FORSCHUNGSZENTRUM JÜLICH GmbH

Jülich Supercomputing Centre
D-52425 Jülich, Tel. (02461) 61-6402

Beratung Netzwerk, Tel. (02461) 61-6440

Technische Kurzinformation

FZJ-JSC-TKI-0411
Dr. Frank Mohr, JSC-KS

23.04.2025

Gebrauch der Notfall-CDs von Avast und Avira

Inhalt

1. Einleitung 1
2. Alternativen zu den Notfall-CDs 3
3. Verwendung des Avast Antivirus Rettungsmediums 4
4. Verwendung der Avira Antivir Rescue System 18 16
5. Troubleshooting 27

1. Einleitung

Mit den Lösungen Avast Antivirus Rettungsmedium und Avira Antivir Rescue System stehen den Mitarbeitern des Forschungszentrums Jülich (auch für den privaten Einsatz) zwei leistungsfähige Notfallmedien („Notfall-CDs“) zur Verfügung, um Windows- und auch Linux-Partitionen (nicht bei Avast) 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 beiden 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 5-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>).

Beide angebotenen Lösungen können keine verschlüsselten Partitionen untersuchen. 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 der anderen Lösung 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.

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 Trellix (ehemals 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 Trellix Stinger:
https://www.trellix.com/downloads/free-tools/stinger/

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 Virenscanner 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://learn.microsoft.com/de-de/defender-endpoint/safety-scanner-download?view=o365-worldwide

Ebenfalls von Microsoft stammt der Windows Defender Offline, der bei einer vermuteten Infektion eine Untersuchung auf Schadsoftware durchführen kann, und bereits in Windows 10/11 integriert ist. Auch dieser wird nur bei Bedarf ausgeführt, ersetzt also keinen Virenscanner.

Kurzanleitung Microsoft Windows Defender Offline:
https://learn.microsoft.com/de-de/defender-endpoint/microsoft-defender-offline

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

Download PC-Welt Rettungs-DVD:
https://www.pcwelt.de/article/1135824/pc-welt-notfall-dvd.html

3. Verwendung des Avast Antivirus Rettungsmediums

Sie finden ein ISO-Image des Avast Antivirus Rettungsmediums auf dem PCSRV unter

\\pcsrv.zam.kfa-juelich.de\public\Notfall-CDs\02-Avast-Antivirus

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

In diesem Verzeichnis liegen zwei ISO-Dateien: `rescuedisk_UEFI.iso` für Systeme mit UEFI (Unified Extensible Firmware Interface) und `rescuedisk_BIOS.iso` für Systeme mit BIOS (Basic Input/Output System). Wählen Sie die iso-Datei aus, die auf Ihr System zutrifft.

Wenn Sie unsicher sind, welcher Fall auf das zu untersuchende System zutrifft, so beginnen Sie bei Systemen ab Baujahr 2006 mit der UEFI-Variante, andernfalls mit der BIOS-Variante. Wenn sich Probleme bei der Ausführung ergeben (z.B. startet nicht oder Laufwerke werden nicht erkannt), so versuchen Sie die jeweils andere iso-Datei.

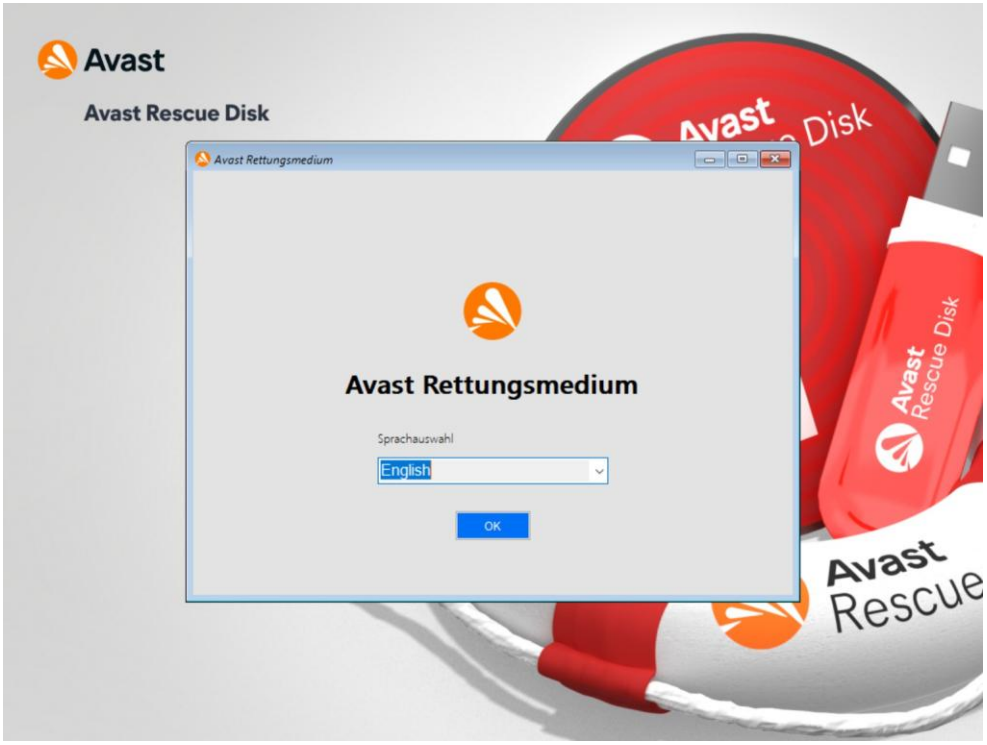
Ergeben sich daraufhin immer noch Probleme, so können Sie bei UEFI-Systemen noch versuchen, im UEFI-Menü `<Secure Boot>` zu deaktivieren und den UEFI-/BIOS-Modus anzupassen (`<Legacy>`).

Starten Sie das betroffene System mit dem Avast Rettungsmedium, indem Sie aus dem ISO-Image einen bootfähigen USB-Stick erzeugen. Benutzen Sie hierzu geeignete Software von Drittanbietern; erfolgreich getestet wurde das Avast-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>`.

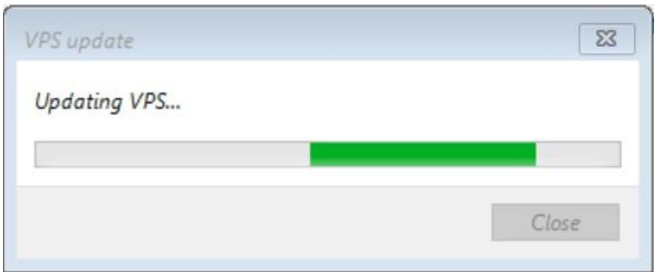
Nach einer kurzen Wartezeit erscheint zunächst die Abfrage, mit welcher Bildschirmsprache das Rettungsmedium ausgeführt werden soll. Wählen Sie die gewünschte Sprache aus und klicken Sie auf <OK>. Nachfolgend wurde die englische Sprache gewählt.



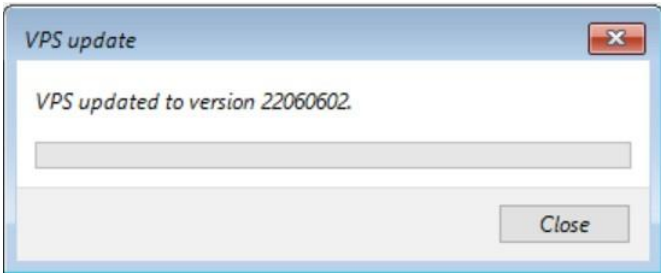
Es folgt der Startbildschirm des Avast Rettungsmediums.

Beginnen Sie mit einem Klick auf die Schaltfläche  (AvastPE Antivirus), um den Virenscanner aufzurufen.

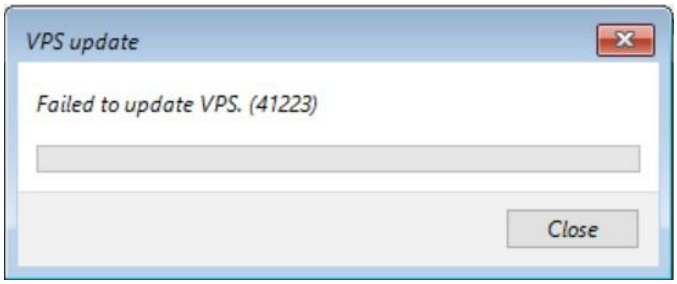
Führen Sie zunächst ein Update der Virusmusterdefinitionen durch, indem Sie auf `<Update VPS>` klicken. Während des Updatevorgangs, der mehrere Minuten dauern kann, sehen Sie diese Meldung:



Wurde das Update erfolgreich durchgeführt, erscheint die nachfolgende Meldung, die Sie mit `<Close>` bestätigen können.



Schlägt das Update dagegen fehl, sehen Sie folgende Meldung:



Der hier gezeigte Fehlercode (41223) bedeutet, dass der Avast-Updateserver nicht erreicht werden konnte. Das zu untersuchende System hat vermutlich keine Verbindung zum öffentlichen Netzwerk; beheben Sie das Problem und nehmen Sie nach Klick auf <Close> einen erneuten Versuch vor. Ziehen Sie ggfs. die Hinweise in Kapitel 5-Troubleshooting hinzu.

Eine Untersuchung ohne Update der Virusmusterdefinitionen ist zwar möglich, aber nur bedingt hilfreich.

Ist das System per WLAN mit dem Netzwerk verbunden, während Sie diese Fehlermeldung erhalten, so versuchen Sie, stattdessen eine kabelgebundene Verbindung herzustellen.

Erhalten Sie einen anderen Fehlercode als 41223, so können Sie diesen per Google-Suche in eine konkrete Fehlermeldung auflösen und versuchen, das Problem entsprechend zu beheben. Verwenden Sie z.B. den Suchbegriff Avast error code xxxxx

Sie befinden sich wieder im Startbildschirm des Virenscanners. Sie können nun entscheiden, ob alle im System gefundenen Festplatten(-partitionen) untersucht werden sollen (Klick auf <All hard disks>), oder ob Sie den Suchbereich eingrenzen wollen (Klick auf <Selected folders/disks>).

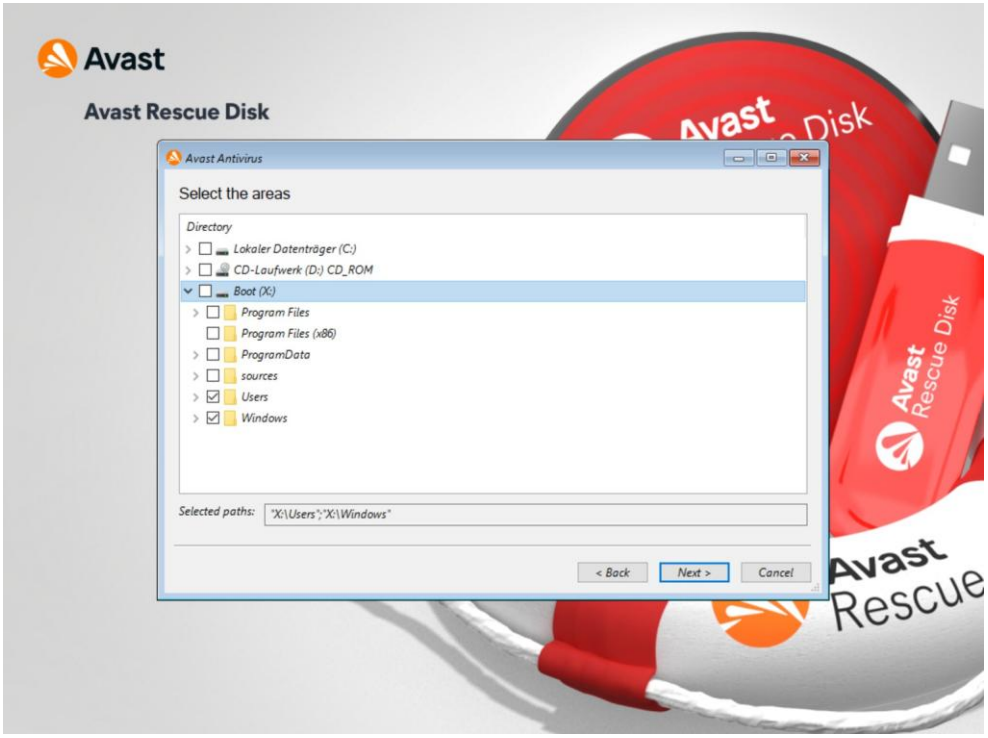
Wenn Sie unsicher sind, ob und in welcher Form die Eingrenzung des Suchbereichs sinnvoll ist, lassen Sie alle Partitionen untersuchen.

Bootfähige Partitionen sollten auf jeden Fall untersucht werden.

Aktivieren Sie auch die Option <scan all archives (takes more time)>, um komprimierte Dateien vollständig untersuchen zu lassen.

Klicken Sie auf <Next> bzw. <Select> (wenn Sie eine eingegrenzte Untersuchung gewählt haben).

Im Fall einer eingegrenzten Untersuchung erhalten Sie nun folgendes Fenster, in dem Sie die Auswahl vornehmen können:

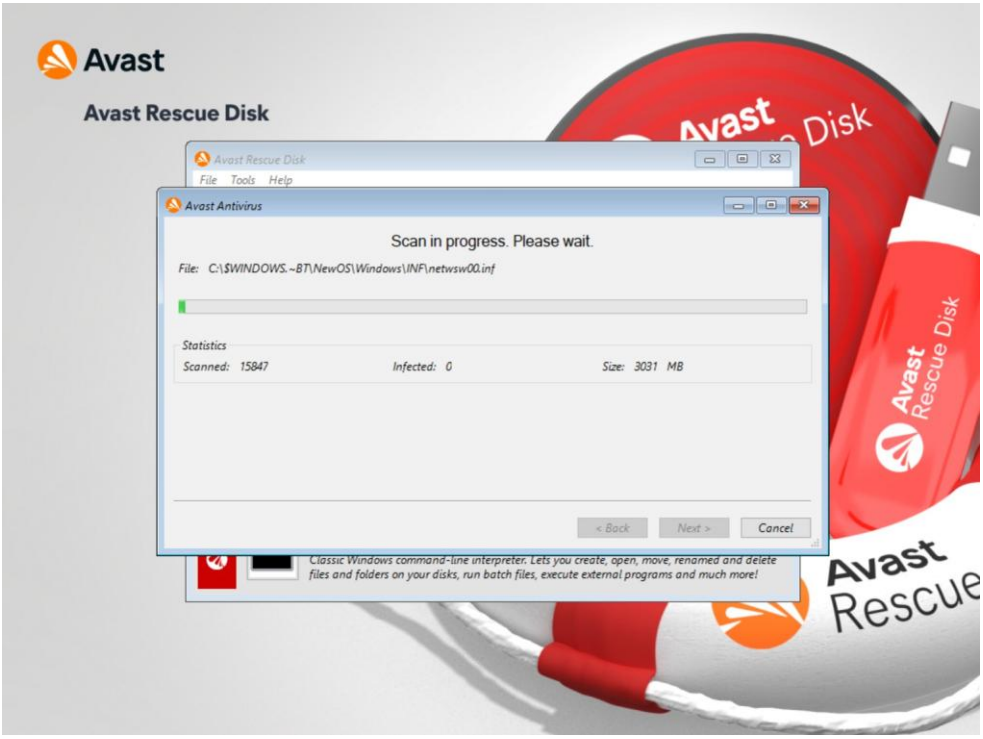


Unter `<Directory>` sehen Sie zunächst alle erkannten Laufwerke und Partitionen. Mittels Klicks auf die Pfeilsymbole können Sie die Verzeichnisstruktur eines Laufwerks öffnen und durch die verschiedenen Verzeichnisebenen navigieren. Markieren Sie alle zu untersuchenden Verzeichnisse durch Aktivieren der vorangestellten Checkbox.

Im Beispiel oben würden auf Laufwerk `X:` die Verzeichnisse `Users` und `Windows` (und deren Unterverzeichnisse) untersucht.

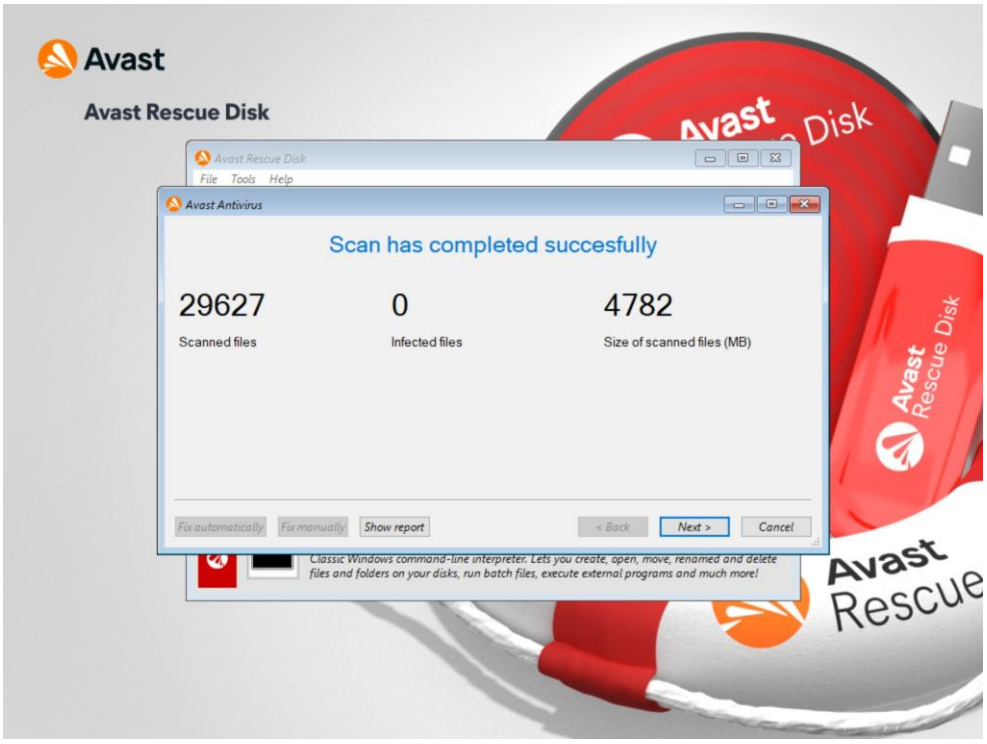
Klicken Sie nach Auswahl aller zu untersuchenden Objekten auf `<Next>`.

Es startet nun die gewählte Untersuchung, die Sie bei Bedarf mittels Klicks auf <Cancel> vorzeitig beenden können:

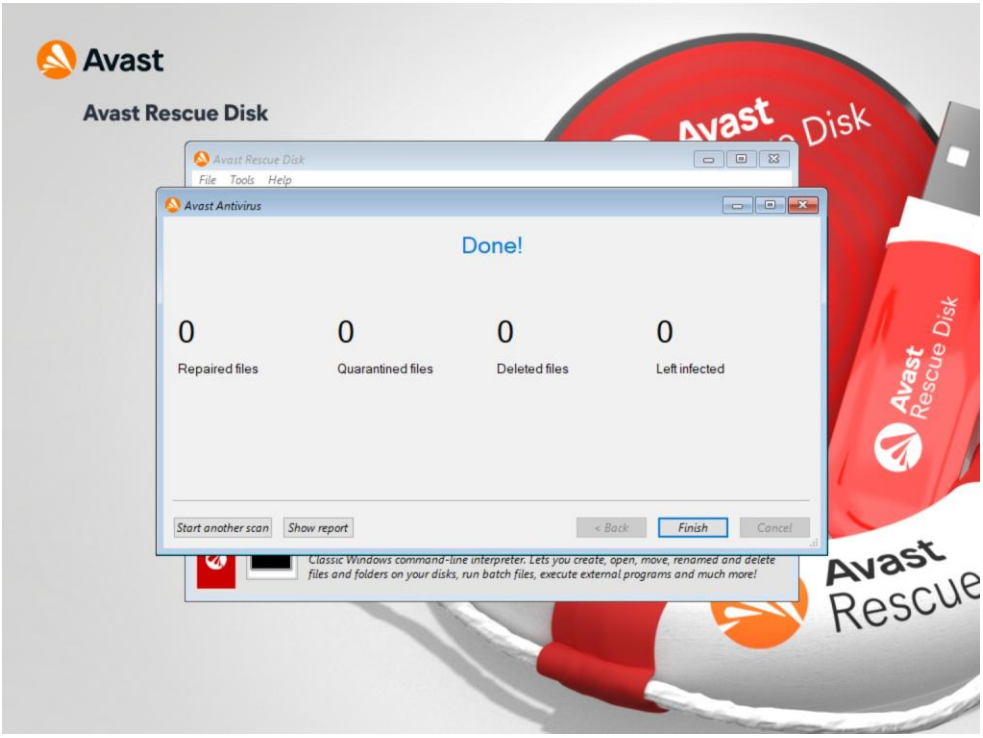


Im Bereich <Statistics> sehen Sie neben dem Eintrag <Infected:>, wie viele Infektionen bereits gefunden wurden.

Wird die Untersuchung ohne Fund von Malware abgeschlossen, erhalten Sie die folgende Meldung:

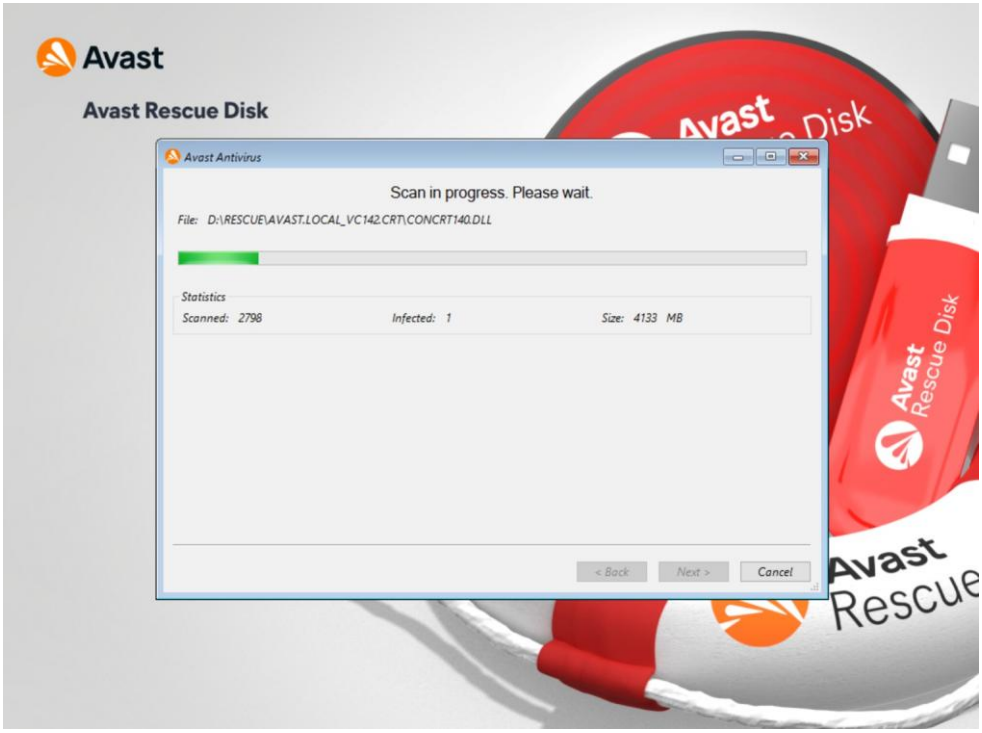


Der Counter <Infected files> zeigt 0; klicken Sie auf <Next>.

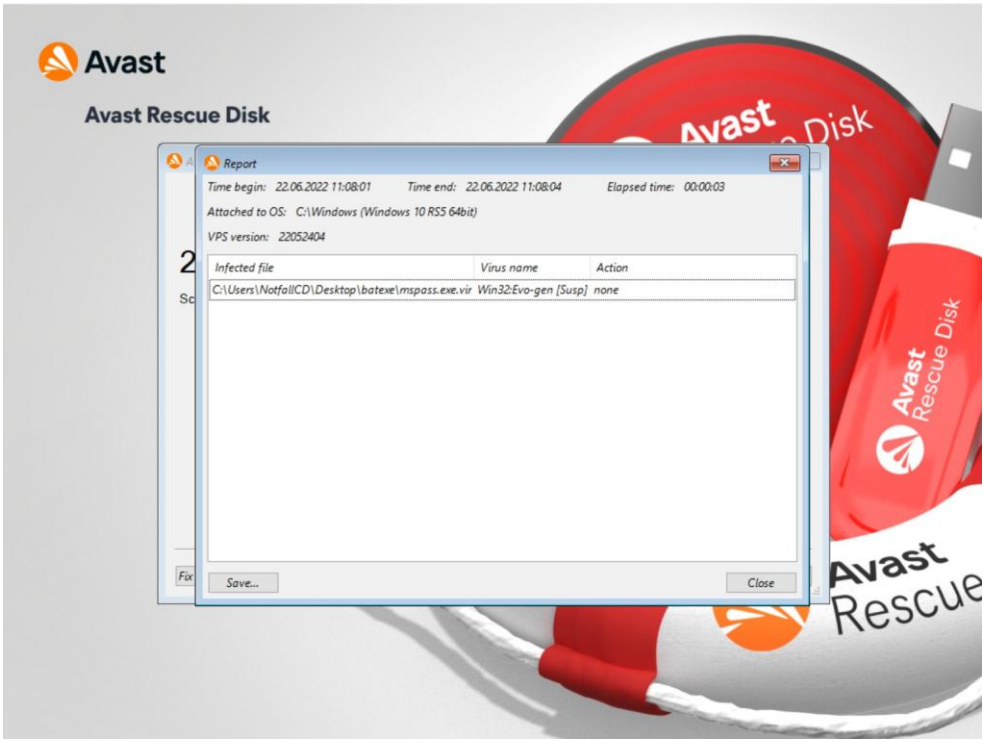


Möchten Sie das Ergebnis durch einen weiteren Scan überprüfen lassen (z.B. indem weitere Laufwerke untersucht werden), so wählen Sie `<Start another scan>`, um in den Startbildschirm des Virenscanners zurückzukehren. Andernfalls wählen Sie `<Finish>`, um das Hauptmenü des Rettungsmediums zurückzukehren.

Werden dagegen Malware-Infektionen gefunden, zählt bereits während der Untersuchung das Feld `<Infected:>` entsprechend hoch:

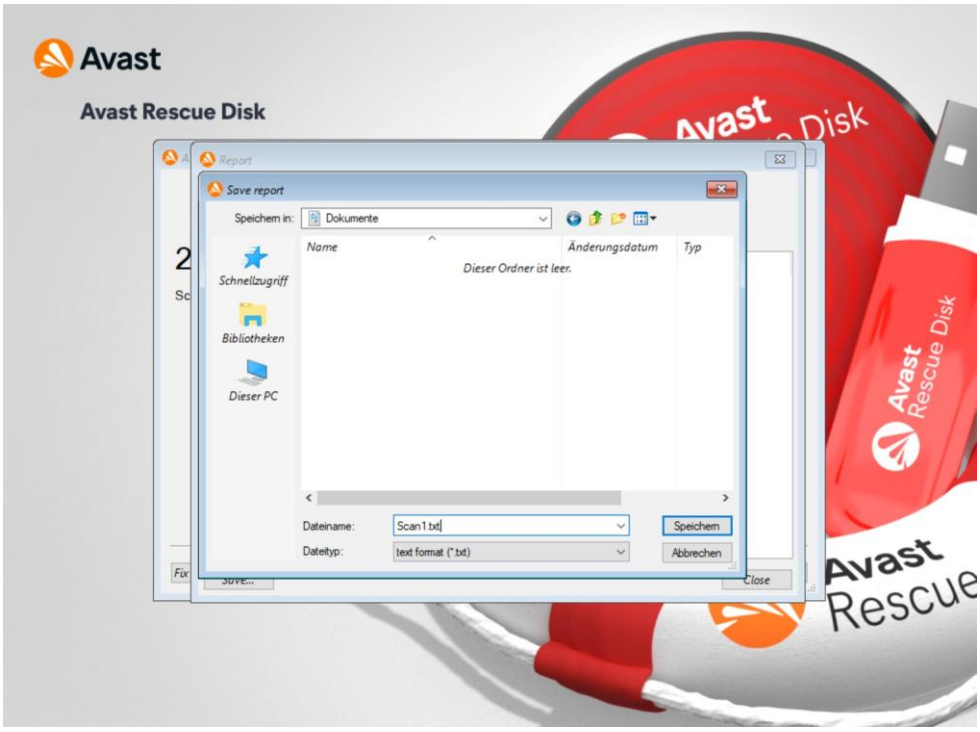


Nach Beendigung des Scanvorgangs erscheint eine Zusammenfassung der gefundenen Infektion(en):



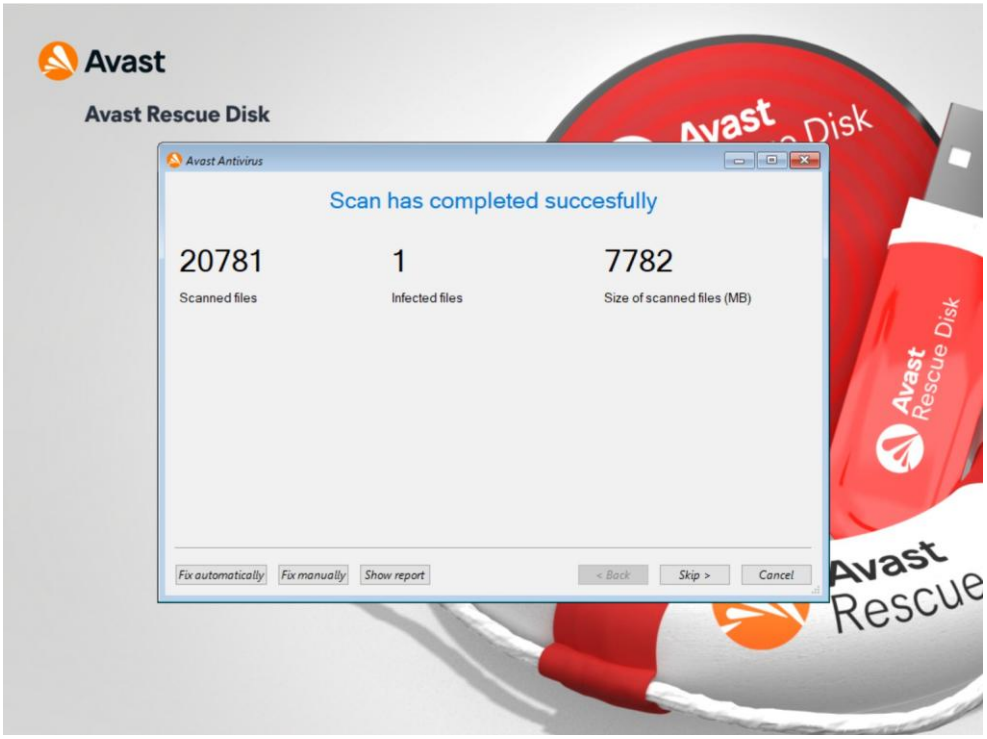
Im obigen Beispiel wurde in der Datei `mspass.exe`, abgelegt unter dem bei `<Infected file>` gezeigten Pfad, ein Trojaner des Typs Win32:Evo gefunden und noch keine weitere Aktion auf diese Datei angewendet (`<Action> = <none>`). Bei mehreren Infektionen finden sich in dieser Übersicht entsprechend weitere Einträge.

Sie können nun, wenn gewünscht, den Inhalt dieser Ansicht als Textdatei abspeichern, indem Sie `<Save...>` wählen.



Wählen Sie den gewünschten Speicherort und geben Sie einen beliebigen Dateinamen ein, die Informationen werden in einer txt-Datei abgelegt.

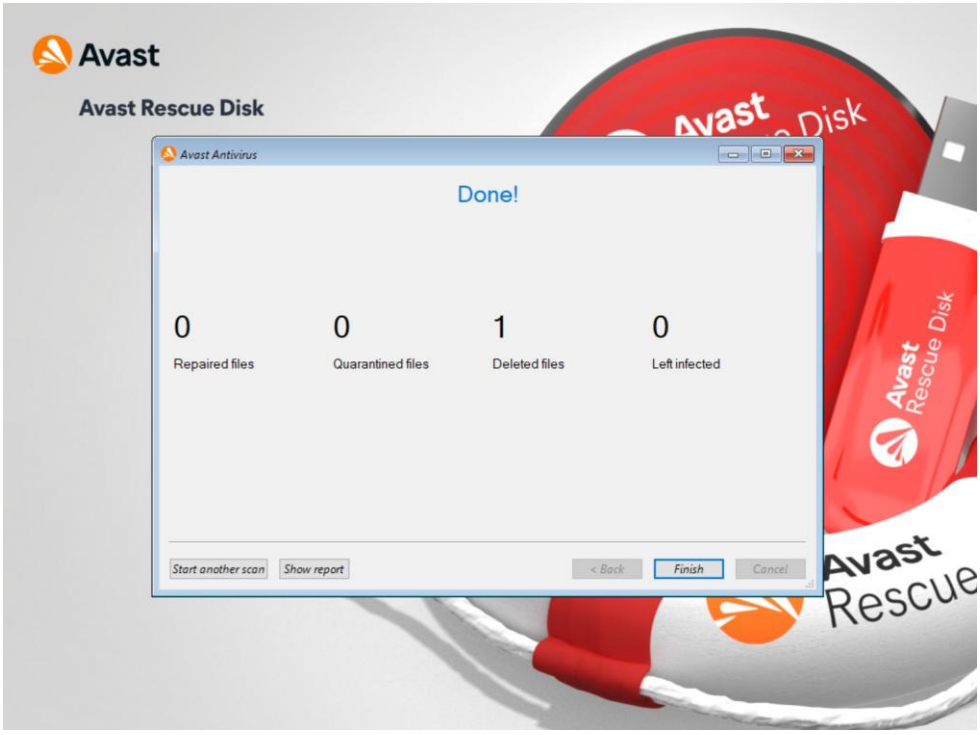
Schließen Sie nun die Ansicht `Report` mittels `<Close>`. Sie gelangen zu dieser Ansicht mit einer Zusammenfassung der Untersuchung:



Treffen Sie nun folgende Auswahl:

- Mittels `<Fix automatically>` versucht das Rettungsmedium, alle infizierten Dateien zu reparieren, d.h. der Virus wird gelöscht, aber die Datei bleibt erhalten. Dateien, deren Reparatur nicht gelingt, werden gelöscht.
- Mittels `<Fix manually>` können Sie für jede Datei selbst entscheiden, wie diese behandelt werden soll (Reparaturversuch oder Löschen).
- Mittels `<Show report>` kehren Sie zur vorherigen Report-Ansicht zurück.
- Mittels `<Skip>` wird nichts unternommen, Sie kommen zum Abschlussbildschirm der aktuellen Untersuchung. Die gefundenen Infektionen bleiben unverändert bestehen!
- Mittels `<Cancel>` kommen Sie ohne weitere Aktion direkt zum Hauptmenü des Rettungsmediums zurück. Die gefundenen Infektionen bleiben unverändert bestehen!

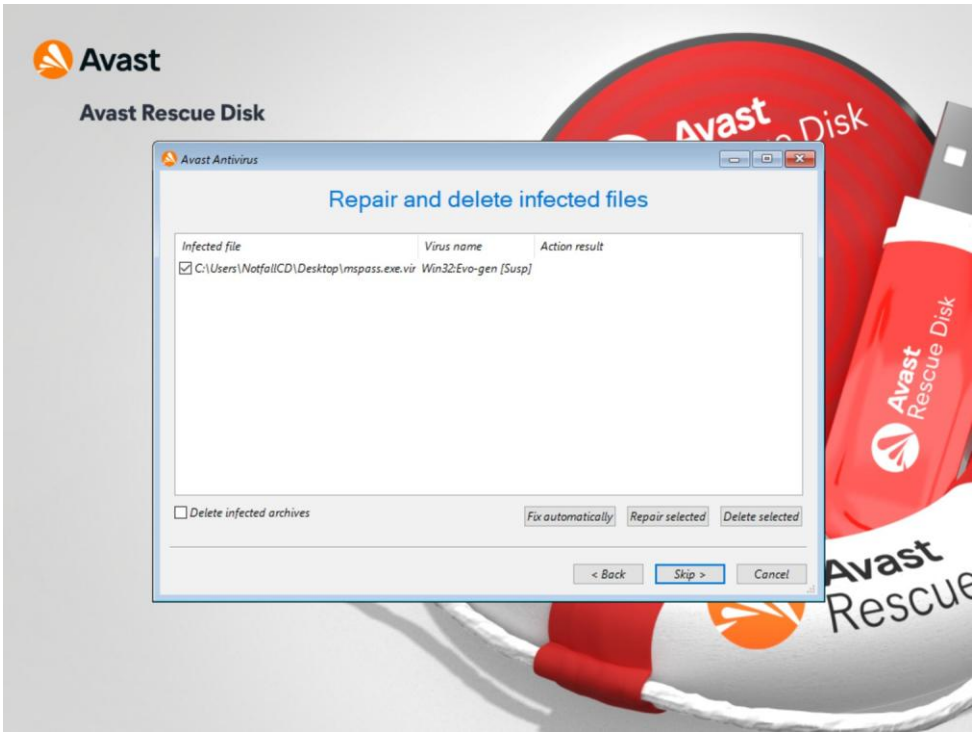
Nachdem Sie `<Fix automatically>` gewählt haben, behandelt Avast jede gefundene Infektion selbsttätig und ohne weitere Meldung. Nach Abschluss der Maßnahmen erhalten Sie eine Zusammenfassung der Ergebnisse:



Im obigen Beispiel wurde eine Datei gelöscht (`<Deleted files> = 1`), da eine Reparatur nicht möglich war (`<Repaired files> = 0`). Es sind keine weiteren bekannten Infektionen im System vorhanden (`<Left infected> = 0`).

Mittels `<Finish>` gelangen Sie zurück ins Hauptmenü.

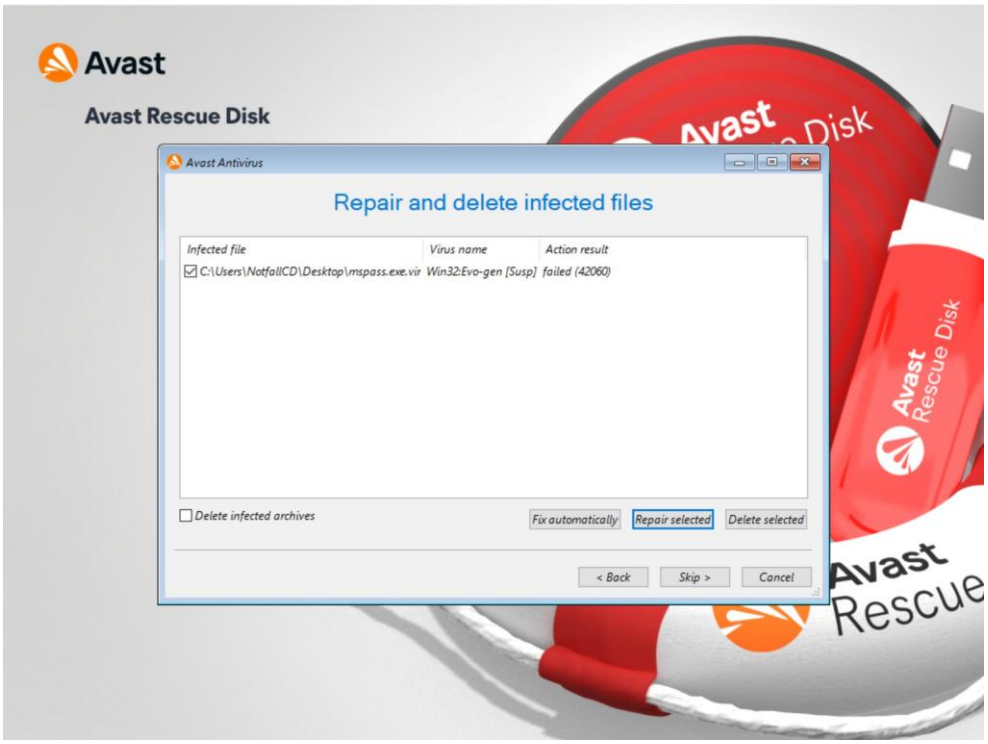
Bei der manuellen Behandlung haben Sie die identischen Wahlmöglichkeiten (Reparatur oder Löschen) mittels der Schaltflächen `<Repair selected>` und `<Delete selected>`:



Aktivieren Sie die Checkboxes vor den Dateinamen (bei mehreren Infektionen) für alle Dateien, die derselben Behandlung unterzogen werden sollen, und wählen Sie die gewünschte Aktion. Mittels `<Skip>` wird nichts unternommen.

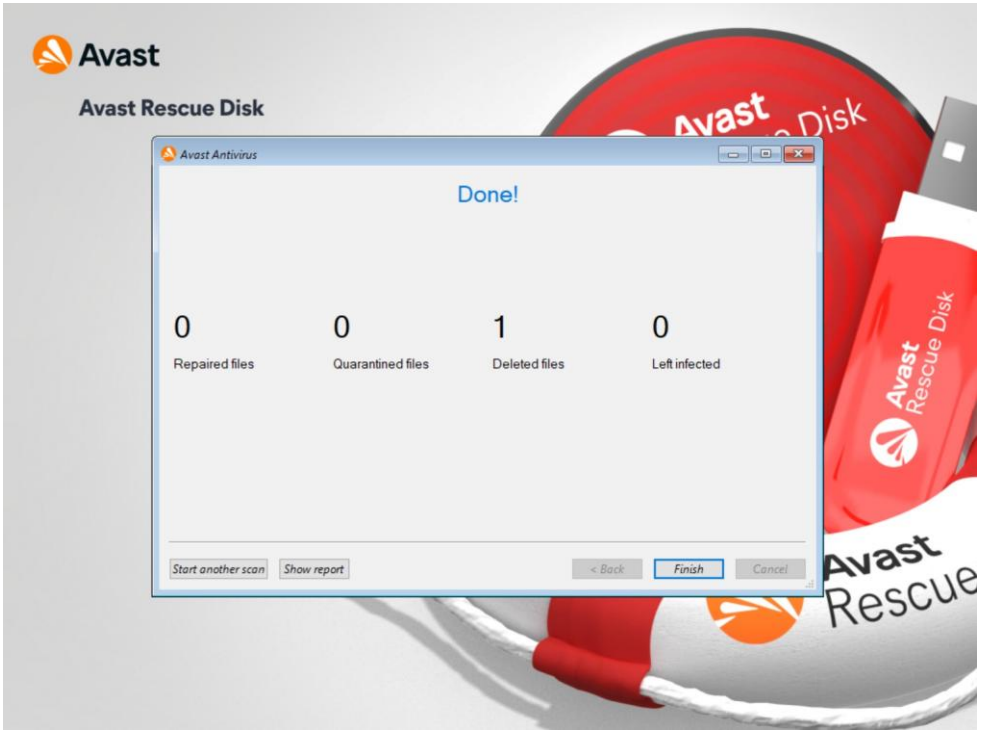
Aktivieren Sie bei Bedarf auch die Checkbox `<Delete infected archives>`.

Wählen Sie `<Repair selected>`, und der Reparaturversuch schlägt fehl, erhalten Sie die folgende Meldung (`<Action result>` = `failed (`*`Errorcode`*`)`):



In diesem Fall bleibt nur die Löschung der Datei. Bei erfolgreicher Löschung sehen Sie unter `<Action result>` den Eintrag `deleted`.

Nach Abschluss aller notwendigen Aktionen wählen Sie `<Skip>`, um den Abschlussbildschirm der Untersuchung zu sehen:



Hier ist nochmals aufgeführt, wie viele Dateien bei dieser Untersuchung repariert (<Repaired files>), gelöscht (<Deleted files>) und unverändert infiziert belassen (<Left infected>) wurden. Schließen Sie diese Ansicht mittels <Finish>, um in das Hauptmenü des Rettungsmediums zurückzukehren.

Hier haben Sie noch folgende Möglichkeiten:

- Eine neue Untersuchung starten (<AvastPE Antivirus>),
- ein Browserfenster öffnen, z.B. um Virusbezeichnungen oder Errorcodes zu suchen (<AvastPE Browser>),
- eine dem Windows-Explorer ähnliche Ansicht des Systems öffnen (<AvastPE Commander>),
- einen Editor der Windows-Registry öffnen (<Registry Editor>),
- eine Windows-Kommandozeile öffnen (<Command-line Tool>),
- das System neu starten (Menü <File>, dann <Restart>) und
- das System ausschalten (Menü <File>, dann <Shut down>).

Der Editor der Windows-Registry wird nur fortgeschrittenen Benutzern empfohlen, bei unsachgemäßen Änderungen kann das Betriebssystem schwerwiegend beschädigt werden.

4. 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

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.

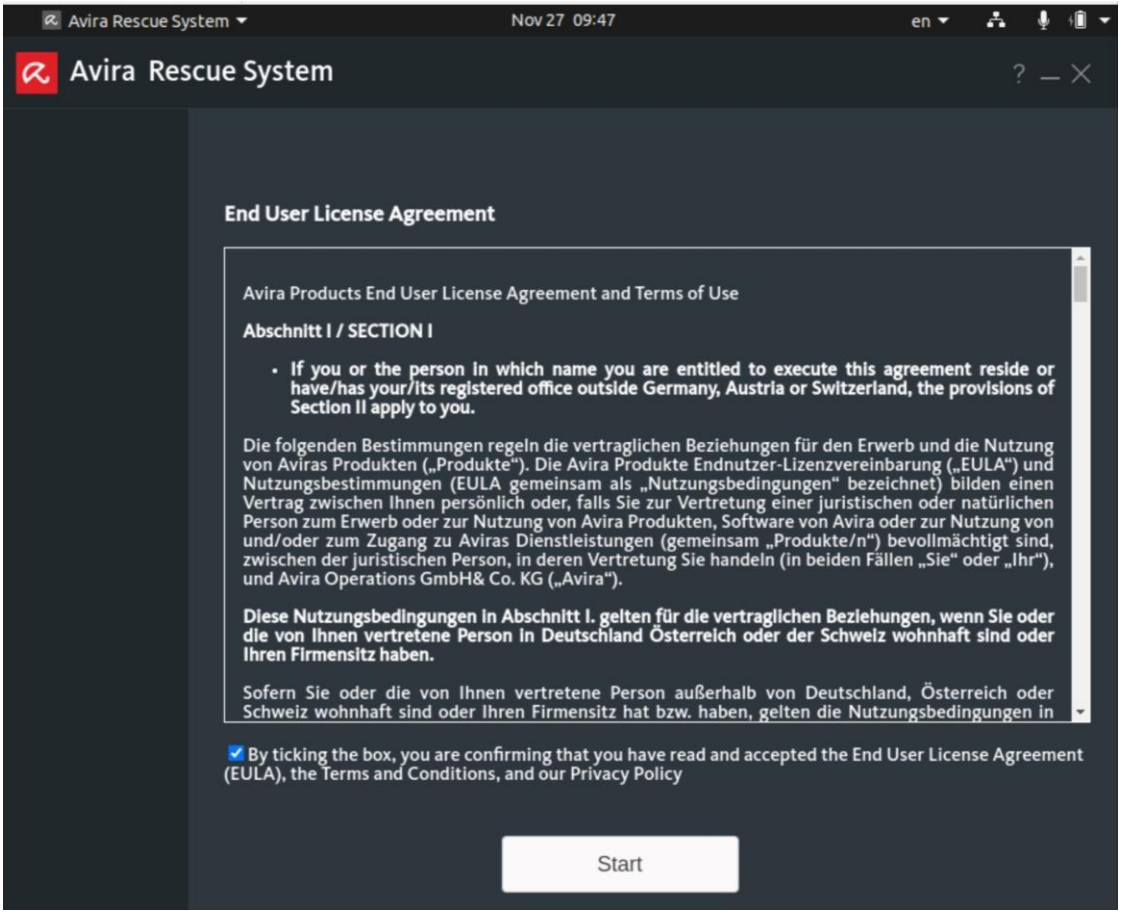
Download Rufus Portable:
https://rufus.ie/de/

Download UNetbootin:
https://unetbootin.github.io/

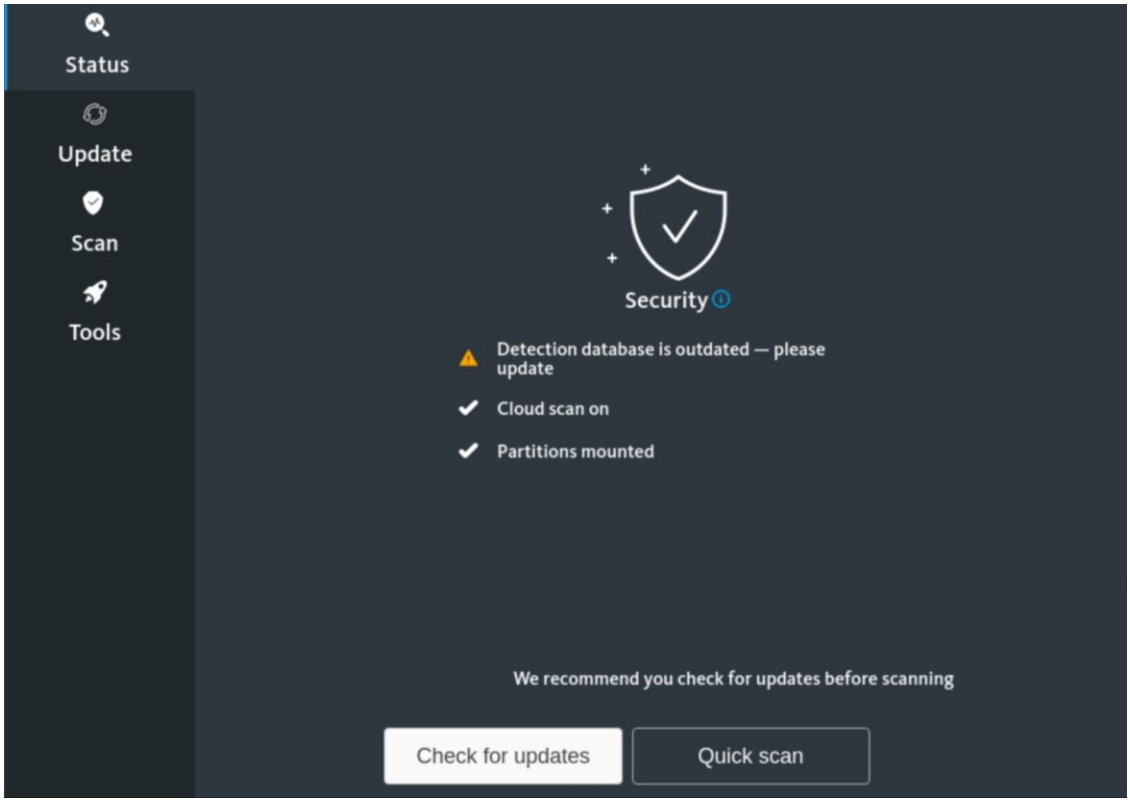
Alternativ können Sie das ISO-Image auch als DVD brennen und von dieser das betroffene System neu starten. Nutzen Sie hierzu das in Ihrem Institut vorhandene Angebot an Software oder die in Windows 10 integrierte Funktion <Datenträgerabbild brennen>.

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.

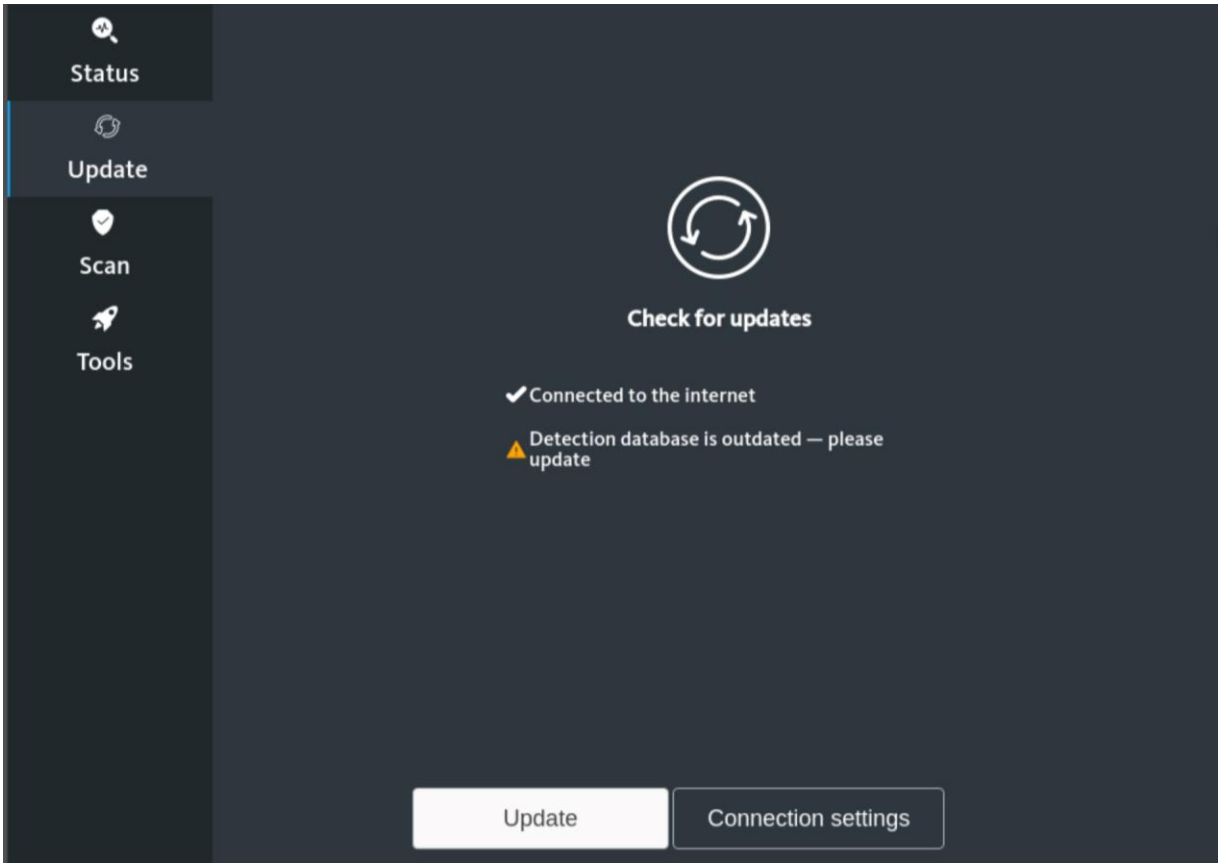
Nach dem Bootvorgang wird zunächst der Lizenzvertrag angezeigt.



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

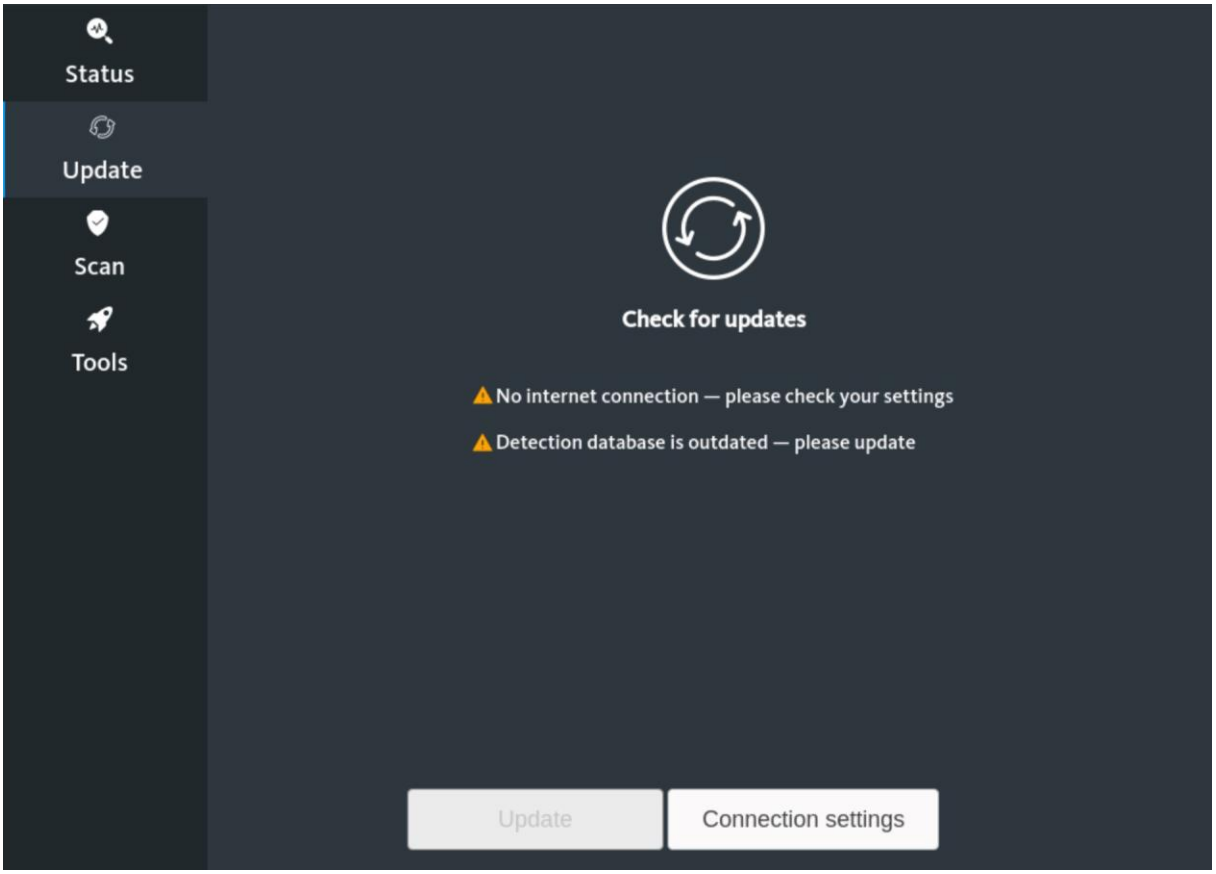


Sie werden darauf hingewiesen, dass die Virusmusterdefinitionen veraltet sind. Klicken Sie daher auf <Check for updates>, um diese zu aktualisieren. Eine Prüfung des Systems kann zwar auch ohne Update vorgenommen werden, diese Vorgehensweise wird jedoch nicht empfohlen.



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>.

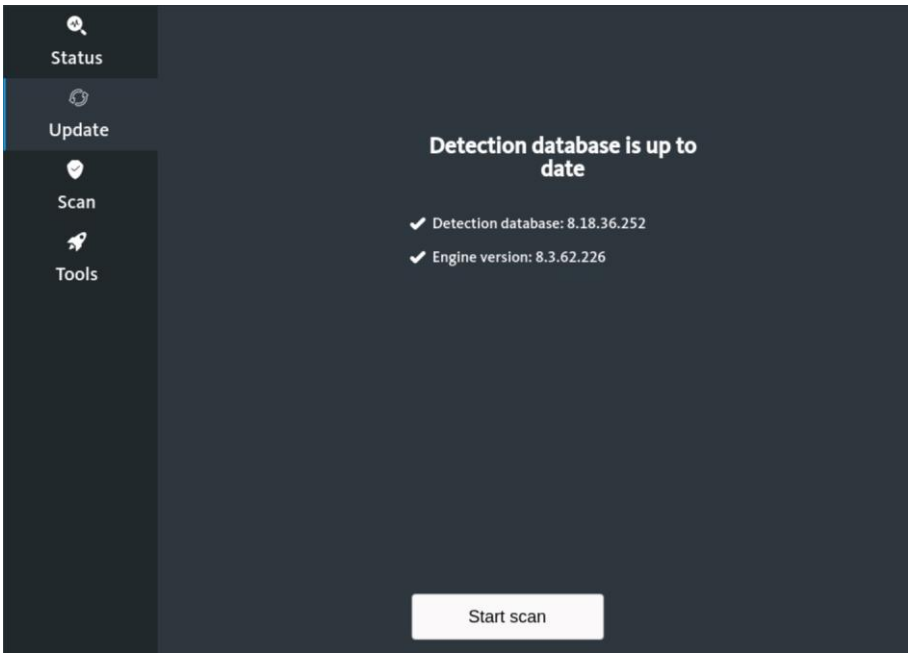
Erhalten Sie dagegen die nachfolgende Meldung <No internet connection…>, so ist das System nicht mit dem öffentlichen Netz verbunden und die Schaltfläche <Update> ist inaktiv. Beheben Sie das Problem und klicken Sie auf <Status>, um zum letzten Schritt zurückzukehren.



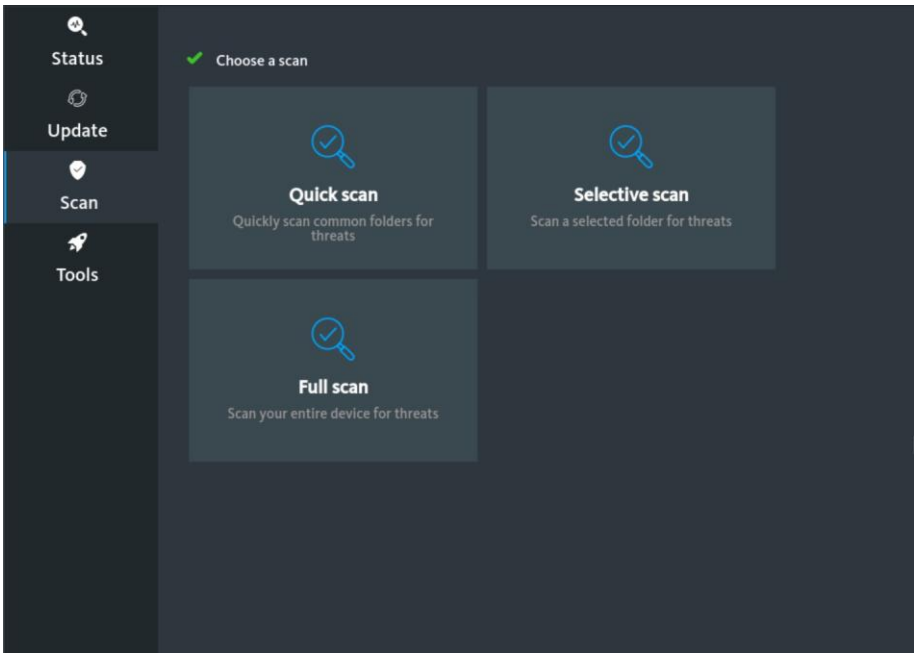
Schauen Sie ggfs. in Kapitel 5-Troubleshooting nach und starten Sie die Notfall-CD neu, damit die automatische Netzwerkerkennung erneut durchgeführt wird.

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

Nach dem Klick auf <Update> wird das Update ausgeführt, es erscheint der Hinweis <Updating…>. Nach einer Weile informiert der folgende Bildschirm über den erfolgreichen Abschluss:

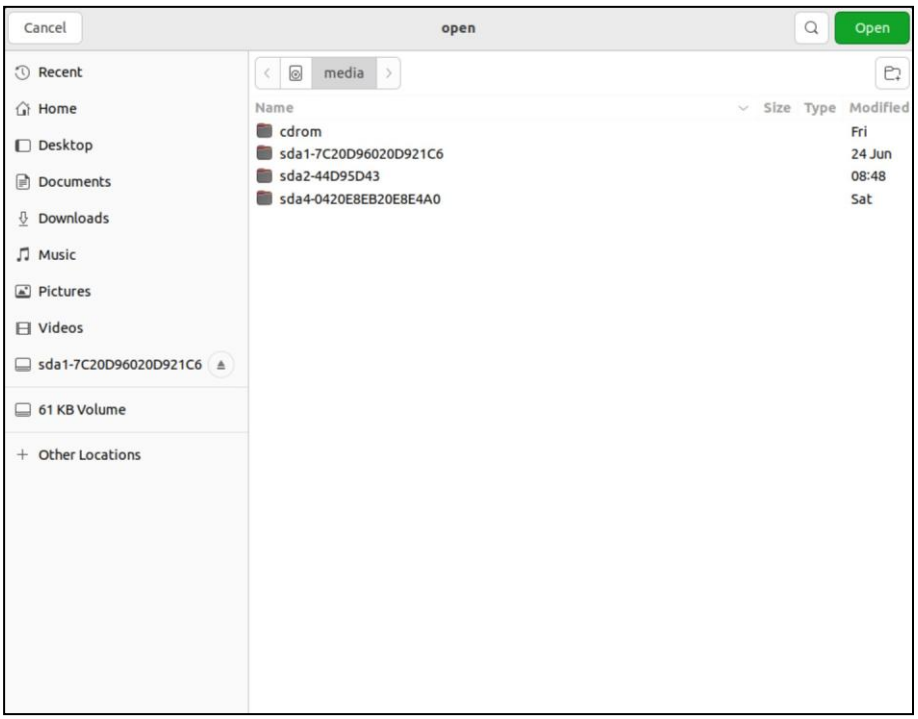


Klicken Sie auf <Start scan>.



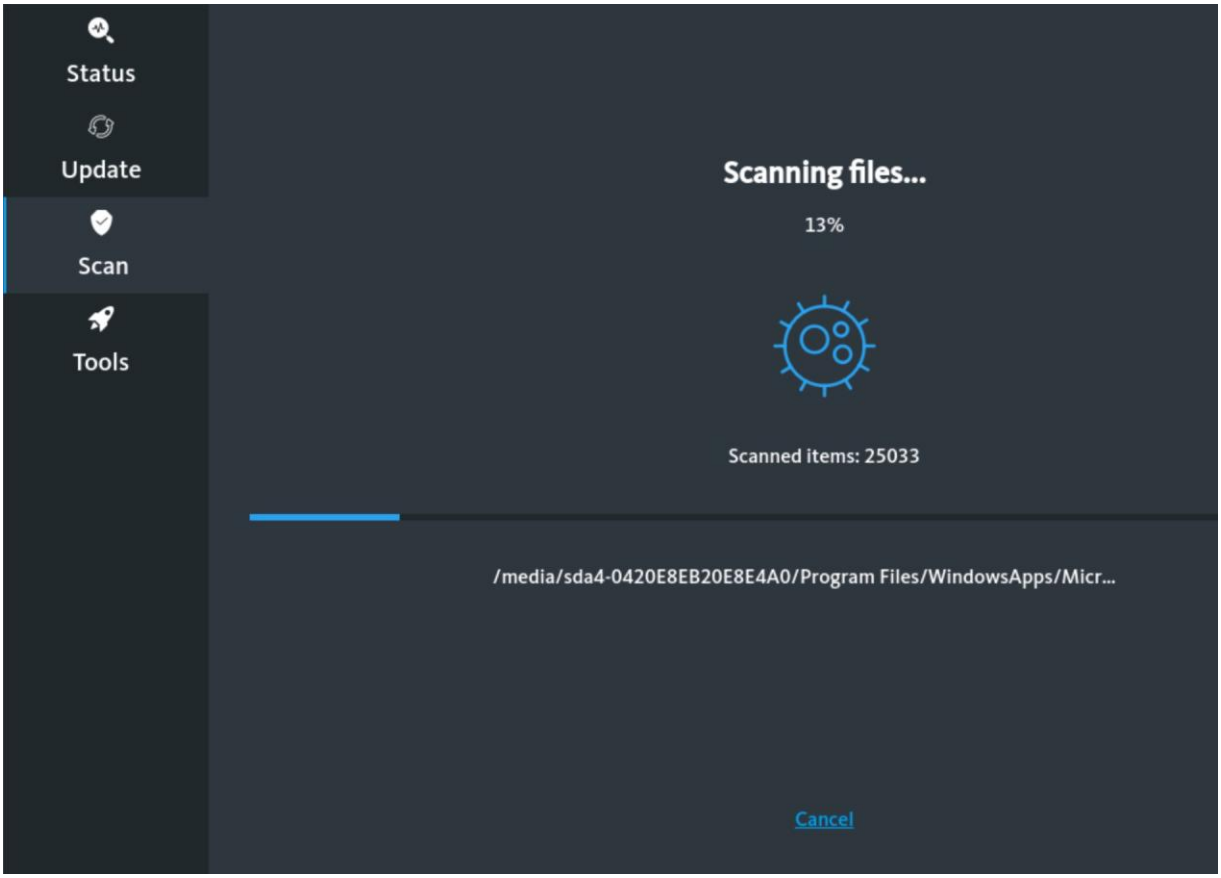
Wählen Sie nun zwischen einer vollständigen Überprüfung des Systems (<Full scan>) oder einer auf bestimmte Ordner beschränkten Prüfung (<Selective scan>). Letztere sollte nur verwendet werden, wenn die Bedrohung bereits vorab auf bestimmte Verzeichnisse eingegrenzt werden konnte. Ist dies nicht der Fall,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

Haben Sie <Selective scan> gewählt, sehen Sie nun eine Explorer-Ansicht, deren Verzeichnisbaum der Struktur von Linux-Systemen entspricht (evtl. müssen Sie eine Meldung <"open" is ready> anklicken):

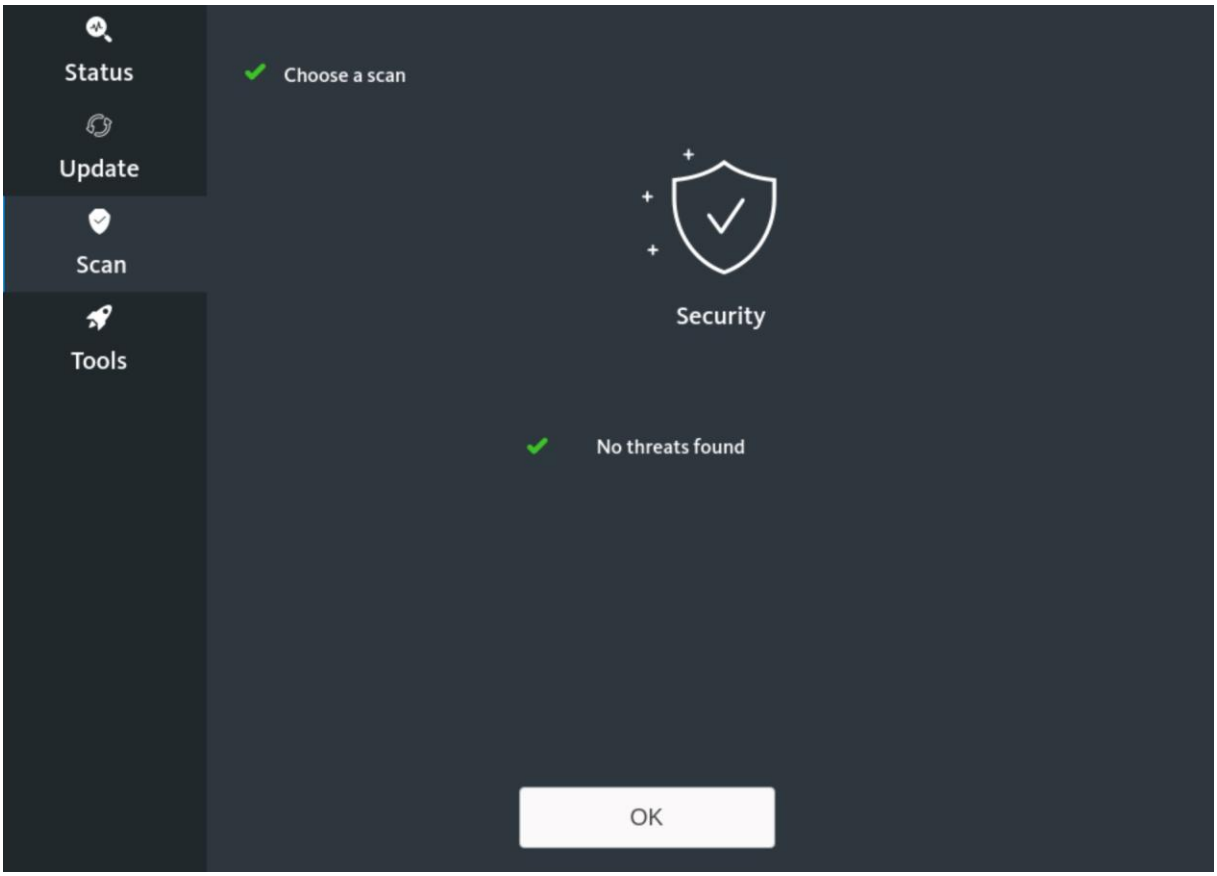


Suchen Sie die zu prüfenden Ordner bzw. Laufwerke und markieren Sie diese. Mittels der <Strg>-Taste können Sie mehrere Einträge der aktuellen Ansicht markieren. Nach einem Klick auf <Open> beginnt die Überprüfung.

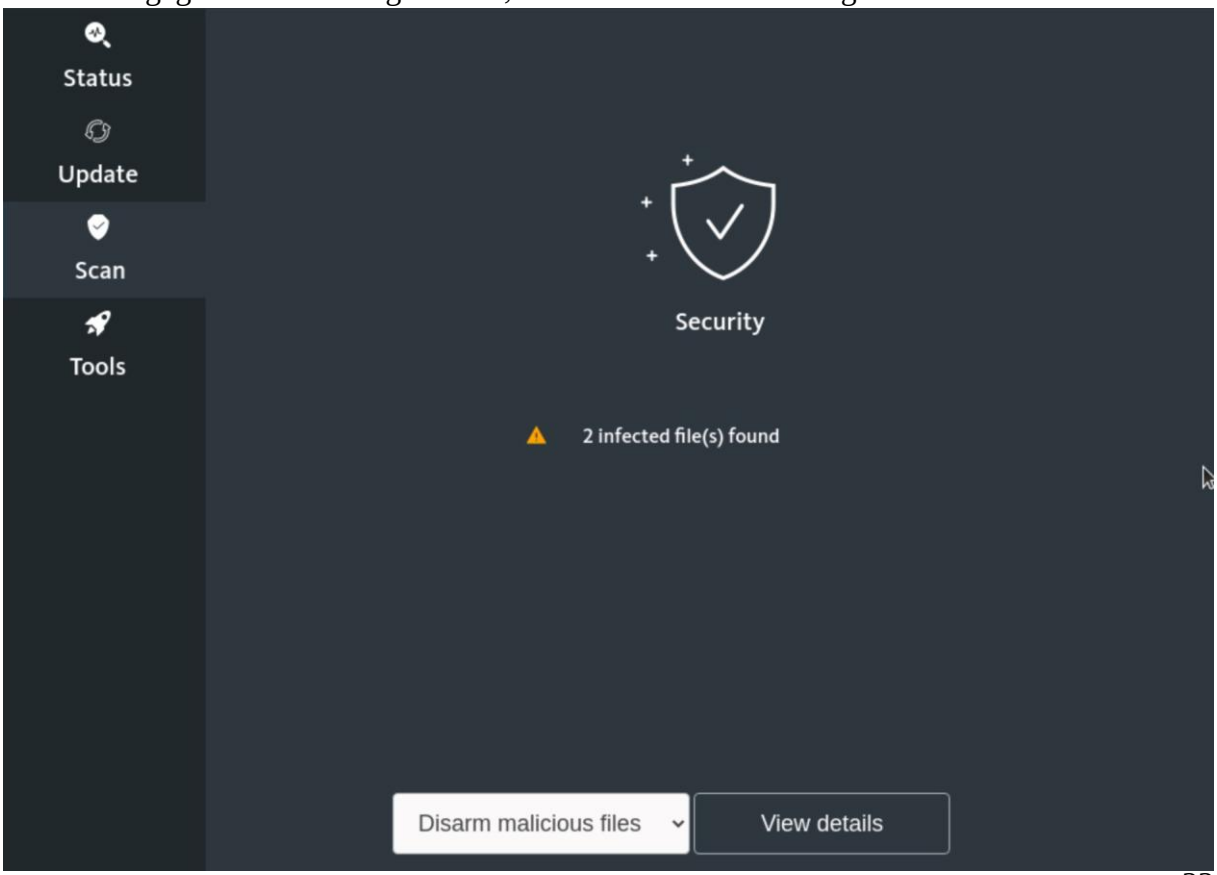
Haben Sie dagegen die vollständige Überprüfung gewählt, beginnt diese sofort ohne weitere Meldung. Während der Prüfung sieht der Bildschirm wie folgt aus, mittels <Cancel> kann sie unterbrochen werden.



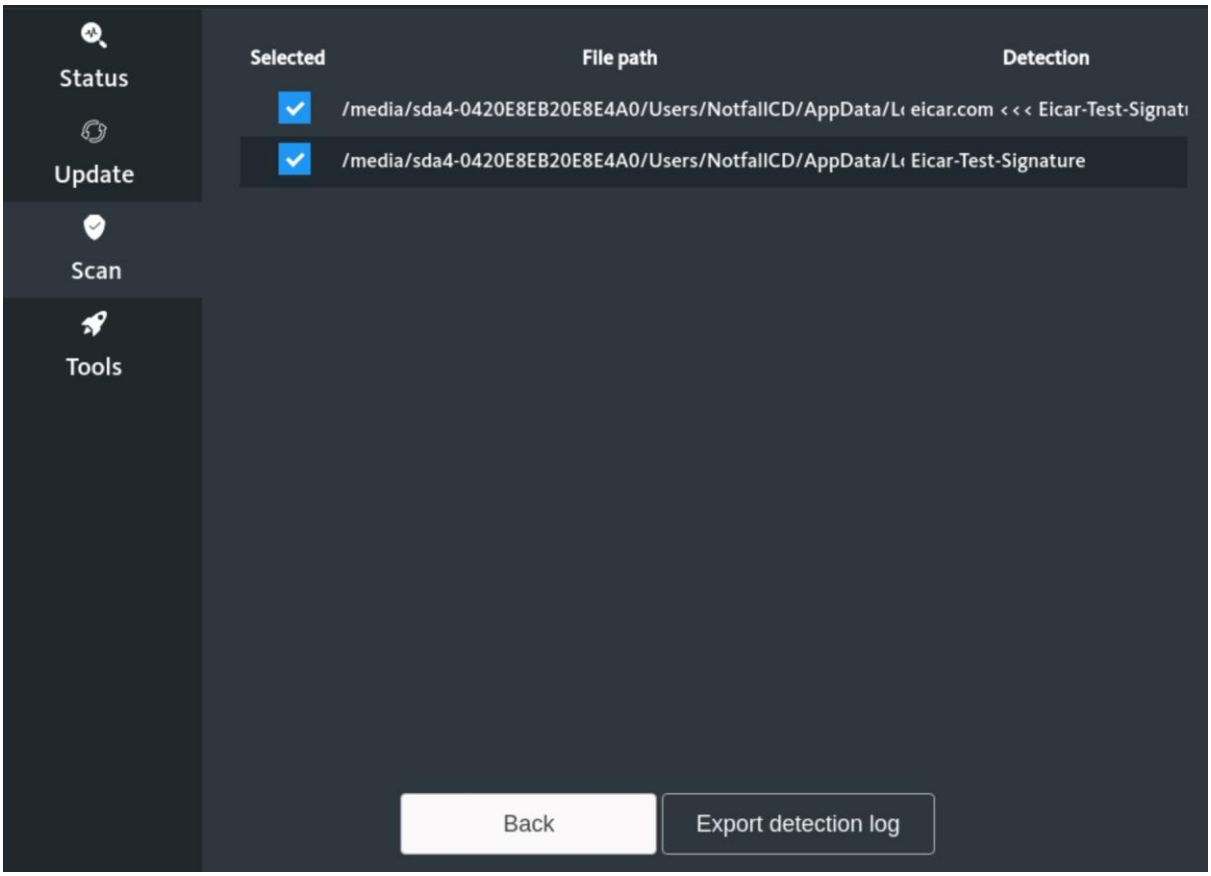
Nach Abschluss der Prüfung erhalten Sie folgende Meldung, wenn keine Infektionen gefunden wurden. Mit einem Klick auf <OK> gelangen Sie zurück in die Hauptansicht der Rubrik <Scan>.



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



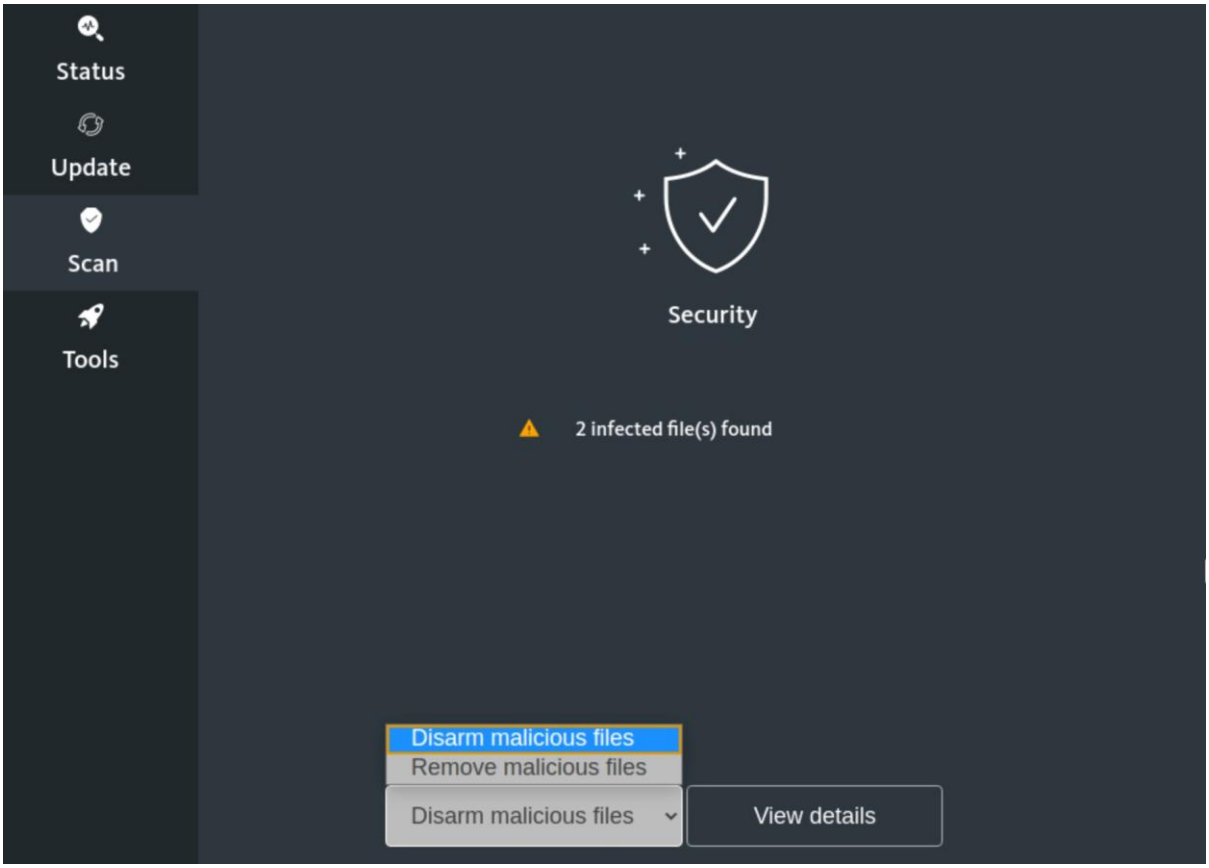
Per Klick auf <View details> erhalten Sie genauere Angaben zu den gefundenen Objekten.



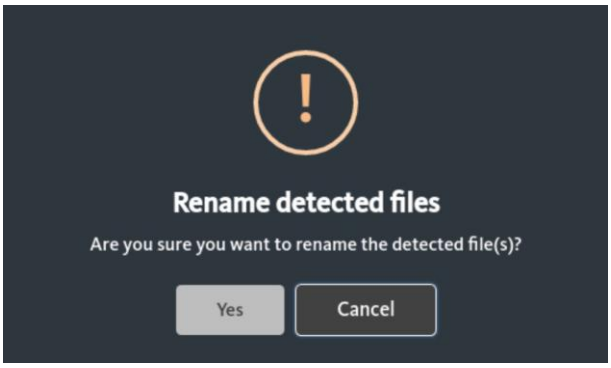
Wenn gewünscht, können Sie die Angaben per Klick auf <Export detection log> auf dem System oder den angeschlossenen Datenträgern speichern. Es erscheint wiederum eine Explorer-Ansicht, in der Sie den Speicherort wählen und <OK> klicken.

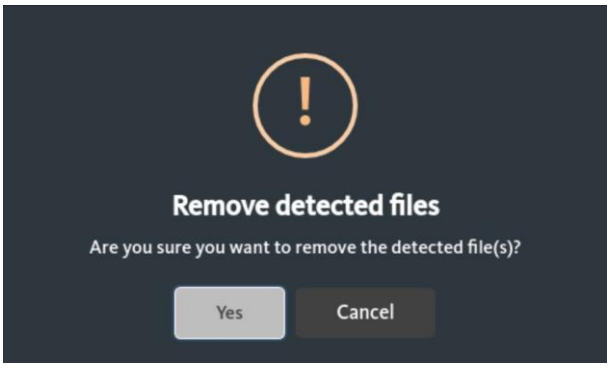
Wählen Sie <Back>, um zurück zur letzten Ansicht zu kommen. Klicken Sie auf <Disarm malicious files>, um die beiden Optionen anzeigen zu lassen, was mit den gefundenen Infektionen geschehen soll:

- 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.

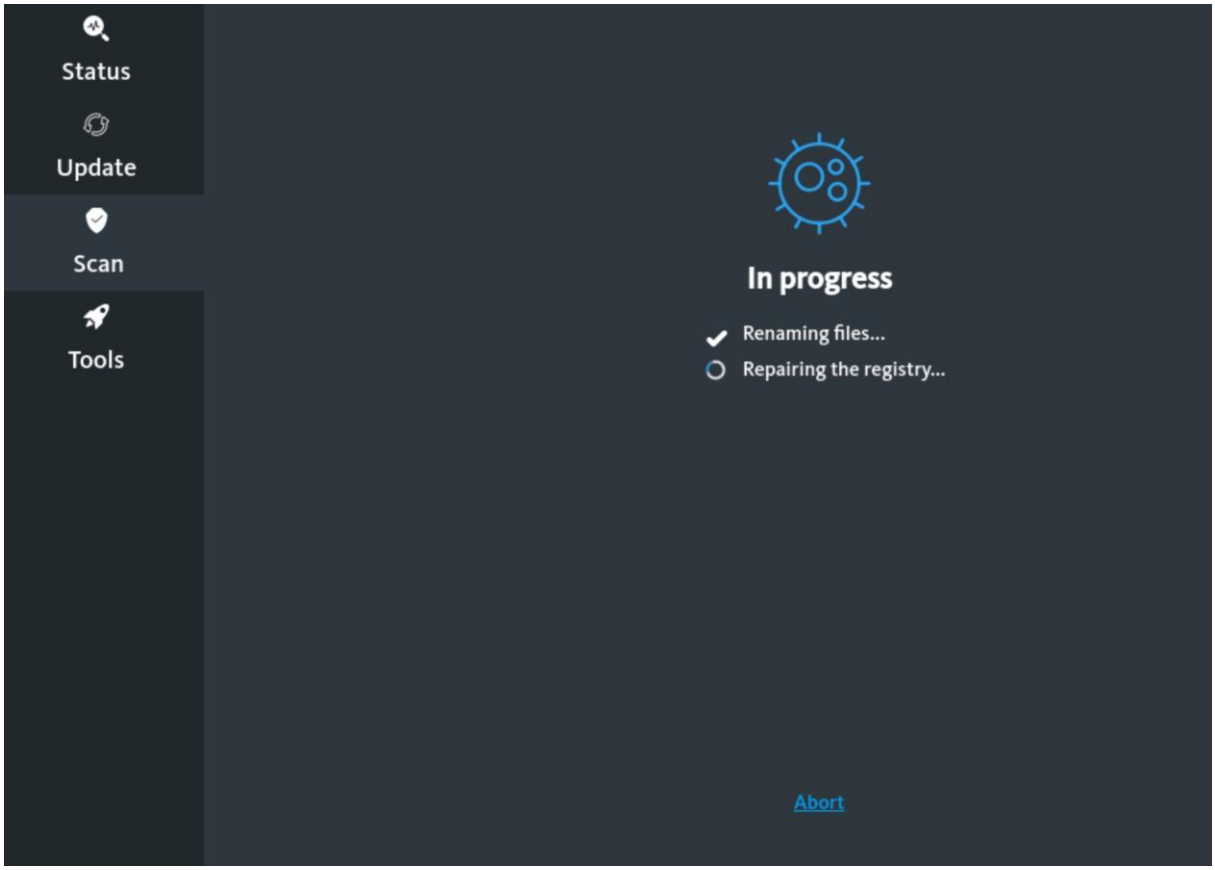


Klicken Sie Ihre Wahl an. In beiden Fällen werden Sie noch aufgefordert, die Aktion zu bestätigen:

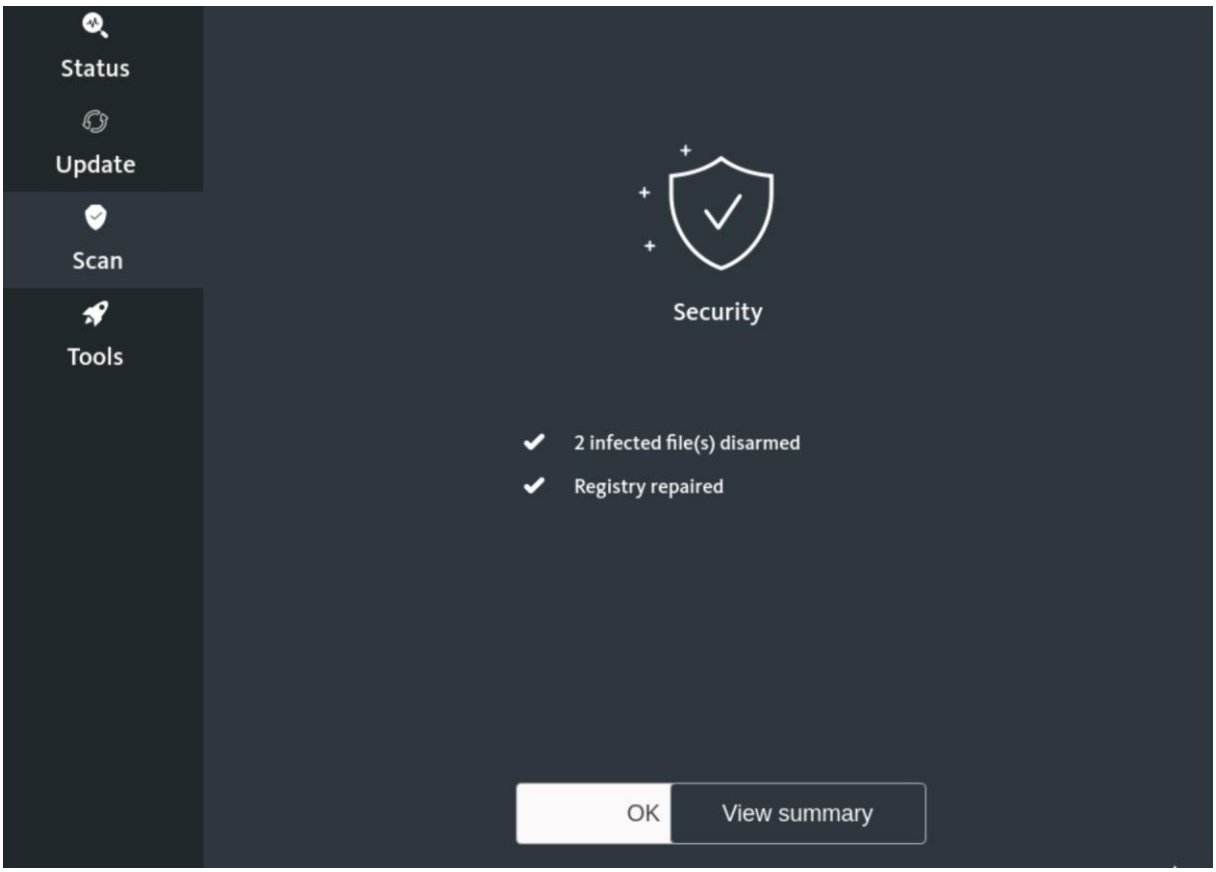




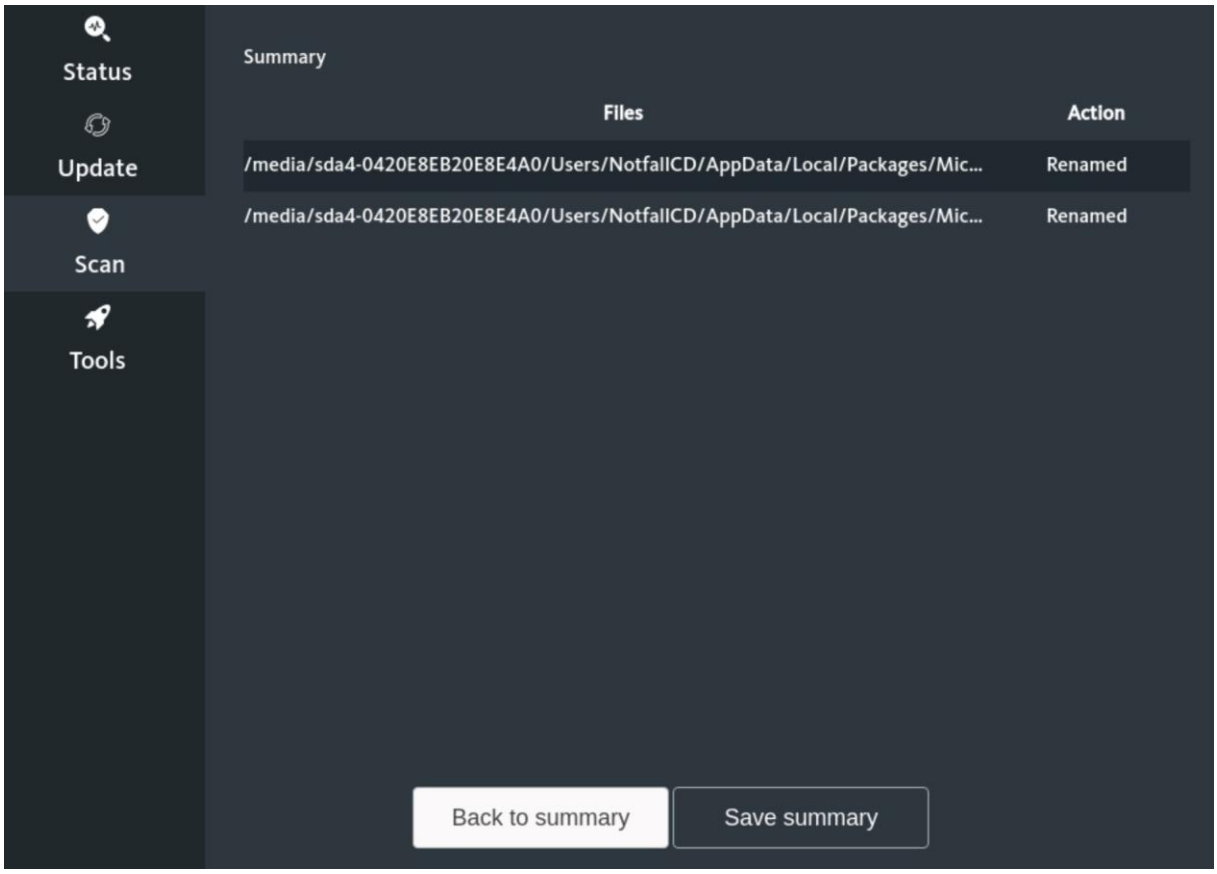
Nach dem Klick auf `<Yes>` wird die Aktion ausgeführt. Währenddessen sehen Sie folgenden Bildschirm:



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 die Symbole und wählen Sie <Power Off / Log Out>, dann <Power Off…> und schließlich <Power Off>.

5. 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 Netzwerkadaptern 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.