Was ist eScan AntiVirus?

Das kostenlose MicroWorld AntiVirus Toolkit Utility (MWAV) ist ein sogenannter On-Demand-Scanner und ist im Grunde eine abgespeckte eScan AntiVirus Version und als solche werde ich es auch im weiteren Verlauf bezeichnen.
Die Vorteile liegen klar auf der Hand, zum einen bedient sich eScan der Kaspersky **[1]** Scan Engine und deren täglich aktualisierten Signaturen und zum anderen muss es nur entpackt und nicht installiert werden.
Leider gibt es trotz allem Positiven eine kleine Einschränkung, die Malware wird nicht mehr automatisch beseitigt, sondern muss manuell entfernt werden.

[1] Einer der führendsten AV Hersteller

Download, entpacken und aktualisieren von eScan:

Nach dem Download, sollte das Archiv mittels WinRAR entpackt **[2]** werden.
Um eScan zu aktualisieren, musst du nun zum Ordner '**C:\Bases_X**' navigieren und die '**kavupd.exe**' ausführen. Ein kleines DOS - Fenster öffnet sich, Signaturen werden erneuert und wird nach getaner Arbeit wieder geschlossen.

[2] Rechtsklick auf die '**mwav.exe**' -> '**Dateien entpacken…**' auswählen -> unter Zielverzeichnis '**C:\Bases_X**' eingeben -> '**OK**'

Einsetzen von eScan – Konfiguration und Scan:

1. Deaktiviere die Systemwiederherstellung **[3]** und wechsle anschliessend in den abgesicherten Modus.

[3] Betrifft nur Windows ME und Windows XP

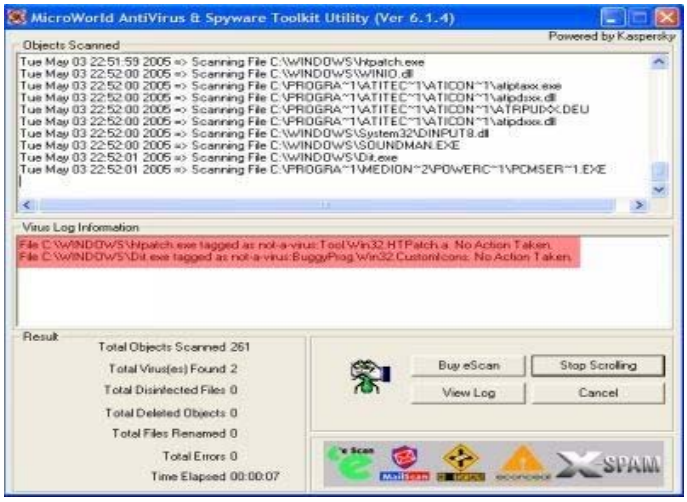
2. Um eScan zu starten, musst du erneut zum Ordner '**C:\Bases_X**' navigieren und die '**mwavscan.com**' ausführen.

3. Beim Start erhältst du folgende Lizenzvereinbarung und akzeptierst diese, nach sorgfältigem Lesen, mit '**OK**':

© Cidre

4. Es öffnet sich das Programmfenster '**Scan Option**'.
Setze nun die blau markierten Haken und starte den Scan mit einem Klick auf den rot markierten Button '**Scan**'.

5. Beim ersten vermeintlichen Fund erhältst du eine '**Virus Detected**' Warnmeldung und bestätigst diese mit '**OK**'.



6. Nachdem der Scan abgeschlossen ist, wird automatisch die Datei '**mwav.log**' im Ordner '**C:\Bases_X**' erstellt. Diese Log-Datei ist enorm wichtig und wird zur späteren Auswertung herangezogen.

Einsetzen von eScan – Auswertung:

Alle von eScan beanstandeten Funde werden in der '**Virus Log Information**' **[4]** angezeigt und sind ebenso in der '**mwav.log**' gespeichert.
Informationen zur entdeckten Malware, kannst du bei Kaspersky einholen.

[4] Aus dieser ist ersichtlich:
- Wo sich dich Malware befindet
- Um welche Malware es sich handelt

1. Möglichkeit: Wenn du dir über die Schadfunktion der aktiven Malware im Klaren bist und du dein System selbst bereinigen willst, dann gehe zum nächsten Schritt '**Beseitigung der Malware**' über.

2. Möglichkeit: Wenn du unsicher bist, dann solltest du einen neuen Thread eröffnen und uns die '**Virus Log Information**' **[5]** zur Verfügung stellen, damit wir dein System analysieren können. Gehe wie folgt vor:

© *Cidre*

[5] Rechtsklick auf die Find.bat -> Ziel speichern unter… z.B. '**C:\Find.bat**' -> '**Find.bat**' doppelklicken und den Scan abwarten -> den Inhalt **[6]** der automatisch erstellten '**C:\eScan_neu.txt**' posten.

An dieser Stelle, vielen Dank an Haui45, dem Autor der Find.bat.
Sollten Probleme beim Ausführen der Find.bat auftreten, dann lies bitte folgenden Thread von Haui45 durch.
Wichtig: Durchsuche das Log-File nach persönlichen Informationen, wie z.B. deinen Realname, und editiere diese, bevor du es postest.

[6] Strg + A (alles markieren) -> Strg + C (kopieren) -> Strg + V (Thread einfügen).

Alternativ:
Öffne die '**mwav.log**' im Ordner '**C:\Bases_X**' -> Bearbeiten -> Suchen -> infected oder tagged eingeben -> Weitersuchen -> Treffer markieren/kopieren und ins Forum übertragen.

Einsetzen von eScan – Beseitigung der Malware:

Wie ich bereits beschrieben habe, erfolgt die Beseitigung der Malware manuell. Auch hier werde ich mehrere Möglichkeiten ansprechen, die erheblich zur Erleichterung beitragen werden.

1. Möglichkeit - Total Commander:
Lade den Total Commander und nimm folgende Einstellung vor:
Total Commander öffnen -> Konfigurieren -> Einstellungen -> Ansicht -> Haken setzen bei '**Versteckte und Systemdateien anzeigen (nur für Experten)**' -> '**OK**'

Navigiere im linken Fenster z.B. zum Ordner C:\Windows\Downloaded Program Files
und lösche (**markieren** -> **F8** -> **JA**) die beanstandeten Dateien.

2. Möglichkeit - KillBox:
Lade und öffne KillBox. Kopiere den Pfad der Malware Datei z.B. C:\WINDOWS\system32\fltmgr.dll -> füge diesen in KillBox ein -> wähle die Option '**Delete on reboot**' -> rotes X anklicken -> die zwei folgenden Fragen mit '**JA**' und '**NEIN**' beantworten -> nächsten Pfad einfügen usw. -> wenn du bei der letzten Datei angekommen bist, dann beantworte beide Fragen mit '**JA**' und ein Neustart deines Systems wird durchgeführt.

3. Möglichkeit - eScan-Checkb9 von Seeker:
Lade eScan-Checkb9 und entpacke das Archiv z.B. in den vorgeschlagenen Ordner '**C:\escheck**' -> Installieren -> Datei -> eScan-Log öffnen -> mwav.log auswählen -> Haken setzen bei '**Backup der gelöschten Dateien anlegen**' und '**Alle Dateien beim Neustart löschen**' -> die gewünschten Dateien anhaken und auf den Button '**Dateien löschen**' klicken.

Egal, welche Möglichkeit du nun auswählst, sei dir darüber im Klaren, dass damit nur die Symptome und nicht die Ursache beseitigt wird.
Sollte eine Malware eine Schadfunktion besitzen, die es erlaubt, dass Dritte auf dein System zugreifen können, dann solltest du ohnehin ein Neuaufsetzen deines Systems mit anschliessender Absicherung in Erwägung ziehen und durchführen. Somit wäre auch die Vertrauenswürdigkeit deines Systems wiedergegeben.

In Zusammenarbeit mit dedies - Team

© *Cidre*