

Vorbemerkung

Veränderungen an den Einträgen der Registry können zu Problemen mit Ihrem Rechner führen. Bitte nur weiterlesen und anwenden wenn Sie wissen was Sie tun und Sie bereit sind im Notfall ihr Betriebssystem neu zu installieren. Ich übernehme keine Haftung für Schäden.

Virenstart der besonderen Art

Neulich hatte ich mal wieder einen Kunden dessen Rechner von Viren befallen war. Nach Deaktivierung der beim Start automatisch gestarteten Programme im Startmenü und der Registry sowie Deaktivierung der Wiederherstellung habe ich gedacht das das Problem gelöst sei. Neustart durchgeführt und nach ein paar Sekunden meckerte der Virenschanner wieder (msdirectx.sys). Nach Deaktivierung einiger verdächtigen Dienste habe ich den Rechner wieder neu gestartet. Es kam wieder diese Meldung des Virenschanners.

Jetzt habe ich mir die laufenden Prozesse im Taskmanager angesehen. Ausser den mir bekannten Prozessen lief da noch ein Prozess mit Namen **sysmon32.exe**.

Darauf habe ich den Registry Editor gestartet und nach dieser Datei gesucht.

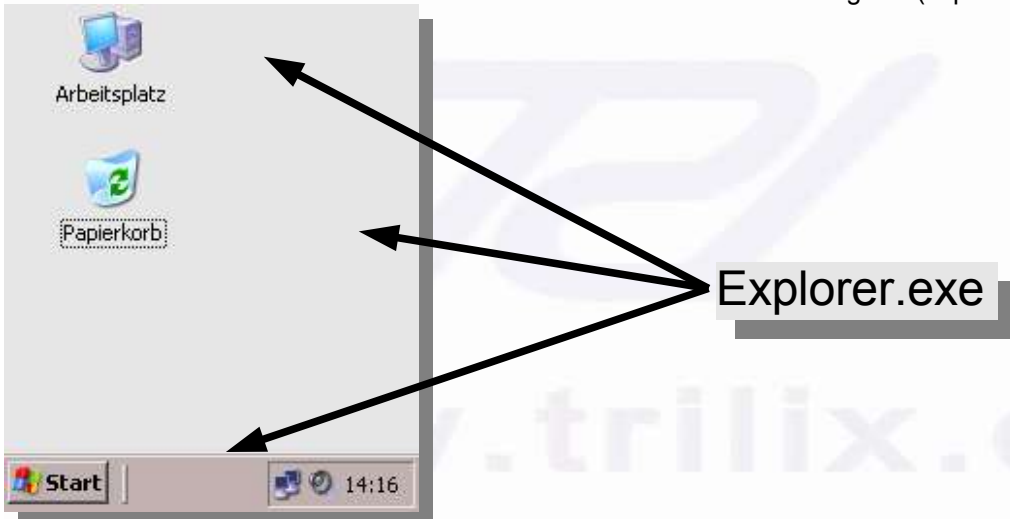
Nach kurzer Zeit habe ich einen Eintrag gefunden.

Der Eintrag steht im Schlüssel

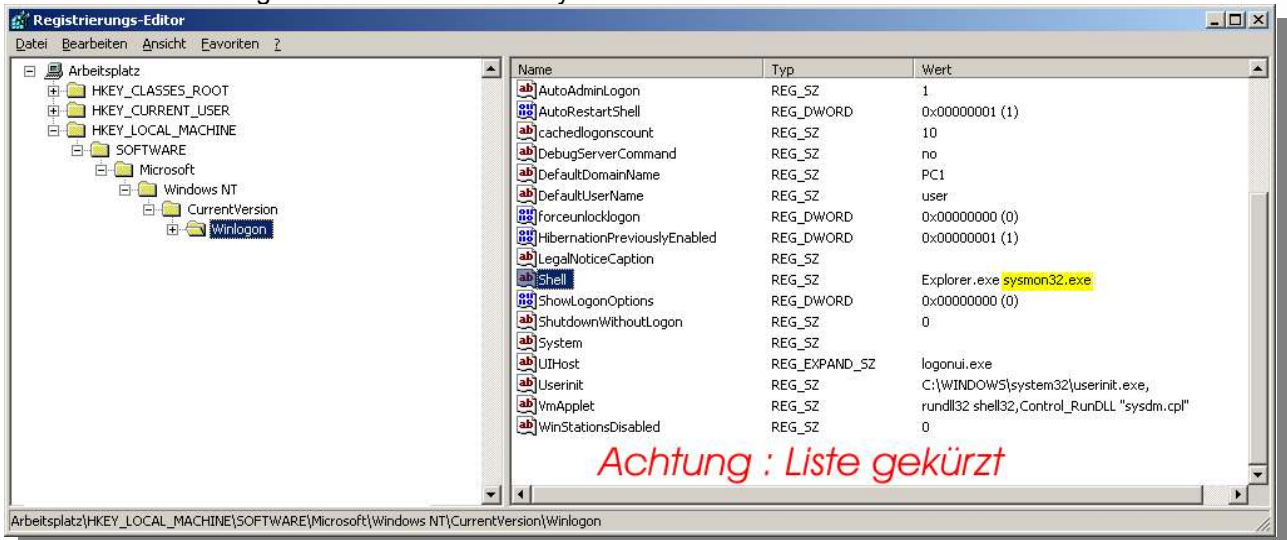
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

Hier stehen die Startparameter für den Logon Prozess drin.

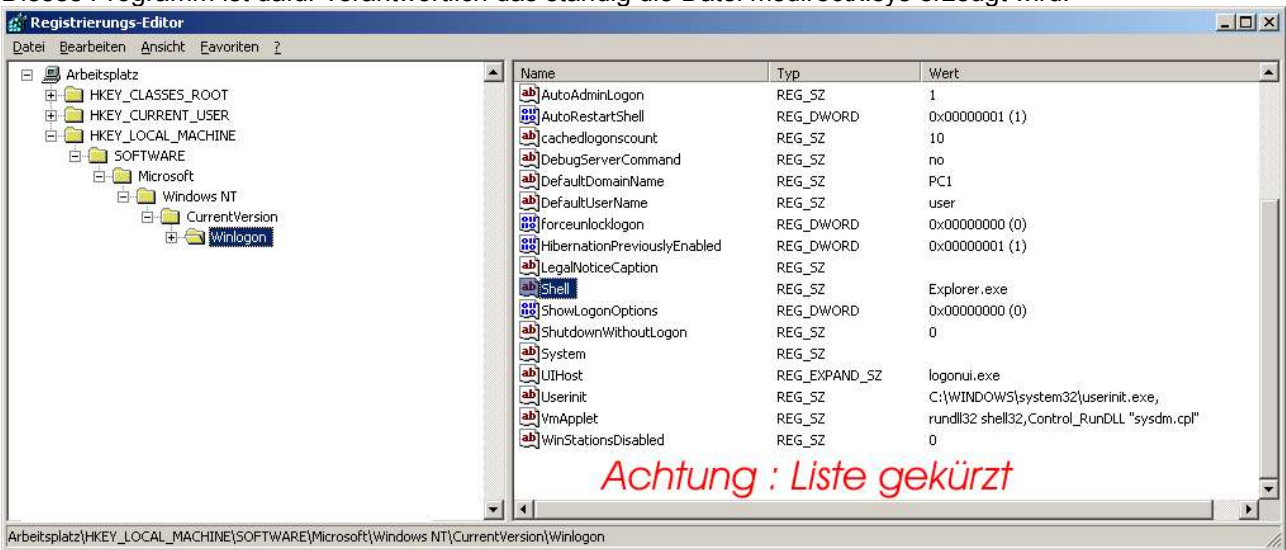
Hier steht auch die Oberfläche drin die die Arbeit mit Windows XP ermöglicht (explorer.exe)



Der Virus war so nett und hat den Startprozess so abgeändert, das nicht nur der Explorer gestartet wird sondern auch ein Programm mit dem Namen sysmon32.exe.



Dieses Programm ist dafür verantwortlich das ständig die Datei msdirectx.sys erzeugt wird.



Nach Löschen der **sysmon32.exe** aus der Registry war wieder Ruhe und der Kunde konnte wieder ohne Störung arbeiten.