

ウイルス解析報告書

ウイルス名	W32/Hunch.I (Bloodhound.W32.VBWORM)
プログラム名及び容量 (添付ファイル名)	73,728バイト
種別	ワーム
プログラム言語:	不詳(Visual Basicと思われる)
発症環境	32ビットWindows環境
発見日時	2002年9月5日
発見場所(発信地)	不明
危険性	中程度
発症条件	ワームプログラムを実行して再起動したとき
ウイルスの活動、影響	<p>W32/Hunch.Iは32ビットWindows環境で動作する大量メール発信型ワームである。</p> <p>本文がTal como te prometi; te envio mi foto en el archivo adjunto...のメールに添付された実行ファイルをダブルクリックするとワームとして実行され、システムフォルダにワームがコピーされる。また、レジストリにワームファイルが登録され、パソコン起動時に実行されるようになる。</p> <p>ワームは感染パソコンが利用しているExchangeサーバーからMAPIを利用してメールアドレスを参照し、そのすべてにワーム添付メールを発信する。</p> <p>ワームは内部に登録された拡張子から1つを選び、ローカルドライブから5つ削除する。</p> <p>また、Autoexec.batファイルを改ざんし、次回起動時にシステムフォルダ内の拡張子がSYS、DLL、OCXのすべてのファイルを削除しようとする。</p>
被害の規模	稀少(日本国内で発見の報告はない)
亜種、変種の有無	A型からI型までが報告されている。
ウイルス動作概要	<p>ワームは実行されると自分自身をシステムフォルダにコピーし、またMsie7en.exeとColas.exe という名前でもコピーを作る。</p> <p>MAPIを利用してワーム添付メールを送信する。MAPIを利用するので、メールの送信者はMAPIの設定に従った物になる。</p> <p>ワームはアドレス帳を列挙してすべてのアドレスにメールを送信する。送信されたメールはメーラーの送信済みに残る。</p> <p>件名はワーム自身のファイル名となる。添付ファイルもワーム自身と同じファイル名となる。本文は下記のとおり。</p> <p>Tal como te prometi; te envio mi foto en el archivo adjunto...</p> <p>ワームは下記の拡張子から1つを乱数で選び、ドライブを再帰的に検索して、見つけたその拡張子のファイルを5つ削除する。削除されたファイルのファイル名をシステムフォルダのMyWife!.scrに保存する。</p> <p>XLS DOC WAV DWG MP3 BAK CDX BMP HTM HLP CHM JPG TGA CPL</p>

	<p>ACD MID CDR MDB DBF ICO</p> <p>ワームはC:_RESTOREを検索してその中のすべてのファイルを削除する。</p> <p>ワームはレジストリの HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Runに 自分自身のファイル名を登録する。</p> <p>ワームはc:\Autoexec.batに</p> <pre>@echo off DEL %s*.DAT DEL %s*.COM DEL %s*.EXE CLS FORMAT C: /u /v:COLAS /autotest</pre> <p>を書き加える。実際には%sはシステムフォルダへのフルパスになる。</p>
感染・発症防止方法	<ul style="list-style-type: none"> ・Outlookのセキュリティパッチ適用 ・不明なメール添付ファイルを安易に実行しない
ウイルスの駆除方法	<p>< 確認 > Autoexec.batをテキストエディタなどで開き、内容に</p> <pre>@echo off DEL %s*.DAT DEL %s*.COM DEL %s*.EXE CLS FORMAT C: /u /v:COLAS /autotest</pre> <p>が含まれないことを確認する。</p> <p>< 駆除 > HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Runに ある不明なファイルおよび、システムフォルダ内のMsie7en.exeとColas.exeという名前のファイルを削除する。</p> <p>上記で確認したAutoexec.batのワームが追加した部分を削除する。</p>
その他	報告書作成:2002年9月12日現在

W32/Hunch.I@MM フローチャート

