■ Auto Start 9805 香港ウィルスについて

Disinfectant 引退のきっかけとなった Auto Start 9805 worm/ 香港ウィルスは、Dr.Solomon が情報を寄せている。

Dr.Solomon の情報は次の通り

1. ウィルスはマウントされたボリュームをスキャンして特定のファイル名で終わっているファイルを探し出す。
   ファイル名の最後が "data"、"cod"、"csa" のいずれかで終わり、データフォークが 100 バイト以上のファイル
   ファイル名の最後が"dat"で終わり、ファイル総サイズが2MB以上のファイル
2. これらのファイルが見つかるとデータの最初の1MB分をランダムに書き換える。
3. その他、感染者からの情報では、Illustrator、IllustratorEPS、llustrator5.5 J /7.0 J アプリケーション本体、ATM フォントが損傷するケースがある。

これは自己増殖するだけで害はないワームではない。また、自己増殖するので自己の複製をつくるプログラムを持たないトロイの木馬でもない。れっきとした新種ウィルスである。このウィルスの予防や発見、除去は簡単である。

▼ 「予防法」
「QuickTime 設定」コントロールパネルで CD-ROM の自動再生のチェックを取る(次の記事「QuickTime 設定の注意」で若干の注意を喚起したい。必ず読んでいただきたい)

▼ 「感染の可能性のある Macintosh」
QuickTime2.0 または 2.5 以降を使用している PowerMacintosh で、かつ「QuickTime 設定」コントロールパネルで CD-ROM の自動再生のチェックが入っているもの。

▼ 「感染しない Macintosh」
CD-ROM の自動再生の機能のある QuickTime2.0 または 2.5 以降を使っていない Macintosh、68k Macintosh。

▼ 「特徴的な症状」
感染したフロッピーや MO などのディスクを挿入すると未感染の Macintosh

は自動的に再起動する30分に一回程度の頻度でMacintoshの処理速度が極端に落ちるメニューバーに瞬間的に "DB" の文字が現れることもある。

▼ 「発見法」

"DB" および "Desktop Print Spooler" ("Desktop Printer Spooler" ではない) の不可視ファイルをファイル検索によって複数検索を行い発見できる。

1. ファイル検索で option キーを押しながら「名前が」などの条件をクリックすると「目に」が現れる。『「目に」「見えない」項目』とする。
2. 「条件を詳しく」をクリックする。
3. 「名前が」「を含む項目」で上記 "" でくくられた文字をいれる。

変種が発見されたので以下の、" " でくくられた文字列を検索すること。

1. "BD" と "Desktop Printr Spooler"
2. "DELDB" と "DELDesktop Print Spooler"

▼ 「除去法」

除去は「ResEdit」や「File Buddy」など不可視ファイルを可視にできるソフトで可視にしてからファイルを削除する。
フリーの駆除ソフトがいくつかあるので利用する。

● 「ResEdit での除去法」

1. ResEdit を入手する。
2. ResEditを起動し、びっくり箱の起動画面をクリックし先に進む。さらに出てくる SF ダイアログ画面もキャンセルする。
3. 「File」メニューの「Get File/Folder info...」を選択し、ダイアログ画面でディスクルートまたはシステムフォルダ/機能拡張フォルダ内の当該のウィルスアプリケーションを選択する。
4. そのファイル属性画面が出るので、下段「Finder Flags」の右中の「Invisible」のチェックをとる。
5. 属性画面を閉じ、保存に OK し、ResEdit を閉じる。
6. ウィルスのアプリケーションがディスクルートまたはシステムフォルダ/機能拡張フォルダ内に現れているのでゴミ箱に捨てて空にする。その際、決してアプリケーションのアイコンになっていると思うが決して起動しないように注意する。

● 「フリーなソフトでの駆除」

1. Autostart Hunter J-1.0b0(J)(64KB)
2. WormScanner(194KB)

Macintoshの主要なユーザであるDTPユーザを中心として日本にも広がりを見せているようなのでこの際徹底的に発見除去に努めていただきたい。発見された場合はフロッピーディスク一枚一枚まで全て検査する必要がある。

追記:

Eradicatorという本ウィルス発見、除去フリーウェアが公開されているがこれは "DB" を削除しない。

追記 2:

WormFood という発見、駆除、予防プログラムが発表された。

追記 3:

Auto Start 9805-B という変種が発見された。より悪質で狡猾になっている。予防法は同じ。発見、除去法は上記の方法をアレンジすることで適用できる。

Auto Start 9805-B の特徴、Auto Start 9805 との違いは以下。

1. ウィルスは "BD" と "Desktop Printr Spooler" という名称のファイルである（AutoStart9805 は "DB" および "Desktop Print Spooler" であった。違いに注意）。
2. QuickTime の自動再生を利用する。
3. 最初の感染時にコンピュータの再起動はない。
4. Auto Start 9805に感染しているコンピュータでは "DB" およびAuto Start 9805 を削除する。
5. ネットワークボリュームには感染しない。
6. 3 分ごとに感染し、6 分ごとにファイルを損傷させる。
7. 10242バイト以上の大きさのJPEG,TIFF,EPSFファイルに損傷を与える。
8. 「機能拡張」フォルダ内の「プリンタ記述ファイル」フォルダ内に "ACR","GEN","COL","LAS" または "DIS" で始まらないファイル名があるとファイルを損傷させる。
9. 最初の10242バイトを越えて1MBのデータをランダムデータに書き換える。
10. 一度に書き換えられるファイルは 20 以下である。
11. 98 年 12 月 24 日以降ウィルスは動作を中止する

追記 4:

Auto Start 9805-C が発見された。

■ QuickTime 設定の注意

Auto Start 9805 worm/香港ウィルスの関連でQuickTime設定に関して注意が必要だと思われる。
QuickTime 設定コントロールパネルは場合によっては外している方も多いと思う。機能拡張マネージャで外したり、手動で外したり、時にはゴミ箱に捨てたり。ところが、これらの場合 QuickTime2.5 以上がインストールされているとQuickTime 設定の自動再生がオンになったまま機能し続けている。

QuickTime設定を再度インストールするかバックアップのものを立ち上げるかしてチェックを取ること。
QuickTime設定はなにもコントロールパネルになくても設定を変更できる。例えばネットワークボリュームをマウントしてその中のQuickTime設定を直接ダブルクリックして設定を変更すればマウントし操作した側のMacintoshの設定が変更されるのでそれでもよい。また、多数の Macintosh、システムを管理している場合は初期設定フォルダの「QuickTime初期設定」をチェックを取ったシステムのものに取り替えてもよい。

QuickTime 設定の「オーディオ CD を自動的に再生する」と同時にオンになっていることも多いため、オーディオCDを入れて確かめる方もいると思うが、めったに使っていない方はモニタ＆サウンドコントロールパネルの設定によっては再生されているのに音が出ない場合もあるのでこの点も慎重に行っていただきたい(オーディオCDプレーヤで確認するか、QuickTime設定を開いて確認した方がよいだろう)。

QuickTime2.0 を使用している場合は 2.5 以上をインストールしてから行えばよい。