportate

La soluzione di riconoscimento delle applicazioni di rete (NBAR) descritta in questo documento richiede la funzionalità di contrassegno basato su classi nel software Cisco IOS®. In particolare, la capacità di individuare corrispondenze in qualsiasi parte di un URL HTTP utilizza la funzionalità di classificazione delle porte secondarie HTTP in NBAR. Di seguito sono riepilogati le piattaforme supportate e i requisiti minimi del software Cisco IOS:

Piattaforma	Versione minima del software Cisco IOS
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)T

Nota: per utilizzare Network-Based Application Recognition (NBAR), è necessario abilitare Cisco Express Forwarding (CEF).

NBAR è supportato anche su alcune piattaforme software Cisco IOS a partire dalla versione 12.1E. Vedere la sezione relativa ai "Protocolli supportati" nella documentazione di Riconoscimento applicazioni basate su rete.

Il contrassegno basato su classi e DNBAR (Distributed NBAR) sono disponibili anche sulle seguenti piattaforme:

Piattaforma	Versione minima del software Cisco IOS
7500	12.1(6)E
FlexWAN	12.1(6)E

Se si distribuisce NBAR, tenere presente l'ID bug Cisco CSCdv06207 (solo utenti registrati). Se si verifica questo difetto, potrebbe essere necessaria la soluzione descritta in CSCdv06207.

La soluzione Access Control List (ACL) è supportata in tutte le versioni correnti del software Cisco IOS.

Per le soluzioni in cui è necessario utilizzare l'interfaccia della riga di comando (CLI) Modular

Quality of Service (QoS) (ad esempio per limitare la velocità del traffico ARP o per implementare la limitazione della velocità con un policer anziché con CAR), è necessaria l'interfaccia della riga di comando Modular Quality of Service disponibile nelle versioni 12.0XE, 12.1E, 12.1T e in tutte le versioni 12.2 del software Cisco IOS.

Per utilizzare Committed Access Rate (CAR), è necessario il software Cisco IOS versione 11.1CC e tutte le versioni 12.0 e successive.

Come ridurre al minimo i danni e limitare le perdite

Questa sezione descrive i vettori di infezione in grado di diffondere il virus Nimda e fornisce suggerimenti per ridurre la diffusione del virus:

- Il worm può diffondersi tramite allegati e-mail di tipo audio/x-wav MIME.**Suggerimenti:**Aggiungere regole nel server SMTP (Simple Mail Transfer Protocol) per bloccare qualsiasi messaggio di posta elettronica contenente i seguenti allegati:Leggimi.exeAdmin.dll
- Il worm può diffondersi quando si esplora un server Web infetto con l'esecuzione Javascript abilitata e si utilizza una versione di Internet Explorer (IE) che è vulnerabile agli attacchi discussi in MS01-020 (ad esempio, IE 5.0 o IE 5.01 senza SP2).**Suggerimenti:**Usare Netscape come browser, disabilitare Javascript su IE o applicare patch di IE a SP II.Utilizzare NBAR (Network-based Application Recognition) di Cisco per impedire il download di file leggimi.eml. Di seguito è riportato un esempio per configurare NBAR:
  ```
  Router(config)#class-map match-any http-hacks
  Router(config-cmap)#match protocol http url "*readme.eml*"
  ```
  Dopo aver individuato la corrispondenza con il traffico, è possibile scegliere di ignorare o instradare il traffico in base ai criteri per monitorare gli host infetti. Esempi di implementazione completa sono disponibili in Utilizzo di elenchi di riconoscimento delle applicazioni e di controllo degli accessi basati sulla rete per bloccare il worm "Code Red".
- Il worm può diffondersi da macchina a macchina sotto forma di attacchi IIS (tenta principalmente di sfruttare le vulnerabilità create dagli effetti di Code Red II, ma anche le vulnerabilità precedentemente sottoposte a patch da MS00-078).**Suggerimenti:**Utilizzare gli schemi di Code Red descritti in:Gestione di mallocfail e di un elevato utilizzo della CPU derivante dal worm "Code Red"Utilizzo di elenchi di riconoscimento e controllo degli accessi delle applicazioni di rete per bloccare il worm "Code Red"
  ```
  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*"
  ```
  Dopo aver individuato la corrispondenza con il traffico, è possibile scegliere di ignorare o instradare il traffico in base ai criteri per monitorare gli host infetti. Esempi di implementazione completa sono disponibili in Utilizzo di elenchi di riconoscimento delle applicazioni e di controllo degli accessi basati sulla rete per bloccare il worm "Code Red".Limita di velocità dei pacchetti TCP di sincronizzazione/avvio (SYN). Ciò non protegge un host, ma consente alla rete di funzionare in modo degradato e di rimanere attiva. Limitando la velocità SYN, si eliminano pacchetti che superano una determinata velocità, quindi alcune connessioni TCP possono passare, ma non tutte. Per gli esempi di configurazione, fare riferimento alla sezione "Limitazione della velocità per i pacchetti TCP SYN" di Utilizzo di CAR durante gli attacchi DOS.Prendere in considerazione il traffico ARP (Address Resolution Protocol) che limita la

velocità se la quantità di scansioni ARP causa problemi alla rete. Per limitare la velocità del traffico ARP, configurare quanto segue:

```
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
```

Questo criterio deve quindi essere applicato all'interfaccia LAN interessata come criterio di output. Modificare le cifre in base al numero di ARP al secondo che si desidera consentire sulla rete.

- Il worm può diffondersi evidenziando un file .eml o .nws in Esplora risorse con Active Desktop attivato (W2K/ME/W98 per impostazione predefinita). In questo modo THUMBVW.DLL eseguirà il file e tenterà di scaricare il file README.EML a cui fa riferimento (a seconda della versione di IE e delle impostazioni di zona).**Suggerimento:** come consigliato in precedenza, utilizzare NBAR per impedire il download di readme.eml.
- Il worm può diffondersi attraverso unità mappate. Tutti i computer infetti che dispongono di unità di rete mappate probabilmente infetteranno tutti i file presenti nell'unità mappata e nelle relative sottodirectory**Suggerimenti:**Blocca il protocollo TFTP (Trivial File Transfer Protocol) (porta 69) in modo che i computer infetti non possano utilizzare il protocollo TFTP per trasferire i file su host non infetti. Verificare che l'accesso TFTP per i router sia ancora disponibile (poiché potrebbe essere necessario il percorso per aggiornare il codice). Se sul router è in esecuzione il software Cisco IOS versione 12.0 o successive, è sempre possibile utilizzare il protocollo FTP (File Transfer Protocol) per trasferire le immagini sui router con software Cisco IOS.Bloccare NetBIOS. NetBIOS non deve lasciare una rete locale (LAN). I provider di servizi devono filtrare il NetBIOS bloccando le porte 137, 138, 139 e 445.
- Il worm utilizza il proprio motore SMTP per inviare messaggi di posta elettronica per infettare altri sistemi.**Suggerimento:** bloccare la porta 25 (SMTP) nella parte interna della rete. Gli utenti che recuperano la posta elettronica utilizzando il protocollo POP (Post Office Protocol) 3 (porta 110) o IMAP (Internet Mail Access Protocol) (porta 143) non devono accedere alla porta 25. Consentire solo l'apertura della porta 25 rivolta verso il server SMTP per la rete. Ciò potrebbe non essere possibile per gli utenti che utilizzano Eudora, Netscape e Outlook Express, tra gli altri, in quanto dispongono di un proprio motore SMTP e genereranno connessioni in uscita tramite la porta 25. Potrebbe essere necessario effettuare alcune ricerche sui possibili utilizzi dei server proxy o di altri meccanismi.
- Server applicazioni/CallManager Cisco puliti**Suggerimento:** gli utenti con i server applicazioni Call Manager e Call Manager nelle reti devono eseguire le operazioni seguenti per interrompere la diffusione del virus. Non devono passare al computer infetto da Gestione chiamate e inoltre non devono condividere alcuna unità sul server Gestione chiamate. Seguire le istruzioni fornite in Pulizia del virus Nimda dai server applicazioni Cisco CallManager 3.x e CallManager per la pulizia del virus Nimda.
- Filtrare il virus Nimda su CSS 1000**Suggerimento:** gli utenti con CSS 11000 devono seguire le istruzioni fornite in Filtering the Nimda Virus on CSS 11000 per pulire il virus NIMDA.
- Risposta di Cisco Secure Intrusion Detection System (CS IDS) al virus Nimda**Suggerimento:** CS IDS dispone di due componenti diversi. Uno è l'IDS basato su host (HIDS) che ha un sensore host e l'IDS basato su rete (NIDS) che ha un sensore di rete, entrambi i quali rispondono in modo diverso al virus Nimda. Per una spiegazione più dettagliata e il

comportamento consigliato, consultare il documento sulla risposta di Cisco Secure IDS al virus Nimda.

Informazioni correlate

- Utilizzo di elenchi di riconoscimento e controllo degli accessi delle applicazioni di rete per bloccare il worm "Code Red"
- Gestione di mallocfail e di un elevato utilizzo della CPU derivante dal worm "Code Red"
- Uso di CAR durante gli attacchi DOS
- Consigli e avvisi sulla sicurezza Cisco
- Documentazione e supporto tecnico – Cisco Systems