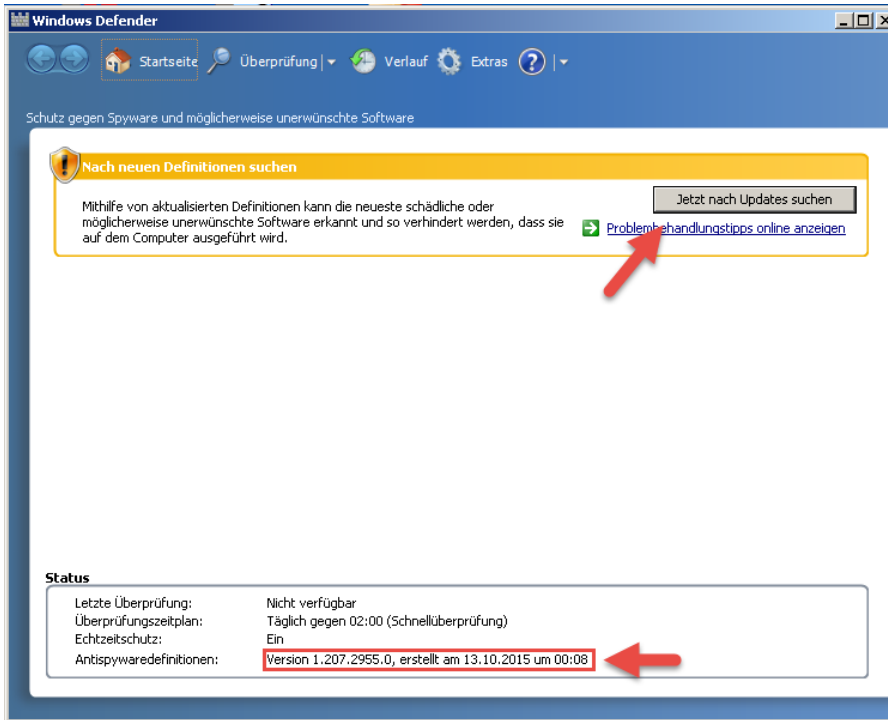


Windows Defender – roll-back Antispywaredefinition

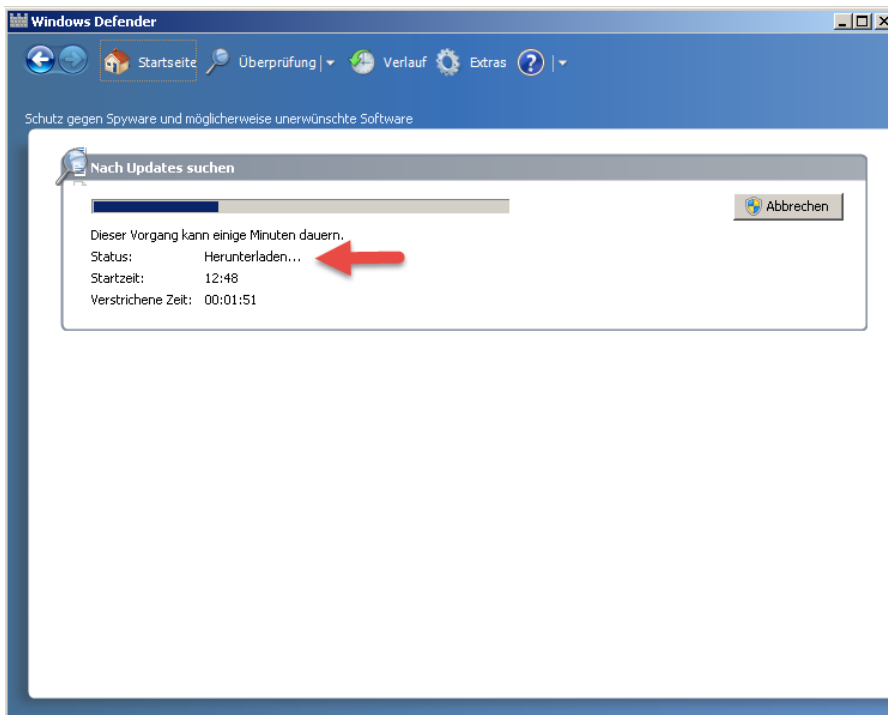
Eine aktuelle Antispywaredefinition, die wir gerade erst aktualisiert haben, kann unter Umständen im Nachgang dafür verantwortlich sein, das gravierende Probleme mit anderen Softwareprodukten oder dem System auftreten können. Was nun?

Und so kehren wir zur vorherigen Antispywaredefinition zurück.

Ursprünglicher Definitionsstand 1.207.2955.0

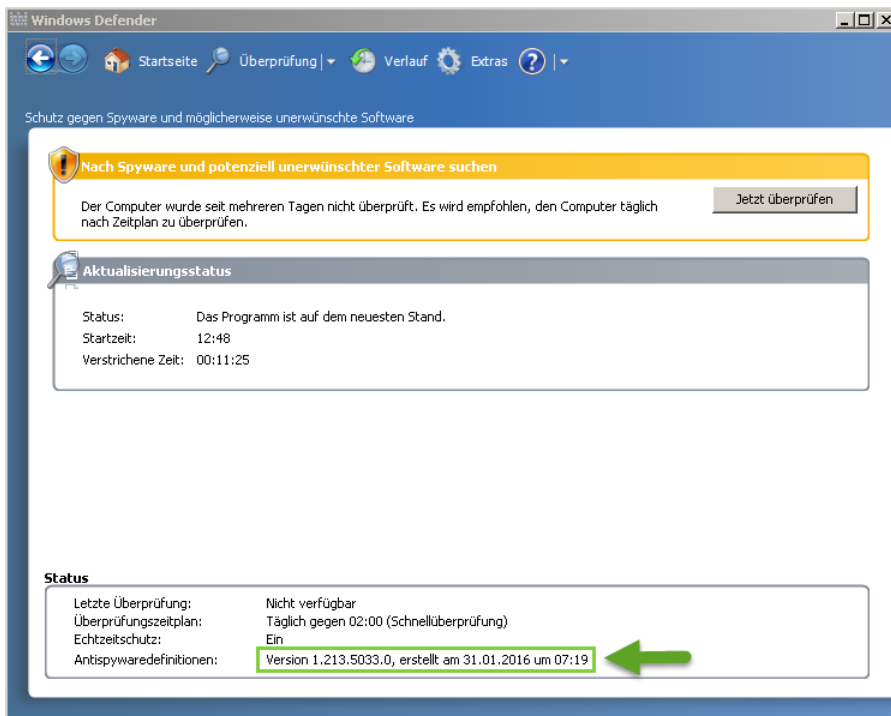


Den uralten Stand werde ich jetzt erst einmal updaten, um einen „roll-back“ zur Vorversion simulieren zu können.



Windows Defender – roll-back Antispywaredefinition

Nach dem Update liegt die neue Antispywaredefinition in der **Version 1.213.5033.0** vor.



Angenommen wir hätten jetzt Probleme mit dem Starten einer Anwendung, weil diese fälschlicherweise (false-positiv Erkennung) durch die aktuelle Antispywaredefinition in der Version "1.213.5033.0" blockiert würde, das Problem mit der Version 1.213.4870 aber nicht besteht?!

Und so rollen wir zur vorherigen Definition zurück:

Wir wechseln in das Programmverzeichnis von Windows Defender und leiten den „roll-back“ mit diesem Befehl ein.

MpCmdRun.exe -RemoveDefinitions

The screenshot shows a command prompt window titled 'Administrator: C:\Windows\system32\cmd.exe'. The user navigates to 'C:\Users\admin>cd %ProgramFiles%\Windows Defender' and then enters the command 'C:\Program Files\Windows Defender>MpCmdRun.exe -RemoveDefinitions'. The output shows the current status: 'Service Version: 6.1.7601.18170', 'Engine Version: 1.1.12400.0', and 'AntiSpyware Signature Version: 1.213.5033.0'. A red arrow points to the command line, and another red arrow points to the current signature version. The next line says 'Starting engine and signature rollback to last known good...Done!'. The final output shows the updated status: 'Service Version: 6.1.7601.18170', 'Engine Version: 1.1.12400.0', and 'AntiSpyware Signature Version: 1.213.4870.0'. A green arrow points to the new signature version.

Windows Defender – roll-back Antispywaredefinition

Das Backup der Definitionen liegt in dem Verzeichnis:

C:\ProgramData\Microsoft\Windows Defender\Definition Updates

