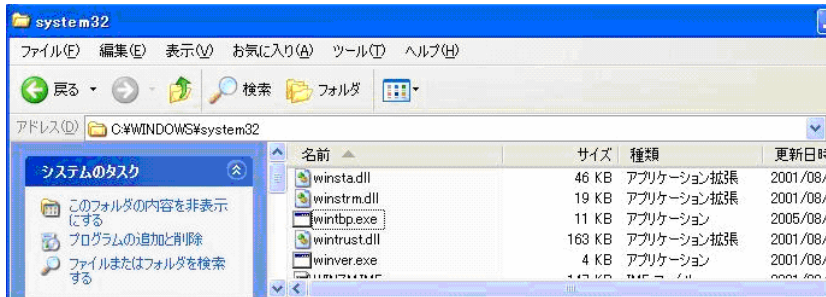


ウイルス解析報告書

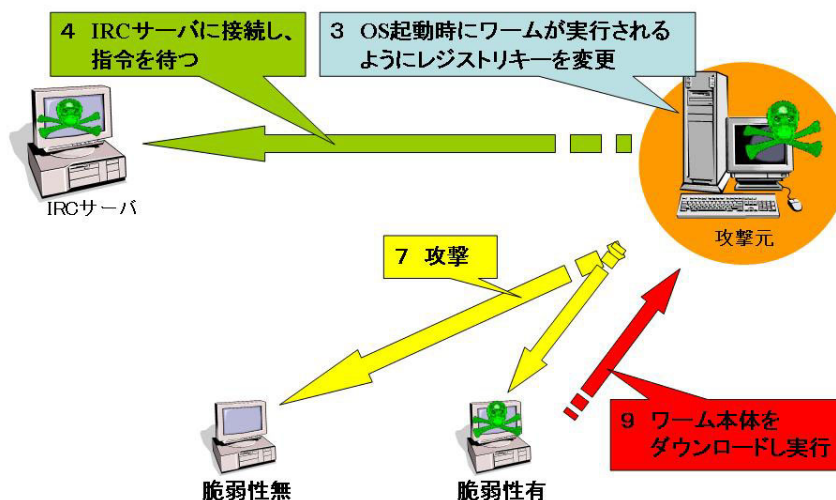
ウイルス名	W32.Zotob.E(別名: CME-540, Win32.Tpbot.A [Computer Associates], Bozori.A [F-Secure], Net-Worm.Win32.Bozori.a [Kaspersky Lab], W32/Bozori.worm.a[CME-540 [McAfee], W32/Tpbot-A [Sophos], WORM_RBOT.CBQ [Trend Micro])
プログラム名及び容量(添付ファイル名)	プログラム名: wintbp.exe 容 量: 10,366 バイト
種別	ワーム
プログラム言語	C/C++
発症環境	Windows 2000
発見日	2005 年 8 月 17 日
発見場所	アメリカ合衆国
危険性	感染力が高い。危険度は 5 段階の 3(5 が最も危険)。
発症条件	Microsoft Windows プラグアンドプレイサービスの脆弱性(MS05-039)が存在するコンピュータが、ワームの攻撃を受けたとき。または、プログラムを直接実行したとき。
ウイルスの活動、影響	このワームは、独自に生成した IP アドレスを持つコンピュータに対して、Microsoft Windows プラグアンドプレイサービスの脆弱性 (MS05-039) を悪用して拡散するワームである。 なお、ワームは Windows95/98/Me/NT4/XP コンピュータ上でも動作し、感染活動を行う。しかし、脆弱性を利用して感染するのは Windows2000 コンピュータだけである。
被害の規模	発見から 31 時間で 57 件の届出がシマンテック社に寄せられている。
亜種、変種の有無	W32.Zotob.A (2005 年 8 月 15 日発見)以降 W32.Zotob.B、W32.Zotob.C 等の多数の亜種が発見されている。
ウイルスの動作概要	<p>このワームが実行されると、次のことを行う。</p> <ol style="list-style-type: none"> 1. コンピュータ上でワームが複数同時に実行されること防ぐため、次のミューテックスを作成する。 wintbp 2. ワーム自身を%System%¥wintbp.exe としてコピーする。 <div style="text-align: center; margin: 10px 0;">  </div> <p>Windows のシステムフォルダ%System% (標準では、C:¥Windows¥System、C:¥Winnt¥System32、または C:¥Windows¥System32)</p> <ol style="list-style-type: none"> 3. Windows の起動時にワームを実行させるため、次のレジストリキーに HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Run 次の値を追加する。 "Wintbp.exe" = "%System%¥wintbp.exe"



4. 特定の IRC サーバの TCP ポート 8080 に接続し、次の命令を待ち受ける。
 - (1) ファイルをダウンロードし実行する。
 - (2) ワームを終了し、ワームを削除する。
 - (3) ワームを終了する。
5. 他のコンピュータへワームを拡散するために、UDP ポート 69 を開く。
6. 感染したコンピュータの IP アドレスを元に、最小 50 個、最大 200 個の IP アドレスを次のように生成する。
 - (1) 1 個目の IP アドレス
感染したコンピュータの IP アドレスをバイナリ値に変換し、その値に、乱数を 512 で割った余りを加算し、256 を減算したもの。
 - (2) 2 個から 33 個目までの IP アドレス
前回生成した IP アドレス(バイナリ値)に、乱数を 1025 で割った余りを加算し、512 を減算したもの。
 - (3) 34 個目以降の IP アドレス
第1から第4オクテットまでをランダムに生成したもの。生成した IP アドレスによって攻撃に成功すれば、その IP アドレス(バイナリ値)を元にして(2)の IP アドレスの生成を 512 回行う。512 回生成終了後は、またランダムな IP アドレスを生成する。
7. 6 で生成した IP アドレスの TCP ポート 445 に対して、Microsoft Windows プラグアンドプレイのバッファオーバーフローの脆弱性(MS05-039)を悪用し攻撃を行う。
攻撃が成功した場合は、成功した IP アドレスを元に 6(2)で生成した IP アドレスに対して攻撃を行う。
8. 攻撃が成功すると、攻撃を受けたコンピュータは TCP ポート 8594 でバックドアを開く。
9. 攻撃元のコンピュータは、バックドアを介して攻撃を受けたコンピュータに、次のファイルを作成し実行する。
%Temp%\%[番号].bat([番号] は 0 から 9 のいくつかのランダムな番号)
このファイルは、攻撃を受けたコンピュータが、攻撃元のコンピュータの UDP ポート 8594 に TFTP 接続し、ワームをダウンロードし実行するスクリプトである。ダウンロードしたファイルは、次のファイル名で保存する。
%Windir%\%a[番号].exe

Windows のインストールフォルダ%Windir%(標準では、C:\Windows または C:\Winnt)
カレントユーザのプロファイルフォルダ%UserProfile%(標準では、C:\Documents and Settings\<カレントユーザ名>)
11. IRC サーバに攻撃が成功した IP アドレスを送信する。

12 動作概要図を下記に示す。



感染・発症防止方法

1. マイクロソフトの提供する修正パッチ (MS05-039) を適用する。
2. リモートにより脆弱性を利用されることを防止するために、TCP ポート 445、8594、UDP ポート 69 をファイアウォールでブロックする。
3. インターネットからダウンロードしたファイルについては、必ずウイルススキャンを実行し、問題がないことが確認できるまでは絶対に起動しない。

ウイルスの駆除方法

手動による修復を行う場合、コンピュータに関する高度な知識が必要とされ、間違えるとコンピュータが正常に起動しなくなる場合もある。

1. 被害拡大防止のため、感染したコンピュータをネットワークから切り離す。
2. システムの復元オプションを無効にする。(Windows Me/XP)
3. コンピュータをセーフモードで再起動する。

4. 感染ファイルを削除する

```
%System%\wintbp.exe
%Temp%\[番号].bat
%Windir%\a[番号].exe
```

5. レジストリに行われた変更を元に戻す

次のレジストリキーから

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
```

次の値を削除します。

```
"wintbp.exe" = "wintbp.exe"
```

各操作については、Microsoft のホームページ、付属のマニュアル等を参照すること。無償修復ツールが、ワクチンベンダーから配布されているので、使用上の注意をよく読み使用すること。

その他

1 このワームについて、各種日本語版 Windows 環境における検証結果を次に示す。

OS	Service Pack	感染の有無
Windows 2000 Professional	なし	無 ※
Windows 2000 Professional	SP4	有
Windows 2000 Server	なし	無 ※
Windows 2000 Server	SP4	有
Windows XP Professional	なし	無
Windows XP Professional	SP2	無
Windows Server 2003	なし	無
Windows Server 2003	SP1	無

※ MS05-039 の脆弱性によって、service.exe のエラーが発生してシステムが再起動する。

2 平成 17 年末現在で 133 件(国内 0 件)の届出がシマンテック社に寄せられている。