



VIRUS: MYDOOM

1. INTRODUZIONE:

Sebbene il virus Mydoom non produca perdita di dati, abbiamo creduto opportuno realizzare questa relazione sulla sua azione per la gran ripercussione sociale che la sua enorme propagazione sta generando.

"Il worm Mydoom sta per diventare uno dei più nocivi tra tutti i virus che si sono estesi attraverso Internet negli ultimi mesi, ogni 6 e-mail 1 è stato infettato. Gli esperti delle compagnie antivirus hanno notato che Mydoom si estende più rapidamente del Sobig F. e del Klez, due dei virus più pericolosi nel 2003.

2. COS'È?

Mydoom è un worm che si diffonde attraverso la posta elettronica in un messaggio con caratteristiche variabili oppure attraverso il programma di filesharing KaZaA.

Ha capacità di backdoor, questo consente ad un utente remoto di accedere al computer infetto. Realizza attacchi di Ddos (Distributed denial of Service) contro le pagine web www.sco.com e www.microsoft.com.

3. QUANTI TIPI VE NE SONO?

Questo worm è una derivazione del virus Mimail, virus senza effetti dannosi, ma con una grande capacità di propagazione attraverso l'invio massivo di e-mail.

È stato identificato per la prima volta il 26 Gennaio 2004 e si presenta in due versioni: versione .A e versione .B, quest'ultima scoperta il 28 Gennaio 2004.

La nuova variante è ancora più pericolosa rispetto alla precedente, perché è stata progettata per impedire a molti programmi antivirus di aggiornarsi correttamente.

La nuova variante presenta un'ulteriore differenza rispetto a Mydoom A.: è stata progettata per lanciare attacchi DDoS contro i server della Microsoft, mentre la prima versione attaccava la web www.sco.com.

Nota: Nelle ultime ore si è rilevata l'apparizione di due nuovi virus legati a Mydoom, uno dei quali si denomina Doomjuice.A (W32/Doomjuice.A.worm). Si tratta di un worm che si diffonde attraverso Internet, utilizzando la porta d'accesso creata da Mydoom.A e Mydoom.B con l'obiettivo di autocopiarci nei computer infettati dai worm. Doomjuice.A lancia attacchi DDoS contro il sito web www.microsoft.com. L'altro virus scoperto è il Deadhat che disinstalla le versioni del virus Mydoom che trova e successivamente cerca di neutralizzare la protezione anti-virus del computer. Entrambi i virus, a differenza del Mydoom originale, non viaggiano attraverso la posta elettronica, ma cercano gli indirizzi e-mail in computer collegati infetti.



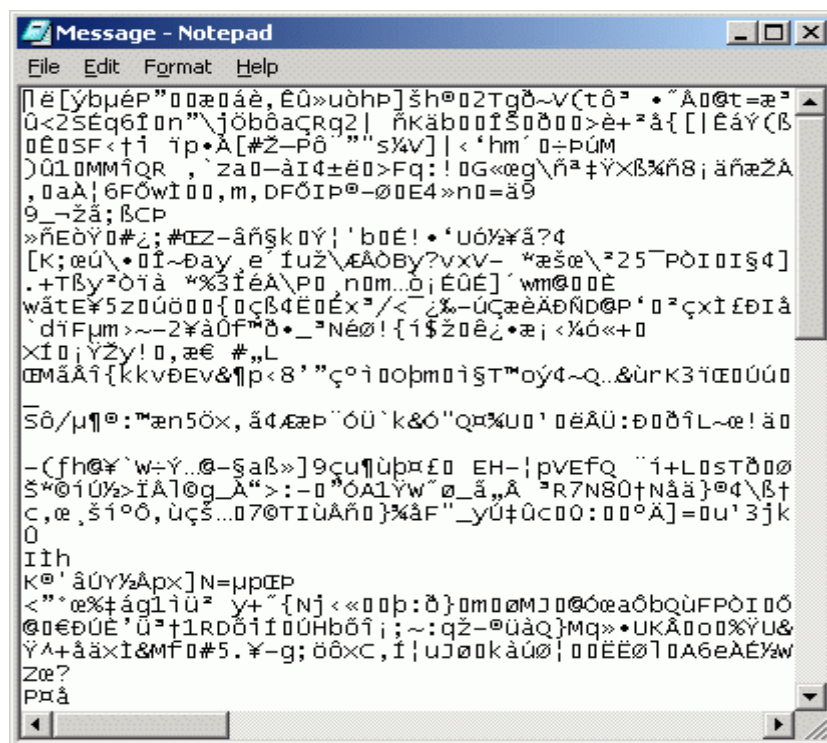
4. COME AGISCE?

W32/MyDoom è un worm da e-mail, con una componente backdoor, che cerca indirizzi nell' hard disk del sistema infettato e li utilizza per inviarsi come mittente, impedendo di identificare la sua esatta provenienza.

Il worm invita l'utente ad aprire un file di programma allegato. L'icona di questo file rappresenta un archivio di testo, per ingannare l'utente.



Quando si esegue per la prima volta, il worm apre il Notepad e mostra caratteri senza senso, del tipo:



Il worm installa il codice dannoso nel sistema ed invia a sé stesso tutti i contatti della Rubrica localizzati in file con estensioni: WAB, TXT, HTM, SHT, PHP, ASP, DBX, TBB, ADB e PL

Usa messaggi con temi, testi e nomi di file allegati variabili. Il messaggio normalmente ha una dimensione che varia da 30 a 35 Kb.



Il messaggio può avere come tema:

[caratteri senza senso o spazio vuoto]
Delivery Error
Error
hello
hi
Mail Delivery System
Mail Transaction Failed
Returned mail
Server Report
Status
Undeliverable: Mail Delivery System

I file in allegato possono chiamarsi:

[caratteri senza senso]
body
data
doc
document
file
message
readme
test
text

Il testo del messaggio, tra altri generati a caso, può essere:

Esempio 1:

*sendmail daemon reported:
Error #804 occurred during SMTP session.
Partial message has been received.*

Esempio 2:

*Mail transaction failed. Partial message
is available.*

Esempio 3:

*The message contains Unicode characters and
has been sent as a binary attachment.*

Esempio 4:

*The message contains MIME-encoded graphics
and has been sent as a binary attachment.*

Esempio 5:

*The message cannot be represented in 7-bit
ASCII encoding and has been sent as a binary
attachment.*



Propagazione attraverso KaZaA

Si autocopia nella cartella condivisa di KaZaa, con i seguenti nomi:

- activation_crack.bat
- activation_crack.pif
- activation_crack.scr
- icq2004-final.bat
- icq2004-final.pif
- icq2004-final.scr
- nuke2004.bat
- nuke2004.pif
- nuke2004.scr
- office_crack.bat
- office_crack.pif
- office_crack.scr
- rootkitXP.bat
- rootkitXP.pif
- rootkitXP.scr
- strip-girl-2.Obdcom_patches.bat
- strip-girl-2.Obdcom_patches.pif
- strip-girl-2.Obdcom_patches.scr
- winamp5.bat
- winamp5.pif
- winamp5.scr

In questo modo altri utenti di KaZaA possono scaricare il virus.

Installazione

Quando viene eseguito, crea i seguenti file nel sistema infettato:

- %TEMP%\Message
- c:\windows\system\shimgapi.dll
- c:\windows\system\taskmon.exe

NOTA : La cartella TEMP si trova in "c:\windows\temp", "c:\winnt\temp", o "c:\documents and settings\[utente]\local settings\temp", secondo il sistema operativo usato.

In ogni caso "c:\windows" e "c:\windows\system" possono variare in funzione del sistema operativo installato ("c:\winnt", "c:\winnt\system32", "c:\windows\system32", etc.).

Inoltre modifica o crea le seguenti entrate nel registro:

HKCU\Software\Microsoft\Windows\CurrentVersion\Run
TaskMon = c:\windows\system\taskmon.exe

HKLM\Software\Microsoft\Windows\CurrentVersion\Run
TaskMon = c:\windows\system\taskmon.exe

HKLM\Software\Microsoft\Windows\CurrentVersion
\Explorer\ComDlg32\Version

HKCU\Software\Microsoft\Windows\CurrentVersion
\Explorer\ComDlg32\Version



Per creare la porta d'accesso aggiunge il file SHIMGAPI.DLL alla directory SYSTEM di Windows, e la esegue come processo figlio (child process) di EXPLORER.EXE.

La chiave di registro modificata per eseguire questa missione è la seguente:

```
HKEY_CLASSES_ROOT\CLSID\{E6FB5E20-DE35-11CF-9C87-00AA005127ED}\InProcServer32  
"(Default)" = %SysDir%\shimgapi.dll
```

Il worm Mydoom B. può inviarsi inoltre a computer già infettati dalla versione A. Infatti, la sua componente backdoor scansiona la rete attraverso indirizzi IP generato a caso, e cerca di collegarsi alle porte TCP/3127, utilizzate da Mydoom. Se rileva un computer infetto, Mydoom vi si installa e si esegue immediatamente. In questo modo i computer infettati vengono aggiornati alla nuova versione, senza bisogno di ricevere un nuovo e-mail con il worm.

Effetti

1. Il worm cerca indirizzi di posta elettronica in tutti i file con le seguenti estensioni : WAB, TXT, HTM, SHT, PHP, ASP, DBX, TBB, ADB e PL, rinviandosi automaticamente.
2. Apre un troiano di accesso backdoor nei computer infettati, consentendo il controllo remoto del pc infettato da parte di un utente esterno.
3. Il worm lancia attacchi DDoS alle seguenti pagine:

www.sco.com (dal 1/2/04), www.microsoft.com (dal 3/2/04)

Questi attacchi consistono nell'invio di un numero elevatissimo di richieste GET HTTP. Entrambi gli attacchi vengono lanciati simultaneamente.

Si prevede che il Mydoom cessi la sua propagazione il 1° Marzo 2004, però la sua routine backdoor continuerà a funzionare.

5. COME ELIMINARLO?

1. Si consiglia innanzitutto essere estremamente cauti rispetto ai messaggi di posta elettronica che si ricevono, inoltre si raccomanda di aggiornare immediatamente le soluzioni antivirus e di contare su un buon firewall.

Nota: spesso gli antivirus informano che "non sono in grado di "riparare il file" nel caso di worm o troiani perché realmente non vi è nulla da riparare, semplicemente bisogna cancellare il file.

2. Nel caso in cui non sia possibile eliminare il file del virus, deve terminare manualmente il processo che il virus esegue. Apre Task (premere i tasti Ctrl+Shift+Esc). Nel sistema operativo Windows 98/Me selezioni il nome del processo "SHIMGAPI.DLL" e lo fermi. In Windows 2000/XP, nella linguetta "Processi" preme click destro sul processo "SHIMGAPI.DLL" e selezioni "Termina Processo". Successivamente provi a cancellare o ripristinare il file.

Successivamente si deve modificare il registro per eliminare i cambiamenti realizzati dal virus. **Attenzione! La consigliamo di manipolare il registro con estrema cautela. Se modifica certe chiavi in modo non corretto corre il rischio di inutilizzare il sistema. Quindi, se non è completamente sicuro di poterlo utilizzare correttamente Le raccomandiamo di non modificare il registro.**

Può accedere al registro attraverso il menù "Avvio", "Esegui" digitando poi "regedit", in modo da aprire l'Editor del Registro con una struttura ad albero.



Elimini questi valori dal registro:

Chiave: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
Valore: TaskMon = c:\windows\system\taskmon.exe

Chiave: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
TaskMon: = c:\windows\system\taskmon.exe

Elimini queste chiavi:

HKEY_LOCAL_MACHINE \Software\Microsoft\Windows\CurrentVersion
\Explorer\ComDlg32\Version

HKEY_CURRENT_USER \Software\Microsoft\Windows\CurrentVersion
\Explorer\ComDlg32\Version
sotto la chiave:

HKEY_CLASSES_ROOT\CLSID\
{E6FB5E20-DE35-11CF-9C87-00AA005127ED}\InProcServer32

Ripristini i seguenti valori:

-In Windows 2000/XP:

(Predeterminato)="%SystemRoot%\System32\webcheck.dll"

-In Windows 98/Me:

(Predeterminato)="Windows\System\webcheck.dll"

3. Riavvii il computer e realizzi una scansione di tutto l' hard disk con un antivirus per assicurarsi di aver eliminato il virus. Se ha disattivato il ripristino di configurazione del sistema, ricordi di riattivarlo.

6. MINIMIZZI I DANNI DI UN VIRUS:

1. Se possiede computer connessi in rete, isoli il computer o pc infettato per evitare la propagazione dell'infezione.
2. Sospenda l'accesso ad Internet del computer infettato.
3. Se possiede software antivirus, contatti col suo fornitore e segua le sue indicazioni per la disinfezione.
4. Aggiorni l'antivirus ed installi i patch di sicurezza del suo sistema operativo.
5. Analizzi il resto dei computer della rete, per assicurarsi che non siano stati infettati.
6. Se il virus contiene un Troiano che permette l'accesso esterno di hacker al suo pc, modifichi le password.
7. Se possiede copie di sicurezza o backup recenti, si assicuri che siano libere da virus prima di recuperarle.
8. Analizzi le falle del suo sistema di sicurezza e corregga gli errori che hanno permesso l'infezione.

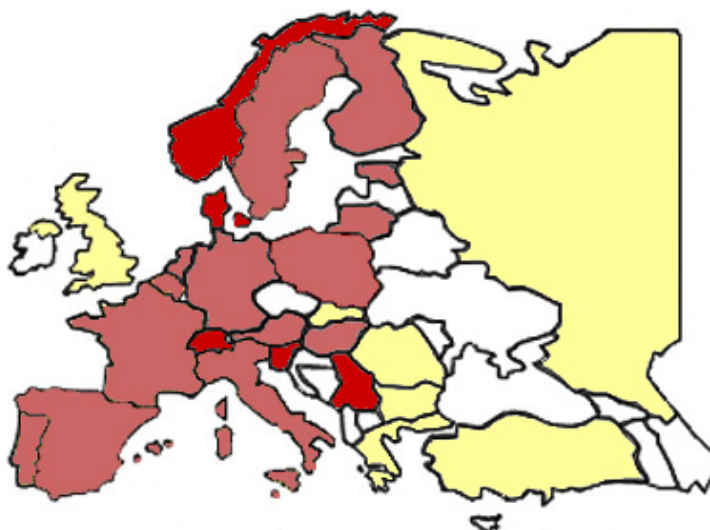


7. ULTERIORI INFORMAZIONI SU VIRUS:

- [Panda Software](http://www.pandasoftware.es/) (http://www.pandasoftware.es/)
- [Trend Micro](http://es.trendmicro-europe.com/) (http://es.trendmicro-europe.com/)
- [Enciclopedia Virus \(Ontinent\)](http://www.enciclopediavirus.com) (http://www.enciclopediavirus.com)
- [McAfee](http://es.mcafee.com) (http://es.mcafee.com)
- [Symantec](http://www.symantec.com/region/es/) (http://www.symantec.com/region/es/)
- [VS Antivirus](http://www.vsantivirus.com) (http://www.vsantivirus.com)
- [Kaspersky \(viruslist.com\)](http://www.viruslist.com/eng/index.html) (http://www.viruslist.com/eng/index.html)
- [Bit Defender](http://www.bitdefender-es.com/) (http://www.bitdefender-es.com/)
- [Sophos](http://esp.sophos.com) (http://esp.sophos.com)
- [Hacksoft](http://www.hacksoft.com.pe) (http://www.hacksoft.com.pe)
- [PerAntivirus](http://www.perantivirus.com/) (http://www.perantivirus.com/)

VIRUS MYDOOM

FEBBRAIO 2004



- □ □ □ □ +

RECOVERY LABS®