

ウイルス解析報告書

ウイルス名	W32.Welchia.B.Worm (別名 :W32/Nachi.worm.b [McAfee], W32/Nachi-B [Sophos], Win32.Nachi.B [Computer Associates], WORM_NACHI.B [Trend], Worm.Win32.Welchia.b [Kaspersky])
プログラム名及び容量 (添付ファイル名)	プログラム名 svchost.exe 容 量 :12,800 バイト
種別	ワーム
プログラム言語	不明
発症環境	Windows 2000, Windows XP
発見日時	2004 年 2 月 12 日
発見場所	アメリカ (最初の感染報告)
危険性	DCOM RPC の脆弱性(MS03-026)、WebDAV の脆弱性(MS03-007)、Workstation サービスのバッファオーバーランの脆弱性(MS03-049)及び Locator Service の脆弱性(MS03-001)の複数の脆弱性を攻撃し、コンピュータへ侵入を試みるため非常に危険。危険度は 5 段階の 3 (6 が最も危険)。
発症条件	脆弱性が存在するコンピュータがワームの攻撃を受けたとき。
ウイルスの活動、影響	<ol style="list-style-type: none"> 1. 感染したコンピュータのロケールが中国語、韓国語、英語の場合、マイクロソフトの Windows Update サイトからマイクロソフト Workstation サービスのバッファオーバーラン等の修正パッチをダウンロード、インストールし、その後、コンピュータを再起動しようとする。W32.Mydoom.A@mm および W32.Mydoom.B@mm ワームの駆除を試みる。生成した IP アドレスに対して攻撃を行う。ただし、2004 年 6 月 1 日以降若しくはワーム本体のファイルのタイムスタンプから 120 日経過後に起動しなくなる。 2. 感染したコンピュータのロケールが日本語の場合、Web ページの改ざんを行い、生成した IP アドレスに対して攻撃を行う。
被害の規模	発見から 4 日間で 793 件 (国内は 30 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.Welchia.Worm (2003 年 8 月)
ウイルスの動作概要	<p>W32.Welchia.B.Worm が実行されると、次のことを行う</p> <ol style="list-style-type: none"> 1. "WksPatch_Mutex" というミューテックスを作成し、ワームが複数同時に起動することを防ぐ。 2. 自分自身をシステムフォルダ %System% の下にある drives\svchost.exe としてコピーする。 %System% フォルダ は不定。標準では C:\Windows\System (Windows 95/98/ Me)、C:\Winnt\System32 (Windows NT/2000)、あるいは C:\Windows\System32 (Windows XP)。 3. 次のサービスを作成する。 サービス名: WksPatch サービスバイナリ: %System%\drives\svchost.exe サービス表示名: <%文字列 1%> <%文字列 2%> <%文字列 3%> の形式となる <%文字列 1%> のグループは、次のいずれかになる。 <ul style="list-style-type: none"> ・ System、Security、Remote、Routing、Performance、Network、License、Internet <%文字列 2%> のグループは、次のいずれかになる。 <ul style="list-style-type: none"> ・ Logging、Manager、Procedure、Accounts、Event <%文字列 3%> のグループは、次のいずれかになる。 <ul style="list-style-type: none"> ・ Provider、Sharing、Messaging、Client 又は無し このサービスは、起動時に自動的に起動するように設定される。 レジストリキー「DisplayName」(例 :System Procedure Client) に記憶された値で

サービスを起動する。
 サービス名が System Procedure Client となった時の例

レジストリ エディタ

レジストリ(R) 編集(E) 表示(V) お気に入り(E) ヘルプ(H)

名前	種類	データ
ab (標準)	REG_SZ	(値の設定なし)
ab Description	REG_SZ	ネットワーク上のコンピュータの最新のー覧を管理し、その...
ab DisplayName	REG_SZ	System Procedure Client
ab ErrorControl	REG_DWORD	0x00000000 (0)
ab ImagePath	REG_EXPAND_SZ	C:\WINNT\System32\drivers\svchost.exe
ab ObjectName	REG_SZ	LocalSystem
ab Start	REG_DWORD	0x00000002 (2)
ab Type	REG_DWORD	0x00000010 (16)

マイ コンピュータ\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WksPatch

サービス

操作(A) 表示(V)

名前	説明	状態	スタートアップの種類	ログオン
Routing and Remote Acce...	ローカル エリア ネットワーク...	無効		LocalSystem
RunAs Service	別の資格情報の...	開始	自動	LocalSystem
Security Accounts Manager	ローカル ユーザー...	開始	自動	LocalSystem
Server	RPC サポートとファ...	開始	自動	LocalSystem
Simple Mail Transport Prot...	ネットワークを使用...	開始	自動	LocalSystem
Simple TCP/IP Services	次の TCP/IP サー...	開始	自動	LocalSystem
Single Instance Storage Gr...	単一インスタンス格...	手動		LocalSystem
Smart Card	コンピュータに接続...	手動		LocalSystem
Smart Card Helper	コンピュータに接続...	手動		LocalSystem
SNMP Service	ネットワーク デバイ...	開始	自動	LocalSystem
SNMP Trap Service	ローカルまたはリモ...	手動		LocalSystem
System Event Notification	Windows ログオン...	開始	自動	LocalSystem
System Procedure Client	ネットワーク上のコ...	開始	自動	LocalSystem
Task Scheduler	プログラムを指定し...	開始	自動	LocalSystem
TCP/IP NetBIOS Helper S...	NetBIOS over TC...	開始	自動	LocalSystem
TCP/IP Print Server	ライン プリンタプロ...	開始	自動	LocalSystem
Telephony	テレフォニー デバイ...	開始	手動	LocalSystem
Telnet	リモート ユーザーが...	手動		LocalSystem
Terminal Services	マルチセッションの...	開始	自動	LocalSystem
Terminal Services Licensi...	ライセンス サーバー...	開始	自動	LocalSystem
Trivial FTP Daemon	Trivial FTP インタ...	手動		LocalSystem

(ローカル コンピュータ) System Procedure Client のプロパティ

全般 ログオン 回復 依存関係

サービス名: WksPatch

表示名(N): System Procedure Client

説明(D): ネットワーク上のコンピュータの最新のー覧を管理し、そのー覧を要

実行ファイルのパス(H): C:\WINNT\System32\drivers\svchost.exe

スタートアップの種類(E): 自動

サービスの状態: 開始

開始(S) 停止(T) 一時停止(P) 再開(R)

ここでサービスを開始するときに適用する開始パラメータを指定してください。

開始パラメータ(M):

OK キャンセル 適用(A)

4. 感染したコンピュータのロケールが日本語の場合、IIS のドキュメント・ルートに設定されているフォルダ (例 :C:\inetpub\wwwroot) 及び IISHelp フォルダ (例 %Windir%\Help\IISHelp\common) で.shtml、.shtm、.stm、.cgi、.php、.html、.htm、.asp 拡張子を持つファイルを検索し、次の.htm ファイルで上書きする。
 %Windir% は不定。(標準では、C:\Windows あるいは C:\Winnt)



5. 感染したコンピュータのロケールが中国語、韓国語、英語の場合、次のレジストリキーを検索し、W32.Mydoom.A@mm および W32.Mydoom.B@mm の存在を確認する。

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion
 \Explorer\ComDlg32\Version
 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion
 \Explorer\ComDlg32\Version

キーが確認できた場合、W32.Mydoom.A@mm および W32.Mydoom.B@mm ワームを駆除するため次のファイルの削除を試みる。

%System%\ctfmon.dll
 %System%\Explorer.exe
 %System%\shimgapi.dll
 %System%\TaskMon.exe

次のレジストリキーから、値 "Taskmon" を削除する。

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

次のレジストリキーの値を

HKEY_LOCAL_MACHINE\CLSID\{E6FB5E20-DE35-11CF-9C87-00AA005127ED}
 \InProcServer32

次の内容に戻す。

@="%SystemRoot%\System32\webcheck.dll"

OS \ ロケール	Windows2000 Professional	Windows2000 Server	WindowsXP Home	WindowsXP Professional
英語				
韓国語				
中国語				
日本語	x	x	x	x

:駆除される x :駆除されない

HOSTS ファイルを次のテキストで上書きする。

```
#
#
127.0.0.1 localhost
```

6. 感染したコンピュータのロケールが中国語、韓国語、英語の場合、マイクロソフトの Windows Update Web サイトから次のうちいずれかの修正プログラムをダウンロードしてインストールし、その後、コンピュータを再起動する。

<http://download.microsoft.com/download/4/d/3/4d375d48-04c7-411f-959b-3467c5ef1e9a/WindowsXP-KB828035-x86-CHS.exe>
(WindowsXP 中国語版 MS03-043)

<http://download.microsoft.com/download/a/4/3/a43ea017-9abd-4d28-a736-2c17dd4d7e59/WindowsXP-KB828035-x86-KOR.exe>
(WindowsXP 韓国語版 MS03-043)

<http://download.microsoft.com/download/e/a/e/ea4109-0870-4dd3-88e0-a34035dc181a/WindowsXP-KB828035-x86-ENU.exe>
(WindowsXP 英語版 MS03-043)

<http://download.microsoft.com/download/9/c/5/9c579720-63e9-478a-bdcb-70087ccad56c/Windows2000-KB828749-x86-CHS.exe>
(Windows2000 中国語版 MS03-049)

<http://download.microsoft.com/download/0/8/4/084be8b7-e000-4847-979c-c26de0929513/Windows2000-KB828749-x86-KOR.exe>
(Windows2000 韓国語版 MS03-049)

<http://download.microsoft.com/download/3/c/6/3c6d56ff-ff8e-4322-84cb-3bf9a915e6d9/Windows2000-KB828749-x86-ENU.exe>
(Windows2000 英語版 MS03-049)

7. IP アドレスを生成し、それらの IP アドレスに対し次の確率で脆弱性に対する攻撃データを選択し、他のシステムへ感染活動を開始する。

• WebDav の脆弱性(MS03-007)を攻撃する場合 (TCP ポート80)

ランダムに IP アドレスを生成する 確率 3/27

• Locator Service の脆弱性(MS03-001)を攻撃する場合 (TCP ポート445)

ランダムに IP アドレスを生成する 確率 3/27

• DCOM RPC の脆弱性(MS03-026)を攻撃する場合 (TCP ポート135)

自己 IP アドレスを元にして加算していく 確率 2/27

• Workstation サービス の脆弱性を攻撃する場合 (TCP ポート445)

自己 IP アドレスを元にして加算していく 確率 1/27

残る 18/27 は、通常 1 時間スリープ状態になった後に攻撃方法の選択に戻るが、ロケールが日本語の場合は、続けて攻撃パターンの選択を行う

IP アドレスの生成

ランダムに IP アドレスを生成する場合、乱数を発生させ、第 1 から第 4 オクテットの数を生成する。この際、各オクテットには値の範囲が存在する。

第 1 オクテットは 2 ~ 239

第 2 オクテットは 0 ~ 255

第 3 オクテットは 0 ~ 255

第 4 オクテットは 1 ~ 254

の範囲の値となるが、第 1 オクテットが 192、10、172 であるか、第 2 オクテットが 168、16、32 のうちいずれかに合致する場合には、IP アドレスを生成し直す。

自己 IP アドレスを元にして加算していく場合は、IP アドレスを加算しながら、ロケールが日本語の場合は 131,072 回、それ以外の場合は 65,536 回攻撃を行う。また、自己 IP アドレスを元に生成される IP アドレスは、

	<ul style="list-style-type: none"> ・ 確率 1/5 で、第 1、第 2 オクテットは、感染したコンピュータの IP アドレスから取得し、第 3 オクテット0、第 4 オクテットは 0 から、アドレスを加算しながら攻撃を行う ・ 確率 2/5 で、感染したコンピュータの IP アドレスから取得し、第 1 オクテットはそのまま第 2 オクテットは、ロケールが日本語の場合 2 を、ロケールがその他の場合は 1 を加算したアドレス (日本語版で IP アドレスが 210.24.0.0 の場合 210.26.0.0 を初期値とする)、第 3 オクテット0、第 4 オクテット0 からアドレスを加算しながら攻撃を行う ・ 確率 2/5 で、感染したコンピュータの IP アドレスから取得し、第 1 オクテットはそのまま、第 2 オクテットはロケールが日本語の場合 2 を、ロケールがその他の場合は 1 を減算したアドレス (日本語版で IP アドレスが 210.24.0.0 の場合 210.22.0.0 を初期値とする)、第 3 オクテット0、第 4 オクテット0 からアドレスを加算しながら攻撃を行う <p>8. ランダムに選択した TCP ポートで Web サーバを実行し、感染させた脆弱なコンピュータがワーム自身のコピーである WksPatch.exe ファイルをダウンロードできるようにする。</p> <p>9. 2004 年 6 月 1 日、あるいは、ワームのファイルのタイムスタンプから 120 日間経過すると、自動的に活動を終了する。</p>
感染 発症防止方法	<ol style="list-style-type: none"> 1. マイクロソフト社の提供する修正パッチ (MS03-001、MS03-007、MS03-026、MS03-049) を適用する。 2. 脆弱性等をリモートから悪用されるのを阻止するために、TCP ポート 80、135、445 に対するインバウンドをファイアウォールでブロックする。
ウイルスの駆除方法	<p>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。</p> <ol style="list-style-type: none"> 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. 感染ファイルを探して削除する。 %System%¥drives¥svchost.exe 5. 次のレジストリのサブキーを削除する。 HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services 削除するサブキー WksPatch <p>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。</p> <p>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。</p>
その他	無