

## ウイルス解析報告書

ウイルス名	W32/Sobig.A-mm (W32.Sobig.A@mm, WORM_SOBIG.A)
プログラム名及び容量 (添付ファイル名)	winmgm32.exe 65,536バイト ( Movie_0074.mpeg.pif, Document003.pif, Untitled1.pif, Sample.pif )
種別	32ビットWindows環境ワーム(メール伝染型)
プログラム言語:	Visual C++
発症環境	Windows9x/ME/NT/2000/XP(32ビットWindows環境)
発見日時	2003年1月9日
発見場所(発信地)	不詳
危険性	中程度 5段階評価で2と3の間あたり。
発症条件	即時
ウイルスの活動、影響	<p>W32/Sobig.A-mmはVisual C++を用いて作成されたと思われる32ビットWindows環境上で動作するワームである。</p> <p>Sobigは主に電子メールの添付ファイルによって伝染する。 このワームメールは件名が、Re: Movies、Re: Sample、Re: Document、Re: Here is that sampleの4つのうちのどれかで、発信人は必ずbig@boss.comである。 また、添付ファイル名は、Movie_0074.mpeg.pif、Document003.pif、Untitled1.pif、Sample.pifの4つのうちいずれかである。</p> <p>このワームプログラムを動作させると、ウィンドウズフォルダにwinmgm32.exeというファイル名でワームがコピーされ、レジストリの自動起動に登録される。</p> <p>さらにワームは次の処理を行う。</p> <ol style="list-style-type: none"> <li>1.送信者名がmail@mail.com、件名はNotifyのメールをpager.icq.comあてに送信する。</li> <li>2. http://www.geocities.com/reteras/reteral.txtに書かれたURLからファイルをダウンロードする。</li> <li>3. ネットワーク共有されたフォルダを検索し、Windowsのスタートアップフォルダにワームをコピーする。(スタートアップフォルダは英語版のそれに限る)</li> <li>4. 拡張子がtxt、eml、html、htm、dbx、wabのファイルをローカルディスクから検索し、内容からメールアドレスを収集してそこにワームメールを発信する。</li> </ol>
被害の規模	広範に広がっている。MessageLabsによれば、2003年1月15日時点で4万件程度の報告があるとされている。
亜種、変種の有無	現時点では知られていない
	<p>ワームは起動するとワーム自身がWindowsフォルダのwinmgm32.exeか調べる。 winmgm32.exeのときには、「Worm.X」という名前のミューテックスを作る。 ミューテックスが作れないときにはワームは終了する。</p> <p>ワームは3つのスレッドを作る。</p> <p>1つめのスレッドでは、pager.icq.comにメールを送信する。 送信者名はmail@mail.com、件名はNotifyになる。</p> <p>2つめスレッドでは、http://www.geocities.com/reteras/reteral.txtからファイルをDownloadする。 DownloadしたファイルはWindowsフォルダにdwn.datという名前で保存される。 ワームはこのファイルで示されるURLからさらにファイルをDownloadする。 このファイルの内容は現在は「http://www.nowhere.com/ba.txt」であるが、変更される可能性もある。 http://www.nowhere.com/ba.txtは現在は存在しない。</p> <p>3つめのスレッドでは、ネットワーク共有されたフォルダを検索して、 Windows¥All Users¥Start Menu¥Programs¥Startup¥</p>

ウイルス動作概要	<p>または Documents and Settings¥All Users¥Start Menu¥Programs¥Startup¥ のいずれかの名前のフォルダを見つけたときに、そこにワーム自身をコピーする。 このフォルダ名は英語版のスタートアップフォルダである。日本語版にはない。 ワームをコピーされた側のパソコンは再起動したときにワームが自動的に実行される。(英語版に限る)</p> <p>ワームは拡張子がtxt、eml、html、htm、dbx、wabのファイルをそれぞれ再帰的に検索する。 そのファイルから正規表現で [A-Za-z0-9]+[A-Za-z0-9_-.]+@[([A-Za-z0-9%-])+([.])+[A-Za-z]+ に一致する文字列(メールアドレスを意図している)をすべて探す。見つけた文字列を記憶する。</p> <p>ワームは収集したメールアドレス宛てにワームを添付してメールを送信する。 メールの送信はワームに内蔵されたSMTPサーバで直接行う。ワームはDNSのMXレコードを問い合わせることで、直接送信先のSMTPサーバに接続する。 メールの受信者は収集したメールアドレスとなり、メールの送信者はbig@boss.comとなる。 本文は「Attached file:」となる。 件名と添付ファイル名は下記の中から選ばれる。</p> <p><b>件名</b> Re: Movies Re: Sample Re: Document Re: Here is that sample</p> <p><b>添付ファイル名</b> Movie_0074.mpeg.pif Document003.pif Untitled1.pif Sample.pif</p> <p>すべてのメールを送信するとワームは終了する。</p> <p>ワームがwinmgm32.exeではないときには、Windowsフォルダにワーム自身を winmgm32.exeという名前でコピーする。 そしてレジストリの HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Run¥WindowsMGM にWindowsフォルダのwinmgm32.exeへのフルパスを登録する。 ワームはWindowsフォルダのwinmgm32.exeを実行して終了する。</p>
感染・発症防止方法	<ul style="list-style-type: none"> <li>・不明なメール添付ファイルを開かない。</li> <li>・共有フォルダを共有されたまま、みだりに放置しない。</li> </ul>
ウイルスの駆除方法	<p>&lt;確認&gt; Windowsフォルダにwinmgm32.exeがあれば感染している。</p> <p>&lt;駆除&gt; Windowsフォルダのwinmgm32.exeを削除する。 またレジストリの HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Run¥WindowsMGM も削除する。 Windowsフォルダにdwn.datがあればそれも削除する。</p>
その他	報告書作成:2003年1月16日現在

W32/Sobig.A-mmフローチャート

