

Q-108.193 - Erkennung des Virus W32.Sober.X@mm [CME-681]

Q-108.193 - Erkennung des Virus W32.Sober.X@mm [CME-681]

aus Tobit KB importiert - vom 01.03.2006 - [Beitrag bei Tobit](#)

Problem

Wird der Virus **W32.Sober.X@mm** [CME-681] beim Einsatz der AntiVirus-Dienste for David (Virus Protection for DvISE / Tobit AntiVirus for Desktops) erkannt?

Antwort

Damit der Virus **W32.Sober.X@mm** [CME-681] erkannt wird, sind mindestens die Virensignaturen vom 22.11.2005 erforderlich.

Minimale Version der DAT-Dateien: 4633Release Datum: 22.11.2005

Prüfen Sie im InfoCenter unter »Archive -> System -> David -> Protokoll«, ob am 22.11.2005 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.....: 4633"

Hinweis:

Die Version 4633 darf durch neuere Virensignaturen selbstverständlich höher liegen.

Beschreibungen des Virus:

Name: W32.Sober.X@mm

Alias: W32/Sober.gen@MM, W32/Sober.Z, Worm/Sober.Y, WORM_SOBER.AG, CME-681

Art: Wurm

Größe des Anhangs: ca. 55 KB

Betriebssystem: Microsoft Windows

Art der Verbreitung: Massenmailing

Verbreitung: hoch

Risiko: mittel

Schadensfunktion: Massenmailing, Beendet Prozesse, Systemgefährdung,

Bekannt seit: 21.11.2005

Beschreibung:

W32.Sober.X@mm ist ein Internetwurm, der sich per Massenmailing verbreitet. Er nutzt dabei, wie seine Vorgänger, die eigene SMTP-Maschine. Die Nachrichten mit diesem Virus haben einen deutschen oder englischen Betreff mit z.B. folgendem Inhalt : "Ihr Passwort", "Account Information", "Paris Hilton & Nicole Richie" oder "SMTP Mail gescheitert". Wird der Dateianhang dieser Mails geöffnet und entpackt, aktiviert sich

der Wurm und trägt sich 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.