

Q-108.029 - Erkennung des Virus W32/IRCbot.worm (W32.Zotob.E)

Q-108.029 - Erkennung des Virus W32/IRCbot.worm (W32.Zotob.E)

aus Tobit KB importiert - vom 17.08.2005 - [Beitrag bei Tobit](#)

Problem

Wird der Virus **W32/IRCbot.worm** (Alias: W32.Zotob.E) beim Einsatz der AntiVirus-Dienste for David (Tobit AntiVirus for Desktops) erkannt?

Antwort

Damit der Virus **W32/IRCbot.worm!MS05-039** beim Einsatz von Tobit AntiVirus for Desktops (mit aktiviertem OnAccess) erkannt wird, sind mindestens die Virensignaturen vom 17.08.2005 erforderlich. Hinweise zur Funktion »OnAccess« von Tobit AntiVirus for Desktops entnehmen Sie den KnowledgeBase Artikel [Q-106.887](#).

Minimale Version der DAT-Dateien: 4560 Release Datum: 17.08.2005

Prüfen Sie im InfoCenter unter »Archive -> System -> David -> Protokoll«, ob am 17.08.2005 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.....: 4560"

Hinweis:

Die Version 4560 darf durch neuere Virensignaturen selbstverständlich höher liegen.

Beschreibungen des Virus:

Name: W32/IRCbot.worm!MS05-039

Alias: W32.Zotob.E, Net-Worm.Win32.Small.d, WORM_RBOT.CBQ

Art: Wurm

Größe: 10.366 Bytes

Betriebssystem: Microsoft Windows

Art der Verbreitung: Netzwerk

Verbreitung: hoch

Risiko: hoch

Schadensfunktion: Bot

Bekannt seit: 16.08.2005

Beschreibung:

W32/IRCbot.worm!MS05-039 ist ein Wurm, der sich über das Netzwerk verbreitet und hierbei eine

Schwachstelle von Windows "Plug and Play" ausnutzt. Informationen und Patches zu dieser Schwäche entnehmen Sie dem deutschen Microsoft Security Bulletin MS05-039. Der Wurm kann sich auf allen Microsoft Betriebssystemen ausbreiten, infiziert aber nur Systeme mit Windows 2000.

Nachdem das System mit diesem Wurm infiziert wurde, versucht dieser eine Verbindung zum IRC-Server 72.20.27.115 auf TCP-Port 8080 aufzubauen um von dort Befehle zu empfangen. Weiterhin startet er einen TFTP-Server auf UDP-Port 69.