




Worm/Sasser.A

Kurzinformationen	
Virusname:	Worm/Sasser.A
Alias:	Sasser
Viren Typ:	Wurm
Dateigröße:	15.872 Bytes
Betriebssysteme:	Microsoft Windows 2000/XP/Server 2003
Ursprung:	unbekannt
Datum:	01.05.2004
Schadensroutine:	Nutzt Sicherheitslücke LSASS aus
VDF Version:	6.25.00.42

**Bedrohung:**

Schaden:  **low**
Verbreitung:  **medium**

Allgemeine Beschreibung:
<p>Worm/Sasser.A hat eine Dateigröße von 15.872 Bytes und kopiert sich als avserve.exe in das Windows Systemverzeichnis. Er nutzt die LSASS (Local Security Authority Subsystem Service) Sicherheitslücke von Microsoft aus.</p> <p>Sollten nicht alle Patches von Microsoft eingespielt sein oder keine aktive Firewall zum Internet bestehen, kann der Wurm sich auf dem Windows XP oder Windows 2000 System installieren..</p>

Symptome:
<ul style="list-style-type: none">• Im Root von Laufwerk C: findet sich eine Datei namens WIN.LOG

Infektionsweg:
<ul style="list-style-type: none">• LSASS Sicherheitslücke von Microsoft

Technische Details:
<p>Worm/Sasser.A verbreitet sich über eine LSASS (Local Security Authority Subsystem Service) Sicherheitslücke von Microsoft. Siehe dazu:</p>

<http://www.microsoft.com/technet/security/bulletin/MS04-011.msp>

Sollte der Anwender die Betriebssystem Windows XP oder Windows 2000 einsetzen und den oben genannte Microsoft Patch nicht eingespielt haben, kann der Wurm auf dem System installieren. Der Wurm scannt über den Port TCP 445 / TCP 9996 nach weiteren Rechnern, die diese Sicherheitslücke aufweisen. Ein FTP Script wird geladen welche sich über den Port 5554 die Dateien via FTP nachlädt.

Der Wurm Worm/Sasser.A kopiert sich in das Windows Verzeichnis als AVSERVE.EXE und legt folgenden Registry Eintrag an, damit er beim nächsten Systemstart automatisch gestartet wird:

- [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
"avserve.exe"="C:\\%WinDir%\\avserve.exe"

Es wird die Datei C:\WIN.LOG angelegt, in die IP Adresse des Localhost steht.

Der Wurm erstellt mehrer Kopien von sich selbst im Windows Systemverzeichnis mit dem Namen <%5 variable Zahlen%>_up.exe.

Entfernungshinweise:

- Mit einem aktuellen Virens scanner z.B. Norton / AntiVir / etc.:
Mit einem aktuellen Virens scanner wird der Virus entfernt. Starten Sie hierzu den Suchlauf und löschen Sie alle infizierten Dateien.

- Manuell bei Windows 2000/ XP:

Um den Virus von Hand zu entfernen, sollten Sie sich im abgesicherten Modus befinden. Drücken Sie die F8-Taste bevor das Bootlogo von Windows erscheint und wählen Sie die Option 'Abgesicherter Modus'. Löschen Sie folgende Dateien:

- \%WinDir%\AVSERVE.EXE
- \%WinDir%\%SystemDir%\<%5 variable Zahlen%>_up.exe
- C:\WIN.LOG

Gehen Sie auf Start und wählen Sie 'Ausführen'. Geben Sie im angezeigten Fenster 'regedit' ein und löschen folgende Registry-Einträge:

- [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
"avserve.exe"="C:\\%WinDir%\\avserve.exe"

Starten Sie den Computer neu und durchsuchen Sie Ihren PC anschließend mit einem aktuellen Virens scanner.

Beachten Sie eventuelle Einträge im Autostart-Ordner und entfernen Sie diese gegebenenfalls.