

Q-107.756 - Erkennung des Virus W32.Sober.O@mm

Q-107.756 - Erkennung des Virus W32.Sober.O@mm

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

Problem

Wird der Virus **W32.Sober.O@mm** von der Virus Protection for DvISE bereits erkannt?

Antwort

Damit der Virus **W32.Sober.O@mm** erkannt wird, sind mindestens die Virensignaturen vom 18.04.2005 erforderlich.

Minimale Version der DAT-Dateien: 4472Release Datum: 18.04.2005

Prüfen Sie im InfoCenter unter »Archive -> System -> David -> Protokoll«, ob am 18.04.2005 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.....: 4472"

Hinweis:

Die Version 4472 darf durch neuere Virensignaturen selbstverständlich höher liegen.

Beschreibungen des Virus:

Name: W32.Sober.O@mm

Alias: W32/Sober-N, WORM_SOBER.N

Art: Wurm

Größe des Anhangs: ca. 73 KB

Betriebssystem: Microsoft Windows

Art der Verbreitung: Massenmailing, Netzwerk

Verbreitung: mittel

Risiko: mittel

Schadensfunktion: Massenmailing, Beenden von Sicherheitsprogrammen

Bekannt seit: 18.04.2005

Beschreibung:

W32.Sober.O@mm ist ein Internetwurm, der sich per Massenmailing verbreitet. Er nutzt dabei, wie seine Vorgänger, die eigene SMTP-Maschine. Des weiteres beendet dieser Wurm Prozesse von Sicherheitsprogrammen.

W32.Sober.O@mm versendet sich selbst als Anhang einer E-Mail. Die Absenderadresse ist mit den gefundenen Adressen gefälscht. Er versendet sich sowohl mit deutschem, als auch mit englischem Text.

Mails enthalten hierbei dem Betreff: »FwD: Ich bin's nochmal« und der Nachrichtentext lautet:

- Verdammt,
ich hatte vergessen Dir meinen Text mitzuschicken.
Aber bitte nicht woanders darueber Reden, ich wuerde mich dann zu Tode
blamieren!

Ich melde mich.

Bis bald ;)Als Anhang ist die Datei »Private-Texte.zip« beigefügt, in dessen Archiv die ausführbare Datei »mail.document.Datex-packed.exe« zu finden ist.

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.