

Q-108.112 - Erkennung des Virus W32.Sober.r@mm [CME-151]

Q-108.112 - Erkennung des Virus W32.Sober.r@mm [CME-151]

aus Tobit KB importiert - vom 23.11.2005 - [Beitrag bei Tobit](#)

Problem

Wird der Virus **W32.Sober.r@mm** [CME-151] beim Einsatz der AntiVirus-Dienste for David (Virus Protection for DvISE / Tobit AntiVirus for Desktops) erkannt?

Antwort

Damit der Virus **W32.Sober.r@mm** [CME-151] (Fwd: Klassentreffen) erkannt wird, sind mindestens die Virensignaturen vom 06.10.2005 erforderlich.

Minimale Version der DAT-Dateien: 4598Release Datum: 06.10.2005

Prüfen Sie im InfoCenter unter »Archive -> System -> David -> Protokoll«, ob am 06.10.2005 oder später ein Eintrag mit dem Betreff "New virus signatures received successful" existiert.

Prüfen Sie auch, ob im »Archive -> System -> David -> Ereignisse« ein Eintrag mit dem Betreff "Virus Engine started" vorhanden ist. Abhängig vom Betriebssystem sollte der Inhalt dieser Nachricht folgendes enthalten:

unter Win32: "Version.....: 4598"

Hinweis:

Die Version 4598 darf durch neuere Virensignaturen selbstverständlich höher liegen.

Beschreibungen des Virus:

Name: W32.Sober.R@mm

Alias: W32/Sober-O, I.WORM_SOBER.U, W32.SOBER.S@mm, CME-151

Art: Wurm

Größe des Anhangs: ca. 12 KB

Betriebssystem: Microsoft Windows

Art der Verbreitung: Massenmailing, Netzwerk

Verbreitung: hoch

Risiko: mittel

Schadensfunktion: Massenmailing

Bekannt seit: 05.10.2005

Beschreibung:

W32.Sober.P@mm ist ein Internetwurm, der sich per Massenmailing verbreitet. Er nutzt dabei, wie seine Vorgänger, die eigene SMTP-Maschine. Des Weiteren trägt sich der Wurm auf infizierten Systemen in die Registry ein, so dass er bei jedem Windows-Neustart automatisch geladen wird.

Generelle Hinweise:

Bei eMails auch von vermeintlich bekannten bzw. vertrauenswürdigen Absendern sollten Sie prüfen, ob der Text der Nachricht auch zum Absender passt (englischer Text von deutschem Partner, zweifelhafter Text oder fehlender Bezug zu konkreten Vorgängen etc.) und ob die Anlage (Attachment) auch erwartet wurde.