Ein Plugin für AntiVir Personal

AntiVir Personal von H+BEDV Datentechnik GmbH, Lindauer Strasse 21, 88069 Tettnang Germany
ist ein hervorragender und kostenfreier Virenscanner, der sich auch international durchzusetzen beginnt. In vielen Länder der Erde wird er auf Grund seiner Zuverlässigkeit geschätzt und weltweit von den Homeusern angewendet. Das Wichtigste an diesem Tool ist, das er einen unschlagbar schnellen Guard besitzt und im Gegensatz zu vielen anderen Tools dieser Kategorie täglich, entsprechend der Situation sogar mehrmals am Tag aktualisiert wird.

Zur Anwendung auf einer BartPE sollte der Scanner ebenfalls regelmäßig neu gebrannt werden. Das erfordert für Homeanwender zumindest eine wöchentliche und für Administratoren eine fast tägliche Aktualisierung der CDRW. Entsprechend meinen Erfahrungen braucht aber nur die ISO aktualisiert werden. Das dauert im Allgemeinen einschlieslich des kopierens der Dateien nach \files\ nur ca. 5 Minuten. Diese ISO kann im Ernstfall von einer gestarteten BartPE mit einem darauf enthaltenem Brennprogramm (zum Beispiel Nero oder Burn4Free) auf eine neue CD geschrieben werden.

Kritiker werden eine Fehlermeldung während des Startes des AVPersonal von der BartPE bemängeln, weil das Hauptprogamm keine Auslagerungsdatei findet. Diese kann BartPE jedoch nicht zur Verfügung stellen und in der Praxis hat sich dieser Mangel zumindest bei mir noch nicht negativ bemerkbar gemacht.

Das PlugIn unterscheidet sich etwas von den anderen bisher beschriebenen. Aus Gründen der Performance wird das Programm in die RAM-Disk kopiert und dort gestartet. Die Suchgeschwindigkeit ist durch diese Maßnahme sehr groß geworden. Noch schneller geht es wohl nicht mehr. Gegenüber anderen Veröffentlichungen wird in dieser Anwendung nicht der Guard sondern das Hauptprogramm aktiviert. Ich habe festgestellt, das nach Aufruf des Guard trotzdem das Hauptprogramm geladen wird. Eine Überwachung während eines Besuches im Internet kommt für diese CD kaum in Frage, zudem Malware an der CD als Bootmedium sich vermutlich die Zähne ausbeisen würde.

Noch ein Hinweis:
Falls nach Beendigung von AV Personal eine weitere speicherintensive Anwendung in die RAM-Disk verlagert wird, sollte diese vorher mit einem Dateimanager gelehrt werden. Die RAM-Disk stöst bei maximal 32 MByte an ihre physikalische Grenze.

```
; AVpersonal.inf
; PE Builder v3 plug-in INF Datei für AntiVir Personal
; Erstellt von Manfred Fiebig

[Version]
Signature= "$Windows NT$"

[PEBuilder]
Name="AV Personal"
Enable=1
Help="AVpersonal.htm"

[WinntDirectories]
a="Programs\avpersonal",2
b="Programs\avpersonal\infected",2
c="Programs\avpersonal\logfiles",2

[SourceDisksFiles]
avpersonal.cmd=a,,1
files\*.*=a,,1

[Append]
nu2menu.xml, avpers_nu2menu.xml
```

```
<NU2MENU>
<MENU ID="Programs">
<MITEM TYPE="ITEM" DISABLED="@Not(@FileExists(@GetProgramDrive()
\Programs\avpersonal\avwin.exe))" CMD="RUN" FUNC="@GetProgramDrive()
\Programs\avpersonal\avpersonal.cmd">AntiVir Personal</MITEM>
</MENU>
</NU2MENU>
```

```
Rem avpersonal.cmd
@echo off
rem
------------------------------------------------------------------------
rem Script zum Start von AntiVir Personal von BartPE
rem Erstellt von Manfred Fiebig
rem
------------------------------------------------------------------------
echo AntiVir wird gestartet...
setlocal
if "%temp%" == "" goto _err
if exist "%temp%\avpersonal\avwin.exe" goto _run
echo Kopieren von "%~dp0*.*" nach "%temp%\avpersonal\"
xcopy /s "%~dp0*.*" "%temp%\avpersonal\"
:_run
start %temp%\avpersonal\avwin.exe
goto _end
:_err
echo.
echo Keine Variable TEMP gesetzt
echo oder Ramdisk gefunden...
echo.
pause.
:_end
endlocal
```

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html><head></head><body><i>PE Builder v3 plugin</i><hr>
<h1>AntiVir Personal</h1>
<span style="font-family: arial;">Hier </span><a style="font-family: arial;"
href="http://www.free-av.de/personal/de/avwinsfx.exe">klicken</a><span style="font-family: arial;">
zum Download von AntiVir Personal. <br>
Installiere es in deinem System und kopiere die Dateien einschlieslich der Unterverzeichnisse nach
\plugin\avpersonal\files.</span><br>
<br style="font-weight: bold;">
<font color="#000080" face="Verdana, Arial" size="2"><strong><span style="font-weight:
normal;">Zitatanfang:</span><br>
Die AntiVir Personal Edition ist für den privaten (individuellen, nicht-kommerziellen) Einsatz kostenfrei!
</strong></font>
<p><font color="#000080" face="Verdana, Arial" size="2"><font color="#000080" face="Verdana, Arial"
size="2">Unzählige Computerviren gibt es mittlerweile - und täglich werden es mehr. Umso wichtiger
ist, dass Sie sich vor digitalen Angreifern wirksam schützen.<br>
<br>
Die Leistungsfähigkeit von AntiVir ist in vielen Tests und Empfehlungen von Fachzeitschriften und
unabhängigen Institutionen dokumentiert. Mit der AntiVir Personal Edition bieten wir Ihnen
zuverlässigen Schutz für den Einsatz auf Ihrem privaten PC.<br><br>
Um Ihnen die Bedienung so einfach wie möglich zu machen, haben wir die AntiVir Personal Edition auf
das Wesentliche konzentriert.<br> Sie werden staunen, wie umfassend AntiVir Sie schützt:
</font></font></p><ul>
<font color="#000080" face="Verdana, Arial" size="2"> <li><font color="#000080" face="Verdana, Arial"
size="2"> Schutz vor kostenverursachenden Einwahlprogrammen (Dialer)<a href="http://www.free-
av.de/umfrage/umfrage.html" target="_blank"> </a> </font></li>
<li><font color="#000080" face="Verdana, Arial" size="2"> erkennt und entfernt über 80.000 Viren
</font></li>
<li><font color="#000080" face="Verdana, Arial" size="2"> zahlreiche Bestnoten bei Tests in
Fachzeitschriften </font></li>
<li><font color="#000080" face="Verdana, Arial" size="2"> der ständig aktive Virenwächter wacht
permanent über Ihre Software,<br>beispielsweise bei Downloads aus dem Internet </font></li>
<li><font color="#000080" face="Verdana, Arial" size="2"> Suche von Makroviren und Reparatur
infizierter Dateien </font></li>
<li><font color="#000080" face="Verdana, Arial" size="2"> Schutz vor bislang unbekannten Makroviren
</font></li>
<li><font color="#000080" face="Verdana, Arial" size="2"> Schutz vor Trojanern, Würmern, Backdoors,
Jokes und anderen schädlichen Programmen </font></li>
<li><font color="#000080" face="Verdana, Arial" size="2"> klare Bedienung </font></li>
<li><font color="#000080" face="Verdana, Arial" size="2"> leichte Aktualisierung durch Internet-Update-
Wizard </font></li>
<li><font color="#000080" face="Verdana, Arial" size="2"> Schutz vor unbekannten Bootsektor- und
Master-Bootsektorviren </font></li>
<li><font color="#000080" face="Verdana, Arial" size="2"> Qualität "Made in Germany" </font></li>
<li><font color="#000080" face="Verdana, Arial" size="2">kostenfreier Support über <font
color="#0000a0"> das</font> <a
href="http://www.free-av.de/cgi-bin/ubb/ultimatebb.cgi" target="_blank">AntiVir Bulletin Board</a>
</font></li></font></ul>
<font color="#000080" face="Verdana, Arial" size="2"><font color="#000080" face="Verdana, Arial"
size="2"><strong>Informationen über die Komplettausstattung der netzwerkfähigen Professional
Edition finden Sie auf der Seite<a href="http://www.antivir.de/"
target="_blank">http://www.antivir.de/.</a><br>
<span style="font-weight: normal;">---Zitatende</span><br></strong></font><br></font>
<hr><font color="#000080" face="Verdana, Arial" size="2"><i>PE Builder Copyright (c) 2002-2003 Bart
Lagerweij. All rights reserved.</i><br><br></font></body></html>
```

AntiVir Personal bei der Arbeit von einer BartPE