

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
Verbreitung: hoch
Risiko: mittel-hoch
Schadensfunktion: Massenmailing,
Installation eines Backdoors,
DoS Angriff gegen www.sco.com
Spezielle Entfernung: Tool
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.

Die Datei **taskmon.exe** wird im Windows-Systemverzeichnis erzeugt. Existiert diese Datei schon, wird sie **durch eine Kopie des Wurms ersetzt**.

Diese 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
.dbx
.tbb
.adb
.pl
.wab
.txt

werden E-Mail-Adressen zur weiteren Verbreitung gesucht.
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

Nachricht: <einer der folgenden>

- 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:

<zufällige Zeichen>

Dateinamen-Erweiterung

.pif
.scr
.exe
.cmd
test

.zip

Größe des Anhangs: 22.528 Bytes

Novarg.A kopiert sich ausserdem in das Download-Verzeichnis von KaZaA, als Datei

winamp5
icq2004-final
activation_crack
strip-girl-2.Obdcom_patches
rootkitXP
office_crack
nuke2004





mit der Dateiendung

.pif
.scr
.bat
.exe

Hinweise zur Entfernung des Wurms

Bei den Betriebssystemen Windows ME oder XP, muß vor der Entfernung die Systemwiederherstellung deaktiviert werden.
Starten Sie den Computer im abgesicherten Modus.

Den Wurm auf einem infizierten Rechner lokalisieren und entfernen können Sie über eines der kostenlosen Entfernungstools von

Symantec (Fxnovarg.exe): [Direkt-Download](#)  oder [Download mit Informationen](#) 
NAI (stinger.exe): [Direkt-Download](#)  oder [Download mit Informationen](#) 

Generelle Hinweise:

Bei E-Mail auch von vermeintlich bekannten bzw. vertrauenswürdigen Absendern 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.

Das BSI empfiehlt, den Versand / Empfang von ausführbaren Programmen (Extend .COM, .EXE, .BAT, ...) oder anderer Dateien, die Programmcode enthalten können (Extend .DO*; XL*, PPT, VBS...) vorher telefonisch abzustimmen. Dadurch wird abgesichert, dass die Datei vom angegebenen Absender geschickt und nicht von einem Virus verbreitet wird.

(Erstellt: 27.01.2004)