Was ist eScan AntiVirus?

Das kostenlose <u>MicroWorld</u> AntiVirus Toolkit Utility (MWAV) ist ein sogenannter <u>On-Demand-Scanner</u> 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 <u>Malware</u> wird nicht mehr automatisch beseitigt, sondern muss manuell entfernt werden.

[1] Einer der führendsten AV Hersteller

geschlossen.

Download, entpacken und aktualisieren von eScan:

Nach dem <u>Download</u>, sollte das Archiv mittels <u>WinRAR</u> 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

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

emein Erweitert	
elverzeichnis (wird erstellt, falls es nicht ex	istient) Anzeigen
\Bases_X	
Aktualisierungs-Modus Dateien entpacken & ersetzen Dateien entpacken & aktualisieren Nur vorhandene Dateien Dateien überschreiben Vorher nachfrägen Ohne Bestätigung Existierende überspringen	Construction C
Verschiedenes Archive in Unterverz, entpacken Beschädigte Dateien nicht löschen Dateien im Explorer anzeigen	
Einstellungen speichern	

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':

ense Agreement		
Please read the follow	ing important information before continuing	
Please read the follow agreement before us	ving license agreement. You must accept the terms of the ng this tool.	
THIS LICENSE AGE CONCERNING THE BETWEEN YOU AN SUPERSEDES ANY UNDERSTANDING AGREEMENT EXEC SUPERCEDE THIS 1. Terms of usage	EEMENT REPRESENTS THE ENTIRE AGREEMENT PROGRAM (MVAW - MicroWoold Antivitus Tooki Utility) D. MicroWoold Technologies Inc. ("ULENSOR"), AND IT 'PRIOR PROPOSAL, REPRESENTATION, OR BETWEEN THE PARTIES, OTHER THAN ANY WRITTEN JUTED BY BOTH OF THE PARTIES, WHICH SHALL LICENSE AGREEMENT. The following terms set forth your rights with respect to use of th	•
Program		~
• Laccept the agre	ement	
C I do not accept th	ne ageement	
	and a second	

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**'.

	us Detected III You will need to buy eSi IY ESCAN or BUY THIS TOOL button to g	can or this tool in ord to our web-store.	er to eliminate this virus	from your System, Click o
		-		
MicroW	orld AntiVirus & Spyware Too	lkit Utility (Ver	6.1.4)	
Objects Sc.	anned			Powered by Kaspersk
Tue May 03 Tue May 03	2252.00 2005 -> Scanning File C. V 2252.00 2005 -> Scanning File C. V	ROGRA-1VATITE ROGRA-1VATITE ROGRA-1VATITE ROGRA-1VATITE VINDOWSVSJUND VINDOWSVDIt.exe ROGRA-1VMEDIO	2114TICON*114ipta 2114TICON*114ipta 2114TICON*114ipta 2114TICON*114ipta 2114TICON*114ipta 2120INPUT8.dl MAN.EXE N*2VPOWERC*11PC	so enee iso: di PUDOC DE U soci di MSER ~1.EXE
Marca I and a	form allow			-
File C. WAN File C. WAN	DDWSNPpatch we tagged as not a not a DDWSNDit eve tagged as not a virus?	nue: Tool Win32 HT Bugg/Phog Win32 C	Patch a No Action Ta ustomicona No Action	iken 1 Taken
Result	Total Objects Scanned 261			
	Total Virus(es) Found 2	*	Buy eScan	Stop Scrolling
	Total Disinfected Files 0		View Log	Cancel
	Total Deleted Objects 0			
	Total Files Renamed 0	Internet States and the		

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.

<u>Einsetzen von eScan – Auswertung:</u>

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

<u>1. Möglichkeit:</u> 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.

<u>2. Möglichkeit:</u> 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: [5] Rechtsklick auf die <u>Find.bat</u> -> 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 <u>Thread</u> 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 <u>Total Commander</u> 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 <u>KillBox</u>. 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 <u>eScan-Checkb9</u> 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 <u>Neuaufsetzen deines Systems mit anschliessender Absicherung</u> in Erwägung ziehen und durchführen. Somit wäre auch die Vertrauenswürdigkeit deines Systems wiedergegeben.

In Zusammenarbeit mit dedies - Team