

ウィルス解析報告書

ウイルス名	WORM_DELODER.A (W32/Deloder.A)
プログラム名及び容量 (添付ファイル名)	Dvldr32.exe 745,984バイト
種別	Windows32ビット(2000/XP)環境用ワーム
プログラム言語	C言語
発症環境	Windows 2000/XP
発見日時	2003年3月9日
発見場所(発信地)	不詳
危険性	中程度(5段階では3程度)
発症条件	Windows2000またはWindowsXPがOSとしてセットアップされているパソコンをインターネット接続している場合
ウイルスの活動、影響	<p>このワームは、インターネット接続を経由して、Windows2000/XPのリモートログインサービス(ポート445)に接続し、ファイルを送り込んで実行することにより感染を広げる。</p> <p>ワームはWindows 2000/XPで動作します。ただしWindows Home Editionでは標準では外部からのログインに失敗するため外部からは感染しない。</p> <p>ワームが実行されると、OSが起動するたびにウイルスが実行されるようになる。</p> <p>ワームは他のマシンにあらかじめ用意されたパスワードでログインを試みる。ログインに成功したときには、そのマシンにウイルスをコピーして実行させる。</p> <p>ワームはVNCとIRCを利用したトロージャンをインストールする。 トロージャンをインストールされた状態では、外部からマシンを操作される可能性がある。</p> <p>ワームは下記のファイルで構成されている。一部はワームではなく、通常のツール等のプログラムを流用したものである。</p> <p>Windowsフォルダ Dvldr32.exe ワーム inst.exe ワーム psexec.exe 通常のプログラム</p> <p>Windowsフォルダのfonts以下 explorer.exe VNC 通常のプログラム omnithread_rt.dll VNC 通常のプログラム VNCHooks.dll VNC 通常のプログラム rundll32.exe ワーム</p> <p>システムフォルダ cygwin1.dll CYGWIN 通常のプログラム</p> <p>その他 C:\Documents and Settings\All Users\Start Menu\Programs\Startup\inst.exe ワーム C:\WINDOWS\Start Menu\Programs\Startup\inst.exe ワーム C:\WINNT\All Users\Start Menu\Programs\Startup\inst.exe ワーム</p>
被害の規模	数十件程度(日本国内にて)
亜種、変種の有無	現在のところ確認されていない
	<p style="text-align: center;">Dvldr32.exeの解析情報</p> <p>ワームは実行されるとワーム自身があるフォルダをカレントフォルダにする。 ワームは実行された環境がWindows 2000またはXP以降のOSではないときには終了する。</p>

	<p>が実行されるようになる。</p> <p>rundll32.exeの解析情報</p> <p>トロージャンは起動すると下記のIRCのチャンネルに接続する。</p> <p>cocket.nailed.org cocket.mo00.com cocket.bounceme.net cocket.phathookups.com cocket.gotdns.com cocket.ma.cx cocket.orgdns.org cocket.minidns.net cocket.dyn.nicolas.cx cocket.dynup.net cocket.pokemonfan.org cocket.staticcling.org cocket.getmyip.com</p> <p>そしてチャンネルsex0rに参加する。</p>
感染・発症防止方法	<p>ファイアーウォールまたはルーターを用いてポート445に対するアクセスを拒絶する。</p>
ウイルスの駆除方法	<p>< 確認 > WindowsフォルダにDvldr32.exeまたはinst.exeがあるか、Windowsフォルダのfonts以下にexplorer.exe、omnithread_rt.dll、VNCHooks.dll、rundll32.exeがあれば感染している。</p> <p>< 駆除 > WindowsフォルダにあるDvldr32.exe、inst.exe、psexec.exe、Windowsフォルダのfonts以下にあるexplorer.exe、omnithread_rt.dll、VNCHooks.dll、rundll32.exeがあれば削除する。システムフォルダにあるcygwin1.dllは不要ならば削除する。誤って同名のWindowsのファイルを削除しないように注意すること。</p> <p>もし下記のファイルがあるならば、それらも削除する。</p> <p>C:\Documents and Settings\All Users\Start Menu\Programs\Startup\inst.exe C:\WINDOWS\Start Menu\Programs\Startup\inst.exe C:\WINNT\All Users\Start Menu\Programs\Startup\inst.exe</p> <p>レジストリの HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 以下にmessnger、Explorer、TaskManがあるならば、それらを削除する。</p>
その他	<p>報告書作成：2003年3月12日現在</p>

W32/Deloder.A フローチャート

