

;) [送信者]
 •God Jul!
 ;) [送信者]
 •God Jul!
 ;) [送信者]
 •Iloista Joulua!
 ;) [送信者]
 •Naujieji Metal!
 ;) [送信者]
 •Wesolych Swiat!
 ;) [送信者]
 •Frohliche Weihnachten!
 ;) [送信者]
 •Prettige Kerstdagen!
 ;) [送信者]
 •Vesele Vanocel!
 ;) [送信者]
 •Joyeux Noel!
 ;) [送信者]
 •Buon Natale!
 ;) [送信者]

添付ファイル: 次のいずれかの拡張子を使用する。ファイル名は不定である。

.bat
 .cmd
 .com
 .pif
 .zip

ワームが実行されると、次のことを行う

1. 自分自身のコピーを次のファイル名で作成する。

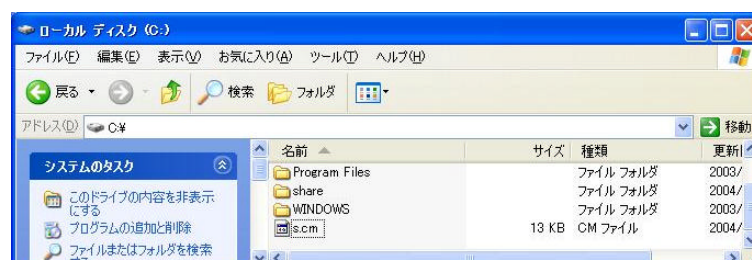
%System%¥Norton Update.exe

次のファイルを作成する。

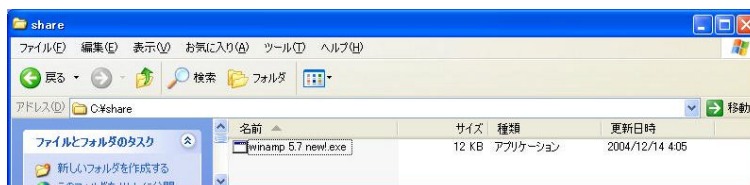
C:¥s.cm



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)



2. 自分自身のコピーを%System% に複数作成する。ファイル名はランダムな文字列、拡張子は .dll である。
3. 次のファイルを、C:ドライブからH:ドライブ内の "share", "upload", "music" という文字列を含むフォルダに作成しようと試みる。
winamp 5.7 new!.exe
ICQ 2005a new!.exe



4. "Wxp4" という名のミュートックスを作成し、ワームが複数同時に起動することを防ぐ。
5. レジストリキーを追加する。
Windows の起動時にワームを起動するために次の値を
"Wxp4" = "%System%\%Norton Update.exe"
次のレジストリキーに追加する。
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run



ワームに関する情報を格納した次のレジストリキーを作成する。
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Wxp4

6. 次のエラーメッセージを表示する。



7. 次の文字列を含むプロセスを停止する。
reged
msconfig
task
8. microsoft.com へ接続を試みる。
9. TCP ポート8181 を開き、感染したコンピュータにバックドアを作成する。
10. 次の文字列を含むフォルダ内の .exe ファイルを探し、発見したファイルのプロセスをすべて停止しようと試みる。
syman

	<p>viru trend secur panda cafee sopho kasper</p> <p>11. 次の拡張子を含むファイルからメールアドレスを収集し、%System% に作成した.dll ファイルに保存する。</p> <p>htm wab txt dbx tbb asp php sht adb mbx eml pmr fpt inb</p> <p>ただし、次の文字列を含む電子メールアドレスは除外する。</p> <p>yaho google win use info help admi ebm micro msn hotm suppor syman viru trend secur panda cafee sopho kasper</p> <p>12. 収集したメールアドレスに対し、独自の SMTP エンジンを使用して電子メールを送信する。</p>
感染・発症防止方法	<p>1. 「ウイルスの動作概要」に記述した内容のメールが届いた場合には、容易にメールを開封しない。</p> <p>2. 予期せぬメールが届いた場合には、添付ファイルを絶対に開かない。</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</p>

	<p>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">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 次のファイルを削除する。 %System%\%Norton Update.exe C:\%s.cm C ドライブからH ドライブ内の "share", "upload", "music" という文字列を含むフォルダから次のファイルを削除する。 winamp 5.7 new!.exe ICQ 2005a new!.exe5. レジストリに行われた変更を元に戻す。 次の値を "Wxp4" = "%System%\%Norton Update.exe" 次のレジストリキーを選択します。 次のレジストリキーから削除する。 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run 次のレジストリキーを削除する。 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Wxp4 <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	<p>メールの件名および本文は多言語である。言語は、英語、ハンガリー語、スペイン語、デンマーク語、スウェーデン語、ルウエー語、フィンランド語、リトアニア語、ポーランド語、ドイツ語、オランダ語、チェコ語、フランス語、イタリア語で、すべて「メリークリスマス」を意味する。</p>