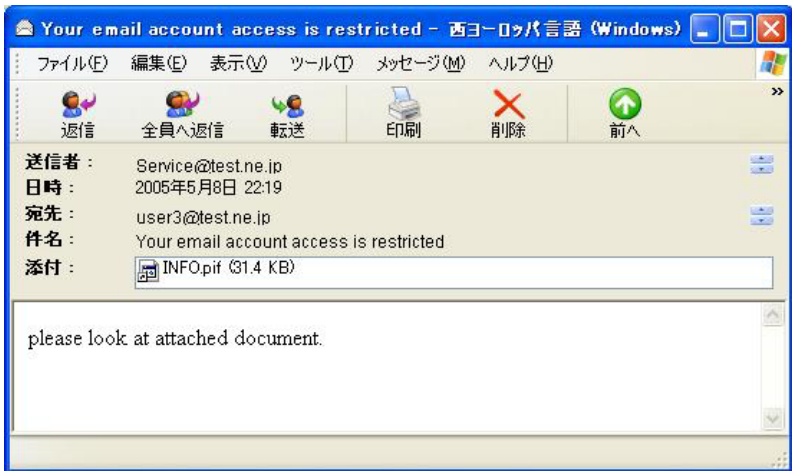


## ウイルス解析報告書

ウイルス名	W32.Mydoom.BO@mm (別名: Net-Worm.Win32.Mytob.au [Kaspersky Lab], W32/Mytob.gen@MM [McAfee], W32/Mytob-BC [Sophos], W32/Mytob-CF [Sophos], WORM_MYTOB.EC [Trend Micro], WORM_MYTOB.ED [Trend Micro])
プログラム名及び容量 (添付ファイル名)	プログラム名: 1hellbot.exe 容 量: 31,358 バイト
種別	ワーム
プログラム言語	C++
発症環境	Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows XP
発見日	2005 年 5 月 8 日
発見場所	アメリカ合衆国
危険性	感染力が高い。危険度は 5 段階の 2 (5 が最も危険)。
発症条件	ワームによって送信されたメールの添付ファイルを実行したとき。
ウイルスの活動、影響	このワームは、独自の SMTP エンジンを使用して自分自身を送信する大量メール送信ワームである。感染したコンピュータから収集したメールアドレスに対してメールを送信する。また、IRC チャンネルに接続し、攻撃者の命令を待つ。
被害の規模	発見から 4 日間で 179 件の届出がシマンテック社に寄せられている。
亜種、変種の有無	W32.Mydoom.A@mm (2004 年 1 月 27 日発見) 以後多数の亜種が存在する。
ウイルスの動作概要	<p>ワームにより送信されるメールには、次の特徴がある。</p> <div style="text-align: center;">  </div> <p><b>差出人:</b> 次のいずれかを使用する。ただし、ワームはコンピュータ内のファイルから収集したメールアドレスを元にして、メールアドレスを詐称する場合もある。</p> <ul style="list-style-type: none"> <li>・john</li> <li>・alex</li> <li>・michael</li> <li>・james</li> <li>・mike</li> <li>・kevin</li> <li>・david</li> <li>・george</li> <li>・sam</li> <li>・andrew</li> </ul>

·jose  
·leo  
·maria  
·jim  
·brian  
·serg  
·mary  
·ray  
·tom  
·peter  
·robert  
·bob  
·jane  
·joe  
·dan  
·dave  
·matt  
·steve  
·smith  
·stan  
·bill  
·jack  
·fred  
·ted  
·adam  
·brent  
·alice  
·anna  
·brenda  
·claudia  
·debby  
·helen  
·jerry  
·jimmy  
·julie  
·linda  
·sam

**件名:**

次のいずれかを使用する。

·Notice: **\*\*Last Warning\*\***  
·Your email account access is restricted  
·Your Email Account is Suspended For Security Reasons  
·Notice:**\*\*\*Your email account will be suspended\*\*\***  
·Security measures  
·Email Account Suspension  
·**\*IMPORTANT\*** Please Validate Your Email Account  
·**\*IMPORTANT\*** Your Account Has Been Locked

**本文:**

次のいずれかを使用する。

·Once you have completed the form in the attached file , your account records will not be interrupted and will continue as normal.  
·To unblock your email account acces, please see the attachement.  
·Please see the attachement.

- We have suspended some of your email services, to resolve the problem you should read the attached document.
- To safeguard your email account from possible termination, please see the attached file.
- please look at attached document.
- Account Information Are Attached!

**添付ファイル:**

添付ファイル名は次のいずれかを使用する。

- email-doc
- email-info
- email-text
- information
- your\_details
- document\_full
- INFO
- IMPORTANT
- info-text

添付ファイルの拡張子は次のいずれかを使用する。

- .pif
- .scr
- .exe
- .cmd
- .bat
- .zip

このワームが実行されると、次のことを行う。

1. コンピュータ上でワームが複数同時に実行することを防ぐため、次のミュートックスを作成する。  
H-e-l-l-B-o-t-3-!!!
2. hosts ファイルに次のテキストを追加し、複数のセキュリティ関連の Web サイトへのアクセスを遮断する。

```
127.0.0.1 www.symantec.com
127.0.0.1 securityresponse.symantec.com
127.0.0.1 symantec.com
127.0.0.1 www.sophos.com
127.0.0.1 sophos.com
127.0.0.1 www.mcafee.com
127.0.0.1 mcafee.com
127.0.0.1 liveupdate.symantecliveupdate.com
127.0.0.1 www.viruslist.com
127.0.0.1 viruslist.com
127.0.0.1 viruslist.com
127.0.0.1 f-secure.com
127.0.0.1 www.f-secure.com
127.0.0.1 kaspersky.com
127.0.0.1 kaspersky-labs.com
127.0.0.1 www.avp.com
127.0.0.1 www.kaspersky.com
127.0.0.1 avp.com
127.0.0.1 www.networkassociates.com
127.0.0.1 networkassociates.com
127.0.0.1 www.ca.com
```

```

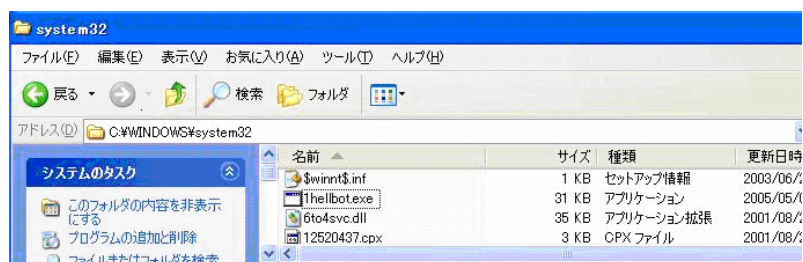
127.0.0.1 ca.com
127.0.0.1 mast.mcafee.com
127.0.0.1 my-etrust.com
127.0.0.1 www.my-etrust.com
127.0.0.1 download.mcafee.com
127.0.0.1 dispatch.mcafee.com
127.0.0.1 secure.nai.com
127.0.0.1 nai.com
127.0.0.1 www.nai.com
127.0.0.1 update.symantec.com
127.0.0.1 updates.symantec.com
127.0.0.1 us.mcafee.com
127.0.0.1 liveupdate.symantec.com
127.0.0.1 customer.symantec.com
127.0.0.1 rads.mcafee.com
127.0.0.1 trendmicro.com
127.0.0.1 www.trendmicro.com
127.0.0.1 www.grisoft.com
127.0.0.1 www.microsoft.com

```

==Copyright (C) 2005-2006 HellBot3 Team All Rights Reserved.==



### 3. ワーム自身を%System%¥1hellbot.exe としてコピーする。



Windows のシステムフォルダ%System% (標準では、C:¥Windows¥System、C:¥Winnt ¥System32、または C:¥Windows¥System32)

- Windows の起動時にワームを実行させるため、次のレジストリキーに
  - ・HKEY\_LOCAL\_MACHINE¥Software¥Microsoft¥Windows¥CurrentVersion¥Run
  - ・HKEY\_LOCAL\_MACHINE¥Software¥Microsoft¥Windows¥CurrentVersion ¥RunServices
 次の値を追加する。  
 "HELLBOT TEST"="1hellbot.exe"



5. 特定のプロセスを停止する。

- ・regedit.exe
- ・msconfig.exe
- ・cmd.exe
- ・taskmgr.exe
- ・netstat.exe
- ・zapro.exe
- ・navw32.exe
- ・navapw32.exe
- ・zonealarm.exe
- ・wincfg32.exe
- ・PandaAVEngine.exe

6. Windows アドレス帳及び、次のフォルダからメールアドレスを収集する。

- ・%Windir%\Temporary Internet Files
- ・%UserProfile%\Local Settings\Temporary Internet Files
- ・%System%

Windows のインストールフォルダ%Windir%(標準では、C:\Windows または C:\Winnt)  
 カレントユーザのプロファイルフォルダ%UserProfile%(標準では、C:\Documents and  
 Settings\<カレントユーザ名>)

7. Cドライブから Yドライブ内の、次の拡張子のファイルからメールアドレスを収集する。  
 注意: \*は任意の 1 文字を示す。

- ・htm\*
- ・sht\*
- ・php\*
- ・asp\*
- ・dbx\*
- ・tbb\*
- ・adb\*
- ・wab\*
- ・pl
- ・txt

8. 収集したメールアドレスに対して、独自の SMTP エンジンを使用しメールを送信する。

9. 特定の IRC サーバの TCP ポート 6667 に接続し、IRC チャンネルに接続する。これによ  
 り、攻撃者は感染したコンピュータに対して次の操作を実行できる。

- ・ファイルのダウンロード及び実行
- ・指定された他の IRC コマンドを実行
- ・コンピュータを再起動

<b>感染・発症防止方法</b>	<ol style="list-style-type: none"> <li>1. 予期せぬメールが届いた場合には、安易に開封したり、添付ファイルを開かない。特に「ウイルスの動作概要」で記述したようなメールには注意する。</li> <li>2. インターネットからダウンロードしたファイルについては、必ずウイルススキャンを実行し、問題がないことが確認できるまでは絶対に起動しない。</li> </ol>
<b>ウイルスの駆除方法</b>	<p>手動による修復を行う場合、コンピュータに関する高度な知識が必要とされ、間違えるとコンピュータが正常に起動しなくなる場合もある。</p> <ol style="list-style-type: none"> <li>1. 被害拡大防止のため、感染したコンピュータをネットワークから切り離す。</li> <li>2. システムの復元オプションを無効にする。(Windows Me/XP)</li> <li>3. コンピュータをセーフモード(WindowsNT では VGA モード)で再起動する。</li> <li>4. 次のファイルを削除する。 %System%¥1hellbot.exe</li> <li>5. レジストリに行われた変更を元に戻す。 次のレジストリキーから HKEY_LOCAL_MACHINE¥Software¥Microsoft¥Windows¥CurrentVersion¥Run 次の値を削除する。 "HELLBOT TEST"="1hellbot.exe" 次のレジストリキーから HKEY_LOCAL_MACHINE¥Software¥Microsoft¥Windows¥CurrentVersion ¥RunServices 次の値を削除する。 "HELLBOT TEST"="1hellbot.exe"</li> </ol> <p>各操作については Microsoft のホームページ、付属のマニュアル等を参照すること。 無償修復ツールがワクチンベンダーから提供されているので、使用上の注意をよく読み使用すること。</p>
<b>その他</b>	平成 17 年末現在で 438 件(国内 53 件)の届出がシマンテック社に寄せられている。