

## ウイルス解析報告書

ウイルス名	W32/Bugbear.A-mm (Tanat, Tanatos, WORM_NATOSTA.A, W32/Bugbear@MM, Worm/Tanatos)
プログラム名及び容量 (添付ファイル名)	ファイル名: 不特定 サイズ: 50,688バイト
種別	ワーム (Windows32ビットプログラム)
プログラム言語:	Visual C++
発症環境	Windows95/98/ME/NT/2000/XP
発見日時	2002年9月30日 (米国時間)
発見場所 (発信地)	米国と思われる
危険性	中程度(5段階で上から3段目) ただし感染力が強いので、これよりも+1段階程度危険性が高まる可能性がある。
発症条件	感染と同時
ウイルスの活動、影響	<p>このワームはWindows95/98/ME/NT/2000/XPで動作する。</p> <p>ワームはディスクを検索してメールアドレスを収集し、収集したメールアドレスにメールを送信する。件名はあらかじめ決められたいくつかの候補から選ばれることもあるが、それ以外の場合もあり不定。本文は空白または不定である。メールの送信者名は収集したメールアドレスの中から選ばれることがある(偽造される)。</p> <p>添付ファイル名はMyDocumentsフォルダの中のファイル名をランダム、あるいはあらかじめ決められたいくつかの候補から乱数で選択される。</p> <p>InternetExplorer5.0/5.5のセキュリティホールを利用して自分自身をユーザーに知られることなく実行させる機能を持つ。 OutlookまたはOutlookExpressメーラーでは、メールを表示またはプレビューするだけでワームに感染する。</p> <p>ワームはネットワークで共有されているフォルダに自身をコピーすることで他のコンピュータに感染する。</p> <p>ワームはアンチウイルスプログラムなどを終了させる機能がある。</p> <p>ウイルスにはバックドアとしての機能があり、感染パソコンのファイル構成やファイル内容を盗まれる可能性がある。</p> <p>キー入力履歴などが第三者に取得される危険がある。</p>
被害の規模	<ul style="list-style-type: none"> <li>・感染メールを送信する事による信用の失墜</li> <li>・ワームメール送信時、送信者偽装による誤解・トラブルの発生</li> <li>・キーロガーによるパスワードやIDなどの機密情報の漏洩</li> <li>・バックドアによるファイルの盗難の可能性</li> </ul>
亜種、変種の有無	現在の所発見されていない
	<p>ワームが作成するファイル名はすべて不定になるが、ディスクのボリューム値をキーにして名前を決めるので、そのシステムでは同じ名前になる。(OSの再インストールなどでボリューム値が変わらない限り何度感染してもそのパソコンでは同一)</p> <p>ワームは自身がシステムフォルダにインストールされたものではないときには、システムフォルダに自分自身をコピーする。ファイル名は*.exeとなる。</p> <p>ワームはAPIのRegisterServiceProcessを取得し、取得できたならばこれを呼び出して自身をサービスとして実行する。</p> <p>ワームはあらかじめ作成しておいた5632バイトのDLLを読み込む。このファイルの名前は不定。読み込みに失敗したときには、システムフォルダに5632バイトのファイルを作り、ロードする。ワームはこのDLLがエクスポートしているAPIを呼び出す。このDLLはキーボードの履歴を読み取る。</p>

## ウイルス動作概要

ワームはレジストリの

HKEY\_CURRENT\_USER¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Explorer¥Shell Folders¥Startup からスタートアップフォルダのフルパスを取得する。さらにそのフォルダにワームをコピーする。ファイル名は不定。

ワームはプロセスの終了時にレジストリの

HKEY\_LOCAL\_MACHINE¥Software¥Microsoft¥Windows¥CurrentVersion¥RunOnce に自身のファイル名を登録する。

ワームは4つのスレッドを作成する。

1つめのスレッドは特定のプロセスを停止する。

ワームは30秒間停止する。

Windows95系ではツールヘルプを使い、NT系ではEnumProcessを使ってプロセスを列挙する。EnumProcessはNT4.0以降からサポートされているので、それ以前ではプロセスの列挙は失敗する。ワームはファイル名が

\_AVP32.EXE、\_AVPCC.EXE、\_AVPM.EXE、ACKWIN32.EXE、ANTI-TROJAN.EXE、APVXDWIN.EXE、AUTODOWN.EXE、AVCONSOLE.EXE、AVE32.EXE、AVGCTRL.EXE、AVKSERV.EXE、AVNT.EXE、AVP.EXE、AVP32.EXE、AVPCC.EXE、AVPDOS32.EXE、AVPM.EXE、AVPTC32.EXE、AVPUPD.EXE、AVSCHED32.EXE、AVWIN95.EXE、AVWUPD32.EXE、BLACKD.EXE、BLACKICE.EXE、CFIADMIN.EXE、CFIAUDIT.EXE、CFINET.EXE、CFINET32.EXE、CLAW95.EXE、CLAW95CF.EXE、CLEANER.EXE、CLEANER3.EXE、DVP95.EXE、DVP95.0.EXE、ENGINE.EXE、ESAFE.EXE、ESPWATCH.EXE、F-AGNT95.EXE、F-PROT.EXE、F-PROT95.EXE、F-STOPW.EXE、FINDVIRU.EXE、FP-WIN.EXE、FPROT.EXE、FRW.EXE、IAMAPP.EXE、IAMSERV.EXE、IBMASN.EXE、IBMAVSP.EXE、ICLOAD95.EXE、ICLOADNT.EXE、ICMON.EXE、ICSUPP95.EXE、ICSUPPNT.EXE、IFACE.EXE、IOMON98.EXE、JEDI.EXE、LOCKDOWN2000.EXE、LOOKOUT.EXE、LUALL.EXE、MOOLIVE.EXE、MPFTRAY.EXE、N32SCANW.EXE、NAVAPW32.EXE、NAVLU32.EXE、NAVNT.EXE、NAVW32.EXE、NAVWNT.EXE、NISUM.EXE、NMAIN.EXE、NORMIST.EXE、NUPGRADE.EXE、NVC95.EXE、OUTPOST.EXE、PADMIN.EXE、PAVCL.EXE、PAVSCHED.EXE、PAVW.EXE、CCWIN98.EXE、PCFWALLICON.EXE、PERSFW.EXE、RAV7.EXE、RAV7WIN.EXE、RESCUE.EXE、AFEWEB.EXE、SCAN32.EXE、SCAN95.EXE、SCANPM.EXE、SCRSKAN.EXE、SERV95.EXE、SMC.EXE、SPHINX.EXE、SWEEP95.EXE、TBSCAN.EXE、TCA.EXE、TDS2-98.EXE、TDS2-NT.EXE、VET95.EXE、VETTRAY.EXE、VSCAN40.EXE、VSECOMR.EXE、VSHWIN32.EXE、VSSTAT.EXE、WEBSCANX.EXE、WFINDV32.EXE、ZONEALARM.EXE

のプロセスを終了させる。プロセスの列挙が終わると30秒間の停止に戻る。

2つ目のスレッドはメールを送信する。

ワームはレジストリの

HKEY\_CURRENT\_USER¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Explorer¥Shell Folders¥Personal のMyDocumentsフォルダのフルパスを取得する。そのフォルダを検索して拡張子が.INIではなく、「.」を含むファイルまたはフォルダを見つけたときには、その名前に乱数でscr、exe、pifのいずれかの拡張子を付ける。確率はscrが1/2で、残りが1/4づつ。

ファイルまたはフォルダが見つからなかったときには「readme」、「Card」、「news」、「images」、「resume」、「video」、「song」の中から1つを乱数で選び、同様に乱数で拡張子を付ける。これを添付ファイル名とする。

ワームはカレントドライブのルートから再帰的にファイルを検索する。

ワームは検索したファイル名が、.DBX、.TBB、.EML、.MBX、.NCH、.MMF、INBOX、.ODSのいずれかを含むときには、そのファイルからメールアドレスを収集する。

ワームはレジストリのHKEY\_CURRENT\_USER¥SOFTWARE¥Microsoft¥Internet Account Manager¥Accounts¥Default Mail Account の値を取得し、その値かレジストリのHKEY\_CURRENT\_USER¥SOFTWARE¥Microsoft¥Internet Account Manager¥Accounts¥以下のキーからデフォルトのメールアカウントのSMTP Serverの値を取得する。

ワームはこのメールサーバに接続してSMTPでメールを送信する。

メールの受信者は見つけたメールアドレスすべてになる。送信者は見つけたメールアドレスの中から選ばれる(送信者を偽装する)。または送信者の名前をレジストリの

HKEY\_CURRENT\_USER¥SOFTWARE¥Microsoft¥Internet Account Manager¥Accounts¥Default Mail Account

の値を取得し、その値かレジストリの

HKEY\_CURRENT\_USER¥SOFTWARE¥Microsoft¥Internet Account Manager¥Accounts¥

以下のキーからデフォルトのメールアカウントのSMTP Email Addressと

SMTP Display Nameの値にする。

	<p>件名は</p> <p>「Greetings!」、「Hi!」、「\$150 FREE Bonus!」、「Your Gift」、「Tools For Your Online Business」、「News」、「its easy」、「SCAM alert!!!」、「new reading」、「25 merchants and rising」、「empty account」、「My eBay ads」、「Market Update Report」、「fantastic」、「bad news」、「New Contests」、「Get a FREE gift!」、「Report」、「Stats」、「Interesting...」、「various」、「history screen」、「Just a reminder」、「hmm..」</p> <p>のいずれかが乱数で選ばれ本文は空白になるか、または見つけたファイルから適当な内容を取り出して件名と本文を構成する。</p> <p>メールにはワームが添付され、InternetExplorerのコンポーネントにセキュリティホールがある場合にはプレビューまたは表示しただけで添付ファイルが実行される。</p> <p>ただし「majordom」、「ticket」、「talk」、「list」、「localdomain」、「localhost」、「nobody@」、「root@」、「postmaster@」、「mailer-daemon」、「trojan」、「virus」、「lyris」、「noreply」、「recipients」、「undisclosed」、「spam」、「remove」を含むメールアドレスは対象外となる。</p> <p>3つ目のスレッドはポート36794で待機する。</p> <p>このスレッドはバックドアとして機能する。 HTTPプロトコルで通信が行われ、コンピュータ名、ディスクのタイプ、フォルダの一覧、ファイルの属性、ファイルの内容が取得できる。 一般的なWebブラウザで感染マシンのIPアドレスとポート番号、フォルダを指定するだけで、情報を取得できる。</p> <p>4つ目のスレッドは共有フォルダにワームをコピーする。</p> <p>ワームはネットワークのリソースを列挙して共有されているフォルダが見つかった場合、そこにスタートアップフォルダがあるか、チェックする。</p> <p>ワームはレジストリの HKEY_CURRENT_USER¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Explorer¥Shell Folders¥Startup からスタートアップフォルダのフルパスを取得して、それを元にして名前を比較する。 スタートアップフォルダが見つかったならば、そこにワームをコピーする。</p> <p><b>【注意】</b> 添付ファイル名やメールの件名の候補が他社の解析情報よりも少ないが、これで問題ない。他社の解析情報にあるような文字列は、単にウイルスに含まれるのみであり、実際に使われるのは、ここで挙げたものだけである。</p>
感染・発症防止方法	InternetExplorer5.0/5.5のアップデートによるセキュリティホール対処(MS01-20) ファイアウォールによる不明プロセスの通信防止、ポート36794のチェックまたは閉鎖
ウイルスの駆除方法	<p>&lt;確認&gt; タスクリストを表示し、見覚えがないプロセスがあれば、それがワームである可能性がある。</p> <p>Windows95/98/MEではプロセスが表示されないため、セーフモードで起動した上で HKEY_LOCAL_MACHINE¥Software¥Microsoft¥Windows¥CurrentVersion¥RunOnce のファイル名に見覚えのない物があるかどうかをチェックすること。 他の装置と比較するとわかりやすいかもしれない。</p> <p>&lt;駆除&gt; プロセスとして動作しているワームを強制終了させ、ワームによって作られたファイルをすべて削除する。 ファイル名は不定なので、プロセス終了時に名前の確認を忘れないこと。その名前のファイルがシステムフォルダにある。</p> <p>Windows95/98/MEではプロセスが表示されないため、セーフモードで起動した上で HKEY_LOCAL_MACHINE¥Software¥Microsoft¥Windows¥CurrentVersion¥RunOnce のファイル名に見覚えのない物があるかどうかをチェックし、削除すること。 他の装置と比較するとわかりやすいかもしれない。</p>
その他	報告書作成:2002年10月4日現在

**W32/Bugbear.A-mm  
フローチャート**