

# PROTOKOLL FÜR KASPERSKY ONLINE SCANNER

Samstag, 28. Juni 2008 21:52:03

Betriebssystem: Microsoft Windows XP Home Edition, Service Pack 2 (Build 2600)

Version von Kaspersky Online Scanner: 5.0.98.1

Letztes Update der Antiviren-Datenbanken: 28/06/2008

Anzahl der Einträge in den Antiviren-Datenbanken: 895473

## Scan-Einstellungen

Folgende Antiviren-Datenbanken zur Untersuchung verwenden

Archive untersuchen ja

Mail-Datenbanken untersuchen ja

## Untersuchungsobjekt

Arbeitsplatz

C:\

D:\

E:\

## Untersuchungsergebnisse

Untersuchte Objekte insgesamt 68893

Viren gefunden 1

Infizierte Objekte gefunden 3

Verdächtige Objekte gefunden 0

Untersuchungszeit 01:31:13

## Name des infizierten Objekts

## Virusname

## Letzte Aktion

C:\WINDOWS\system32\config\system.LOG

Das Objekt ist gesperrt

übersprungen

C:\WINDOWS\system32\config\software.LOG

Das Objekt ist gesperrt

übersprungen

C:\WINDOWS\system32\config\default.LOG

Das Objekt ist gesperrt

übersprungen

C:\WINDOWS\system32\config\SECURITY

Das Objekt ist gesperrt

übersprungen

C:\WINDOWS\system32\config\SAM

Das Objekt ist gesperrt

übersprungen

C:\WINDOWS\system32\config\SAM.LOG

Das Objekt ist gesperrt

übersprungen

C:\WINDOWS\system32\config\SECURITY.LOG

Das Objekt ist gesperrt

übersprungen

C:\WINDOWS\system32\config\SYSTEM

Das Objekt ist gesperrt

übersprungen

C:\WINDOWS\system32\config\SOFTWARE

Das Objekt ist gesperrt

übersprungen

C:\WINDOWS\system32\config\DEFAULT

Das Objekt ist gesperrt

übersprungen

C:\WINDOWS\system32\config\SysEvent.Evt

Das Objekt ist gesperrt

übersprungen

C:\WINDOWS\system32\config\AppEvent.Evt

Das Objekt ist gesperrt

übersprungen

C:\WINDOWS\system32\config\SecEvent.Evt

Das Objekt ist gesperrt

übersprungen

C:\WINDOWS\system32\wbem\Repository\FS\MAPPING1.MAP

Das Objekt ist gesperrt

übersprungen

C:\WINDOWS\system32\wbem\Repository\FS\MAPPING2.MAP

Das Objekt ist gesperrt

übersprungen

C:\WINDOWS\system32\wbem\Repository\FS\MAPPING.VER

Das Objekt ist gesperrt

übersprungen

C:\WINDOWS\system32\wbem\Repository\FS\INDEX.MAP

Das Objekt ist gesperrt

übersprungen

C:\WINDOWS\system32\wbem\Repository\FS\OBJECTS.MAP

Das Objekt ist gesperrt

übersprungen

C:\WINDOWS\system32\wbem\Repository\FS\OBJECTS.DATA

Das Objekt ist gesperrt

übersprungen

C:\WINDOWS\system32\wbem\Repository\FS\INDEX.BTR

Das Objekt ist gesperrt

übersprungen

C:\WINDOWS\system32\CatRoot2\edb.log

Das Objekt ist gesperrt

übersprungen

C:\WINDOWS\system32\CatRoot2\tmp.edb

Das Objekt ist gesperrt

übersprungen

C:\WINDOWS\system32\h323log.txt	Das Objekt ist gesperrt	übersprungen
C:\WINDOWS\Debug\PASSWD.LOG	Das Objekt ist gesperrt	übersprungen
C:\WINDOWS\Sti_Trace.log	Das Objekt ist gesperrt	übersprungen
C:\WINDOWS\wiaservc.log	Das Objekt ist gesperrt	übersprungen
C:\WINDOWS\wiadebug.log	Das Objekt ist gesperrt	übersprungen
C:\WINDOWS\WindowsUpdate.log	Das Objekt ist gesperrt	übersprungen
C:\WINDOWS\SchedLgU.Txt	Das Objekt ist gesperrt	übersprungen
C:\WINDOWS\SoftwareDistribution\ReportingEvents.log	Das Objekt ist gesperrt	übersprungen
C:\Dokumente und Einstellungen\NetworkService\NTUSER.DAT	Das Objekt ist gesperrt	übersprungen
C:\Dokumente und Einstellungen\NetworkService\Lokale Einstellungen\Anwendungsdaten\Microsoft\Windows\UsrClass.dat	Das Objekt ist gesperrt	übersprungen
C:\Dokumente und Einstellungen\NetworkService\Lokale Einstellungen\Anwendungsdaten\Microsoft\Windows\UsrClass.dat.LOG	Das Objekt ist gesperrt	übersprungen
C:\Dokumente und Einstellungen\NetworkService\ntuser.dat.LOG	Das Objekt ist gesperrt	übersprungen
C:\Dokumente und Einstellungen\LocalService\NTUSER.DAT	Das Objekt ist gesperrt	übersprungen
C:\Dokumente und Einstellungen\LocalService\Lokale Einstellungen\Verlauf\History.IE5\index.dat	Das Objekt ist gesperrt	übersprungen
C:\Dokumente und Einstellungen\LocalService\Lokale Einstellungen\Temporary Internet Files\Content.IE5\index.dat	Das Objekt ist gesperrt	übersprungen
C:\Dokumente und Einstellungen\LocalService\Lokale Einstellungen\Anwendungsdaten\Microsoft\Windows\UsrClass.dat	Das Objekt ist gesperrt	übersprungen
C:\Dokumente und Einstellungen\LocalService\Lokale Einstellungen\Anwendungsdaten\Microsoft\Windows\UsrClass.dat.LOG	Das Objekt ist gesperrt	übersprungen
C:\Dokumente und Einstellungen\LocalService\Cookies\index.dat	Das Objekt ist gesperrt	übersprungen
C:\Dokumente und Einstellungen\LocalService\ntuser.dat.LOG	Das Objekt ist gesperrt	übersprungen
C:\Dokumente und Einstellungen\Marina\NTUSER.DAT	Das Objekt ist gesperrt	übersprungen
C:\Dokumente und Einstellungen\Marina\ntuser.dat.LOG	Das Objekt ist gesperrt	übersprungen
C:\Dokumente und Einstellungen\Marina\Lokale Einstellungen\Temp\~DFF928.tmp	Das Objekt ist gesperrt	übersprungen
C:\Dokumente und Einstellungen\Marina\Lokale Einstellungen\Temp\~DF259.tmp	Das Objekt ist gesperrt	übersprungen
C:\Dokumente und Einstellungen\Marina\Lokale Einstellungen\Verlauf\History.IE5\index.dat	Das Objekt ist gesperrt	übersprungen
C:\Dokumente und Einstellungen\Marina\Lokale Einstellungen\Temporary Internet Files\Content.IE5\index.dat	Das Objekt ist gesperrt	übersprungen
C:\Dokumente und Einstellungen\Marina\Lokale Einstellungen\Anwendungsdaten\Microsoft\Windows\UsrClass.dat	Das Objekt ist gesperrt	übersprungen
C:\Dokumente und Einstellungen\Marina\Lokale Einstellungen\Anwendungsdaten\Microsoft\Windows\UsrClass.dat.LOG	Das Objekt ist gesperrt	übersprungen
C:\Dokumente und Einstellungen\Marina\Lokale Einstellungen\Anwendungsdaten\Google\Google Desktop\55371ecc45c6\dbeam	Das Objekt ist gesperrt	übersprungen
C:\Dokumente und Einstellungen\Marina\Lokale Einstellungen\Anwendungsdaten\Google\Google Desktop\55371ecc45c6\dbeao	Das Objekt ist gesperrt	übersprungen
C:\Dokumente und Einstellungen\Marina\Lokale Einstellungen\Anwendungsdaten\Google\Google Desktop\55371ecc45c6\dbdam	Das Objekt ist gesperrt	übersprungen
C:\Dokumente und Einstellungen\Marina\Lokale Einstellungen\Anwendungsdaten\Google\Google Desktop\55371ecc45c6\bdbao	Das Objekt ist gesperrt	übersprungen

C:\Dokumente und Einstellungen\Marina\Lokale Einstellungen\Anwendungsdaten\Google\Google Desktop\55371ecc45c6 \dbu2d.ht1	Das Objekt ist gesperrt	übersprungen
C:\Dokumente und Einstellungen\Marina\Lokale Einstellungen\Anwendungsdaten\Google\Google Desktop\55371ecc45c6 \dbc2e.ht1	Das Objekt ist gesperrt	übersprungen
C:\Dokumente und Einstellungen\Marina\Lokale Einstellungen\Anwendungsdaten\Google\Google Desktop\55371ecc45c6 \dbvmh.ht1	Das Objekt ist gesperrt	übersprungen
C:\Dokumente und Einstellungen\Marina\Lokale Einstellungen\Anwendungsdaten\Google\Google Desktop\55371ecc45c6 \dbvm.cf1	Das Objekt ist gesperrt	übersprungen
C:\Dokumente und Einstellungen\Marina\Lokale Einstellungen\Anwendungsdaten\Google\Google Desktop\55371ecc45c6\dbm	Das Objekt ist gesperrt	übersprungen
C:\Dokumente und Einstellungen\Marina\Lokale Einstellungen\Anwendungsdaten\Google\Google Desktop\55371ecc45c6 \fiih.ht1	Das Objekt ist gesperrt	übersprungen
C:\Dokumente und Einstellungen\Marina\Lokale Einstellungen\Anwendungsdaten\Google\Google Desktop\55371ecc45c6 \fii.cf1	Das Objekt ist gesperrt	übersprungen
C:\Dokumente und Einstellungen\Marina\Lokale Einstellungen\Anwendungsdaten\Google\Google Desktop\55371ecc45c6 \rpmh.ht1	Das Objekt ist gesperrt	übersprungen
C:\Dokumente und Einstellungen\Marina\Lokale Einstellungen\Anwendungsdaten\Google\Google Desktop\55371ecc45c6 \rpm.cf1	Das Objekt ist gesperrt	übersprungen
C:\Dokumente und Einstellungen\Marina\Lokale Einstellungen\Anwendungsdaten\Google\Google Desktop\55371ecc45c6 \rpm1mh.ht1	Das Objekt ist gesperrt	übersprungen
C:\Dokumente und Einstellungen\Marina\Lokale Einstellungen\Anwendungsdaten\Google\Google Desktop\55371ecc45c6 \rpm1m.cf1	Das Objekt ist gesperrt	übersprungen
C:\Dokumente und Einstellungen\Marina\Lokale Einstellungen\Anwendungsdaten\Google\Google Desktop\55371ecc45c6 \hpt2i.ht1	Das Objekt ist gesperrt	übersprungen
C:\Dokumente und Einstellungen\Marina\Lokale Einstellungen\Anwendungsdaten\Google\Google Desktop\55371ecc45c6\hp	Das Objekt ist gesperrt	übersprungen
C:\Dokumente und Einstellungen\Marina\Lokale Einstellungen\Anwendungsdaten\Google\Google Desktop\55371ecc45c6 \safeweb\goog-black-urlm.cf1	Das Objekt ist gesperrt	übersprungen
C:\Dokumente und Einstellungen\Marina\Lokale Einstellungen\Anwendungsdaten\Google\Google Desktop\55371ecc45c6 \safeweb\goog-white-domainmh.ht1	Das Objekt ist gesperrt	übersprungen
C:\Dokumente und Einstellungen\Marina\Lokale Einstellungen\Anwendungsdaten\Google\Google Desktop\55371ecc45c6 \safeweb\goog-white-domainm.cf1	Das Objekt ist gesperrt	übersprungen
C:\Dokumente und Einstellungen\Marina\Lokale Einstellungen\Anwendungsdaten\Google\Google Desktop\55371ecc45c6 \safeweb\goog-malware-domainm.cf1	Das Objekt ist gesperrt	übersprungen
C:\Dokumente und Einstellungen\Marina\Lokale Einstellungen\Anwendungsdaten\Google\Google Desktop\55371ecc45c6 \safeweb\goog-malware-domainmh.ht1	Das Objekt ist gesperrt	übersprungen
C:\Dokumente und Einstellungen\Marina\Lokale Einstellungen\Anwendungsdaten\Google\Google Desktop\55371ecc45c6 \safeweb\goog-black-urlmh.ht1	Das Objekt ist gesperrt	übersprungen
C:\Dokumente und Einstellungen\Marina\Lokale Einstellungen\Anwendungsdaten\Google\Google Desktop\55371ecc45c6 \safeweb\goog-black-enchashm.cf1	Das Objekt ist gesperrt	übersprungen
C:\Dokumente und Einstellungen\Marina\Lokale Einstellungen\Anwendungsdaten\Google\Google Desktop\55371ecc45c6 \safeweb\goog-black-enchashmh.ht1	Das Objekt ist gesperrt	übersprungen
C:\Dokumente und Einstellungen\Marina\Cookies\index.dat	Das Objekt ist gesperrt	übersprungen

C:\Programme\Trend Micro\HijackThis\backups\backup-20080626-195021-668.dll

Infizierte Objekte: not-a-virus:AdTool.Win32.MyWebSearch.a übersprungen

C:\System Volume Information\\_restore{2F240ADB-6ABD-4E73-ADBC-333BC02FFE7E}\RP177\A0026935.DLL

Infizierte Objekte: not-a-virus:AdTool.Win32.MyWebSearch.a übersprungen

C:\System Volume Information\\_restore{2F240ADB-6ABD-4E73-ADBC-333BC02FFE7E}\RP177\A0026942.dll

Infizierte Objekte: not-a-virus:AdTool.Win32.MyWebSearch.a übersprungen

C:\System Volume Information\\_restore{2F240ADB-6ABD-4E73-ADBC-333BC02FFE7E}\RP181\change.log

Das Objekt ist gesperrt übersprungen

D:\System Volume Information\MountPointManagerRemoteDatabase

Das Objekt ist gesperrt übersprungen

**Die Untersuchung wurde abgeschlossen.**