

Q-107.682 - Erkennung des Virus W32/Bagle.bj@MM

Q-107.682 - Erkennung des Virus W32/Bagle.bj@MM

aus Tobit KB importiert - vom 12.10.2005 - [Beitrag bei Tobit](#)

Problem

Wird der Virus **W32/Bagle.bj@MM** von der Virus Protection for DvISE bereits erkannt?

Antwort

Damit der Virus **W32/Bagle.bj@MM** erkannt wird, sind mindestens die Virensignaturen vom 27.01.2005 erforderlich.

Minimale Version der DAT-Dateien: 4423Release Datum: 27.01.2005

Prüfen Sie im InfoCenter unter »Archive -> System -> David -> Protokoll«, ob am 27.01.2005 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.....: 4423"

Hinweis:

Die Version 4423 darf durch neuere Virensignaturen selbstverständlich höher liegen.

Beschreibungen des Virus:

Name: W32/Bagle.bj@MM

Alias: W32/Bagle.bk@MM, WORM_BAGLE.AY / AZ

Art: Wurm

Größe des Anhangs: ca. 18 kB

Betriebssystem: Microsoft Windows

Art der Verbreitung: Massenmailing

Verbreitung: hoch

Risiko: mittel

Schadensfunktion: Massenmailing

Bekannt seit: 26.01.2005

Beschreibung:

W32/Bagle.bk@MM ist ein Internetwurm, der sich per Massenmailing verbreitet. Er nutzt dabei, wie seine Vorgänger, die eigene SMTP-Maschine. Der Wurm versendet sich selbst als Anhang einer E-Mail

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.