REVOウィルスの駆除

完全に駆除できたかどうかは、これからのＰＣの症状を見てからですが、現状、REVO ウィルスの再発はないようですので、私が試みた駆除方法を記載します。

OS については、XP が前提です。Vista は隠しファイルとはならないようで、容易に削除できました。

Ⅰ．対象ＰＣウィルス

revo.exe
mmvo.exe

Ⅱ．対処した方法

１．インターネットオプションから一時ファイルを削除

Cookie・ファイルともに削除。ついでに履歴も。

２．インターネットを「オフライン作業」とする

ファイル　→　「オフライン作業」をチェック。

３．　システムの復元オプションを無効に

Vista のシステム復元機能を無効にする方法
マイコンピュータ　右クリック　→　プロパティ　→　システムの保護　→　利用できるディスクのチェックを外す　→　適用　チェックがなくなったことを確認して　OK

４．バッチファイルの作成

次のバッチファイルをワードパッド（アクセサリーの中にあります。）により作成。
ファイルネームは、仮に abcd.bat としました（*.bat であれば何でもよい）。

```
cd ¥windows¥system32
attrib -s -h -r revo.exe
del revo.exe
attrib -s -h -r revo0.dll
del revo0.dll
attrib -s -h -r revo1.dll
del revo1.dll
attrib -s -h -r mmvo.exe
del mmvo.exe
attrib -s -h -r mmvo0.dll
del mmvo0.dll
attrib -s -h -r mmvo1.dll
del mmvo1.dll
cd ¥
attrib -s -h -r autorun.inf
del autorun.inf
attrib -s -h -r f.exe
del f.exe
attrib -s -h -r c.cmd
del c.cmd
```

このバッチファイルをシステムディスク上のルートに置く。
abcd.bat を一度、実行。

５．abcd.bat の自動実行の設定

ウィンドウズキー+R　→名前に「regedit」と入力(「」は入力しません)
次のレジストリエントリへ移動して abcd.bat を登録します。
HKEY_CURRENT_USER¥Software¥Microsoft¥Windows¥CurrentVersion¥Run

６．スタートアップから revo や mmvo を起動しないようにする

ウィンドウズキー+R　→名前に「msconfig」と入力　→システム構成ダイアログが表示されますので、スタートアップタブをクリック　→スタートアップ項目(一覧表)

スタートアップに revo、mmvo や kmmsoft があれば、一覧表のチェックを外す。
タブの BOOT.INI でセーフモードを選択。再起動。

７．システムディスクのルートにある abcd.bat を実行

コマンドプロンプト（アクセサリの中にある）から実行してもよい（＞の右に abcd.bat と入力しエンター)。

８．セーフモードでリブート

９．Prefetch ファイルの削除

¥windows¥prefetch の中で、mmvo、revo、f.exe、c.cmd、uu.exe などが含まれているファイルを削除（shift+del)。
フォルダが explorer で開けない場合は（ウィルスが邪魔をしている場合がある)、６に戻ってセーフモードで再度リブート。

１０．レジストリから、以下の手順で、値を変更

ウィンドウズキー+R　→名前に「regedit」と入力
(1) 次のレジストリサブキーのレジストリエントリを確認し、変更されていたら、それらを復元。
（エントリを選択し右クリック　→　修正　→　値のデータ）
HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Explorer¥Advanced¥Folder¥Hidden¥SHOWALL¥"CheckedValue"
　　値　0　の場合には　1　とする
HKEY_CURRENT_USER¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Explorer¥Advanced¥"Hidden"
　　値　2　の場合には　1　とする
HKEY_CURRENT_USER¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Explorer¥Advanced¥"ShowSuperHidden"
　　値　0　の場合には　1　とする
(2) レジストリエディタを終了（×で閉じる）

１１．フォルダオプションを変更して、隠しファイル・システムファイルをすべて表示

マイコンピュータを explorer で開き（マイコンピュータで右クリック　→　エクスプローラで開く　　ダブルクリックしない）　ツール→フォルダオプション
表示タブの表示→ファイルとフォルダの表示で
「すべてのファイルとフォルダを表示」にチェック
「システムフォルダの内容を表示する」をチェック
「登録されている拡張子は表示しない」のチェックをはずす
「保護されたオペレーティングシステムファイルを表示しない」のチェックをはずす。確認メッセージがでますが「はい」をクリック。最後に OK をクリック。これで隠しファイルが表示されます。
なお、フォルダが explorer で開けない場合は（ウィルスが邪魔をしている場合がある)、６に戻ってセーフモードで再度リブート。

１２．ルートにあるウィルス・ソフトの削除

ルートにある、*.cmd、*.exe、*.com といった実行型のファイルを全て削除（shift+del)。

１３．テンプフォルダ上のファイルの削除

(1) マイコンピュータ　→システムディスク　→Documents and Settings　→ユーザ名のフォルダ　→Local Settings　→Temp
uu.exe、rbw.dll 等があれば削除（shift+del)。その他実行型ファイルや dll ファイルがあれば全て削除（shift+del)。なお、全てのファイルを削除してもよい。
(2) マイコンピュータ　→システムディスク　→Documents and Settings　→ユーザ名のフォルダ　→Local Settings　→Temporary Internet Files
uu12.txt、uu.rar、uu.*があれば、これらを削除（shift+del)。なお、全てのファイルを削除してもよい。

１４．レジストリに登録されている起動部分を削除

ウィンドウズキー+R　→名前に「regedit」と入力。
次の処理を実行（「たま（ご）の記録：mmvo除菌録」

http://txmxkxmxontheball.spaces.live.com/blog/cns!772A2551521E51A0!458.entry
より)。
HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥SharedTools¥MSConfig¥startupreg¥kmmsoft
↑これを消すことでスタートアップ時の発症が直る。(ニュートラル・グッドな日常さんより)
HKEY_CURRENT_USER¥SoftWare¥Microsoft¥Windows¥CurrentVersion¥Explore¥MountPoint2¥
の中で、f.exe、c.cmd が登録されているフォルダを全て削除。

１５．Bitkv*.dll の実行停止

ウィンドウズキー+R　→名前に「regedit」と入力。
「編集」→「検索」で、「Bitkv」を検索し、見つけしだいこれを含むフォルダを全て削除。
Bitkv0.dll、Bitkv1.dll 等は uu21.txt を作成している模様（？)。uu21.txt を何度削除しても再生するのは、こいつのせいか。uu21.txt にはURLが記載されているが、ここからネット経由でuu.exeを呼び込んでいるのだろうか？

１６．セーフモードでリブート

ウィンドウズキー+R　→名前に「msconfig」と入力　→システム構成ダイアログが表示されますので、スタートアップタブをクリック　→スタートアップ項目(一覧表)
スタートアップに revo、mmvo や kmmsoft があれば、一覧表のチェックを外す。
タブの BOOT.INI でセーフモードを選択。再起動。

１７．ウィルスの有無の確認

システムディスクを見て、隠しファイルが表示されていたら駆除はほぼ完了。
確認の上、ウィンドウズキー+R　→名前に「msconfig」と入力　→システム構成ダイアログが表示されますので、スタートアップタブをクリック　→スタートアップ項目(一覧表)
スタートアップに revo、mmvo や kmmsoft の有無の確認。
タブの BOOT.INI でセーフモードのチェックをはずし、再起動。

１８．Bitkv*.dll の削除

スタート→ファイル検索で「Bitkv*」を選択し、Bitkv0.dll、Bitkv1.dll 等が見つかればこれらを全て削除。

１９．通常モードでの確認

システムディスクを見て、隠しファイルが表示されていたら駆除は全て完了。
その後、再発するのであれば、ウィルスファイルが隠れていた可能性があるため、念入りに再度１から１８までを実行。

なお、怖いため、未だ復元オプションを有効にしていません。
久しぶりに DOS コマンドを使ってしまいました。

パソコン応援隊「ウィルスに感染しました　kavo mmvo　続き」にはお世話になりました。
ついでに文章もつまみ食いでお借りしています。
http://sturnus.net/mt/2008/01/kavo-mmvo-1.html

警察の方、このウィルスの作成者を逮捕して！！
顔が見たい。
犯罪的ですよ、これは。何台も感染して参りました。

都築