

Q-106.895 - Erkennung des Virus W32.Novarg.A@mm bzw. W32/Mydoom@MM

Q-106.895 - Erkennung des Virus W32.Novarg.A@mm bzw. W32/Mydoom@MM

aus Tobit KB importiert - vom 07.01.2005 - [Beitrag bei Tobit](#)

Problem

Wird der Virus **W32.Novarg.A@mm** bzw. **W32/Mydoom@MM** von der Virus Protection for DvISE bereits erkannt?

Antwort

Damit der Virus **W32.Novarg.A@mm** bzw. **W32/Mydoom@MM** erkannt wird, sind mindestens die Virensignaturen vom 27.01.2004 erforderlich.

Minimale Version der DAT-Dateien: 4319Release Datum: 27.01.2004

Prüfen Sie im Tobit InfoCenter unter »Archive -> System -> David -> Protokoll«, ob am 27.01.2004 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.....: 4319"

Hinweis:

Die Version 4319 darf durch neuere Virensignaturen selbstverständlich höher liegen.

Beschreibungen des Virus:

Name: W32.Novarg.A@mm

Alias:W32/Mydoom@MM [McAfee],WORM_MIMAIL.R [Trend]

Art: Wurm

Größe des Anhangs: 22.528 Bytes

Betriebssystem: Microsoft Windows

Art der Verbreitung: Massenmailing, Netzwerk

Verbreitung: hoch

Risiko: mittel - hoch

Schadensfunktion: Massenmailing, Installation eines Backdoors,DOS Angriff gegen <http://www.sco.com,%c3%9cberschreiben> von Systemdatei

bekannt seit: 26. Januar 2004

Beschreibung:

W32.Novarg.A@mm ist ein Internet-Wurm, der sich in Dateien mit den Endungen .bat, .cmd, .exe, pif, .scr

und .zip versendet. Zusätzlich verbreitet er sich über KaZaA.

Bei der Infektion des Systems installiert der Wurm ein Backdoor-Programm, das die TCP-Ports 3127 bis 3198 öffnet. Damit hat ein Angreifer die Möglichkeit, den infizierten Rechner fernzusteuern. Außerdem kann dieses Backdoor weitere Dateien aus dem Internet laden.

Am 1. Februar startet der Wurm eine Denial of Service (DOS) Attacke gegen eine bestimmte Internetseite. Ab dem 12. Februar verbreitet er sich nicht weiter.

Der Wurm erzeugt die Datei shimgapi.dll im Systemverzeichnis von Windows. Dieses Programm öffnet die TCP-Ports 3127 bis 3198 und arbeitet als Proxy-Server.

Durch den Registrierungs-Schlüssel **HKEY_CLASSES_ROOT\CLSID\{E6FB5E20-DE35-11CF-9C87-00AA005127ED}\InProcServer32 "(Default)" = %SysDir%\shimgapi.dll** wird die Datei gestartet, wenn Explorer.exe geöffnet wird. Das Windowsprogramm taskmon.exe im Systemverzeichnis von Windows wird durch eine Kopie des Wurms ersetzt.

Dieses startet automatisch durch den Registrierungs-Schlüssel **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run** oder **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run** mit dem Wert **TaskMon = %System%\taskmon.exe**. Weiterhin wird die Datei **message** im Temp-Verzeichnis angelegt.

In Dateien mit den Endungen:

- .htm
- .sht
- .php
- .asp
- .tbb
- .adb
- .pl
- .wab
- .txt

werden eMail-Adressen zur weiteren Verbreitung gesucht. Dabei werden keine Adressen aus der Top-Level-Domain .edu verwendet. Novarg.A verwendet zur Verbreitung seine eigene SMTP-Maschine.

Die E-Mail hat folgende Charakteristik:

Von: »Adresse gefälscht«

Betreff: »eine der folgenden«:

- test
- hi
- hello
- Mail Delivery System
- Mail Transaction Failed
- Server Report
- Status
- Error

Mail transaction failed. Partial message is available.

The message contains Unicode characters and has been sent as a binary attachment.

The message cannot be represented in 7-bit ASCII encoding and has been sent as a binary attachment.

Name des Anhangs:

- document
- readme
- doc
- text
- file
- data
- test
- message
- body

Datei-Endung

- pif
- scr
- exe
- cmd
- bat
- zip

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.