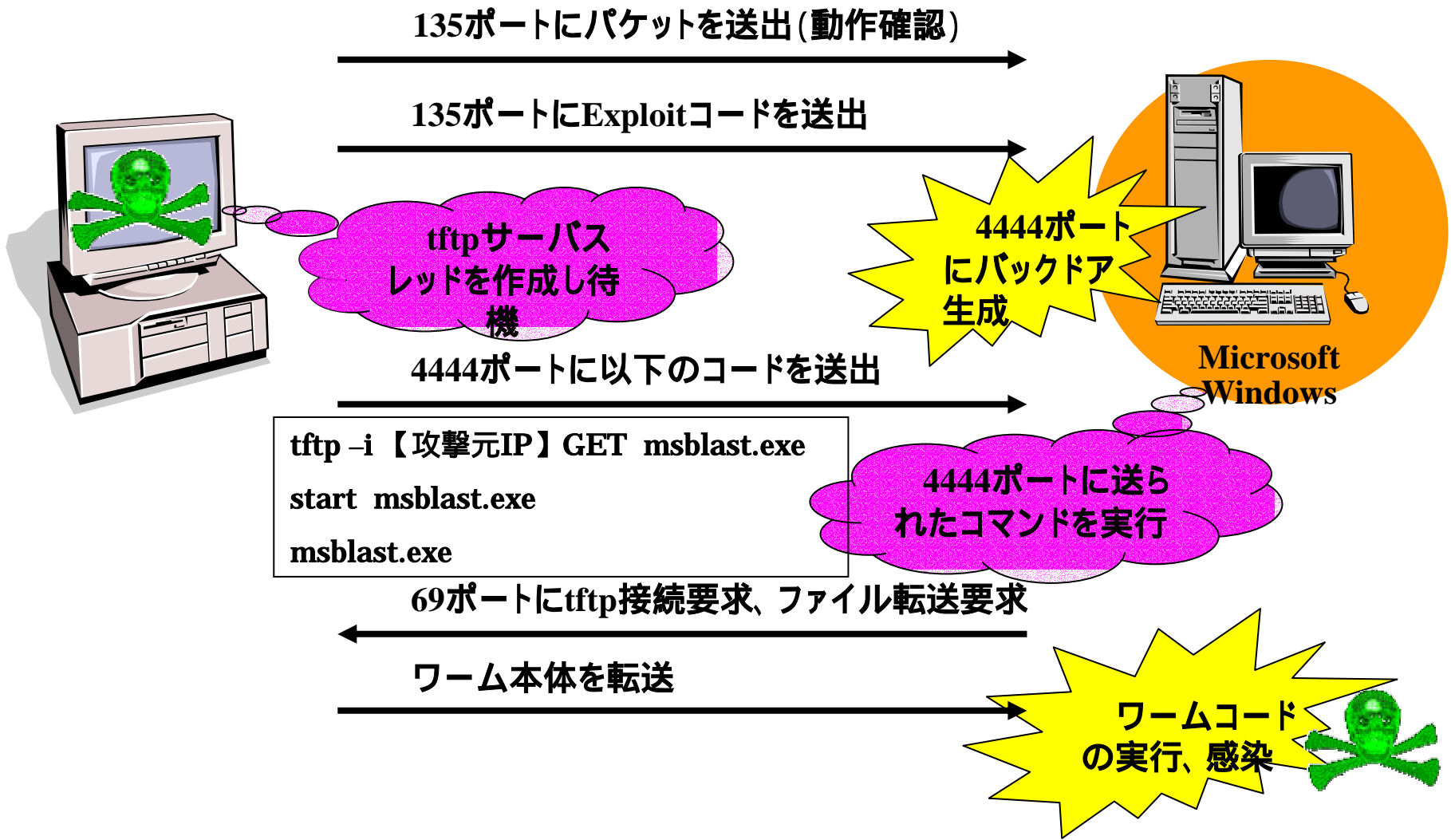


# W32.Blaster.Wormの感染動作概要



# W32.Blaster.WormのDoS攻撃動作概要

(1月から8月は16日以降、9月から12月は連日攻撃)

windowsupdate.comのIPアドレス取得

送出元IPアドレスの生成

- ・第1第2オクテットは感染時と同じ
  - ・第3第4オクテットは乱数でランダムに生成
- Synパケットを作成

windowsupdate.comにパケット送出

から が無限ループで繰り返される

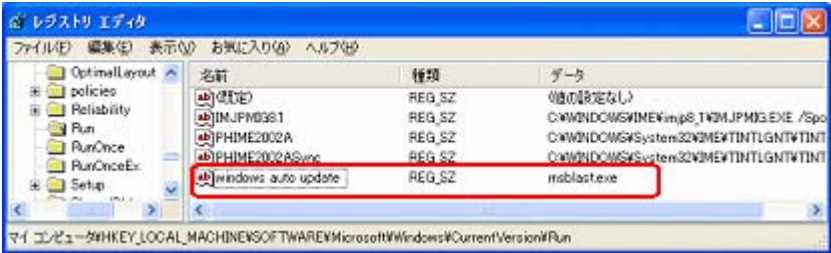


OS	パッチ	
	未適用	適用
Windows NT		-
Windows 2000	×	
Windows XP	×	
Windows 2003		

パッチ有効性検証結果

- ： 感染しない
- ×： 感染する
- ： 感染しないが再起動する
- ： 未検証

## ウイルス解析報告書

<b>ウイルス名</b>	W32.Blaster.Worm ( 別名 : W32/Lovsan.worm.a [McAfee], Win32.Poza.A [CA], Lovsan [F-Secure], WORM_MSBLAST.A [Trend], W32/Blaster-A [Sophos], W32/Blaster [Panda], Worm.Win32.Lovsan [KAV])
<b>プログラム名及び容量(添付ファイル名)</b>	プログラム名: msblast.exe 容 量 : 6,176 バイト
<b>種 別</b>	ワーム
<b>プログラム言語</b>	不明, UPX で圧縮されている。
<b>発 症 環 境</b>	Windows 2000, Windows XP
<b>発 見 日 時</b>	2003 年 8 月 12 日
<b>発見場所(発信地)</b>	ドイツ(最初の感染報告)
<b>危 険 性</b>	DCOM RPC の脆弱性(マイクロソフト セキュリティ情報 MS03-026)を悪用し侵入するため、修正プログラムが適用されていないコンピュータは非常に危険。危険度は 5 段階の 4(5 が最も危険)。
<b>発 症 条 件</b>	セキュリティホールが存在する PC では攻撃コードを受信したとき。
<b>ウイルスの活動、影響</b>	<ol style="list-style-type: none"> <li>1. TCP ポート 135 を使って DCOM RPC の脆弱性(マイクロソフト セキュリティ情報 MS03-026)を悪用するワーム。</li> <li>2. msblast.exe というファイルをダウンロードし実行する。</li> <li>3. ユーザが DCOM RPC の脆弱性を解消する修正プログラムを適用できないようにするために、windowsupdate.com に対しサービス拒否攻撃を行う。</li> </ol>
<b>被 害 規 模</b>	世界的に大規模に感染している。
<b>変種 亜種の有無</b>	無
<b>ウイルスの動作概要</b>	<p>W32.Blaster.Worm が実行されると、次のことを行う。</p> <ol style="list-style-type: none"> <li>1. コンピュータが既にワームに感染しているのかをチェックし、既に感染している場合には動作しない。ワームの 2 重起動を防止。</li> <li>2. Windows の起動時に必ずワームが実行されるように設定するため、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。 "windows auto update"="msblast.exe"</li> </ol>  <p>The screenshot shows the Windows Registry Editor window. The left pane shows the tree structure expanded to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run. The right pane shows a list of registry values. A new value 'windows auto update' of type REG_SZ is added with the data 'msblast.exe'. The value is highlighted with a red box.</p> <ol style="list-style-type: none"> <li>3. 2通りの方法により IP アドレスを生成し、そのアドレスのコンピュータに攻撃を行い感染を試みる。IP アドレスは次のアルゴリズムに基づいて生成される。 <ul style="list-style-type: none"> <li>・ 40%の確率で IP アドレスは、第1,第2オクテットは感染元と同じである。また、第3オクテットについては、40%の確率で値が 20 よりも大きいかどうかを確認し、20 より大きい場合は、値から 20 未満のランダムな値を差し引いた値が使用される。第4オクテットは 0 から 254 まで順次増加させる。</li> <li>・ 60%の確率で IP アドレスは、ランダムに第1～第3オクテット生成し、第4オクテットは 0 から 254 まで順次増加させる。</li> </ul> </li> </ol>

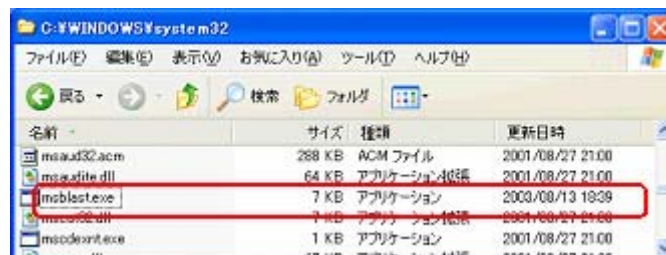
4. DCOM RPC の脆弱性を攻撃するコードを生成した IP アドレスの TCP ポート 135 に送信する。また、Windows XP 攻撃用と Windows 2000 攻撃用の 2 通りのコードのうちいずれか一方を送信し、Windows XP 用コードが送信される確率は 80%、Windows 2000 用コードが送信される確率は 20% で、ワームの起動時に選択される。

- ・ この結果、ローカルサブネットが、TCP ポート 135 への要求で飽和状態になる。
- ・ W32.Blaster.Worm は、Windows NT、Windows 2003 にまで感染を広げる能力はないが、修正パッチを適用していない場合、ワームが脆弱性の利用を試みた結果として、これらの OS を異常終了させてしまう可能性がある。また、このワームを Windows NT、Windows 2003 上に手動で置き、実行することで、実行・拡散する。
- ・ 攻撃コードの組み立て手法がランダムなため、送信されるコードが不適切なものであった場合、コンピュータが異常終了することがある。不適切なコードが送信された結果、svchost.exe がエラーを生成する。
- ・ RPC サービスがクラッシュした場合、Windows XP や Windows 2003 サーバでは、コンピュータが再起動される場合がある。

5. TCP ポート 4444 で待機するリモートシェル cmd.exe を作成する。その cmd.exe には隠しファイル属性が設定されている。これにより、攻撃者は、感染したシステムに対してリモートコマンドを発行することができる。

6. UDP ポート 69 で接続を待機する。DCOM RPC の脆弱性を利用して接続することができたコンピュータからの接続要求を受信すると、そのコンピュータに対し Msblast.exe を送信し、実行するためのコマンドを送信する。Msblast.exe は、コンピュータのシステムフォルダ%System%に保存される。

(システムフォルダ%System%は、標準で C:\WINNT\System32 (Windows NT/2000)または C:\Windows\System32 (Windows XP)である。



7. このワームは現在の日付の「月」が 1 月から 8 月の場合はその月の 16 日から月末まで、9 月から 12 月の場合は毎日発病し、Windows Update の web サイトにサービス拒否(DoS)攻撃を仕掛けようとする。しかし、このワームが DoS 攻撃に成功するのは以下の状況を満たした場合に限る。

- ・ 発症期間中に感染した、あるいは、再起動された Windows XP 上でワームが動作している場合。
- ・ 発症期間中に感染し、感染後一度も再起動されていない Windows 2000 上でワームが動作している場合。
- ・ 発症期間中に感染し、感染後に再起動された Windows 2000 上でワームが動作しており、かつ、そのコンピュータに現在ログインしているユーザが管理者権限を持っている場合。

8. windowsupdate.com に対するサービス拒否(DoS)攻撃のトラフィックには、次のような特徴がある。

- ・ windowsupdate.com のポート 80 で SYN flood 状態。
- ・ HTTP パケットを毎秒 50 個ずつ送信しようとする。
- ・ 各パケットのサイズは 40 バイト。
- ・ windowsupdate.com のエントリが DNS 上に見つからない場合、宛先アドレスに

	<p>255.255.255.255 を使用する。</p> <p>このトラフィックに固有の TCP と IP ヘッダーの特徴は以下の通り</p> <ul style="list-style-type: none"> <li>・ IP identification = 256</li> <li>・ Time to Live = 128</li> <li>・ Source IP address = a.b.x.y ( a.b はホスト IP の先頭 2 つの値, x.y はランダムな値, ab もランダムな値の場合もある。)</li> <li>・ Destination IP address = "windowsupdate.com" の dns 変換値。</li> <li>・ TCP Source port 1000 - 1999</li> <li>・ TCP Destination port = 80</li> <li>・ TCP Sequence number 下位バイト 2 つは常に 0 に設定されている。上位バイト 2 つはランダム。</li> <li>・ TCP Window size = 16384</li> </ul> <p>9. このワームには次のテキストが含まれてるが、画面に表示されることはない。</p> <p>I just want to say LOVE YOU SAN!!</p> <p>billy gates why do you make this possible ? Stop making money and fix your software!!</p>
<p><b>感染・発症防止方法</b></p>	<p>1. W32.Blaster.Worm は、DCOM RPC の脆弱性を利用する。詳細については、マイクロソフト セキュリティ情報 MS03-026 を参照。そこから修正パッチをダウンロードすることができる。</p> <p>2. 感染予防策として、ファイアウォールで TCP ポート 4444 へのアクセスをブロックする。次のアプリケーションを使用していない場合は、次の該当するポートもブロックする。</p> <ul style="list-style-type: none"> <li>・ TCP ポート 135, "DCOM RPC"</li> <li>・ UDP ポート 69, "TFTP"</li> </ul>
<p><b>ウイルスの駆除方法</b></p>	<p><b>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。</b></p> <p><b>1. インターネット接続を回復する</b></p> <p>Windows 2000/XP では多くの場合、リモートコントロールプロシジャ (RPC) サービスの設定を変更することで、コンピュータをシャットダウンさせることなく、インターネットへの接続を可能にする。次の手順を行う</p> <ol style="list-style-type: none"> <li>1. [スタート]ボタンを押し、[ファイル名を指定して実行]をクリックする ([ファイル名を指定して実行]ダイアログボックスが表示される)。</li> <li>2. SERVICES.MSC /S と入力する。</li> </ol> <p>その後、[OK]をクリックする。(サービスウィンドウが開く)</p> <ol style="list-style-type: none"> <li>3. 右側の画面で、"Remote Procedure Call (RPC)" を探す。 ( "Remote Procedure Call (RPC) Locator" というサービスがあるが、これら 2 つのサービスは異なる。)</li> <li>4. "Remote Procedure Call (RPC)" を選択後、右クリックし、プロパティを開く。</li> <li>5. 回復タグをクリックする。</li> <li>6. ドロップダウンリストを使用し、「最初のエラー」、「次のエラー」、「その後のエラー」の値を "サービスを再起動する" に変更する。</li> <li>7. 適用をクリックし、次に OK をクリックする。</li> </ol> <p><b>注意: ワームの駆除後、これらの設定は必ず元に戻す。</b></p> <p><b>2. 有害なプロセスを停止する</b></p> <ol style="list-style-type: none"> <li>1. Ctrl+Alt+Delete キーを同時に押す。</li> <li>2. [タスクマネージャ]をクリックする。</li> <li>3. [プロセス]タブをクリックする。</li> </ol>

	<ol style="list-style-type: none"> <li>4. リスト最上部のイメージ名をダブルクリックしてプロセスをアルファベット順に並べ替える。</li> <li>5. リストをスクロールして、msblast.exe を探す。</li> <li>6. 該当するファイルを発見したら、それをクリックして[プロセスの終了]をクリックする。</li> <li>7. タスクマネージャを閉じる。</li> </ol> <p><b>3. 感染ファイルを探して削除する</b> Windows エクスプローラを開き、%System%フォルダにある msblast.exe を探して削除する。</p> <p><b>4. 変更されたレジストリを元に戻す</b></p> <ol style="list-style-type: none"> <li>1. [スタート]ボタンを押し、[ファイル名を指定して実行]をクリックする。([ファイル名を指定して実行]ダイアログボックスが表示される。)</li> <li>2. regedit と入力します。 その後、[OK]をクリックする。(レジストリ エディタが開く。)</li> <li>3. 次のレジストリキーを選択する。 HKEY_LOCAL_MACHINE¥Software¥Microsoft¥Windows¥CurrentVersion¥Run</li> <li>4. 画面右側で次の値を削除する。 "windows auto update"="msblast.exe"</li> <li>5. レジストリエディタを終了する。</li> </ol> <p><b>5. DCOM RPC の脆弱性を解消するためマイクロソフト社の修正パッチを入手・適用する</b> W32.Blaster.Worm は、コンピュータに感染する目的で、TCP ポート 135 を使い、DCOM RPC を悪用する。また、windowsupdate.com に対しサービス拒否攻撃(DoS 攻撃)を仕掛けようとする。これらの問題を解消するためには、マイクロソフト社の修正パッチを早急に適用する必要がある。修正パッチは、マイクロソフト セキュリティ情報 MS03-026 から入手することができる。</p> <p><b>なお、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自己責任において使用すること。</b></p>
<p><b>その他</b></p>	<p><b>DoS によるネットワーク負荷の緩和</b></p> <p>2003 年 8 月 15 日、マイクロソフトは、windowsupdate.com の DNS レコードを除去した。これにより、ワームの DNS を悪用する機能が、マイクロソフトの Windows Update 機能自体に影響を与えることはない。ネットワーク管理者は、次の推奨策を利用することで、サービス拒否攻撃(DoS)によるネットワーク負荷を緩和することができる。</p> <ul style="list-style-type: none"> <li>・ windowsupdate.com を特定の社内 IP アドレスに再ルーティングする。IDS などを有する場合感染したコンピュータに警告が通知される。</li> <li>・ ルータに詐称対策(アンチスプーフイング)ルールを設定する。これにより、大半のパケットがネットワークの外部に送信されることを阻止することができる。uRPF または送出側の ACL を使用すると非常に効果的である。</li> </ul>