

ウィルス解析報告書

ウイルス名	DTHN Trojan (BackDoor-ANF)
プログラム名及び容量 (添付ファイル名)	サーバープログラム(トロイの木馬) 453,632 バイト、クライアントプログラム 518,144 バイト
種別	トロイの木馬 (バックドア機能を持つトロイの木馬)
プログラム言語	Visual Basic 5
発症環境	Windows 9x/ME/NT/2000/XP 上で、かつ VisualBasic5のランタイムライブラリが存在する環境
発見日時	2002年12月24日 (詳細は不明)
発見場所 (発信地)	不詳
危険性	バックドア経由リモートコントロールによる機密漏洩、分散型サービス妨害攻撃、ジャンクメール発信、パソコンのクラッシュ等
発症条件	リモートコントロールにより随時
ウイルスの活動、影響	<p>このプログラムはVisualBasic5により作成され、Windows 9x/ME/NT/2000/XP 上で動作するバックドアプログラムである。 通常このプログラムは悪意の利用者がトロイの木馬として設定し、被害者に実行させることによって動作させる。 目的は主にDDoS (分散型サービス妨害) やポートスキャン、ジャンクメールなどを送信する踏み台としての利用である。</p> <p>トロイの木馬は動作させるとパソコン内の任意の場所にコピーを作成し、レジストリに登録して自動起動が行われるようになる。 悪意の利用者はこの被害者パソコンに専用のクライアントプログラムを使ってインターネット経由で接続し、被害者パソコンの情報を取り出したり、DDoS攻撃を行わせたり、または任意のプログラムを送り込んで実行できるようになる。</p> <p>なお、このトロイの木馬は悪意の利用者が自由にカスタマイズできるため、ファイル名・トロイの木馬のコピー場所・コントロール用ポートアドレス等は決まった値とは限らない。またプラグイン機能によって機能の追加が可能であるため、必ずしも被害は上記の内容にとどまるとは限らない。</p>
被害の規模	被害報告無し(2002年12月25日時点)
亜種、変種の有無	無し
	<p>このトロージャンはVisual Basicで作られている。日本語環境ほかいくつかの2バイト言語環境ではトロージャン自身のコピー以外は、トロージャンが作成するファイルが壊れる</p> <p>file sign.exeはnettrojan.exe、conf.ini、dthn.dthnを読み込んで 配布用のnettrojan.exe.appd.READY.exeを作成する。 1、2、3と赤で示されたボタンを順番に押すことでファイルは作られる。(図1参照)</p>

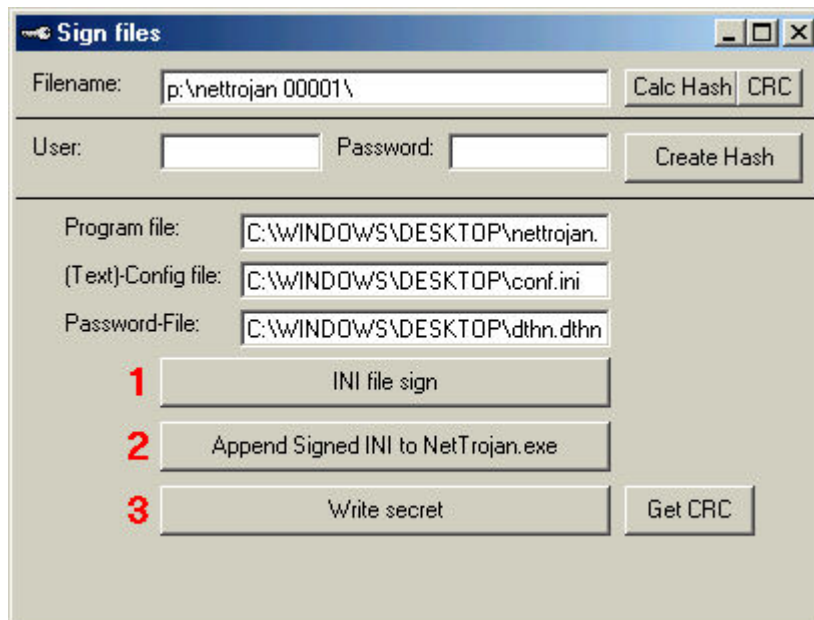


図1. トロージャンプログラムのカスタマイズ

中間ファイルとしてconf.ini.signedとnettrojan.exe.appdが作られる。

nettrojan.exe.appd.READY.exeはnettrojan.exeに暗号化された conf.iniとdthn.dthnがファイルの末尾に付いている。

nettrojan.exe.appd.READY.exeが実行されると、標準の設定では トロージャン自身をWindowsフォルダに unwise.exeという名前でコピーする。

ただしコピー先のフォルダとファイル名は上記のconf.iniで変更可能。

フォルダはWindowsフォルダ、システムフォルダ、テンポラリフォルダ、プログラムファイルフォルダ、Windowsフォルダがあるドライブのルート、または任意のパスに変更できる。

ウイルス動作概要

トロージャンは下記のレジストリを設定して起動時にコピーした ウィルスが実行されるようにする。

%sはコピーしたトロージャンのフルパス(例、C:\WINDOWS\UNWISE.exe)。

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce\WinLoader=%s
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnceEx\000x\WinLoader=!!%s
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\run\WinLoader=%s
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices\WinLoader=%s
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce\WinLoader=%s
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Runonce\WinLoader=%s
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\WinLoader=%s
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices\WinLoader=%s
```

トロージャンは下記のレジストリを設定して拡張子に関連付けられたプログラムが 実行されるときにトロージャンが実行されるようにする。

下記のデフォルトの値を「%s /exec:%s」(最初の%sはトロージャンのフルパス、次の%sはレジストリのキーの元の値)に変更する。

```
HKEY_CLASSES_ROOT\txtfile\shell\open\command
HKEY_CLASSES_ROOT\exefile\shell\open\command
HKEY_CLASSES_ROOT\comfile\shell\open\command
HKEY_CLASSES_ROOT\batfile\shell\open\command
HKEY_CLASSES_ROOT\piffile\shell\open\command
HKEY_CLASSES_ROOT\htmlfile\shell\open\command
HKEY_CLASSES_ROOT\giffile\shell\open\command
HKEY_CLASSES_ROOT\jpegfile\shell\open\command
```

また下記に上記の元の値を保存する。

```
HKEY_CLASSES_ROOT\txtfile\shell\open\command\winampold
HKEY_CLASSES_ROOT\exefile\shell\open\command\winampold
HKEY_CLASSES_ROOT\comfile\shell\open\command\winampold
HKEY_CLASSES_ROOT\batfile\shell\open\command\winampold
```

```
HKEY_CLASSES_ROOT¥piffile¥shell¥open¥command¥winampold
HKEY_CLASSES_ROOT¥htmlfile¥shell¥open¥command¥winampold
HKEY_CLASSES_ROOT¥giffile¥shell¥open¥command¥winampold
HKEY_CLASSES_ROOT¥jpegfile¥shell¥open¥command¥winampold
```

トロージャンは下記のレジストリを作成する。Installedの値はトロージャンが実行された日付になる。

```
HKEY_LOCAL_MACHINE¥Software¥Microsoft¥Windows¥CurrentVersion¥InstallCID
HKEY_CURRENT_USER¥Software¥VB and VBA Program Settings¥VB5¥Date¥Installed
```

トロージャンはWindowsフォルダのsystem.iniのbootセクションのshellキーの値を「explorer.exe %s」に変更する。%sはコピーしたトロージャンのフルパス。
またWindowsフォルダのsystem.iniのwindowsセクションのrunキーにコピーしたトロージャンのフルパスを設定する(200文字の空白が先頭に挿入される)。

トロージャンはautoexec.batに¥xff(日本語で表記不可能な1文字)だけの行を書き加える。またWindowsフォルダに¥xff.batを作成する。その内容は下記のとおり。
%sはコピーしたトロージャンのフルパス。

```
@echo off
@if exist %s goto end
@:end
```

トロージャンは最後に下図のようなダイアログボックスを表示する場合がある。

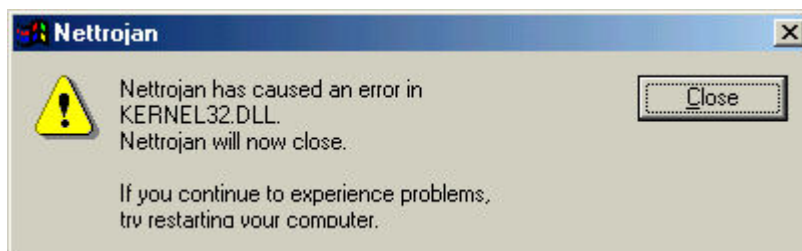


図2. トロージャン実行時に表示されることのあるダイアログ

トロージャンには専用のクライアントプログラムで接続する。ポートはconf.iniの設定による。接続にはユーザーIDとパスワードが必要。dthn.dthnおよびconf.iniで設定する。

クライアントプログラムからトロージャンに感染したマシンに 任意のファイルを転送することができる。

トロージャンはIRCのサーバに接続して、クライアントプログラムで指定されたチャンネルにメッセージを送信することができる。IRCのユーザー名は conf.iniで設定する。乱数やあらかじめ決められた候補の組み合わせにすることができる。IRCサーバはconf.iniでいくつかの候補を指定する。これはIRCに対するDDoSとして機能する。

トロージャンはクライアントプログラムで指定されたIPアドレスに対して ポートスキャンを行う。

トロージャンはクライアントプログラムで指定されたIPアドレスに対して PingによるDDoS攻撃を行うことができる。

トロージャンはTCP接続をリダイレクトする機能がある。これを利用するとトロージャンに感染したマシンはProxyとして機能する。

トロージャンはクライアントプログラムで指定されたメールを送信する機能がある。トロージャンはSMTPサーバとしての機能を内蔵しており、独自にメールの送信を行う。

感染・発症防止方法

不明なプログラム(メール添付ファイルや出所不明のディスクメディア)を安易に実行しない。ネットワークを利用する場合、ファイアウォールプログラムを利用し、不要なポートを閉じる。

ウイルスの駆除方法

<確認>
このトロージャンは特定のファイル名のファイルが作成されるとは限らないため、レジストリに登録されている自動起動プログラムを普段から把握しておき、不審なプログラムが登録されていないかどうかを確認するよりない。また、タスクマネージャなどから不明なプロセスが起動していないかどうか確認する。

<駆除>

	レジストりに登録されている自動起動プログラムに、不振なプログラムが登録されていた場合はこれを休止に設定、または削除する。 タスクマネージャなどから確認し、不明なプロセスが起動していれば終了させる。 その後該当のプログラムファイルを削除する。
その他	報告書作成: 2002年12月27日現在

