# Come Cisco Secure IDS risponde al virus Nimda

## Sommario



## Introduzione

Questo documento spiega come Cisco Secure Intrusion Detection System (IDS) identifichi e prevenga i compromessi dei server Web dagli attacchi del worm Nimda (noto anche come virus Concept). I complessi meccanismi tecnici del worm esulano dall'ambito di questo bollettino e sono ben documentati altrove. Una delle migliori descrizioni tecniche del verme Nimda è disponibile in CERT® Advisory CA-2001-26 Nimda Worm .

## Prerequisiti

### Requisiti

Nessun requisito specifico previsto per questo documento.

### Componenti usati

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

### Convenzioni

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

## Premesse

Il verme Nimda è un verme ibrido e un virus che si sta diffondendo in modo aggressivo su Internet. Per comprendere Nimda e le capacità di Cisco IDS di mitigarne la diffusione, è importante definire

questi due termini:

- **Il termine worm** si riferisce al codice dannoso che si diffonde automaticamente, senza intervento umano.
- **Il termine virus** si riferisce al codice dannoso che si diffonde attraverso alcuni tipi di intervento umano, ad esempio quando si apre un messaggio di posta elettronica, si sfoglia un sito Web infetto o si esegue manualmente un file infetto.

Il verme Nimda è in realtà un ibrido che mostra le caratteristiche sia di un verme che di un virus. La Nimda infetta in molti modi, la maggior parte dei quali richiede l'intervento umano. Cisco IDS Host Sensor blocca metodi di infezione simili a quelli dei worm che si diffondono attraverso le vulnerabilità in Microsoft Internet Information Server (IIS). Cisco IDS non blocca i metodi di infezione manuali simili ai virus, ad esempio quando si apre un allegato di posta elettronica, si esplora un sito Web infetto o si esegue manualmente un file infetto.

## Cisco IDS Host Sensor protegge da Nimda

Cisco IDS Host Sensor previene gli attacchi di tipo Directory Traversal, inclusi quelli utilizzati dal worm Nimda. Quando il worm tenta di compromettere un server Web protetto con Cisco IDS, l'attacco non riesce e il server non viene compromesso.

Queste regole Cisco IDS Host Sensor impediscono il successo del worm Nimda:

- Attraversamento directory IIS (quattro regole)
- Attraversamento directory IIS ed esecuzione codice (quattro regole)
- Attraversamento directory con codifica Double Hex IIS (quattro regole)

Cisco IDS Host Sensor, inoltre, impedisce modifiche non autorizzate al contenuto Web e impedisce al worm di modificare le pagine Web per diffondersi ad altri server.

Cisco IDS è conforme alle best practice in materia di sicurezza standard per proteggere i server Web da Nimda. Queste procedure consigliate prevedono di non leggere la posta elettronica o di esplorare il Web da un server Web di produzione, nonché di non avere condivisioni di rete aperte su un server. Cisco IDS Host Sensor impedisce che il server Web venga compromesso da attacchi HTTP e IIS. Le procedure ottimali di cui sopra garantiscono che il worm Nimda non arrivi sul server Web con qualche mezzo manuale.

## Cisco IDS Network Sensor identifica Nimda

Cisco IDS Network Sensor identifica gli attacchi alle applicazioni Web, inclusi quelli utilizzati dal worm Nimda. Network Sensor è in grado di identificare gli attacchi e fornire dettagli sugli host colpiti o compromessi per isolare l'infezione da Nimda.

I seguenti allarmi del sensore di rete Cisco IDS attivano:

- Accesso a WWW WinNT cmd.exe (SignatureID 5081)
- Doppia decodifica CGI IIS (Signature ID 5124)
- Attacco Unicode IIS WWW (SigID 5114)
- IIS Attacco esecuzione punto punto (Signature ID 3215)
- IIS Dot Dot Crash Attack (Signature ID 3216)

Gli operatori non vedono un allarme che identifica Nimda per nome. Vedono una serie di allarmi

annotati come Nimda prova diversi exploit per compromettere il bersaglio. Gli allarmi identificano l'indirizzo di origine degli host compromessi che devono essere isolati dalla rete, puliti e a cui devono essere applicate patch.

## Azioni consigliate

Attenersi alla seguente procedura per la protezione dal verme Nimda:

1. Applica gli aggiornamenti più recenti per Microsoft Outlook, Outlook Express, Internet Explorer e IIS disponibili in Microsoft .
2. Aggiornare il software antivirus con la patch più recente per ridurre la diffusione del virus.**Nota:** puoi scaricare la patch più recente per proteggere il PC dall'infezione. Se il PC è già stato infettato, questa patch per virus consente di eseguire manualmente la scansione del disco rigido del PC e di pulire l'infezione dal computer.
3. Implementare Cisco IDS per ridurre la minaccia, contenere l'infezione e proteggere i server.

## Informazioni correlate

- Come proteggere la rete dal virus Nimda
- Consigli e avvisi sulla sicurezza dei prodotti Cisco
- Pagina di supporto per Cisco Secure Intrusion Detection
- Supporto tecnico – Cisco Systems