
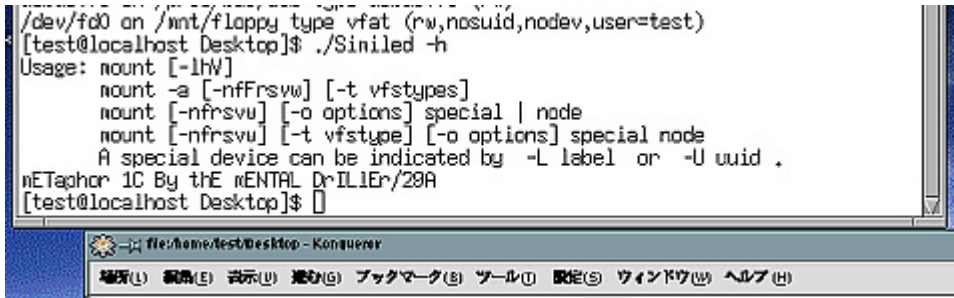


ウイルス解析報告書

ウイルス名	Linux.Simile (W32.Simile.D, Linux/Smile.D, W32/Simile.D)
プログラム名及び容量 (添付ファイル名)	プログラム名不定(ウイルス型感染のため)、容量不定(ポリモーフィック暗号化のため。平均増容量約110KB)
種別	ウイルス(Windows32ビット環境PEファイル感染、Linux環境ELFファイル感染)
プログラム言語:	アセンブラ
発症環境	Windows9x/ME/2000/XP/NT、Linux(RedHat6.2/7.0を想定) ただしIntel系CPUのコンピュータ上でのみ動作する。
発見日時	2002年5月20日
発見場所(発信地)	不明
危険性	非常に低い
発症条件	毎年3月および9月の17日(Windows)、毎年3月および5月の17日(Linux)
ウイルスの活動、影響	<p>このウイルスは32ビットWindows環境とLinux環境の双方で動作する、マルチプラットフォーム型ウイルスである。 ウイルスは暗号化(*1)されており、また、ポリモーフィック暗号化(*2)を取り入れたウイルスでもある。</p> <p>WindowsとLinuxの両環境で動作するウイルスも、ポリモーフィック暗号化ウイルスも過去に例は存在するが、この双方が同時に盛り込まれたウイルスはこのウイルスが初めてのケースとなる。</p> <p>PE型実行ファイルに感染したものはWindows環境で、ELF形式実行ファイルに感染したものはLinux環境でのみ動作する。</p> <p>これら双方のファイルが同時にアクセス可能な場合のみクロス感染が行われる。この条件が満たされる環境はFAT32ファイルシステムがリードライト可能になっているLinux環境や、双方OSのファイルが置いてあるファイルサーバーなど、かなり限られた環境と考えられる。 従って、このウイルスが広範囲にわたって蔓延する可能性は低い。</p> <p>Windows環境では毎年3月および9月の17日(Windows)に発病し、感染プログラムを実行した際に、下記のようなダイアログメッセージを表示する。メッセージ文字の大文字・小文字は実行の度に变化する。</p>  <p>Linux環境では毎年3月および5月の17日に発病し、感染プログラムを実行した際に、メッセージをコンソールに表示する。(下図参照)</p>  <p>*1)暗号化ウイルス:一般的なワクチンはウイルスコードのごく一部を比較情報としてその内部に持ち、ディスク内のファイルにそれと同じ情報が無いかが検索することによってウイルスを発見する。そのため、ウイルス作者はそれを回避するために、 ・感染の度に变化するキーワードを作り、</p>

	<p>・それを使ってプログラムの大部分に論理演算を行って暗号化することで、感染毎にウイルスプログラムを異なるイメージに変化させ、ワクチンで発見されることから逃れようと試みた。</p> <p>*2)ポリモーフィック暗号化:暗号化ウイルスの発想は斬新ではあったが、ワクチンから逃れることはほとんど不可能であった。なぜなら、暗号化すればプログラムとして実行できなくなるため、それを元に戻す復号ルーチンが必須となり、これ自体は暗号化できないからである。つまり復号ルーチンを比較対象にすれば、暗号化ウイルスは発見できるのである。そこでウイルス作者は、復号ルーチンも感染毎に変化させてワクチンの発見を逃れる手法を考えた。これがポリモーフィック暗号化である。</p> <p>具体的には、ジャンプ命令や実行しても意味のない命令の組み合わせ(同じ数を足してひく、掛けて割る、必ず成立する条件ジャンプ)などを織り交ぜて、「動作は全く同じだが、イメージやサイズの異なるプログラム(復号ルーチン)を自動生成する」という手法である。ポリモーフィック暗号化が施されたウイルスは感染毎にサイズとバイナリーイメージが完全に異なったものとなり、単なるコードの比較一致で発見することはできない。また解析も困難なものになる。</p>
被害の規模	2002年6月5日時点、被害報告は0件(シマンテック社発表)
亜種、変種の有無	A型とD型が確認されている。詳細は不明。
ウイルス動作概要	<p>このウイルスは32ビットWindows環境とLinux環境の双方で動作する、マルチプラットフォーム型ウイルスである。</p> <p>ウイルスはポリモーフィック暗号化されている。</p> <p>ウイルスには異なる2つのファイルに感染するためのそれぞれのルーチンと、共通して利用されるポリモーフィック復号ルーチンジェネレータなどの共通部分がある。</p> <p>PE型実行ファイルに感染したものはWindows環境で、ELF形式実行ファイルに感染したものはLinux環境でのみ動作する。</p> <p>これら双方のファイルが同時にアクセス可能な場合のみクロス感染が行われる。この条件が満たされる環境はFAT32ファイルシステムがリードライト可能になっているLinux環境や、双方OSのファイルが置いてあるファイルサーバーなど、かなり限られた環境と考えられる。従って、このウイルスが広範囲にわたって蔓延する可能性は低い。</p> <p>このウイルスの感染手法は複雑である。通常のウイルスは寄生宿主プログラムのエントリー部分を書き換えることによってウイルス自身のプログラムコード領域に実行を移させるが、このウイルスは寄生宿主プログラムの中途部分にある命令の行き先アドレスを変更してウイルスコード領域に実行を移させる。</p> <p>また、寄生宿主プログラムのオフセットアドレスは移動され、それに合わせてリロケーションが行われる。</p> <p>すなわち、感染宿主のどの部分がウイルスによって書き変わるか予測できないうえ、書き換えられた部分のプログラム情報が永遠に失われて元に戻すことができなくなると言う問題が発生し、特に感染プログラムの修復が非常に困難になる。</p> <p>この手法はW32/MTXウイルスに見られた手法と似ているが、アンチウイルス製品によるウイルス駆除および修復を非常に困難なものにさせている。</p>
感染・発症防止方法	出所不明のプログラムファイルを実行しない。
ウイルスの駆除方法	<p><確認></p> <p>・パソコンのシステム時計を3月17日に変更し、感染のおそれのあるプログラムを実行する。 ウイルス発病によるメッセージが見られた場合、感染している。</p> <p>・システムディスクまたはマスターディスク等のオリジナルプログラムと、プログラムサイズで比較し、ファイル日付が同じであるにもかかわらず、サイズが100KB以上大きくなっていた場合は感染の可能性はある。</p> <p><駆除></p> <p>・ハードディスク内容を消去し、システムを再インストールした後、バックアップから感染ファイルを上書きして修復する。</p>
その他	<p>29Aと呼ばれるウイルス作者グループが製作に関与しているものと思われる。 29Aから(挑戦的な意味で)アンチウイルスベンダーに送り届けられた模様。 報告書作成:2002年6月11日現在</p>

Linux.Simile.Dウイルス ゼネラルフローチャート

