

Q-106.981 - Erkennung des Virus W32.Beagle.J@mm

Q-106.981 - Erkennung des Virus W32.Beagle.J@mm

aus Tobit KB importiert - vom 17.03.2004 - [Beitrag bei Tobit](#)

Problem

Wird der Virus **W32.Beagle.J@mm** von der Virus Protection for DvISE bereits erkannt?

Antwort

Damit der Virus **W32.Beagle.J@mm** erkannt wird, sind mindestens die Virensignaturen vom 02.03.2004 erforderlich.

Minimale Version der DAT-Dateien: 4332Release Datum: 02.03.2004

Prüfen Sie im Tobit InfoCenter unter »Archive -> System -> David -> Protokoll«, ob am 02.03.2004 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.....: 4332"

Hinweis:

Die Version 4332 darf durch neuere Virensignaturen selbstverständlich höher liegen.

Beschreibungen des Virus:

Name: W32.Beagle.J@mm

Alias: WORM_BAGLE.J, W32/Bagle.j@MM

Art: Wurm

Größe des Anhangs: 12.288 Bytes

Betriebssystem: Microsoft Windows

Art der Verbreitung: Massenmailing, Netzwerk

Verbreitung: mittel

Risiko: mittel

Schadensfunktion: Massenmailing, Installation eines Backdoors, bekannt seit: 02. März 2004

Beschreibung:

W32.Beagle.J@mm ist ein Massenmailer-Wurm, der sich über seine eigene SMTP-Maschine versendet. Er verbreitet sich auch über Netzwerkfreigaben, die den Wortteil shar enthalten. Dies trifft beispielsweise für die Tauschbörse KaZaA zu. Mit dem W32.Beagle.J@mm verbreitet sich erstmals massiv ein Wurm in versendeten ZIP-Dateien, die mit einem Kennwort verschlüsselt sind. Dabei erzeugt der Wurm selbständig immer wechselnde Kennwörter. Dem Anwender wird in der gefälschten Absenderadresse eine

vertrauenswürdige Stelle in der eigenen (Empfänger-) Domain vorgespielt.

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.

Hinweis zur aktuellen Version der Scan-Engine

Beachten Sie, dass nicht nur die Virensignaturen auf dem aktuellen Stand sein sollten, sondern auch die verwendete Scan-Engine. Die aktuelle Version der Scan-Engine für den in DvISE integrierten Virens Scanner können Sie im Downloadbereich des Club Tobit Software kostenlos runterladen. Hinweise zur Installation entnehmen Sie dem jeweiligen Download.