

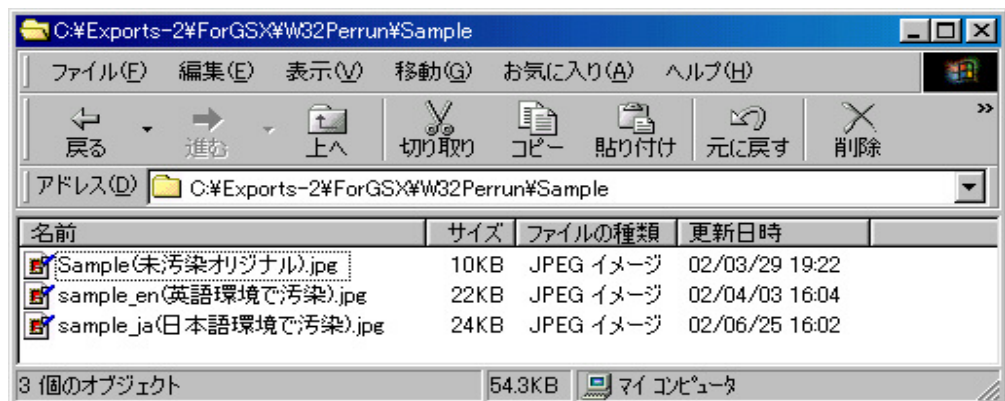
ウイルス解析報告書

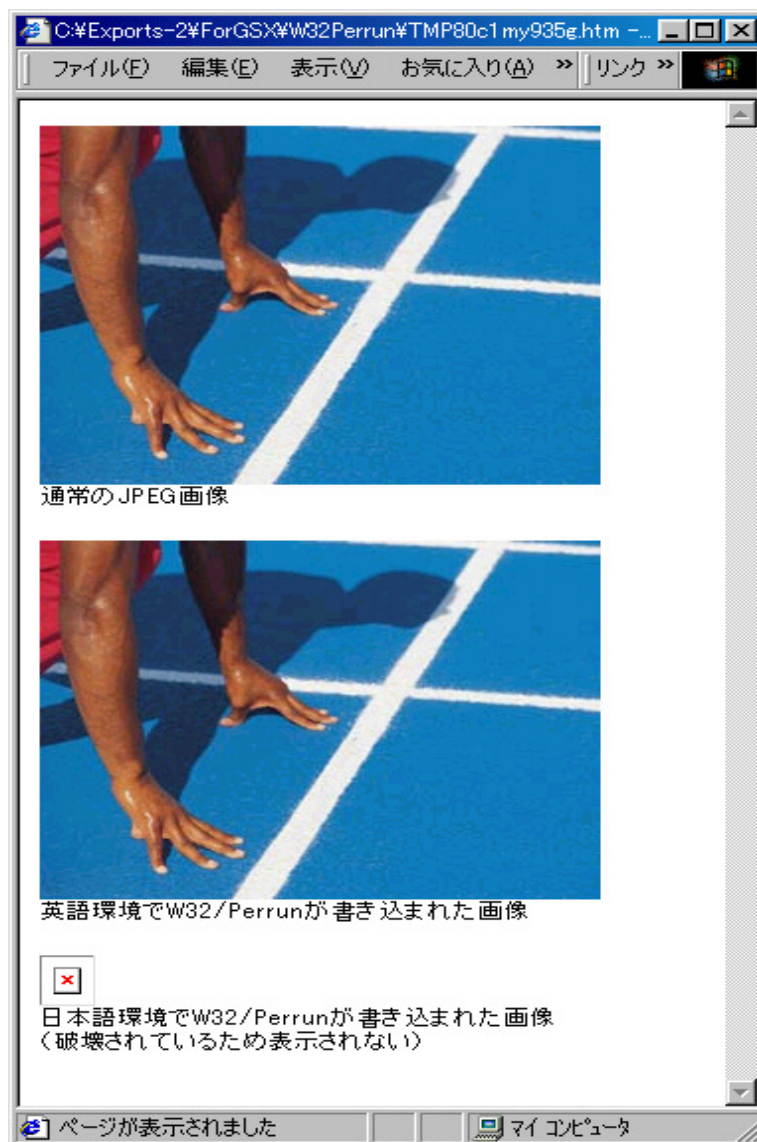
ウイルス名	W32/Perrun
プログラム名及び容量 (添付ファイル名)	Proof.exe(11,780バイト)
種別	トロイの木馬
プログラム言語	Visual Basic 6
発症環境	Windows 9x/ME (Windowsフォルダがc:\windowsであること)
発見日時	2002年6月13日
発見場所(発信地)	米国
危険性	きわめて低い(日本国内では皆無)
発症条件	発病は無い

ウイルスの活動、影響

W32/PerrunはWindows環境で動作するVB6で記述されたトロイの木馬である。このプログラムの本体はProof.exeと名付けられたEXEファイルで、実行すると次のような動作をする。

- 1.実行されるとカレントフォルダにreg.mp3というファイルと extrk.exe というファイルを作る。reg.mp3はレジストリを変更するためのファイルである。このファイル作成は、日本語環境では失敗する。
- 2.レジストリ変更によって、拡張子jpgのファイルが開かれるとき、必ずextrk.exeが実行されるようになる。
- 3.extrk.exeはカレントフォルダにあるJpegファイルを検索し、「Perrun形式(便宜上の名称)」で取り付けられている実行ファイルを別ファイルとして切り出し、それを実行する。
- 4.extrk.exeはカレントフォルダにあるJpegファイルを検索し、未汚染のjpegファイルに「Perrun形式」で自分自身をファイル末尾に取り付ける。この動作は英語環境でのみ正しく動作し、日本語環境ではjpegファイル自体が破壊される。





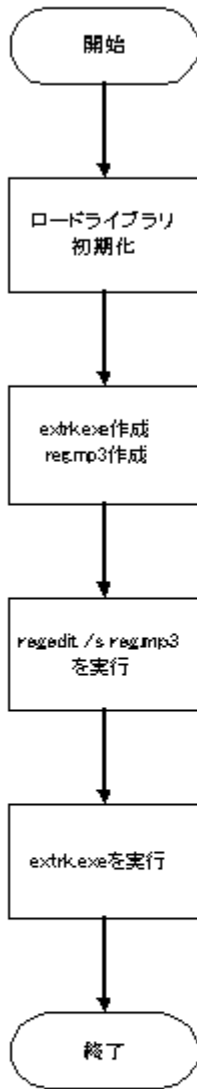
汚染されたJpegファイルは、通常、画像ファイルとしてのみ扱われるため、開いたりダブルクリックしたりしてもトロイの木馬として実行される事はなく、そのため画像ファイルによってトロイの木馬の被害が広がるようなことはない。

被害の規模	2002年6月25日現在、報告はない。
亜種、変種の有無	無
ウイルス動作概要	<p>トロージャンは11780バイトのPEファイル。</p> <p>トロージャンは実行されるとカレントフォルダにreg.mp3というファイルとextrk.exeというファイルを作る。reg.mp3の中身は下記の通り。 @=以降のダブルクォーテーション内はトロージャンが作成したextrk.exeへのフルパスに「%1」を付け加えた文字列になる。</p> <p>REGEDIT4</p> <p>[HKEY_CLASSES_ROOT\jpegfile\shell\open\command] @="<extrk.exeのフルパス> %1"</p> <p>トロージャンは「regedit /s reg.mp3」を実行する。 ウイルスはカレントフォルダを「*.jpg」で検索して最初に見つけたファイルの末尾にトロージャン自身を書き加える。jpegファイルの末尾がalcoのときには既に汚染しているとみなして次のファイルを検索する。</p> <p>extrk.exeはファイルに書き込まれる。jpegファイルの末尾がalcoのときには、jpegファイルの末尾の余分なデータをx.exeという名前で保存して実行する。</p>

	<p>extrk.exeは 「rundll32.exe C:¥WINDOWS¥SYSTEM¥SHIMGVW.DLL,ImageView_Fullscreen %1」 を実行する。</p> <p>このトロージャンにはバグがあり、日本語環境に置いて動作させたとき、jpegファイルにトロージャンを書き加える時点で元の画像データが破壊される。</p> <p>またextrk.exeは正しいイメージで出力されないため、日本語環境ではプログラムとして動作しない。</p>
感染・発症防止方法	入手元の不明なファイル等は実行しない。
ウイルスの駆除方法	<p><確認> ・ローカルドライブ内にextrk.exeという名前のファイルがあれば、このトロージャンの存在が疑われる。 ・HKEY_CLASSES_ROOT¥jpegfile¥shell¥open¥commandに"<パス名>¥extrk.exe %1"が設定されているか確認する。</p> <p><駆除> ・extrk.exeという名前のファイルを削除。 ・HKEY_CLASSES_ROOT¥jpegfile¥shell¥open¥commandに、"C:¥PROGRA 1¥INTERN 1¥explore.exe" -nohome を設定する。 (CドライブにIEがインストールされている場合)</p>
その他	報告書作成:2002年6月25日現在

W32/Perrun ゼネラルフローチャート

proof.exeフロー



extrk.exeフロー

