
Gebrauch der Notfall-CDs von ESET, Kaspersky und Avira

Inhalt

1. Einleitung	1
2. Alternativen zu den Notfall-CDs.....	3
3. Verwendung der ESET SysRescue	4
4. Verwendung der Kaspersky Rescue Disk 2018	15
5. Verwendung der Avira Antivir Rescue System 18	24
6. Troubleshooting	35

1. Einleitung

Mit den Lösungen ESET SysRescue, Kaspersky Rescue Disk 2018 und Avira Antivir Rescue System stehen den Mitarbeitern des Forschungszentrums Jülich (auch für den privaten Einsatz) drei leistungsfähige Notfallmedien („Notfall-CDs“) zur Verfügung, um Windows- und auch Linux-Partitionen auf Malware zu untersuchen. Dabei sollen eventuelle Infektionen erkannt und bekämpft werden.

Voraussetzung hierfür sind tagesaktuelle Virensignaturen, weswegen alle Lösungen entsprechende Update-Prozeduren besitzen. Es wird dringend empfohlen, vor der eigentlichen Untersuchung auch tatsächlich ein solches Update durchzuführen, damit die Notfall-CDs ihre volle Leistungsfähigkeit entfalten können.

Bei allen drei Lösungen können die bereitgestellten ISO-Images sowohl in Form eines USB-Sticks genutzt als auch als CD/DVD gebrannt werden. Zwecks Vereinfachung wird im weiteren Verlauf einheitlich von Notfall-CDs gesprochen.

Grundsätzlich kann keine Garantie übernommen werden, dass die Notfall-CDs mit allen vorliegenden Hard- und Softwarekombinationen korrekt funktionieren, oder dass die Update-Prozeduren mit allen verfügbaren Netzwerkadaptern zusammenarbeiten. Sollten

diesbezüglich Probleme auftreten, sind einige Tipps in den jeweiligen Anleitungen sowie in Kapitel 6-Troubleshooting aufgeführt; ebenso können Sie sich an ihren PC-Ansprechpartner oder –Dienstleister sowie die JuNet-Hotline unter der Durchwahl 6440 wenden.

Auf vielen, insbesondere jüngeren, Hardware-Plattformen ist eine Anpassung der UEFI-Einstellungen notwendig, damit die Notfall-CDs korrekt funktionieren. Darauf wird in den jeweiligen Kapiteln kurz eingegangen; grundsätzlich ist bei Problemen hilfreich, <Secure Boot> zu deaktivieren. Evtl. muss auch der UEFI-/BIOS-Modus angepasst werden (<Legacy>).

Alle drei Lösungen können keine verschlüsselten Partitionen untersuchen, was auch den Sicherheitserwartungen hinsichtlich der Medienverschlüsselung widersprechen würde. Eine zu untersuchende Partition muss daher zunächst vom Benutzer manuell entschlüsselt werden, bevor die Notfall-CDs eingesetzt werden. Fortgeschrittene Benutzer finden im World Wide Web Anleitungen, wie einige der gängigen Verschlüsselungstechniken den Notfall-CDs individuell hinzugefügt werden können, hierauf wird in dieser TKI nicht weiter eingegangen.

Darüber hinaus kann keine Garantie übernommen werden, dass jede Infektion durch die Notfallmedien korrekt erkannt und geheilt werden kann. Wird ein System von einer Notfall-CD als nicht oder nicht mehr infiziert gemeldet, sollte dies vorsichtshalber von mindestens einer der anderen Lösungen bestätigt werden. Einmal befallene Systeme sind zunächst als nicht mehr vertrauenswürdig anzusehen, auch wenn eine Notfall-CD eine erfolgreiche Bekämpfung meldet. In Abhängigkeit der Umstände ist mittelfristig eine erneute Untersuchung oder gar eine Neuinstallation sinnvoll.

JSC empfiehlt die Anwendung mit der hier gewählten Priorität: Zuerst die ESET SysRescue, dann Kaspersky Rescue Disk 2018 und schließlich die Avira Antivir Rescue System.

2. Alternativen zu den Notfall-CDs

Einige Alternativen zu den Notfall-CDs sollen noch genannt werden, die den Benutzer eines verdächtigen Systems unterstützen können. Dies ist insbesondere bei Hardwarekonflikten hilfreich, die die Nutzung der Notfallmedien verhindern.

Zunächst wird McAfee Stinger erwähnt, der (im Gegensatz zu den Notfall-CDs) direkt auf der Windows-Oberfläche des zu prüfenden Systems eingesetzt wird. Die Virusdatenbank umfasst dabei die zum jeweiligen Zeitpunkt als höchst bedrohlich eingestuften Viren, daher ist Stinger stets tagesaktuell herunterzuladen.



Download McAfee Stinger:

<https://downloadcenter.mcafee.com/products/mcafee-avert/stinger/stinger32.exe>

Ebenso handelt es sich beim Microsoft Safety Scanner um ein Tool, das direkt auf der Oberfläche eines verdächtigen Windows-Systems eingesetzt werden kann, wenn dem lokalen Virens scanner nicht mehr vertraut wird. Es kann im konkreten Bedrohungsfall kostenlos heruntergeladen und 10 Tage lang benutzt werden.



Download Microsoft Safety Scanner und eine Kurzeinführung:

<https://docs.microsoft.com/de-de/windows/security/threat-protection/intelligence/safety-scanner-download>

Ebenfalls von Microsoft stammt der Windows Defender Offline, der bei einer vermuteten Infektion eine Untersuchung auf Schadsoftware durchführen kann, und bereits in Windows 10 integriert ist. Auch dieser wird nur bei Bedarf ausgeführt, ersetzt also keinen Virens scanner.



Kurzanleitung Microsoft Windows Defender Offline:

<https://support.microsoft.com/de-de/help/17466/windows-defender-offline-help-protect-my-pc>

Zuletzt wird noch auf die PC-Welt Rettungs-DVD verwiesen, die neben mehreren Virens scannern auch weitere Administrationstools für Windows-Systeme enthält, z.B. Hardware-Diagnose, Datenrettung und Backups.



Download PC-Welt Rettungs-DVD:

<https://www.pcwelt.de/downloads/PC-WELT-Notfall-DVD-3890747.html>

3. Verwendung der ESET SysRescue

Sie finden ein ISO-Image der ESET SysRescue auf dem PCSRV unter



[\\pcsrv.zam.kfa-juelich.de\public\Notfall-CDs\01-ESET-SysRescue](https://pcsrv.zam.kfa-juelich.de/public/Notfall-CDs/01-ESET-SysRescue)

welches in regelmäßigen Abständen aktualisiert wird (was jedoch nicht das tagesaktuelle Update der Virensignaturen ersetzt).



Auf EFI/UEFI-Systemen ist die ESET SysRescue je nach Hardwarekonfiguration nur dann lauffähig, wenn Sie im System Setup <Secure Boot> deaktivieren und den UEFI-Modus <Legacy> bzw. <Legacy only> wählen.

Starten Sie das betroffene System mit der ESET SysRescue, indem Sie aus dem ISO-Image einen bootfähigen USB-Stick erzeugen. Benutzen Sie hierzu geeignete Software von Drittanbietern; erfolgreich getestet wurde das ESET-Image z.B. mit Rufus Portable. Beachten Sie, dass der bisherige Inhalt des USB-Sticks gelöscht wird.



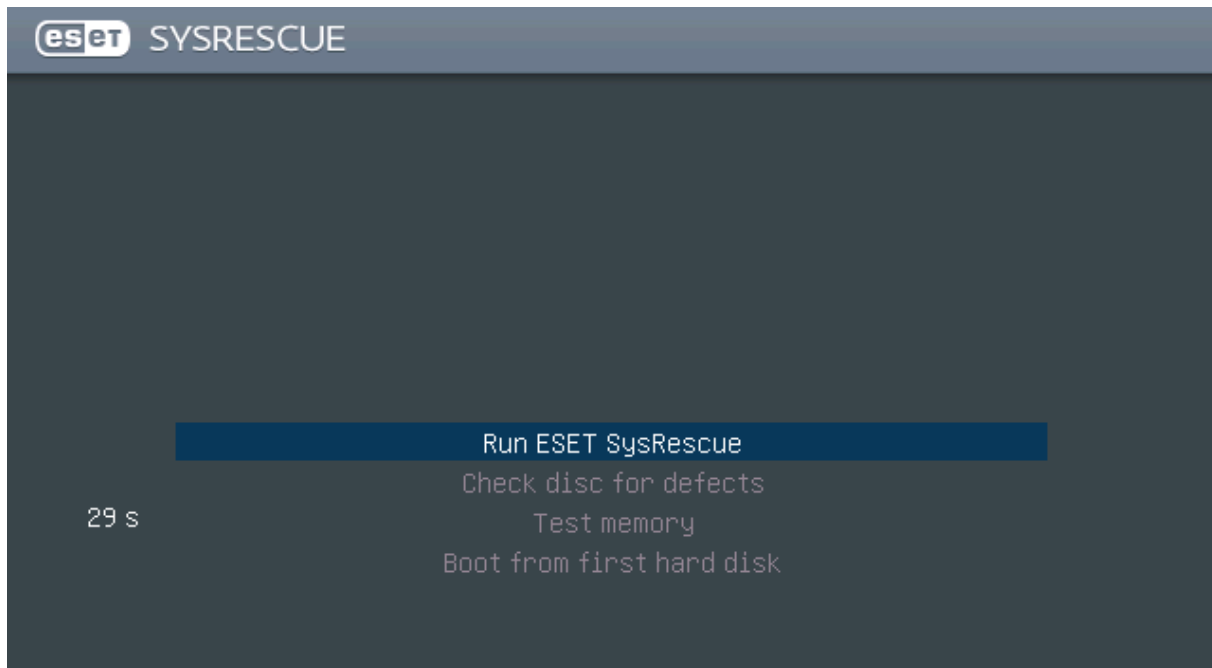
Download Rufus Portable:

<https://rufus.ie/de/>

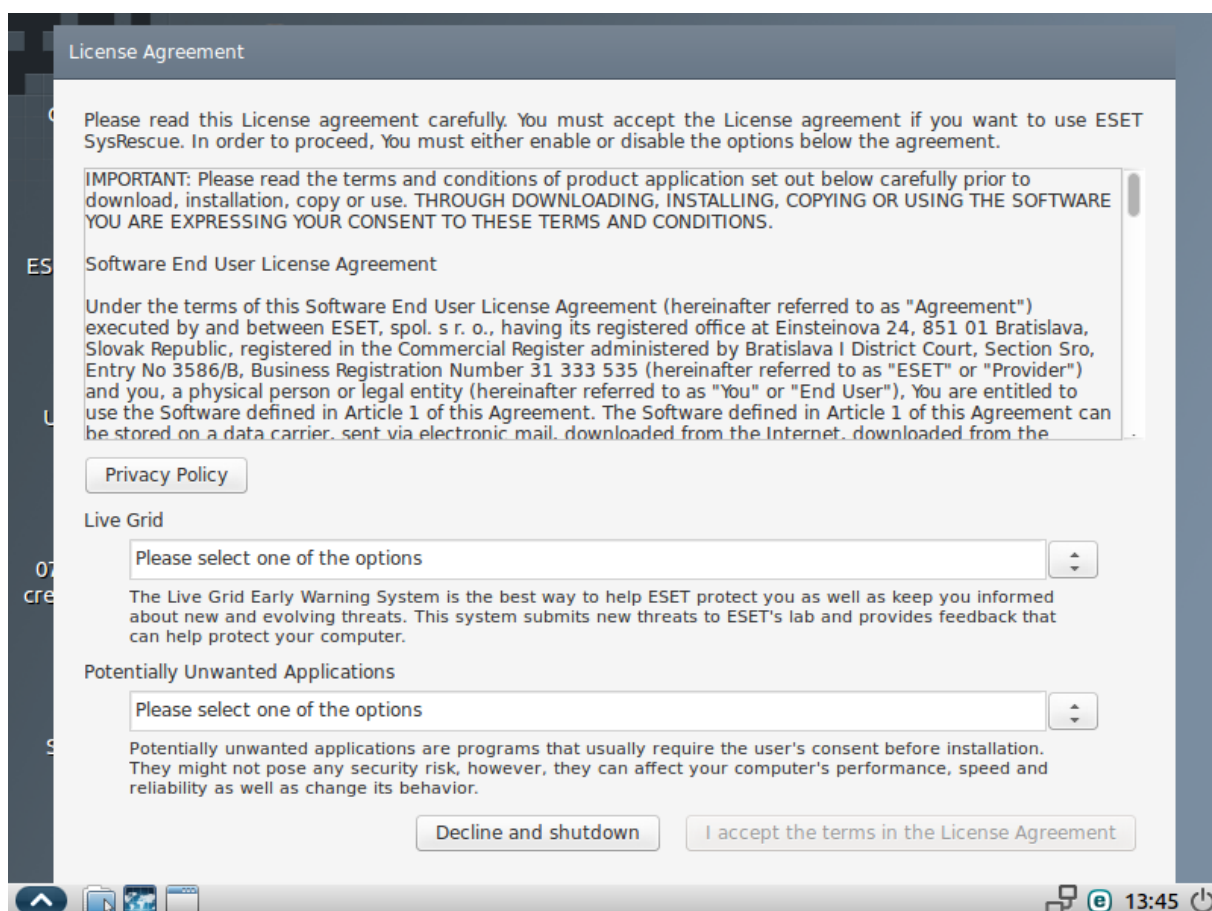


Alternativ können Sie das ISO-Image auch als CD/DVD brennen und von dieser das betroffene System neu starten. Nutzen Sie hierzu das in Ihrem Institut vorhandene Angebot an Software oder die in Windows 10 integrierte Funktion <Datenträgerabbild brennen>.

Es erscheint das Bootmenü der Notfall-CD.



Bestätigen Sie <Run ESET SysRescue> mit <Return>. Nach einer Wartezeit von 30 Sekunden startet der Bootvorgang selbsttätig, wenn Sie keine Eingabe machen.

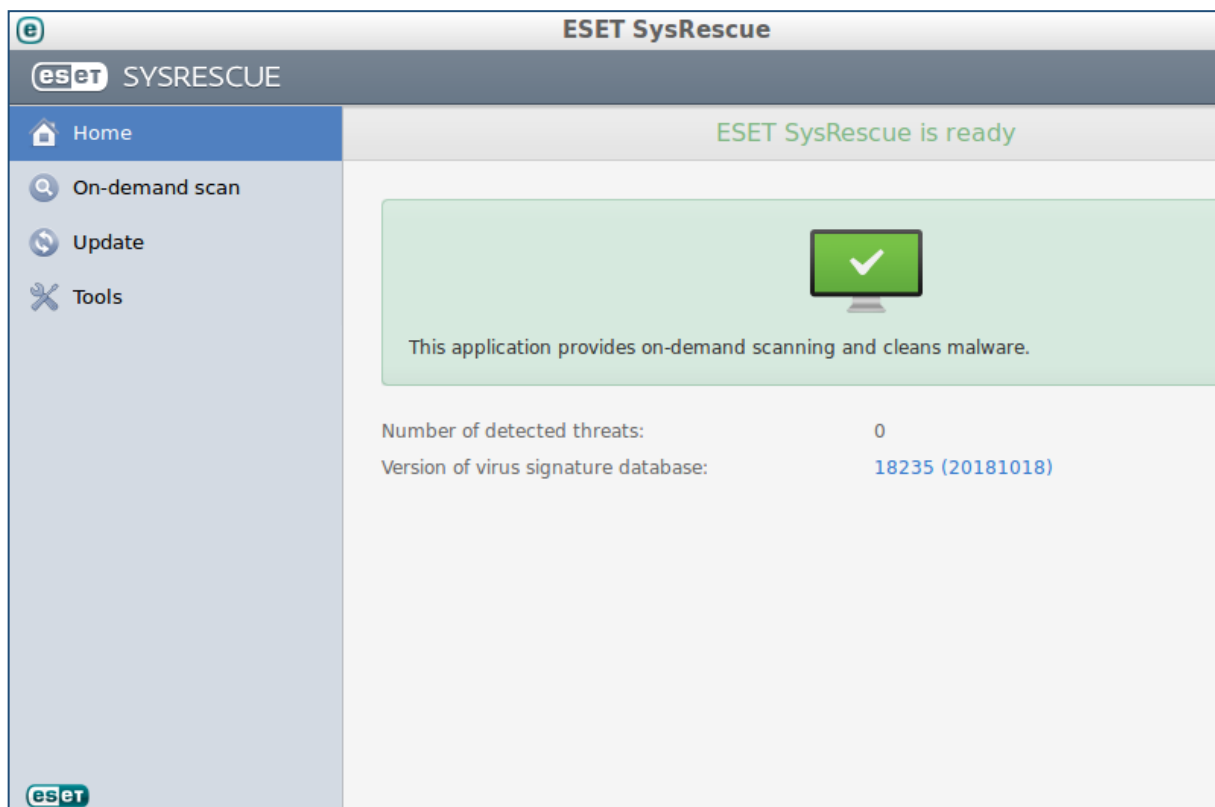


Zunächst wird der Lizenzvertrag angezeigt; um diesen bestätigen zu können, müssen Sie noch zwei Optionen wählen:

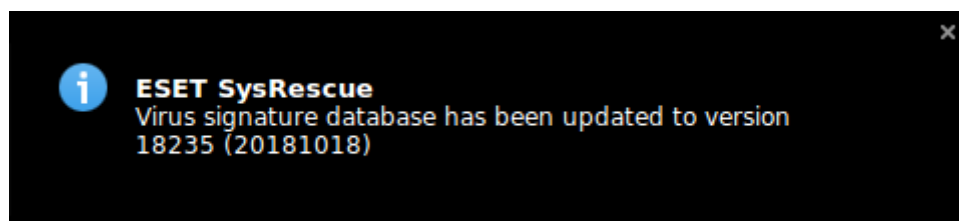
Live Grid: Wenn Sie <Enable Live Grid Early Warning System> wählen, werden Informationen über gefundene Malware an den Hersteller versendet, um die Früherkennung neuer Bedrohungen zu verbessern. Wenn Sie dies nicht wünschen, wählen Sie <Disable...> aus, die Notfall-CD ist auch dann voll funktionstüchtig.

Potentially Unwanted Applications: Wählen Sie hier <Enable...> aus, so prüft die Notfall-CD auch auf Programme, die keine Malware im engeren Sinne sind, aber Vertraulichkeit und Performanz Ihres Systems herabsetzen können. Dies betrifft z.B. bestimmte Werbemaßnahmen oder Spyware. Wenn Sie die Prüfung nicht für notwendig halten, wählen Sie <Disable...>, die Prüfung auf Malware findet dennoch normal statt.

Nach der Auswahl beider Felder können Sie mittels <I accept the terms in the License Agreement> bestätigen. Es erscheint das Hauptmenü der Notfall-CD.

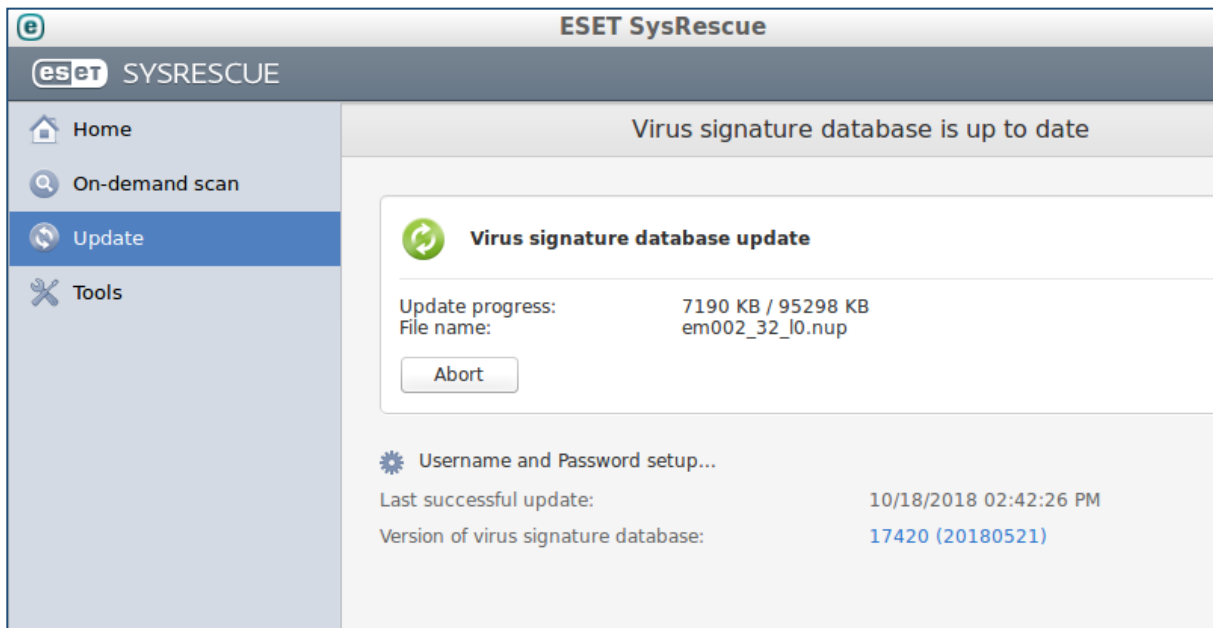


Bei einer bestehenden Verbindung zum öffentlichen Netz erhalten Sie eventuell bereits jetzt die folgende Meldung, dass ein Update der Virusmusterdefinitionen erfolgreich durchgeführt wurde:

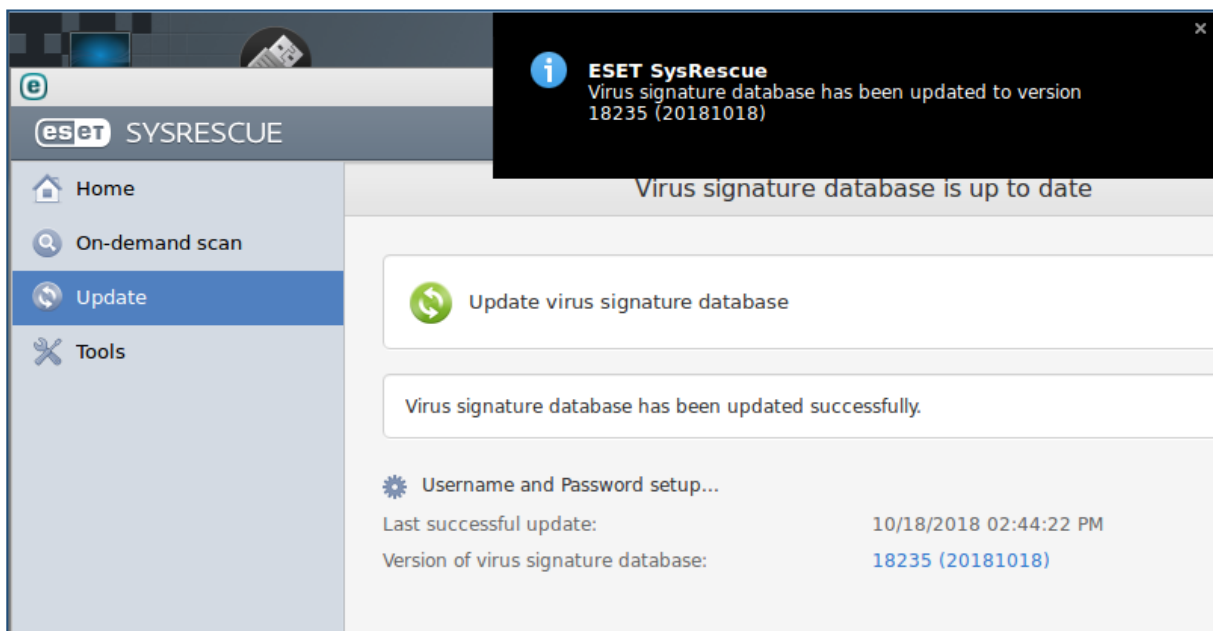


In diesem Fall müssen Sie kein weiteres Update mehr vornehmen, Sie können direkt weiter unten mit der Verwendung der Notfall-CD fortfahren.

Haben Sie dagegen noch keine solche Meldung gesehen, klicken Sie im Hauptmenü auf <Update>. Wenn Sie die folgende Ansicht erhalten, besteht eine Verbindung zum öffentlichen Netz und es wird gerade ein Update durchgeführt:

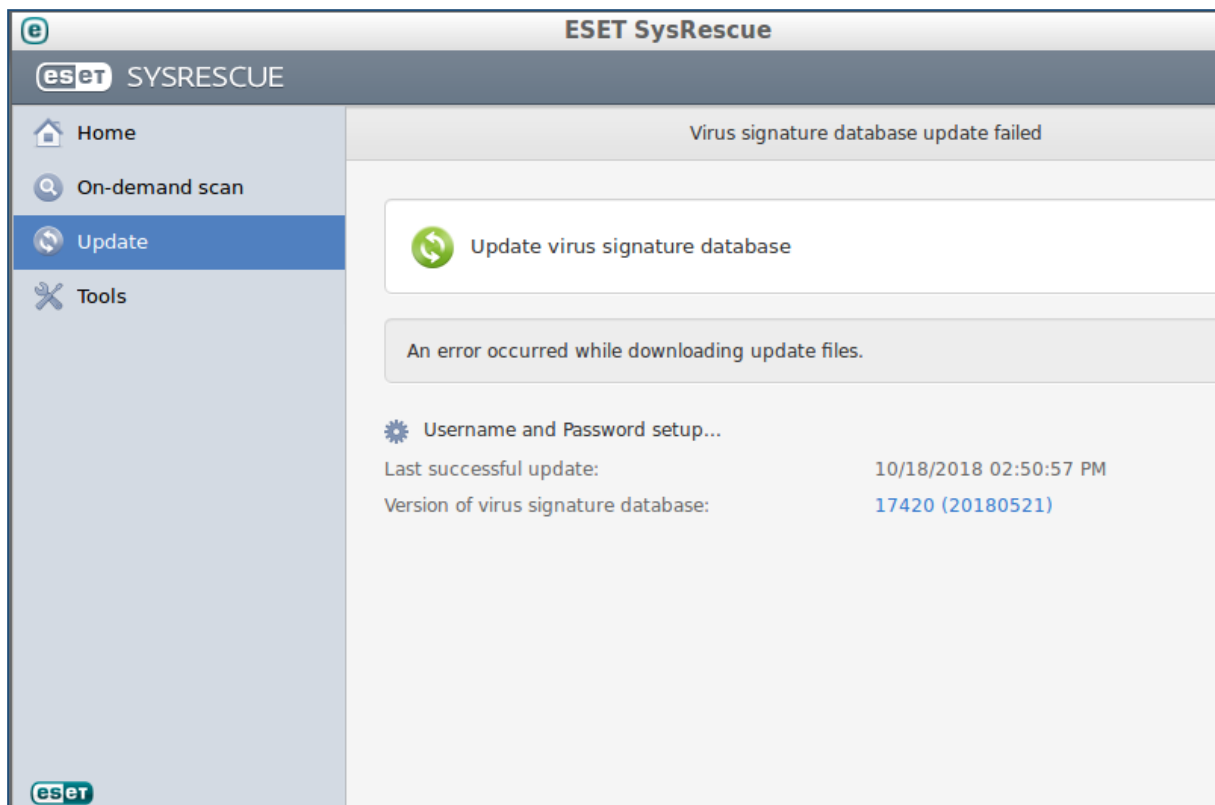


In diesem Fall brauchen Sie nur abzuwarten, bis das Update abgeschlossen ist und die folgende Meldung erscheint:




Sie können dann weiter unten mit der normalen Verwendung der Notfall-CD fortfahren.

Erhalten Sie dagegen die nachfolgend gezeigte Meldung „An error occurred while downloading update files.“, so konnte ein Update der Virismusterdefinitionen nicht erfolgreich durchgeführt werden.



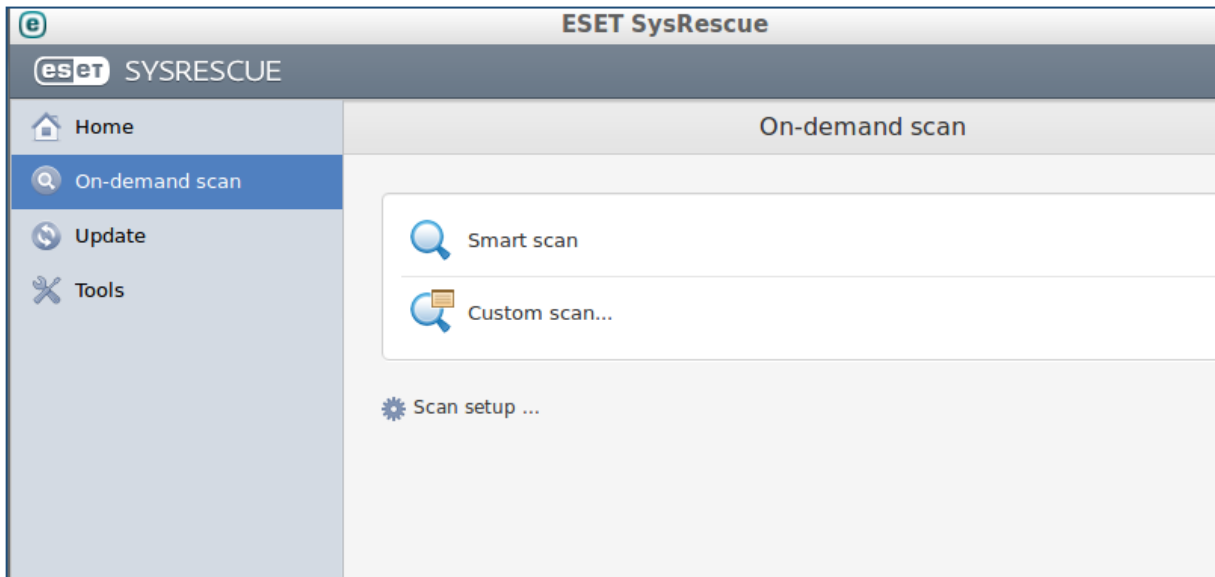
Vermutlich bestand zum Zeitpunkt des Updateversuchs keine Verbindung zum öffentlichen Netz. Beheben Sie das Problem und starten Sie einen erneuten Versuch mittels Klick auf <Update virus signature database>. Ziehen Sie ggfs. die Tipps unter Kapitel 6-Troubleshooting hinzu.



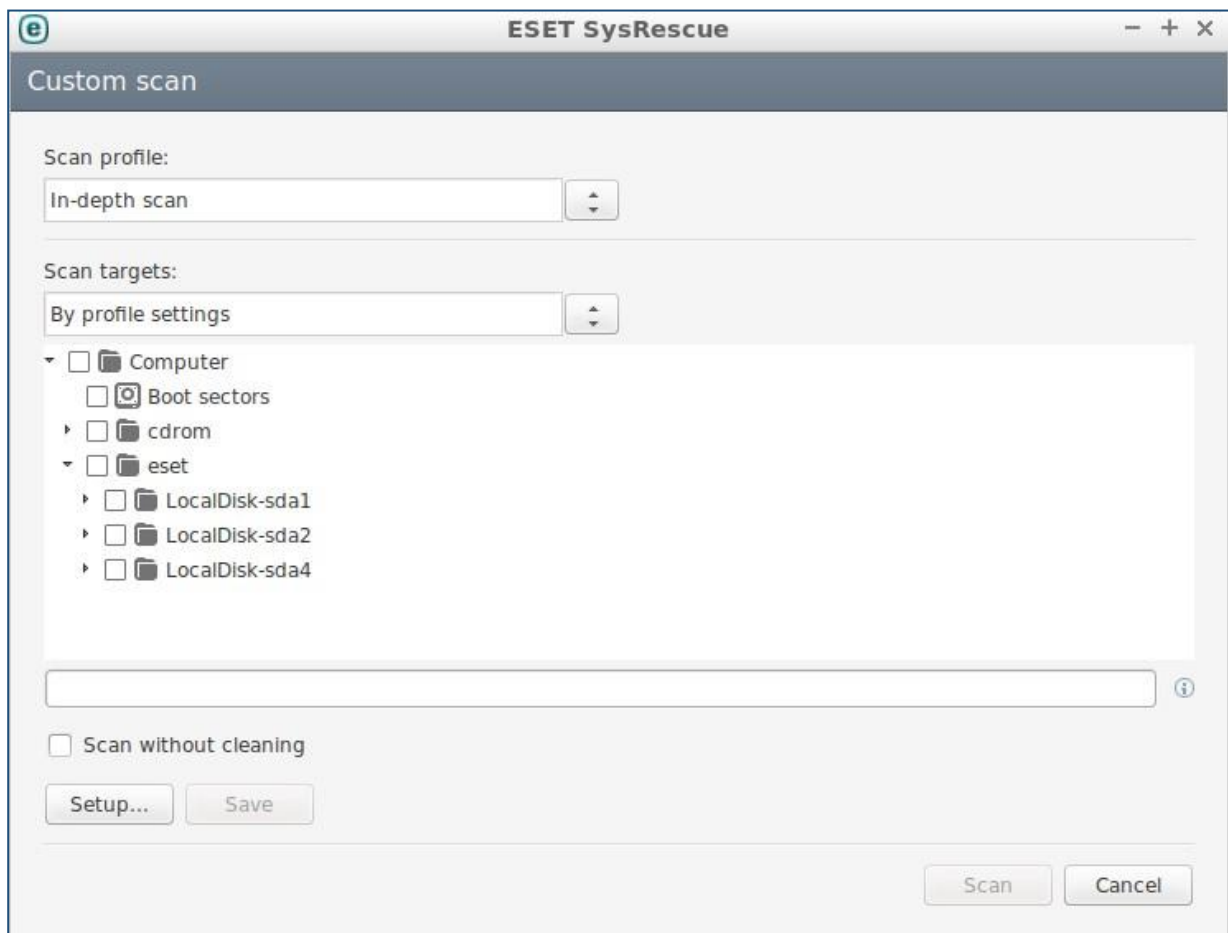
Fortgeschrittene Benutzer können eine manuelle Konfiguration der Netzwerkverbindung versuchen, indem Sie auf der Benutzeroberfläche unter  erst <Preferences> und dann <Network Connections> wählen.

Die Verwendung der Notfall-CD ist auch ohne ein Live-Update möglich, jedoch ist bei veralteten Virusmusterdefinitionen die Erkennung aktueller Bedrohungen nur stark eingeschränkt möglich.

Nach dem Update klicken Sie im Hauptmenü der Notfall-CD auf <On-demand scan>.



Klicken Sie auf <Custom scan...>, um eine vollständige Untersuchung des Systems mit hoher Intensität durchzuführen. Alternativ können Sie mit <Smart scan> auch einen schnelleren Scan durchführen, der jedoch nur mit niedrigerer Intensität durchgeführt wird.



Achten Sie darauf, dass im Feld <Scan profile:> die Auswahl <In-depth scan> eingestellt ist, wählen Sie diese ggfs. aus. Damit ist der Scan hoher Intensität voreingestellt und Sie müssen keine weiteren Angaben machen. Alternativ können Sie auch mit Klick auf <Setup...> die Scanparameter einsehen und verändern:

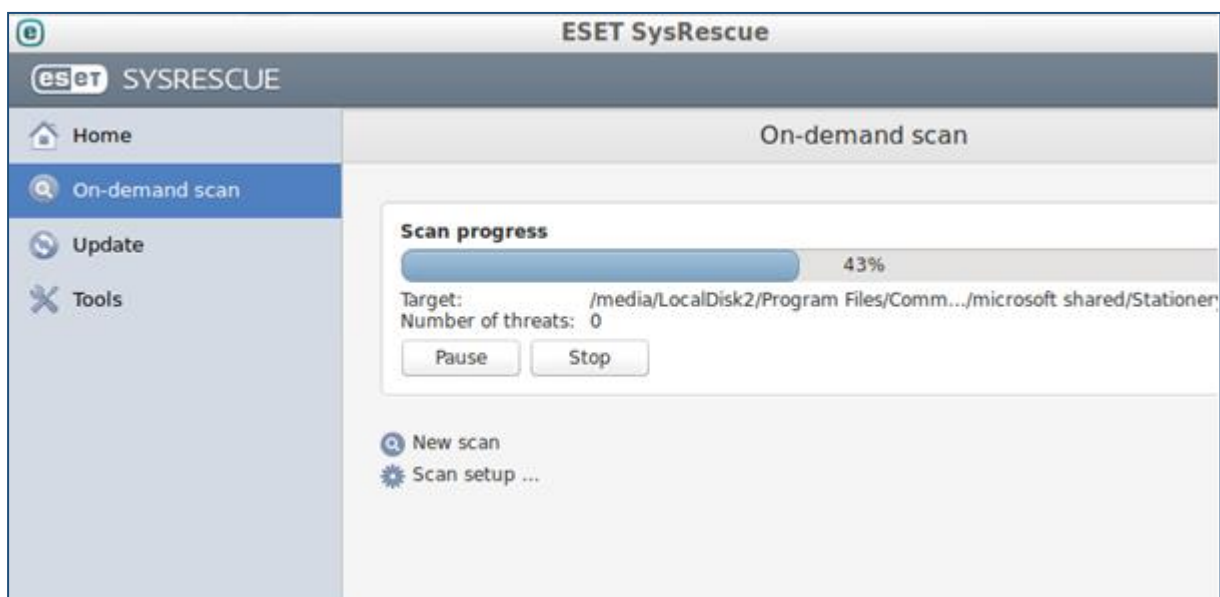


Verlassen Sie diese Ansicht wieder mittels <OK>. Wählen Sie nun in der vorherigen Ansicht alle Laufwerke (LocalDisk...) aus, die von der Notfall-CD überprüft werden sollen. Wenn Sie nicht sicher sind, welche Laufwerke von einer Infektion betroffen sein könnten, wählen Sie alle Laufwerke aus.



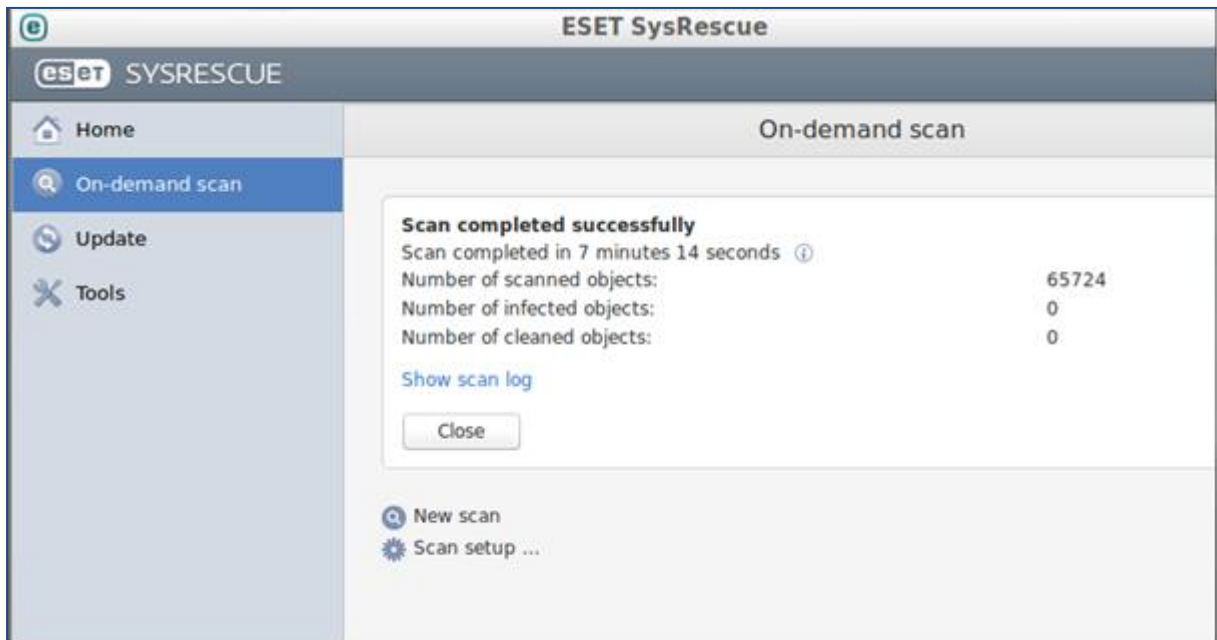
Bootfähige Partitionen sollten auf jeden Fall eingebunden werden. Wählen Sie auch den Eintrag <Boot sectors>.

Klicken Sie nach der Laufwerksauswahl auf <Scan>. Es beginnt die eigentliche Untersuchung des Systems.

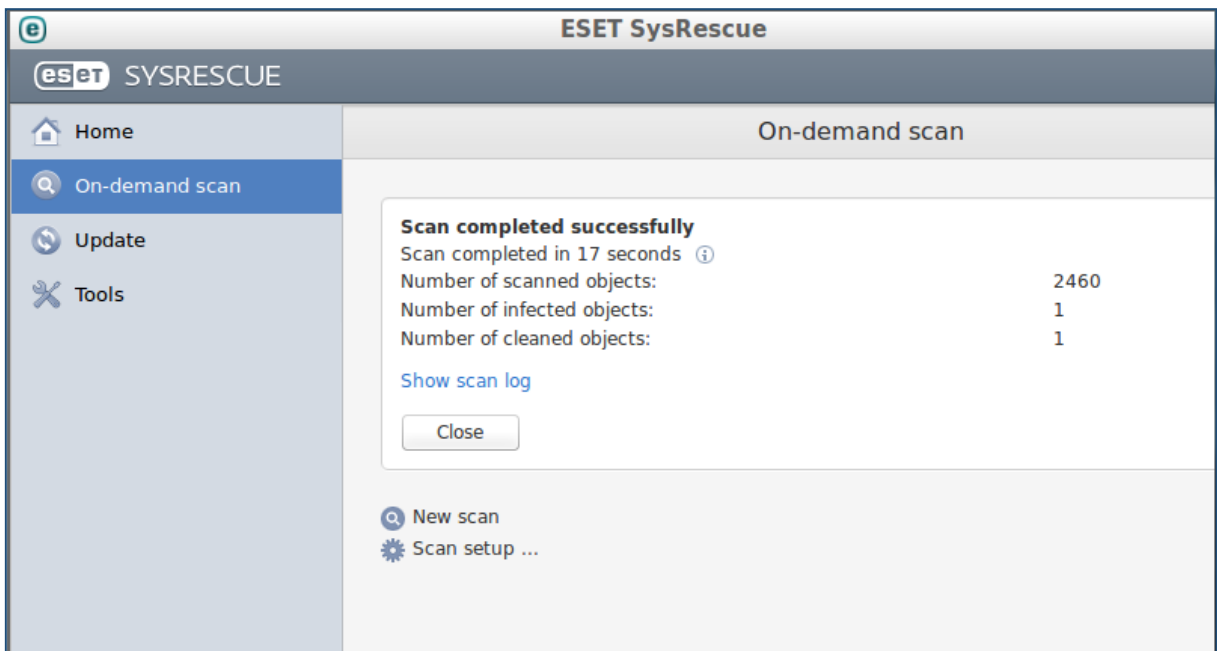


Mit <Pause> und <Stop> kann der laufende Scan unter- bzw. abgebrochen werden. Im Feld `Number of threats`: finden Sie die Angabe, wie viele (mögliche) Infektionen bereits gefunden wurden.

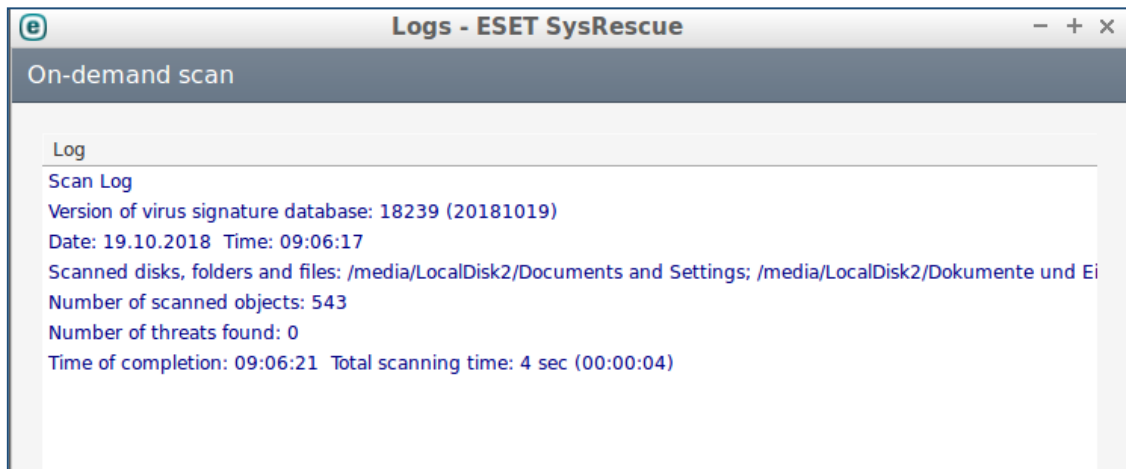
Nach Abschluss des Scans erhalten Sie eine Zusammenfassung. Sofern keine Bedrohungen gefunden wurden, sind die Werte `Number of infected objects` und `Number of cleaned objects` jeweils 0.



Wurden dagegen Bedrohungen gefunden, zählen diese Werte entsprechend hoch:

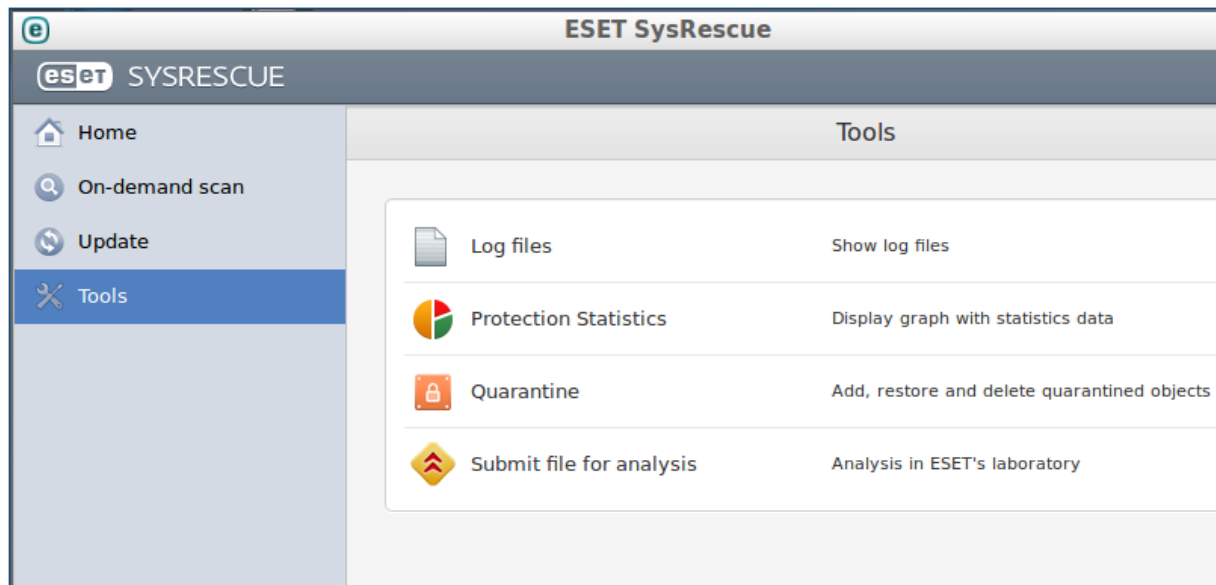


Mittels Klick auf <Show scan log> können Sie sich Informationen über die Funde anzeigen lassen:



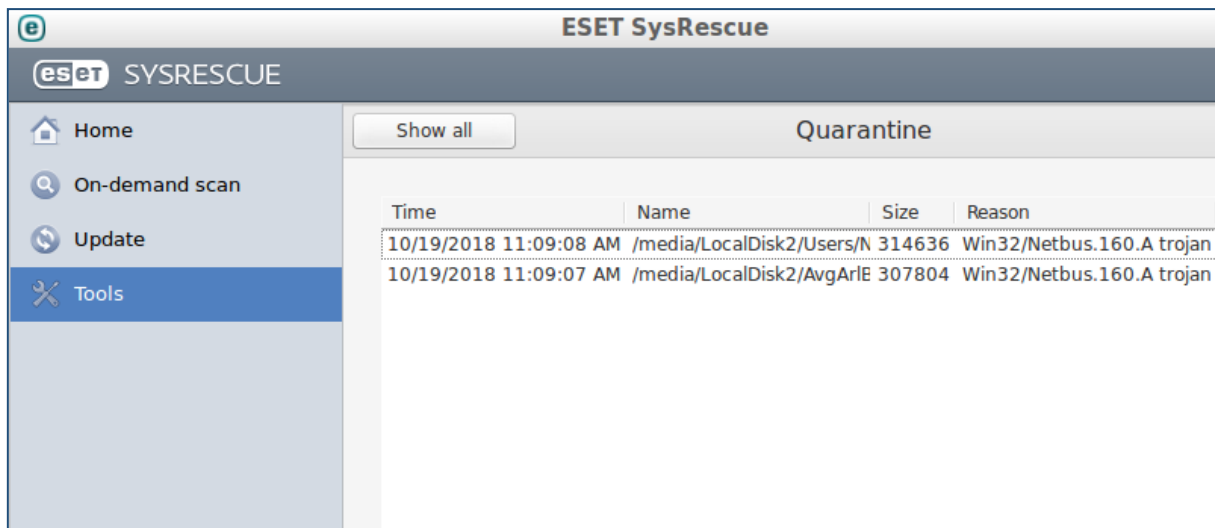
Verlassen Sie diese Ansicht mittels <Close>. In der vorherigen Ansicht können Sie nun nach Bedarf mittels <Scan setup...> die Scanparameter ändern und danach mittels <New scan> einen neuen Scan veranlassen.

Außerdem sei noch auf die Tools im Hauptmenü hingewiesen:



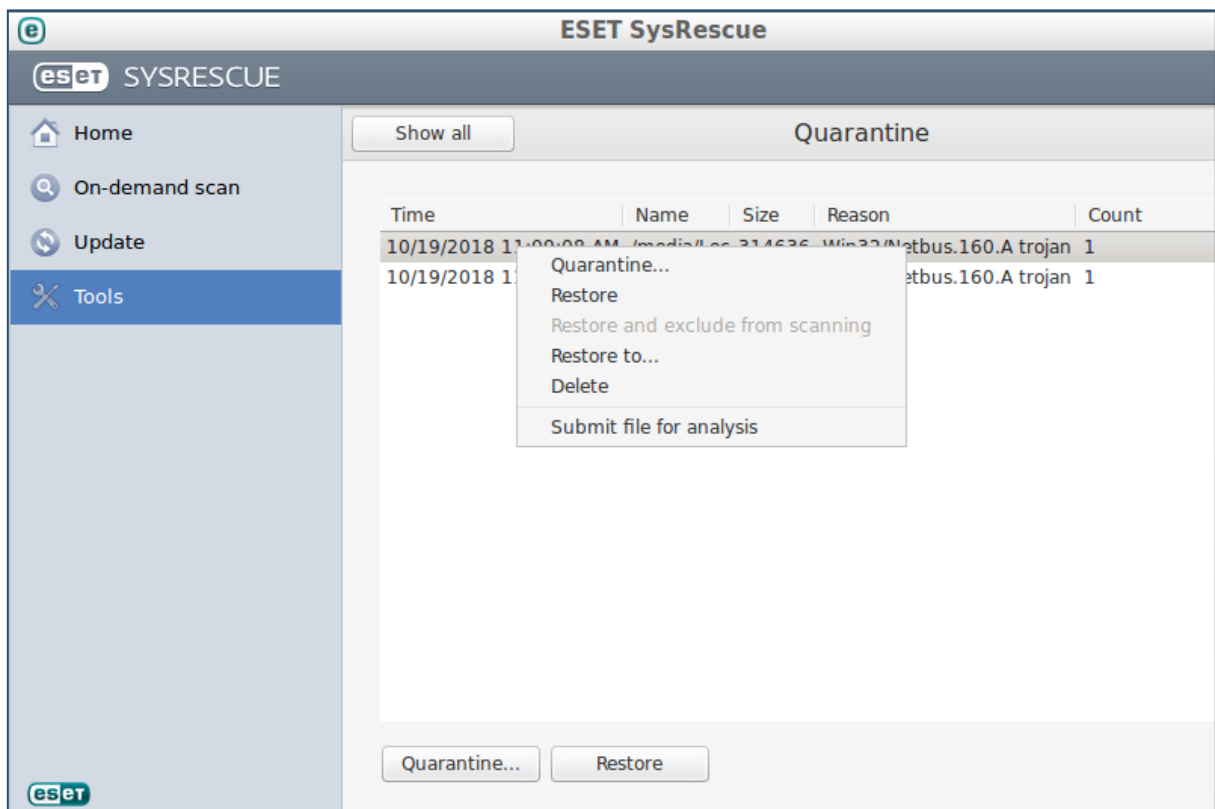
<Log files> bietet die Möglichkeit, die Ergebnisse aller Scanvorgänge der laufenden Sitzung erneut anzeigen zu lassen. <Protection Statistics> stellt die Scanergebnisse in einem Schaubild dar. Mittels <Submit file for analysis> können Sie eine verdächtige Datei an ESET zur Diagnose übermitteln; dies funktioniert allerdings nur, wenn Sie bei der Bestätigung des Lizenzvertrages Live Grid Early Warning System aktiviert haben.

Alle gefundenen Bedrohungen werden von der ESET SysRescue zunächst in einen Quarantäne-Ordner verschoben, eine Übersicht können Sie mit <Quarantine> aufrufen:



Im hier gezeigten Beispiel wurden zwei Infektionen gefunden. In den Spalten finden Sie den Zeitstempel des Fundes (Time), Pfadangabe und Dateinamen (Name), die Dateigröße (Size), eine Kurzbeschreibung der Infektion (Reason, hier ein Trojaner vom Typ Netbus.160.A) und die Anzahl (Count).

Sie können auf jeden Eintrag der Liste per Rechtsklick ein Kontextmenü öffnen:



Mittels <Quarantine...> können Sie die Datei aus dem vordefinierten Quarantänebereich in ein beliebiges anderes Verzeichnis verschieben. Mit <Delete> löschen Sie die Datei endgültig.

Mittels <Restore> stellen Sie die verdächtige Datei in ihrem ursprünglichen Verzeichnis unverändert wieder her. Dies sollten Sie natürlich nur tun, wenn die Datei als sicher betrachtet werden kann. Mit <Restore to...> wird die verdächtige Datei in einem Verzeichnis Ihrer Wahl wiederhergestellt.

<Submit file for analysis> überträgt die Datei an ESET zur weiteren Analyse. Dies funktioniert allerdings nur, wenn Sie bei der Bestätigung des Lizenzvertrages Live Grid Early Warning System aktiviert haben (siehe oben).

Nach Beendigung der Untersuchung können Sie die Notfall-CD mittels Klick auf verlassen und das System herunterfahren (<Shutdown>) oder neu booten (<Reboot>).



4. Verwendung der Kaspersky Rescue Disk 2018

Sie finden ein ISO-Image der Kaspersky Rescue Disk 2018 auf dem PCSRV unter



<\\pcsrv.zam.kfa-juelich.de\public\Notfall-CDs\02-Kaspersky-Rescue-Disk-2018>

welches in regelmäßigen Abständen aktualisiert wird (was jedoch nicht das tagesaktuelle Update der Virensignaturen ersetzt).

Starten Sie das betroffene System mit der Kaspersky Rescue Disk, indem Sie aus dem ISO-Image einen bootfähigen USB-Stick erzeugen. Benutzen Sie hierzu geeignete Software von Drittanbietern; erfolgreich getestet wurde das Kaspersky-Image z.B. mit Rufus Portable sowie UNetbootin. Beachten Sie, dass der bisherige Inhalt des USB-Sticks gelöscht wird.



Download Rufus Portable:

<https://rufus.ie/de/>



Download UNetbootin:

<https://unetbootin.github.io/>



Alternativ können Sie das ISO-Image auch als CD/DVD brennen und von dieser das betroffene System neu starten. Nutzen Sie hierzu das in Ihrem Institut vorhandene Angebot an Software oder die in Windows 10 integrierte Funktion <Datenträgerabbild brennen>.



Wünschen Sie genauere Angaben zur Erzeugung des USB-Sticks, finden Sie diese hier:

<https://support.kaspersky.com/14226>

Im Startbildschirm der Rescue Disk wählen Sie zunächst die gewünschte Sprache mit den Tasten <↓> und <↑> und bestätigen mit <Return>. Nachfolgend wurde die englische Sprache gewählt.



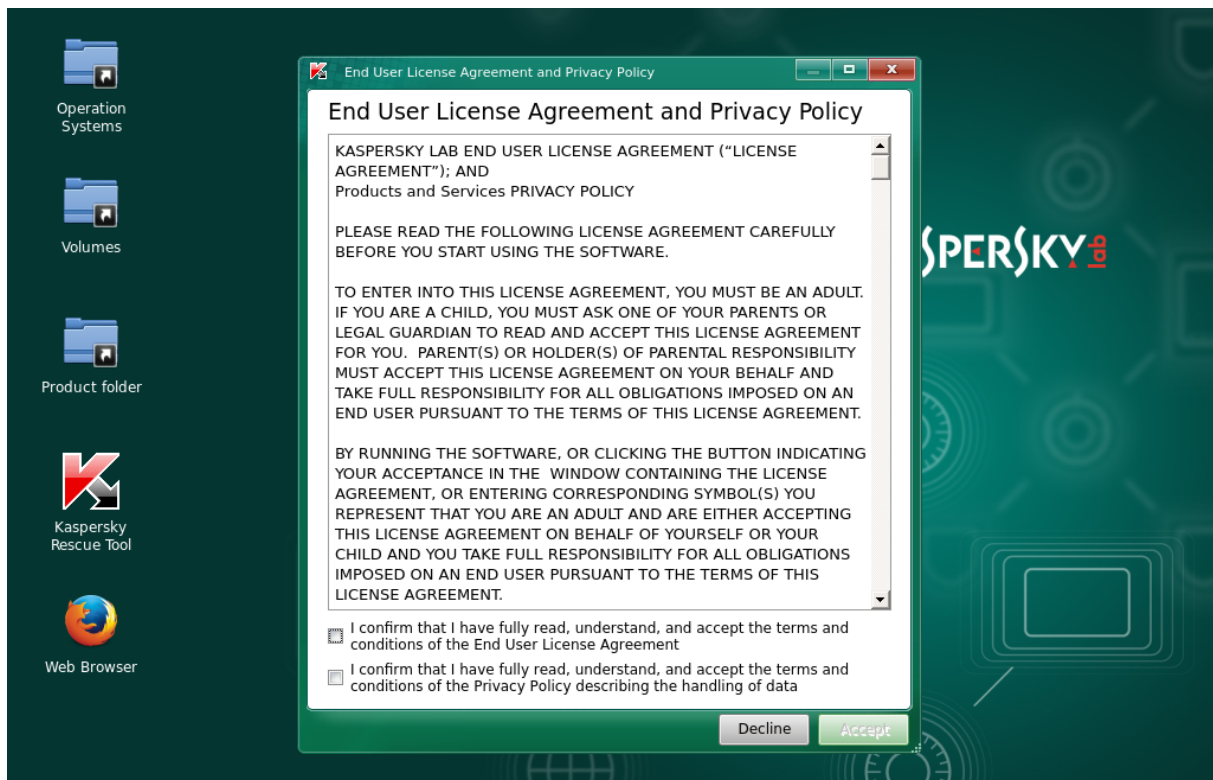
Starten Sie die eigentliche Rescue Disk, indem Sie <Kaspersky Rescue Disk. Graphic Mode> bestätigen.



Sollte es im weiteren Verlauf zu Problemen mit der Rescue Disk kommen, versuchen Sie einen Neustart mit der Auswahl <Kaspersky Rescue Disk. Limited graphic mode>. Die Bedienung ist in beiden Fällen identisch.

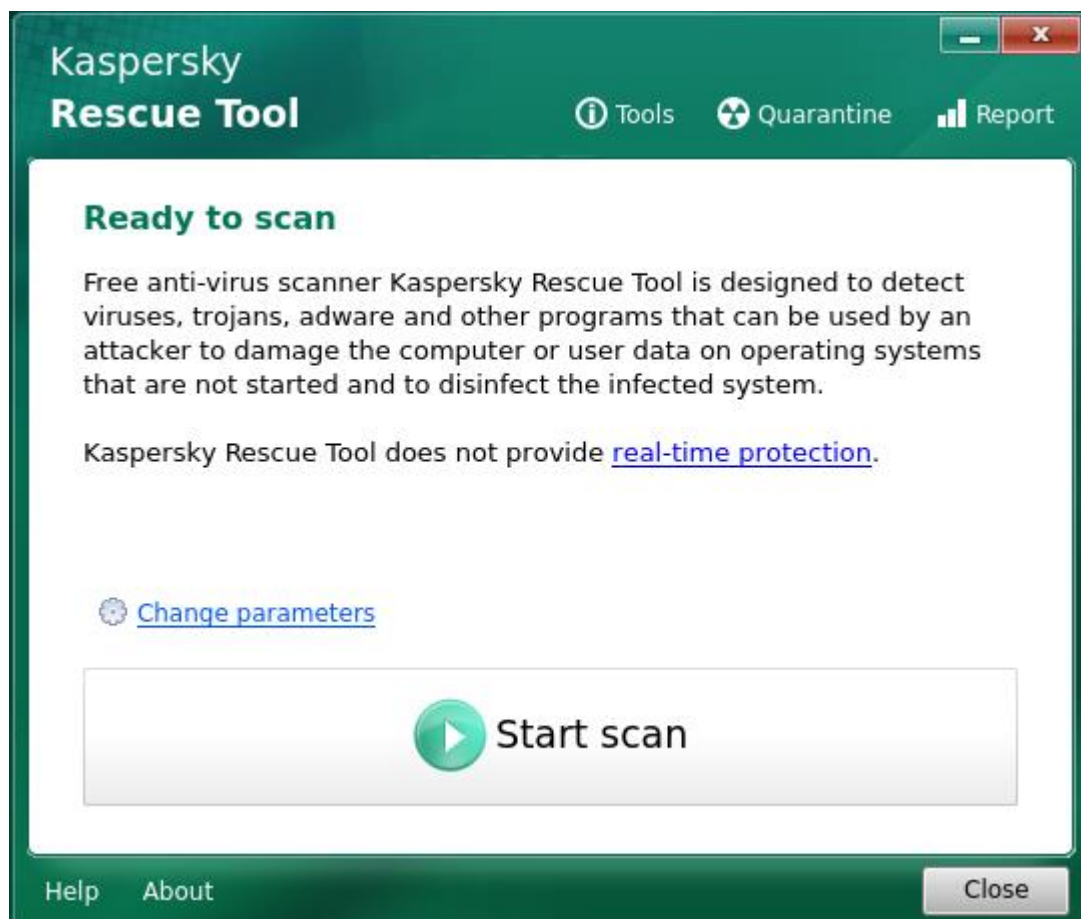
Die Rescue Disk wird nun gebootet, was insbesondere auf virtuellen Maschinen mit einer Wartezeit von einigen Minuten verbunden sein kann.

Es erscheint die Benutzeroberfläche der Rescue Disk 2018, und die Lizenzbedingungen werden angezeigt.

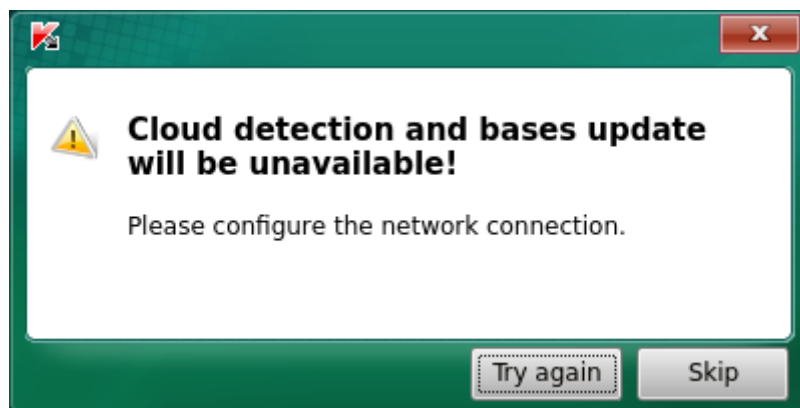


Aktivieren Sie beide Checkboxes im unteren Bereich und klicken Sie auf <Accept>.

Es erscheint das Fenster des Kaspersky Rescue Tool.



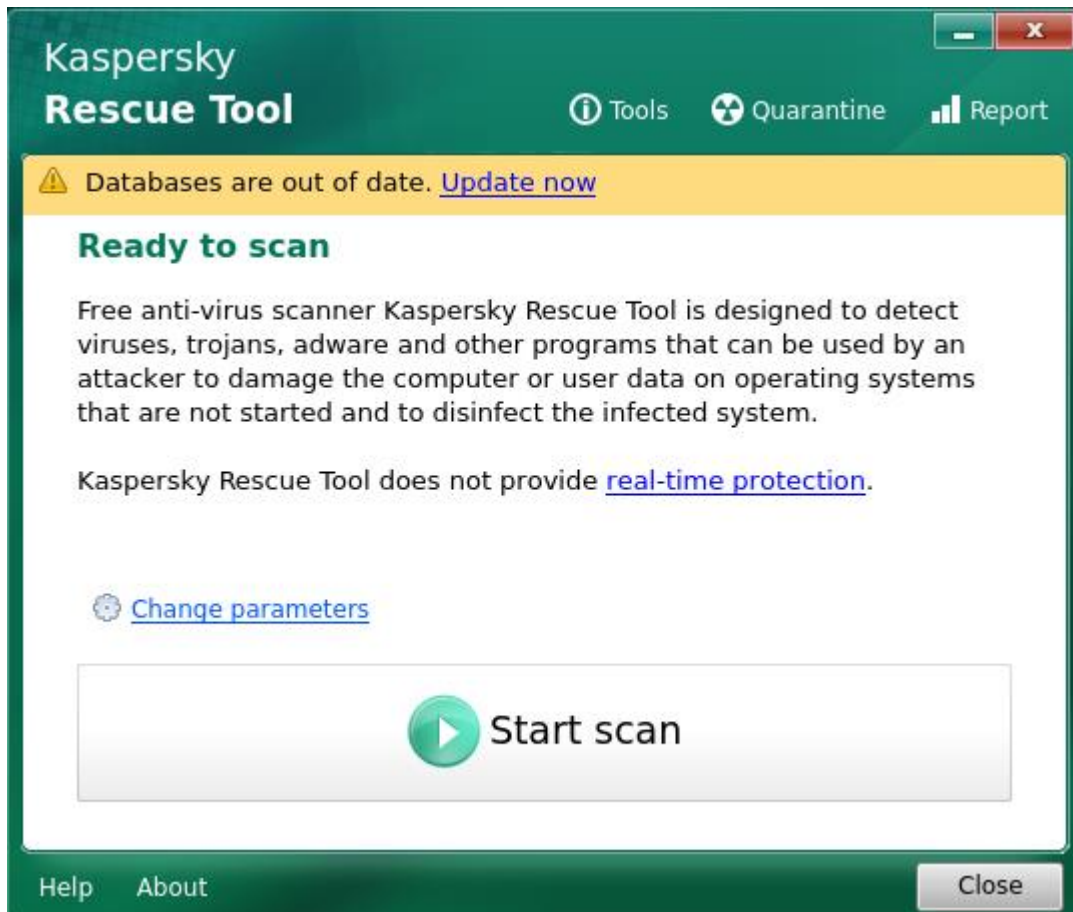
Erscheint dagegen die nachfolgende Meldung, besteht keine Verbindung zum öffentlichen Netz, weswegen kein Update der Virusmusterdefinitionen durchgeführt werden konnte.



Wurde der Update-Vorgang nicht korrekt ausgeführt, schauen Sie in Kapitel 6-Troubleshooting nach und starten Sie die Notfall-CD neu, damit die automatische Netzwerkerkennung erneut durchgeführt wird.

Fortgeschrittene Nutzer können über die Bordmittel der Benutzeroberfläche eine manuelle Konfiguration versuchen.

Je nach Alter der Virusmusterdefinitionen erhalten Sie im Hauptfenster des Kaspersky Rescue Tool eine gelb hinterlegte Meldung, dass die Virusdatenbank nicht mehr aktuell ist:



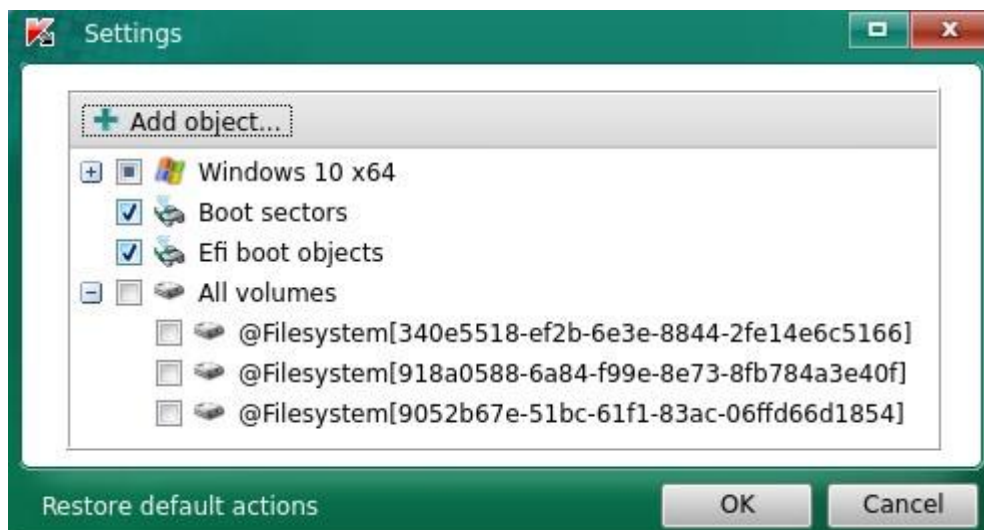
Klicken Sie in diesem Fall auf <Update now> (sollten Sie keine solche Meldung erhalten haben, überspringen Sie diesen Schritt einfach). Es wird ein Online-Update der Virusmusterdefinitionen durchgeführt, was natürlich nur bei einer aktiven Verbindung zum öffentlichen Netz funktionieren kann. Während des Update-Vorgangs erscheint ein Terminal-Fenster mit dem aktuellen Status:

```

Terminal
Prepare for updating...
Directory </mnt/KRD2018/Volumes/sda2/KRD2018_Data/Updates> was deleted successfully
Directory </mnt/KRD2018/Volumes/sda2/KRD2018_Data/Updates> was created successfully
Preparation is done
Downloading new bases...
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
   0      0     0     0     0     0      0     0  ---:--:--  ---:--:--  ---:--:--    0
100    154   100    154     0     0    154     0  0:00:01  ---:--:--  0:00:01    0
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
   0      0     0     0     0     0      0     0  ---:--:--  ---:--:--  ---:--:--    0
26   125M    26  33.4M     0     0  2856k     0  0:00:44  0:00:12  0:00:32  2688k
  
```

Nach erfolgreichem Abschluss kehrt die Notfall-CD wieder in die Hauptansicht zurück, Sie müssen dabei ggfs. den Lizenzvertrag erneut bestätigen.

Wählen Sie in der Hauptansicht <Change parameters> an. Erweitern Sie im nächsten Dialog alle Einträge mittels der <+>-Schaltflächen.



Im hier gezeigten Beispiel erkennt die Rescue Disk eine Windows 10-Installation („Windows 10 x64“) und drei Laufwerke bzw. Partitionen.

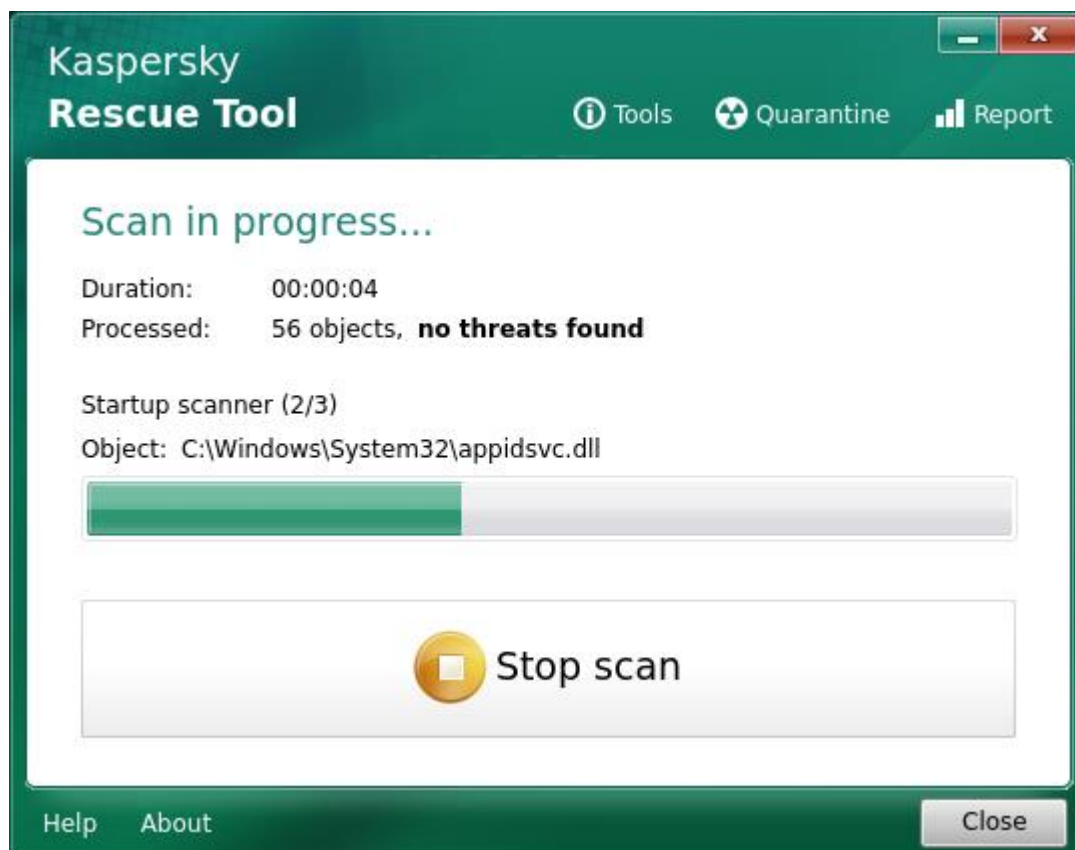
Sie können nun auswählen, welche Objekte einer Untersuchung unterzogen werden sollen: Hauptspeicher (Fileless objects), Autostart-Objekte (Startup objects), das Systemlaufwerk (System drive) und Bootsektoren (Boot sectors, Efi boot objects). Im unteren Bereich können Sie zusätzlich ganze Festplatten bzw. Partitionen zu- und abwählen. Je nach Systemkonfiguration werden evtl. nicht alle hier gezeigten Punkte aufgeführt.

Wählen Sie alle Einträge bzw. Partitionen aus, die befallen sein könnten und geprüft werden sollen. Sind Sie nicht sicher, welche dies sind, wählen Sie alle aufgeführten Einträge aus.



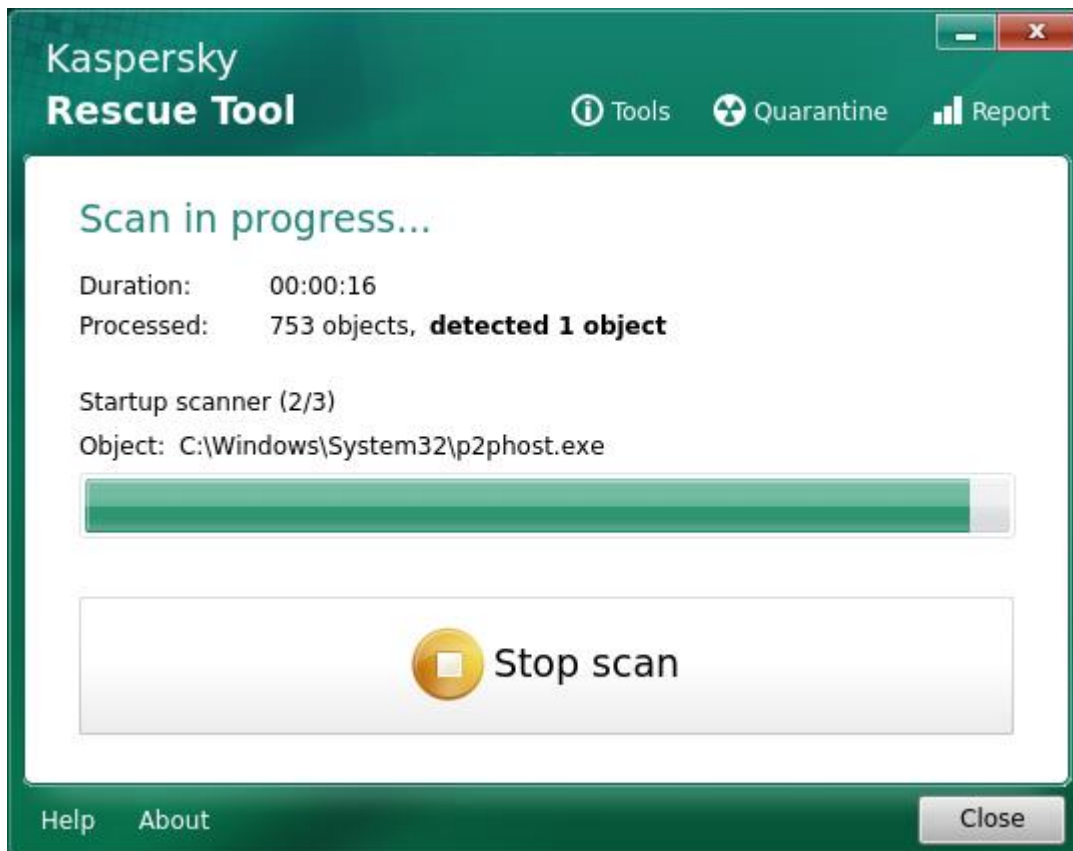
Bootfähige Partitionen sollten auf jeden Fall eingebunden werden. Wählen Sie auch die Einträge <Boot sectors> und <Efi boot objects>.

Bestätigen Sie Ihre Auswahl mit <OK>. Zurück in der Hauptansicht des Kaspersky Rescue Tool können Sie die eigentliche Untersuchung nun mit <Start Scan> beginnen. Während der Untersuchung sieht der Bildschirm wie folgt aus:

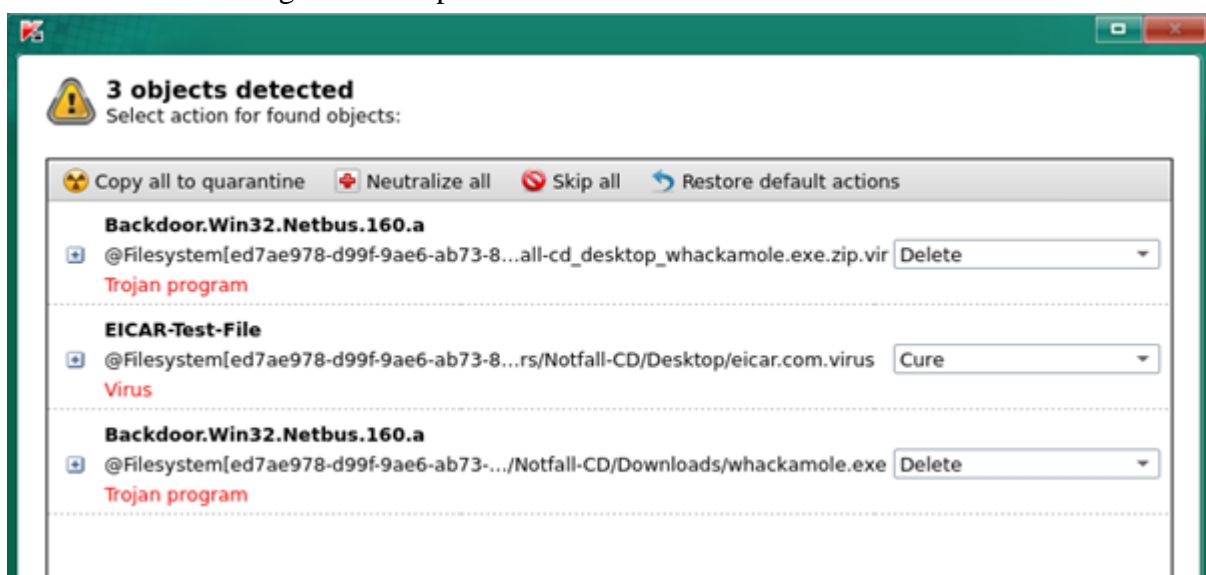


Mittel <Stop scan> kann die Untersuchung vorzeitig beendet werden.

Der Hinweis **no threats found** zeigt an, dass bislang keine verdächtigen Dateien gefunden wurden; andernfalls ist an dieser Stelle die Meldung **detected x object(s)** zu finden:



Nach Abschluss der Untersuchung wird eine Zusammenfassung angezeigt, sofern verdächtige Elemente gefunden wurden. Wurden solche nicht gefunden, kehrt das Kaspersky Rescue Tool ohne weitere Meldung in die Hauptansicht zurück.



Im oben gezeigten Beispiel wurden drei Infektionen gefunden. Es wird jeweils die Bezeichnung ausgegeben, z.B. **Backdoor.Win32.Netbus.160.a**, gefolgt vom Dateinamen samt Pfadangabe und dem Typ der Malware, hier **Trojan program**.

Im Auswahlfeld hinter jedem Listeneintrag schlägt das Rescue Tool eine Aktion vor, wie mit der Infektion umgegangen wird. Es kommen in Frage:

<Skip>: Ignorieren, keine weitere Aktion.

<Cure>: Das Rescue Tool versucht, die Infektion aus der Datei zu entfernen, wobei diese intakt bleiben soll.

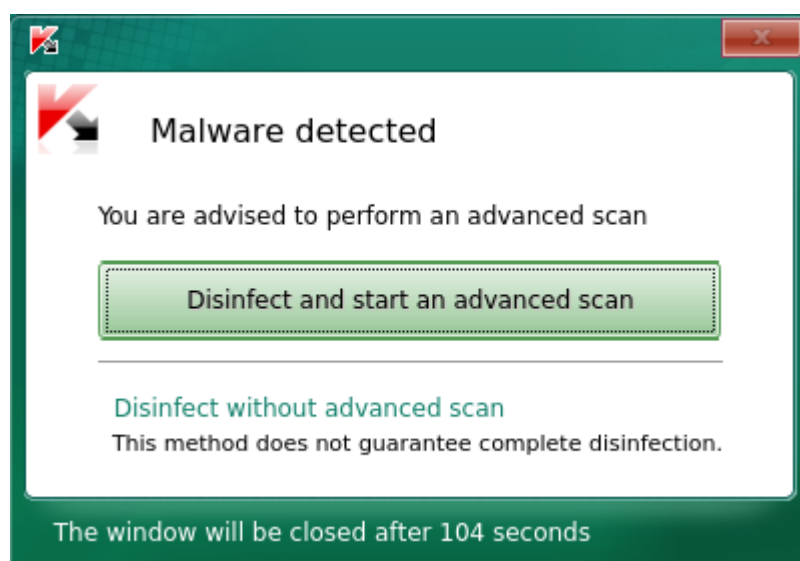
<Delete>: Die infizierte Datei wird gelöscht.

<Copy to quarantine>: Die infizierte Datei wird in einen Quarantäne-Bereich verschoben, um bei zukünftigen Systemstarts nicht mehr aktiviert zu werden.

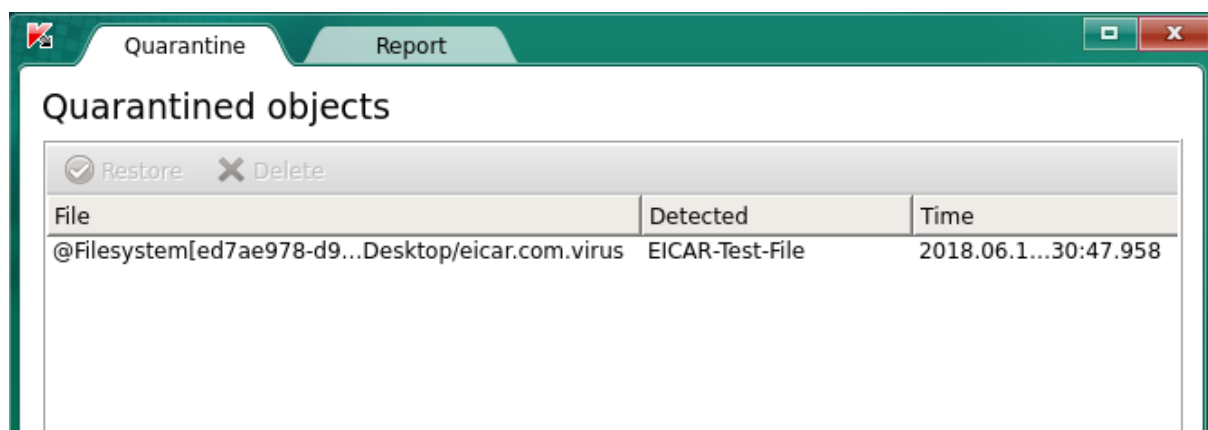
Der Benutzer kann nun für jeden Listeneintrag eine individuelle Aktion einstellen. Andernfalls kann mit den Schaltflächen im oberen Bereich auch eine einheitliche Aktion für alle Listeneinträge gewählt werden: **<Copy all to quarantine>** für den Quarantäne-Bereich, **<Neutralize all>** für Heilung/Löschung (je nachdem, ob Heilung möglich) und **<Skip all>** zum Ignorieren. Mittels **<Restore default actions>** können die vom Rescue Tool vorgeschlagenen Aktionen wiederhergestellt werden.

Bestätigen Sie Ihre Auswahl mit **<Continue>**.

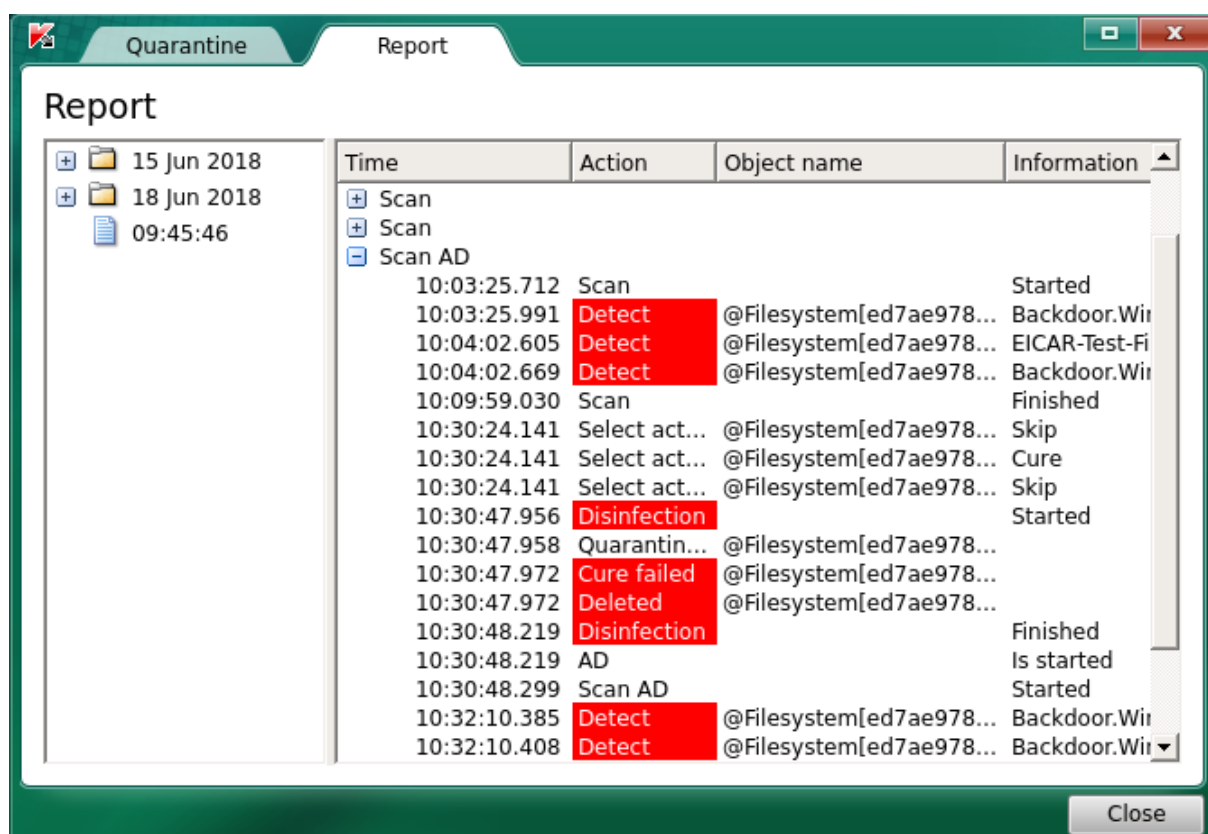
Abhängig von den gefundenen Bedrohungen schlägt die Notfall-CD vor, einen intensiveren, deutlich zeitaufwändigeren Scanvorgang durchzuführen. Wählen Sie zu dessen Durchführung **<Disinfect and start an advanced scan>**, was empfohlen wird; möchten Sie diesen dagegen nicht durchführen, können Sie diesen Schritt mit **<Disinfect without advanced scan>** überspringen.




Wurden die gewählten Aktionen durchgeführt, kehrt die Notfall-CD in die Hauptansicht zurück. Mittels Klick auf <Quarantine> können Sie eine Übersicht der Dateien im Quarantäne-Bereich aufrufen:



Mittels Klick auf <Report> können Sie eine Übersicht aller Scan-Vorgänge aufrufen. Erweitern Sie den Eintrag eines Vorgangs mittels der Schaltfläche <+>, um weitere Informationen anzeigen zu lassen. Nun können Sie sehen, welche Aktionen die Notfall-CD durchgeführt hat und ob sie erfolgreich verlaufen sind.



Im Beispiel oben ist beim Zeitindex 10:30:47.972 der Versuch einer Heilung fehlgeschlagen, weswegen die Datei schließlich gelöscht wurde.

Um die Nutzung der Notfall-CD zu beenden, klicken Sie auf  und wählen Sie <Leave>. Wählen Sie anschließend zwischen <Restart> für einen Neustart und <Shut Down> für das Ausschalten der Maschine.

5. Verwendung der Avira Antivir Rescue System 18

Sie finden ein ISO-Image der Avira Antivir Rescue System 18 auf dem PCSRV unter



[\\pcsrv.zam.kfa-juelich.de\public\Notfall-CDs\03-Avira-Antivir](https://pcsrv.zam.kfa-juelich.de/public/Notfall-CDs/03-Avira-Antivir)

welches in regelmäßigen Abständen aktualisiert wird (was jedoch nicht das tagesaktuelle Update der Virensignaturen ersetzt).



Auf EFI/UEFI-Systemen ist die Avira Antivir je nach Hardwarekonfiguration nur dann lauffähig, wenn Sie im System Setup <Secure Boot> deaktivieren.

Starten Sie das betroffene System mit der Avira Antivir, indem Sie aus dem ISO-Image einen bootfähigen USB-Stick erzeugen. Benutzen Sie hierzu geeignete Software von Drittanbietern; erfolgreich getestet wurde das Avira-Image z.B. mit Rufus Portable sowie UNetbootin. Beachten Sie, dass der bisherige Inhalt des USB-Sticks gelöscht wird.



Download Rufus Portable:

<https://rufus.ie/de/>



Download UNetbootin:

<https://unetbootin.github.io/>

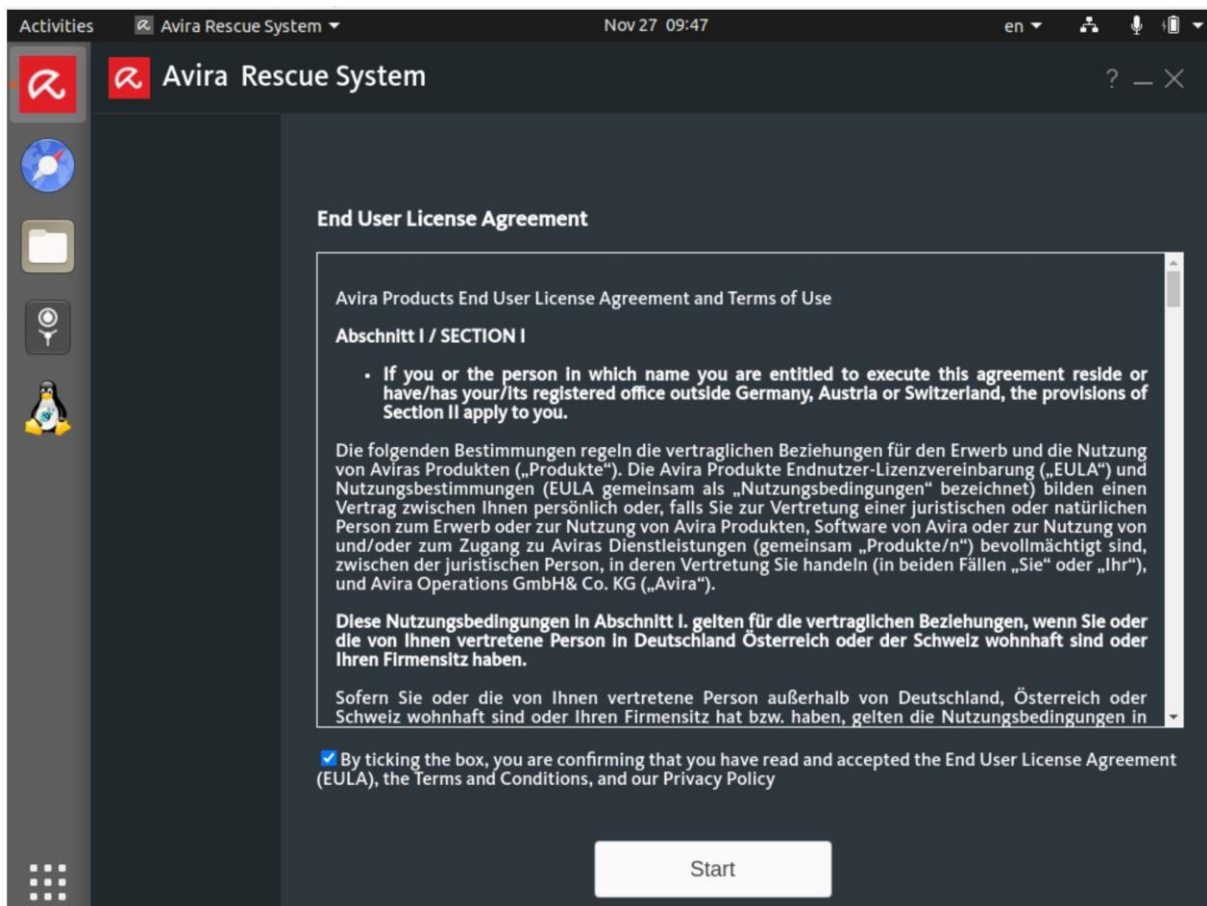


Alternativ können Sie das ISO-Image auch als DVD brennen und von dieser das betroffene System neu starten. Nutzen Sie hierzu das in Ihrem Institut vorhandene Angebot an Software oder die in Windows 10 integrierte Funktion <Datenträgerabbild brennen>.

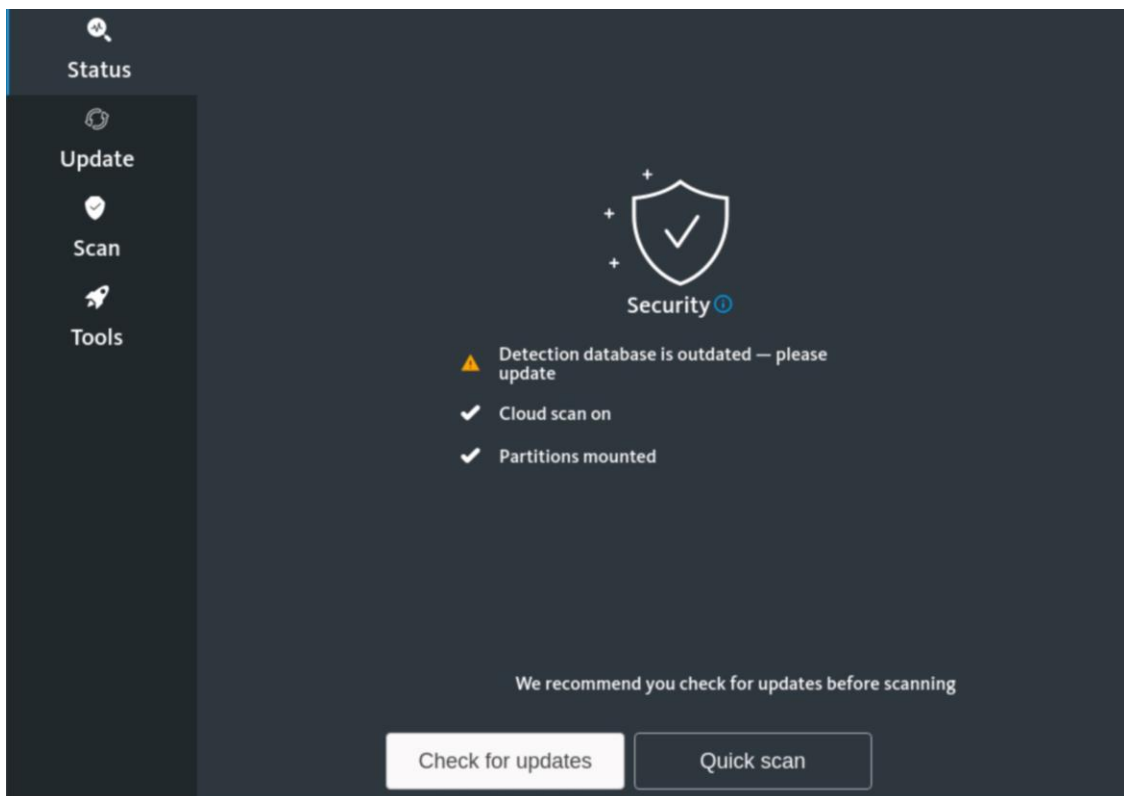
Zunächst erscheint der Bootbildschirm des Avira Rescue System. Wählen Sie die gewünschte Sprache mit den Tasten <↓> und <↑> und bestätigen Sie mit <Return>. Nachfolgend wurde die englische Sprache gewählt.



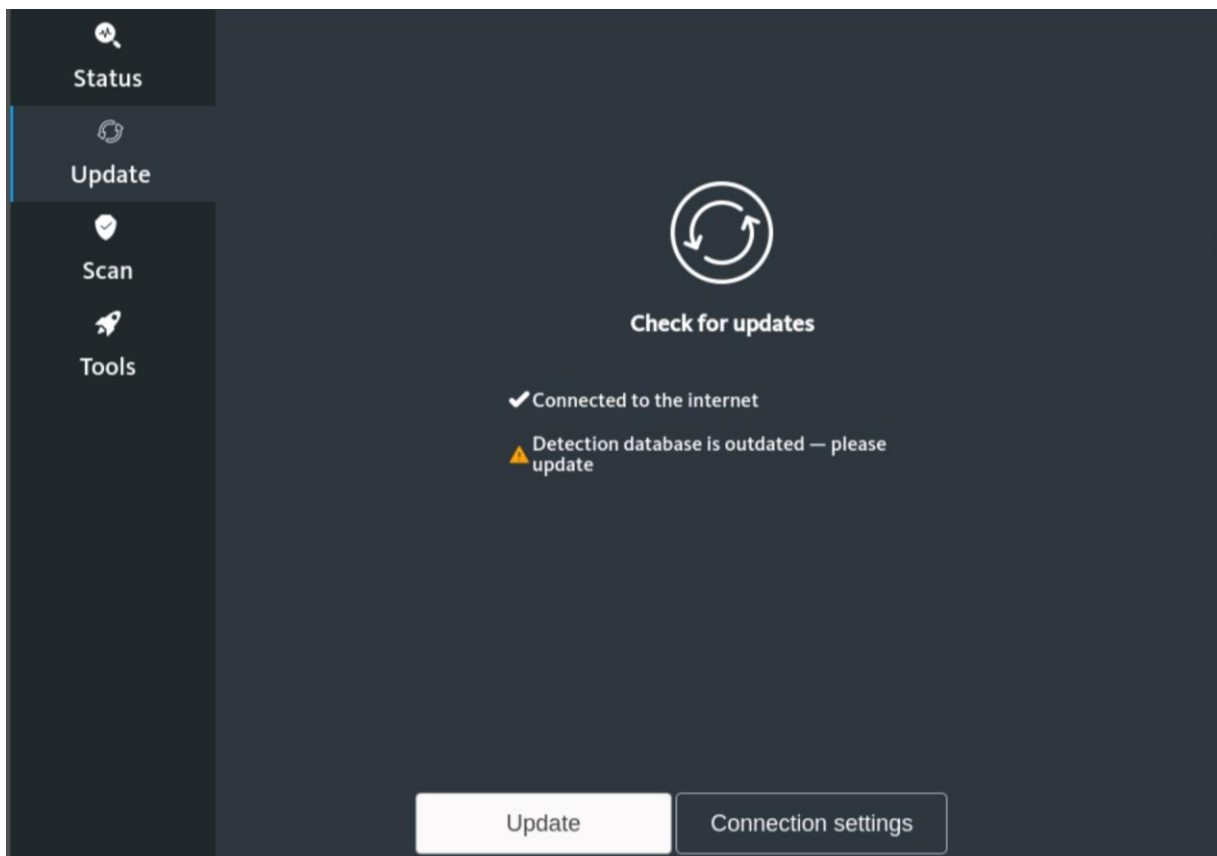
Nach dem Bootvorgang wird zunächst der Lizenzvertrag angezeigt.



Aktivieren Sie die Checkbox im unteren Bildbereich (<By ticking the box...>) und klicken Sie auf <Start>.

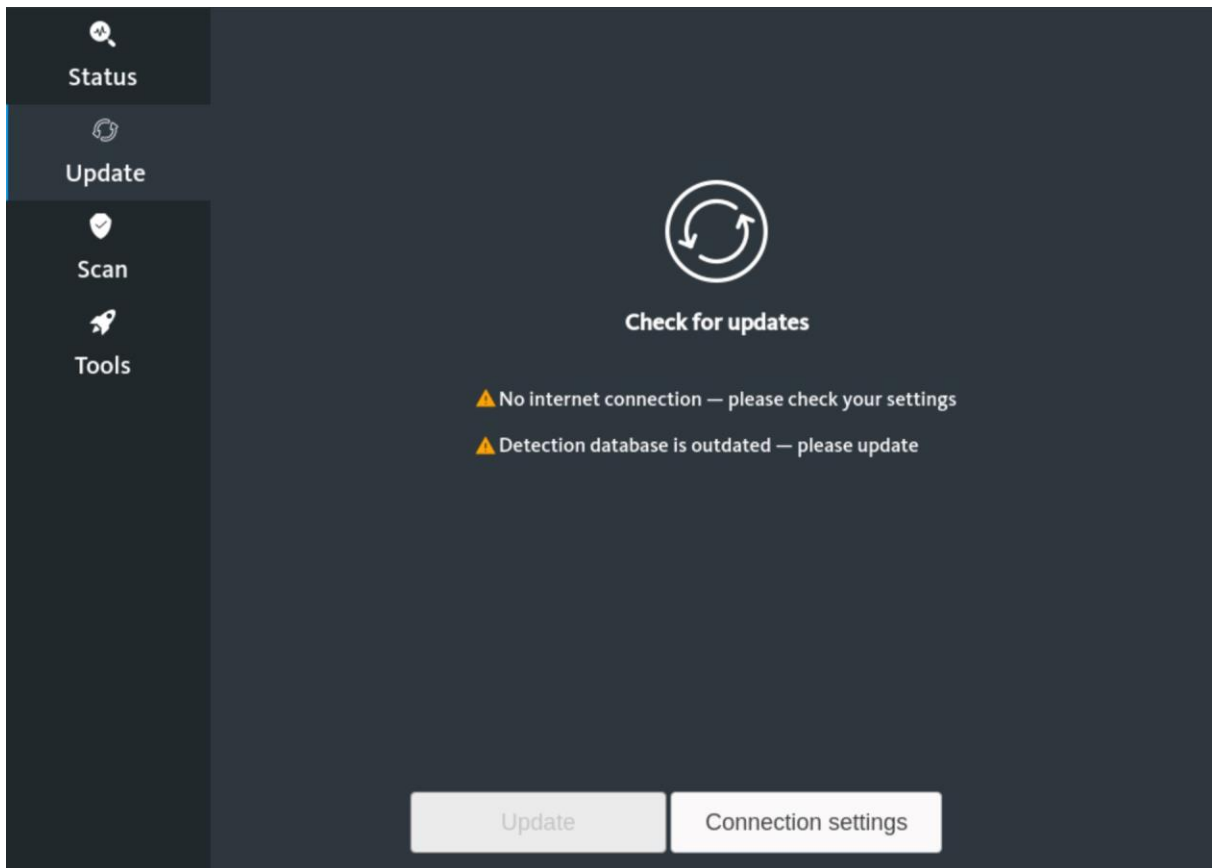


Sie werden darauf hingewiesen, dass die Virusmusterdefinitionen veraltet sind. Klicken Sie daher auf <Check for updates>, um diese zu aktualisieren. Eine Prüfung des Systems kann zwar auch ohne Update vorgenommen werden, diese Vorgehensweise wird jedoch nicht empfohlen.



Erscheint die oben gezeigte Meldung <✓ Connected to the internet>, so ist das System mit dem öffentlichen Netz verbunden und ein Update kann durchgeführt werden. Klicken Sie hierfür auf <Update>.

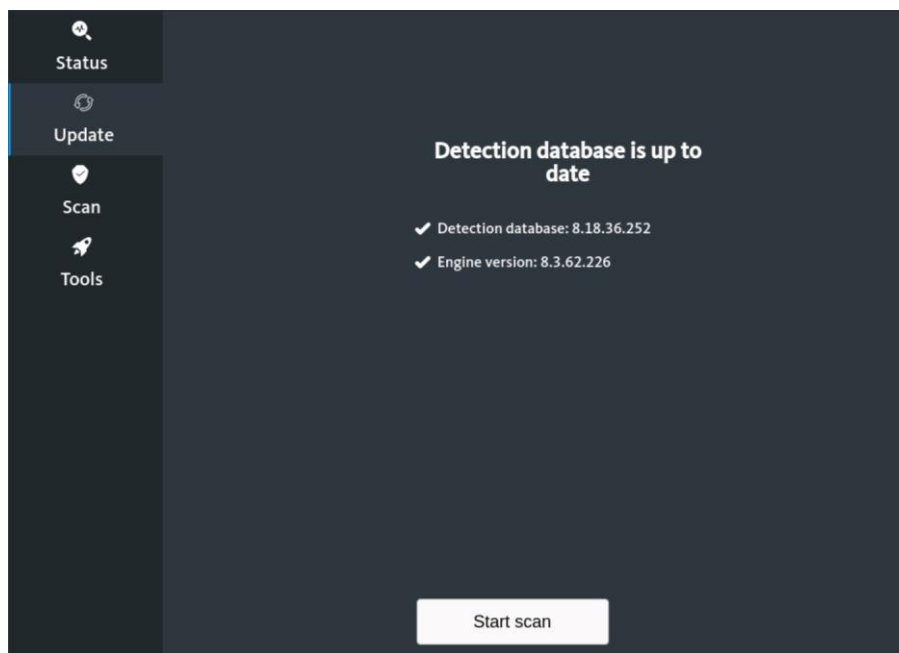
Erhalten Sie dagegen die nachfolgende Meldung <No internet connection...>, so ist das System nicht mit dem öffentlichen Netz verbunden und die Schaltfläche <Update> ist inaktiv. Beheben Sie das Problem und klicken Sie auf <Status>, um zum letzten Schritt zurückzukehren.



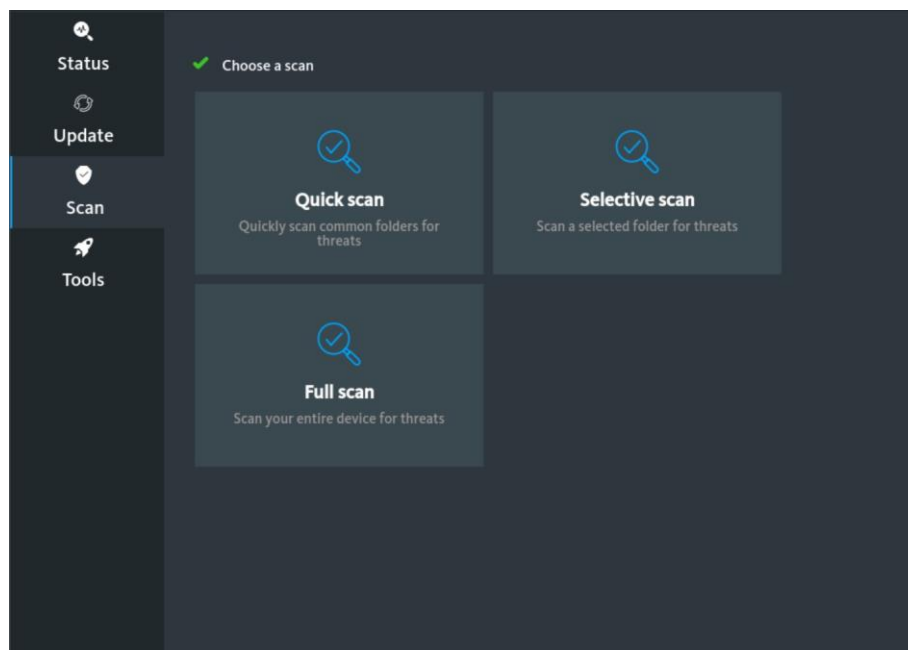
Schauen Sie ggfs. in Kapitel 6-Troubleshooting nach und starten Sie die Notfall-CD neu, damit die automatische Netzwerkerkennung erneut durchgeführt wird.

Fortgeschrittene Nutzer können über <Connection settings> eine manuelle Konfiguration der Netzwerkverbindungen versuchen.

Nach dem Klick auf <Update> wird dieses im Hintergrund ausgeführt, ohne dass das Avira Rescue System hierüber eine gesonderte Meldung ausgibt. Nach einer Weile informiert der folgende Bildschirm über den erfolgreichen Abschluss:

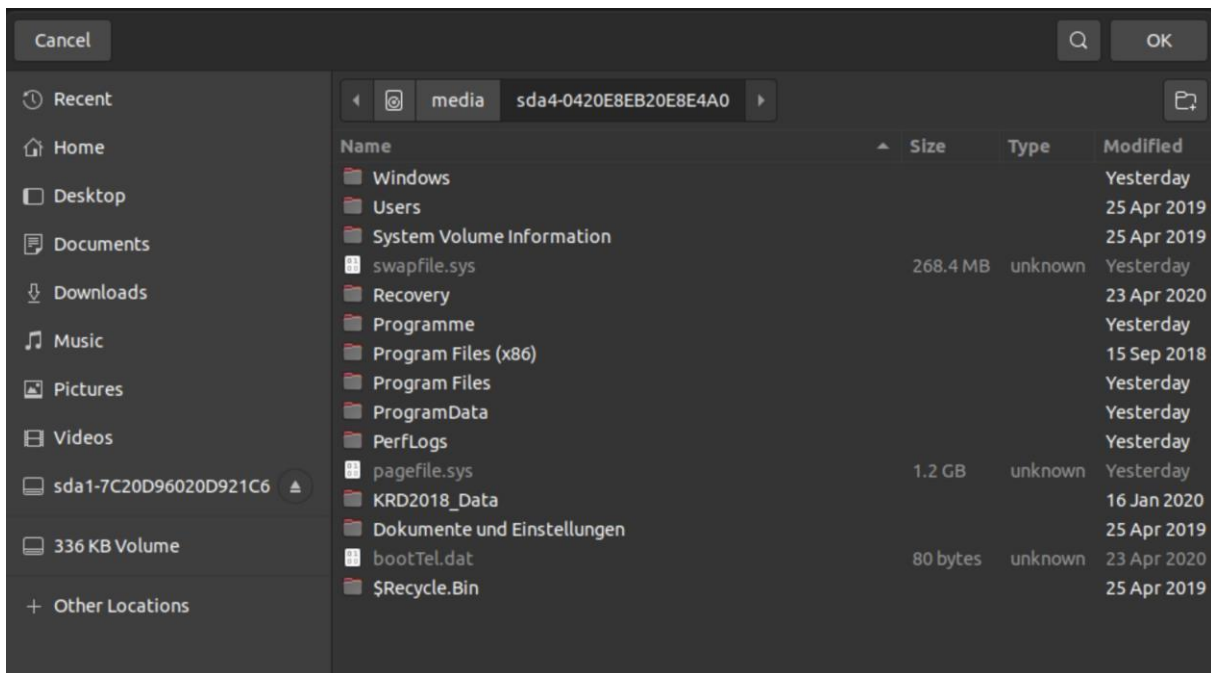


Klicken Sie auf <Start scan>.



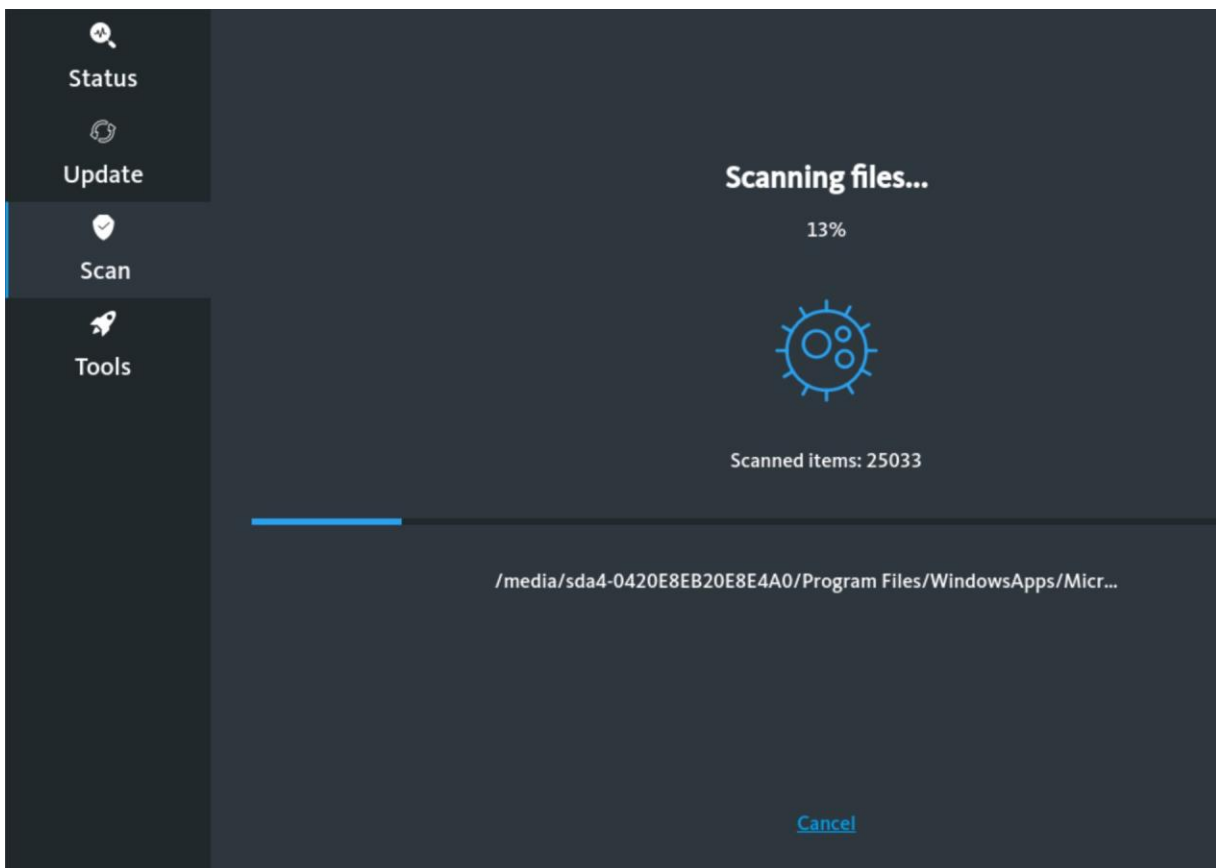
Wählen Sie nun zwischen einer vollständigen Überprüfung des Systems (<Full scan>) oder einer auf bestimmte Ordner beschränkten Prüfung (<Selective scan>). Letztere sollte nur verwendet werden, wenn die Bedrohung bereits vorab auf bestimmte Verzeichnisse eingegrenzt werden konnte. Ist dies nicht der Fall, wählen Sie den vollständigen Scan.

Haben Sie <Selective scan> gewählt, sehen Sie nun eine Explorer-Ansicht, deren Verzeichnisbaum der Struktur von Linux-Systemen entspricht:

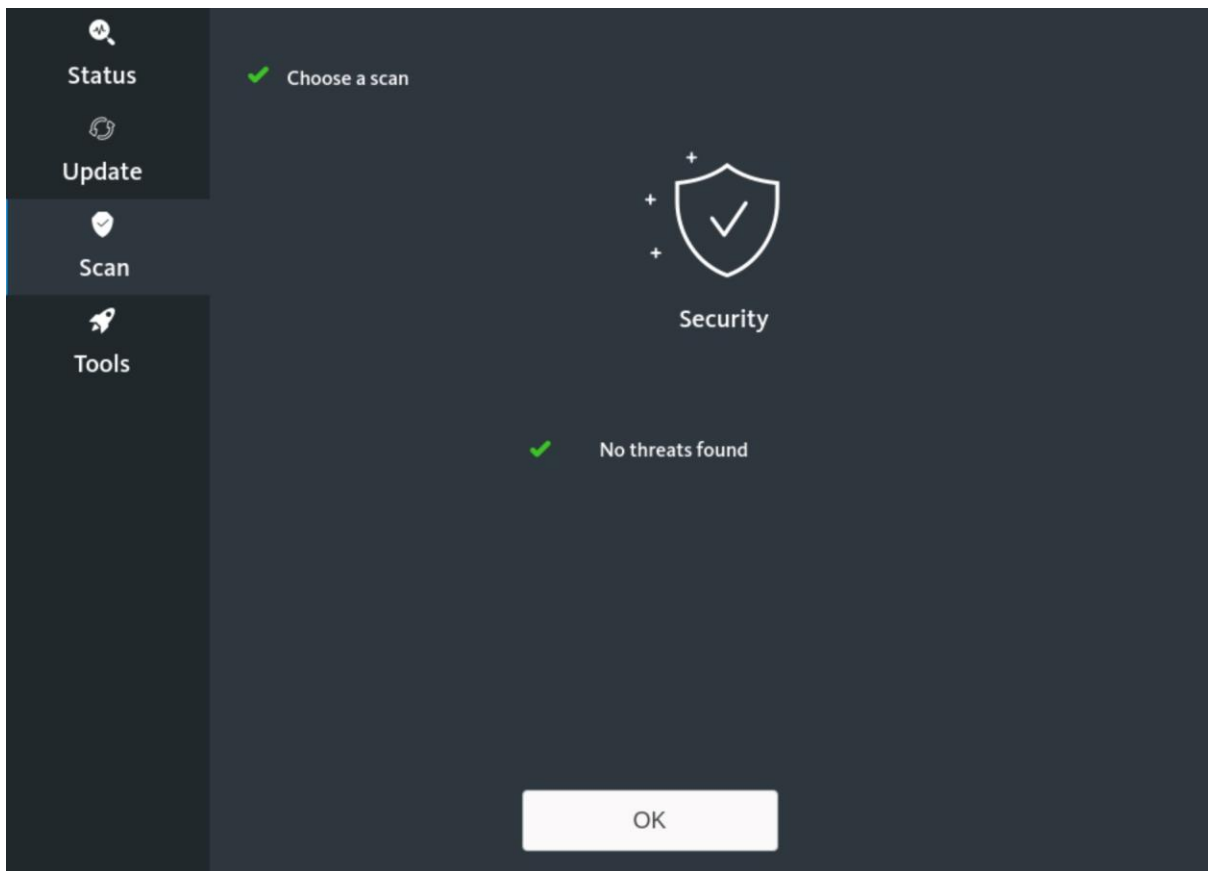


Suchen Sie die zu prüfenden Ordner bzw. Laufwerke und markieren Sie diese. Mittels der <Strg>-Taste können Sie mehrere Einträge der aktuellen Ansicht markieren. Nach einem Klick auf <OK> beginnt die Überprüfung.

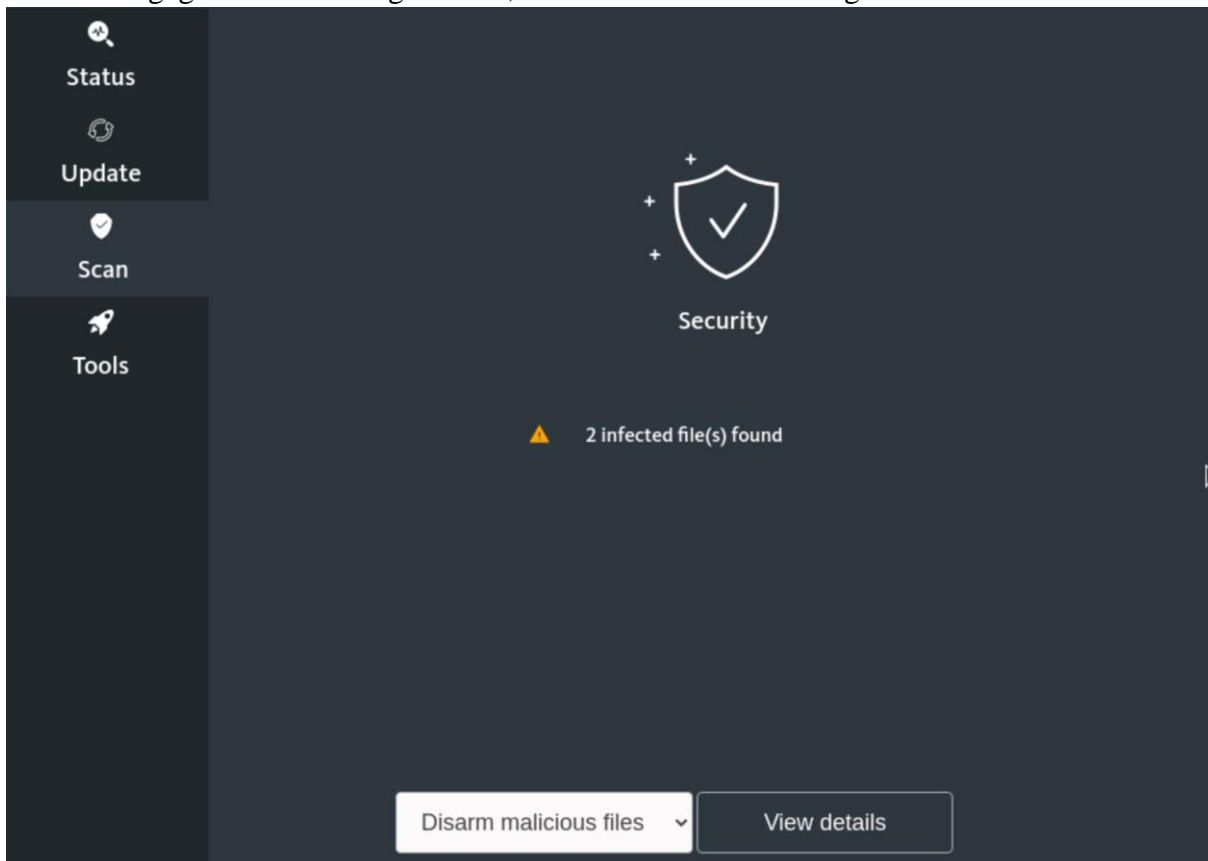
Haben Sie dagegen die vollständige Überprüfung gewählt, beginnt diese sofort ohne weitere Meldung. Während der Prüfung sieht der Bildschirm wie folgt aus, mittels <Cancel> kann sie unterbrochen werden.



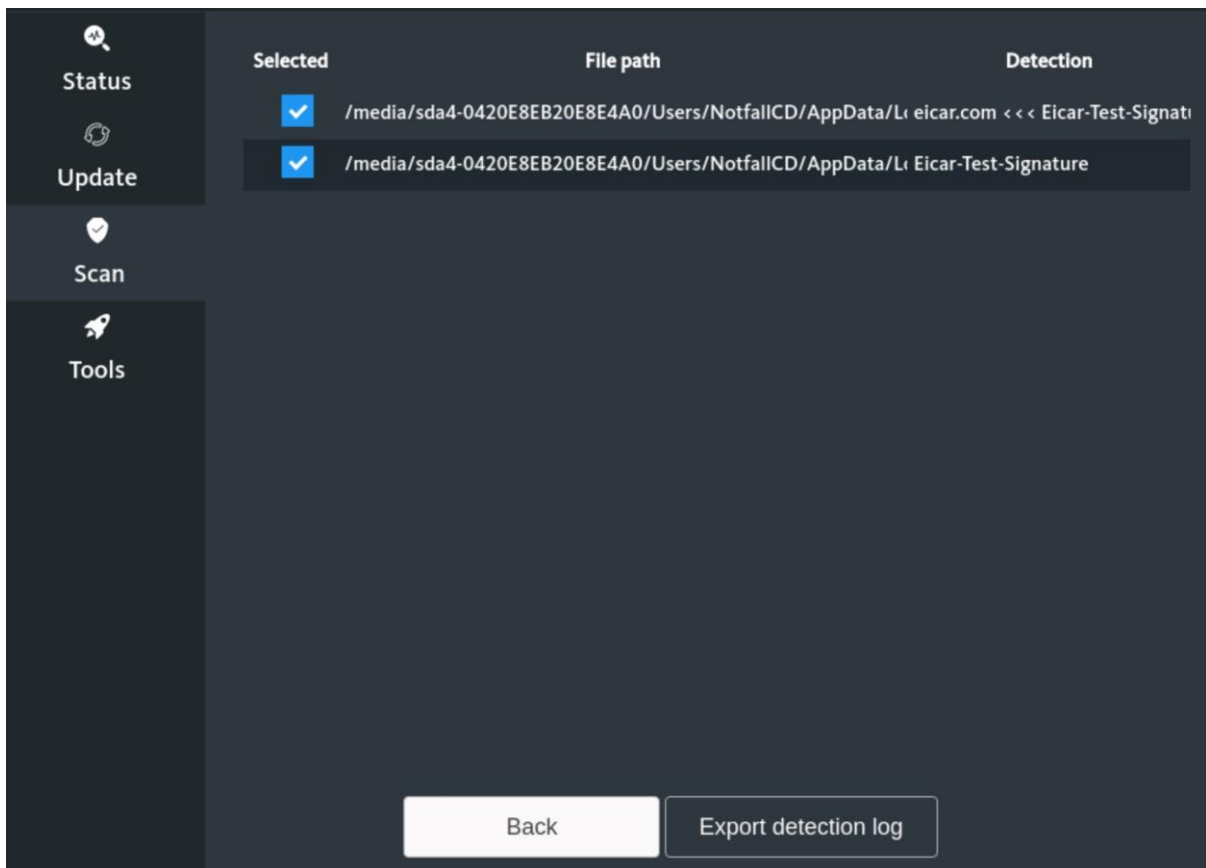
Nach Abschluss der Prüfung erhalten Sie folgende Meldung, wenn keine Infektionen gefunden wurden. Mit einem Klick auf <OK> gelangen Sie zurück in die Hauptansicht der Rubrik <Scan>.



Wurden dagegen Infektionen gefunden, erhalten Sie eine Meldung wie diese:



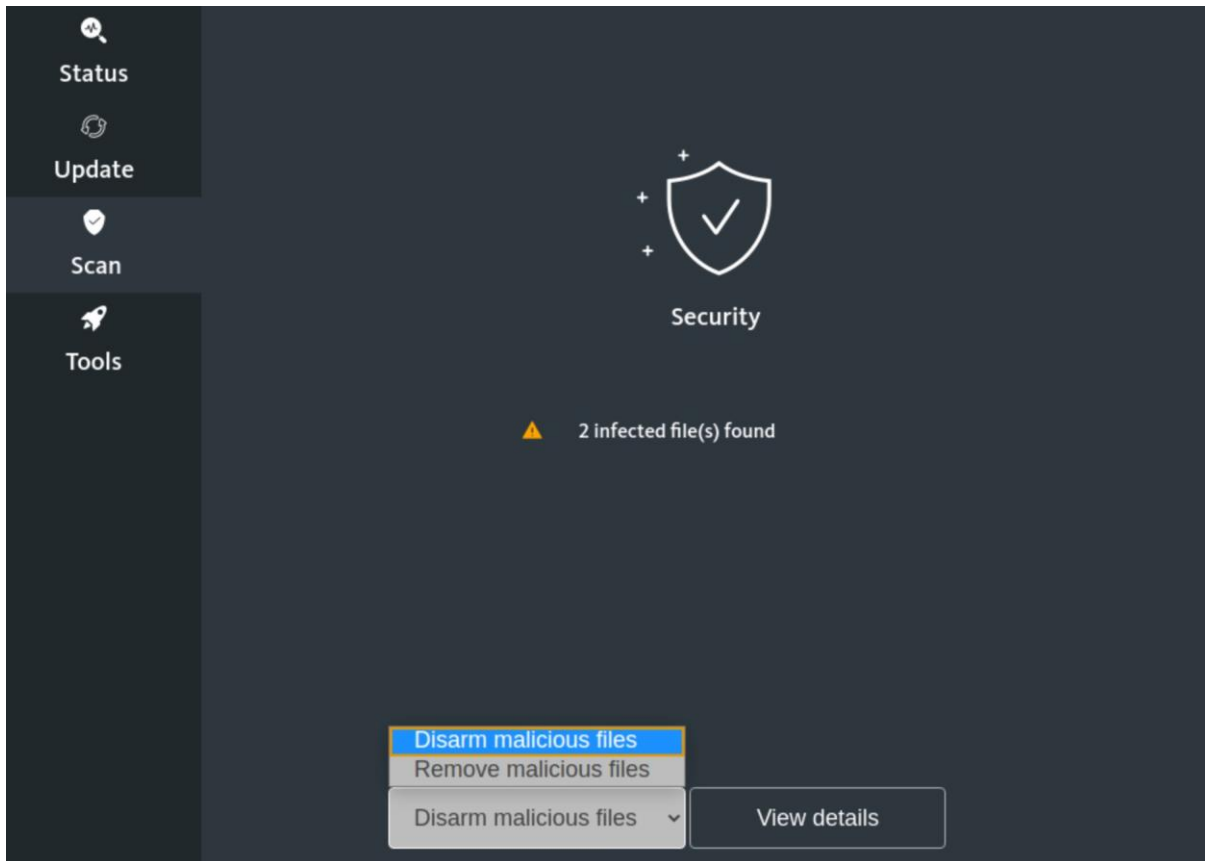
Per Klick auf <View details> erhalten Sie genauere Angaben zu den gefundenen Objekten.



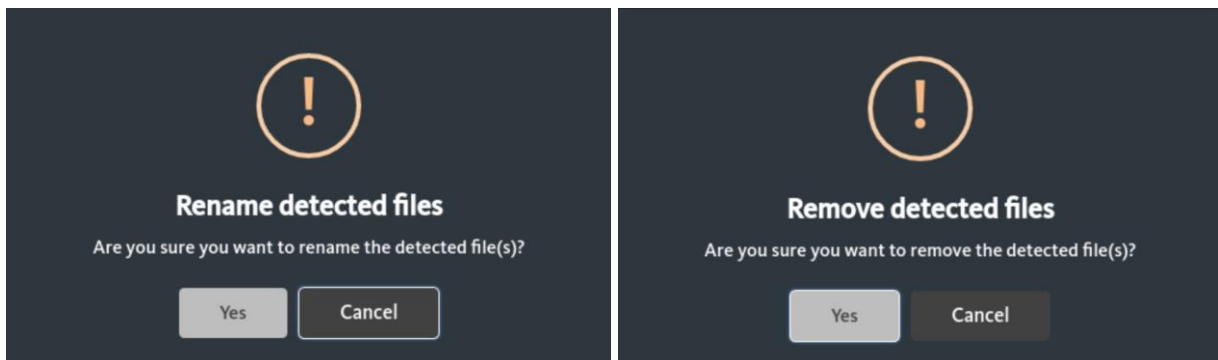
Wenn gewünscht, können Sie die Angaben per Klick auf <Export detection log> auf dem System oder den angeschlossenen Datenträgern speichern. Es erscheint wiederum eine Explorer-Ansicht, in der Sie den Speicherort wählen und <OK> klicken.

Wählen Sie <Back>, um zurück zur letzten Ansicht zu kommen. Klicken Sie auf <Disarm malicious files>, um die beiden Optionen anzeigen zu lassen, was mit den gefundenen Infektionen geschehen soll:

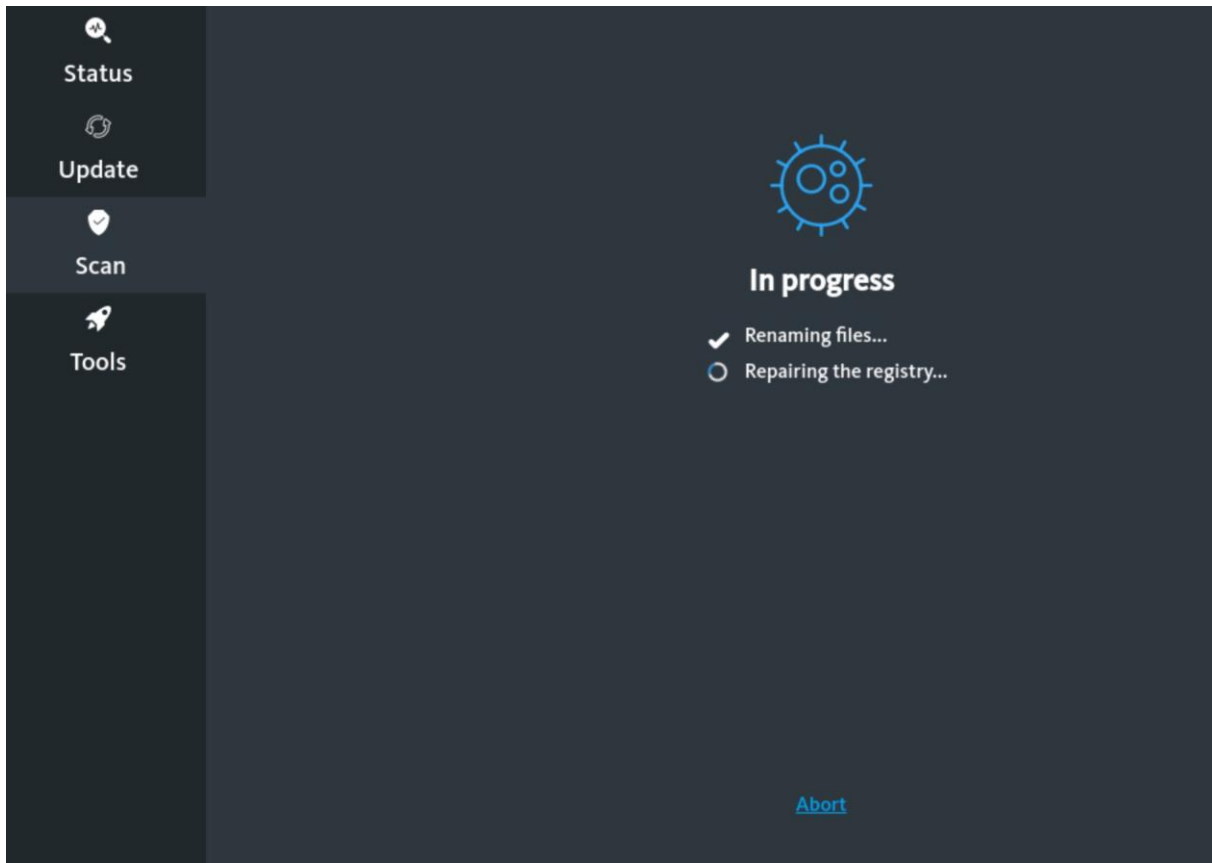
- Disarm malicious files: Die infizierten Dateien werden nicht gelöscht, sondern nur umbenannt, damit sie beim nächsten Systemstart nicht mehr geladen werden. Dies ist bei Dateien sinnvoll, die noch benötigt werden (könnten).
- Remove malicious files: Die infizierten Dateien werden gelöscht. Wählen Sie diese Option nur bei Sicherheit, dass die Dateien nicht mehr benötigt werden.



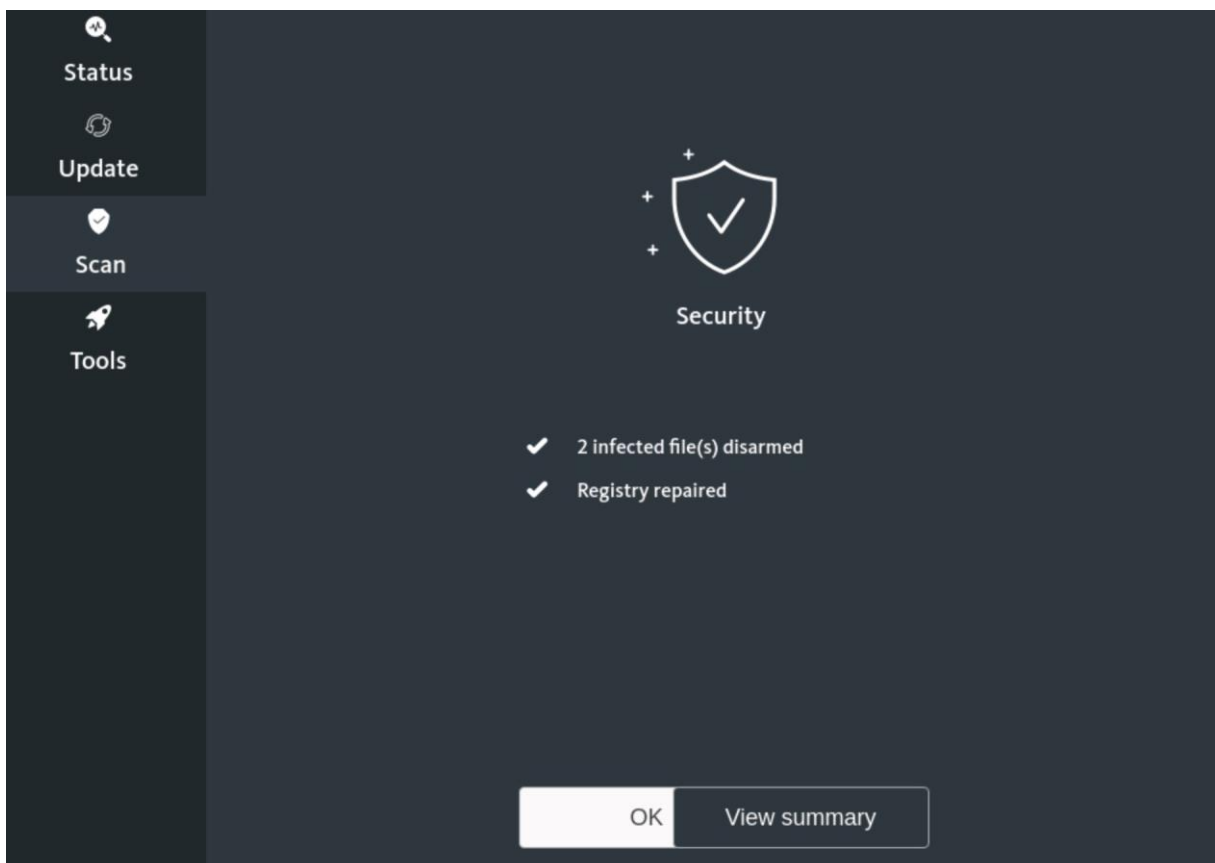
Klicken Sie Ihre Wahl an. In beiden Fällen werden Sie noch aufgefordert, die Aktion zu bestätigen:



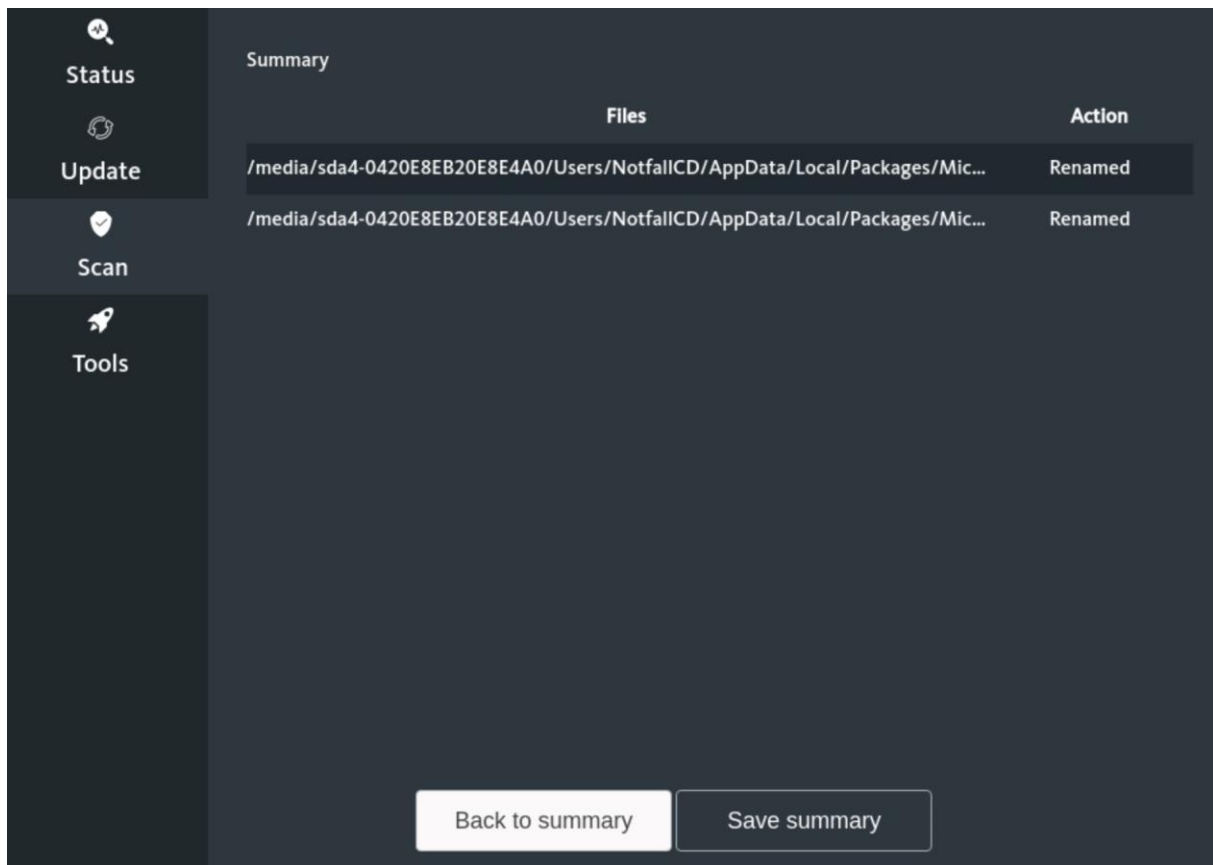
Nach dem Klick auf <Yes> wird die Aktion ausgeführt. Währenddessen sehen Sie folgenden Bildschirm:



Nach erfolgreichem Abschluss sehen Sie diese Meldung:




Mittels <View summary> können Sie sich eine Zusammenfassung anzeigen lassen, die der bereits bekannten Ansicht der gefundenen Infektionen entspricht:



Mittels <Save summary> können Sie auch diese Informationen auf dem System abspeichern, wie dies oben bereits erläutert wurde.

Per <Back to summary> gelangen Sie zurück zur letzten Ansicht. Klicken Sie dort auf <OK>, um wieder zur Hauptansicht der Rubrik <Scan> zu gelangen.

Führen Sie nun nach Bedarf weitere Scans durch, indem Sie die gezeigten Schritte wiederholen.

Möchten Sie die Nutzung der Avira Rescue System beenden, klicken Sie oben rechts auf das Symbol  und wählen Sie <Power Off / Log Out>, dann <Power Off...> und schließlich <Power Off> (System abschalten) oder <Restart> (Neustart des Systems).

6. Troubleshooting

Sollte die Internet-Verbindung unter den Notfall-CDs nicht korrekt funktionieren, überprüfen Sie bitte die nachfolgenden Punkte (deren aufgeführte Reihenfolge nicht verbindlich ist, hier muss vielmehr situationsabhängig entschieden werden):

- Der verwendete Netzwerkadapter muss richtig gewählt werden, die Notfall-CDs wählen den Adapter zunächst automatisch. Eventuell werden einige WLAN-Adapter sowie USB-basierte Lösungen nicht korrekt erkannt; binden Sie das betroffene Gerät daher für die Dauer des Update-Vorgangs mittels einer internen Netzwerkkarte über einen kabelgebundenen Anschluss an, sofern möglich.

Achten Sie bei fest integrierten Netzwerkadaptoren darauf, dass diese im BIOS bzw. UEFI aktiviert sind. Achten Sie bei nachgerüsteten Netzwerkkarten darauf, dass der verwendete Slot/Anschluss im BIOS bzw. UEFI aktiviert ist.

- Prüfen Sie, ob das System tatsächlich mit einem Datenanschluss mit Zugang zum öffentlichen Netz verbunden ist. Bei Experimentnetzen u.ä. ist dies i.d.R. nicht der Fall!
- Für die korrekte Funktion des Update-Vorgangs muss das betroffene System idealerweise seine Netzwerk-Konfiguration vom DHCP-Server beziehen (oder ansonsten manuell konfiguriert werden). Sollte das System aufgrund der Infektion für die JuNet-Nutzung gesperrt sein, ist ein Update-Vorgang daher nicht möglich. Halten Sie in diesem Fall Rücksprache mit der JuNet-Hotline unter der Durchwahl 6440.
- Beachten Sie, dass die Verwendung von KVM-Switches bei der Anwendung der Notfall-CDs zu Problemen mit der Bildschirmdarstellung führen kann. Binden Sie den PC ggfs. für die Dauer der Maßnahmen direkt an einen Monitor an.

Führen auch diese Maßnahmen nicht zum Erfolg, wenden Sie Sich an Ihren institutseigenen IT-Ansprechpartner, IT-Dienstleister oder die JuNet-Hotline 6440.

Ein Fortfahren mit der Nutzung der verschiedenen Notfall-CDs ist zwar auch ohne Update möglich, jedoch ist die Wahrscheinlichkeit beschränkt, dass eventuelle Infektionen mit Malware erkannt und beseitigt werden können.