
# Schützen Sie Ihren PC

# Informationen zum Wurm Sasser, seinen Varianten und deren Beseitigung

Microsoft bestätigt Berichte, nach denen sich der Wurm **Sasser** (W32.Sasser.A und seine Varianten B, C und D) derzeit stark im Internet verbreitet. Der Wurm nutzt eine Sicherheitsanfälligkeit, gegen die Microsoft mit dem Security Bulletin MS04-011 (http://www.microsoft.com/germany/ms/technetservicedesk/bulletin/bulletinms04-011.htm) am 13. April 2004 ein Sicherheitsupdate zur Verfügung gestellt hat.

**Betroffene Produkte**

- Microsoft Windows® XP und Windows XP Service Pack 1
- Windows 2000 Service Pack 2, Windows 2000 Service Pack 3 und Windows 2000 Service Pack 4

**Nicht betroffene Produkte**

- Windows XP 64-Bit Edition Version 2003
- Windows Server 2003
- Windows XP 64-Bit Edition Service Pack 1
- Windows Millennium Edition
- Windows 98 Second Edition
- Windows 98
- Windows NT 4.0 Service Pack 6a

Führen Sie folgende Schritte aus, um sich gegen Sasser und seine Varianten zu schützen oder Sasser von Ihrem PC zu entfernen.

## Schritt 1: Aktivieren Sie eine Firewall

Bevor Sie irgendeinen anderen Schritt unternehmen, stellen Sie sicher, dass auf Ihrem Computer eine Firewall aktiviert ist, die diesen vor einer Infektion schützt. Falls Sie für Ihre Internetverbindung zu Hause oder im Firmennetzwerk eine Hardware-Firewall verwenden, wird der Wurm mit großer Wahrscheinlichkeit blockiert. Dies gilt auch, wenn Sie die in Windows XP integrierte Internetverbindungsfirewall nutzen. Falls Ihr Computer bereits infiziert ist, sorgt das Aktivieren der Firewall dafür, dass die Auswirkungen des Wurms eingeschränkt werden. Eine umfassende Anleitung zur Installation und Aktivierung von Firewalls finden Sie auf der Webseite Schützen Sie Ihren PC in 3 Schritten (http://www.microsoft.com/germany/protect).

## Schritt 2: Installieren Sie das erforderliche Update

Um Ihren Computer vor dem Wurm Sasser und seinen Varianten zu schützen, installieren Sie das Sicherheitsupdate MS04-011 (835732):

1. **Bei einer Einwahlverbindung (z.B. Modem) ins Internet**

   Herunterladen und Installieren des einzelnen Updates

- Wenn Sie Microsoft Windows® XP oder Windows XP Service Pack 1 einsetzen, laden Sie das Sicherheitsupdate MS04-011 hier herunter (http://www.microsoft.com/downloads/details.aspx?FamilyId=3549EA9E-DA3F-43B9-A4F1-AF243B6168F3&displaylang=de) und installieren Sie es.
- Wenn Sie Windows 2000 Service Pack 2, Windows 2000 Service Pack 3 oder Windows 2000 Service Pack 4 einsetzen, laden Sie das Sicherheitsupdate MS04-011 hier herunter (http://www.microsoft.com/downloads/details.aspx?FamilyId=0692C27E-F63A-414C-B3EB-D2342FBB6C00&displaylang=de) und installieren es.
- Falls Sie nicht wissen, welches Betriebssystem auf Ihrem Computer ausgeführt wird, klicken Sie hier (http://www.microsoft.com/germany/ms/security/checkos.mspx).

2. **Bei einer Breitband-Verbindung (z.B. DSL) ins Internet**
   Gehen Sie auf Windows Update (http://windowsupdate.microsoft.com/) um alle noch nicht installierten Sicherheitsupdates herunterzuladen und zu installieren.

   **Hinweis**: Wenn Sie das Sicherheitsupdate MS04-011 (835732) vor dem 30. April 2004 auf Ihrem Computer installiert haben, sind Sie vor einer Infektion durch Sasser geschützt.

## Schritt 3: Überprüfen Sie Ihren Computer auf eine Infektion und entfernen Sie Sasser

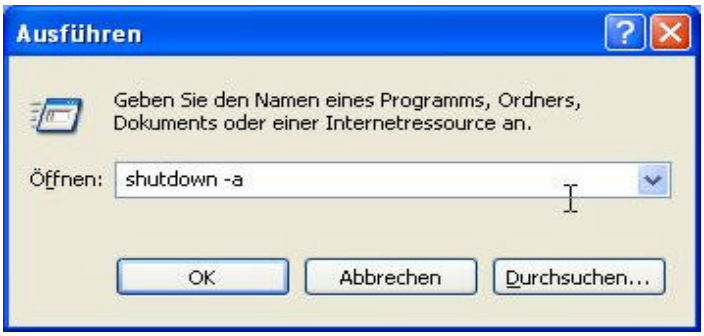
Microsoft stellt ein kostenfreies Tool zur Verfügung, das Ihren Computer automatisch auf eine Sasser-Infektion hin untersucht und den Wurm von Ihrem System entfernt. Downloaden Sie dieses englischsprachige "Sasser.A and Sasser.B Worm Removal Tool" (http://www.microsoft.com/downloads/details.aspx?FamilyId=76C6DE7E-1B6B-4FC3-90D4-9FA42D14CC17&displaylang=en) und führen Sie es aus.

**Hinweis**: Dieses Tool funktioniert nur auf Windows XP und Windows 2000 PCs, auf denen das Sicherheitsupdate MS04-011 (835732) bereits installiert ist.

**Manuelle Schritte zum Beseitigen des Wurmes**

1. Herunterfahren des PCs verhindern

Falls Ihr PC bereits vom Sasser-Wurm befallen ist, äußert sich dies in der Regel durch instabiles Verhalten. Insbesondere stürzt der Prozess LSASS.EXE ab. so dass der PC nach 60 Sekunden von selbst herunterfährt. Sie können das Herunterfahren auf Windows XP-PCs unterbinden, indem Sie unter **Start -> Ausführen** den Befehl „shutdown –a“ eingeben:




Auf Windows 2000-PCs können Sie den Vorgang des Herunterfahrens nicht abbrechen. Trennen Sie deshalb hier zunächst den PC vom Netzwerk (dies gilt für die Internet- und auch für jede andere Netzwerkverbindung).

Gehen Sie dann – sowohl bei Windows XP als auch Windows 2000 – wie folgt vor:

Erstellen Sie im Verzeichnis **%systemroot%\debug** eine Datei namens **dcpromo.log** und setzen Sie die Berechtigungen der Datei auf **Lesezugriff**. Geben Sie hierfür unter **Start -> Ausführen** den Befehl **cmd** ein und klicken Sie auf **OK**. Geben Sie dann in dem Fenster, das sich nun öffnet, folgenden Befehl ein und drücken Sie die Enter-Taste:

***echo dcpromo > %systemroot%\debug\dcpromo.log & attrib +r %systemroot%\debug\dcpromo.log***

**Hinweis:** Hierdurch wird der Wurm sowohl daran gehindert, den Rechner zu infizieren, als auch auf befallenen Rechnern zur Ausführung zu kommen und sich weiter zu verbreiten.

2. Prozesse des Wurms beenden

Falls Ihr PC mit dem Wurm Sasser befallen ist, wird er unter Umständen gleich nach Wiederverbinden mit dem Internet die Netzwerkverbindung verstopfen. Dies macht es unter Umständen unmöglich, das erforderliche Sicherheitsupdate MS04-011 (835732) herunterzuladen und zu installieren. Stoppen Sie deshalb die möglichen Prozesse des Wurms wie folgt:

1. Klicken Sie auf **Start** und dann auf **Ausführen**.
2. Geben Sie **taskmgr.exe** ein und klicken Sie auf **OK**.
3. Öffnen Sie im Task-Manager die Registerkarte **Prozesse**.
4. Suchen Sie in der Liste nach Prozessen, die folgende Kriterien erfüllen:
   - Der Name endet mit **_up.exe**.
   - Der Name beginnt mit **avserv**.
   - Der Name lautet **hkey.exe**.
   - Der Name lautet **skynetave.exe**.
   - Der Name lautet **msiwin84.exe**.
   - Der Name lautet **wmiprvsw.exe** (nicht mit **wmiprvse.exe** verwechseln!).
5. Klicken Sie auf jeden dieser Prozesse mit der rechten Maustaste und wählen Sie dann im erscheinenden Menü **Prozess beenden**. Bestätigen Sie durch einen Klick auf **Ja**.

Jetzt können Sie jetzt den PC wieder mit dem Internet verbinden und das Update herunterladen und installieren:

- Wenn Sie die deutsche Version von Windows XP einsetzen, öffnen Sie die Seite: http://www.microsoft.com/downloads/details.aspx?FamilyId=3549EA9E-DA3F-43B9-A4F1-AF243B6168F3&displaylang=de
- Wenn Sie die deutsche Version von Windows 2000 einsetzen, öffnen Sie die Seite: http://www.microsoft.com/downloads/details.aspx?FamilyId=0692C27E-F63A-414C-B3EB-D2342FBB6C00&displaylang=de
- Klicken Sie auf der Webseite rechts oben auf **Download** und bestätigen Sie mit einem Klick auf **Öffnen**.
- Folgen Sie den Anweisungen des Installationsprogramms.
- Wenn Sie zum Neustart des Rechners aufgefordert werden, bestätigen Sie mit **Ja**.

Führen Sie nach dem Neustart das Programm zur Entfernung des Sasser-Wurms aus. Hier stehen Ihnen zwei Optionen zur Auswahl:

1. Ein ActiveX basiertes Programm zum Entfernen des Sasser-Wurms:
   - Öffnen Sie die Seite http://www.microsoft.com/security/incident/sasser.asp.
   - Klicken Sie in der Mitte der Seite auf **CHECK MY PC FOR INFECTION**.
   - Klicken Sie den Punkt **I agree** an und bestätigen mit **Continue**.
   - Bestätigen Sie die erscheinende Sicherheitswarnung mit **Ja**.
2. Eine Variante des Programms zum Herunterladen unter: http://www.microsoft.com/downloads/details.aspx?FamilyId=76C6DE7E-1B6B-4FC3-90D4-9FA42D14CC17&displaylang=en

Wir wünschen Ihnen viel Erfolg bei der Beseitigung des Sasser-Wurms. Zudem möchten wir Sie darauf hinweisen, wie Sie sich in Zukunft besser vor Würmern und Viren schützen können. Bitte lesen Sie sich die entsprechenden Schritte auf unserem Sicherheitsportal durch:

- Schützen Sie Ihren PC in 3 Schritten (http://www.microsoft.com/germany/protect).

Wenn Sie zusätzliche Hilfe benötigen oder Probleme mit diesen Schritten haben, wenden Sie sich telefonisch unter folgenden Nummern an das Contact Center Privatkundenbetreuung von Microsoft:

- Deutschland: 01805 251199 (0,12 Euro pro Minute)