


ウイルス解析報告書

ウイルス名	W32.Reatle@mm (別名: Win32.Reatle.A [Computer Associates], Lebreath [F-Secure], Net-Worm.Win32.Lebreath.gen [Kaspersky Lab], W32/Reatle.gen@MM [McAfee], W32/Lebreath-A [Sophos], WORM_REATLE.A [Trend Micro])
プログラム名および容量(添付ファイル名)	プログラム名: windows.exe, attach.tmp 容 量: 15,261 バイト
種別	ワーム
プログラム言語	C
発症環境	Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows XP
発見日	2005年7月15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2(5が最も危険)。
発症条件	ワームによって送信されたメールの添付ファイルを実行したとき。または、Microsoft Windows Local Security Authority Service の脆弱性(MS04-011)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	このワームは、独自の SMTP エンジンを使用して自分自身を送信するメール送信ワームである。また、TCP ポート 445 を使用して Microsoft Windows Local Security Authority Service の脆弱性(MS04-011)を悪用することにより拡散する。
被害の規模	発見から4日間で11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	なし
ウイルスの動作概要	<p>ワームにより送信されるメールには、次の特徴がある。</p> <div style="text-align: center;">  </div> <p>差出人: 次のいずれかを使用する。</p> <ul style="list-style-type: none"> ・adam ・admin ・alerts ・alex ・bob ・brenda ・brent ・dan ・david ・fred

- helen
- jack
- jane
- jerry
- joe
- john
- jon
- josh
- leo
- linda
- mary
- matt
- michael
- mike
- paul
- ray
- robert
- root
- sales
- steve
- support
- ted
- tom

ドメインは次のいずれかを使用する。

- @nai.com
- @gmail.com
- @trendmicro.com
- @support.com
- @matrix.com
- @aol.com
- @ca.com
- @mcafee.com
- @arcor.com
- @antivirus.com
- @google.com
- @hotmail.com
- @yahoo.com
- @microsoft.com
- @msn.com
- @symantec.com

件名:

次のいずれかを使用する。

- Message could not be delivered
- Bug
- Error
- Email
- Mail Delivery System
- Importnat Information
- **WARNING** Your Account Currently Disabled.
- Password
- info
- Hello

本文:

次のいずれかを使用する。

- ・Your credit card was charged for \$500 USD. For additional information see the attachment.
 - ・Binary message is available.
 - ・The message contains Unicode characters and has been sent as a binary attachment.
 - ・Here are your banks documents
 - ・The original message was included as an attachment.
 - ・We have temporarily suspended your email account checkout the attachment for more info.
 - ・You have successfully updated the password of your domain account checkout the attachment for more info.
 - ・Important Notification checkout the attachment for more info.
 - ・Your Account Suspended checkout the document.
 - ・Your password has been updated checkout the document.
 - ・checkout the attachment.
 - ・Hello,
- I was in a hurry and I forgot to attach an important document. Please see attached.

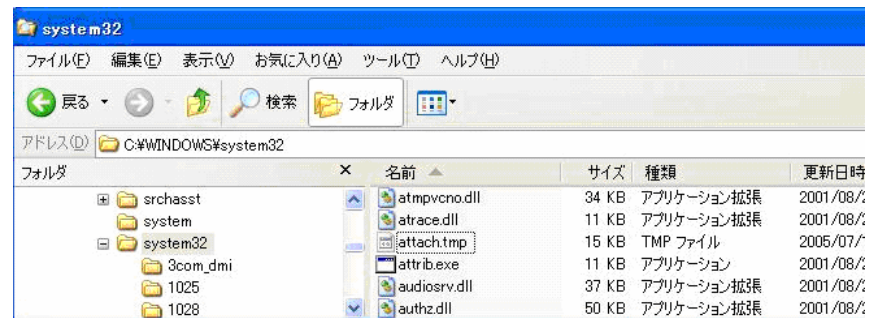
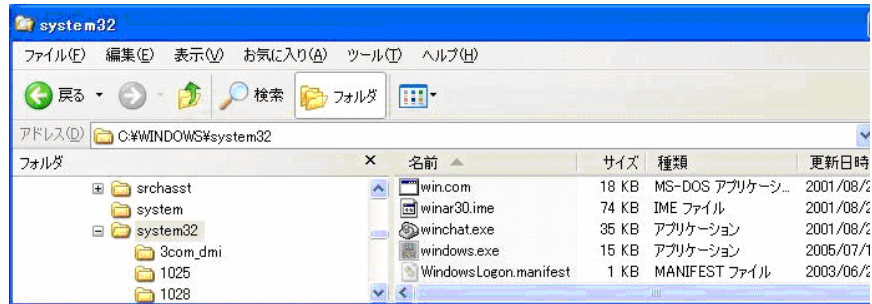
添付ファイル:

次のいずれかを使用する。

- ・payment.doc [多数のスペース] .scr
- ・about.doc [多数のスペース] .bat
- ・help.doc [多数のスペース] .exe
- ・account-report.exe
- ・about.cpl
- ・about.scr
- ・admin.bat
- ・archive.cpl
- ・archive.exe
- ・box.bat
- ・box.scr
- ・data.bat
- ・data.scr
- ・doc.pif
- ・docs.cpl
- ・docs.scr
- ・document.cpl
- ・document.exe
- ・file.cpl
- ・inbox.cpl
- ・inbox.exe
- ・order.cpl
- ・order.exe
- ・read.cpl
- ・read.exe
- ・readme.cpl
- ・readme.scr

このワームが実行されると、次のことを行う。

1. ワーム自身を%System%¥Windows.exe、%System%¥attach.tmpとしてコピーする。

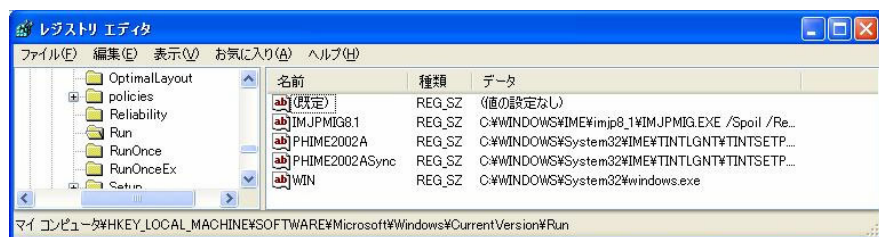


Windows のシステムフォルダ%System% (標準では、C:¥Windows¥System、C:¥Winnt¥System32、または C:¥Windows¥System32)

2. 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
 - ・HKEY_LOCAL_MACHINE¥Software¥Microsoft¥Windows NT¥CurrentVersion¥Windows

次の値を追加する。

・"WIN"="C:¥WINNT¥System32¥windows.exe"



Windows の Firewall の設定を変更するため、次のレジストリキーの

- ・HKEY_LOCAL_MACHINE¥Software¥Policies¥Microsoft¥WindowsFirewall¥DomainProfile
- ・HKEY_LOCAL_MACHINE¥Software¥Policies¥Microsoft¥WindowsFirewall¥StandardProfile
- ・HKEY_CURRENT_USER¥Software¥Policies¥Microsoft¥WindowsFirewall¥DomainProfile
- ・HKEY_CURRENT_USER¥Software¥Policies¥Microsoft¥WindowsFirewall¥StandardProfile

次の値を変更する。

・"EnableFirewall"="1"

Windows のセキュリティ機能を無効にするため、次のレジストリキーの

- ・HKEY_CURRENT_USER¥Software¥Policies¥Microsoft¥WindowsUpdate¥AU
- ・HKEY_LOCAL_MACHINE¥Software¥Policies¥Microsoft¥WindowsUpdate¥AU

次の値を変更する。

- ・"NoAutoUpdate"="1"
- ・"AUOptions"="1"

同様に、次のレジストリキーを

- ・HKEY_CURRENT_USER¥Software¥Microsoft¥Security Center
- ・HKEY_LOCAL_MACHINE¥Software¥Microsoft¥Security Center

次の値に変更する。

- ・"AntiVirusDisableNotify"="1"
- ・"UpdatesDisableNotify"="1"
- ・"FirewallDisableNotify"="1"

システムの復元機能を無効にするため、次のレジストリキーを

- ・HKEY_CURRENT_USER¥Software¥Microsoft¥Windows NT¥CurrentVersion¥SystemRestore
- ・HKEY_LOCAL_MACHINE¥Software¥Microsoft¥Windows NT¥CurrentVersion¥SystemRestore

次の値に変更する。

- ・"DisableSR"="1"

タスクマネージャおよびレジストリツールを無効にするため、次のレジストリキーを

- ・HKEY_CURRENT_USER¥Software¥Microsoft¥Windows¥CurrentVersion¥Policies¥System
- ・HKEY_LOCAL_MACHINE¥Software¥Microsoft¥Windows¥CurrentVersion¥Policies¥System

次の値に変更する。

- ・"DisableTaskMgr"="1"
- ・"DisableRegistryTools"="1"

3. TCP ポート 8885 を開く。

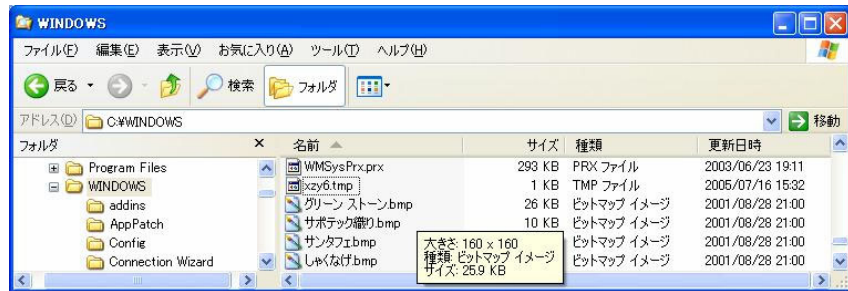
4. 次の拡張子を持つファイルからメールアドレスを収集し、%Windir%¥xzy6.tmp ファイルに保存する。

- ・.asp
- ・.txt
- ・.adb
- ・.tbb
- ・.dbx
- ・.html
- ・.htm
- ・.wab

ただし、次の文字列を含むメールアドレスは無視する。

- ・icrosof
- ・.gov
- ・panda
- ・f-secur
- ・icrosoft
- ・winrar
- ・winzip
- ・@mcafee
- ・@trendmicro

- ・@mm
- ・@noreply
- ・@sopho
- ・@norman
- ・@virusli
- ・@norton
- ・@fsecure
- ・@panda
- ・@avp
- ・@microsoft
- ・@symantec



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>)

5. 収集したメールアドレスに対し、独自の SMTP エンジンを使用してメールを送信する。
6. www.symantec.com に対し、ランダムな IP アドレスを送信元として ICMP による DoS 攻撃を行う。
7. 次の IP アドレスを生成し、生成した IP アドレスの TCP ポート 445 に対して Microsoft Windows Local Security Authority Service の脆弱性(MS04-011)を悪用し、攻撃元のコンピュータの TCP ポート 8885 に接続させ、ワームをダウンロードし実行させる。
 - (1) 全てのオクテットがランダムな IP アドレス
 - (2) 感染したコンピュータの IP アドレスを元に、第 3、第 4 オクテットをランダムな IP アドレス
8. 次のファイルをダウンロードし実行する。このファイルは、W32.Rants@mm である。
 ・[http://jOr.biz/\[削除\]/update3.exe](http://jOr.biz/[削除]/update3.exe)

感染・発症防止方法

1. 予期せぬメールが届いた場合には、安易に開封したり、添付ファイルを開かない。特に「ウイルスの動作概要」で記述したようなメールには注意する。
2. Microsoft Windows Local Security Authority Service の脆弱性 (MS04-011) のパッチを適用する。
3. リモートから脆弱性を悪用されることを防止するために、TCP ポート 8885 等をファイアウォールでブロックする。
4. 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(WindowsNT では VGA モード)で再起動する。
4. 次のファイルを削除する。
- %System%\Windows.exe
 - %System%\attach.tmp
 - %Windir%\xzy6.tmp
5. レジストリに行われた変更を元に戻す。(レジストリエディタを開けない場合は、ワクチンベンダーから提供されているツール等を使用して、レジストリエディタが使用できるように設定する必要がある。

次のレジストリキーから

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Windows

次の値を削除する。

- "WIN"="C:\WINNT\System32\windows.exe"

セキュリティ機能を保つため、必要に応じて以下のように設定する。

次のレジストリキーを

- HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\DomainProfile
- HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\StandardProfile
- HKEY_CURRENT_USER\Software\Policies\Microsoft\WindowsFirewall\DomainProfile
- HKEY_CURRENT_USER\Software\Policies\Microsoft\WindowsFirewall\StandardProfile

次の値に変更する。

- "EnableFirewall" = "1"

次のレジストリキーを

- HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\WindowsUpdate\AU
- HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate\AU

次の値に変更する。

- "NoAutoUpdate" = "1"
- "AUOptions" = "1"

次のレジストリキーを

- HKEY_CURRENT_USER\Software\Microsoft\Security Center
- HKEY_LOCAL_MACHINE\Software\Microsoft\Security Center


次の値に変更する。

- "AntiVirusDisableNotify" = "0"
- "UpdatesDisableNotify" = "0"
- "FirewallDisableNotify" = "0"

次のレジストリキーを

- HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\SystemRestore
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\SystemRestore

次の値に変更する。

	<p>・"DisableSR"="0"</p> <p>次のレジストリキーを</p> <ul style="list-style-type: none"> ・HKEY_CURRENT_USER¥Software¥Microsoft¥Windows¥CurrentVersion¥Policies¥System ・HKEY_LOCAL_MACHINE¥Software¥Microsoft¥Windows¥CurrentVersion¥Policies¥System <p>次の値に変更する。</p> <ul style="list-style-type: none"> ・"DisableTaskMgr"="0" ・"DisableRegistryTools"="0" <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>その他</p>	<p>1 Windows 2000 Professional SP4(日本語版)は、このワームが悪用する Microsoft Windows Local Security Authority Service の脆弱性(MS04-011)の攻撃を受けた場合、次のダイアログを表示し再起動するため、このワームには感染しない。</p> <div data-bbox="694 689 1177 1025" style="border: 1px solid gray; padding: 5px; margin: 10px 0;"> <p style="text-align: center;">システムのシャットダウン</p> <div style="display: flex; align-items: center;">  <div> <p>システムはシャットダウンされます。進行中の作業をすべて保存し、ログオフしてください。保存されていない情報は失われます。シャットダウンは、NT AUTHORITY¥SYSTEM によって開始されました</p> <p style="text-align: center;">シャットダウンまで： 00:00:26</p> <p>メッセージ</p> <p>システム プロセス 'C¥WINNT¥system32¥lsass.exe' は、状態コード 128 で突然終了しました。システムをシャットダウンし、再起動します。</p> </div> </div> </div> <p>2 平成 17 年末現在で 15 件(国内 0 件)の届出がシマンテック社に寄せられている。</p>