

ウィルス解析報告書

ウイルス名	SQLsnake (JS/Spida, Worm.SQL.Spida, SQL.spida, Double Tap)
プログラム名及び容量 (添付ファイル名)	services.exe(fscan.exe) sqlexec.exe clemail.exe sqlinstall.bat sqlprocess.js sqldir.js run.js pwdump2.exe samdump.dll timer.dll
種別	ワーム
プログラム言語:	JScript (マイクロソフト仕様JavaScript)
発症環境	Microsoft SQLサーバー稼働環境
発見日時	2002年5月20日
発見場所(発信地)	
危険性	<ul style="list-style-type: none"> ・MS SQLサーバー管理アカウントにパスワードが設定されていない場合、そのMS SQLサーバーはワームの侵入を受ける。 ・侵入されたサーバーはメールアドレスのパスワードを盗まれる恐れがある。 ・ワームに侵入され、感染したコンピュータは、他のコンピュータに対してワームの感染を試みる。このためポート1433に相当量のアクセスが行われる。
発症条件	パスワードを収集する機能が働くのは、Syskeyが無効になっている場合のみ。SyskeyはWindows NT 4.0ではデフォルトで無効になっており、Windows 2000/XPではデフォルトで有効になっている。
ウイルスの活動、影響	<p>このワームは2001年11月に、Cbladワームによって狙われた経歴のある、「パスワードの設定されない管理アカウントからの侵入」問題と同じ問題点を狙う。</p> <p>この管理アカウントはsaと呼ばれ、SQLサーバープログラムのインストールや設定に利用されるものであるが、インストール後もパスワードの無い状態で放置される可能性がある。</p> <p>ワームはポート1433経由でコンピュータにアクセスし、パスワードの設定されていないsaを発見すると、これに対し、自動的にログインを行い、自身をインストールする。</p> <p>感染に成功すると、そのサーバーに設定されているメールアドレスのパスワードを収集し、組み込まれた特定のメールアドレスに送信する。</p> <p>また、適当に作成したIPアドレスに対し、ポートスキャンプログラムを利用して他のSQLサーバーを検索する。</p>
被害の規模	コンピュータ研究機関のSANS Instituteによると、5月20日時点で1600台程度が感染していると報告されている。以後不明。
亜種、変種の有無	A型とB型が確認されている。この2種類はファイル構成が異なるが、これ以外の差異や詳細については未確認である。
	<p>ワームは複数のファイルによって構成されているが、本体はJScriptで書かれた.jsファイルである。</p> <p>services.exe Foundstoneのfscan.exeというプログラム。ポートスキャンプログラムで、このプログラムは、本来ワームとして利用されるためのプログラムではない。シェアウェアである。</p> <p>clemail.exe コマンドラインEメールプログラム(シェアウェア)。</p> <p>pwdump2.exe パスワード取得プログラム</p>

ウイルス動作概要	<p>samdump.dll パスワード取得プログラム用DLL</p> <p>timer.dll タイマー用DLL</p> <p>sqlinstall.bat インストールバッチファイル</p> <p>sqlprocess.js ワームサブプログラム</p> <p>sqldir.js ワームサブプログラム</p> <p>run.js ワームメインプログラム</p>
感染・発症防止方法	<p>・SQLサービスをインターネットに解放しない(本来、SQLは内部向けサービスの筈なので、当然の処置といえる)</p> <p>・マイクロソフト社の情報ページ「Microsoft SQL Server を狙ったワームに関する情報」に従って、saのパスワードを設定する。</p>
ウイルスの駆除方法	<p><確認> ワームファイルに該当するものをファイル名でチェックする。また、ポート1433の使用状況を確認する。</p> <p><駆除> ワームファイルのプロセスをタスクマネージャーで停止して該当ファイルを削除する。</p>
その他	<p>このワームに感染したとしても、サーバーに目立った変化は現れないので、おそらく被害者も気づかないと思われる。 報告書作成:2002年5月24日現在</p>

SQLsnake フローチャート

