

Q-107.003 - Erkennung des Virus W32.Sober.f@MM

Q-107.003 - Erkennung des Virus W32.Sober.f@MM

aus Tobit KB importiert - vom 05.04.2004 - [Beitrag bei Tobit](#)

Problem

Wird der Virus **W32.Sober.f@MM** von der Virus Protection for DvISE bereits erkannt?

Antwort

Damit der Virus **W32.Sober.f@MM** erkannt wird, sind mindestens die Virensignaturen vom 04.04.2004 erforderlich.

Minimale Version der DAT-Dateien: 4347Release Datum: 04.04.2004

Prüfen Sie im Tobit InfoCenter unter »Archive -> System -> David -> Protokoll«, ob am 04.04.2004 oder später ein Eintrag mit dem Betreff "New virus signatures received successful" existiert.

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

unter Win32: "Version.....: 4347"

Hinweis:

Die Version 4347 darf durch neuere Virensignaturen selbstverständlich höher liegen.

Beschreibungen des Virus:

Name: W32.Sober.f@MM

Alias: W32/Sober.f@MM, Win32.Sober.F, WORM_SOBER.F

Art: Wurm

Größe des Anhangs: 42.496 Bytes

Betriebssystem: Microsoft Windows

Art der Verbreitung: Massenmailing, Netzwerk

Verbreitung: hoch

Risiko: mittel

Schadensfunktion: Massenmailing, lädt Programm aus dem Internet nachbekannt seit: 03. April 2004

Beschreibung:

W32.Sober.f@mm ist ein Massenmailing-Wurm. Er verbreitet sich mit einer eigenen SMTP-Maschine. Der Wurm wird durch die Ausführung der angehängten Datei aktiviert.

Generelle Hinweise:

Bei eMail 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.