



VÍRUS MYDOOM

Apesar de que o vírus Mydoom não produz perda de dados, julgamos oportuno realizar este relatório sobre a sua acção devido à grande repercussão social e à enorme propagação que está a apresentar.

"O verme Mydoom pode vir a converter-se num dos vírus mais nocivos dentre os que se estenderam pela Internet nos últimos meses (1 de cada 6 mensagens de correio foi infectada). Os peritos das companhias antivírus advertiram que o Mydoom se prolifera mais rapidamente que o Sobig F. E o Klez, dois dos vírus mais perigosos de 2003."

1. O QUE É?

O *Mydoom* é um verme que se propaga através do correio electrónico numa mensagem com características variáveis e através do programa de ficheiros compartilhados KaZaA.

Tem capacidades de porta traseira, o que permite que um usuário remoto possa acessar o equipamento infectado.

Realiza ataques de recusa de serviço aplicada contra as páginas *web* www.sco.com e www.microsoft.com.

2. QUE CLASSES HÁ?

Este verme provém do vírus Mimail, vírus sem efeitos daninhos, mas com grande capacidade de propagação através do envio massivo de correios.

Foi identificado pela primeira vez em 26 de Janeiro de 2004, e apresenta-se em duas versões: versão .A e .B, esta última detectada em 28 de Janeiro de 2004.

A nova variante é ainda mais perigosa que a anterior, já que foi desenvolvida para impedir que muitos programas antivírus possam actualizar-se correctamente.

Outra diferença da nova variante, com relação ao Mydoom.A, é que foi desenvolvida para causar ataques de recusa de serviço aplicada contra os servidores da companhia Microsoft, enquanto que a primeira lançava ataques contra a *web* www.sco.com.

NOTA: nas últimas horas, detectou-se a aparição de dois novos vírus relacionados com o Mydoom. Um deles é o Doomjuice.A (W32/Doomjuice.A.worm). Trata-se de um verme que se propaga através da Internet, para tanto utiliza a porta traseira criada pelo Mydoom.A e Mydoom.B com o fim de realizar cópias de si mesmo nos computadores afectados por estes vermes. O Doomjuice.A propaga ataques de Recusa de Serviço Distribuída (DDoS) contra a *web*. O outro é o Deadhat e desinstala as versões do vírus Mydoom que encontre e logo trata de neutralizar a protecção anti-vírus do computador. Ambos, diferentemente do Mydoom original, não viajam por correio electrónico, mas procuram endereços de e-mail em máquinas conectadas infectadas.

3. COMO ACTUA?

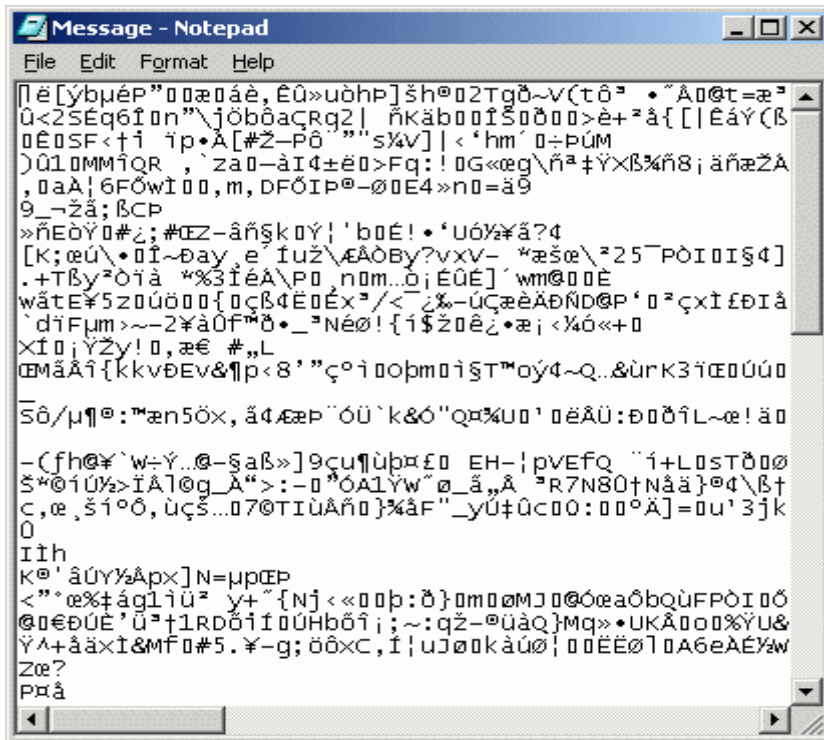
O W32/MyDoom é um verme de e-mail, com um componente de porta traseira, que procura endereços no disco rígido do sistema infectado e os utiliza para se enviar também como remetente, por isso não se sabe de onde procede realmente.

O verme incita o usuário a abrir um ficheiro de programa anexo. O ícone desse ficheiro representa um ficheiro de texto, a fim de enganar o usuário. A surpresa em ambos casos chegará quando o utilizador tem conhecimento que a sua conta se encontra a zeros, e o banco o informa de que foi vítima de um engano denominado Phishing.





Quando se executa pela primeira vez, o verme abre o bloco de papel de notas e mostra caracteres sem sentido, do tipo:



O verme instala o código daninho no sistema e envia-se a si mesmo a todos os contactos da lista de endereços localizados em ficheiros com as seguintes extensões: WAB, TXT, HTM, SHT, PHP, ASP, DBX, TBB, ADB e PL.

Usa mensagens com assuntos, textos e nomes de ficheiros anexos variáveis. A mensagem costuma medir de 30 a 35Kb.

A mensagem pode ter algum dos seguintes assuntos:

- [caracteres sem sentido ou vazio]
- Delivery Error
- Error
- hello
- hi
- Mail Delivery System
- Mail Transaction Failed
- Returned mail
- Server Report
- Status
- Undeliverable: Mail Delivery System



Os ficheiros anexos podem ter algum dos seguintes nomes:

[caracteres sem sentido]

*body
data
doc
document
file
message
readme
test
text*

O texto da mensagem pode ser algum dos seguintes, entre outros gerados ao azar:

Exemplo 1:

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

Exemplo 2:

*Mail transaction failed. Partial message
is available.*

Exemplo 3:

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

Exemplo 4:

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

Exemplo 5:

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

Difusão mediante o KaZaA

Copia-se a si mesmo à pasta partilhada do KaZaa, com os seguintes nomes:

- 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

Desta forma outros usuários do KaZaA podem descarregar o vírus.

INSTALAÇÃO

Quando se executa, cria os seguintes ficheiros no sistema infectado:

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

NOTA : A pasta TEMP está localizada em "c:\windows\temp", "c:\winnt\temp", ou "c:\documents and settings\[usuário]\local settings\temp", de acordo com o sistema operacional.

Em todos os casos, "c:\windows" e "c:\windows\system" podem variar de acordo com o sistema operacional instalado ("c:\winnt", "c:\winnt\system32", "c:\windows\system32", etc.).

E modifica ou cria as seguintes entradas no registo:

```
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
```

Para criar a porta traseira adiciona o ficheiro SHIMGAPI.DLL no directório SYSTEM do Windows, e o executa como um processo filho (child process) do EXPLORER.EXE.

A chave de registo modificada para esta tarefa é a seguinte:

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

O verme Mydoom B. pode além do mais enviar-se a equipamentos já infectados pela versão A. Para tanto, o seu componente backdoor escaneia a rede por endereços IP gerados ao azar, e tenta conectar-se a portas TCP/3127, utilizadas pelo Mydoom. Se a máquina escaneada está infectada, então o Mydoom transfere-se a ela e é executado imediatamente. Desse modo os computadores infectados são actualizados à nova versão sem necessidade de receber um novo correio com o verme.



EFEITOS

1. O verme procura endereços de correio electrónico em todos os ficheiros com as seguintes extensões (WAB, TXT, HTM, SHT, PHP, ASP, DBX, TBB, ADB e PL), reenviando-se automaticamente;
2. Abre um troiano de acesso por porta traseira nas máquinas infectadas permitindo que um possível intruso controle o equipamento infectado de forma remota;
3. O verme realiza ataques de recusa de serviço aos seguintes endereços:

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

Estes ataques consistem no envio de rajadas de petições GET HTTP. Ambos os ataques se realizam de forma simultânea.

No dia 1 de Março de 2004, prevê-se que o Mydoom deixe de propagar-se, mas a sua rotina backdoor continuará a funcionar

4. COMO ELIMINÁ-LO?

1. Aconselha-se aumentar as precauções com as mensagens de correio electrónico recebidas, assim como actualizar o antes possível as soluções antivírus e contar com um bom Firewall.

Nota: frequentemente os antivírus informam que 'não pode reparar um ficheiro' no caso de vermes ou troianos devido ao facto de que não há nada que reparar, simplesmente terá que eliminar o ficheiro;

2. No caso de que não se possa eliminar o ficheiro do vírus, deve-se terminar manualmente o processo em execução do vírus. Abra o Administrador de tarefas (pressione Control+Maiúsculas+Esc). No Windows 98/Me seleccione o nome do processo "SHIMGAPI.DLL" e detenha-o. No Windows 2000/XP, em 'Processos' clique com o botão direito no processo "SHIMGAPI.DLL" e seleccione 'Terminar Processo'. A seguir, volte a tentar a sua eliminação ou a reparação do ficheiro.

A seguir, terá de editar o registo para desfazer as mudanças realizadas pelo vírus. **Seja extremamente cuidadoso ao manipular o registo. Se modificar certas chaves de maneira incorrecta pode deixar o sistema inutilizável. Por isso recomendamos que se não estiver completamente seguro de como utilizá-lo correctamente, não modifique o registo.**

Pode acessar o registo através do menu Início, Executar e teclar "regedit", então se abrirá o editor com uma estrutura em árvore.

Elimine os seguintes valores do registo:

Chave: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

Valor: TaskMon = c:\windows\system\taskmon.exe



Chave: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

TaskMon: = c:\windows\system\taskmon.exe

Elimine as seguintes chaves:

HKEY_LOCAL_MACHINE \Software\Microsoft\Windows\CurrentVersion

\Explorer\ComDlg32\Version

HKEY_CURRENT_USER \Software\Microsoft\Windows\CurrentVersion

\Explorer\ComDlg32\Version

Sob a seguinte chave:

HKEY_CLASSES_ROOT\CLSID\

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

5. MINIMIZE OS DANOS DE UM VÍRUS:

1. Se possuir computadores conectados em rede, isole o computador ou PC infectado para que a infecção não se propague;
2. Suspenda o acesso à Internet do computador infectado;
3. Se possuir software antivírus, contacte o seu fornecedor e siga as indicações para a sua desinfecção;
4. Actualize o antivírus e instale os sistemas de segurança do seu sistema operacional;
5. Analise o resto dos equipamentos da rede, se por acaso foram infectados;
6. Se o vírus contiver um Troiano que permite o acesso externo de hackers ao seu equipamento, troque as contra-senhas;
7. Se possuir cópias de segurança ou backups recentes, assegure-se de que estão livres de vírus antes de recuperá-los;
8. Analise as falhas do seu sistema de segurança e corrija os erros que permitiram a infecção.



6. MAIS INFORMAÇÃO SOBRE VÍRUS:

- (<http://www.pandasoftware.es/>)
- (<http://es.trendmicro-europe.com/>)
- (<http://www.enciclopediavirus.com>)
- (<http://es.mcafee.com>)
- (<http://www.symantec.com/region/es/>)
- (<http://www.vsantivirus.com>)
- (<http://www.viruslist.com/eng/index.html>)
- (<http://www.bitdefender-es.com/>)
- (<http://esp.sophos.com>)
- (<http://www.hacksoft.com.pe>)
- (<http://www.perantivirus.com/>)