

ウイルス解析報告書

ウイルス名	W32.Mydoom.A@mm (別名: W32.Novarg.A@mm[Symantec], W32/Mydoom@MM [McAfee], WORM_MIMAIL.R [Trend], Win32.Mydoom.A [Computer Associates], W32/Mydoom-A [Sophos], I-Worm.Novarg [Kaspersky])
プログラム名及び容量 (添付ファイル名)	プログラム名 taskmon.exe (添付ファイル名は不定 (添付ファイルの拡張子は、.pif、.scr、.exe、.cmd、.bat、あるいは .zip のいずれか) 容 量 22,528 バイト
種 別	ワーム
プログラム言語	不明
発 症 環 境	Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows XP
発 見 日 時	2004年1月27日
発見場所 (発信地)	アメリカ (最初の感染報告)
危 険 性	感染したコンピュータにバックドアを仕掛け、任意のファイルをダウンロードしたり実行したりすることが可能となる。また、特定のWebサイトに対して DoS 攻撃も行うため非常に危険である。危険度は5段階の4 (6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開いたとき
ウイルスの活動、影響	大量メール送信型ワーム。拡張子が .bat、.cmd、.exe、.pif、.scr、.zip の添付ファイルを伴って届く 感染すると TCP ポート3127 ~ 3198 番のいずれかをバックドアに利用する。これは、攻撃者が感染したコンピュータへ接続すること及び、感染したコンピュータをプロキシとして利用し (コンピュータの接続されている) ネットワーク・リソースへアクセスすることを可能にする。このバックドアは、任意のファイルをダウンロードし、実行することが可能である。 このワームは、2004年2月1日に「www.sco.com」に対しDoS 攻撃を開始し、2004年2月12日に攻撃を停止するが、バックドアはそのまま機能する。
被 害 規 模	発見から3時間で256件 (国内は0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	無
ウイルスの動作概要	<p>ワームによって送信されるメールには次のような特徴がある。</p> <p>差出人: 詐称している可能性がある。</p> <p>題 名:</p> <ul style="list-style-type: none"> • test 又は Test • hi 又は Hi • hello 又は Hello • Mail Delivery System • Mail Transaction Failed • Server Report • Status • Error 等 <p>本 文:</p> <ul style="list-style-type: none"> • Mail transaction failed. Partial message is available. • The message contains Unicode characters and has been sent as a binary attachment. • The message cannot be represented in 7-bit ASCII encoding and has been sent as a binary attachment. 等 <p>メールの中には意味不明なものもある。</p>

添付ファイル名: (次のうちのいずれか)

- document
- readme
- doc
- text
- file
- data
- test
- message
- body

が使用され、拡張子には次のものが使用される。

- .pif
- .scr
- .exe
- .cmd
- .bat
- zip (なお、拡張子が zip の場合、worm のヘッダ部分、フッタ部分に zip 形式のヘッダ、フッタを追加するため、若干ファイルサイズが大きくなる)

また、2重拡張子となっている場合もあり、その場合1つ目の拡張子は、

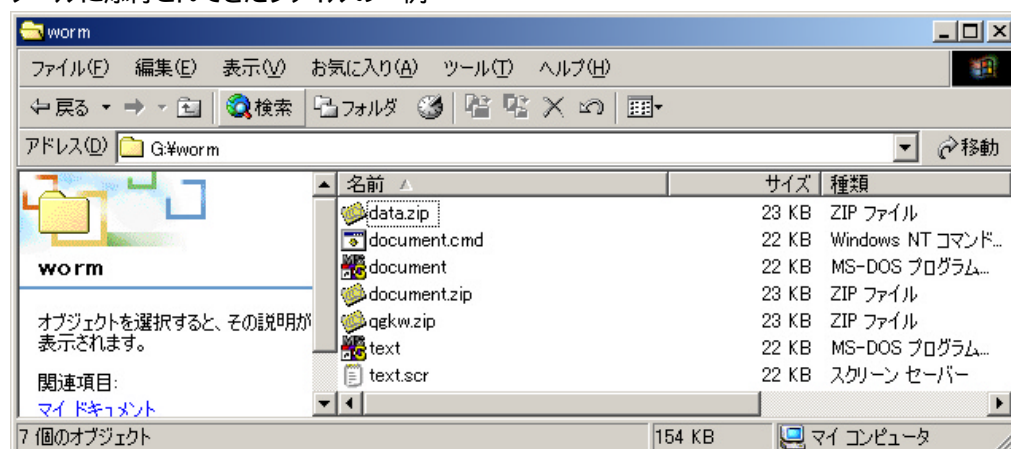
- .htm
- .txt
- .doc

となる。

フォームが ".exe" あるいは ".scr" の拡張子を持つ場合、普段テキストファイルを表すために使用されているアイコンを表示する。



その他の場合、アイコンは次のように表示される。

**メールに添付されてきたファイルの一例**

ワームが実行されると次のような動作を行う

1. 次のファイルを作成する。

- %System%\Shimgapi.dll

このファイルは、プロキシサーバとして動作するバックドアプログラムで、TCP ポート 3127 ~ 3198 番のいずれかを使用したバックドアを作成し待機する。このバックドアは、任意のファイルをダウンロードし、実行することが可能である。このファイルは、UPX で圧縮された実行形式プログラムである。

- %Temp%\Message

このファイルは、ランダムな文字を含んでおり、Notepad を起動して表示する。最初にワームが実行された場合、notepad.exe が %Temp%\Message を表示する。

- %System%\Taskmon.exe

%System% フォルダに作成されるこのファイルは、ワーム本体であり UPX で圧縮されている。

Taskmon.exe は、Windows 95/98/Me オペレーティングシステム環境下において正規のファイルであり %Windir% フォルダ(標準では C:\Windows あるいは C:\Winnt)に格納されている。%Windir% フォルダに格納されている正規のファイルを削除しないよう注意する必要がある。

%System% フォルダは不定。標準設定では C:\Windows\System(Windows95/98/Me)、C:\Winnt\System32 (Windows NT/2000)、あるいは C:\Windows\System32 (Windows XP)。

2. 次の値を

"(標準)" = "%System%\shimgapi.dll"

次のレジストキーに追加する。

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

これにより、EXPLORER.exe が Shimgapi.dll をロードしバックドアを作成する。

3. 次の値を

TaskMon = %System%\taskmon.exe

次のレジストキーに追加する。

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

これにより、Windows を起動する際に ワームの本体である taskmon.exe が実行される。

4. HTTP の GET リクエストを送信する 64 のスレッドを作成し、www.sco.com に対して DoS 攻撃を試みる。(ポート80番に直接接続する。)

DoS 攻撃が実施されるのは、協定世界時間で2004年2月1日午後4時9分18秒(日本時間2月2日午前1時9分18秒)から2004年2月12日までである。

5. 次のレジストキーを作成する。

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

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

6. 次の拡張子を持つファイル内の電子メールアドレスを検索し、抽出する。

- .htm
- .sht
- .php
- .asp

- .dbx
- .tbb
- .adb
- .pl
- .wab
- .txt

抽出されたメールアドレスは、偽装に使用され、ユーザ名とドメイン名を分割し組み合わせて新しくメールアドレスを作成することもある。

7. ワーム自身を持つ SMTP エンジンを利用して電子メールの送信を試みる。電子メールを送信する前に、受取人が使用するメールサーバを調査する。調査に失敗した場合、代替手段としてローカルのメールサーバを使用する。

次の文字列を含むドメインに対しては、電子メールの送信を行わない。

- avp
- syma
- icrosoft
- msn.
- hotmail
- panda
- sopho
- borlan
- inpris
- example
- mydomai
- nodomai
- ruslis
- .gov
- gov.
- .mil
- foo.
- berkeley
- unix
- math
- bsd
- mit.e
- gnu
- fsf.
- ibm.com
- google
- kernel
- linux
- fido
- usenet
- iana
- ietf
- rfc-ed
- sendmail
- arin.
- ripe.
- isi.e
- isc.o

- secur
- acketst
- pgp
- tanford.e
- utgers.ed
- mozilla

次の文字列と一致するアカウントに対しても、電子メールの送信を行わない。

- root
- info
- samples
- postmaster
- webmaster
- noone
- nobody
- nothing
- anyone
- someone
- your
- you
- me
- bugs
- rating
- site
- contact
- soft
- no
- somebody
- privacy
- service
- help
- not
- submit
- feste
- ca
- gold-certs
- the.bat
- page

次の文字列を含むアカウントに対しても、電子メールの送信を行わない。

- admin
- icrosoft
- support
- ntivi
- unix
- bsd
- linux
- listserv
- certific
- google
- account

ワームは、メールアドレスを作成するためにあらかじめ次の文字列を準備している。

ユーザ名として

- john
- alex
- michael
- james
- mike
- kevin
- david
- george
- sam
- andrew
- jose
- leo
- maria
- jim
- brian
- serg
- mary
- ray
- tom
- peter
- robert
- bob
- jane
- joe
- dan
- dave
- matt
- steve
- smith
- stan
- bill
- bob
- jack
- fred
- ted
- adam
- brent
- alice
- anna
- brenda
- claudia
- debby
- helen
- jerry
- jimmy
- julie
- linda
- sandra

ドメイン名として

- hotmail.com

	<ul style="list-style-type: none"> • yahoo.com • mcn.com • aol.com <p>8. 自身を KaZaA ダウンロードディレクトリに、次のいずれかのファイル名でコピーする。</p> <ul style="list-style-type: none"> • winamp5 • icq2004-final • activation_crack • strip-girl-2.0bdcom_patches • rootkitXP • office_crack • nuke2004 <p>拡張子は、次のいずれかになる。</p> <ul style="list-style-type: none"> • pif • scr • bat • exe <p>9. ワームは、起動時にミュートックスを使い、2重起動を防ぐ。</p> <p>10. 初めてワームが実行された場合、notepad.exe が無意味な文字列を表示する場合がある。</p> <p>11. ワームが使用するレジストリ名、URL、ファイル名などの文字列のいくつかはシーザー暗号により暗号化されている。</p>
感染・発症防止方法	<p>1. ワームは、送信者を巧みに詐称しており、添付ファイルを開いたときに動作するため、拡張子が2重拡張子である添付ファイルは安易に開封しない。</p> <p>2. 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。</p>
ウイルスの駆除方法	<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がある。</p> <ol style="list-style-type: none"> 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。 2. システムの復元オプションを無効にする。(Windows Me/XP) 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。 4. 感染ファイルを削除する。 <ul style="list-style-type: none"> %System%\%Shimgapi.dll %Temp%\%Message %System%\%Taskmon.exe KaZaA ダウンロードディレクトリの感染ファイルを削除する。 5. 次の変更されたレジストリを戻す。 <ul style="list-style-type: none"> 次のレジストリキー HKEY_CLASSES_ROOT\CLSID\{E6FB5E20-DE35-11CF-9C87-00AA005127ED}\InProcServer32 次の値を削除する。 (標準) = "%System%\%shimgapi.dll" 次のレジストリキー HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

	<p>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run 次の値を削除する。 TaskMon = %System%\taskmon.exe</p> <p>6. webcheck.dll ファイルを登録し直す。 [スタート] ボタンを押し、[ファイル名を指定して実行] をクリックします。([ファイル名を指定して実行] ダイアログボックスが表示されます。) 次のテキストを入力するか、あるいは、コピー & ペーストします。 regsvr32 webcheck.dll [OK] をクリックします。"DllRegisterServer in webcheck.dll succeeded" というメッセージが表示されたら、[OK] をクリックします。</p> <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。</p> <p>無償修復ツールがワクチンベンダーから配布されているので、使用上の注意をよく読み自己責任において使用すること。</p>
その他	無