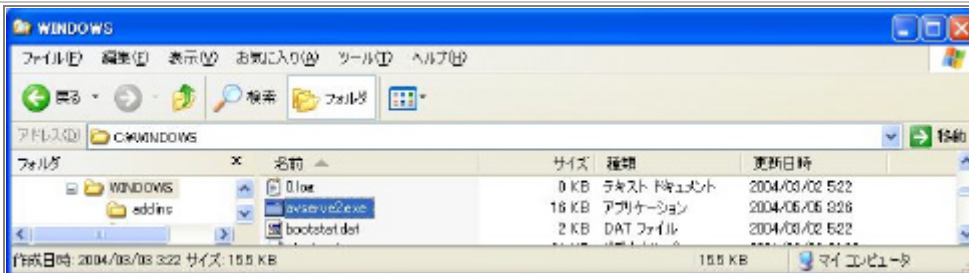
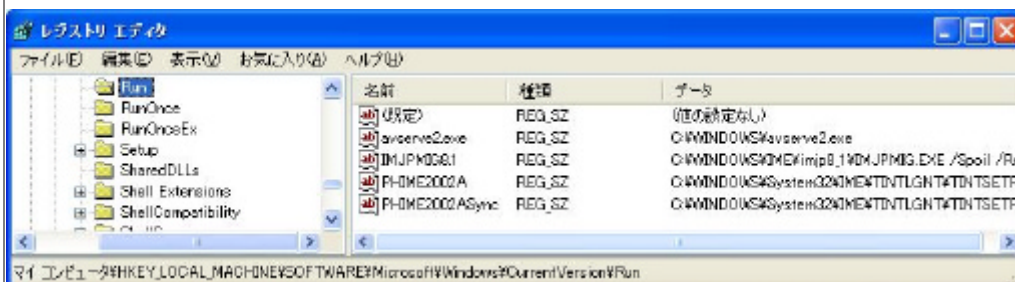


ウイルス解析報告書

ウイルス名	W32.Sasser.B.Worm (別名 :WORM_SASSER.B [Trend], W32/Sasser.worm.b [McAfee], Worm.Win32.Sasser.b [Kaspersky], W32/Sasser-B [Sophos], Win32.Sasser.B [Computer Associates], Sasser.B [F-Secure], W32/Sasser.B.worm [Panda], Win32/Sasser.B.worm [RAV], W32/Sasser.B [F-Prot])																																														
プログラム名及び容量 (添付ファイル名)	プログラム名 avserve2.exe 容 量 :15,872 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 5 月 2 日																																														
発見場所	ドイツ (最初の感染報告)																																														
危険性	感染力が強い。短時間で多くの届出が寄せられた。危険度は 5 段階の 4 (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	<p>このワームは、ランダムに生成した IP アドレスを持つコンピュータに対して Microsoft Windows LSASS の脆弱性 (MS04-011) を利用することにより感染を行い、脆弱性に未対応のシステムを介して拡散する。</p> <p>なお、このワームは Windows 95/98/Me コンピュータ上でも動作するが、感染活動は行わない。Windows 95/98/Me システムは、このワームに感染することはないものの、脆弱なシステムに接続するためにワームによって利用される可能性がある。</p>																																														
被害の規模	発見から 52 時間で 5877 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	<p>Sasser については 5 月初旬に出現し、5 月 6 日時点で 4 種類の Sasser が確認されている。それぞれのバージョンについて比較を記す。</p> <p>Sasser.A, Sasser.B に対して、Sasser.C は攻撃が高速化 (スレッド数の増加) している。また、Sasser.D は Nachi(Welchia)ワーム同様、攻撃前に ICMP (echo) でサーチを行い応答があったもののみ感染活動を行うなど動作が変移している。</p> <table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <thead> <tr> <th>種別</th> <th>サイズ (バイト)</th> <th>ファイル名</th> <th>発生日付 (US)</th> <th>スレッド数</th> <th>攻撃ポート</th> <th>ftp ポート</th> <th>ハットドア</th> </tr> </thead> <tbody> <tr> <td>A</td> <td>15,872</td> <td>avserve.exe</td> <td>4 月 30 日</td> <td>128</td> <td>445/tcp</td> <td>5554</td> <td>9996</td> </tr> <tr> <td>B</td> <td>15,872</td> <td>avserve2.exe</td> <td>5 月 1 日</td> <td>128</td> <td>445/tcp</td> <td>5554</td> <td>9996</td> </tr> <tr> <td>C</td> <td>15,872</td> <td>avserve2.exe</td> <td>5 月 1 日</td> <td>1024</td> <td>445/tcp</td> <td>5554</td> <td>9996</td> </tr> <tr> <td>D</td> <td>16,384</td> <td>skynetave.exe</td> <td>5 月 3 日</td> <td>128</td> <td>icmp 445/tcp</td> <td>5554</td> <td>9995</td> </tr> </tbody> </table> <p>sasser.C はスレッド数 1024 のため、445/tcp による感染攻撃のペースが速く CPU 使用率が 100% 近くになる。</p>							種別	サイズ (バイト)	ファイル名	発生日付 (US)	スレッド数	攻撃ポート	ftp ポート	ハットドア	A	15,872	avserve.exe	4 月 30 日	128	445/tcp	5554	9996	B	15,872	avserve2.exe	5 月 1 日	128	445/tcp	5554	9996	C	15,872	avserve2.exe	5 月 1 日	1024	445/tcp	5554	9996	D	16,384	skynetave.exe	5 月 3 日	128	icmp 445/tcp	5554	9995
種別	サイズ (バイト)	ファイル名	発生日付 (US)	スレッド数	攻撃ポート	ftp ポート	ハットドア																																								
A	15,872	avserve.exe	4 月 30 日	128	445/tcp	5554	9996																																								
B	15,872	avserve2.exe	5 月 1 日	128	445/tcp	5554	9996																																								
C	15,872	avserve2.exe	5 月 1 日	1024	445/tcp	5554	9996																																								
D	16,384	skynetave.exe	5 月 3 日	128	icmp 445/tcp	5554	9995																																								
ウイルスの動作概要	<p>W32.Sasser.B.Worm が実行されると、次のことを行う</p> <ol style="list-style-type: none"> JumpallsNlsTillt というミューテックスを作成し、コンピュータ上でワームが複数同時に起動することを防ぐ。 Jobaka3 というミューテックスを作成する。 ワーム自身を %Windir%\Avserve2.exe としてコピーする。 %Windir% は Windows のインストール先フォルダで、標準では C:\Windows または C:\WINNT。 																																														



4. Windows の起動時に必ずワームが実行するようにレジストリの値を追加する。
次の値を
"avserve2.exe"="%Windir%\avserve2.exe"
次のレジストリキーに追加する。
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run



5. AbortSystemShutdown API を使用し、コンピュータのシャットダウンや再起動を妨害する。
6. 他のホストへワームを拡散させるために、TCP ポート5554 でFTP サーバを起動する。
7. 次の IP アドレスを除くすべてのホストアドレスを繰返しスキャンする。
127.0.0.1
10.x.x.x
172.16.x.x - 172.31.x.x (inclusive)
192.168.x.x
169.254.x.x
発見した IP アドレスを基に次の確率でランダムな IP アドレスを生成する。
52% (16/31) の確率で、
第 1 ~ 第 4 オクテット全てランダムに生成
25% (240/961) の確率で、
第 1,2 オクテットは自アドレス同一、第 3,4 オクテットはランダムに生成
23% (225/961) の確率で、
第 1 オクテットは自アドレスと同一、第 2,3,4 オクテットはランダムに生成
8. 生成した IP アドレスの TCP ポート445 への接続を試み、リモートコンピュータとの接続が確立すると、そのコンピュータにリモートシェルを奪取するコードを送信する。奪取したシェルを利用し TCP ポート9996 にバックドアを開く。
9. リモートコンピュータ上に作成したバックドアを使用して、感染しているコンピュータの TCP ポート5554 で動作中の FTP サーバに逆接続させ、ワームのコピーを転送する。その際ワームコピーには、4 桁または 5 桁の数字の後に .up.exe が続くファイル名が使用される。
10. Lsass.exe プロセスは、ワームが Windows の LSASS の脆弱性を攻撃した後でクラッシュする。その結果、Windows がアラートを表示し、1 分後にシステムがシャットダウンする。

	<p>11. C:\win2.log ファイルを作成する。このファイルには、ワームが最近感染を試みたコンピュータの IP アドレスと台数が記録される。</p>																								
<p>感染 発症防止方法</p>	<p>1. マイクロソフト社の提供する修正パッチ (MS04-011) 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5554、9996、445 をファイアウォールでブロックする。</p>																								
<p>ウイルスの駆除方法</p>	<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> <p>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。</p> <p>2. システムの復元オプションを無効にする。(Windows Me/XP)</p> <p>3. コンピュータをセーフモードで再起動する。</p> <p>4. 感染ファイルを削除する。 %Windir%\avserve2.exe</p> <p>5. レジストリに行われた変更を元に戻す。 次の値を "avserve2.exe"="%Windir%\avserve2.exe" 次のレジストリキーから削除する。 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run</p> <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>																								
<p>その他</p>	<p>Sasser.D について、各種日本語版 Windows 環境における感染状況を記す。</p> <table border="1" data-bbox="459 1294 1380 1585"> <thead> <tr> <th>OS 種別</th> <th>2000 Pro.</th> <th>2000 Sv</th> <th>XP Home</th> <th>XP Pro.</th> <th>2003 Sv</th> </tr> </thead> <tbody> <tr> <td>SP なし</td> <td>感染しないが、 レポート</td> <td>感染しないが、 レポート</td> <td>感染後、 レポート</td> <td>感染後、 レポート</td> <td>感染しない</td> </tr> <tr> <td>SP あり [2000.sp2 4] [XP.sp1]</td> <td>感染しないが、 レポート (SP2 同様)</td> <td>感染しないが、 レポート (SP2 同様)</td> <td>感染後、 レポート</td> <td>感染後、 レポート</td> <td>-</td> </tr> <tr> <td>MS04-011 パッチ適用</td> <td>感染しない</td> <td>感染しない</td> <td>感染しない</td> <td>感染しない</td> <td>-</td> </tr> </tbody> </table> <p>SP はサービスパックの略</p>	OS 種別	2000 Pro.	2000 Sv	XP Home	XP Pro.	2003 Sv	SP なし	感染しないが、 レポート	感染しないが、 レポート	感染後、 レポート	感染後、 レポート	感染しない	SP あり [2000.sp2 4] [XP.sp1]	感染しないが、 レポート (SP2 同様)	感染しないが、 レポート (SP2 同様)	感染後、 レポート	感染後、 レポート	-	MS04-011 パッチ適用	感染しない	感染しない	感染しない	感染しない	-
OS 種別	2000 Pro.	2000 Sv	XP Home	XP Pro.	2003 Sv																				
SP なし	感染しないが、 レポート	感染しないが、 レポート	感染後、 レポート	感染後、 レポート	感染しない																				
SP あり [2000.sp2 4] [XP.sp1]	感染しないが、 レポート (SP2 同様)	感染しないが、 レポート (SP2 同様)	感染後、 レポート	感染後、 レポート	-																				
MS04-011 パッチ適用	感染しない	感染しない	感染しない	感染しない	-																				