



VIRUS MYDOOM

Obwohl der Mydoom Virus keine Datenverluste auslöst, haben wir es dennoch für richtig befunden, einen Bericht über seine Aktion anzufertigen, da er so grosses Gesellschaftliches Echo hervorrief und so weit verbreitet ist.

"Der Wurm Mydoom ist auf dem Wege, einer der schädlichsten zu werden, die sich in den letzten Monaten über das Internet verbreitet haben (1 von 6 Emails ist infiziert) Die Experten der Antivirusfirmen haben gewarnt, dass Mydoom sich schneller verbreitet als Sobig F. Und Klez, zwei der gefährlichsten Viren des Jahres 2003."

1. WAS IST ES?

Mydoom ist ein Wurm, der sich durch die Email in einer Botschaft variabler Merkmale und durch das Programm des Dateienaustauschs KaZaA verbreitet.

Er hat eine Back-Orifice-Fähigkeit, wodurch ein entfernter Benutzer sich Zugang zu dem infizierten Gerät verschaffen kann.

Er führt Dienstverweigerungsangriffe gegen die Websites www.sco.com und www.microsoft.com durch.

2. WAS FÜR ARTEN GIBT ES?

Dieser Wurm kommt vom Virus Mimail, ein Virus ohne schädliche Effekte, aber mit grosser Verbreitungskraft durch das massive Aussenden von Email.

Er wurde erstmalig am 26. Januar 2004 identifiziert und es gibt ihn in zwei Versionen: Version A und B, diese letzte wurde am 28. Januar 2004 entdeckt.

Die neue Variante ist noch gefährlicher als die vorige, die entworfen wurde, um die Aktualisierung vieler Antivirusprogramme zu verhindern.

Ein weiterer Unterschied der neuen Variante gegenüber dem Mydoom.A. ist, dass er zum Dienstverweigerungsangriff gegen die Server der Firma Microsoft entworfen wurde, während der erste Angriffe gegen die Website www.sco.com lancierte.

BEMERKUNG: In den letzten Stunden wurden zwei neue, mit dem Mydoom verbundene Viren entdeckt. Einer von ihnen ist der Doomjuice A (W32/Doomjuice.A.worm). Es handelt sich um einen Wurm, der sich über das Internet verbreitet und hierzu die von Mydoom A und B geschaffene Backdoor benutzt, und so Kopien seiner selbst in den von diesen Viren befallenen Computern macht. Doomjuice A führt Angriffe zur Verweigerung von Service (DDoS – Distributed Denial of Service) gegen die Website www.microsoft.com durch. Der andere ist Deadhat, der die gefundenen Versionen des Mydoom Virus desinstalliert und dann versucht, den Antivirusschutz des Computers zu neutralisieren. Im Gegensatz zum Original-Mydoom reisen beide nicht durch die Email, sondern sie suchen Emailadressen in den infizierten, angeschlossenen Computern.

3. WIE FUNKTIONIERT ER?

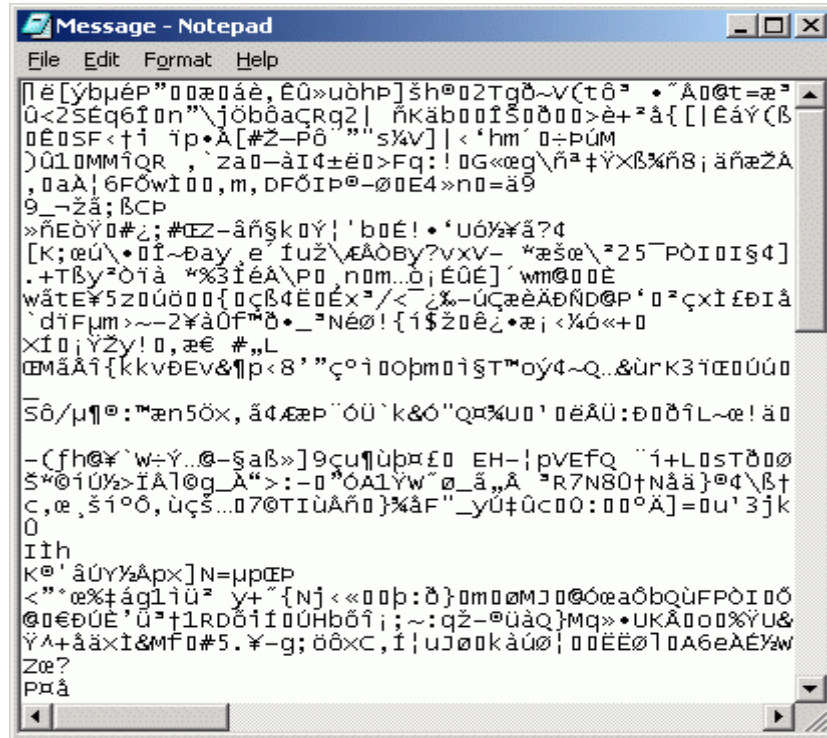
W32/MyDoom ist ein Email Wurm, mit dem Back Orifice Komponenten, der Emailadressen auf den infizierten Computern sucht und diese nutzt, um sich selbst als Absender zu senden, weswegen es schwer ist, herauszufinden, woher er zuerst kam.

Der Wurm bewegt den Benutzer dazu, einen Dateianhang zu öffnen. Der Anhang stellt einen

Texticon dar, um den Benutzer zu täuschen.



Wenn er sich zum ersten Mal ausführt, öffnet der Wurm den Notizblock und zeigt eine Serie sinnloser Schriftzeichen, dieser Art:



Der Wurm installiert den schädlichen Code im System und sendet sich selbst an alle Adressen der Adressbücher, die sich in Dateien mit folgenden Endungen befinden: WAB, TXT, HTM, SHT, PHP, ASP, DBX, TBB, ADB und PL

Es benutzt eine Nachricht mit Betreff, Texten und Namen von verschiedenen Dateianhängen. Die Nachricht hat eine Grösse von 30 bis zu 35 Kb.

Die Nachricht kann einen der folgenden Betreffe aufweisen:

- sinnlose Schriftzeichen oder Leer]*
- Delivery Error*
- Error*
- hello*
- hi*
- Mail Delivery System*
- Mail Transaction Failed*
- Returned mail*
- Server Report*
- Status*
- Undeliverable: Mail Delivery System*



Die Dateianhänge können einen der folgenden Namen aufweisen:

[sinnlose Schriftzeichen]
body
data
doc
document
file
message
readme
test
text

Der Text kann, unter anderen frei erfundenen, einer der folgenden sein:

Beispiel 1:

sendmail daemon reported
Error #804 occured during SMTP session.
Partial message has been received.

Beispiel 2:

Mail transaction failed. Partial message
is available.

Beispiel 3:

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

Beispiel 4:

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

Beispiel 5:

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

Verbreitung durch KaZaA

Er kopiert sich selbst in den shared files folder der KaZaA, mit folgenden Namen:

- 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-2.0bdcom_patches.bat
- strip-girl-2.0bdcom_patches.pif
- strip-girl-2.0bdcom_patches.scr
- winamp5.bat
- winamp5.pif
- winamp5.scr



Auf diese Art können andere Benutzer des KaZaA Programms den Virus herunterladen.

Installierung

Bei seiner Ausführung, erstellt er die folgenden Dateien im infizierten System:

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

BEMERKUNG: Das Verzeichnis Temp ist in "c:\windows\temp", "c:\winnt\temp", oder "c:\documents and settings\[user]\local settings\temp", je nach Betriebssystem.

In allen Fällen kann "c:\windows" y "c:\windows\system" je nach installiertem Betriebssystem verschieden sein ("c:\winnt", "c:\winnt\system32", "c:\windows\system32", usw.).

Und er verändert oder schafft die folgenden Einträge im Register:

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

Um eine Backdoor oder Back Orifice zu schaffen, legt er die Datei SHIMGAPI.DLL im Verzeichnis SYSTEM von WINDOWS an, und führt es als eine Tochterfunktion (child process) von EXPLORER.EXE. aus

Der für diese Aufgabe veränderte Registereintrag ist der folgende:

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

Der Wurm Mydoom B kann sich zusätzlich an bereits mit Version A infizierte Computer versenden. Hierzu durchsucht sein Backdoorkomponent das Netz nach frei kreierten IP Adressen und versucht, sich mit Ports oder Schnittstellen TCP/3127, die von Mydoom benutzt werden, in Verbindung zu setzen. Wenn der durchsuchte Computer infiziert ist, überträgt Mydoom sich auf diesen und wird sofort ausgeführt. Auf diese Art werden die Viren auf den infizierten Computern mit der neuesten Version aktualisiert, ohne dass eine erneute, infizierte Email empfangen werden müsste.



Auswirkungen

1. Der Wurm durchsucht alle Verzeichnisse mit den Endungen (: WAB, TXT, HTM, SHT, PHP, ASP, DBX, TBB, ADB und PL) nach Emailadressen und versendet sich dann automatisch an diese.
2. Er schafft einen Trojanischen Zugang mit Backdoor in den infizierten Computern, womit es sogar ermöglicht wird, dass Eindringlinge den Computer fernsteuern können.
3. Der Wurm führt Serviceverweigerungsangriffe auf folgende Adressen durch:

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

Die Angriffe bestehen aus der Versendung von Salven von GET HTTP Anträgen. Beide Angriffe erfolgen simultan.

Es wird vorgesehen, dass der Mydoom am 1. März 2004 aufhört, sich zu verbreiten, aber seine Backdoor Methode funktioniert weiter.

4. WIE BESEITIGT MAN IHN?

1. Es wird geraten, die Vorsicht mit Emailnachrichten zu verschärfen, sowie den Antivirus baldmöglichst zu aktualisieren und eine gute Firewall zu haben.

Bemerkung: Häufig teilen die Antivirusprogramme mit, dass sie eine Datei nicht reparieren konnten, im Falle von Würmern und Trojanern ist nichts zu reparieren. In diesen Fällen ist lediglich die Datei zu löschen.

2. Falls die Virusdatei nicht gelöscht werden kann, muss ihre Ausführung per Hand beendet werden. Öffnen sie den Task Manager (Tasten Control + Shift + Del). In Windows 98 wählen Sie den Namen des Vorgangs "SHIMGAPI.DLL" und stoppen Sie ihn. In Windows 2000/XP, in der Mappe „Vorgänge“ klicken Sie mit dem rechten Mausknopf auf den Vorgang "SHIMGAPI.DLL" und wählen Sie ‚Vorgang beenden‘. Dann können Sie die Löschung oder Reparatur der Datei erneut versuchen.

Dann muss das Register editiert werden, um die darin vorgenommenen Veränderungen rückgängig zu machen. **Seien Sie bei Änderungen im Register extrem vorsichtig. Wenn Sie gewisse Codes falsch ändern, könnten Sie das System lahmlegen. Daher raten wir, das Register nicht zu verändern, wenn Sie nicht vollkommen sicher sind, es richtig zu tun.**

Sie können das Register durch das Menü Start, Run und dann „regedit“ öffnen, und der Editor wird in Form eines Verzeichnisbaums geöffnet.

Löschen Sie folgende Einträge aus dem Register:

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

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

Löschen Sie folgende Codes:

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

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



Unter folgendem Code:

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

Restaurieren Sie folgende Codes:

- In Windows 2000/XP:
(Vorgegeben)="%SystemRoot%\System32\webcheck.dll"

- In Windows 98/ME:
(Vorgegeben)="Windows\System\webcheck.dll"

3. Starten Sie Ihren Computer erneut und untersuchen Sie die ganze Festplatte mit einem Antivirusprogramm, um sicher zu sein, den Virus gelöscht zu haben. Wenn Sie die Restaurierung des Systems abgestellt haben, erinnern Sie, diese wieder zu aktivieren.

5. VERRINGERN SIE DIE SCHÄDEN EINES VIRUS:

1. Wenn Sie im Netz arbeitende Computer haben, isolieren Sie den infizierten Computer oder PC, damit die Infizierung nicht verbreitet wird.
2. Unterbrechen Sie den Internetzugang des infizierten Computers.
3. Wenn Sie eine Antivirus Software haben, setzen Sie sich mit dem Hersteller in Verbindung und befolgen Sie seine Anweisungen zur Reinigung.
4. Aktualisieren Sie den Antivirus und installieren Sie die Sicherheitspatches für ihr Betriebssystem.
5. Analysieren Sie den Rest der vernetzten Geräte, falls diese infiziert wurden.
6. Wenn der Virus einen Trojaner enthält, der Hackern den Zugang zu ihrem Computer ermöglicht, wechseln Sie die Passwörter.
7. Wenn Sie über neuere Sicherheitskopien oder Back Ups verfügen, überprüfen Sie, dass diese virusfrei sind, bevor sie sie benutzen.
8. Analysieren Sie die Sicherheitsfehler ihres Computers und beheben Sie die Fehler, die die Infizierung ermöglichten.

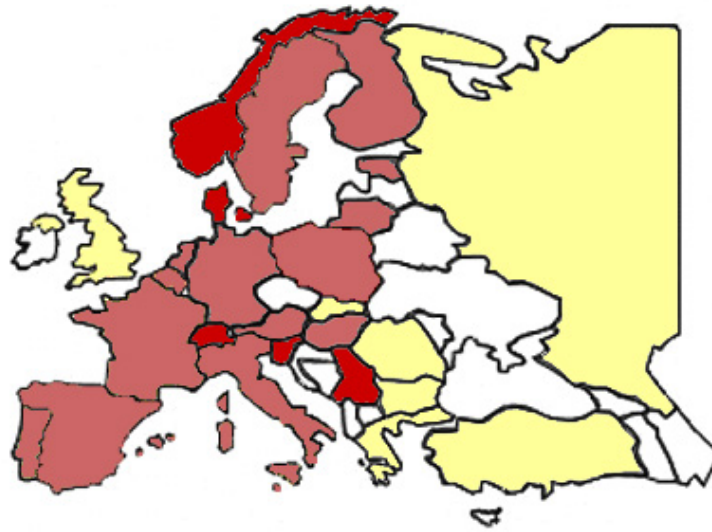
MEHR INFORMATIONEN ÜBER VIREN:

- [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

Febrero 2004



- □ □ □ □ +

RECOVERY LABS®

Virus Mydoom
Februar 2004