DIETMAR **W**ALKER - **P**C-**B**LITZHELFER-**N**OTDIENST
Nationalgasse 14 • **7**2124 **P**liezhausen • ∅ **T**el. 07127 / 89194 - **F**ax 89118
Internet: http://www.pc-blitzhelfer.de – **M**obil 0172-882 79 55

Emsisoft Emergency Kit benutzen

So finden und beseitigen Sie Malware-Infektionen mit Emsisoft Emergency Kit

In Sicherheitswissen by Jochen on June 9, 2015 | Русский, Italiano, Français, English, Deutsch

Emsisoft Emergency Kit ist das einzige gratis, 100% portable Dual-Engine-Säuberungs-Tool, mit dem Sie Ihren PC auf Malware und potenziell unerwünschte Programme (PUPs) prüfen und davon befreien können. Das kostenlose Tool ist die beste Wahl als **Scanner zum Einholen einer Zweitmeinung** und verträgt sich mit anderen Antivirenprogrammen. **Verwenden Sie es, wenn Sie eine Infektion auf Ihrem Computer vermuten**, andere Schutz- und Säuberungslösungen jedoch daran scheitern, Sie aus Ihrer Misere zu erlösen. Das dauert gar nicht einmal lange – ein Scan mit Emsisoft Emergency Kit dauert üblicherweise nur eine Minute.

In diesem Tutorial liefern wir Ihnen eine Schritt-für-Schritt-Anleitung dazu, wie Sie Ihren Computer überprüfen und säubern.

1. Emsisoft Emergency Kit herunterladen und ausführen

Herunterladen: Falls Sie noch nicht Emsisoft Emergency Kit haben, laden Sie es bitte hier herunter. Zur privaten Verwendung ist es kostenlos und 100 % portabel; es ist also keinerlei Installation erforderlich. Der Inhalt der heruntergeladenen Datei wird in einen Zielordner Ihrer Wahl wie “C:\EEK\” entpackt und auf Ihrem Desktop eine Verknüpfung erstellt.

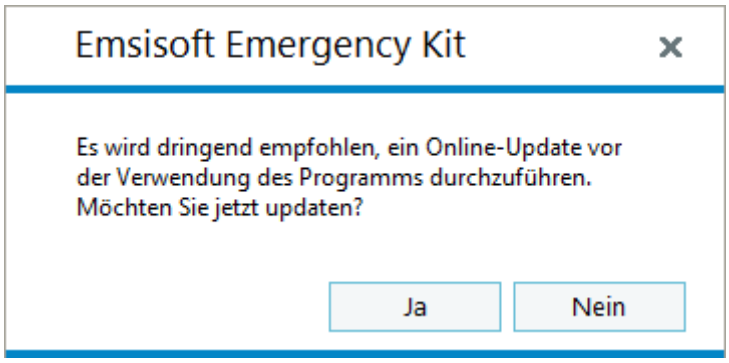
Hinweis: Sobald Sie die Software nicht mehr benötigen, löschen Sie einfach den gesamten Ordner und die Verknüpfung.

Ausführen: Doppelklicken Sie einfach auf die Verknüpfung zu Emsisoft Emergency Kit, die Sie auf dem Desktop finden, um den Scanner zu starten. Sollte Windows eine Warnmeldung anzeigen und Sie um Erlaubnis zum Ausführen des Programms mit Administratorrechten bitten, stimmen Sie bitte zu.

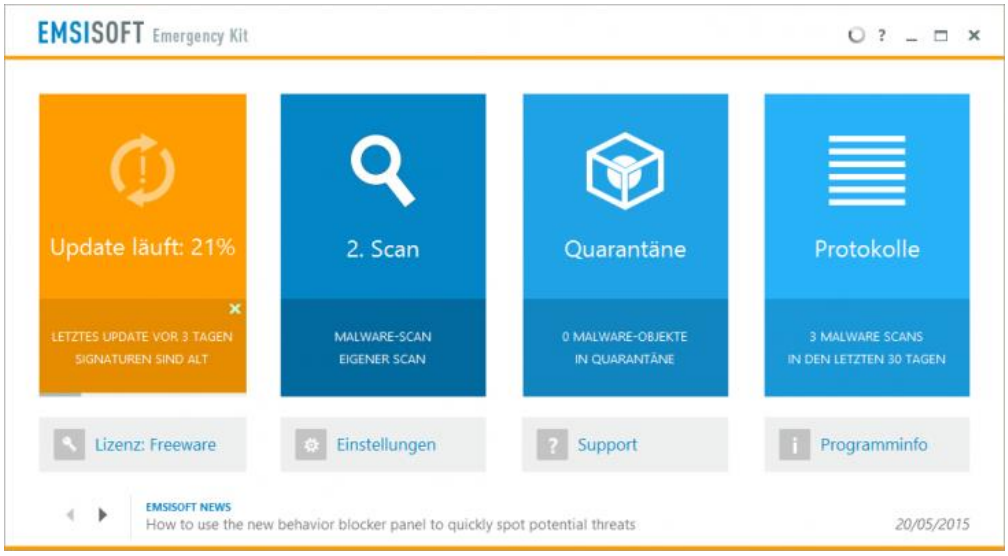
Die Software lässt sich ebenso von einem schreibgeschützten Medium wie CDs, DVDs oder BDs oder jedem anderen schreibgeschützten USB-Speicher starten. Auch wenn dabei keine Online-Updates möglich sind, so bleibt die Software selbst jedoch vollkommen funktionstüchtig für Scans und zur Säuberung, ohne dass Sie dabei das Risiko einer versehentlich Infektion des angeschlossenen Laufwerks eingehen.

2. Auf die neuesten Online-Updates prüfen

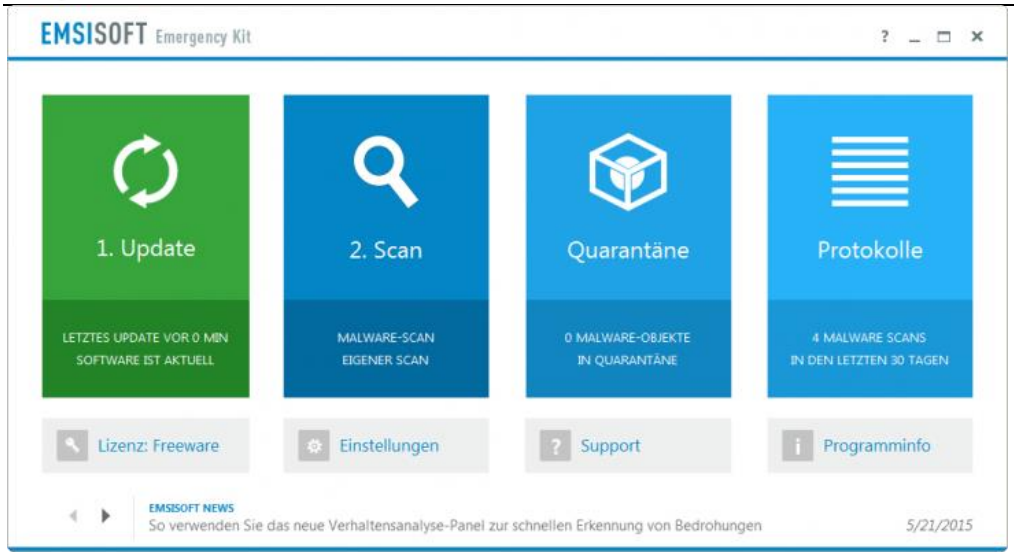
Wir raten Ihnen, jedes Mal vor einem Scan ein Online-Update durchzuführen, damit Sie stets über die neuesten Malware-Signaturen verfügen. Beim ersten Start des Programms werden Sie ebenso selbsttätig dazu aufgefordert.



Ebenso empfehlen wir Ihnen, "Ja" auszuwählen, wenn Sie bezüglich der Erkennung potenziell unerwünschter Programme (PUPs) durch unsere Software gefragt werden. Emsisoft ist ein Experte in der Beseitigung von PUPs, wie z. B. nutzlosen Browser-Toolbars oder nerviger Adware, die bekanntermaßen Ihren Rechner zumüllt und ausbremst.



Nach erfolgreichem Abschluss des Updatevorgangs ändert sich die Farbe des ersten Menüblocks von Orange zu Grün.

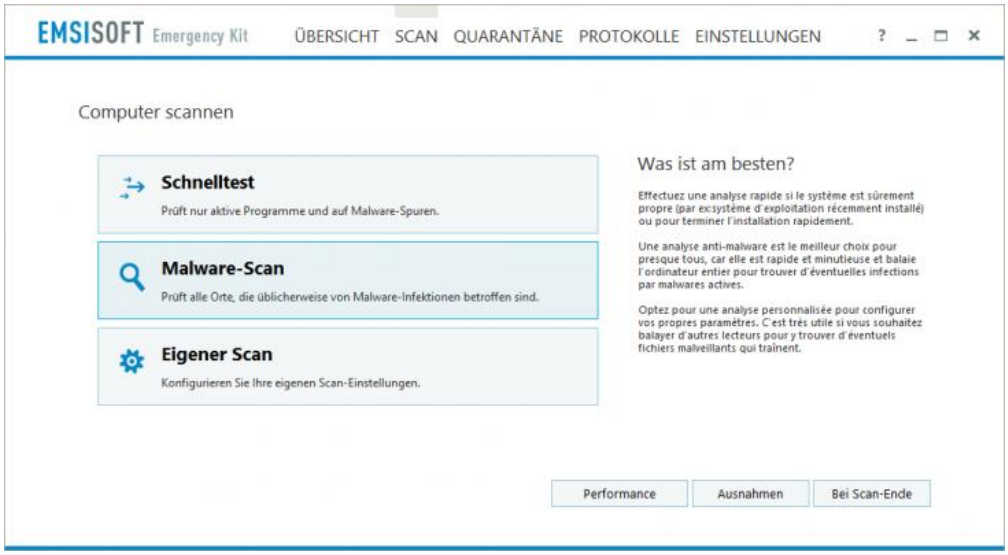


Nach Abschluss des Updates klicken Sie auf “SCANNEN” im Hauptmenü.

3. Einen Scan ausführen und den PC säubern

Nun können Sie einen Scan ausführen. Es stehen Ihnen drei Optionen zur Verfügung: Schnelltest, Malware-Scan und Eigener Scan.

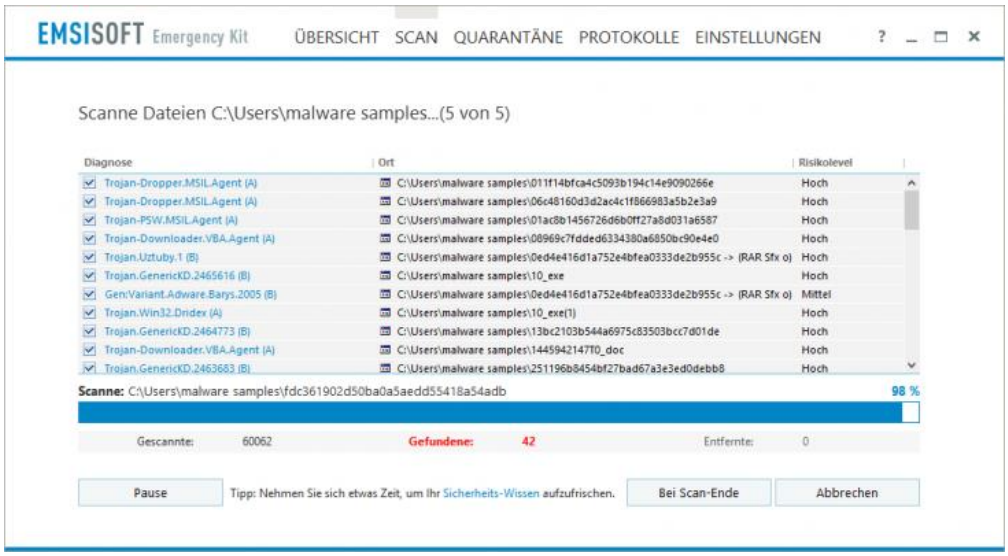
Beim Malware-Scan handelt es sich um die beste Wahl für die meisten Nutzer, da er auf die Prüfung von Speicherorten optimiert ist, die häufig von Malware befallen werden. Dabei entgeht üblicherweise keine Malware; jedoch sollten Sie, um 100 % gründlich vorzugehen und auch inaktive Malware-Dateien zu finden (oder auch beim ersten Scans Ihres PCs) einen “Eigenen Scan” auswählen. Dabei werden standardmäßig alle Inhalte Ihres PCs geprüft, auch lokale Laufwerke usw. Dieser Scan erweist sich als ebenfalls nützlich, wenn Sie eigene Scaneinstellungen vornehmen, zusätzliche Laufwerke auf Malware prüfen oder bestimmte Verzeichnisse ausschließen möchten.



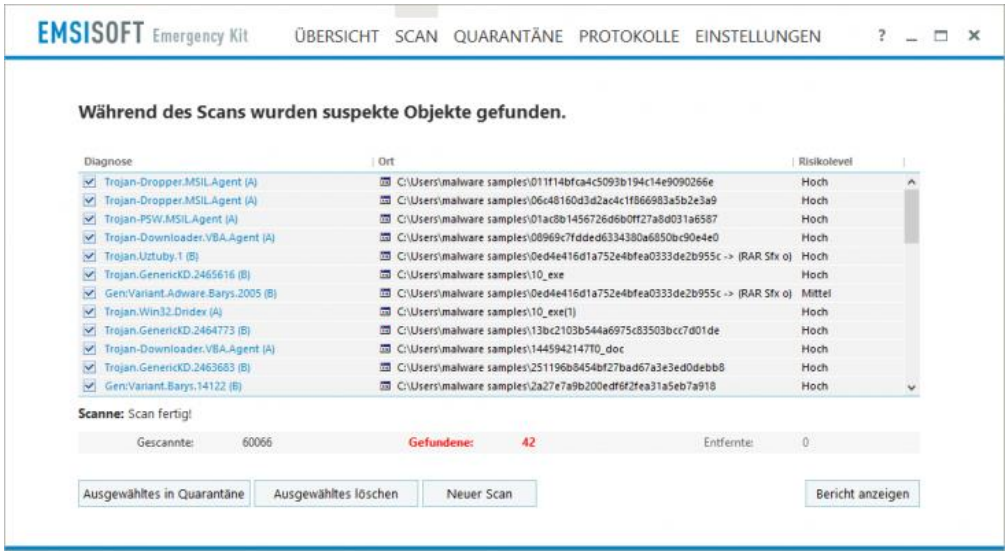
Entscheiden Sie sich für einen Schnelltest, wenn Sie sich sicher sind, dass Ihr System sauber ist, z. B. bei einem neuen Computer. Dabei werden nur aktive Programme geprüft und eine schnelle Suche nach bekannten Malware-Spuren im Dateisystem und der Registry erkannt.

4. So verfahren Sie bei Malware-Funden

Sollten bei dem Scan etwaige Malware oder PUPs auf Ihrem Computer erkannt werden, werden alle Funde angezeigt und bereits ausgewählt.



Sie können erkannte Objekte wahlweise unter Quarantäne stellen oder löschen. Wir empfehlen Ihnen in den meisten Fällen, Objekte unter Quarantäne zu stellen, da durch diese Option Malware vollständig inaktiv gemacht wird, indem sie in einen verschlüsselten Container verschoben. Dies macht die Malware unschädlich, die von einem unserer Techniker dann untersucht oder im unwahrscheinlichen Falle einer Fehlerkennung wiederhergestellt werden kann.

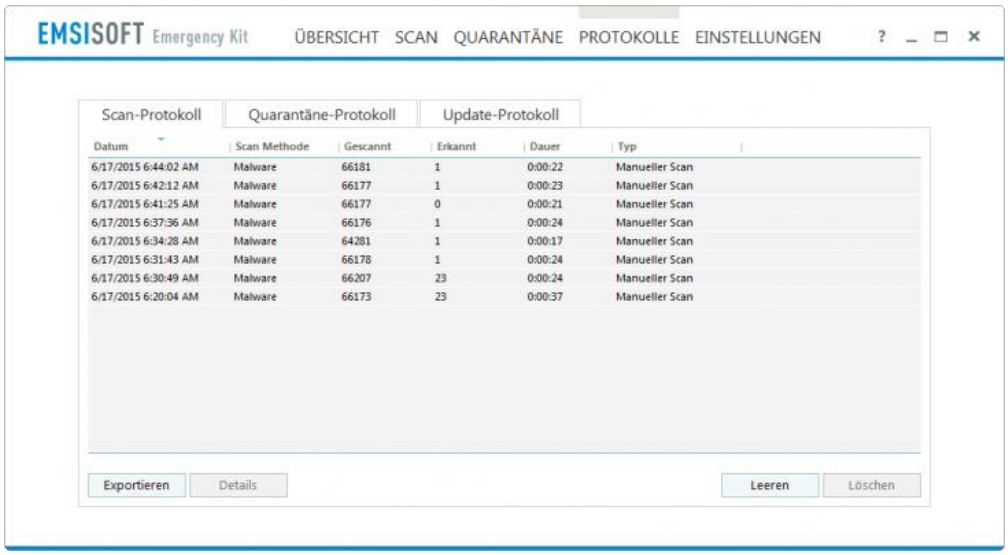


Falls Sie sich für die zweite Option entscheiden, so werden die erkannten Dateien sofort unwiderruflich gelöscht – verfahren Sie daher nur so, wenn Sie sich vollkommen sicher sind, dass es sich um bösartige Dateien handelt.

In sehr seltenen Fällen wird bei einem Scan auch ein Rootkit erkannt, das nicht ohne Weiteres gelöscht werden kann, ohne dass Ihr System beträchtlichen Schaden nimmt. In diesen Fällen werden Sie gebeten, mit einem unserer Malware-Beseitigungs-Experten im Emsisoft-Supportforum Kontakt aufzunehmen. Folgen Sie dessen Anweisungen, um Ihr System wieder funktionstüchtig zu bekommen.

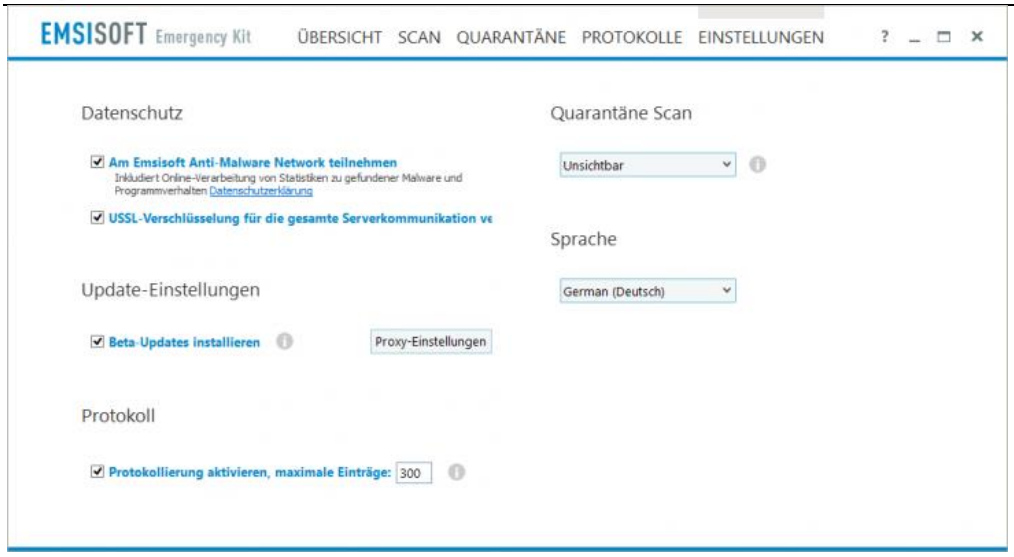
Scanprotokolle anzeigen

Alle Ereignisse beim Scannen, der Quarantäne und beim Update werden sorgsam protokolliert und lassen sich in "PROTOKOLLE" einsehen. Protokolle können unseren Analysten dabei helfen, falls Sie auf Probleme stoßen.



Zusätzliche Datenschutzeinstellungen und -optionen

In den "EINSTELLUNGEN" können Sie die Arbeitsweise von Emsisoft Emergency Kit bestimmen, insbesondere hinsichtlich des Datenschutzes. Sie können am Emsisoft Anti-Malware Network teilnehmen, unserer Cloud-basierten Datenbank, in der Informationen über alle möglichen Arten von Programmen, gutartigen wie bösartigen, gespeichert sind, die in Echtzeit überprüft werden. Durch Teilnahme an dem Programm stimmen Sie zu, dass anonyme Informationen über auf Ihrem Computer gefundene Malware gesammelt werden, die uns bei der Verbesserung der Malware-Erkennung unserer Produkte helfen können.



In diesem Abschnitt können Sie ebenso die SSL-Verschlüsselung für sämtliche Serverkommunikation deaktivieren, falls Sie die Informationen untersuchen möchte, die an die Webserver von Emsisoft gesendet und von diesen empfangen werden.

Eine erneute Überprüfung der Quarantäne wird standardmäßig jedes Mal durchgeführt, dass neue Signaturen-Updates heruntergeladen werden. Sollten sich ein fälschlicherweise erkanntes Objekt in der Quarantäne befinden, so werden Sie bei Überprüfung mit korrigierten Erkennungssignaturen gefragt, ob Sie dieses Objekt an seinen ursprünglichen Speicherort wiederherstellen möchten.

Aktivieren Sie die Beta-Updates nur dann, wenn Sie ein erfahrenerer Nutzer sind und von den neueste noch nicht getesteten Software-Updates profitieren möchten. Wenn Sie weitere Einblicke wünschen, dann melden Sie sich bitte bei unserem Beta-Tester-Programm an.

5. Für unsere Geeks: Emsisoft Commandline Scanner

Systemadministratoren, Sicherheitsexperten und erfahrene Kommandozeilennutzer werden dieses Tool zu schätzen wissen. Emsisoft Emergency Kit bietet ebenso Emsisoft Commandline Scanner, eine Anwendung für die Konsole

Emsisoft Commandline Scanner

für Profis, die keine grafische Benutzerschnittstelle benötigen. Er bietet die beinahe gleichen Funktionen wie der Emsisoft Emergency Kit Scanner mit grafischer Schnittstelle, und Fachleute nennen die neueste Version “einen der durchdachtesten Kommandozeilenscanner der Welt”.

Mit Emsisoft Commandline Scanner werden sich wiederholende Scans ein Leichtes, die sich ideal zur Verwendung in automatisierten Batch-Scripts eignen. Das Tool lässt sich einfach in Multi-Engine-Scan-Tools integrieren, und die erstellten Logdateien sind leicht auszulesen. Für weitere Informationen siehe die Produktdetails.

Zum Ausführen von Emsisoft Commandline Scanner gehen Sie entweder zu “C:\EEK\” und führen die Datei “Start Commandline Scanner.exe” aus, um eine Übersicht der verfügbaren Parameter zu sehen, oder Sie suchen direkt nach der Datei “a2cmd.exe” im Ordner “bin” und starten das Tool von dort aus.

Quelle: http://blog.emsisoft.com/de/2015/06/09/so-finden-und-beseitigen-sie-malware-infektionen-mit-emsisoft-emergency-kit/?ref=news150716&utm_source=newsletter&utm_medium=newsletter&utm_content=blog&utm_campaign=news150716