# c't Desinfec't

## Das Rettungssystem bei Virenbefall


***DAS c't-Sicherheitstool als Download für USB-Sticks***

- ***Entfernt Trojaner und Viren unter Windows***
- ***Mit 3 Scannern: ClamAV, Eset, WithSecure***
- ***Signatur-Updates gratis bis Oktober 2025***

## Virenbefall! Das müssen Sie tun

Step-by-Step-Anleitung: So entfernen Sie Viren mit Desinfec't

Scannen, löschen, retten: Das kann das c't-Sicherheitstool

## Dateien wiederherstellen

Verloren geglaubte Fotos und Dateien retten

Daten von NAS-Platten kratzen

## Zusatz-Werkzeuge für Profis nutzen

Malware-Analyse mit brandneuen Experten-Tools

Zwei Extra-Scanner selbst konfigurien

Mehr Software: Desinfec't erweitern

€ 16,90
CH CHF 29.20
AT € 18,60
LUX € 19,50

4 197665 616908 03

# Editorial

Liebe Leserin, lieber Leser,

wenn sich Ihr Windows-PC seltsam verhält und beispielsweise Werbefenster auf dem Desktop aufploppen, schlägt die Stunde für das c't-Sicherheitstool Desinfec't 2024/25. Damit untersuchen Sie Windows aus einer sicheren Entfernung, um Viren aufzuspüren und Daten zu retten. Mit den Anleitungen in diesem Heft kriegen das auch Computereinsteiger hin.

Das Besondere an Desinfec't ist, dass es sein eigenes Live-Betriebssystem mitbringt, das statt Windows direkt von einem USB-Stick startet. So ist sichergestellt, dass Trojaner im inaktiven Windows nicht noch mehr Unheil anrichten. Außerdem können Sie so auf Ihre Daten zugreifen, wenn Windows gar nicht mehr startet. Um Ihre Dateien in Sicherheit zu bringen, kopieren Sie sie einfach auf den Desinfec't-Stick.

Das Sicherheitstool bringt unter anderem Scanner von Eset und WithSecure mit, die Viren aufspüren. Um aktuellen Schädlingen auf die Spur zu kommen, sind ein Jahr lang Gratis-Signaturupdates inklusive. Wer an bestimmten Stellen nicht weiterkommt, ruft mit dem integrierten Fernwartungsclient den Familienadmin zu Hilfe.

Desinfec't 2024/25 kann aber noch mehr und bringt einige neue Profitools zur Malware-Analyse mit. Zusätzlich nutzen Profis den Open Threat Scanner und den Thor Lite Scanner mit selbst erstellten maßgeschneiderten Suchregeln.

Viel Erfolg bei der PC-Rettung mit dem neuen Desinfec't!

Viel Freude beim Lesen!

Dennis Schirrmacher

# Inhalt



Direkt loslegen!

## Viren jagen mit Desinfec't

Mit dem c't-Sicherheitstool Desinfec't 2024/25 untersuchen Sie Windows aus sicherer Entfernung auf Trojaner. Das Live-System startet von einem USB-Stick und schaut mit mehreren Virenscannern von unter anderem Eset und WithSecure auf das inaktive Windows. Damit Desinfec't auch aktuelle Schädlinge erkennt, sind ein Jahr lang kostenlose Signatur-Updates inklusive. Schlägt einer der Scanner an, können Sie die Gefahr eingrenzen und gegebenenfalls beseitigen.

Dank diverser Tools bringen Sie mit Desinfec't zudem beispielsweise wichtige Daten in Sicherheit. Um das Sicherheitstool zu nutzen, laden Sie zuerst das Zip-Archiv von Desinfec't 2024/25 herunter. Anschließend erstellen Sie einen USB-Stick und starten es von dort. Weitere Informationen dazu finden Sie in der Schritt-für-Schritt-Anleitung ab Seite 10.




## Zum Heft

# Desinfec‘t 2024/25 im Überblick

**Die neue Version von Desinfec’t bringt mehrere Virenscanner mit, die Windows-Systeme auf Trojanerbefall untersuchen. So eliminieren Sie PC-Schädlinge und retten Ihre Daten. Damit kommen auch Computereinsteiger klar.**

Von **Dennis Schirrmacher**

Desinfec’t ist das langjährig erprobte Sicherheitstool der c’t-Redaktion. Wenn sich ein Windows-PC seltsam verhält und Sie befürchten, dass Schadcode das System zersetzt, hilft Desinfec’t bei der Diagnose. Dank eines Kniffes geschieht das aus einer sicheren Position heraus, sodass Viren nicht noch mehr Unheil anrichten können. Desinfec’t 2024/25 bringt ein Jahr lang kostenlose Signaturupdates mit, sodass Sie auch für aktuelle Bedrohungen gerüstet sind.

## Was ist Desinfec’t?

Wenn Sie Desinfec’t bereits kennen, werden Sie in den folgenden Abschnitten nichts Neues erfahren. Springen Sie am besten gleich zum nächsten Artikel, um die Virenjagd ohne Umschweife zu beginnen. Dort steht unter anderem verständlich erklärt, wie Sie das Sicherheitstool auf einem USB-Stick installieren, es starten, Viren jagen und Daten retten.

Um Missverständnissen gleich vorzubeugen: Das Sicherheitstool ist keine Windows-Anwendung, die man installiert und dann wie etwa einen Virenscanner startet. Vielmehr bringt es sein eigenes Betriebssystem auf Linux-Basis mit und startet direkt von einem USB-Stick. Demzufolge müssen Sie Ihrem PC sagen, dass er nicht von der Festplatte mit Windows, sondern vom Stick starten soll.

Dieser Ansatz bringt den großen Vorteil mit, dass Windows inaktiv bleibt, sodass ein Virus ebenfalls

stillgelegt ist und das System nicht noch weiter verbiegen kann. Da Desinfec't auf Linux basiert, kann ein auf Windows zugeschnittener Schädling aus Kompatibilitätsgründen nicht auf das System überspringen. So gelingt die Untersuchung aus sicherer Entfernung. Desinfec't bringt Virenscanner von unter anderem Eset und WithSecure mit. Damit untersuchen Sie Windows-Festplatten auf Schädlingsbefall. Schlagen die Scanner Alarm, helfen Tools bei der Einordnung von Funden. Schließlich sind Fehlalarme nicht ausgeschlossen. Das Scannen klappt übrigens auch mit verschlüsselten Windows-Partitionen.

Mit verschiedenen Expertentools kommen Malwareprofis noch tieferliegenden PC-Problemen auf die Spur. Neu sind in Desinfec't 2024/25 weitere Analysewerkzeuge wie Capa und FLOSS hinzugekommen. (siehe Artikel „Neue Malware-Analysetools für Profis").

Sie können Desinfec't privat einsetzen und gerne auch im Familien- und Freundeskreis verteilen. Die Nutzung ist grundsätzlich auch im beruflichen Umfeld, etwa in Büros, Unternehmen und Universitäten erlaubt. Wollen Sie Desinfec't dort aber mit mehreren Kopien parallel einsetzen, benötigen Sie fairerweise mehrere Lizenzen. Kontaktieren Sie dafür gerne den heise Shop (shop@heise.de).

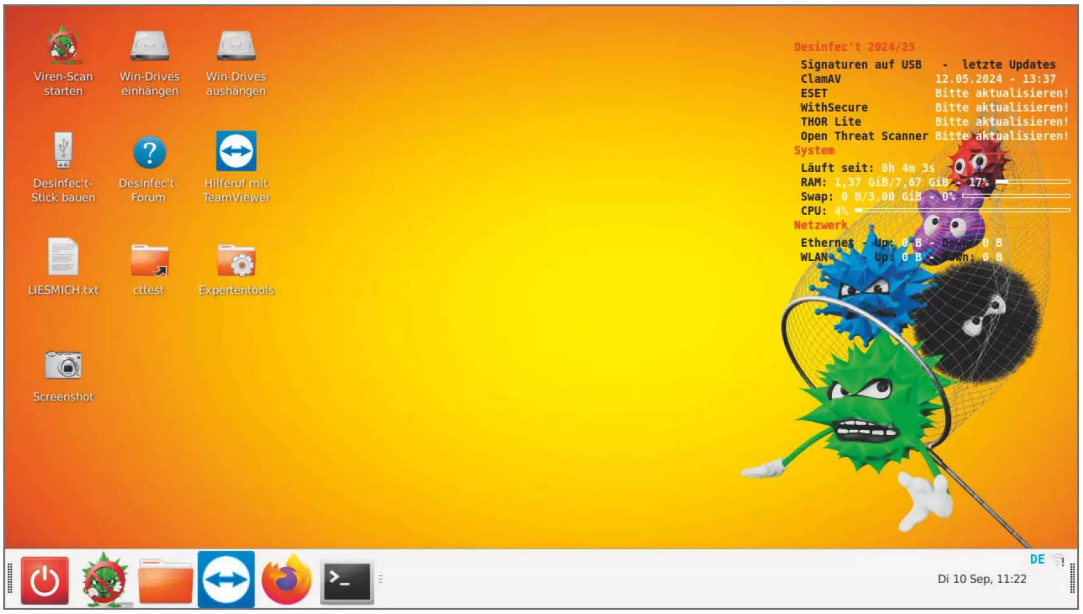
## Keine Angst

Auch wenn der Begriff Linux bei nicht so versierten Computernutzern Fragezeichen über deren Köpfen schweben lässt: Lassen Sie sich davon nicht verunsichern. Wir haben das Sicherheitstool bewusst simpel gehalten und optisch orientiert es sich am Windows-Desktop. Darüber hinaus haben wir viele vom eigentlichen Einsatzzweck ablenkende Linux-Tools entfernt, sodass so wenig wie möglich von der Virenjagd ablenkt. Dementsprechend sollten damit auch Onkels und Tanten zurechtkommen.

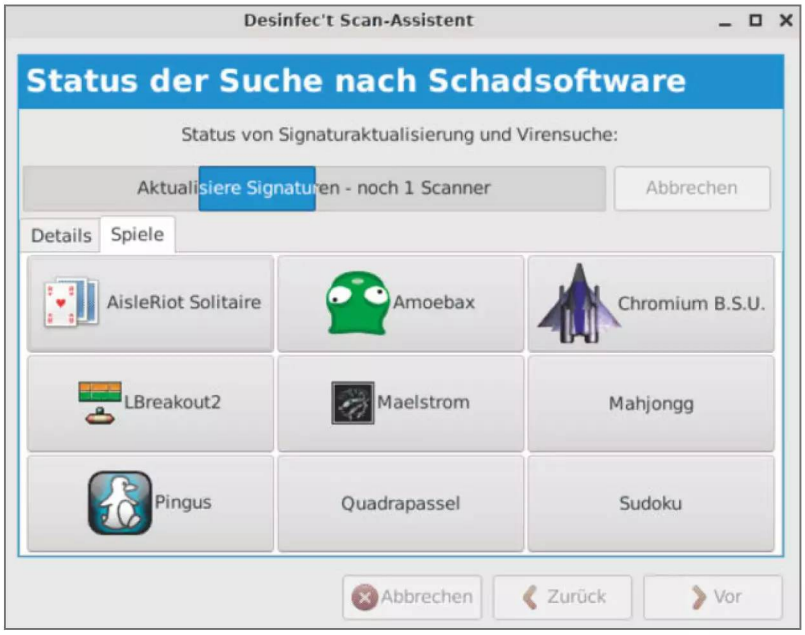
Wer sich trotzdem davon erschlagen und überfordert fühlt, kann mit dem integrierten TeamViewer-Client die Hilfe des Familien-Admins einfordern. Der übernimmt dann über das Internet die Kontrolle über den Problem-PC, um bei der Bedienung zu helfen und die Trojanerjagd einzuleiten. Dafür muss er sich nur den kostenlosen TeamViewer-Client auf seinem PC installieren. In Desinfec't ist der Client ab Werk enthalten.

## Für den Ernstfall gerüstet

Um Windows zu untersuchen, müssen Sie das System lediglich herunterladen und auf einem USB-




**Damit auch Computereinsteiger mit Desinfec't klarkommen, orientiert sich die Optik am Windows-Desktop.**




**Während des Scans vertreiben Sie sich die Zeit mit diversen Mini-Spielen.**

Stick mit mindestens 16 GByte installieren. Das ist gar nicht schwer, schließlich ist unser Installer Desinfect2USB im Download-Archiv enthalten. Wie die Installation im Detail funktioniert und wie Sie Desinfec't statt Windows starten, steht im Artikel „PC-Schädlinge finden und entsorgen".

Die Installation ist in wenigen Minuten erledigt. Da es sich bei Desinfec't um ein Live-System handelt, das direkt aus dem Arbeitsspeicher läuft, sollte Ihr Computer über mindestens 8 GByte RAM verfügen. Vor allem die Scanner machen sich im Zuge der Signaturupdates gerne im Arbeitsspeicher breit.

Theoretisch läuft Desinfec't auch von einer DVD. Das ist aber nicht zu empfehlen, da das System so keine Signaturupdates speichern kann. Demzufolge müssen Sie die Scanner nach jedem Neustart erneut aktualisieren. Außerdem läuft das System von einer DVD fühlbar langsamer. Auf einem USB-Stick überleben die Signaturupdates einen Neustart und die Nutzung geht fühlbar flotter von der Hand. Außerdem speichert der Stick Scanergebnisse.

Weil es unzählige Hardware-Konfigurationen gibt, startet Desinfec't leider nicht auf allen PCs. Wir geben unser Bestes, um die Kompatibilität so groß wie möglich zu halten. Doch das klappt bedauerlicherweise nicht immer. Bei Bootproblemen gibt es für alte, aber auch brandneue Computer spezielle Startoptionen, die Abhilfe schaffen können. Weitere Infos dazu finden Sie im Artikel „PC-Schädlinge finden und entsorgen".

## Virenjagd starten

Haben Sie Desinfec't erfolgreich installiert und gestartet, kann die Trojanerjagd beginnen. Dafür müssen Sie lediglich auf das Icon „Viren-Scan starten" klicken, um den Scan-Assistenten zu starten. Standardmäßig ist nur der Scanner von Eset ausgewählt. Das reicht aber in der Regel aus, damit Sie sich einen ersten Überblick verschaffen können.

Damit die Scanner auch für aktuelle Schädlinge gerüstet sind, muss der zu untersuchende PC mit dem Internet verbunden sein. Ist das gegeben, aktualisieren sich die Virenjäger von Eset und WithSecure automatisch, bevor sie loslegen. Ist das erledigt, können Sie den Stick auch an einem Offline-PC nutzen.

Standardmäßig untersuchen die Scanner alle Laufwerke. Auf Wunsch können Sie sie aber auch nur auf bestimmte Partitionen oder Ordner loslassen. Selbstverständlich können Sie auch am PC angeschlossene Datenträger scannen. Haben Sie keine Angst, etwas kaputtzumachen: Standardmäßig kann Desinfec't nur lesend auf Windows-Festplatten zu-

greifen. Schreibzugriffe und somit Veränderungen am System müssen Sie explizit erlauben.

Ist der Scan beendet, öffnet sich die Ergebnisliste automatisch in Firefox. Dort können Sie die Funde begutachten und etwa über einen Upload zum Online-Analysedienst VirusTotal Fehlalarme eingrenzen. Praktischerweise legt Desinfec't für jeden Computer einen individuellen Projektordner auf dem Stick an, in dem die Scanergebnisse abgelegt werden. So verlieren Sie nicht den Überblick, wenn Sie mehrere Computer im Freundes- und Familienkreis untersuchen.

Aus der Ergebnisliste können Sie entdeckte Trojaner auch unschädlich machen. Dafür löscht Desinfec't die jeweilige Datei nicht, sondern benennt Sie um. Das hat den Vorteil, dass Sie so im Nachhinein doch legitime Dateien mit wenig Aufwand wiederherstellen können.

Beachten Sie aber, dass Desinfec't kein Patentrezept zur kompletten Heilung infizierter PCs ist. Vielmehr dient es als Diagnosetool und Notfallsystem, um Zugriff auf ein nicht mehr startendes Windows zu bekommen.

## Weitere Funktionen

Gerade dieser Fall kann Panik auslösen, wenn auf dem nicht mehr bootenden Computer wichtige Dateien wie Bewerbungen liegen. Aus Desinfec't heraus greifen Sie auf Windows-Festplatten zu, um so persönliche Daten in Sicherheit zu bringen und auf den Stick zu kopieren. Außerdem klonen Profis mit den Expertentools unter anderem ganze Windows-Installationen oder retten sogar verloren geglaubte Dateien, die man aus Versehen gelöscht hat.

Mit weiteren Scannern für erfahrene Virenjäger wie dem Open Threat Scanner (OTS) und Thor Lite Scanner graben Sie noch tiefer nach Trojanern. Wie man die Profi-Scanner am wirkungsvollsten nutzt, beschreibt der Artikel „Neue Malware-Analysetools für Profis".

## Hilfe bekommen

Es ist klar, dass wenn der PC spinnt und vielleicht ein Trojaner im Hintergrund fleißig private Daten kopiert oder verschlüsselt, die Nerven blank liegen. Doch versuchen Sie, nicht in Panik zu verfallen und lesen Sie, um das volle Potenzial von Desinfec't zu nutzen, zunächst konzentriert den Artikel „PC-Schädlinge finden und entsorgen". Dort finden Sie neben Schritt-für-Schritt-Anleitungen auch Lösungen für Probleme bei der Installation und zum Start von Desinfec't.

Wenn auch der Familien-Admin über TeamViewer nicht mehr helfen kann, finden Sie im offiziellen Desinfec't-Forum oft Hilfe (siehe ct.de/waw8). Dort hat die Community schon in vielen Fällen Probleme erfolgreich gelöst. Bei Bugs und Fehlern im System versuchen wir, so schnell wir möglich ein sich automatisch installierendes Update bereitzustellen. (des) c't

**Desinfec't-Forum**
ct.de/waw8

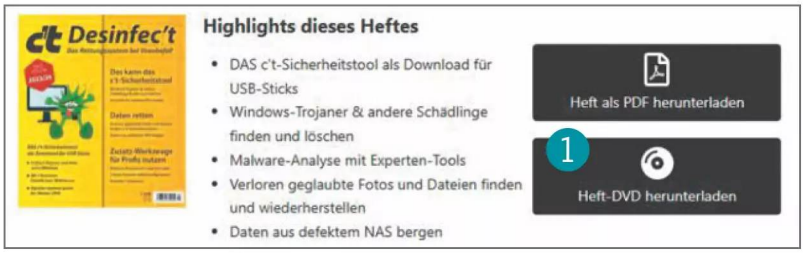
# Desinfec’t 2024/25 im Nu einsetzen

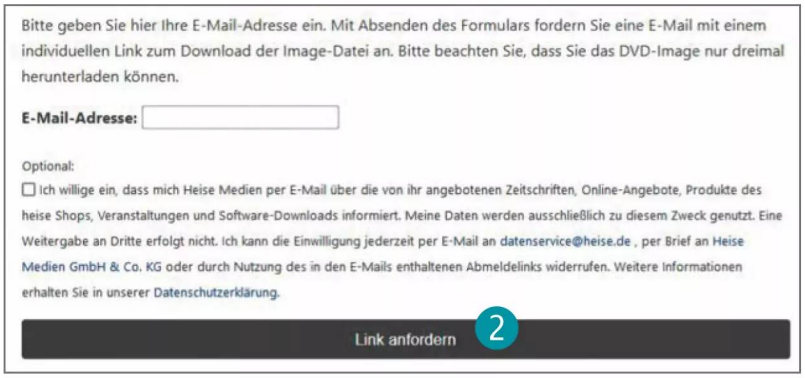
**Um mit dem c’t-Sicherheitstool einen PC zu untersuchen, müssen Sie es nur herunterladen und auf einem USB-Stick installieren. Mit dieser Anleitung ist das gar nicht schwer und in wenigen Minuten erledigt.**

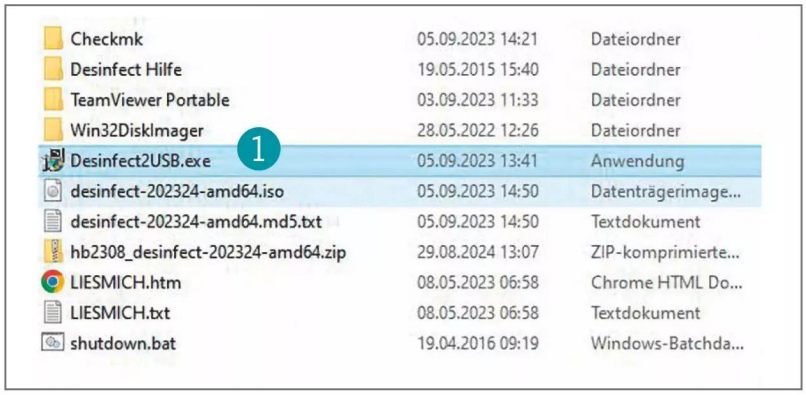
Von **Dennis Schirrmacher**

Herunterladen, entpacken, installieren und starten. Das sind die grundlegenden Schritte, die Sie vor dem Scan eines Windows-Computers erledigen müssen. Läuft Desinfec’t 2024/25, müssen Sie nur noch die Virensignaturen aktualisieren und schon kann die Untersuchung beginnen. Damit Sie dabei nicht den Überblick verlieren, nimmt Sie diese bebilderte Schritt-für-Schritt-Anleitung an die Hand und zeigt Ihnen, wo Sie klicken müssen. Wundern Sie sich in den folgenden Screenshots nicht über abweichende Jahreszahlen. Zum Zeitpunkt der Erstellung dieser Anleitung war Desinfec’t 2024/25 noch nicht final und die Downloadseite war noch offline. Deswegen stammen die Bilder aus der Vorgängerversion. Die Schritte sind aber alle gleich geblieben. (des) *c't*

**Desinfec't 2024/25 herunterladen:** Wenn Sie das Heft als digitale Einzelausgabe bestellt haben, gelangen Sie über den Link aus der E-Mail zur Auftragsbestätigung zum Download von Desinfec't 2024/25. Wenn Sie das Heft am Kiosk gekauft haben, tippen Sie einfach dir URL ct.de/desinfect2024-sh in das Adressfeld eines Webbrowsers. Wenn Sie mit Ihrem heise-Shop-Konto eingeloggt sind, klicken Sie auf „Heft-DVD herunterladen" (1). Haben Sie keinen heise-Shop-Account, landen Sie auf einer anderen Downloadwebsite. Hier müssen Sie lediglich ihre E-Mail-Adresse angeben und dann auf „Link anfordern" klicken (2). Im Anschluss kommt der Downloadlink via Mail. Der Haken im Feld für Werbung von Heise Medien ist optional.

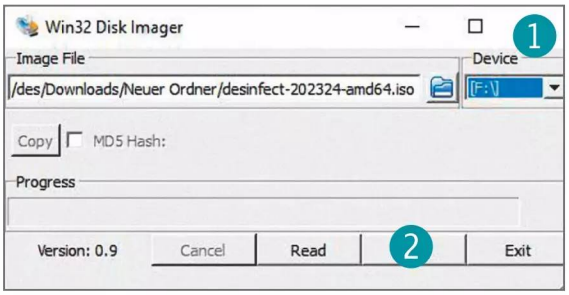


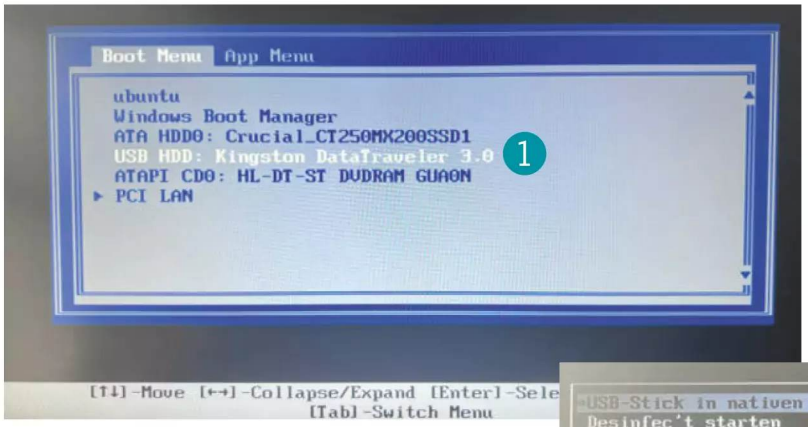



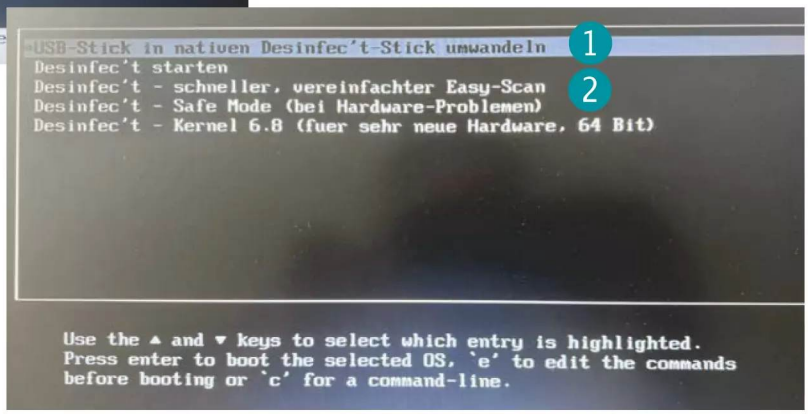

**Installationsassistent starten:** Ist der Download des circa 4 GB großen Archivs mit Desinfec't 2024/25 abgeschlossen, entpacken Sie es. Um nach dem Entpacken mit der Installation auf einem USB-Stick zu beginnen, starten Sie unser Installationstool „Desinfect2USB" mit einem Doppelklick (1). Im Anschluss fragt der Installationsassistent, ob auch wirklich nur der USB-Stick angeschlossen ist, auf dem Desinfec't installiert werden soll. Das ist wichtig, da der ausgewählte Datenträger im folgenden ohne weitere Nachfragen überschrieben wird.

**Desinfec't 2024/25 auf USB-Stick installieren:** Unter „Device" können Sie sicherstellen (1), dass der korrekte Stick ist. Stimmt alles, müssen Sie nur noch auf „Write" klicken (2), damit die Installation startet. Ist der Vorgang abgeschlossen, fragt der Assistent, ob Sie den Computer direkt vom Desinfec't-Stick neu starten wollen. Wundern Sie sich nicht, wenn Windows den Stick nach der Installation nicht anzeigt: Das ist normal, der Stick muss erst im nächsten Schritt umgewandelt werden.





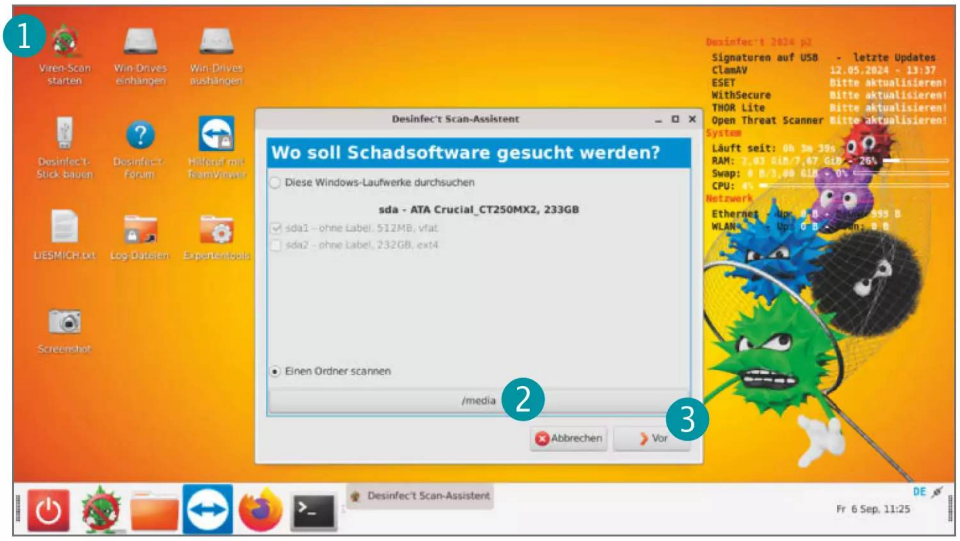

**Desinfec't 2024/25 starten:** Welche Möglichkeiten es gibt, Ihren PC vom Desinfec't-Stick anstatt Windows zu starten, steht im Artikel auf Seite 16. Hier sehen Sie den sichersten Weg über das BIOS-Bootmenü, bei dem ein möglicherweise verseuchtes Windows nicht laufen muss. Wählen Sie an dieser Stelle den USB-Stick mit Desinfec't aus (1). Das Menü sieht übrigens auf PCs von verschiedenen Herstellern anders aus. Auch die Bezeichnung von am PC angeschlossenen USB-Sticks variiert. Lassen Sie sich davon nicht verunsichern.



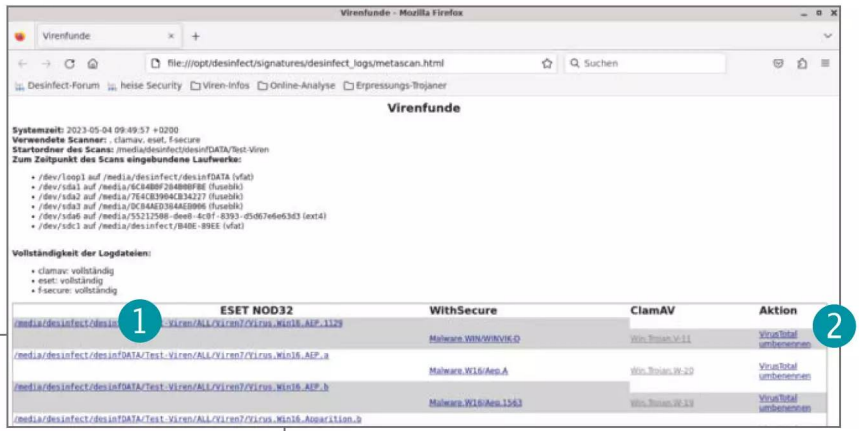

**Desinfec't-Stick einmalig umwandlen:** Damit sich ein Desinfec't-Stick auch aktualisierte Virensignaturen merkt, müssen Sie ihn einmalig umwandeln. Wählen Sie dafür den ersten Punkt aus (1). Ist dieser Vorgang abgeschlossen, wählen Sie in Zukunft stets den Punkt „Desinfec't starten" aus. Alternativ können Sie an dieser Stelle auch „Easy Scan" auswählen (2). Dann startet der PC ohne Umwege mit dem Virenscan mit Eset.

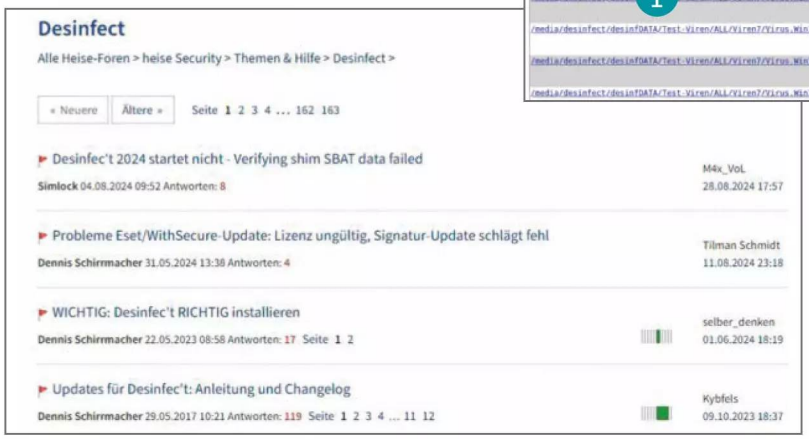

**Nach dem ersten Start:** Booten Sie Desinfec't auf einem Computer das erste Mal, müssen Sie einen Projektordner anlegen (1). Das ist praktisch, wenn Sie den Stick an verschiedenen PCs benutzen. Mit Projektordner-Namen wie „Spiele-PC" oder „Arbeitscomputer" verlieren Sie nicht den Überblick. In diesem Ordner speichert Desinfec't unter anderem Scan-Ergebnisse.

**Virenscan starten:** Damit die Scanner in Desinfec't auch aktuelle Trojaner finden, stellen Sie vor einem Scan sicher, dass der PC online ist. Starten Sie dann durch einen Doppelklick auf das Viren-Scan-starten-Icon auf dem Desktop den Scan-Assistenten (1). In dem Fenster wählen Sie zuerst aus, wie die Scanner suchen sollen. Standardmäßig untersuchen sie die komplette Windows-Installation. Auf Wunsch können Sie unter /media (2) aber auch einzelne Ordner oder externe USB-Speicher auswählen. Um den Scan zu starten, klicken Sie auf „Vor" (3) und im nächsten Fenster auf „Anwenden". Vor jedem Scan aktualisieren sich die Virensignaturen automatisch.




**Trojaner unschädlich machen:** Nach einem erfolgreichen Scan öffnet sich die Liste mit den Ergebnissen automatisch in Firefox. Hier sehen Sie den Dateipfad des Fundes (1). Um Fehlalarme einzugrenzen, laden sie einen Fund zur Online-Analysplattform VirusTotal hoch. Sind Sie sich sicher, dass es sich um einen Trojaner handelt, klicken Sie auf „Umbenennen" um den Virus unschädlich zu machen (2).




**Hilfe finden:** Im Forum helfen Leser Lesern. An dieser Stelle können Sie Probleme diskutieren und hoffentlich lösen. Dort finden Sie auch Information zu Desinfec't-Updates.

# PC-Schädlinge finden und entsorgen

**Wenn Windows komische Dinge tut und Sie befürchten, dass ein Trojaner private Daten abschnorchelt, ist schnelles, aber bedachtes Handeln gefragt. Mit wenigen Handgriffen erstellen Sie einen Desinfec't-Stick, der Ihnen bei der Diagnose hilft und Ihre Daten rettet.**

Von **Dennis Schirrmacher**

Um mit dem Sicherheitstool Desinfec't 2024/25 in Windows Trojaner aufzuspüren und zu erledigen, müssen Sie es lediglich herunterladen, auf einem USB-Stick installieren, Ihren PC vom Stick starten und schon kann die Virenjagd beginnen. Mit den Anleitungen aus diesem Artikel ist das zügig erledigt. Hier finden Sie auch Tipps, um Probleme zu lösen. Außerdem gibt es noch einen Überblick, was Desinfec't noch alles kann.

## Vorbereitungen

Einen möglicherweise infizierten PC untersuchen Sie am besten „von außen" – also nicht mit dem kompromittierten Windows, auf dem der Trojaner eventuell aktiv ist. Hier kommt Desinfec't mit seinem Linux-Live-System ins Spiel, das statt Windows startet. Falls Sie noch keinen Desinfec't-Stick in der Schublade haben, müssen Sie das Sicherheitstool auf einem Stick installieren. Das geht natürlich nicht mit einem potenziell attackierten Computer. Wer keinen Zweit-PC hat, muss die folgenden Schritte beispielsweise am Computer eines Bekannten durchführen.

Wie Sie Desinfec't 2024/25 herunterladen, steht im Kasten „Wie Sie Desinfec't 2024/25 herunterladen". Haben Sie das Archiv auf einer Festplatte gespeichert und entpackt müssen Sie Desinfec't unter Windows mit unserem im Download enthaltenen Tool „Desinfect2USB" auf einen USB-Stick installieren. Der Stick muss dafür über mindestens 16 GByte Speicherplatz verfügen und wird komplett von Desinfec't vereinnahmt. Damit das Sicherheitstool korrekt funktioniert, müssen Sie es zwingend mit unserem Installer installieren. Andernfalls kommt es im Betrieb unweigerlich zu Fehlern und etwa aktualisierte Virensignaturen werden nicht gespeichert. Das bloße Kopieren der Daten auf einen Stick oder mithilfe von Tools wie Rufus funktioniert nicht.

Nur Desinfect2USB legt die für den Betrieb notwendigen Partitionen korrekt an. Die Systempartition setzt sich dabei aus Sicherheitsgründen nach jedem Neustart in den Ausgangszustand zurück. Die Partition für die Virensignaturen kann sich aber Daten merken, genauso wie die unter Windows sichtbare Partition, in der das Tool unter anderem Scanergebnisse speichert.

Um die Installation zu starten, schließen Sie den USB-Stick an Ihren Computer an. Wir empfehlen Ihnen, einen flinken USB-3.0-Stick eines Markenherstellers zu nutzen. Die häufigste Fehlerursache beim Betrieb von Desinfec't sind billige Sticks mit hoher Fehlerrate. Während der Installation läuft eine Prüfung des USB-Sticks. Taucht an dieser Stelle eine entsprechende Warnung auf, sollten Sie, um Probleme im Betrieb vorzubeugen, die Installation abbrechen und einen besseren Stick kaufen.

## Wie Sie Desinfec't 2024/25 herunterladen

Käufer der digitalen Einzelausgabe bekommen mit ihrer Auftragsbestätigung via E-Mail einen Downloadlink für die Zip-Datei mit Desinfec't 2024/25.

Auch Kioskkäufer können Desinfec't herunterladen. Dafür müssen Sie lediglich die Website ct.de/desinfect2024-sh öffnen. Nach der Angabe Ihrer E-Mail-Adresse erhalten Sie einen Downloadlink, der dreimal gültig ist. Bei Problemen wenden Sie sich bitte an leserservice@heise.de.

Um die Integrität des Desinfec't-Downloads sicherzustellen, finden Sie auf der Download-Website Prüfsummen, mit deren Hilfe Sie die heruntergeladene Datei abgleichen bzw. verifizieren können.

Achtung: Desinfect2USB löscht den kompletten Stick, bevor es das Sicherheitstool installiert. Benutzen Sie also einen neuen Stick oder einen mit Daten, die Sie nicht mehr benötigen. Nach einem Doppelklick auf Desinfect2USB öffnet sich der Win32 Disk Imager. Stellen Sie sicher, dass wirklich nur der USB-Stick am PC angeschlossen ist, auf dem Sie Desinfec't installieren wollen. Prüfen Sie im nächsten Schritt im Feld „Device", dass auch wirklich der richtige Stick ausgewählt ist. Das erkennen Sie am Laufwerksbuchstaben, den Sie im Explorer gegenprüfen können. Wählen Sie an dieser Stelle versehentlich ein anderes Laufwerk, wird das im nächsten Schritt ohne weitere Nachfragen überschrieben. Passt alles, klicken Sie auf „Write" und der Installationsvorgang beginnt. Das dauert in der Regel nur wenige Minuten.

## Stick umwandeln

Ist der Vorgang abgeschlossen, zeigt Windows den Stick nicht mehr im Explorer an. Das ist normal und kein Fehler, wundern Sie sich also nicht. Um einen vollwertigen Stick zu erhalten, müssen Sie ihn beim ersten Start einmalig umwandeln. Geschieht das nicht, verhält sich der Stick wie ein nicht beschreib-


**Praktisch: Mittels einer Hardware-ID erkennt Desinfec't verschiedene PCs und legt für jeden Computer einen eigenen Projektordner an, in dem unter anderem die Scanergebnisse gespeichert werden.**

barer DVD-Datenträger und speichert keine aktualisierten Signaturen.

Im Desinfec't-Bootmenü wählen Sie den Punkt „in nativen Desinfec't-Stick umwandeln aus". Der Vorgang dauert nur wenige Minuten. Im Anschluss ist eine Datenpartition unter Windows sichtbar, sodass Sie dort gespeicherte Scanergebnisse einsehen können. Diese Partition dient auch als Speicherplatz für die in Sicherheit gebrachten Daten.

## Installation unter Linux

Alternativ können Sie Desinfec't als root mit folgendem Befehl auch unter Linux installieren: `dd if=desinfect-202401-amd64.iso of=/dev/sdx status=progress`. Anstelle der Kennzeichnung „sdx" müssen Sie die korrekte Bezeichnung Ihres Sticks eintragen. Auch hier gilt: Kontrollieren Sie das lieber doppelt und dreifach, denn bei Angabe eines falschen Ziels zerstören Sie Daten.

Wenn Desinfec't 2024/25 bereits läuft, können Sie für Freunde und Verwandte direkt aus dem laufenden System Sticks erstellen. Das hat den Vorteil, dass auch gleich aktualisierte Signaturen für den neuen Stick übernommen werden. Außerdem müssen Sie einen auf diesem Weg erzeugten Desinfec't-Stick nicht mehr umwandeln.

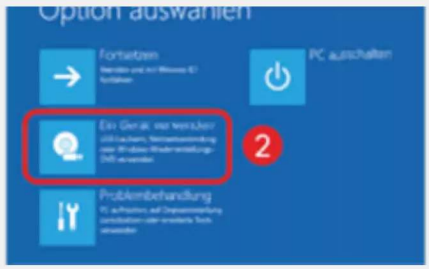
Um einen Stick zu erstellen, klicken Sie auf das Desktop-Icon „Desinfec't-Stick bauen". Wählen Sie nun unter „Ziellaufwerk" den Stick aus. Die Einstellung können Sie so belassen. Klicken Sie auf „Anwenden", um die Erstellung zu starten. Mit einem flinken Stick ist der Vorgang innerhalb weniger Minuten abgeschlossen.

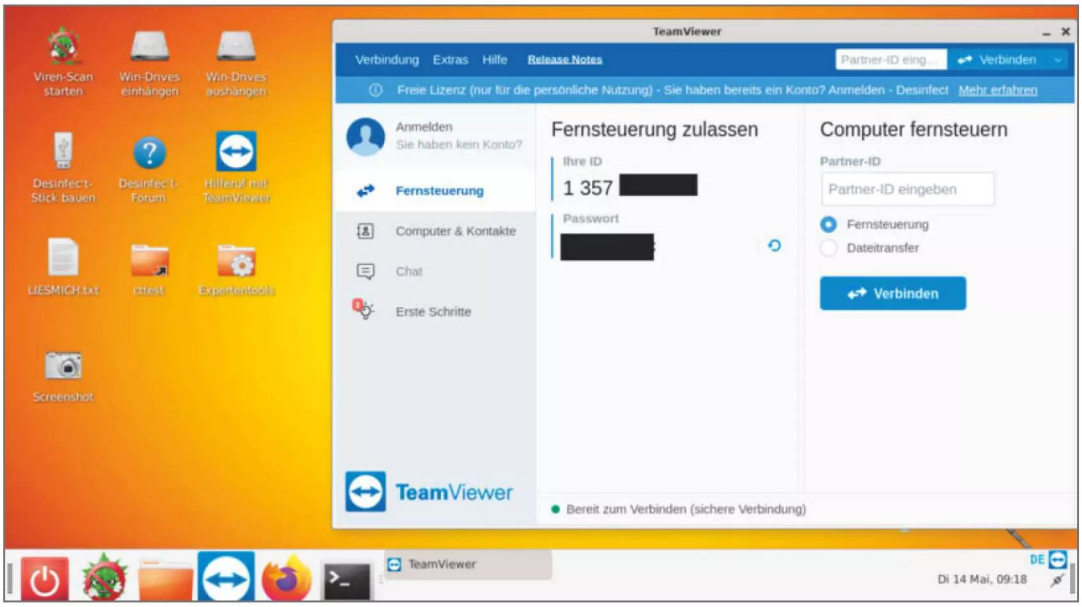
## Desinfec't starten

Vermuten Sie, dass ein Schädling sein Unwesen auf Ihrem Windows-PC treibt, fackeln Sie nicht lange und fahren Sie den Computer herunter. Schließen Sie dann den Desinfec't-Stick an. Schalten Sie den PC wieder ein und drücken sofort entweder F8, F10, F11 oder F12, damit das BIOS-Bootmenü erscheint. Bei manchen Computern rufen Sie dieses Menü mit der Esc- oder Enter-Taste auf. Wenn all das nicht klappt, suchen Sie auf Ihrem Smartphone nach Ihrem Computermodell sowie „BIOS Bootmenü", um die richtige Taste zu finden.

Erscheint das Menü, wählen Sie im Anschluss das Medium mit Desinfec't aus und starten Sie davon. Funktioniert das nicht, müssen Sie den Umweg über das vollständige BIOS-Menü gehen. Dieses rufen Sie meist durch das Drücken der Taste Entf oder F2 auf, aber je nach PC sind auch andere Tasten denkbar.

Im BIOS stellen Sie die Boot-Reihenfolge so ein, dass das Medium mit Desinfec't zuerst startet. Wollen Sie nur einen Routinecheck machen, können Sie Desinfec't auch direkt aus einem Windows 10 oder 11 starten. Das funktioniert aber nur, wenn das System im UEFI-Modus läuft. Dafür halten Sie die Umschalttaste (Shift) gedrückt (1) und klicken im Startmenü auf Neustart. Im anschließend auftauchenden Bildschirm bestätigen Sie den Punkt „Ein Gerät verwenden" (2). Als Nächstes wählen Sie das Medium mit Desinfec't aus (3). Nun fährt Windows herunter und bootet automatisch das Notfallsystem. Klappt der Start partout nicht, wählen Sie bitte im Desinfec't-Bootmenü die Option „Safe Mode" aus.


**Wenn Sie gar nicht mehr weiterkommenden, rufen Sie mit dem integrierten TeamViewer-Client den Familien-Admin zuhilfe, der sich über das Internet mit dem PC-Problem verbindet und den Computer dann fernsteuert.**

Wenn Sie einen Stick für Computerneulinge erstellen wollen, wählen Sie die Option „Easy Scan“ aus. Ein derartiger Desinfec’t-Stick startet direkt in den Scanmodus und der Scanner von der Eset untersucht automatisch die gesamte Windows-Festplatte.

Profis können in den Optionen auch einen Btrfs-Stick erstellen (siehe Artikel „Desinfec’t via Btrfs erweitern“. Mittels der Snapshot-Funktion des Btrfs-Dateisystems ist es möglich, den Stick dauerhaft mit selbst installierten Anwendungen oder Treibern auszustatten. Dafür benötigen Sie aber einige Linux-Kenntnisse.

## Der Start

Damit Sie die Scanner aus Desinfec’t auf eine Windows-Installation loslassen können, müssen Sie Ihren PC vom Stick statt der Festplatte starten. Wie das im Detail funktioniert, erklärt der Kasten „Desinfec’t starten“. Damit das System auf so vielen PCs wie möglich bootet, führen wir Tests mit verschiedenen PCs und Laptops der vergangenen Jahre durch. Dabei prüfen wir unter anderem, ob Festplatten/SSDs erkannt werden und eine WLAN-Verbindung möglich ist. Wir testen auch die Aktualisierung der Virensignaturen und das Scannen von Festplatten. Weil es aber in der PC-Welt unzählige Hardwarekombinationen gibt, können wir leider nicht garantieren, dass Desinfec’t auf allen Computern startet.

Wenn der Start mit den Standardeinstellungen nicht klappt, haben Sie im Desinfec’t-Bootmenü zwei alternative Startoptionen. Wenn Ihr PC sehr neu ist, probieren Sie mal den Eintrag 6.10-Kernel aus. Der bringt noch weitere Treiber mit. Als letzte Möglichkeit gibt es noch die Safe-Start-Option.

Leider kann es in naher Zukunft zu Startproblemen kommen, die aber nicht auf unsere Kappe gehen: Weil Microsoft derzeit am Schutzmechanismus Secure Boot werkelt, könnte Desinfec’t auf manchen Systemen bald den Start verweigern. Da der Prozess noch nicht abgeschlossen ist, bleibt vieles noch im Unklaren (siehe Kasten „Secure-Boot-Problem: Linux ausgesperrt“). Wir werden die Entwicklung jedoch aufmerksam verfolgen, und wo möglich Probleme mit Updates entschärfen.

## Viren jagen

Nach dem Start von Desinfec’t geben Sie im automatisch auftauchenden Feld den Namen des Projektordners an. Desinfec’t erkennt PCs an einer Hardware-ID und so können Sie für mehrere Computer verschiedene Projektordner wie „Spielemaschine“ oder „Homeoffice-PC“ anlegen, damit Sie nicht den Über-

## Das ist neu in Desinfec't 2024/25

- Gratis Signaturupdates bis Oktober 2025
- Neue Malwareanalyse-Tools wie FLOSS
- Zahlreiche Verbesserungen bei den Skripten, insbesondere Persistenz und Signaturupdates
- Kernel 6.8 (optional 6.10 für neue Hardware)

blick verlieren. In dem Ordner werden unter anderem die Scanergebnisse gespeichert. Sie können dort aber auch dauerhaft etwa Screenshots ablegen.

Bevor Sie die Trojanerjagd starten, müssen Sie die Virensignaturen auf den aktuellen Stand bringen. Damit ausgerüstet kommen die Scanner auch aktuellen Bedrohungen auf die Spur. Dazu muss das System entweder per LAN oder WLAN mit dem Internet verbunden sein. Falls es zu Fehlern bei der Aktualisierung kommt, lesen Sie bitte den FAQ-Beitrag „Probleme beim Signaturupdate“. (siehe Artikel „Desinfec't 2024/25“

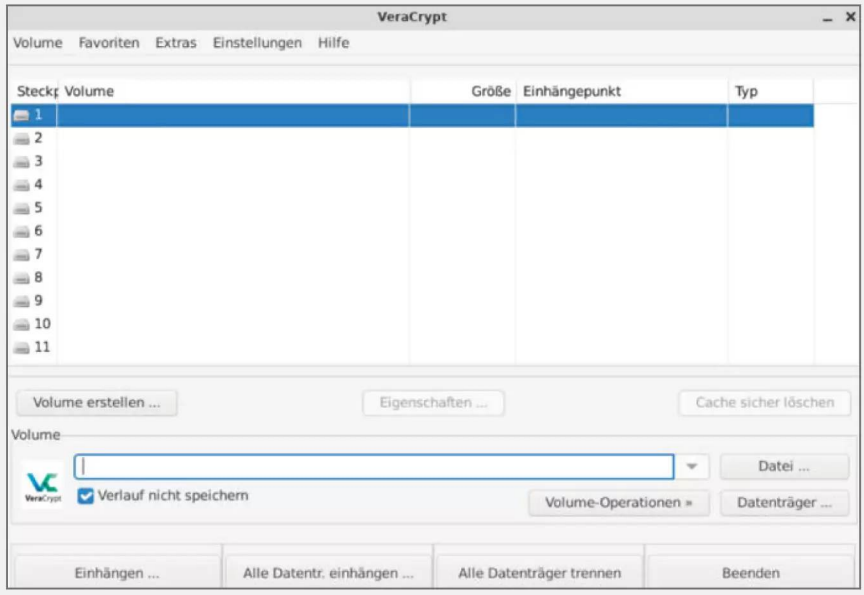
Öffnen Sie nun den Scan-Assistenen über das Icon auf dem Desktop „Viren-Scan starten“, der eine

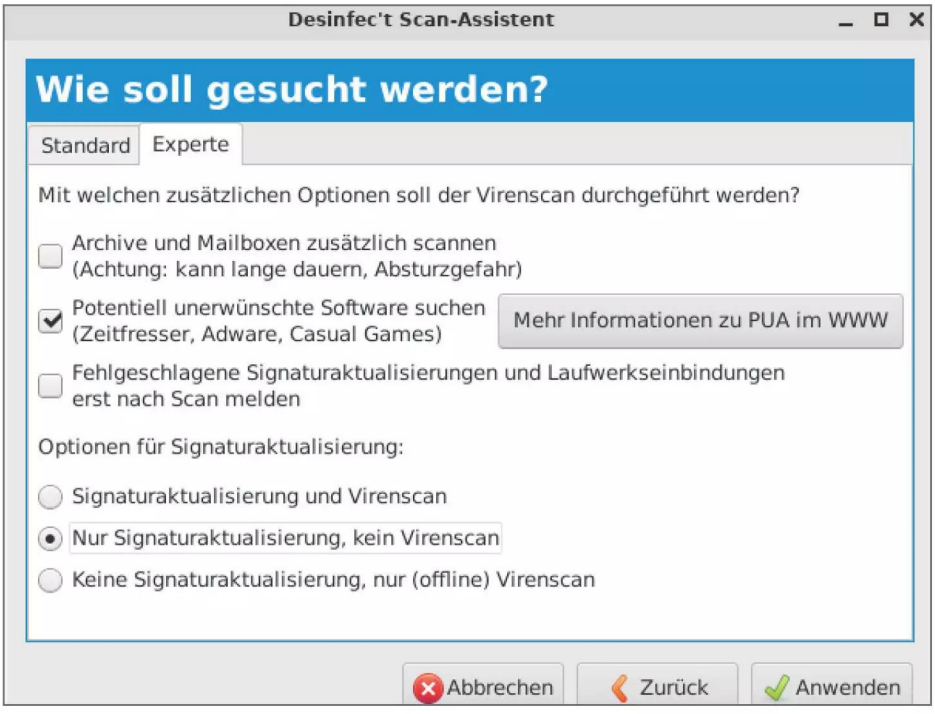
## Verschlüsselte Festplatten scannen

Wer seine Festplatte mit Microsofts Bitlocker verschlüsselt hat, kann das Laufwerk direkt aus dem Scan-Assistenten heraus einbinden. Dafür müssen Sie es lediglich auswählen und nach den Scanner-Updates das Bitlocker-Passwort eingeben. Das klappt auch, wenn Sie den PC via TPM entsperren und den 48-stelligen Wiederherstellungsschlüssel eingeben.

Im Test hat das in der Redaktion problemlos mit einer unter einem aktuellen Windows 10 und 11 verschlüsselten Systempartition und mit einem USB-Stick geklappt. Mit kommenden Windows-Updates könnte es aber nicht mehr funktionieren. Das Problem ist, dass Microsoft in Windows-Updates manchmal an der Bitlocker-Schraube dreht und die Entwickler der Mount-Tools unter Linux erst mal nachziehen müssen. Wenn das erfolgt ist, bringen wir Desinfec't auf den aktuellen Stand.

Wer mit VeraCrypt verschlüsselte Daten scannen möchte, muss die Container beziehungsweise Laufwerke über den VeraCrypt-Client im Expertentools-Ordner einbinden. Um Festplatten einzubinden, müssen Sie VeraCrypt starten. Nun wählen Sie den verschlüsselten Datenträger aus und mounten diesen im VeraCrypt-Client. Die Festplatte taucht dann im Scan-Assistent zur Auswahl auf. Haben Sie Ihre Systemplatte komplett verschlüsselt, müssen Sie noch die Option „Partition mithilfe der Systemverschlüsselung einhängen (Pre-Boot Authentifizierung)“ auswählen. Im Scan-Assistenten taucht die Festplatte aber nicht als Windows-Partition auf, sondern Sie müssen sie über „einen Ordner scannen“ auswählen.






**Auf Wunsch können Sie nur die Virensignaturen aktualisieren ohne einen anschließenden Scan durchzuführen. Das ist praktisch, wenn Sie einen Offline-PC untersuchen wollen.**

Internetverbindung herstellen will. Wählen Sie an dieser Stelle Ihr WLAN aus und geben Sie das Passwort ein. Auf Wunsch speichern Sie es über die entsprechende Option. Entscheiden Sie sich dafür, verbindet sich Desinfec't nach jedem Start automatisch mit dem WLAN. In diesem Fall liegt das Passwort aber im Klartext auf dem Stick, und gerät er in falsche Hände, ist das WLAN-Passwort verbrannt. Alternativ gelingt die Verbindung auch ohne Speicherung des Kennworts. Dafür müssen Sie nach jedem Neustart auf das WLAN-Symbol in der Taskleiste unten rechts klicken und das Passwort eingeben.

Im nächsten Fenster des Scan-Assistenten selektieren Sie die zu scannenden Laufwerke. Anschließend wählen Sie die Scanner aus, die Windows untersuchen sollen. Verfallen Sie nicht gleich in Panik, wenn die Scanner Alarm schlagen: In der sich automatisch in Firefox öffnenden Ergebnisliste studieren Sie die Funde und kommen möglichen Fehlalarmen auf die Spur. Das sind Meldungen der Virenscanner, die harmlose Dateien verdächtigen; vor allem ClamAV neigt dazu. Um das eingrenzen zu können, klicken Sie in der Liste auf „VirusTotal“, um den Fund zum Analyseservice hochzuladen. Dort schauen nochmal mehr als 60 Online-Scanner auf die Datei und geben eine Einschätzung ab. Außerdem finden Sie dort in einigen Fällen auch Kommentare von anderen Uploadern, die bei der Einordnung eines Fundes helfen können.

## Funktionsumfang ausreizen

Beachten Sie, dass Desinfec't ein von einem Virus zerfressenes Windows nicht reparieren kann. Es ist vielmehr ein Diagnose- und Datenrettungstool. Mit dem auf Yara-Regeln basierenden Open Threat Scanner (OTS) und dem Thor Lite Scanner haben Sicherheitsprofis mächtige Werkzeuge an der Hand, um Systeme tiefgehend zu untersuchen. Wie, erklärt der Praxisartikel „Profi-Scanner effektiv nutzen“.

Mit den Werkzeugen aus dem Expertentools-Ordner retten Sie unter bestimmten Bedingungen Daten mit Photorec, klonen ganze Festplatten und bearbeiten mit Fred die Windows Registry. Aber Vorsicht: Wie der Ordnername schon sagt, sollten man die Werkzeuge nur nutzen, wenn man genau weiß, was man tut. Andernfalls kann man damit richtig was kaputt machen. (des) c't

# Desinfec’t 2024/25

**Das c’t-Sicherheitstool leistet Hilfe, wenn Trojaner Windows auseinandernehmen. Im Betrieb kann es immer mal wieder zu Problemen kommen, die in der Regel aber mit diesen Tipps schnell gelöst sind.**

Von **Dennis Schirrmacher**

**? Wenn ich die Signaturen des Scanners WithSecure aktualisieren will, kommt oft die Fehlermeldung, dass die Lizenz ungültig ist. Mit ClamAV und Eset klappt das Update hingegen problemlos. Was läuft da schief?**

! Um das zu erklären, müssen wir etwas weiter ausholen: Desinfec’t basiert auf der Linux-Distribution Ubuntu und dementsprechend laufen nur mit Linux kompatible Scanner. Davon gibt es mittlerweile nicht mehr so viele. WithSecure bietet zum Glück noch einen an, der auch noch mit überzeugenden Scan-Ergebnissen punktet. Jetzt kommt das Aber: Der Scanner ist für den Einsatz auf einem Mail- oder Dateiserver ausgelegt. In so einem Szenario läuft der Update-Daemon konstant durch, die einzelnen Update-Schritte sind eher klein. Beim Einsatz von Desinfec’t müssen jedoch auf einen Schlag Updates für Wochen oder gar Monate geladen und installiert werden, was dann deutlich länger dauert und zu Timeouts oder anderen unerwarteten Problemen führen kann.

Aufgrund der bereits erwähnten Treffsicherheit haben wir uns trotz der Problematik für eine Integra-


**Neben mit VeraCrypt verschlüsselten Festplatten können Sie auch Bitlocker-Laufwerke untersuchen. Das Einbinden klappt direkt aus dem Scan-Assistenten.**

tion in Desinfec't entschieden, die wir auch stetig verbessern. In Desinfec't 2024/25 haben wir vorsorglich die Timeouts erhöht und lassen das Update-Skript für Nutzer leichter zu verstehende Fehlermeldungen und Handlungsanweisungen ausgeben. Die erhöhten Timeouts bedeuten, dass bei der Auswahl aller Scanner der Aktualisierungsvorgang bis zu einer Stunde einfordern kann, bevor der Virenscan starten kann. Wenn Sie nicht so lange warten wollen, können Sie zunächst einen Virenscan mit anderen Scannern durchführen und parallel die Signaturen von WithSecure aktualisieren. Der Scan-Assistent aktualisiert die Signaturen automatisch.

Sie können das Signatur-Update von WithSecure im Terminal aber auch händisch anstoßen: `sudo/opt/desinfect/update_withsecure.sh`. Gelingt das Update nicht, versucht der Update-Daemon im Hintergrund weiterhin die Update-Server zu kontaktieren. Sie können in diesem Fall einfach warten. Sind die Signaturen erfolgreich heruntergeladen, zeigt der Systemmonitor rechts oben auf dem Desinfec't-Desktop ein aktuelles Datum der Signaturen an.

In den Fällen, in denen das Bootstrapping oder die Lizenzaktivierung fehlschlägt, gibt das Skript am Ende Meldungen aus, was Sie unternehmen müssen. Bei einer fehlgeschlagenen Aktivierung genügt es, das Update-Skript zu einem späteren Zeitpunkt noch einmal aufzurufen. Bei misslungenem Bootstrapping müssen die Signaturen von WithSecure zurückgesetzt (siehe entsprechendes Skript aus dem Expertentools-Ordner) und Desinfec't muss neu gestartet werden. Dann kann ein weiterer Versuch erfolgen.

## Desinfec't-Installation schlägt fehl

**? Ich habe das Archiv mit Desinfec't 2024/25 heruntergeladen und halte mich penibel an die Installationsanleitung im Heft. Aber immer, wenn ich Desinfect2USB ausführen will, verweigert mein Windows-PC die Installation mit der Fehlermeldung „Error 5: Zugriff verweigert". Was mache ich falsch?**

! Sie machen gar nichts falsch. Schuld an dem Fehler ist ein übereifriger Virenscanner oder bestimmte Komponenten von Acronis-Software. Die wollen eigentlich Gutes tun und den für die Desinfec't-Installation am Computer angeschlossenen USB-Stick vor bösartigen Löschversuchen schützen. Das ist in diesem Fall natürlich unangebracht und

Sie müssen die Echtzeitüberwachung temporär für die Installation des Sicherheitstools auf einem Stick deaktivieren. Vergessen Sie aber nicht, den Schutzmechanismus nach der Installation wieder einzuschalten.

## Desinfec't startet nicht

**? Ich habe Desinfec't erfolgreich auf einem Stick installiert. Nun taucht der Stick aber unter Windows nicht auf und ich kann das Sicherheitstool dementsprechend nicht starten. Habe ich da etwas übersehen?**

! Dass der Stick nach der Installation unter Windows nicht sichtbar ist, ist vollkommen normal. Sie müssen verstehen, dass Desinfec't keine Windows-Anwendung ist, die Sie über einen Doppelklick starten. Es bringt sein eigenes Live-Linux-System mit, das direkt vom Stick statt Windows startet. Wie das geht, steht im Artikel „PC-Schädlinge finden und entsorgen" im Kasten „Desinfec't starten". Nach dem ersten Booten des PCs vom Stick müssen Sie ihn einmalig umwandeln. Erst dann ist Desinfec't voll funktionstüchtig und der Stick beziehungsweise dessen Datenpartition ist auch wieder unter Windows sichtbar. In der im Explorer angezeigten Partition können Sie übrigens Ihre Daten von verseuchten PCs in Sicherheit bringen und auf einen anderen PC kopieren.

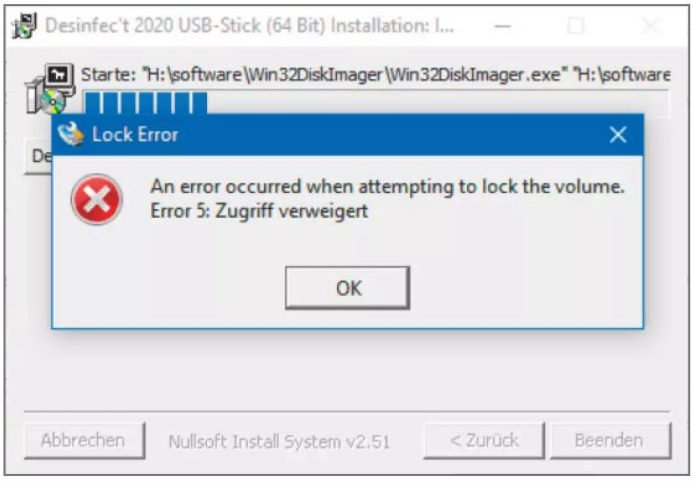
## Zu neue Hardware für Desinfec't?

**? Ich habe mir jüngst einen PC mit brandneuen Komponenten zusammengestellt. Leider startet Desinfec't auf meinem Computer nicht. Gibt es dafür vielleicht einen Workaround?**

! Um die Kompatibilität mit aktueller Hardware wie Prozessoren und NVME-SSDs zu erhöhen, haben wir neben dem standardmäßig aktiven Linux-Kernel 6.8 und noch den 6.10er-Kernel implementiert. Dieser bringt noch weitere Treiber mit. Um Desinfec't damit zu starten, wählen Sie im Desinfec't-Bootmenü einfach den passenden Eintrag aus.

## Verschlüsselte Festplatte nicht sichtbar

**? Ich habe meine Windows-Festplatte vollständig mit VeraCrypt verschlüsselt. Leider kann ich die Partition nicht scannen.**




**Einige übereifrige Virenscanner wollen USB-Sticks vor einem bösartigen Löschen schützen. Damit Sie Desinfec't installieren können, pausieren Sie den Virenwächter für die Dauer der Installation.**

! Starten Sie VeraCrypt innerhalb von Desinfec't im Expertentools-Ordner und wählen die verschlüsselte Festplatte aus. Bei einer Vollverschlüsslung von Windows müssen Sie noch den Punkt „Mount partition using system encryption" aktivieren. Nach der Eingabe des Passworts für die verschlüsselte Platte sollte diese im Scan-Assistenten auftauchen. Mit Bitlocker verschlüsselte Laufwerke binden Sie direkt über den Scan-Assistenten ein.

## Leerer Desktop

**? Ich habe Desinfec't 2024/25 erfolgreich auf einem USB-Stick installiert und gestartet. Leider sehe ich nur einen leeren Desktop und kann mit dem System so nichts anfangen. Was läuft da schief?**

! Das klingt so, als hätten Sie an Ihren PC zwei Monitore angeschlossen und einen nicht eingeschaltet. Offensichtlich stuft Desinfec't den ausgeschalteten Bildschirm fälschlicherweise als primären Monitor ein und zeigt dort den vollständigen Desktop an. Ziehen Sie mal den Stecker vom zweiten Monitor und starten Sie das System neu. Dann sollte es klappen. des) *ct*

**Hilfe im Desinfec't-Forum**
**ct.de/wnja**

inside agile

# 7. PRODUCT OWNER DAY

## So geht agiles Produktmanagement besser

## 4. November • Online

Product Owner und Produktmanagerinnen stellen sicher, dass die **richtigen Produkteigenschaften** ausgewählt werden.

Beim **siebten Product Owner Day** geht es um folgende Themen:

- Produktstrategie richtig anwenden
- Agilität trifft Unternehmenskultur
- Startup-Erfahrungen: Customer Focus & Product-Market-Fit
- Die Product-Owner-Rolle skalieren
- Praxis: Vom liebgewonnenen Altsystem zur zukunftsfähigen Software

Die Konferenz richtet sich an **Product Owner** und **Produktmanagerinnen,** die die agilen Grundlagen kennen und bereits Erfahrung in der Rolle mitbringen.

**pod.inside-agile.de**

Jetzt Tickets mit **Frühbucher-rabatt** sichern!

**Workshops am 5. und 6. November zu High-Impact-Teams und OKR**

Veranstalter

iX Magazin für professionelle IT

dpunkt.verlag

Kooperationspartner

Agile Academy

it-agile

Die Produktwerker

# Trends bei Trojanern & Co.

**Was hat sich im Bereich Ransomware getan? Welche Malwaretypen sind derzeit auf dem Vormarsch, und welche Angriffswege gilt es besonders im Auge zu behalten? Um diese und weitere Fragen zu klären, durchkämmt dieser Artikel die aktuelle Malware-Landschaft.**

Von **Olivia von Westernhagen**

Cyberkriminalität ist weiterhin auf dem Vormarsch: Laut Bundeslagebild Cybercrime des Bundeskriminalamts (BKA) ist die Zahl der Straftaten in diesem Bereich 2023 im Vergleich zum Vorjahr erneut gestiegen. Die Angriffsszenarien sind vielfältig: Politisch motivierte DDoS (Distributed Denial of Service)-Attacken legen Behörden-Websites lahm, Betrüger ziehen ihren Opfern mittels Social Engineering Geld aus der Tasche und „Crime-as-a-Service"-Angebote aus dem Darknet machen Online-Erpressungen für jeden durchführbar und erschwinglich. Dabei spielt Malware in verschiedenen Ausführungen nach wie vor eine große Rolle.

Eine der Anlaufstellen für unsere Recherchen ist das unabhängige Forschungsinstitut für IT-Sicherheit AV-TEST. Das führt Statistiken zu neu entdeckten Mal-

ware-Samples, die es vorrangig aus einer Art Ringtausch mit AV-Herstellern bezieht. Seit Jahresanfang kamen dabei insgesamt 62.603.359 neue Schadcode-Dateien sowie 2.993.211 PUA zusammen. Das klingt erst einmal extrem viel; zu beachten ist aber, dass schon winzige Veränderungen am Code aus einem alten ein neues „Unique Sample“ machen. Neue Funktionen oder gar Malware-Familien sind hierfür nicht notwendig.

Hinter der Abkürzung PUA verbergen sich „potenziell unerwünschte Anwendungen“, die etwa verborgen in einem undurchsichtigen Installer, zusammen mit seriösen Programmen auf den Rechner gelangen. PUA sind nicht schädlich, können aber die PC-Performance beeinträchtigen und durch Werbung oder andere Einblendungen schlichtweg nerven.

## Malwareverteilung & -typen

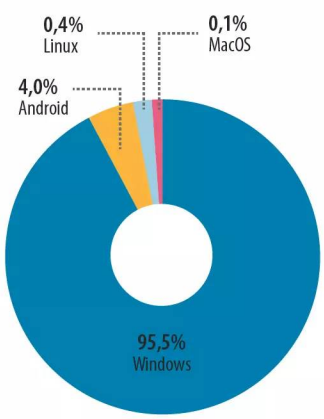
Die prozentuale Verteilung aller Neuzugänge inklusive PUA auf verschiedene Betriebssysteme birgt zunächst einmal keine Überraschungen: Mit einem Anteil von 95,5 Prozent ist Windows weiterhin das mit Abstand beliebteste Angriffsziel. Angriffe auf dieses Betriebssystem haben sich jahrzehntelang bewährt und versprechen dank seines weiterhin höchsten Marktanteils im Desktop-PC-Bereich eine große Reichweite. Aktuellen Werten von Statista zufolge ist Microsofts Betriebssystem in Deutschland auf rund 76 Prozent der Desktop-PCs und Notebooks installiert.

Auf Android als Marktführer unter den mobilen Betriebssystemen entfallen hingegen nur fünf Prozent der Samples: Die Zahl neu entdeckter Samples für Googles Linux-basiertes Betriebssystem ist bereits 2022 stark zurückgegangen und seither stagniert. Wichtiger Gründe hierfür dürften die immer strenger werdenden Sicherheitsmechanismen von Googles Play-Store sowie die Tatsache darstellen, dass Nutzer nach und nach auf neue Geräte mit von Haus aus besser abgesicherten Android-Versionen umsteigen.

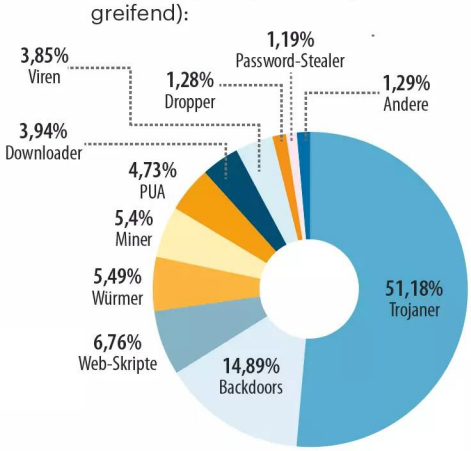
Bei betroffenen Linux-Systemen, auf die lediglich 0,4 Prozent der frisch erfassten Samples abzielten, handelt es sich laut AV-TEST größtenteils um Server sowie um Internet-of-Things (IoT)-Geräte - etwa im

**Durch AV-TEST neu erfasste Schadcode- und PUA-Samples von Jahresbeginn bis inklusive 31.7.2024**

Prozentual aufgeschlüsselt nach Betriebssystem:




Prozentual aufgeschlüsselt nach Malware-Typen (betriebssystemübergreifend):




**Weil Windows auf Desktop-PCs und Notebooks nach wie vor sehr weit verbreitet ist, bleibt es ein beliebtes Angriffsziel für alle Malware-Varianten.**

Verhältnis 50:50. Das Schlusslicht im positiven Sinne bildet macOS mit einem verschwindend geringen Anteil von 0,1 Prozent. Apples mobiles Betriebssystem iOS ist bislang aufgrund allzu weniger Sample-Funde überhaupt nicht Teil der Statistik.

Malware-Kategorien fasst AV-TEST oftmals unter generischen Erkennungen zusammen, die die Eigenschaften und Fähigkeiten des entdeckten Codes beschreiben. Betrachtet man die betriebssystemübergreifende „Top 10" der Malware-Kategorien in Bezug auf ihren Anteil an neu entdeckten Samples, so machen Trojaner mehr als 50 Prozent aller Funde aus. Der Begriff beschreibt definitionsgemäß Schadsoftware, die sich als nützliches Programm tarnt.

Dahinter folgen mit knapp 15 Prozent Schädlinge, die eine Hintertür auf Systemen öffnen. Unter den übrigen, kleineren Gruppen sind noch Miner erwähnenswert: Sie scheffeln heimlich Kryptowährungen auf infizierten PCs und erzeugen gelegentlich – höchstwahrscheinlich kursabhängig – den einen oder anderen Peak in den Statistiken.

## Ransomware unverändert gefährlich

„Und was ist mit Ransomware?", wird sich manch eine(r) nun fragen. Denn in der besagten Top 10 taucht erpresserischer Schadcode nicht auf. Ein für die Statistiken verantwortlicher Mitarbeiter schätzt den Ransomware-Anteil an allen neu erfassten Windows-Malwaresamples (ohne PUA) auf rund vier Prozent – allerdings unter Berücksichtigung der Tatsache, dass die automatische Kategorisierung diese aufgrund spezifischer Eigenschaften mitunter anders einordnet.

Wer hinter diesem eher kleinen Anteil eine geringe Relevanz erpresserischen Codes vermutet, liegt jedoch komplett falsch. Denn schließlich lässt die bloße Anzahl neuer Unique Samples keinerlei Rückschlüsse auf die Gefährlichkeit einer Malware-Kategorie zu. Am ehesten lässt sich daraus schließen, dass die überschaubare Zahl großer Player der Ransomware-Welt mit dem bereits vorhandenen Material so gut fährt, dass ständige Modifizierungen oder gar komplett neuer Code weitgehend überflüssig sind.

Ransomware, vom BKA im Bundeslagebild Cybercrime für 2023 als „primäre Bedrohung" bezeichnet, befindet sich unverändert auf Erfolgskurs. Und sie ist nach wie vor die Cashcow für Cyberkriminelle, die damit Millionenbeträge erpressen. Daran haben auch zwei großangelegte Operationen internationaler Strafverfolgungsbehörden nicht viel geändert: Im Februar dieses Jahres gelang es Ermittlern im Zuge der Operation „Cronos", die Darknet-Präsenz der Ransomware-Gang Lockbit zu übernehmen, deren mutmaßlichen Kopf zu enttarnen und tausende Keys für die Entschlüsselung sicherzustellen. Im Bundeslagebild hatte das BKA Lockbit als gefährlichste Ransomware-Bedrohung aufgeführt. Auf Cronos folgte im Mai die Operation „Endgame" gegen sechs Schadsoftware-Familien, die als sogenannte Dropper vielfach auch Ransomware verteilten.

Anders als in vielen Medienberichten geschildert, wurde Lockbit durch Cronos aber nicht etwa zerschlagen; Die Erpresser sind nach wie vor aktiv. Zu beobachten ist derzeit allerdings eine Verschiebung der Kräfteverhältnisse innerhalb der Ransomware-Szene: Gangs wie etwa Phobos oder die recht neue Gruppe RansomHub haben von Lockbits Schwächung profitiert. Wie ihr großer Konkurrent verfolgen auch sie das überaus beliebte Modell von „Ransomware-as-a-Service" (RaaS), bei dem der erpresserische Code, meist nebst kompletter Infrastruktur und Konfigurationsmöglichkeiten, an zahlende Kunden vermietet wird.

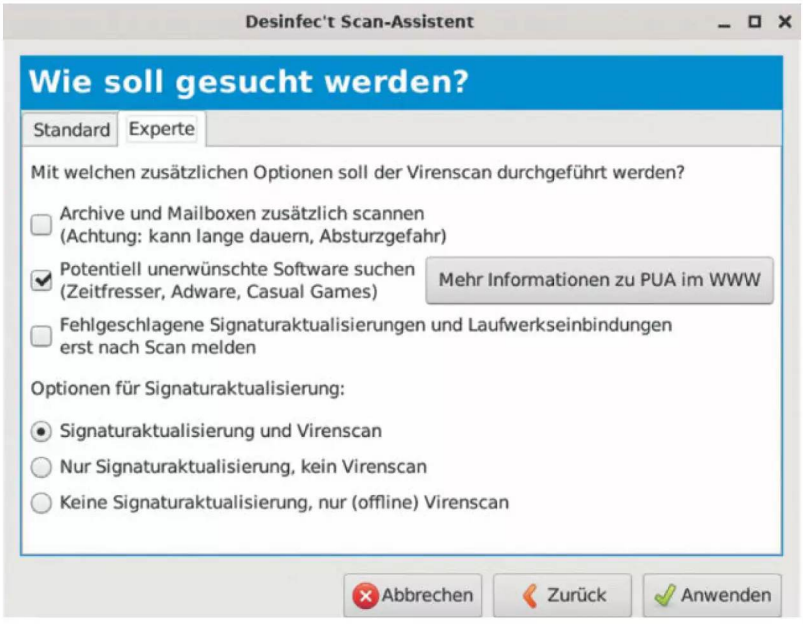
Im Fokus der Angriffe stehen weiterhin größtenteils große Unternehmen sowie Behörden und Verwaltungen. Sie sind in der Lage, sehr hohe Lösegelder zu zahlen. Zudem stehen sie unter größerem Zugzwang, da sie in hohem Maße auf eine funktionierende IT-Infrastruktur angewiesen und mit der Veröffentlichung interner Daten besonders gut erpressbar sind.

Auch wenn – oder gerade weil – die Häufigkeit von Angriffen auf Privatpersonen schwer zu beziffern ist, sollten sich diese aber nicht allzu sehr in Sicherheit wiegen. Denn auch sie können, etwa im Zuge einer breit gestreuten RaaS-Kampagne per E-Mail, jederzeit Opfer von Ransomware werden.

## Informationsdiebstahl nimmt zu

Das Prinzip der doppelten Erpressung mittels Verschlüsselung und kopierter Daten mit der Androhung von Datenleaks ist in den vergangenen Jahren zum Standard geworden. Doch nicht nur Ransomware-Macher schlagen Profit aus sensiblen Informationen: Unter Windows ist den AV-TEST-Zahlen zufolge seit August vergangenen Jahres ein Malware-Typ im Kommen, den der übergeordnete Begriff „Infostealer" recht gut charakterisiert.

Zwei Sample-Gruppen, die das Forschungsinstitut den Malware-Familien Berbew und Padodor zuord-




**Die Suche nach PUA kann man im Scan-Assistent auf Wunsch abwählen.**

net, machen im aktuellen Jahr zusammen rund 24 Prozent des beobachteten Gesamtaufkommens unter Windows aus. Damit liegen sie zahlenmäßig direkt hinter der bei diesem Betriebssystem führenden Kategorie „Agent“ (30 Prozent). Es handelt sich dabei um eine generische Bezeichnung, die von vielen AV-Herstellern verwendet wird, um ganz unterschiedliche Malware-Typen zusammenzufassen, die sonst in keine Kategorie passen.

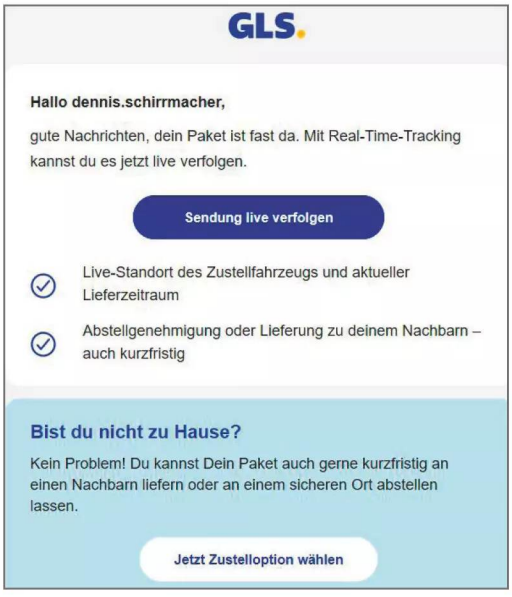
Berbew und Padodor sammeln auf infizierten Rechnern sensible Informationen wie Log-in- und Kreditkartendaten und eröffnen den Angreifern Zugriffsmöglichkeiten aus der Ferne. Kopierte Daten werden oftmals im Darknet zum Kauf angeboten.

Dass der Infostealer-Trend nicht nur Windows betrifft, zeigte auch Anatsa - eine jener Android-Malwares, die es in den vergangenen Monaten trotz aller Sicherheitsvorkehrungen in Googles Play Store schafften. Im Stil eines klassischen Banking-Trojaners verbarg sie sich bis zu ihrer Entdeckung in mehr als 90 vermeintlich legitimen Apps, die es auf insgesamt rund 5,5 Millionen Downloads brachten. Der Schadcode nutzte Androids Overlay- und Barrierefreiheit-Techniken, um speziell Banking-Zugangsdaten sowie Informationen aus globalen Finanz-Apps abzugreifen.

## Angriffstrends

Mit der Zunahme des Infostealing steigt die Gefahr von Angriffen mittels gestohlener Zugangsdaten. Nutzer sollten deshalb besonders wachsam etwa gegenüber Log-in-Versuchen sein, die ihnen von Mail-Providern, Diensten oder Systemen gemeldet werden. Bei verdächtigen Anmelde-Versuchen sollten Betroffene ihr Passwort ändern. Außerdem sollte als zusätzliche Absicherung, wenn verfügbar, eine Zwei-Faktor-Authentifizierung aktiviert werden. Auf der Website haveibeenpwned.com kann man prüfen, ob eigene E-Mails-Adressen oder Passwörter bereits in Datenleaks vorhanden sind.

Ein „Dauerbrenner“ unter den Malware-Einfallstoren sind nach wie vor Phishing-Angriffe via E-Mails mit schädlichen Anhängen oder Schadcode, der etwa auf verlinkten Websites lauert. Bereits für 2023 verzeichnete das BKA im Bundeslagebild eine steigende Anzahl derartiger Attacken. Ein aktuelles Beispiel von April 2024 ist eine auf Unternehmen abzielende E-Mail-Kampagne, die wiederum einen Infostealer namens Rhadamanthys verteilte. Er verbarg sich in gefälschten Rechnungen des Metro-Großhandels, die sich durch glaubwürdige Absenderadressen auszeichneten.




**Haupteinfallstor E-Mail: Cyberkriminelle versuchen Opfer mit gefälschten Mails aufs Glatteis zu führen. Um PCs zu schützen, sollte man nicht auf Links klicken oder Dateianhänge öffnen.**

Auch Privatpersonen werden immer wieder zum Ziel von Phishing-Kampagnen, die entweder Malware verteilen oder aber zur Eingabe sensibler Daten auf gefälschten Internetseiten verleiten sollen. Im Zweifel empfiehlt es sich, beim Absender der E-Mail nachzuhaken, statt leichtfertig vertrauliche Daten preiszugeben.

Im Zusammenhang mit aktuellen Angriffstrends weiterhin unbedingt erwähnenswert ist die wachsende Gefahr, die von Soft- und Hardwareschwachstellen als Malware-Einfallstore ausgeht. In seinem Lagebericht zur IT-Sicherheit in Deutschland wies das Bundesamt für Sicherheit in der Informationstechnik (BSI) schon im vergangenen Jahr darauf hin, dass die Zahl der täglich gemeldeten Software-Schwachstellen im Vergleich zu 2022 um 24 Prozent gestiegen sei.

Dass sich dieser Trend fortsetzt, zeigt etwa auch der derzeitige Rückstau in der NVD, einer Online-Datenbank für Software-Schwachstellen: Die Verantwortlichen kommen mit dem Hinzufügen ergänzender Informationen nicht mehr hinterher. Als einen der Gründe hierfür nennen sie die extreme Zunahme der Menge veröffentlichter Software und - in der Konsequenz - auch darin klaffender Sicherheitslücken.

Eine weitere Entwicklung, die sich im Auge zu behalten lohnt, sind Phishing-Versuche und Schadcode auf Basis von Künstlicher Intelligenz (KI). Wie der bereits erwähnte Infostealer Rhadamanthys zeigt, sind solche Phänomene längst keine Zukunftsmusik mehr: Der Schadcode, der sich in Gestalt eines Skripts in den Anhängen der vermeintlichen Metro-Mails verbarg, wies laut Forschern Charakteristiken KI-generierten Codes auf. Selbstlernende Sprachmodelle (LLM) können den Schreibstil einer Person imitieren und auf diese Weise Social Engineering über Phishing-Mails oder andere Kommunikationskanäle auf ein ganz neues Level heben. Wirklich ausgereift ist die Technik aber noch nicht. Angesichts des hohen KI-Potenzials ist jedoch zu erwarten, dass Cyberkriminelle weiterhin fleißig daran arbeiten.

## Prävention & erste Hilfe

Die Statistiken zeigen, dass Schadcode im Cybercrimebereich immer noch eine zentrale Rolle spielt. Für digitale Erpressungen stellt Ransomware weiterhin das beliebteste Werkzeug dar. Auch bei gezielten Hackerangriffen mit gestohlenen Zugangsdaten kommt oft Schadcode zum Einsatz, der unter anderem unbemerkt Informationen sammelt, Hintertüren öffnet und mit den Servern der Angreifer kommuniziert. In einigen Fällen missbrauchen Angreifer dafür sogar legitime Tools wie PowerShell, um eine Entdeckung durch AV-Software zu erschweren. Auf diesem Wege lässt sich unter anderem skriptbasierter Schadcode auszuführen, der anschließend als „file-

less malware“ im Arbeitsspeicher werkelt, ohne auf der Festplatte des Rechners aufzutauchen.

Deutlich wurde beim Streifzug durch die Malware-Landschaft auch, dass der Appetit krimineller Akteure auf sensible Daten stetig wächst. In gleichem Maße nimmt die Bedeutung geeigneter Schutzmaßnahmen wie die Verwendung von sicheren Passwörtern und Passwortmanagern, Multi-Faktor-Authentifizierung (MFA) sowie das Wissen um Social-Engineering-Techniken zu. Mit aktuellen Phishing-Gefahren speziell im Bereich Onlinebanking setzt sich ein eigener, ausführlicher c’t-Artikel auseinander [1].

Nach wie vor ist die zeitnahe Installation verfügbarer Sicherheitsupdates essenziell. Vor allem auf Windows-PCs sollte ein Virenschutz laufen. Der standardmäßig aktive Defender bietet schon einen ausreichenden Grundschutz. Er kann sogar in gewissem Maße – unter anderem dank verhaltensbasierter Erkennungsmechanismen und Scans nach skriptbasierten Angriffen – auch dateilosen Bedrohungen einen Riegel vorschieben. Außerdem sollte man sicherstellen, E-Mails kritisch zu prüfen und etwa bei kryptischen Absenderadresse auf keine Links klicken oder sogar Dateianhänge zu öffnen.

Sollten privater PC oder Firmenrechner dennoch einmal einer erfolgreichen Attacke zum Opfer fallen, hilft Desinfec't weiter. Das Tool startet mit seinem Live-System direkt von einem USB-Stick und untersucht inaktive Windows-Installationen mit mehreren AV-Scannern auf Malware.

Abschließend noch ein Tipp: Im Desinfec't-Expertenordner, der ausdrücklich Malware-Profis vorbehalten ist, stecken nützliche Werkzeuge, um beispielsweise verloren geglaubte Daten zu retten oder mit eigenen Signaturen Schadcode zu jagen.

In Desinfec't 2024/25 frisch hinzugekommen sind Tools zur detaillierten statischen Analyse verdächtiger Dateien (siehe Artikel S. 38). So hilft etwa Detect It Easy (DIE) beim initialen Bestimmen von Dateiformaten, FLOSS extrahiert interessante Strings aus EXE-Dateien und spezielle Python-Skripte spüren gefährlichem Code in Office- und PDF-Dateien nach. Eine Liste im Expertenordner (“01_Tool_Liste_.txt“) schlüsselt alle verfügbaren Werkzeuge auf. (des) c't

## Literatur

[1] Markus Montz, Konten-Phishing 3.0, Wie organisierte Kriminalität Bankkunden ausplündert, c’t 16/24, S. 116

# Profi-Scanner effektiv nutzen

**Für tief gehende Systemscans stehen in Desinfec't zwei Profi-Werkzeuge zur Verfügung. Wir zeigen ihre jeweiligen Stärken und wie man damit passgenau auf Bedrohungen reagiert.**

Von **Olivia von Westernhagen**

Seit einigen Jahren sind der Open Threat Scanner (OTS) sowie Thor Lite aus dem Hause Nextron Systems fester Bestandteil des c't-Sicherheitstools Desinfec't. Beide unterstützen Malwareexperten bei der Bedrohungssuche in Windows.

Um eins gleich vorwegzunehmen: Diese Scanner richten sich an Admins und Spezialisten, die sich bereits mit der Malwareanalyse auskennen. Sie sind nichts für „normale" Nutzer von Desinfec't, die mal eben den Computer der eigenen Oma überprüfen wollen. Dafür sind die Desinfec't-Scanner von Eset und WithSecure da.

## Einsatzszenarien

Im Grunde funktionieren die Profitools wie klassische Anti-Viren-Scanner und führen automatisierte Systemscans durch. Die beiden Scanner arbeiten dabei mit extrem frischen Signaturen, die die Security-Community beim Auftauchen einer neuen

Bedrohung erstellt. So erkennen sie brandaktuelle Gefahren; manchmal sind die Signaturen aber auch mit heißer Nadel gestrickt, sodass es False Positives oder missverständliche Beschreibungstexte geben kann, die Laien verunsichern würden.

Zum Erstellen der Signaturen extrahieren IT-Experten zunächst Bedrohungsinformationen aus Malware-Funden. Diese verpacken sie im nächsten Schritt in sogenannte YARA-Regeln, selbst geschriebene Virensignaturen auf Basis einer leicht erlernbaren Syntax, und fügen sie den Profi-Werkzeugen mit wenigen Schritten hinzu.

So können sie flexibel auf individuelle Sicherheitsvorfälle im professionellen Umfeld reagieren. Etwa wenn PC-Schädlinge so neu sind, dass es noch keine Signaturen für konventionelle Scanner gibt. Das hat etwa 2019 die Justus-Liebig-Universität Gießen nach einer Trojaner-Attacke auf ihr Netzwerk erfolgreich gemacht, um so ihre Computer im großen Stil effektiv mit dem OTS zu untersuchen.

Obwohl beide Tools mit YARA-Regeln arbeiten, setzen sie doch ganz unterschiedliche Schwerpunkte: Während sich Thor Lite als Hilfsmittel zur umfassenden Suche nach typischen Spuren einer Kompromittierung versteht, spürt der OTS als individualisierter Virenscanner präzise ganz spezifischen Schadcode auf. Sie sind demzufolge keine Doppelung im Desinfec't-Profi-Werkzeugkasten, sondern zwei nützliche Hilfsmittel, die Sie im Zuge der Incident Response als starke Combo einsetzen können.

Um Ihnen die Einsatz-, Erweiterungs- und Kombinationsmöglichkeiten des OTS und Thor Lite in Desinfec't näherzubringen, startet dieser Artikel mit YARA-Basics. Anschließend widmet er sich nacheinander beiden Tools und ihrer unterschiedlichen Art der Regel-Verwendung. Sie erfahren, welche Signaturen die Profi-Tools standardmäßig nutzen und wie Sie eigene hinzufügen. Ein Blick auf die Struktur des resultierenden Reports sowie Tipps zum Kombinieren und Weiterlesen runden die Einführung ab.

## YARA als Basis

Nehmen wir einmal an, Sie hätten auf dem Desktop eines kompromittierten Windows-Rechners eine ominöse Textdatei entdeckt. „Infected by R3vengeT3am, have a nice day!“, lautet der darin enthaltene Liebesgruß einer Cybergang. Dabei handelt es sich zum Glück nur um eine simulierte Erpresserbotschaft, die wir hier als Beispiel verwenden.

Folgende selbst geschriebene, vergleichsweise simple YARA-Regel durchsucht PCs nach dieser Datei:

```
rule revenge {
strings:
$text_string = "Infected by R3vengeT3am"

condition:
$text_string and filesize < 10KB
}
```

Jede YARA-Regel beginnt mit dem Schlüsselwort `rule`, gefolgt von ihrem Namen. Die wichtigsten Elemente zwischen den geschweiften Klammern sind die Strings, nach denen YARA suchen soll, sowie eine oder mehrere Bedingungen für einen Suchtreffer (`condition`). Unsere Bedingung ist nur dann erfüllt, wenn die betreffende Datei exakt den genannten Teilstring enthält und außerdem kleiner als 10 Kilobyte ist. Letztere Einschränkung schließt zahlreiche Dateiformate aus, um Fehlalarme zu minimieren und die Suche effektiver zu machen.

Wer lernen will, die mächtige YARA-Syntax voll auszuschöpfen, findet umfassende Hilfestellung nebst Beispielen in der Online-Dokumentation des YARA-Frameworks (siehe ct.de/wres). Eine Abkürzung auf dem Weg zu komplexen Regeln bietet das bei GitHub frei verfügbare Tool YarGen. Lässt man es auf Verzeichnisse mit sichergestelltem Schadcode los, generiert es automatisch passende YARA-Signaturen.

Um erstmals mit den Suchkünsten des OTS und Thor Lite zu experimentieren, reicht die obige YARA-Beispielregel aber vollkommen aus. Dazu speichern Sie sie in einer Datei namens revenge.yar in Ihrem Desinfec't-Projektordner ab. Im Desktopverzeichnis des Windows-Laufwerks, das sie später einhängen und durchsuchen wollen, platzieren Sie als Köder eine Datei namens infected.txt. Diese muss den String `"Infected by R3vengeT3am"` enthalten. Die Datei kann auch in einem anderen Verzeichnis oder Ordner liegen, in unserem Beispiel haben wir uns für den Desktop entschieden. Wie Sie beide Profiwerkzeuge jeweils mit der selbst geschriebenen Signatur füttern, erklären wir später.

## Spurensuche mit Thor Lite

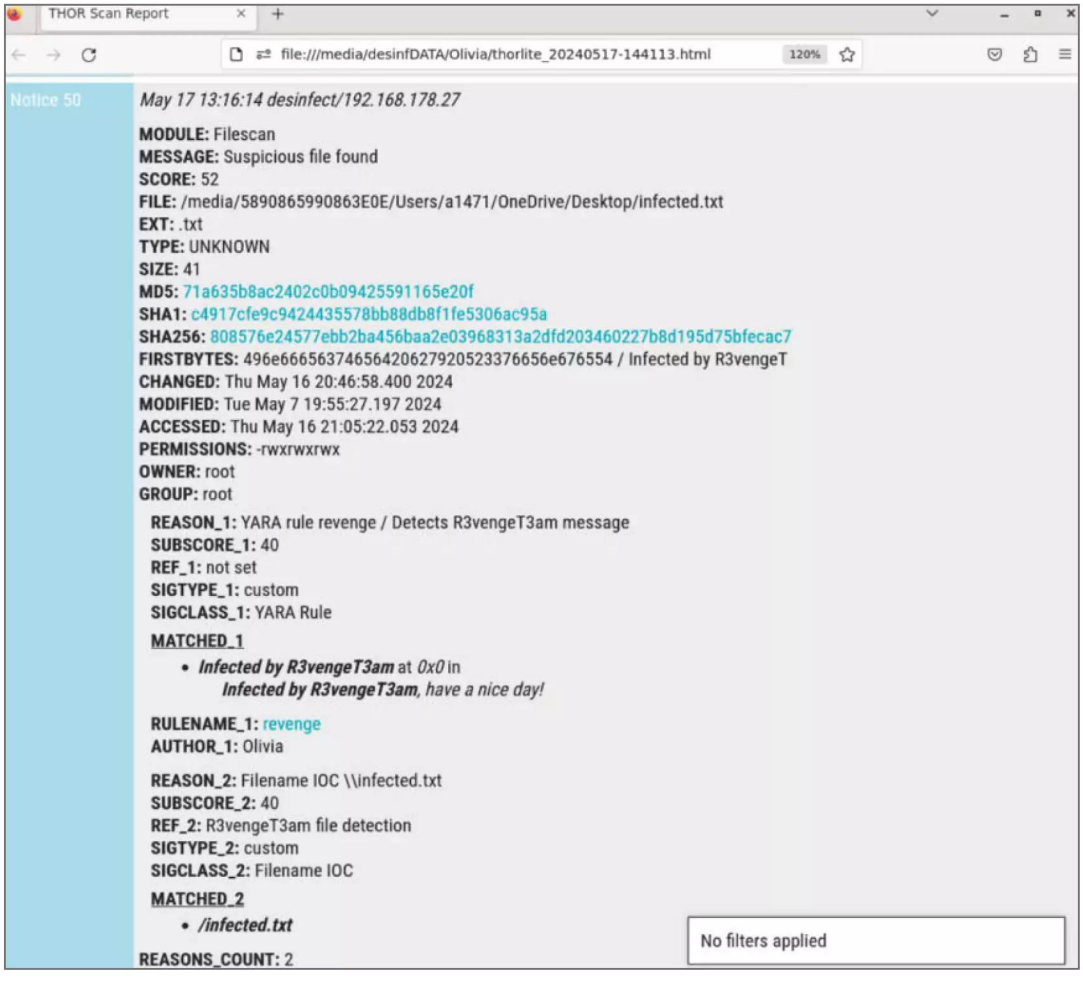
Nach mehrstufigen Hackerangriffen wie auch bei Infektionen mit komplexer, tief im System verborgener Malware ist die Sachlage oft erst einmal undurchsichtig. „Was ist überhaupt passiert?“, lautet die initiale Frage, bei deren Klärung Thor Lite helfen kann.

Beim Scannen stehen eine Vielzahl potenzieller Einbruchsspuren, sogenannter Kompromittierungs-

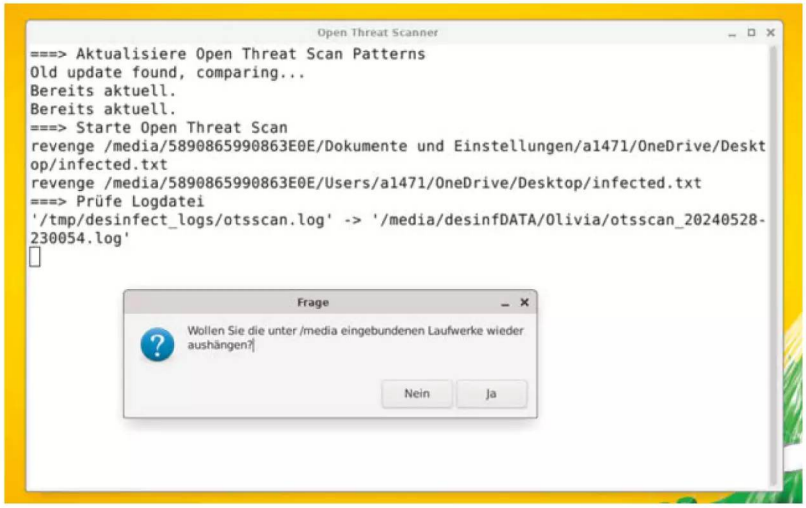
indikatoren (Indicators of Compromise, IoCs) auf der Fahndungsliste des Werkzeugs. Das können etwa verdächtige IP-Adressen, bestimmte Dateinamen oder Strings wie im „R3vengeT3am“-Beispiel sein. Zudem erkennt Thor Lite von Haus aus zahlreiche Hackertools, die als potenzielle Angriffswerkzeuge nur bedingt die Aufmerksamkeit klassischer AV-Scanner erregen.

Die bei einer Suche mit Thor Lite erzielten Treffer sind nicht eindeutig, sondern müssen im Kontext der gescannten Umgebung betrachtet und entsprechend von einem Experten eingeordnet werden. So kann beispielsweise eine auf dem System entdeckte Software für den Fernzugriff auf einen Einbruch hindeuten, genauso gut aber auch zum alltäglichen Handwerkszeug des PC-Nutzers gehören. Ein selbst geschriebenes Skript, das zufälligerweise typische Merkmale schädlichen Codes aufweist, kann unabsichtlich die Bedingung einer YARA-Regel erfüllen. Gleiches gilt für Packer zum Komprimieren ausführbarer Dateien, die Malware-Autoren gern zum Verschleiern schädlichen Codes nutzen.

Wie wir später noch sehen werden, sind Thor-Lite-Reports in der Konsequenz deutlich umfangreicher als die vom OTS erzeugten Logfiles. Das ist jedoch kein Manko, sondern exakt so gewollt, um auch unscheinbare Spuren und Hinweise nicht zu übersehen.




**Blick auf die Darstellung unserer fiktiven „R3vengeT3am“-Bedrohung als „Notice“ im Thor-Lite-Report. Aus den Subscores wurde intern ein Gesamtwert berechnet; weitere Metadaten und Kommentare dienen als ergänzende Informationen.**




**Rundum-Service: Der OTS hängt Laufwerke ein und aus, zeigt Funde übersichtlich im Terminal an und speichert sie zusätzlich in einer von Desinfec't automatisch erzeugten Logdatei im persönlichen Projektordner.**

## Internes Scoring

Derart „ungewisse" Treffer in großer Zahl ohne ergänzende Beschreibung oder Bewertung richtig einzuordnen, würde selbst Profis vor eine kaum zu bewältigende Herausforderung stellen. Aus diesem Grund bietet Thor Lite Hilfestellung in Form eines internen Scoring-Systems. Dieses fußt auf einer Kombination aus dem Schweregrad des Fundes (Severity) und der Vertrauenswürdigkeit des Alarms (Confidence).

0 ist der niedrigste, 100 der höchstmögliche Score. Werte ab 40 aufwärts sorgen im finalen Report für die Ausgabe eines einfachen Hinweises („Notice"), sozusagen der niedrigsten Gefahrenstufe. Ein Wert ab 60 aufwärts verursacht stattdessen eine Warnung („Warning"). Liegt der Score über 80, kündet ein „Alert" von Gefahr.

Um YARA-Regeln einen Score zuzuordnen, nutzt man die Thor-spezifische Metavariable `score`. Metadaten, eingeleitet durch das Schlüsselwort `meta`, sind von Haus aus ein optionaler Bestandteil des Open-Source-Frameworks YARA. Mit ihnen kann man der Regel zum Beispiel auch eine Beschreibung oder den Namen ihres Autors hinzufügen:

```
rule revenge {
meta:
author = "Olivia"
description = "R3vengeT3am message detection"
score = 40

[...]
}
```

Wenn Sie unsere Beispielregel auf diese Weise bearbeiten, löst sie beim Scan eine „Notice" aus. Das ergibt im konkreten Fall Sinn, schließlich ist die Textdatei für sich betrachtet nicht schädlich, sondern „nur" ein Hinweis auf einen erfolgten Einbruch und die Präsenz weiterer, deutlich gefährlicherer Relikte auf dem System. Würden Sie stattdessen auf eine Score-Angabe in der YARA-Regel verzichten, würde ihr Thor Lite den Defaultwert 75 zuordnen.

Wie Sie im abschließenden Report sehen werden, können sich niedrige (Sub-)Scores zu einer höheren Gesamtpunktzahl aufrechnen. Denn wenn ein Fund gleich mehrere YARA-Regeln triggert, erhöht dies natürlich die Wahrscheinlichkeit, dass der Alarm berechtigt ist.

## Regeln versus IoCs

Thor Lite finden Sie auf dem Desinfec't-Desktop im „Expertentools"-Ordner. Skripte automatisieren und erleichtern die Verwendung innerhalb der Desinfec't-Umgebung. Sie stellen beispielsweise sicher, dass sich die Signaturen automatisch beim Start des Werkzeugs aktualisieren. Außerdem hängen sie die zu scannenden Windows-Laufwerke ein und starten Thor Lite mit speziellen Parametern für den Dateisystem-Scan. Übrigens: Falls Sie Thor Lite aktualisieren möchten, ohne einen Scan anzustoßen, können sie einfach das ebenfalls im Expertentools-Ordner befindliche Skript „update_signatures.desktop" starten. Es bringt auch gleich den OTS sowie sämtliche Virenscanner auf den aktuellen Stand.

Anders als die kommerzielle Software Thor verwendet Thor Lite Open-Source-Signaturen. Die von Nextron Systems gepflegte, rund 4000 Einträge umfassende Datenbank ist auf GitHub verfüg- und einsehbar (siehe ct.de/wres).

In Desinfec't finden Sie das persistente Verzeichnis zum Hinzufügen eigener Signaturen unter /opt/thorlite/custom-signatures. Um selbst erstellte YARA-Regeln wie revenge.yar an Thor Lite zu übergeben, kopieren Sie diese einfach in den darin befindlichen Unterordner yara.

Es gibt aber noch eine weitere Möglichkeit, Thor-Lite-Scans zu personalisieren: Sie schlummert in

einem weiteren custom-signatures-Unterordner namens iocs beziehungsweise in iocs/templates. In die darin enthaltenen Beispiel-Templates können Sie eigene IoCs einfügen, die beim Scan berücksichtigt werden sollen.

Anhand von Keywords im Template-Namen, zum Beispiel „c2“, „domains“, „filename“, „hash“ oder „keywords“, identifiziert Thor Lite die jeweiligen IoC-Typen. In einigen Fällen ist es möglich, zusätzlich einen Score hinzuzufügen.

Gemäß unserem Beispiel könnten Sie etwa die im Template-Ordner befindliche Datei custom-filename-iocs.txt.template um die folgenden zwei Zeilen ergänzen, wobei die erste einen Kommentar darstellt:

```
# R3vengeT3am file detection
\\revenge.txt;40
```

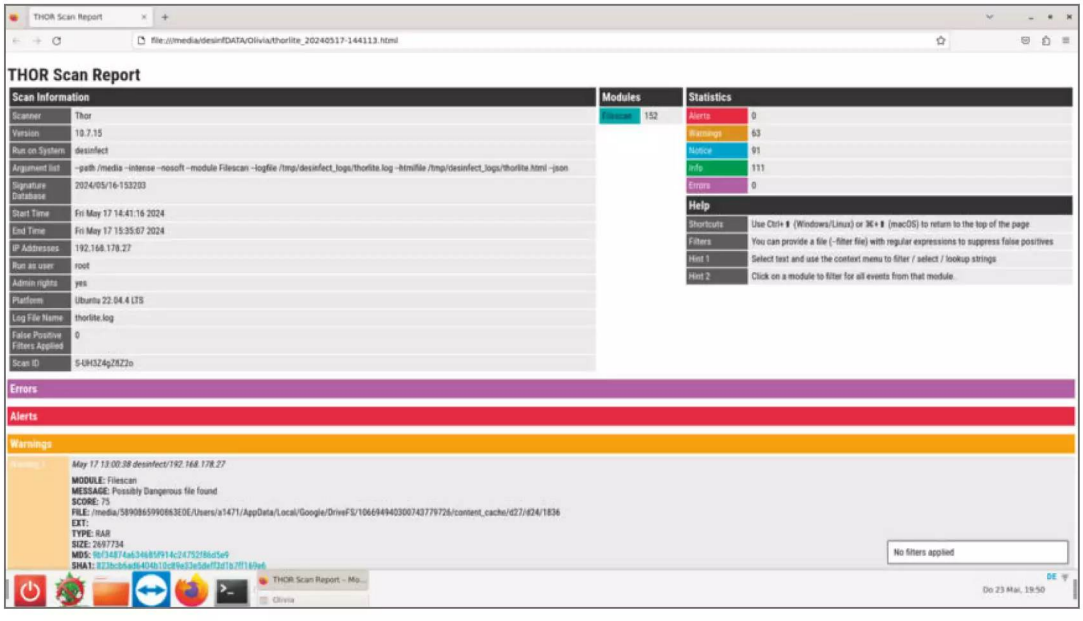
Thor Lites Filename-IoC-Dateien arbeiten mit regulären Ausdrücken. Wer sich damit auskennt, kann unter anderem zu berücksichtigende Pfade eingrenzen oder Dateien finden, deren Namensgebung in Teilen variieren. Dies ist keine Seltenheit bei Schadcode, der zur Laufzeit extrahierte Komponenten vor Scanprozessen verbergen will. Auch kann man negative Scores vergeben, um Suchtreffer in bestimmten Verzeichnissen sozusagen zu neutralisieren. Die ausführliche Thor-Onlinedokumentation verrät weitere Details (siehe ct.de/wres).

Wenn Sie nun noch die Endung „.template“ der soeben bearbeiteten Datei entfernen, um die IoCs scharf zu schalten, sollte Thor Lite die auf dem Windows-Desktop befindliche infected.txt beim nächsten Scan sowohl per YARA-Regel als auch anhand des Dateinamens finden.

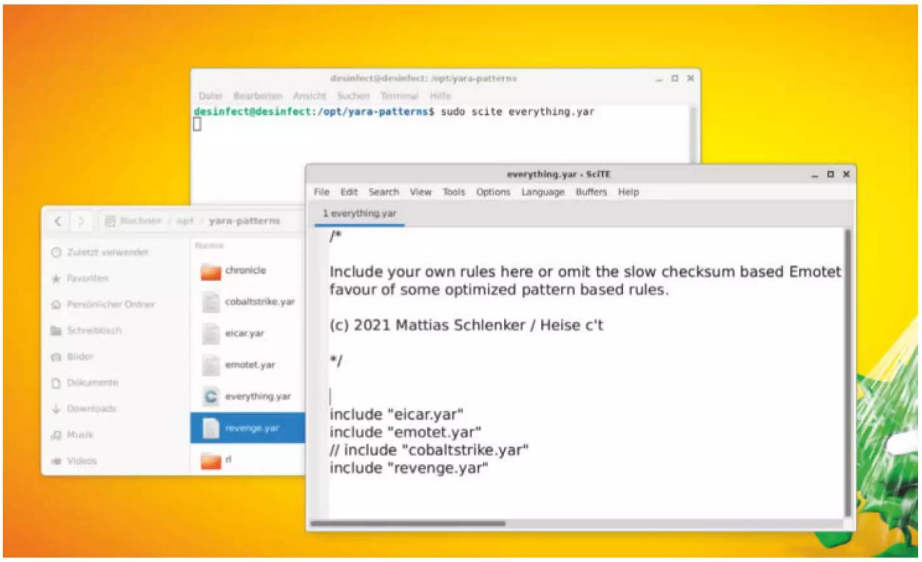
## Einbruchsspuren aufgeschlüsselt

Im persönlichen Projektordner von Desinfec’t stehen im Anschluss an den Thor-Lite-Scan eine Logdatei im Textformat sowie eine HTML-Fassung des Scan-Reports zur Auswahl. Für wen Meldungen zu geladenen Scanmodulen und erfolgreich kompilierten YARA-Regeln nicht so spannend sind, der findet in der HTML-Datei eine deutlich übersichtlichere Auflistung der Scan-Resultate.

Alerts, Warnings und Notices sind farbig aufgeschlüsselt und zu jedem Treffer liefert Thor Lite Details wie Dateinamen, -pfade und -größe sowie das Datum des letzten Zugriffs und natürlich den oder die Score(s). Falls Sie unser Beispiel ausprobiert haben, können Sie sich in diesem Zusammenhang anschauen, wie Thor Lite Metadaten wie `author` und




**Der HTML-Report von Thor Lite schlüsselt Suchtreffer anhand der zugeordneten Scores farbig auf.**




**Mit SciTE ergänzen Sie die Regeldatei everything.yar um eigene Regeln oder kommentieren vorhandene aus.**

`description`, aber auch den Kommentar aus der Filename-IoC-Datei als Zusatzinformationen ausgibt (siehe Thor-Bild oben).

Die beiden „40"-Subscores summierten sich in unserem Testlauf zu einem internen Gesamtscore von 52. Dass niedrige Scores eher gering gewichtet werden und den Gesamtscore niemals massiv anheben können, ist Nextron Systems zufolge so gewollt. Das passt auch zu unserem Beispiel: Trotz zweier Suchtreffer sowohl durch YARA als auch durch den einzelnen IoC ist und bleibt der Fund weiterhin nur eine vergleichsweise harmlose Textdatei. Der Schweregrad des Fundes bleibt also gleich; lediglich die Vertrauenswürdigkeit des Alarms (Confidence) steigt. Wer sich für die zugrundeliegende Formel interessiert, wird in der Online-Dokumentation zu Thor fündig (siehe ct.de/wres).

Praktisch: Sie können einzelne Passagen des Reports markieren, um bestimmte Informationen auszufiltern, die Häufigkeit ihres Vorkommens zählen zu lassen oder eine Suche über Google, VirusTotal oder die Threat-Intelligence-Datenbank RiskIQ anwerfen.

## Präzise suchen mit dem OTS

Thor Lite ist es nun also gelungen, die Textdatei unserer fiktiven Malware-Gruppe R3vengeT3am aufzuspüren. In einem echten Bedrohungsszenario ließe ein solcher Fund Rückschlüsse auf die Drahtzieher hinter dem Einbruch zu. Eine anschließende, gezielte Webrecherche würde mit hoher Wahrscheinlichkeit typische, wiederkehrende Angriffsmuster dieser Cybergang zutage fördern.

Mit diesen Informationen und weiteren IoC-Fundauswertungen könnten Sie auf dem System verborgene, bislang unerkannte Malware einkesseln. Haben Sie diese gefunden und analysiert oder von YarGen durch die Mangel nehmen lassen, um eine passende YARA-Regel zu erstellen, kommt der Open Threat Scanner zum Einsatz. Mit ihm durchsuchen Sie unter Verwendung der aus der Thor-Lite-Suche angereicherten YARA-Regel schnell und einfach eine größere Zahl von Systemen.

Die Basis für den OTS bildet der ursprüngliche, bei GitHub frei verfügbare Scanner des YARA-Projekts. Dessen Nachteil besteht darin, dass er manuell über die Kommandozeile mit einzelnen Regeldateien und Suchpfadangaben gefüttert werden muss. Ein wenig praktikables Vorgehen, wenn Eile geboten ist.

Der OTS macht Scannen mit YARA deutlich komfortabler und effizienter: Skripte und Konfigurationsdateien übernehmen sämtliche Schritte vom Ein- und abschließenden Aushängen der Windows-Laufwerke über deren automatisierten Scan mit YARA bis hin zum Erstellen einer Logdatei im Projektordner

des Desinfec't-Nutzers. Wird das Tool fündig, gibt es zusätzlich eine Warnmeldung aus.

Das OTS-Logfile zeigt Zeile für Zeile die Namen der ausgelösten Regeln an, gefolgt vom aufgespürten Objekt nebst Dateipfad. Auf etwaige Zusatzinformationen oder beschreibende Aliases, wie Anti-Virenprogramme sie verwenden, verzichtet der OTS.

Die Beschränkung auf das Wesentliche und die daraus resultierende Übersichtlichkeit der Reports kommt Profis entgegen, wenn es schnell gehen muss. Anders als bei Thor Lite geht es hier nicht um das Zusammentragen möglichst vieler Verdachtsfälle, sondern um präzise Treffer.

## Signaturen nach Maß

Auch den OTS finden Sie im Ordner „Expertentools". Sofern eine Internetverbindung besteht, aktualisiert das Programm beim Start automatisch die Signaturen.

Dabei greift der OTS auf das öffentliche GitHub-Repository der IT-Sicherheitsfirma ReversingLabs zu. Bei den regelmäßig aktualisierten Signaturen konzentriert sich das Unternehmen nach eigenen Angaben auf eine hohe Erkennungsrate bei zugleich möglichst geringer Anfälligkeit für Fehlalarme. Die zweite YARA-Quelle für den OTS ist ein Repository des Google Cloud Threat Intelligence Teams (GCTI). Es enthält Erkennungsregeln für sogenannte Cobalt Strike Beacons, die Cyberkriminelle gern nutzen, um dauerhaften und umfassenden Zugang zu infizierten Systemen zu erlangen. Damit ausgerüstet ist der OTS schonmal gut gewappnet, um Schädlingen vom Schlage Emotet auf die Spur zu kommen.

Die OTS-Standardsignaturen finden Sie nach dem Update unter /opt/desinfect/signatures/desinfect-signatures/yara nebst Unterverzeichnissen. Die leicht lesbaren und nach Malwaretypen sortierten ReversingLabs-Signaturen im Unterverzeichnis „rl" lassen sich gut als Referenz für eigene Regeln nutzen. Denn letztlich liegt die größte Stärke des OTS in seiner individuellen Konfigurierbarkeit.

Um eigene Regeln in den Scan einzubinden, hinterlegen Sie diese als Dateien mit der Endung „yar" im Ordner /opt/yara-patterns. Achtung: Für den schreibenden Zugriff auf /opt benötigen Sie Rootrechte. Die Beispielregel revenge.yar kopieren Sie mit dem Befehl `sudo cp [Quelle] [Ziel]`. An Thor-Lite-spezifischen Metadaten wie `score` aus unserem Beispiel stört sich der OTS beim Verarbeiten einer Regel nicht. Sie müssen ihm nun aber noch mitteilen, dass er sie beim Scannen mit einbeziehen soll. Dazu fügen Sie den Regelnamen in einer eigenen Zeile der Datei everything.yar hinzu, die sich ebenfalls in /opt/yara-patterns befindet. Sie können die Datei mit dem vorinstallierten Texteditor SciTE bearbeiten und speichern. Tippen Sie dafür folgende Befehle ein:

```
sudo scite /opt/yara-patterns/everything.yar
```

Falls Sie den Scan komplett individualisieren möchten, können Sie einzelne oder alle bereits vorhandenen Regelquellen in everything.yar auskommentieren. Zulässig sind sowohl ein- als auch mehrzeilige Kommentare („//" bzw. „/*(...)*/"). Beim Testen eigener Regeln spart dies Zeit.

A propos Testen: Sofern Sie die Köderdatei infected.txt wie beschrieben auf einem Windows-Laufwerk abgelegt haben, sollte der Scanner sie beim nächsten Suchdurchlauf finden und in seinem Report auflisten.

## Kombinieren & experimentieren

Es sollte deutlich geworden sein, dass sich aus den sehr unterschiedlichen Schwerpunkten der beiden Profi-Werkzeuge interessante Kombinationsmöglichkeiten ergeben. Zum einen können Sie auf Basis der mit Thor Lite identifizierten Hinweise und anschließender Onlinerecherchen präzise Schadcode-spezifische YARA-Regeln für den OTS erstellen. Umgekehrt kann auf einen erfolgreichen Malwarefund mit dem OTS und die Eindämmung der akuten Gefahr eine auf die Funde abgestimmte Thor Lite-Suche nach Einbruchsrelikten folgen, um den Vorfall umfassend zu dokumentieren und weitere Aufräumarbeiten zu planen.

Wie gut die Tools ihre jeweiligen Stärken ausspielen und versierten Experten dienlich sein können, hängt letztlich stark von der Qualität der verwendeten YARA-Regeln und IoCs ab. Es lohnt also, sich eingehender mit diesem Thema zu befassen, um die weit über unser einfaches Beispiel hinausgehenden Möglichkeiten auszuschöpfen. Insbesondere ermöglichen zusätzliche Thor-spezifische Metavariablen zum Beispiel die Angabe von Dateipfaden, -endungen oder -größe, um die Bedingung für einen Treffer noch genauer zu spezifizieren.

Verweise zu allen genannten Online-Dokumentationen und Repositories finden Sie via ct.de/wres. Als weiterführenden Lesestoff haben wir dort auch einen ausführlichen Hintergrundartikel von heise Security zum Thema IoCs verknüpft. (des) c't

**Hintergründe zu YARA, OTS und Thor**

**ct.de/wres**

# IMPRESSUM


## Redaktion

**Postfach 61 04 07, 30604 Hannover**
**Karl-Wiechert-Allee 10, 30625 Hannover**
**Telefon: 05 11/53 52-300**
**Telefax: 05 11/53 52-417**
**Internet: www.heise.de**

**Leserbriefe und Fragen zum Heft:**
sonderhefte@ct.de

Die E-Mail-Adressen der Redakteure haben die Form xx@heise.de oder xxx@heise.de. Setzen Sie statt „xx“ oder „xxx“ bitte das Redakteurs-Kürzel ein. Die Kürzel finden Sie am Ende der Artikel und hier im Impressum.

**Chefredakteur:** Torsten Beeck (tbe, verantwortlich für den Textteil), Dr. Volker Zota (vza)

**Konzeption:** Dennis Schirrmacher (des)

**Koordination:** Jobst Kehrhahn (keh, Leitung), Pia Groß (piae), Tom Leon Zacharek (tlz)

**Redaktion:** Mirko Dölle (mid), Dennis Schirrmacher (des), Peter Siering (ps)

**Mitarbeiter dieser Ausgabe:** Thorsten Leemhuis, Mattias Schlenker, Olivia von Westernhagen

**Assistenz:** Susanne Cölle (suc), Tim Rittmeier (tir), Martin Triadan (mat)

**DTP-Produktion:** Dörte Bluhm, Lara Bögner, Beatrix Dedek, Madlen Grunert, Steffi Martens, Leonie Preuß, Lisa Reich, Marei Stade, Matthias Timm, Christiane Tümmler, Ninett Wagner, Nicole Wesche

**Digitale Produktion:** Christine Kreye (Leitung), Thomas Kaltschmidt, Martin Kreft, Pascal Wissner

**Fotografie:** Andreas Wodrich, Melissa Ramson

**Titel:** Steffi Martens, www.freepik.com

## Verlag

**Heise Medien GmbH & Co. KG**
**Postfach 61 04 07, 30604 Hannover**
**Karl-Wiechert-Allee 10, 30625 Hannover**
**Telefon: 05 11/53 52-0**
**Telefax: 05 11/53 52-129**
**Internet: www.heise.de**

**Herausgeber:** Christian Heise, Ansgar Heise, Christian Persson

**Geschäftsführer:** Ansgar Heise, Beate Gerold

**Mitglieder der Geschäftsleitung:** Jörg Mühle, Falko Ossmann

**Anzeigenleitung:** Michael Hanke (-167)
(verantwortlich für den Anzeigenteil),
www.heise.de/mediadaten/ct

**Anzeigenverkauf:** Verlagsbüro ID GmbH & Co. KG,
Tel.: 05 11/61 65 95-0, www.verlagsbuero-id.de

**Leiter Vertrieb und Marketing:** André Lux (-299)

**Service Sonderdrucke:** Julia Conrades (-156)

**Druck:** Firmengruppe APPL Druck GmbH & Co. KG,
Senefelder Str. 3–11, 86650 Wemding

**Vertrieb Einzelverkauf:**
DMV DER MEDIENVERTRIEB GmbH & Co. KG
Meßberg 1
20086 Hamburg
Tel.: 040/3019 1800, Fax: 040/3019 145 1815
E-Mail: info@dermedienvertrieb.de
Internet: dermedienvertrieb.de

**Einzelpreis:** € 16,90; Schweiz CHF 29.20;
Österreich € 18,60; Luxemburg € 19,50

**Erstverkaufstag: 27.09.2024**





Hergestellt und produziert mit Xpublisher: www.xpublisher.com

Printed in Germany.

# Neue Malware-Analysetools für Profis

**Zusätzliche mächtige und vielseitige Werkzeuge in Desinfec't 2024/25 helfen bei der Analyse von kompromittierten PCs: Damit entlocken Experten verdächtigen Windows-Executables, Office-Dateien und PDFs ihre Geheimnisse.**

Von **Olivia von Westernhagen**

Eingehängte Windows-Laufwerke mit Antivirensoftware scannen, die Schädlinge findet und bestenfalls zur Strecke bringt: So sieht das klassische Einsatzszenario für das c't-Sicherheitstool Desinfec't im privaten Bereich aus. Für Malware-Profis hat das Live-System aber noch weit mehr zu bieten und es stehen etwa der Open Threat Scanner (OTS) für Scans mit maßgeschneiderten Signaturen und Thor Lite für die umfassende Suche nach Einbruchsspuren bereit (siehe Artikel „Profi-Scanner effektiv nutzen").

Desinfec't 2024/25 erweitert das Profi-Arsenal im Ordner „Expertentools" auf dem Desktop nochmals – und zwar um Werkzeuge, die auf die tiefgehende

Analyse verdächtiger Dateien spezialisiert sind. Darunter fallen nicht nur ausführbare Windows-Programme und ihre Komponenten; auch verschiedene Office-Formate und PDF-Dateien kann man mit ihnen durchleuchten. Dieser Artikel stellt die neue, starke Tool-Kombo und ihre vielfältigen Einsatzmöglichkeiten anhand praktischer Beispiele vor. Alle im Artikel genannten Werkzeuge funktionieren übrigens auch mit vielen anderen Linux-Distributionen wie Ubuntu, das die Basis für Desinfec't bildet, und macOS und Windows.

Achtung: Alle hier vorgestellten Tools richten sich an erfahrene IT-Sicherheitsexperten, die im Zuge einer Angriffsanalyse (Incident Response) das Maximum aus Desinfec't herausholen wollen. Wer nicht über das nötige Vorwissen verfügt oder nur mal eben Omas PC auf Schadcode prüfen will, sollte vom Inhalt des Expertenordners lieber die Finger lassen. Schließlich kann man damit auch etwas im System kaputt machen, sodass Windows im schlimmsten Fall nicht mehr startet oder wichtige Daten unwiederbringlich verloren gehen.

## Einfach ausprobieren

Am leichtesten fällt der Zugang zu den Werkzeugen, wenn Sie selbst mit ihnen experimentieren. Dafür stellen wir vier Malware-Samples in einem mit dem Passwort „infected“ geschützten Zip-Archiv zum Download (siehe ct.de/wp1z) bereit. Diese Samples dienen nachfolgend als Beispiele, um die vielfältigen Funktionsweisen zu demonstrieren.

Vorsicht: Hier handelt es sich um echten Schadcode, bei dem beispielsweise der Windows Defender Alarm schlägt. Am sichersten und bequemsten ist es daher, die Dateien beim Download direkt in den geschützten Desinfec't-Kontext zu importieren. Speichern Sie ihn am besten in Ihrem persönlichen, persistenten Desinfec't-Projektordner. Damit Sie alles gut zuordnen können, haben wir die Malware-Beispiele wie nachfolgend im Artikel angegeben benannt (Sample1 etc.). Die Quellen der Samples finden Sie im Archiv in der Textdatei Quellen.txt.

Mit Ausnahme der oletools, die aus zwölf Einzelkomponenten bestehen und jeweils direkt über das Terminal aufgerufen werden, haben wir für alle in diesem Artikel erwähnten Werkzeuge Verknüpfungen im Ordner Expertentools auf dem Desinfec't-Desktop angelegt. Beim Doppelklick auf eines der Kommandozeilen-Tools landen Sie im Terminal, das die jeweilige Hilfefunktion anzeigt und Ihnen dadurch die Bedienung erleichtert. Oftmals lohnt es sich, die verfügbaren Parameter zu studieren und ein wenig damit zu experimentieren. Informationen zu den oletools und wie man sie aufruft finden Sie ebenfalls im Expertentools-Ordner: Die Textdatei „03_Oletools_.txt“ schlüsselt alle in oletools enthaltenen Werkzeuge auf.

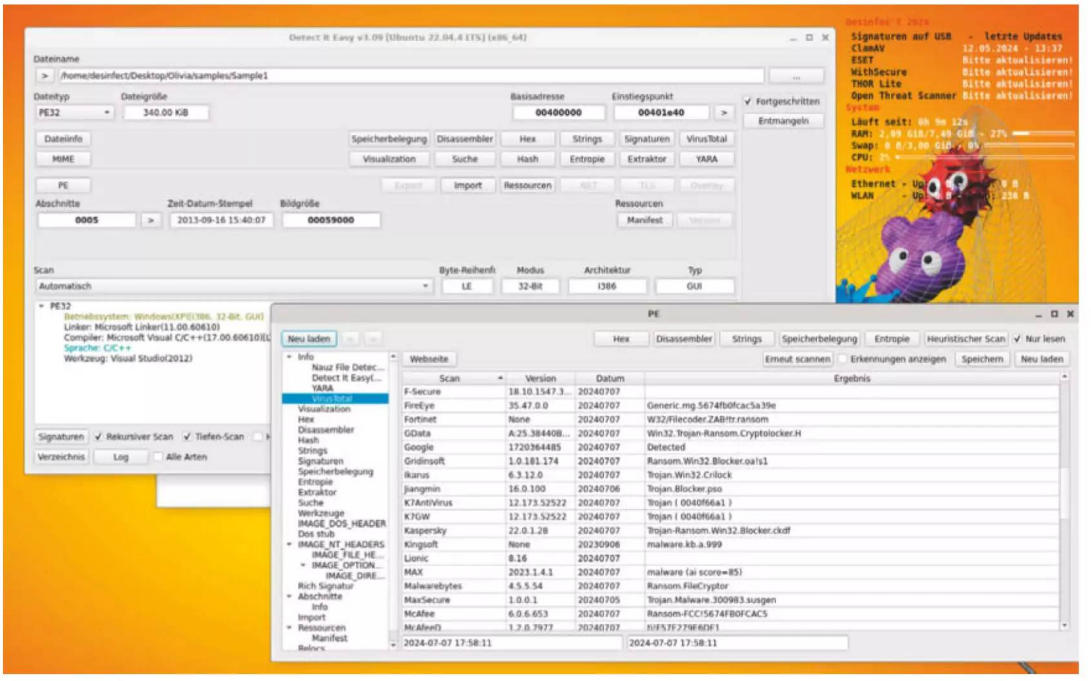
Für den Fall, dass Sie grundsätzlich lieber auf der Kommandozeile arbeiten, finden Sie die benötigten Befehle für die anderen Tools ebenfalls in diesem Artikel. Dabei gehen wir der Einfachheit halber jeweils davon aus, dass das Terminal bereits im Verzeichnis mit den Samples geöffnet wurde. Ansonsten müssen Sie beim Übergeben der Samples an die Tools den Dateipfad angeben.

## Trojaner enttarnen

Zur Tarnung zeigt Malware oft keine Dateiendung an oder täuscht einen falschen Dateityp vor. Mit dem Tool „Detect It Easy“, kurz: „DIE“ meistern Sie diese Schwierigkeit problemlos: DIE kann eine große Zahl von Dateitypen automatisch identifizieren und anschließend analysieren. Dazu zählen neben ausführbaren Formaten für Windows, macOS und Linux verschiedene Archivformate, Video-, Audio- und Bild-

### Malware-Tools in Desinfec't 2024/25

- Detect It Easy erkennt Dateitypen und bietet einen ersten Überblick über Malware-Eigenschaften.
- UPX kann komprimierten Schadcode entpacken und so die Analyse erleichtern.
- FLOSS extrahiert verborgene Strings aus Executables.
- Capa erkennt die Fähigkeiten von Malware und schlüsselt sie übersichtlich auf.
- Die Werkzeugsammlung oletools hilft beim Untersuchen diverser Office-Formate.
- pdfid.py und pdf-parser.py gehen den Geheimnissen verdächtiger PDFs auf den Grund.



**Das Tool „Detect It Easy“ (DIE) erkennt viele Dateiformate und trägt statische Analyseergebnisse zusammen.**

dateien, Skripte und vieles mehr. Zur Bestimmung des Formats nebst zahlreicher spezifischer Eigenschaften bedient sich DIE einer mitgelieferten, derzeit mehr als 2000 Einträge umfassenden Signaturdatenbank. An der Weiterentwicklung von DIE und dessen Ergänzung um neue Signaturen beteiligt sich eine sehr aktive GitHub-Community.

Zum Starten des Tools doppelklicken Sie auf die DIE-Verknüpfung im Expertentools-Ordner. Im nächsten Schritt müssen Sie es mit der zu analysierenden Datei füttern – zum Beispiel mit unserem Sample1. Das geht ganz einfach per Drag-and-drop auf das GUI von DIE oder per Klick auf die drei Punkte rechts oben im DIE-Interface.!

Die Ergebnisse erscheinen direkt in der grafischen Oberfläche. Sie zeigen unter anderem, dass es sich bei Sample1 um eine Portable Executable (PE), also eine ausführbare Datei für Windows handelt. Der Programmcode wurde in C oder C++ programmiert und mit Visual Studio 2012 kompiliert und gelinkt. Der von DIE aus dem Dateiheader ausgelesene Zeitstempel weist auf 2013 als Entstehungszeitpunkt der 32-Bit-Anwendung hin. Zudem verrät uns DIE, dass Sample1 offenbar über eine grafische Oberfläche („Typ: GUI“) verfügt.

## Tiefer graben

Für eine erste Bestandsaufnahme sind dies schon eine ganze Menge Informationen. DIE kann unserem Sample jedoch noch weit mehr Details entlocken. Um alle Möglichkeiten zu entdecken, müssen Sie das Fortgeschritten-Feld in der rechten GUI-Hälfte anhaken: Es blendet beschriftete Buttons ein, hinter denen sich weitere Analyseergebnisse verbergen.

Sie kennen die Struktur verschiedener Dateiformate wie Ihre Westentasche, deuten mühelos jede API-Funktion und glänzen mit Assembler-Kenntnissen? Wenn das zutrifft, können Sie beispielsweise in DIEs Disassembler- oder Hex-Ansicht tief in die Funktionsweise des Codes eintauchen, sich alle Felder der Dateiheader übersichtlich aufgliedern lassen und einen Überblick über die Speicherbelegung und Dateistruktur gewinnen. Auch über importierte Programmbibliotheken und Funktionsaufrufe im Code gibt DIE Auskunft.

Falls Ihnen solch fundierte Vorkenntnisse fehlen, können Sie dennoch von vielen bereitgestellten Informationen profitieren: Starten Sie die nähere Analyse von Sample1 beispielsweise mit einem Klick auf den Button „Strings“ und scrollen Sie in der sich

öffnenden Übersicht nach unten. Sie werden Textschnipsel entdecken, die von „encrypted files“, einem „unique public key“ und einer „method of payment“ künden. Vermutlich ahnen Sie nun schon, dass wir es hier mit einer – laut Zeitstempel etwas älteren – Ransomware zu tun haben, die zur Laufzeit ihre Erpresserbotschaft in einem grafischen Interface ausgibt.

Wie dieses Interface aussieht, verrät Ihnen die „Extraktor“-Funktion von DIE. Nach einem Klick auf die zugehörige Schaltfläche erscheint eine Liste der enthaltenen Ressourcen – im konkreten Beispiel mehrere Bilder. Per Klick auf den Button „Alles ausgeben“ und nach Auswahl eines Verzeichnisses können Sie diese extrahieren, speichern und anschließend ansehen.

Letzte Gewissheit im Hinblick auf den Ransomware-Verdacht liefert der Analysedienst VirusTotal. Ein Klick auf den VirusTotal-Button lädt die Datei hoch, die Ergebnisse erscheinen direkt im Programmfenster von DIE. Einige Aliase der Hersteller verweisen im Fall von Sample1 konkret auf CryptoLocker, eine Ransomware, die 2013 und 2014 aktiv war. Gut zu wissen: Wenn Sie auf den „Webseite“-Button oberhalb der Auflistung klicken, gelangen Sie zur Onlinefassung des Scanreports als vielversprechenden Ausgangspunkt für weitere Recherchen.

Es lohnt, DIE auf eigene Faust und mit unterschiedlichen Dateiformaten durchzutesten. Nehmen Sie dazu ruhig mal eine MS-Office- oder PDF-Datei her. Denn das Tool blickt nicht nur hinter die Kulissen von Executables, sondern eignet sich auch als Ausgangspunkt zum Untersuchen nahezu jeder verdächtigen Datei.

## Malware auspacken

Leider lässt sich nicht jede Portable-Executable-Datei (PE) mittels statischer Analyse so einfach inspizieren wie Sample1. Bei einer statischen Analyse wird im Gegensatz zur dynamischen Analyse kein Code ausgeführt. Zur Tarnung verwenden Malware-Entwickler häufig sogenannte Packer, um den Schadcode zu komprimieren und dadurch die Analyse zu erschweren. Da viele dieser Packer nicht nur komprimieren, sondern auch verschlüsseln oder verschleiern – man spricht dann von einem Crypter oder Protector –, ist das Umkehren dieses Vorgangs für Analysten oft schwer bis unmöglich.

Doch DIE ist auch dafür gewappnet: Das Programm kann eine Vielzahl unterschiedlicher Packer, Crypter und Protectoren erkennen und bestimmen. Gute Chancen zum Entpacken bestehen, wenn DIE das Packprogramm UPX (the Ultimate Packer for eXecutables) entdeckt. Das quelloffene Kommandozeilentool wendet nämlich keinerlei Verschlüsselungs- oder andere Schutzmechanismen auf Dateien an, sondern ist wirklich „nur“ zum Komprimieren gedacht. Es ist Packer und Entpacker in einem – und neuerdings fester Bestandteil von Desinfec’t. Mit dem folgenden Befehl können Sie UPX schnell und einfach an unserem Sample1 ausprobieren: `upx -9 Sample1 -o Sample1-upx`

Das Flag `-9` steht für eine starke Kompression – zulässig sind Werte von 1 bis 9. Darauf folgen der Name der zu komprimierenden Datei sowie eine Bezeichnung für die von UPX zu erstellende komprimierte Kopie, die standardmäßig im selben Ordner landet wie die Ausgangsdatei.

Wenn Sie die Kopie nun wiederum in DIE öffnen, sehen Sie im Hauptfenster die UPX-Erkennung. Ein Klick auf die Schaltfläche „Entropie“ verdeutlicht, auf welche Weise das Komprimieren die Datei verändert hat: Der Großteil des Codes wurde in gepackter Form in zwei Bereichen namens UPX1 und UPX2 verstaut. Ganz im Sinne von Malware-Autoren, die ihr Tun verschleiern wollen, ist dadurch auch die Erpressungsbotschaft nicht mehr lesbar. Sie können sich im „Strings“-Bereich von DIE selbst davon überzeugen. Zum Glück ist auch das Dekomprimieren ganz einfach, und zwar per: `upx -d Sample1-upx`.

## An Klartext kommen

Die Verwendung von Packern ist nur eine gängige Methode, um etwa Adressen eines Command-and-Control-Servers (C2) oder Bitcoin-Adressen einer Ransomware vor statischen Analysemethoden zu verstecken. Eine andere, mindestens ebenso verbreitete Taktik besteht darin, solche Informationen erst zur Laufzeit des Codes mittels spezieller Programmfunktionen zu entschlüsseln. Somit wäre eigentlich eine Code-Ausführung – also eine dynamische Analyse – nötig, um diese lesen zu können.

Gut, dass Desinfec’t neuerdings ein Werkzeug parat hat, das verschlüsselte Informationen auch extrahieren kann, ohne das Schadprogramm auszuführen: Das Tool FLOSS (FLARE Obfuscated String Solver) von Mandiant emuliert stattdessen die Assemblerbefehle potenzieller Entschlüsselungsfunktionen im Schadcode und gibt dem Nutzer dekodierte Strings zurück. Genauere technische Details zur Funktionsweise erklärt ein Dokument des Entwicklerteams (siehe ct.de/wp1z).

Da Sample1 keine interessanten verschlüsselten Strings enthält, haben wir zum Ausprobieren von FLOSS eine andere Datei für Sie herausgesucht: Sample2 ist eine Programmbibliothek (DLL) mit der Fähigkeit, Schadcode nachzuladen: ein sogenannter Downloader.

Der FLOSS-Aufruf über die Kommandozeile ist denkbar einfach: `floss Sample2`. Die Terminalausgabe der extrahierten Strings ist unterteilt in Static Strings, Stack Strings, Tight Strings und Decoded Strings. Die erste Gruppe könnten Sie ebenso gut auch in DIE betrachten: Es handelt sich um jene Strings, die im Klartext in der Datei liegen. Spannend sind aber diejenigen, die zur Laufzeit auf dem Stack zusammengesetzt beziehungsweise entschlüsselt werden. Pro-Tipp: Wenn Sie statische Strings bei der FLOSS-Nutzung von vornherein herausfiltern möchten, können Sie dem Aufruf einfach das Flag `--no static` anhängen.


**Geheimnisse enthüllt: FLOSS dekodiert verschlüsselte Strings in Schadcode.**

FLOSS erkennt in Sample2 gleich mehrere dekodierte Strings: Stack-Strings wie wininet.dll, HttpSendRequestW und InternetConnectW belegen die Downloader-Fähigkeiten des Codes und zeigen, dass dieser offenbar Funktionen der Windows-Internet-API (WinINet) verwendet. Außerdem enthalten die dekodierten Strings eine IP-Adresse (103.133.139.17) für den Verbindungsaufbau.

## Malware-Fähigkeiten einschätzen

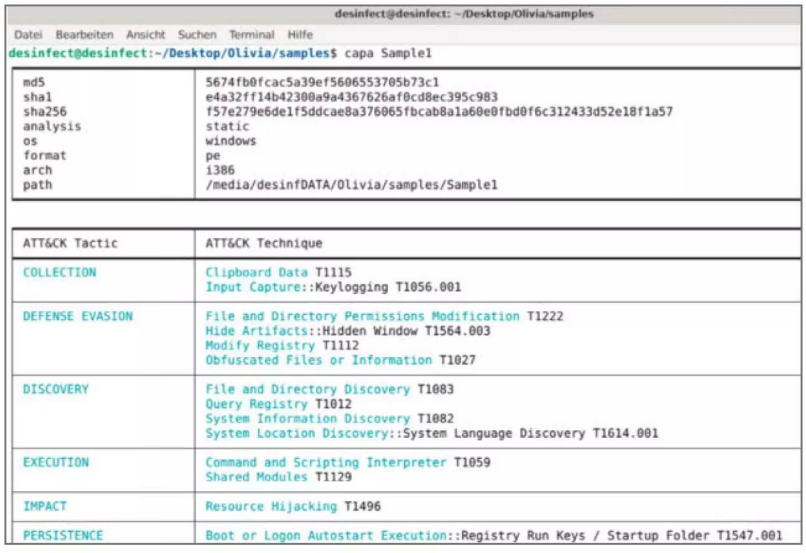
Auch Capa kann Experten bei der Analyse ausführbarer Windows-Dateien ein großes Stück Arbeit abnehmen – allerdings auf abstrakterer Ebene. Das wie FLOSS vom Mandiant-Team entwickelte Tool bestimmt im Rahmen eines Scans die spezifischen Fähigkeiten (Capabilities) einer Malware. Es kann beispielsweise erkennen, ob der Schadcode die Registry manipuliert, mit C2-Servern kommuniziert oder Tastatureingaben mitloggt. Dafür verwendet die Software Signaturen, die als Capa-Regeln bezeichnet werden.

Mit gepackten Dateien und zur Laufzeit entschlüsseltem Code kann Capa aufgrund seines statischen Analyseansatzes wenig anfangen. Ebenfalls zu beachten ist, dass es Schadcode nicht als solchen identifizieren kann, sondern lediglich ganz neutral die Fähigkeiten eines Programms auflistet. Deren Interpretation ist dann Ihre Aufgabe. Würden Sie beispielsweise den ebenfalls in Desinfec't enthaltenen TeamViewer scannen, würde Capa bei diesem korrekterweise feststellen, dass er Funktionen für den Fernzugriff enthält. In der Tat missbrauchen auch viele Angreifer legitime Fernhilfeprogramme als Hintertür. Ob ein solches auf den Rechner gehört oder Teil eines Angriffs ist, müssen Sie selbst einschätzen. Die Analyse mit Capa erfordert also in aller Regel immer zusätzliche Kontextinformationen.

Unsere beiden Beispieldateien eignen sich gut, um Capa auszuprobieren. Übergeben Sie dem Programm einfach die gewünschte Datei mit dem Befehl `capa (Dateiname)`.

## Analyseergebnisse deuten

Die Resultate der soeben gestarteten Analyse erscheinen wie bei FLOSS direkt im Terminal. Capa gliedert sie in mehrere Kästen mit je zwei Spalten. Der oberste Kasten benennt sogenannte „ATT&CK Tactics“ nebst zugeordneten „ATT&CK Techniques“. Diese Bezeichnungen referenzieren das in Security-Kreisen bekannte und bewährte ATT&CK-Framework der MITRE




**Um die Fähigkeiten von Malware zu analysieren, orientiert sich Capa an MITREs ATT&CK-Framework.**

Corporation. Die Datenbank dient dem einheitlichen Klassifizieren von Angriffsstrategien anhand durchnummerierter Einträge (siehe ct.de/wp1z).

Für Sample1 gibt Capa unter anderem die ATT&CK Tactic „Persistence“ zurück und ordnet unserem Beispiel die konkrete Technik „Boot or Logon Autostart Execution“ zu. Auch die Nummer zum Nachschlagen in MITREs Onlinedatenbank (T1547.001) ist Teil der Capa-Ausgabe. Auf der Website attack.mitre.org erfahren Sie im zugehörigen Eintrag, dass unsere Beispiel-Malware Persistenz, also dauerhafte Präsenz auf infizierten Systemen erlangt, indem sie spezielle Run-Registry-Keys anlegt, um eine Kopie von sich selbst zu starten.

Der zweite von Capa ausgegebene Kasten mit den Spaltenüberschriften „MBC Objective“ und „MBC Behavior“ bezieht sich auf den sogenannten „Malware Behavior Catalog“. Auch dieser ist ein online abrufbares MITRE-Projekt (siehe ct.de/wp1z). Er soll die vorhandenen ATT&CK-Taktiken für den spezifischen Anwendungsfall der Malware-Analyse erweitern und verfeinern, sodass unterm Strich ein detailliertes Gesamtbild des Codes entsteht.

Unterhalb der beiden bereits genannten Kästen des Capa-Reports liefert ein dritter mit der Überschrift „Capabilities“ kurze, leicht verständliche Textbeschreibungen der entdeckten Malware-Fähigkeiten nebst ihrer Häufigkeit im Schadcode.

Um die zweite Spalte dieses Kastens (Namespace) zu verstehen, müsste man tiefer in das Thema Capa-Regeln einsteigen. Das ist durchaus spannend und lohnenswert, würde jedoch den Rahmen dieses Artikels sprengen. Mehr Informationen zum Thema liefert ein ausführlicher Capa-Hintergrundartikel auf heise Security (siehe ct.de/wp1z). Darin erfahren Sie unter anderem auch, wie man mit zusätzlichen Flags spezielle Rahmenbedingungen für Scans und Reports definiert.

## Verdächtige Dokumente analysieren

Unsere Beispiele haben gezeigt, dass FLOSS und Capa kompiliertem Code wertvolle Informationen entlocken. Doch nicht nur Executables können Gefahren bergen: Oftmals dienen Office-Dokumente oder PDF-Dateien als Einfallstor für PC-Schädlinge. Dank der Werkzeugsammlung oletools sowie den Python-Skripten pdfid.py und pdf-parser.py des Sicherheitsforschers Didier Stevens untersucht Desinfec’t neuerdings auch solche Verdachtsfälle für Sie.

Zum Ausprobieren der oletools für Office-Dokumente dient das unter ct.de/wp1z hinterlegte Sample3 - ein Word-Dokument (.doc) mit gefährlichem Makro-Code, das als Anhang von Spam-E-Mails vor ein paar Jahren die Ransomware Gandcrab auf Windows-PCs holte. Unser PDF (Sample4) ist hingegen im Grunde harmlos: Es wurde von Didier Stevens als Beispieldatei erstellt und zeigt anschaulich, welches Gefahrenpotenzial auch in diesem Dateiformat schlummern kann.

Vor der Anwendung der jeweiligen formatspezifischen Tools lohnt wiederum ein schneller Röntgenblick mit DIE: So können Sie aus Sample3 mit der Extraktor-Funktion ein Bild extrahieren, das die grundsätzliche Strategie des schädlichen Word-Dokuments enthüllt. Und bei Sample4 geben DIEs Hex- und Strings-Ansichten schon vorab Aufschluss über die eingebettete Payload des PDFs.

Mit der Werkzeugsammlung oletools kann man primär Dateien im OLE2-Format analysieren. Typische Dateiendungen dieses Formats, die im Malware-Kontext im Zusammenhang mit Makro-Schadcode auftauchen, sind .doc oder .xls. Einige in Desinfec’t enthaltene Werkzeuge zielen auch auf das aktuellere Office Open XML-Format (etwa .docx und .xlsx) sowie auf das Rich Text Format (.rtf) ab. Hier wollen wir nur kurz auf einige Tools eingehen, die zum Durchleuchten unseres Sample3 mit .doc-Endung nützlich sind.

Die vorab mit dem DIE-Extraktor sezierte Abbildung aus dem Word-Dokument zeigt das offizielle Microsoft-Office-Logo oberhalb des Schriftzuges „This document is protected“. Mit dieser seriös wirkenden Aufmachung wollen die Schadcode-Autoren das Opfer dazu bringen, die Schaltfläche zum Aktivieren von Makro-Code in Office zu betätigen. Eine englischsprachige Schritt-für-Schritt-Anleitung dafür ist ebenfalls Teil der Masche.

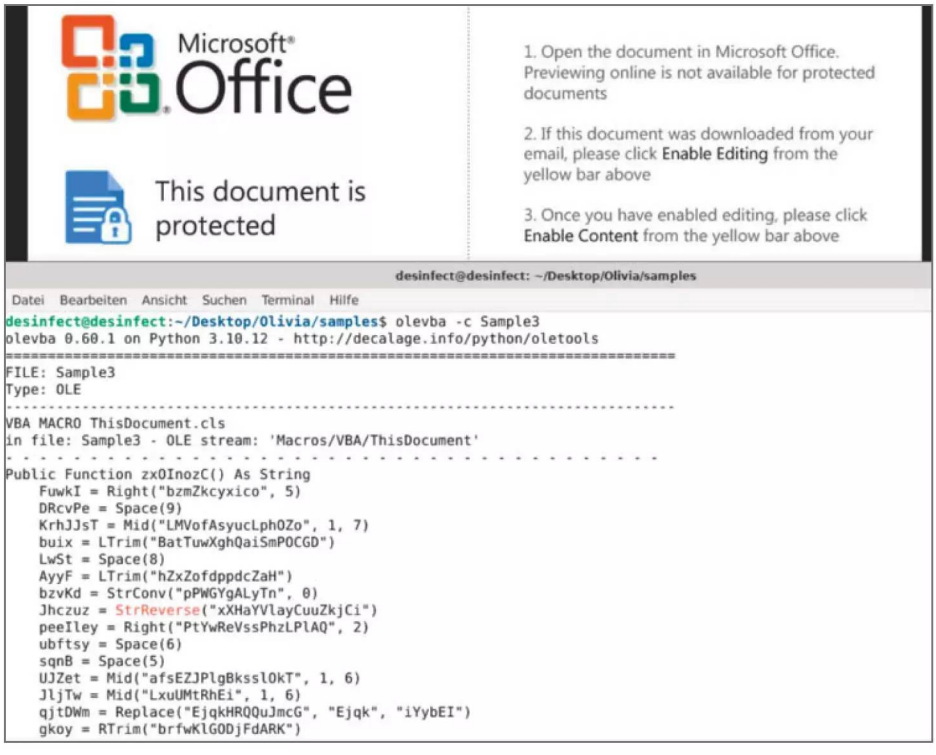
Um den Verdacht zu bestätigen, rufen Sie die oletools-Komponente „oleid“ auf: `oleid Sample3`. Oleid untersucht das Format des Word-Dokuments – in diesem Fall „MS Word 97-2003 Document or template“ – und schätzt das Risiko anhand verschiedener Kriterien wie etwa vorhandener Verschlüsselung und enthaltener Makros.

Und tatsächlich: Das Tool entdeckt in VBA (Visual Basic for Applications) geschriebenen Makro-Code im Sample, stuft diesen aufgrund enthaltener Keywords als verdächtig ein und ordnet ihm die Risikostufe „High“ zu. Überdies empfiehlt es weitere Analysen mit den oletools „mraptor“ und „olevba“. Beide können Sie nach demselben Muster aufrufen wie oleid.

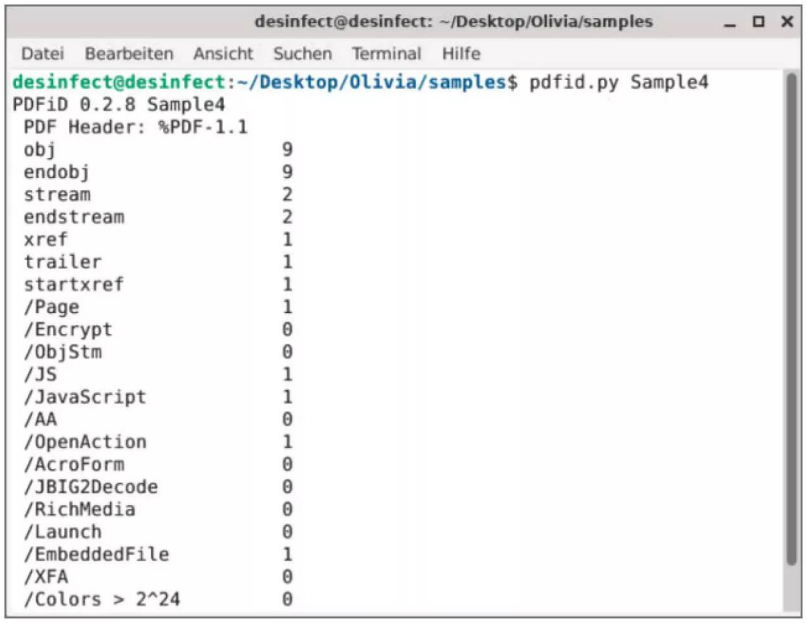
Auch mraptor hält den Makro-Code für verdächtig, nachdem es ihn mithilfe von Keywords unter die Lupe genommen hat. Offenbar wird er beim Öffnen des Word-Dokuments automatisch gestartet und führt anschließend Dateien oder Befehle außerhalb des VBA-Kontexts aus.

Zum Extrahieren des Makrocodes dient olevba: Es zeigt ihn im Terminal an und versucht sich zusätzlich an einer Analyse verschlüsselter beziehungsweise verschleierter Funktionen. Da dies im Falle des stark verschleierten Codes aus Sample3 nicht gut funktioniert, empfehlen wir den Aufruf mittels `olevba -c Sample3`. Mit dem Zusatz `-c` gibt olevba nämlich nur den Code zurück und verzichtet auf Analysen. Diesen könnte man nun kopieren und näher untersuchen.

Im konkreten Fall würde man an dieser Stelle zu dynamischen Analysemethoden etwa in Gestalt einer Online-Sandbox wie any.run wechseln, statt sich an der starken Obfuskierung abzuarbeiten. Oder




**Office-Schwindel: Eine seriös wirkende Aufforderung im Word-Dokument (oben) soll den Nutzer zum Aktivieren von Makros bringen. Klappt dies, wird der obfuskierte VBA-Schadcode (unten) ausgeführt.**




**Kryptisch, aber nützlich: pdfid.py zählt verdächtige Keywords in PDF-Dateien.**

einfach einen Blick auf die Webversion des VirusTotal-Reports in DIE werfen. Sie verrät uns, dass der Makro-Code letztlich ein PowerShell-Skript extrahiert und aufruft, um Schadcode (GandCrab) aus dem Internet nachzuladen.

Unser Beispiel hat jedoch gezeigt, dass man sich mit dieser Tool-Kombo auch ganz ohne Vorwissen und zusätzliche Quellen vergleichsweise einfach davon überzeugen kann, ob ein Office-Dokument Böses im Schilde führt beziehungsweise als Urheber einer mit Desinfec't aufgespürten Windows-Infektion infrage kommt.

## PDFs sezieren

Zu guter Letzt lüften wir noch die Geheimnisse des PDFs (Sample4). Sofern Sie auch dieses vorab in DIE untersucht haben, dürften Ihnen unter anderem die Strings „/EmbeddedFiles“ und „eicar-dropper.doc“ aufgefallen sein. Ja, richtig: Das PDF enthält ein eingebettetes Word-Dokument, das seinerseits per Makro-Code den Testvirus EICAR auf das System befördert. Dieser ist vollkommen harmlos und wurde vom European Institute for Computer Antivirus Research zum Testen von Antivirensoftware ersonnen.

Um zu ergründen, wie die Infektionskette im Einzelnen funktioniert, übergeben Sie Sample4 wie folgt an pdfid.py: `pdfid.py Sample4`. Der Output des Tools dürfte Ihnen ohne nähere Erläuterungen erst einmal seltsam vorkommen. Des Rätsels Lösung: pdfid.py sucht nach bestimmten Strings, die formatbedingt häufig in PDFs vorkommen, und gibt die Anzahl der Suchtreffer für das Dokument aus. Beim Interpretieren der Ergebnisse hilft ein Blogeintrag von Didier Stevens (siehe ct.de/wp1z).

Unser Sample4 hat nur eine Seite (/Page = 1), was laut Stevens häufig auf schädliche PDFs zutrifft. Es enthält offenbar JavaScript-Code (/JS und JavaScript = 1). Die Vermutung, dass dieser verwendet wird, um das enthaltene Word-Dokument (/EmbeddedFile = 1) zu öffnen, liegt nahe. Auf eine automatisierte Aktion beim Öffnen, also etwa eine Skriptausführung, weist auch das einmalige Vorkommen von /OpenAction hin.

Nach dieser ersten Analyse und der Bestätigung, dass die Datei verdächtig ist, besteht der zweite und für uns letzte Schritt darin, pdf-parser.py mit dem Befehl `pdf-parser.py Sample4` auszuführen. Ganz unten in der Terminal-Ausgabe des Skripts sehen Sie nun den JavaScript-Code, der beim Öffnen des PDFs das eingebettete Word-Dokument ausführt:

```
this.exportDataObject({cName: ↵
↳"eicar-dropper.doc", nLaunch: 2});
```

Somit ist es uns gelungen, die interne Infektionskette mithilfe der Python-Skripte zu rekonstruieren. Völlig ohne Nutzerinteraktionen funktioniert die Infektion übrigens nicht: Das Opfer müsste dem Öffnen des Word-Dokuments durch das PDF sowie der anschließenden Ausführung von Makro-Code aktiv zustimmen, bevor die EICAR-Testdatei tatsächlich auf dem System landen kann.

## Alles im Kasten

Unser Artikel sollte Ihnen einen guten ersten Überblick über die neuen Expertentools in Desinfec't vermittelt haben. Um sich den vollständigen Inhalt des Desinfec't-Werkzeugkastens jederzeit in Erinnerung zu rufen, lohnt ein Blick in die Textdatei „01_Tool_Liste_.txt“ im Expertentools-Ordner. Darin finden Sie eine Übersicht über alle verfügbaren Werkzeuge nebst kurzer Beschreibungen. Wir wünschen weiterhin viel Erfolg bei der Schadcode-Jagd und -Analyse mit Desinfec't! (des) c't

**Weitere Informationen und Sample-Downloads**
ct.de/wp1z

# Desinfec’t via Btrfs erweitern

**Bisher konnte man Desinfec’t nur bis zu einem gewissen Grad modifizieren, etwa um kleine Tools nachzuinstallieren. Dank dem hinzugekommenen Btrfs-Dateisystem können Sie Desinfec’t nun beispielsweise zu einem vollständigen Notfallarbeitsplatz inklusive Office-Anwendungen und aktuellen Treibern ausbauen.**

Von **Mattias Schlenker**

Wer das Live-System Desinfec't auf einem USB-Stick mit Tools aus den Ubuntu-Paketquellen erweitern will, musste bis jetzt immer einen Umweg gehen. Der Grund dafür ist, dass Desinfec't selbst auf einem USB-Stick nicht veränderbar ist und nach jedem Neustart wieder den Originalzustand herstellt. Damit man Tools dennoch dauerhaft installieren kann, müssen die einzelnen Debian-Pakete auf der beschreibbaren Signatur-Partition liegen. Die Desinfec't-Startskripte installieren diese dann bei jedem Systemstart neu. Dieser Ansatz klappt in der Regel mit kompakten Tools problemlos – darauf setzen wir auch bei der Installation von Desinfec't-Updates. Doch will man komplexere Anwendungen oder Treiber nachinstallieren, klappt das auf diesem Weg nicht.

Seit Desinfec't 2017 haben wir diese Probleme gelöst und führen ein anderes Konzept ein: Mit ein paar Vorbereitungen installieren Sie Anwendungen, Tools und Treiber dauerhaft direkt im System.

Dazu setzt Desinfec't auf das Dateisystem Btrfs, mit dem man Veränderungen in sogenannten Snapshots abspeichern kann. Diese liegen dann in Form von Subvolumes schichtweise über dem nach wie vor unveränderten Original (siehe Grafik unten „So funktioniert ein Btrfs-Stick"). Schlägt eine Modifikation fehl, wechseln Sie einfach zu einem funktionierenden Subvolume zurück.

## Btrfs-Stick erstellen

Standardmäßig setzt ein Desinfec't-Stick allerdings noch nicht auf Btrfs: Sie müssen ihn erst mit einer speziellen Option erstellen. Damit Desinfec't mit Btrfs vernünftig läuft, ist ein flinker USB-Stick oder besser noch eine USB SSD mit mindestens 64GB erforderlich. Dieser Platz ist nötig, da Desinfec't durch das Anlegen neuer Subvolumes mittels der Snapshot-Funktion wächst.

Am einfachsten erstellen Sie einen Btrfs-Stick aus einem laufenden Desinfec't: Dort klicken Sie auf dem Desktop das Icon „Desinfec't-Stick bauen" an. Im Anschluss setzen Sie lediglich ein Häkchen bei „Btrfs als Standard nutzen".

In den folgenden Beispielen erweitern Sie Desinfect't Schritt für Schritt, erzeugen Snapshots und starten das angepasste System aus einem neuen Subvolume.

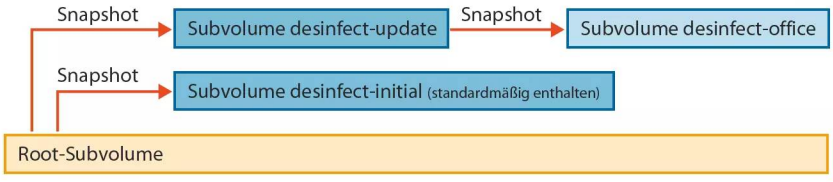
## Los gehts!

Als erstes Praxisbeispiel aktualisieren Sie Desinfec't und machen das Update persistent. Dafür installieren Sie es zuerst nach der alten Methode, sodass es aus dem RAM läuft. Dann verweben Sie das Update mit einem neu angelegten Subvolume, damit es dauerhaft in Desinfec't integriert ist.

Prüfen Sie zuerst, ob das Desinfec't-Update bereits installiert ist – das sollte in der Regel automatisch geschehen. Steht im Statusfenster oben rechts auf dem Desktop zum Beispiel „Desinfec't 2024/25 p1", hat es geklappt. Steht dort nur „Desinfec't 2024/25", müssen Sie den Update-Vorgang manuell anstoßen. Dafür öffnen Sie zunächst das Terminal, holen das Update aus unserem Repository und machen ein Upgrade von Desinfec't:

### So funktioniert ein Btrfs-Stick

Im Root-Subvolume befindet sich das Original-Desinfec't. Via Snapshot erstellt man ein neues Subvolume, das zunächst ein Klon des vorhergehenden ist. Neue Daten werden erst kopiert, wenn sich etwas ändert – etwa wenn Tools dazukommen. Nach einer Erweiterung startet man Desinfec't aus dem neuen Subvolume. Da das darunterliegende Subvolume unangetastet bleibt, kann man bei Problemen zurückwechseln.



```
sudo apt-get update
sudo apt-get -y dist-upgrade
```

Als Nächstes müssen Sie Schreibrechte für den Speicherort der Subvolumes unter /cdrom vergeben und die LZO-Komprimierung für neu geschriebene Dateien aktivieren – das spart Speicherplatz auf dem Stick. Dieser Schritt ist essenziell und für jede Subvolume-Operation in /cdrom nötig. Wenn im Folgenden mal etwas nicht klappt, prüfen Sie, ob Sie den Befehl eingegeben haben. Darüber hinaus sind für nahezu jede Aktion Root-Rechte (sudo) unabdingbar – wenn es hängt, überprüfen Sie auch das:

```
sudo mount -o remount,rw,compress=lzo /cdrom
```

Nun erstellen Sie via Snapshot ein neues Subvolume namens „desinfect-update“:

```
sudo btrfs subvolume snapshot ↴
↳/cdrom /cdrom/desinfect-update
```

Unter cdrom/desinfect-update/casper/filesystem.dir- findet sich darauffolgend eine deckungsgleiche Kopie vom Original-Desinfec’t. Damit Sie die Updates dort installieren können, hängen Sie den Ordner mit den deb-Archiven in das neu angelegte Subvolume:

```
sudo mount -o bind/var/cache/apt/archives
↳/cdrom/desinfect-update/casper/↴
↳filesystem.dir/var/cache/apt/archives
```

Nun wechseln Sie mit chroot (change root) in das neu angelegte Subvolume desinfect-update und installieren vorhandene Desinfec’t-Update-Pakete dort:

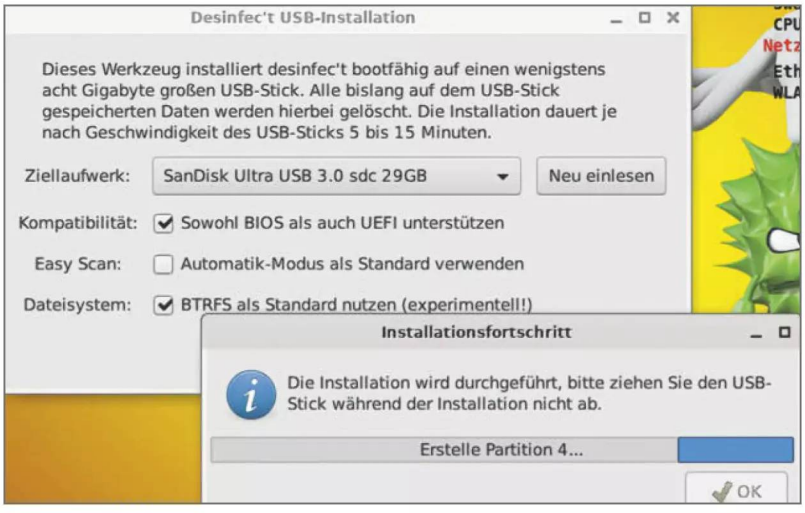
```
sudo chroot /cdrom/desinfect-update/↴
↳.casper/filesystem.dir
dpkg -i /var/cache/apt/archives/↴
↳.desinfect-meta*.deb
```

Mit exit verlassen Sie die chroot-Umgebung.

Nun sind Sie fast fertig und müssen nur noch das neue Subvolume mit aktualisiertem Desinfec’t als Standard-Subvolume setzen, damit das Sicherheitstool künftig daraus startet. Dafür brauchen Sie zunächst die ID des neuen Subvolumes, die sich via

```
sudo btrfs subvolume list /cdrom
```

ablesen lässt. Dort steht ganz oben immer das Subvolume desinfect-initial mit der ID 261. Neu angelegte Subvolumes zählt Btrfs jeweils immer um eins hoch. In diesem Beispiel trägt das Subvolume mit dem Desinfec’t-Update die ID 262. Um dieses als neues Standard-Subvolume festzulegen, geben Sie Folgendes ein:




**Um einen Desinfec’t-Stick mit Btrfs zu erstellen, müssen Sie die Option „Btrfs als Standard nutzen“ explizit anwählen.**

```
sudo btrfs subvolume set-default 262 /cdrom
```

Nun müssen Sie noch das Update-Paket „desinfect-meta“ aus /opt/desinfect/signatures/deb löschen, damit sich Btrfs und die alte Installationsmethode nicht in die Quere kommen. Das können Sie über den Filemanager machen (sudo thunar). Nach dem Löschen booten Sie Desinfec’t neu und fortan sollte das Sicherheitstool immer in der aktualisierten Version starten. Aus welchem Subvolume Desinfec’t bootet, sehen Sie nach der Eingabe von

```
cat /proc/mounts | grep /cdrom
```

unter „subvolid=ID“.

## Ubuntu-Pakete installieren

Um zusätzliche Anwendungen, Aktualisierungen und Treiber aus den Ubuntu-Paketquellen nachzuinstallieren, ist etwas mehr Vorarbeit als beim Desinfec’t-Update nötig. Das liegt daran, dass Sie hier

Anwendungen direkt in ein Subvolume downloaden und installieren und dafür eine vollständige chroot-Umgebung benötigen. In dem folgenden Beispiel rüsten Sie Desinfec't in einem Rutsch mit dem vollständigen Libreoffice aus und installieren einen Treiber für einen WLAN-Stick. Die folgende Herangehensweise ist exemplarisch für die Nachinstallation und Aktualisierung von Anwendungen und Treibern und muss bei jeder neuen Subvolume-Session von Anfang an durchgeführt werden. Damit sich die folgende Vorarbeit lohnt, empfiehlt es sich, wie in diesem Beispiel gleich mehrere Sachen hinzuzufügen.

Ausgangspunkt ist der Start aus dem Subvolume desinfect-update. Daraus erzeugen Sie mit der Snapshot-Funktion ein neues Subvolume namens „desinfect-office" – dieses ist ein direkter Abkömmling von desinfect-update. Damit Ubuntu-Pakete mittels apt-get im neuen Subvolume landen, sind weitere Mounts nötig:

```
sudo su
mount -o remount,rw,compress=lzo /cdrom
btrfs subvolume snapshot /cdrom ↵
↳/cdrom/desinfect-office
CHROOT=/cdrom/desinfect-office↵
↳casper/filesystem.dir
mount --bind /dev $CHROOT/dev
mount --bind /proc $CHROOT/proc
mount --bind /sys $CHROOT/sys
mount -t devpts devpts $CHROOT/dev/pts
mount -t tmpfs tmpfs $CHROOT/tmp
```

Nun machen Sie Nameserver in der chroot-Umgebung bekannt. Die DNS-Einstellung gelingt via

```
mount --bind /run/resolvconf/↵
↳resolv.conf $CHROOT/run/↵
↳resolvconf/resolv.conf
```

Jetzt erzeugen Sie noch ein Dummy-Shell-Skript, damit bei der Nachinstallation keine Dienste dazwischenfunken. Das gelingt mit einem Editor wie Scite:

```
scite $CHROOT/usr/sbin/policy-rc.d
```

Das Skript umfasst nur zwei Zeilen:

```
#!/bin/sh
exit 101
```

Nun speichern Sie die Änderungen, schließen die Datei und machen sie ausführbar:

```
chmod 0755 $CHROOT/usr/sbin/policy-rc.d
```

Ein kleines Skript kümmert sich um die Mounts, die DNS-Einstellung und das Dummy-Shell-Skript. Sie installieren und starten es wie folgt:

```
sudo su

apt-get update
apt-get install desinfect-btrfs-tools
CHROOT=/cdrom/desinfect-office/↵
↳casper/filesystem.dir
chrootbindmounts mount $CHROOT
```

Damit Desinfec't auf die Ubuntu-Paketquellen zugreifen kann, müssen Sie diese via

```
scite $CHROOT/etc/apt/sources.list
```

aktivieren. Dafür entfernen Sie in der Liste die Doppelkreuze vor den Einträgen „Main", „Updates" und „Security" und sperren den Zugriff auf das Desinfec't-Repository mittels eines Doppelkreuzes, sonst könnte es im Folgenden zu Konflikten kommen. Speichern und schließen Sie die Datei. Anschließend

## Desinfec't, Btrfs und Windows 10

Bei Desinfec't 2024/25 haben wir uns dazu entschieden, Btrfs nicht als Standard zu nehmen – Sie müssen diese Option explizit auswählen. Im aktuellen Desinfec't hat das Dateisystem noch experimentellen Status. Der Grund dafür ist, dass wir die Integration von Btrfs zurückstellen mussten, weil Windows 10 seit Version 1703 zusätzliche Partitionen auf USB-Sticks erkennt. Steckt man einen Btrfs-Stick in den Rechner, bietet das Betriebssystem jetzt eine Formatierung aller für Windows unlesbaren Partitionen an. Das ist nicht nur lästig, sondern auch gefährlich: Dadurch kann man sich einen Btrfs-Stick zerschießen. Da wir bislang keinen Weg gefunden haben, Windows das abzugewöhnen, mussten wir zu einem Hack greifen: Das reguläre Desinfec't 2024/25 arbeitet mit versteckten Partitionen. Bisher konnten wir dieses Schema allerdings nicht für einen Btrfs-Stick anwenden – aber wir arbeiten daran.

wechseln Sie per chroot in das Verzeichnis des Subvolumes und aktualisieren die Paketlisten:

```
chroot $CHROOT
apt-get update
```

Nun können Sie mittels

```
apt-get install libreoffice libreoffice-l10n-de
```

das LibreOffice-Paket installieren. An dieser Stelle müssen Sie nichts aus /opt/desinfect/signatures/ deb löschen, da Anwendungen aus den Ubuntu-Paketquellen im Gegensatz zu Desinfec't-Updates nicht standardmäßig auf der Signatur-Partition landen.

Zusätzlich fügen Sie mit dieser Installationsmethode neue Firmware und Treiber hinzu. Das folgende Beispiel stattet den in Desinfec't enthaltenen Treiber für WLAN-Sticks auf Broadcom-Basis für eine erweiterte Kompatibilität mit einer proprietären Firmware aus. Alternativ können Sie das Ganze natürlich auch mit passenden Treibern für WLAN-Sticks mit Chips von anderen Herstellern durchspielen:

```
apt-get install b43-fwcutter ↵
↳firmware-b43-installer
```

Erkennt Desinfec't nach dem Neustart Ihren Broadcom-Stick immer noch nicht, können Sie mit den folgenden Befehlen einen proprietären Broadcom-Treiber installieren. Erstellen Sie dafür zuerst eine Datei via

```
scite /etc/modprobe.d/blacklist-b43.conf
```

und fügen Sie folgende Zeilen ein:

```
b43
b43legacy
```

Anschließend installieren Sie wie folgt den proprietären Broadcom-Treiber:

```
sudo apt-get install broadcom-sta-source ↵
↳broadcom-sta-common broadcom-sta-dkms
```

Wenn Sie eine Subvolume-Session aus den Ubuntu-Repositorys beenden und nichts mehr installieren möchten, leiten Sie dies mit dem Befehl apt-get clean ein. Nun verlassen Sie mit exit die chroot-Umgebung. Dann löschen Sie die eingangs angelegte Datei mit

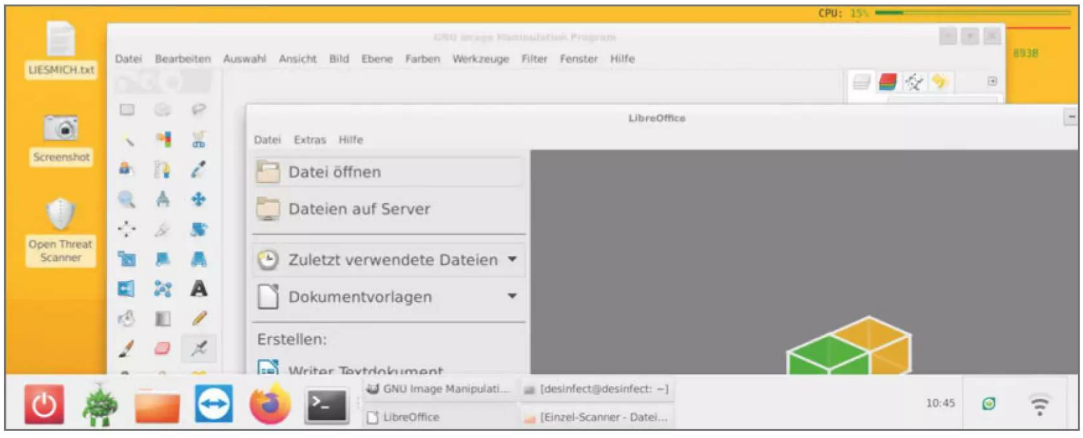
```
sudo rm $CHROOT/usr/sbin/policy-rc.d
```

Alternativ erledigen Sie dies und das Lösen der Mounts nach der Eingabe von apt-get clean mit dem Skript aus unseren Btrfs-Tools.

```
chrootbindmounts umount $CHROOT
```

Als Nächstes kommentieren Sie noch die Ubuntu-Repositories via

```
scite $CHROOT/etc/apt/sources.list
```




**Dank Btrfs können Sie Desinfec't um größere Anwendungen erweitern und sich so ein Notfallsystem mit kompletter Office-Umgebung bauen.**

## Mountpoint /cdrom fehlt?

Mit neueren Kerneln kann es vorkommen, dass der Mountpoint /cdrom nicht mehr sichtbar ist, nachdem Ubuntus Bootscripte das Rootverzeichnis gewechselt haben. Für diesen Fall haben wir im Bootmenü den Eintrag „Desinfec't im DVD Modus booten“ hinzugefügt. Er startet nicht vom /cdrom/casper/filesystem.dir, sondern einem auf der Btrfs-Partition abgelegten ISO-Image. Die weitere Vorgehensweise ist dann identisch zur bisherigen.

aus und reaktivieren die Desinfec't-Paketquelle. Abschließend legen Sie desinfect-office als Standard fest:

```
sudo btrfs subvolume set-default 263 /cdrom
```

Jetzt starten Sie Desinfec't neu – erst dann stehen die eben installierten Anwendungen und Treiber zur Verfügung.

## Andere Kernel nutzen

Ist die verwendete Hardware zu neu oder zu alt, helfen oft ältere oder neuere Kernel. Bei betagten PCs kann es sinnvoll sein, einen der alten Long-Term-Support-Kernel zu nutzen. Ist die Hardware brandneu, müssen aktuelle Mainline-Kernel her – bei Redaktionsschluss war dies 6.10 Ubuntu stellt diese Kernel ohne Patches und ohne Tests bereit. Seit Ubuntu 18.04 kann man die Mainline-Kernel auch mit Live-Systemen verwenden. Der einfachste Weg ist, zunächst auf www.kernel.org nachzusehen, welche Mainline-Kernel aktuell sind. Dann kann man direkt im Mainline-Archiv (siehe ct.de/wy18) den gewünschten Kernel herunterladen – brandneue Kernel sind in der Regel bereits einige Stunden nach der Veröffentlichung erhältlich.

Installieren Sie linux-modules*generic*.deb und linux-image*generic*.deb des gewünschten Kernels simpel mit den Befehlen `dpkg -i dateiname`. Nach der Installation kopieren Sie den Kernel „vmlinuz*“ und das Initramfs „initrd*“ des neuen Kernels auf die Boot-Partition (Label „desinfSYS“) in den Ordner „casper“. Entweder überschreiben Sie den vorhandenen Kernel oder Sie benennen ihn entsprechend um, beispielsweise „initrd.6x und vmlinuz.6x“. Beachten Sie, dass Syslinux Dateinamen in der 8.3-Konvention erfordert. Editieren Sie dann die beiden Bootdateien „boot/grub/grub.cfg“ und „isolinux/ os.cfg“, wo Sie einfach den ersten vorhandenen Eintrag kopieren und mit angepassten Dateinamen versehen, damit Desinfec't den neu installierten Kernel nutzt.

## Zurücksetzen

Wenn beim Anpassen etwas schiefgelaufen ist, können Sie mit wenigen Schritten zum Root-Subvolume wechseln, um Desinfec't in den Originalzustand zurückzuversetzen:

```
sudo mount -o remount,rw,compress=lzo /cdrom
sudo btrfs subvolume set-default 5 /cdrom
```

Falls Desinfec't nach einer Modifikation nicht mehr startet, müssen Sie den Umweg über die DVD, einen Desinfec't-Stick oder eine andere Linux-Distribution gehen. Läuft das System, greifen Sie daraus auf den am Computer angeschlossenen defekten Btrfs-Stick zu, in unserem Fall ist das sdd5, und führen folgende Befehle aus:

```
mkdir /tmp/btrfs
sudo umount /dev/sdd5
```

Nun aktivieren Sie auf dem Stick das Root-Subvolume:

```
sudo mount -o rw /dev/sdd5 /tmp/btrfs
sudo btrfs subvolume set-default 5 /tmp/btrfs
sudo umount /tmp/btrfs
```

Anschließend sollte Desinfec't wieder laufen und im Originalzustand starten.

## Basteln auf eigene Gefahr

Dank Btrfs und unseren Anleitungen können Sie Desinfec't quasi grenzenlos erweitern. Geht dabei etwas kaputt, wechseln Sie problemlos zu einem funktionierenden Subvolume zurück. Im offiziellen Desinfec't-Forum (siehe heise.de/s/00MMk) tauschen sich außerdem Tüftler aus. Also keine Angst und viel Spaß beim Basteln! (des) ct

**Desinfec't-Forum**
heise.de/s/00MMk

**Tipps & Tricks für Btrfs-Sticks**
ct.de/wy18


# Hilfe bei Windows-Problemen

**Wenn Windows brachliegt, kann unser Linux-basiertes Notfallsystem helfen – egal, ob nun gerade kein anderes Werkzeug zur Hand ist oder Sie sich auf der Unix-Kommandozeile wohler fühlen. Dieser Artikel lotet die Möglichkeiten aus.**

Von **Peter Siering**

Bei Schädlingsverdacht ist es immer eine gute Idee, ein neutrales Werkzeug von einem Wechseldatenträger zu starten und das vermeintlich verseuchte System zu untersuchen. Nur das liefert unabhängige Ergebnisse. Unser Desinfec't ist genau dafür gemacht: Sie können es aber ebenso gut dafür verwenden, eine aus anderen Ursachen vergurkte Windows-Installation zu reparieren oder ihr nur auf den Zahn zu fühlen, etwa sonst nicht zugängliche Dateien zu inspizieren.

Im Grundlagen-Artikel „Desinfec't 2024/25 im Nu einsetzen“ (Seite 10) steht, wie Sie Desinfec't auf einen USB-Stick bannen und benutzen. Das Folgende baut darauf auf und geht davon aus, dass Sie einen solchen Stick erfolgreich an einem Windows-PC starten konnten. Um überhaupt auf ein auf dem PC installiertes Windows und seine Laufwerke zunächst lesend zugreifen zu können, sollten Sie auf dem Desinfec't-Desktop „Win-Drives einhängen“ doppelt anklicken. Anschließend können Sie sich im Dateimanager (Desinfec'ts Explorer) gefahrlos umsehen, den Sie über das Ordnersymbol in der Taskleiste erreichen. Die Windows-Laufwerke finden Sie in der Seitenleiste des Dateimanagers unter „+ Andere Orte“. Sie tauchen dort namentlich auf, oft aber mit kryptischer Bezeichnung. Achtung: Wenn Sie direkt eine solche Bezeichnung anklicken, hängt Desinfec't das Laufwerk beschreibbar ein.

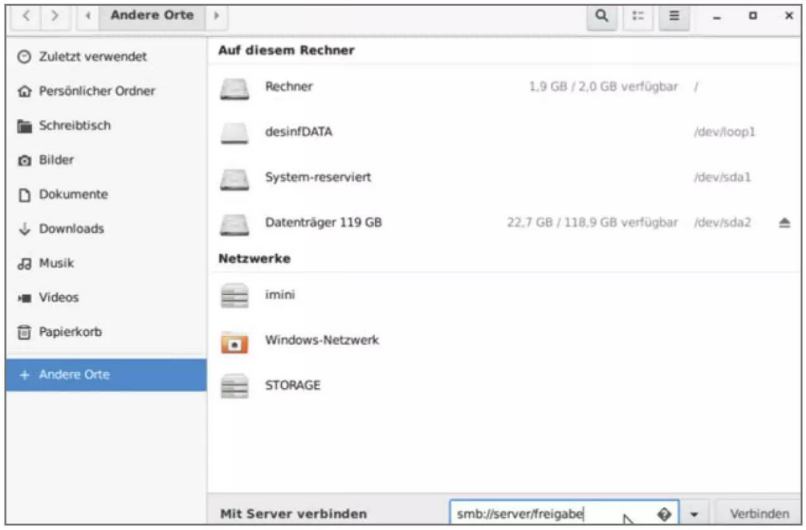
Wenn Sie sich im Dateibaum eines Windows-Systemlaufwerks umsehen, fällt auf, dass die Ordner englische Namen in Desinfec't tragen; der Windows-Explorer zeigt normalerweise deutsche Bezeichnungen. Anders als unter Windows ist auch: Sie können sich frei in allen Verzeichnissen bewegen. Desinfec't schert sich nicht um die in Windows gesetzten Zugriffsrechte, beachtet also die ACLs nicht. Sollten Sie bisher geglaubt haben, dass Zugriffsrechte für Dateien neugierigen Zeitgenossen den Zugriff verwehren, werden Sie hier eines Besseren belehrt.

## Windows-Daten finden

Somit ist es mit Desinfec't einfach möglich, Dateien von einem Windows-PC herunterzukratzen, eben auch dann, wenn Sie sich nicht einmal mit einem Konto daran anmelden können. Die Dateien der Nutzer finden Sie üblicherweise unterhalb des Ordners „Users". Dort speichert Windows wirklich alles, was ein Konto betrifft, auch den benutzerspezifischen Teil der Registry, später mehr dazu.

Der Dateimanager kennt die üblichen Operationen wie Kopieren und Einfügen. Sie können Tastenkürzel (Strg+C und Strg+V) nutzen oder das Menü dazu bemühen. Beachten Sie: So wenig, wie sich Desinfec't überhaupt um die ACLs kümmert, kopiert es sie auch. Die einzige Möglichkeit, unter Linux Dateien auf einem NTFS-Laufwerk inklusive der ACLs auf ein anderes zu kopieren, besteht im Anfertigen einer 1:1-Kopie (etwa mit ntfsclone oder dem nachinstallierbaren Clonezilla).

Sollten Sie Ihre Windows-Partition nicht finden, etwa weil mehrere kleinteilig partitionierte Festplatten im System stecken, hilft die Laufwerksübersicht „Gnome Disks" im Expertentools-Ordner auf dem Desinfec't-Desktop. Dort können Sie gezielt einzelne Partitionen einhängen, also erreichbar machen. Doch Vorsicht: Wenn Sie diesen Weg gehen, dann bindet Desinfec't diese nicht nur les-, sondern beschreibbar ein. Unsere Empfehlung ist, das nur in begründeten Ausnahmefällen zu tun.




**Im Desinfec't-Dateimanager führt „+Andere Orte" zu den Windows-Partitionen und auch ins Netzwerk. Vorsicht beim Klicken auf Windows-Laufwerke: Sie werden gleich beschreibbar eingehängt. Besser bemühen Sie „Win-Drives einhängen" auf dem Desktop. So besteht keine Gefahr, dass Sie versehentlich Daten auf die Laufwerke schreiben.**

Die Linux-Funktionen für Zugriffe auf NTFS benutzen eine eigene Implementierung des Dateisystems – die birgt immer die Gefahr, dass beim Schreiben Daten in Mitleidenschaft gezogen werden. Deswegen geht Desinfec't auch konservativ vor und benennt als schädlich erkannte Dateien nur um, anstatt sie zu verschieben oder zu löschen. Wann immer möglich sollten Sie ebenso vorgehen. Wenn Sie schreiben lassen, tun Sie das idealerweise nur mit einem Backup oder Image in der Hinterhand.

Es gibt Dateien, an die Desinfec't nicht herankommt: Einzelne verschlüsselte NTFS-Dateien (EFS) erreicht es nicht ohne vorherigen Export von Schlüsseln, da die an Windows-Benutzerkonten geknüpft sind. Kein Problem stellen hingegen Laufwerke dar, die mit Bitlocker geschützt sind, also mit der Laufwerksverschlüsselung von Windows. Ein solches Laufwerk lässt sich auf der Kommandozeile mit wenigen Befehlen aufsperren. Wie das geht, steht im Artikel „PC-Schädlinge finden und entsorgen".

Eine Anmerkung noch zu Windows-Installationen oder Datenplatten, die auf einem Software- beziehungsweise BIOS-RAID gründen: Das hinter dem Symbol auf dem Desinfec't-Desktop „Win-Drives einhängen" hinterlegte Skript schafft es nicht, die Windows-Partition zu finden und einzuhängen. Benutzen Sie in einem solchen Fall besser die Laufwerksübersicht.

Halten Sie dort Ausschau nach RAID-Laufwerken, meiden Sie andere, die Teil eines RAID-Verbundes sind. Die Warnung ist präventiv: Bei uns weigerte sich Desinfec't, RAID-Mitglieder anzurühren, aber wir sind nicht sicher, ob das in jedem Fall so ist. Da die Laufwerksübersicht stets beschreibbar einhängt, können Sie im Nachgang Desinfec't die Schreiboption entziehen – den Namen des Einhängpunktes müssen Sie anpassen:

```
sudo mount -o ro,remount ↵
↳/media/desinfect/thinkssd
```

## Passwort vergessen

Ein typisches Problem auf Windows-PCs ist, dass sie von einem auf den anderen Tag den Benutzer nicht mehr hineinlassen. Das kann diverse Ursachen haben: Der Benutzer hat sein Kennwort vergessen

oder das Benutzerprofil ist so stark beschädigt, dass Windows die Anmeldung verweigert oder ein Ersatzprofil verwendet. Ein Seiteneffekt kann sein, dass keine Anmeldung mehr mit administrativen Rechten möglich ist.

Das vergessene Kennwort kann man mit verschiedenen Mitteln angehen: Desinfec't enthält das Programm `chntpw`, das direkt die Benutzerdatenbank in der Registry einer Windows-Installation (SAM genannt) bearbeiten kann. Dabei verhält es sich wie mit den Schreibzugriffen auf NTFS: Man sollte das nur in Notfallsituationen und nicht ohne Backup seiner Daten tun. Und ganz wichtig: Finger weg von Passwortänderungen, wenn Dateien EFS-verschlüsselt sind, die kriegt man danach nie wieder im Klartext zu sehen.

Damit der Zugriff auf die Passwortdatenbank gelingt, müssen Sie die Windows-Partition so einhängen, dass sie beschreibbar ist. Das muss in jedem Fall sein, selbst wenn Sie zunächst nur schauen, aber nichts ändern wollen. Klicken Sie auf dem Desktop „Win-Drives aushängen" (wenn Sie die zuvor eingehängt haben). Öffnen Sie dann in den Expertentools die Laufwerksübersicht „Gnome Disks", wählen Sie die Windows-Partition aus und klicken Sie den „Play"-Knopf (das nach rechts gerichtete Dreieck) an. Desinfec't hängt die Partition dann beschreibbar ein.

Achtung: Die anderen Bedienelemente in der Laufwerksübersicht bergen hohes Gefahrenpotenzial. Sie können hier mit wenigen Klicks auch Ihre Windows-Partition löschen – die Programme fragen nach, aber wir wollten das hier nicht unangesprochen lassen. Generell sollten Sie sich stets bewusst sein, dass Sie Ihre Windows-Partition als beschreibbares Medium eingehängt haben – minimieren Sie den Zeitraum. Lassen Sie die Laufwerksübersicht offen und betätigen Sie den Stop-Knopf zum Aushängen so bald wie möglich.

Zunächst aber entnehmen Sie dem Programm den Einhängpunkt für Ihre Windows-Installation. Öffnen Sie ein Terminalfenster und wechseln Sie mit

```
cd /media/desinfect/WinPladde/⮒
↳Windows/System32/config
```

in das Verzeichnis, in dem die Registry Ihrer Windows-Installation liegt. `WinPladde` müssen Sie durch den Volume-Namen Ihrer Systempartition ersetzen.

Jetzt können Sie mit `chntpw -l SAM` eine Liste der bekannten Konten ausgeben lassen. Mit `chntpw -u <user> SAM` rufen Sie ein Konto zur Bearbeitung auf. Das Programm zeigt dann ein detailliertes Menü mit diversen Details zum jeweiligen Benutzerkonto. So können Sie zum Beispiel das standardmäßig nicht benutzbare Administrator-Konto aktivieren oder das Kennwort eines Benutzers löschen, sodass er sich ohne anmelden kann (Vorsicht: EFS-Dateien des Benutzers sind danach nicht mehr lesbar).

Wir empfehlen vor solchen Eingriffen, die betroffene Datei „SAM" als Versicherung zunächst auf den USB-Stick zu kopieren (mit `sudo/opt/desinfect/signatures`). Geht der Eingriff schief, können Sie die gegebenenfalls wiederherstellen – sollte Ihnen das Schreiben von NTFS mit Linux missfallen, können Sie dafür einen anderen Windows-PC einspannen, an den Sie die Festplatte stöpseln, auf der Ihre Windows-Installation residiert. Das Rücksetzen des Passwortes klappt leider nur für lokale Konten, nicht aber für ein Microsoft-Konto.

## Profil futsch

Mit `chntpw` können Sie auf der Kommandozeile auch die Registry durchstöbern und ändern. Das Prinzip ist das gleiche wie beim Ändern von Kennwörtern. Als Parameter übergeben Sie den Namen der Registry-Datei (die Sie idealerweise vorher kopieren): `chntpw -e SYSTEM` würde beispielsweise den Systemteil der Registrierung Ihrer Windows-Installation zugänglich machen. Wenn Sie lieber mit der Maus unterwegs sind: Starten Sie im Terminalfenster `fred`.

Die Datei, die die benutzerspezifischen Teile der Registry enthält, finden Sie als versteckte Datei NTUSER.DAT in den Profilverzeichnissen der Konten unter „Users" (in einem solchen Verzeichnis mit `chntpw -e NTUSER.DAT` zu öffnen). Solch eine Datei nimmt durchaus mal Schaden.

Dass das der Fall ist, merkt der Nutzer beim Anmelden: Windows sagt plötzlich, es bereite etwas vor (wie bei der allerersten Anmeldung). Manchmal weist es direkt darauf hin, dass eine Anmeldung beim Konto nicht möglich sei. Oft erscheint der Hinweis „Sie wurden mit einem temporären Profil angemeldet" gekoppelt mit der Drohung, dass angelegte Dateien verloren gehen. Ältere Windows-Versionen legen von sich aus neue Profilverzeichnisse in \Users an, Windows 10 gerät gern in eine Anmeldeschleife.

Desinfec't kann vornehmlich bei der Diagnose helfen: Eine Null Byte große NTUSER.DAT ist eindeutig. Eine NTUSER.DAT, die nicht mal der Registry-Editor von chntpw zu öffnen vermag, kann man wohl auch abschreiben. Wenn das betroffene Konto das einzige auf dem PC war, das über Administrationsrechte verfügt hat, können Sie mit dem zuvor ge-

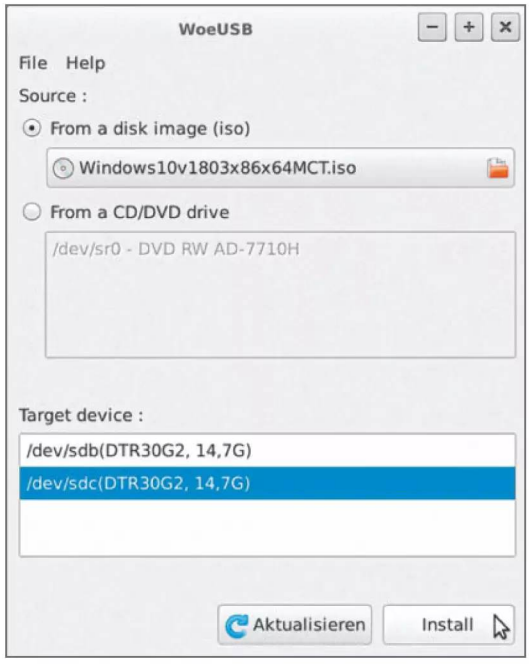
**Weitere Hinweise**
ct.de/w9ax

nannten Kniff, das bei der Installation angelegte, aber deaktivierte Konto namens „Administrator“ anknipsen und sich auf diese Weise Zutritt zum PC verschaffen.

Das weitere Vorgehen hängt von Ihrem Experimentierwillen ab: Man könnte die NTUSER.DAT eines frisch angelegten neuen Nutzers in das Verzeichnis des beschädigten Profils kopieren und eine Anmeldung versuchen. Besser ist es in der Regel, gezielt die alten Daten in ein neues Profil zu kopieren, also sich einzeln die Verzeichnisse vorzunehmen wie Desktop, Documents, Links und woran sonst das Glück des betroffenen Nutzers hängt.

Wenn Windows partout auf das falsche Profil-Verzeichnis zugreift (manchmal legt es die auch einfach unter einem abgewandelten Namen neu an), hilft womöglich ein Eingriff in der Registry. Unter HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList (Datei SOFTWARE im o.g. Verzeichnis) existiert für jeden dem System bekannten Benutzer ein Schlüssel, der als Namen den SID des Nutzers hat (eine Windows-interne ID für Benutzer).

Klicken Sie sich einfach durch, bis Sie den richtigen Nutzer identifiziert haben und passen Sie gegebenenfalls den Wert in ProfileImagePath an.




**Mit WoeUSB kommt man auch ohne lauffähiges Windows nur mit Desinfec’t im Gepäck zu einem USB-Installationsstick für eine frische Windows-Installation – ISO, Installationsmedium oder Internet-Zugang vorausgesetzt.**

## Desinfec’t erweitern

Die soweit erwähnten Werkzeuge stecken bereits in Desinfec’t. Eine Stick-Installation können Sie in Eigenregie erweitern, indem Sie Pakete über die Debian-/Ubuntu-Paketverwaltung installieren. Das geht mit wenigen Handgriffen – öffnen Sie ein Terminalfenster und bearbeiten Sie in einem Editor die Paketquellen

```
sudo nano /etc/apt/sources.list
```

Entfernen Sie das Kommentarzeichen (#) vor den ersten drei Zeilen und speichern Sie mit Strg+O. Mit STRG+X beenden Sie den Editor Nano.

Mit `sudo apt-get update` müssen Sie zuerst die Paketverzeichnisse einlesen lassen und können dann mit `sudo apt-get install <Paketname>` jedes erreichbare Paket installieren. Das Ganze hat Grenzen: Nicht alles aus der Ubuntu-Welt lässt sich installieren (das aktuelle Desinfec’t baut auf Jammy Jellyfish auf). Das Live-System zwackt Teile des Hauptspeichers ab und der ist nun mal begrenzt. Dasselbe gilt für den Stick: Auch hier ist der Platz endlich.

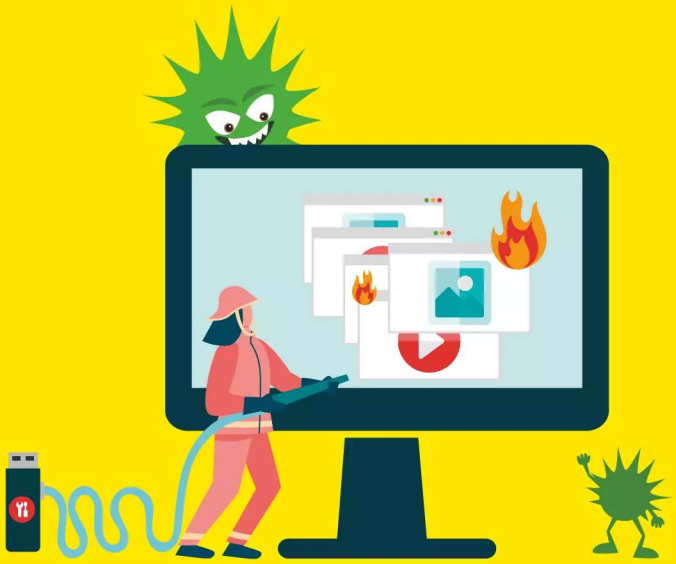
Die Änderung der Paketquellen und die anschließend hinzugefügten Pakete gehen verloren, wenn Sie Desinfec’t herunterfahren. Die Paketeinrichtung können Sie erhalten, indem Sie nach der Installation die Pakete in einem Terminalfenster auf den Stick kopieren:

```
sudo cp /var/cache/apt/archives/* ↴
↳/opt/desinfect/signatures/deb
```

Ein nützliches Programm ist WoeUSB. Es bringt Desinfec’t bei, bootfähige Installationssticks für Windows anzufertigen. Wenn Sie die Pakete nicht wie zuvor beschrieben dauerhaft auf Ihren Stick packen, ist der Spuk aber nach einem Reboot vorbei, denn Desinfec’t verwirft hinzugefügte Paketquellen bei jedem Neustart. Zunächst aber fügen Sie das Hilfsprogramm hinzu:

```
sudo apt-get update
sudo apt-get install woeusb
```

Anschließend können Sie mit `woeusbgui` die Bedienoberfläche des Helfers starten. Er erwartet eine ISO-Datei oder DVD als Quelle (Source) und einen USB-Stick als Kopierziel (Target). Achten Sie darauf, dass Sie nicht versehentlich den Desinfec’t-Stick erwischen – davor schützt das Programm nicht. (ps) **c't**



# Fotos und Dateien retten

**Hat man versehentlich den falschen USB-Stick formatiert oder die USB-Festplatte vom Schreibtisch gefegt, wird einem oft erst bewusst, welch wichtige Daten darauf gespeichert waren. Mit Desinfec't haben Sie ein gutes Werkzeug, um zumindest einen Teil Ihrer Daten zu retten.**

Von **Mirko Dölle**

Ein kurzer Moment der Unachtsamkeit genügt, um Hochzeitsfotos, Buchführungsunterlagen oder die E-Mails der letzten Jahre ins Nirvana zu befördern, weil man den falschen USB-Stick oder die falsche SD-Karte formatiert oder überschreibt. Auch wenn heutige USB-Sticks und SSDs robuster als frühere externe Festplatten sind, Hardware-Defekte treten weiterhin auf: Bei billigen Sticks versagen die Flash-Speicher, beim Runterfallen reißen Lötpads ab oder die Controller werden Opfer statischer Elektrizität – das Spektrum ist breit.

Zeigen sich die ersten Anzeichen von Datenverlust, fehlen Dateien oder ganze Verzeichnisse oder Sie können auf einzelne Dateien oder ganze Laufwerke nicht mehr zugreifen, sollten Sie zunächst den Stand Ihres letzten Backups prüfen: Von wann ist es und wie viel Arbeit müssten Sie investieren, um die Daten aus dem Backup auf den aktuellen Stand zu bringen?

Der Hintergrund ist, dass Datenrettung viel Zeit erfordert und der Ausgang ungewiss ist. Im Zweifel sind Sie besser beraten, mit dem Backup vom Vortag weiterzuarbeiten und die heutige Arbeitszeit verloren zu geben, als sich stundenlang mit der Datenrettung zu versuchen und am Ende nichts zu gewinnen.

Auch die Möglichkeit, einen professionellen Datenretter zu beauftragen, sollte man nicht vergessen.

Die Erstdiagnose, die einen verbindlichen Kostenvoranschlag für die spätere Datenrettung umfasst, kostet je nach Anbieter und Dringlichkeit zwischen 50 und 300 Euro.

Je nach Schaden (physisch oder logisch), Speichertyp und -größe kostet die Datenrettung im Schnitt zwischen 60 und 1500 Euro. Das ist für die Rettung einer Schulhausaufgabe sicher zu viel, für die gerade aufgenommenen Hochzeitsfotos, um eine Steuerschätzung des Finanzamts zu verhindern oder um eine Abschlussarbeit termingerecht fertigzubekommen aber wahrscheinlich gerechtfertigt. In diesen Fällen sollten Sie jedoch alle Selbstversuche unterlassen, denn dadurch können die Daten schlimmstenfalls unwiederbringlich zerstört werden.

## Physisch, logisch?

Wie gut Ihre Aussichten sind, die Daten in Eigenregie wiederherstellen zu können, hängt von der Art der Beschädigung ab. Hardware-Fehler lassen sich mit Hausmitteln fast nie reparieren. Hinzu kommt, dass sich mechanische Defekte auf Festplatten und nicht mehr zugreifbare Zellen in Flash-Speichern schnell vermehren, wenn das Medium weiter in Betrieb bleibt.

Deshalb gilt es bei Hardware-Defekten, das Medium in einem Durchgang ein letztes Mal auszulesen, bevor Sie es außer Betrieb nehmen. Das dabei erstellte Abbild dient Ihnen anschließend als Grundlage für die Datenrettung.

Für diesen Zweck eignet sich Desinfec't besonders gut, da es die wichtigsten Tools zur Datenrettung bereits an Bord hat und die Dateisysteme von Windows, macOS und Linux unterstützt. Alles, was Sie benötigen, ist die Desinfec't-DVD oder einen USB-Stick mit Desinfec't. Außerdem eine ausreichend große Datenhalde, die Ihre geretteten Daten aufnimmt – ein großer USB-Stick oder eine externe Festplatte sind hierfür gut geeignet. Wie Sie Desinfec't auf einem USB-Stick installieren und booten, haben wir im Artikel „Trojaner, Backdoors & Co. aufspüren“ bereits ausführlich beschrieben.

Ein erstes Indiz für einen mechanischen Defekt sind veränderte Laufgeräusche und Zugriffsgeräusche der Festplatte. SSDs und andere Flash-Speicher machen natürlich keine Geräusche, sodass Sie hier per Software nach Fehlern fahnden müssen (siehe Artikel „Profi-Scanner effektiv nutzen“). Für die Diagnose der Hardware eignet sich vor allem die Self-Monitoring, Analysis and Reporting Technology, kurz S.M.A.R.T oder auch Smart genannt. Dabei überprüft sich das Laufwerk in regelmäßigen Abständen selbst und zeichnet außerdem besondere Vorkommnisse wie Lese- und Schreibfehler, aber auch zu hohe Laufwerkstemperaturen auf.

Um die Daten mit den Smartmon-Tools unter Linux abzurufen, müssen Sie zunächst den Laufwerksnamen ermitteln. Dazu rufen Sie, bevor Sie das defekte Laufwerk anschließen, im Terminal den Befehl `lsblk` auf. Er listet alle aktuell verfügbaren physischen und virtuellen Laufwerke auf. Dann schließen Sie das defekte Laufwerk an und rufen erneut `lsblk` auf. Durch den Vergleich der beiden Aufrufe finden Sie zuverlässig den Namen Ihres Laufwerks heraus.

Etwas schwieriger ist es, wenn die defekte Festplatte oder SSD noch im Rechner eingebaut ist. Dann müssen Sie die Einträge durchforsten und anhand der Größenangaben der Laufwerke herausfinden, welchen Namen Ihre interne Festplatte hat, etwa `/dev/sda` oder `/dev/sdb`. Doch Vorsicht, auch ein Desinfec't-USB-Stick bekommt einen Laufwerksnamen zugeordnet, manchmal sogar /dev/sda.

Sofern die Partitionstabelle des defekten Laufwerks noch lesbar war, zeigt `lsblk` neben dem Laufwerksnamen, zum Beispiel /dev/sdb, auch noch die Namen der einzelnen Partitionen an, etwa /dev/sdb1 oder /dev/sdb2. Auch hier können Sie anhand der Größenangabe abschätzen, welche Daten wohl darauf gespeichert sind. Um die Beispiele verständlich zu halten, verwenden wir nachfolgend /dev/sdb als Laufwerksnamen. Sollte Ihr Laufwerk einen anderen Namen erhalten haben, müssen Sie das in den Beispielen entsprechend anpassen. Mit dem Befehl

```
sudo smartctl -a /dev/sdb
```

bekommen Sie die Selbsttestdaten des Laufwerks /dev/sdb angezeigt. Die zugegeben wenig übersichtliche Liste hat numerische IDs am Anfang der Datenzeilen, über die Sie die einzelnen Angaben leicht wiederfinden können.

Bei defekten Laufwerken finden Sie üblicherweise eine hohe Raw Read Error Rate (ID 1), die (korrigierbare) Lesefehler anzeigt. Da Festplatten und SSDs automatisch schlechte Sektoren gegen gute aus einem reservierten Bereich tauschen, sollten Sie außerdem ein Auge auf die IDs 5, 196 und 197 haben: Hier finden Sie heraus, wie viele schlechte Sektoren bereits ausgetauscht wurden (ID 5), wie oft das vorkam (ID 196) und wie viele schlechte Sektoren noch nicht ausgetauscht werden konnten, weil

sie noch mit Daten belegt sind (ID 197) – der Austausch erfolgt immer dann, wenn ein schlechter Sektor überschrieben wird.

Während Sie bei rein logischen Laufwerksfehlern risikolos mit dem Befehl

```
sudo dd if=/dev/sdb of=disk.img
```

ein vollständiges Image des beschädigten Laufwerks im aktuellen Verzeichnis erstellen können, müssen Sie bei Hardware-Defekten abwägen, mit welcher Methode Sie das Image Ihrer Daten erstellen: Jeder Leseversuch eines beschädigten Bereichs kann dazu führen, dass noch mehr Daten unlesbar werden. Außerdem bricht `dd` beim ersten Lesefehler ab.

Ist das beschädigte Laufwerk größtenteils belegt, verwenden Sie am Besten ddrescue, um das Image zu erstellen:

```
ddrescue -A /dev/sdb disk.img
```

Während `dd` das Medium sequenziell, Sektor für Sektor, ausliest, springt `ddrescue` beim ersten Lesefehler großzügig über den beschädigten Sektor hinweg und versucht, sich vom hinteren Ende dem defekten Bereich zu nähern. Das verlangsamt durch die längeren Zugriffszeiten zwar den Kopiervorgang, vermeidet aber, dass sich das Programm an einem größeren defekten Bereich „festfrisst“ und stattdessen einen Bereich anspringt, wo es möglicherweise noch gute Daten gibt.

Müssen Sie die Daten einer weitgehend leeren Windows-Partition retten, können Sie zu `ntfsclone` greifen:

```
ntfsclone --rescue -o ntfs.img ↵
↳/dev/sdb1
```

## Auf Eis gelegt

Lesefehler bei Festplatten und Flash-Speichern treten häufig temperaturabhängig auf oder verschlimmern sich mit zunehmender Laufwerkstemperatur. So werden defekte MicroSD-Karten mitunter derart heiß, dass sie manchmal sogar das Gehäuse des Kartenlesers anschmelzen.

Kühlt man die Medien, lassen sich manchmal mehr Daten wiederherstellen als bei höheren Temperaturen. Ein Tipp ist deshalb, widerspenstige Medien sprichwörtlich auf Eis zu legen und sie im Tiefkühler per USB-Adapter auszulesen, indem man das USB-Kabel durch die Dichtung nach außen zum Rechner führt. Zur besseren Wärmeableitung sollte man außerdem das Plastikgehäuse von USB-Sticks und -Kartenlesern entfernen.

Bei Festplatten ist es wichtig, Feuchtigkeitsschäden durch Tauwasser zu vermeiden. Deshalb müssen Festplatten zunächst auf Zimmertemperatur abgekühlt werden, bevor man sie für einige Stunden in den Kühlschrank legt und sie unter den Taupunkt herunterkühlt. Erst dann kommen sie in den Tiefkühler.

**Lesefehler nehmen oft mit steigender Temperatur des Mediums zu. Im Tiefkühler auf Eis gelegt, lassen sich mitunter mehr Daten wiederherstellen, als wenn das Medium heiß läuft.**

Denken Sie daran, dass Sie bei `ntfsclone` als letzten Parameter die auszulesende Partition und nicht wie bei `dd` und `ddrescue` den Laufwerksnamen angeben müssen.

Damit greift das Programm lediglich auf Bereiche der Festplatte zu, die tatsächlich noch mit Nutzdaten belegt sind. Damit werden Sektoren gar nicht erst angesteuert, die zu gelöschten Dateien oder zu sonstigen freien Bereichen der NTFS-Partition gehören – Sie erhalten also die reinen Nutzdaten Ihrer Windows-Partition. Damit ist ein mit `ntfsclone` erzeugtes Image allerdings auch ungeeignet, um verlorengegangene oder versehentlich gelöschte Dateien wiederherzustellen.

## Eingehängt

Ein weiterer Vorteil der Dateisystem-Images von `ntfsclone`: Sie können sie ohne Umwege direkt einhängen. Dazu klicken Sie das Image im Dateimanager mit der rechten Maustaste an und wählen im Kontextmenü unter „Öffnen mit“ die Option „Einhängen von Laufwerksabbildern“. Im Terminal verwenden Sie folgenden Befehl:

```
sudo mount -o loop ntfs.img /mnt
```

Dann können Sie sich auf dem Image umsehen und etwa mit dem grafischen Dateimanager von Desinfec’t Ihre Dateien auf ein anderes Laufwerk kopieren, etwa einen zusätzlich angeschlossenen USB-Stick oder eine externe Festplatte.

Bei Laufwerks-Images, die Sie mit `dd` oder `ddrescue` erstellt haben, führt der Weg über die Kommandozeile. Der Grund dafür ist, dass diese Images nicht mit dem Dateisystem der ersten Partition beginnen, sondern mit dem Bootsektor und der Partitionstabelle des ursprünglichen Mediums. Die Dateisystemanfänge der einzelnen Partitionen sind also nach hinten verschoben. Das Kommandozeilenprogramm `kpartx` liest die Partitionstabelle eines solchen Images ein und erstellt virtuelle Laufwerke, die auf die Anfänge der jeweiligen Dateisysteme zeigen:

```
sudo kpartx -av disk.img
```

Wenn alles gut geht, verrichtet `kpartx` seine Arbeit wortlos. Die virtuellen Laufwerke finden Sie anschließend im Verzeichnis /dev/mapper, `loop0p1` ist die erste Partition, `loop0p2` die zweite und so weiter. Das Einbinden müssen Sie anschließend ebenfalls von Hand erledigen:

```
sudo mount /dev/mapper/loop0p1 /mnt
```

Anschließend können Sie das Verzeichnis /mnt nach zu rettenden Dateien durchstöbern. Wenn Sie fertig sind, dürfen Sie nicht vergessen, das virtuelle Laufwerk mittels

```
sudo umount /mnt
```

wieder auszuhängen und die virtuellen Laufwerke mit dem Befehl

```
sudo kpartx -d disk.img
```

zu entfernen, bevor Sie Desinfec’t herunterfahren oder den Datenträger mit dem Laufwerks-Image herausziehen.

## Aufgestöbert

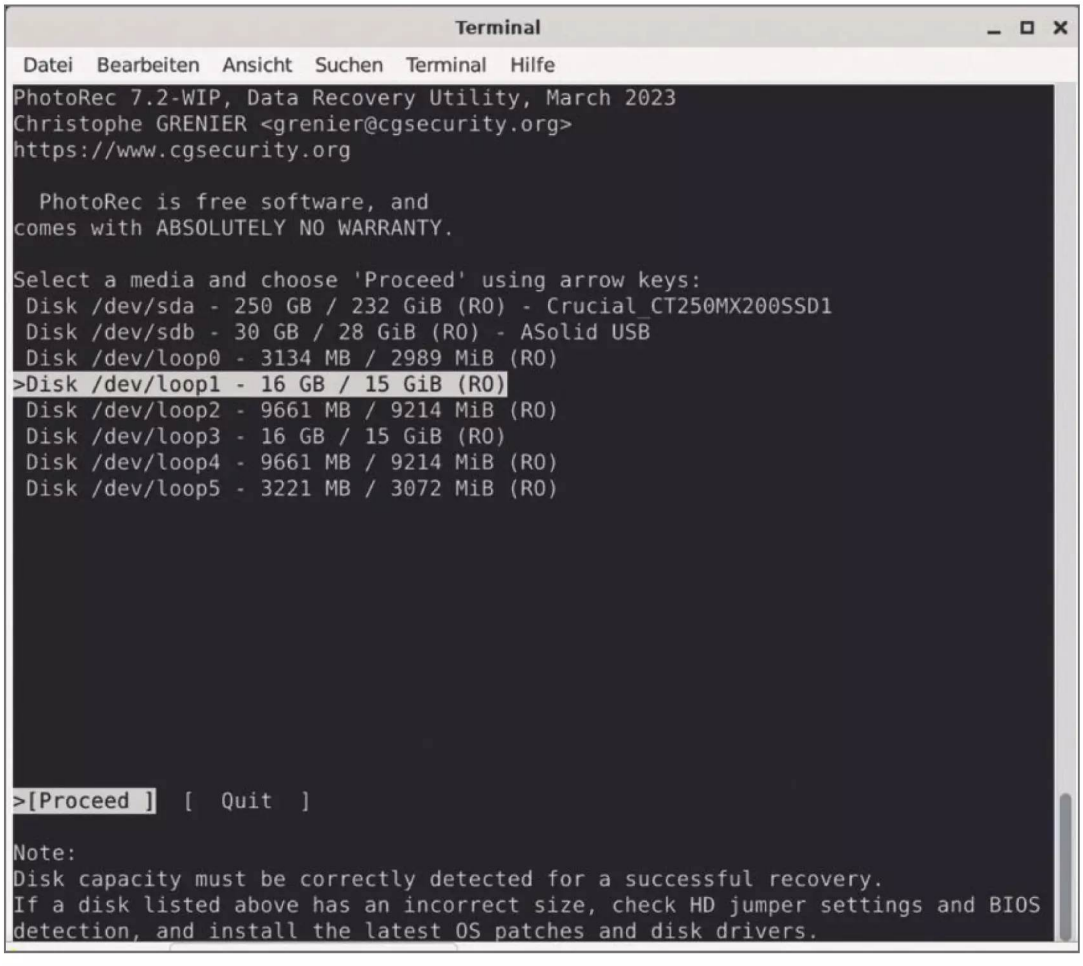
Bei größeren Defekten oder logischen Fehlern, wo etwa ein Absturz des Treibers oder Rechners das Dateisystem beschädigt hat, lassen sich die Dateisysteme nicht mehr einbinden oder es fehlen ganze Verzeichnisse, weil die Verzeichnisstruktur fehlerhaft ist. Selbst wenn Sie das Medium versehentlich (schnell-)formatiert und somit sämtliche Dateiinformationen zerstört haben, gibt es noch Chancen, Daten retten zu können.

Die erste Wahl ist das interaktive Konsolenprogramm `photorec`. Es durchsucht das Image oder Laufwerk nach typischen Dateianfängen verschiedenster Dateiformate. Ursprünglich war es zum Wiederherstellen versehentlich formatierter Speicherkarten von Kameras gedacht, daher der Name. Inzwischen beherrscht Photorec jedoch Dutzende Dateiformate, von Bildern über Office-Dokumente bis hin zu Dateiarchiven.

Soll Photorec den Datenträger direkt auslesen, etwa weil nur ein logischer Fehler vorliegt, aber die Hardware in Ordnung ist, so müssen Sie Photorec beim Aufruf Root-Rechte verschaffen:

```
sudo photorec /dev/sdb1
```

Arbeiten Sie hingegen mit einem Image, genügen die Standardrechte des Desinfec’t-Benutzers. Dann sollten Sie den Dateinamen der Image-Datei aber auch gleich beim Start von Photorec als Parameter angeben, um sich nicht erst umständlich durch den gesamten Verzeichnisbaum von Desinfec’t hangeln zu müssen:




**Ursprünglich entwickelt, um Fotos von versehentlich formatierten Kamera-Speicherkarten zu retten, beherrscht Photorec inzwischen unzählige Dateiformate.**

```
photorec disk.img
```

Leider wurde die Photorec-Version mit grafischer Oberfläche noch nicht für das Framework Qt 6 portiert. Demzufolge finden Sie im Expertentools-Ordner von Desinfec't nur die Version, die auf der Kommandozeile läuft. Doch die Bedienung ist gar nicht schwer.

Nach der Auswahl eines Laufwerks mit wiederherzustellenden Daten können Sie im Grunde direkt über die Auswahl von „Search" loslegen. Damit der Wiederherstellungsvorgang startet, müssen Sie nach der Auswahl von Search noch das Dateisystem des zu durchsuchenden Datenträgers festlegen. Unter „Options" können Sie etwa den Betrieb auf Systemen mit wenig Arbeitsspeicher optimieren. Unter „File Opt" wählen Sie die zu suchenden Dateitypen aus.

Für die Dateiwiederherstellung benötigt Photorec viel Platz, weshalb Sie unbedingt einen zusätzlichen USB-Stick oder eine Festplatte als Datenhalde anschließen müssen. Wichtig ist, dass Sie den Zieldatenträger zunächst im Dateimanager einhängen, bevor Sie ihn in Photorec über die Verzeichnisstruktur als Ziel auswählen.

## Musterknabe

Das ursprünglich von der NSA entwickelte Konsolen-Tool `foremost` ist weniger komfortabel zu bedienen als Photorec. Dafür ist es aber flexibler, wenn es darum geht, eigene Datenfilter zu definieren. So

kann man effektiver Suchen. Ein gutes Beispiel sind dafür Visitenkarten im VCARD-Format, wie sie auch von verschiedenen Smartphone-Apps als Backup-Format verwendet werden.

Foremost unterstützt bereits out of the box nahezu alle Standard-Dateiformate, die auch Photorec beherrscht. Das VCARD-Format jedoch nicht, weshalb Sie zum Wiederherstellen Ihrer Kontaktdaten erst die Filterdatei vcf.conf anlegen und dort das Dateiformat beschreiben müssen. Hier ein Beispiel einer solchen Visitenkarte, die wiederhergestellt werden soll:

```
BEGIN:VCARD
VERSION:2.1
N:;Koch;;;
TEL;CELL:01711111
END:VCARD
```

Am Anfang steht die Analyse, welche Elemente konstant und welche variabel sind. Visitenkarten beginnen stets mit der Zeile `BEGIN:VCARD` und enden mit `END:VCARD`, die eigentlichen Kontaktdaten liegen dazwischen. Damit Foremost nach diesen Zeichenketten sucht und sie als Datei mit der Endung .vcf speichert, tragen Sie folgende Zeile in der Filterdatei vcf.conf ein:

```
vcf y 10000 BEGIN:VCARD END:VCARD
```

Am Anfang steht die Dateiendung, das „y“ dahinter bedeutet, dass Foremost Groß-/Kleinschreibung beachten soll. Dahinter steht die maximale Größe einer Datei, hier 10 000 Bytes – das sollte selbst umfangreiche Kontaktdaten abdecken.

Am Ende der Zeile stehen die Zeichenketten für den Anfang und – optional – für das Ende der Datei. Sofern es sich um Klartext handelt, können Sie diesen direkt eingeben, für Bytefolgen verwenden Sie am besten die hexadezimale Schreibweise, etwa `\x20`. Außerdem kennt Foremost den Platzhalter `?`, der für ein beliebiges einzelnes Zeichen steht, und die Escape-Sequenz `\s` für das Leerzeichen. Die Escape-Sequenz ist notwendig, weil für Foremost alle sogenannten White Spaces Trennzeichen zwischen den einzelnen Parametern sind. Soll eine Zeichenkette also ein Leerzeichen enthalten, so müssen Sie es durch die Escape-Sequenz `\s` ersetzen.

Wählen Sie die maximale Größe mit Bedacht, denn Foremost wird, nachdem es die Anfangs-Zeichenkette gefunden hat, so lange Daten herauskopieren, bis es entweder die End-Zeichenkette gefunden oder das Größenlimit erreicht hat. Bei einem zu hohen Limit entstehen schnell viele große Dateien mit Datenmüll, weil Foremost über den Anfang einer vor langer Zeit gelöschten Datei gestolpert ist. Damit Foremost ausschließlich nach dem gerade beschriebenen Dateiformat sucht, rufen Sie das Programm folgendermaßen auf:

```
foremost -v -c vcf.conf -i disk.img
```

Foremost ist standardmäßig äußerst schweigsam, mit dem Parameter `-v` erfahren Sie mehr darüber, was das Programm gerade tut. Hinter `-c` steht der Name der Filterdatei und hinter `-i` der Name des Laufwerkabbilds.

Bei manchen Dateiformaten gibt es keine Zeichenfolge, die das Ende definiert. Ein Beispiel dafür sind E-Mails, deren Anfang man zwar gut anhand des Mail-Headers erkennen kann, wo es aber kein Ende-Zeichen gibt. In diesen Fällen lassen Sie die End-Zeichenkette weg:

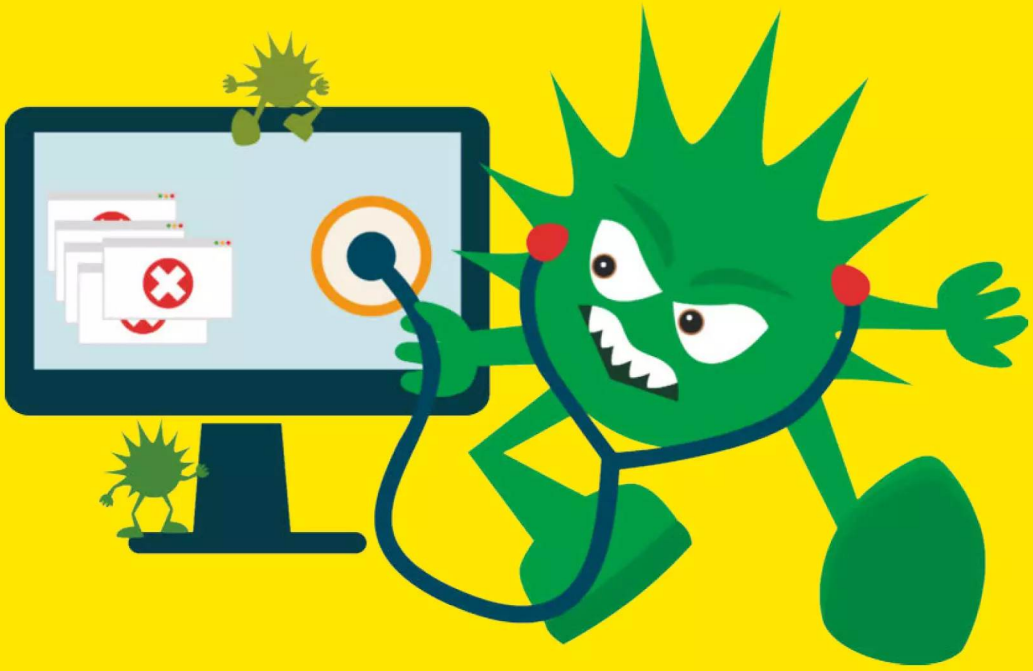
```
eml n 20000000 \x0aMessage-ID:\s
```

Das führt allerdings dazu, dass Foremost für jede gefundene E-Mail 20 MByte Daten sichert. Zwar gibt es keine Zeichenkette, die das Ende einer Nachricht kennzeichnet – doch wenn Foremost über den Beginn der nächsten Nachricht stolpert, darf es aufhören zu kopieren. Dafür definieren Sie die Beginn-Zeichenkette gleichzeitig als End-Zeichenkette und fügen den Parameter `NEXT` an:

```
eml n 20000000 \x0aMessage-ID:\s ↵
↳\x0aMessage-ID:\s NEXT
```

Damit weiß das Konsolen-Tool Foremost, dass die End-Zeichenkette bereits der Beginn der nächsten Datei ist und kopiert sie nicht mit, sondern verarbeitet sie – und das ist entscheidend – ein zweites Mal: Ohne den Parameter `NEXT` würde Foremost die weiteren Daten erst hinter der End-Zeichenkette untersuchen – und somit die unmittelbar folgende E-Mail nicht erkennen, da ja die Beginn-Zeichenkette bereits als End-Zeichenkette der vorherigen E-Mail verarbeitet wurde.

Auf diese Weise können Sie selbst ungewöhnliche oder proprietäre Dateiformate wiederherstellen. Besser als jede Datenrettung ist jedoch die Datensicherung: Mit täglichen Backups, so unkomfortabel sie sind, benötigen Sie die hier beschriebenen Klimmzüge erst gar nicht. (mid) c't



# PCs mit Diagnose-Tools untersuchen

**Von DVD oder Stick ein Live-Linux wie Desinfec't starten und eines von vielen Diagnosetools aufrufen: Schon sprudeln Informationen aus eigenen oder fremden Systemen nur so heraus. So können Sie Hardware eindeutig identifizieren und dafür passende Treiber beschaffen. Auch Reparaturwerkzeuge sind dabei.**

Von **Thorsten Leemhuis**

Muckt Ihr Betriebssystem? Oder wollen Sie einen fremden, unbekannten Rechner untersuchen, der womöglich keines hat? Dann sind von USB-Stick oder DVD startende Linux-Distributionen wie Desinfec't ideal, denn sie haben Hunderte Diagnose-Tools bereits an Bord. Die Testumgebung ist sofort einsatzbereit, nachdem Sie Desinfec't von DVD oder einen damit bespielten USB-Stick booten. Wie das geht, haben wir bereits ausführlich beschrieben (siehe Artikel „Trojaner, Backdoors & Co. aufspüren"). Die erwähnten Diagnose-Tools sind übrigens auch Bestandteil anderer Linux-Distribu-

tionen, daher funktionieren nahezu alle der im Folgenden genannten Kommandos auch mit den Live-Versionen von Ubuntu, Fedora & Co.

Alle der erwähnten Testwerkzeuge müssen Sie in einem Kommandozeilen-Terminal ausführen. Bei Desinfec't starten Sie ein solches über das überwiegend schwarze Icon mit der Eingabeaufforderung, das in der Bedienleiste am unteren Bildschirmrand rechts vom Firefox-Symbol liegt. Falls Ihnen die Schrift im daraufhin erscheinenden Terminal-Fenster zu klein sein sollte, können Sie deren Größe über Bearbeiten/Einstellungen beim Reiter „Aussehen" erhöhen.

## Hardware auflisten

Einen groben Überblick über die im System verbaute Hardware samt Einteilung der erkannten Datenträger liefert das Kommandozeilenprogramm lshw:

```
sudo lshw -short
```

Durch das vorangestellte `sudo` läuft das Programm mit Systemverwalterrechten, die es braucht, um gewisse Informationen abzurufen.

Ignorieren Sie ruhig die numerischen Angaben, die `lshw` in der ersten Spalte zeigt: Sie spezifizieren lediglich eine Position in einer Baumstruktur, die die Hardware-Komponenten abbildet. Die wichtigsten Informationen finden Sie in der dritten und vierten Spalte, denn dort nennt das Programm den Typ einer Komponente samt einer Beschreibung. Ganz oben in der Aufstellung steht der Name des Systems, sofern der Hersteller ihn beim BIOS hinterlegt hat. Es folgen meist die Bezeichnung des Mainboards sowie einige Informationen zu Prozessor und Speichermodulen; anschließend listet das Programm die per PCIe, USB & Co. erreichbaren Chips auf, bevor die erkannten Datenträger samt der Partitionen, die es Volume nennt, an die Reihe kommen. Bei einigen der Komponenten zeigt `lshw` in der zweiten Spalte die Gerätebezeichnung, über die sich die Hardware unter Linux ansprechen lässt.

Deutlich mehr Infos erhalten Sie, wenn Sie die Option `-short` weglassen. Die Detailfülle erschlägt dann aber leicht; der Umbruch langer Zeilen erschwert den Überblick weiter. Übersichtlicher wird es auf diese Weise:

```
sudo lshw | gedit -
```

Die Ausgaben von `lshw` landen dabei in einem neuen Fenster des Texteditors Gedit, der einen besseren Überblick verschafft. Auf Wunsch können Sie die Ausgaben dort auch gleich in eine Datei speichern oder einzelne Angaben über die Zwischenablage abgreifen, um etwa danach mit Firefox im Web zu suchen. Der Trick mit dem angehängten `| gedit -` funktioniert übrigens auch mit allen anderen Kommandozeilenbefehlen, die der Text im Folgenden nennt. Erfahrene Linuxer können die Ausgaben auch via `| less` an einen Textbetrachter übergeben, den man mit der Taste Q beendet.

`lshw` bietet aber noch eine weitere Ansicht, die mehr Überblick bietet: die HTML-Ausgabe. Diese können Sie in eine Datei umleiten und gleich mit Firefox anzeigen lassen:

```
sudo lshw -html >hwliste.htm
firefox hwliste.htm
```

Auf einigen Testsystemen konnte Firefox die Datei allerdings nicht darstellen, weil `lshw` aufgrund von Warnmeldungen unsauberes HTML produzierte. Das Programm hat noch andere Schwächen. Für einen kurzen Überblick ist es gut genug, für einen genaueren Blick sollten Sie aber zu spezialisierten Werkzeugen greifen, die besser gepflegt und enger mit der Linux-Entwicklung verzahnt sind.

## BIOS und Speichermodule

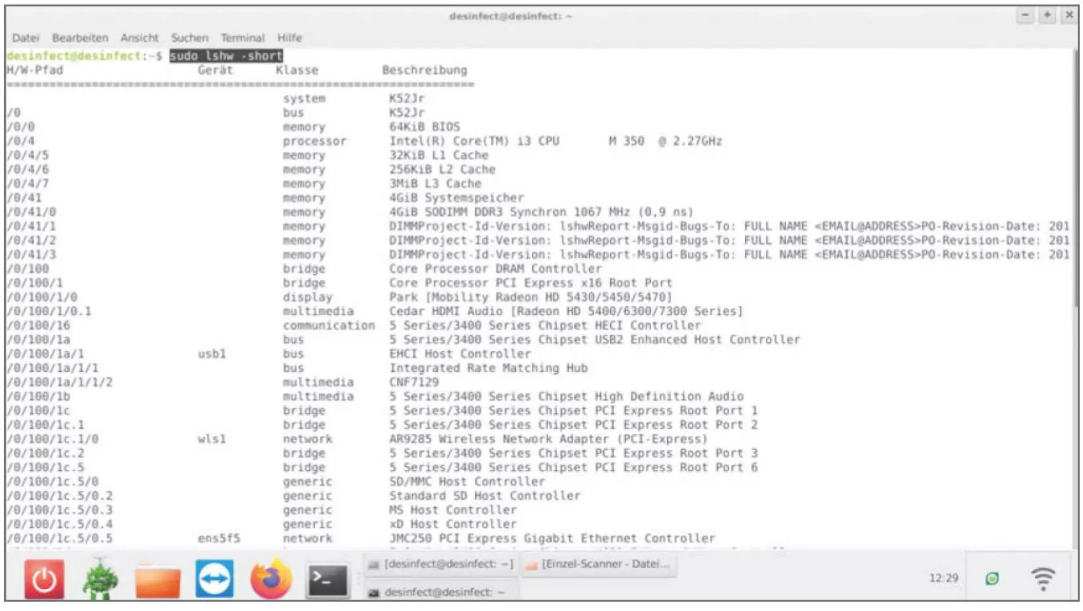
Eines davon ist `dmidecode`, das vom BIOS generierte DMI-Tabellen mit der Selbstbeschreibung des Systems anzeigt. Der Befehl

```
sudo dmidecode
```

gibt im oberen Bereich beispielsweise Mainboard-Name und BIOS-Version aus. Das Programm zeigt dort auch Modellnamen und Seriennummer des Systems an, sofern der Hersteller diese Infos hinterlegt hat; gerade kleinere Unternehmen vergessen das oft. Ignorieren Sie die Angaben daher, wenn diese offensichtlich fehlerhaft sind. Die Details zu den verbauten Speichermodulen sind indes akkurat, denn die bezieht das BIOS direkt aus den DIMMs. Eine Suche nach dem Text „DIMM" führt Sie schnell zu den Bereichen mit diesen Daten. Alternativ können Sie die Ausgabe via

```
sudo dmidecode -t memory
```

auf Informationen rund um den Arbeitsspeicher beschränken, darunter etwa die Speicherkapazität der




**Desinfec't bringt viele Kommandozeilenwerkzeuge mit, die Details zur Hardware-Ausstattung liefern; einen guten Kurzüberblick bietet der Befehl lshw.**

verbauten Speichermodule und freie DIMM-Slots. Vor einer Speicheraufrüstung sollten Sie diese Angabe aber durch einen Blick in das Gehäuse verifizieren, denn es kommt vor, dass Hersteller bei günstigeren Board-Varianten weniger DIMM-Sockel auflöten.

## Prozessor

`dmidecode` liefert auch Infos zum Prozessor. Die bessere Anlaufstelle dafür ist aber das Kommando `lscpu`. Das nennt 64-Bit-Tauglichkeit, Cache-Größen, Turbo-Takt und vieles andere. Detaillierte Angaben wie den Codenamen oder die maximale Leistungsaufnahme fehlen allerdings auch dort. Diese liefert das Web – für Intel-CPUs beispielsweise, wenn Sie auf ark.intel.com nach dem von `lscpu` angezeigten Modellnamen wie „i5-3350P“ suchen.

`lscpu` gibt auch aus, ob der Prozessor Virtualisierungsfunktionen wie AMD-V oder Intels VT-x beherrscht. Das heißt aber nicht, dass diese auch nutzbar sind, denn bei vielen PCs müssen die im BIOS-Setup freigeschaltet sein. Das ist der Fall, wenn ein `ls /dev/kvm` keine Fehlermeldung erzeugt.

Der Linux-Kernel liefert auch einige Hinweise, ob der Prozessor für Sicherheitslücken anfällig ist:

```
head /sys/devices/system/cpu/vulnerabilities/*
```

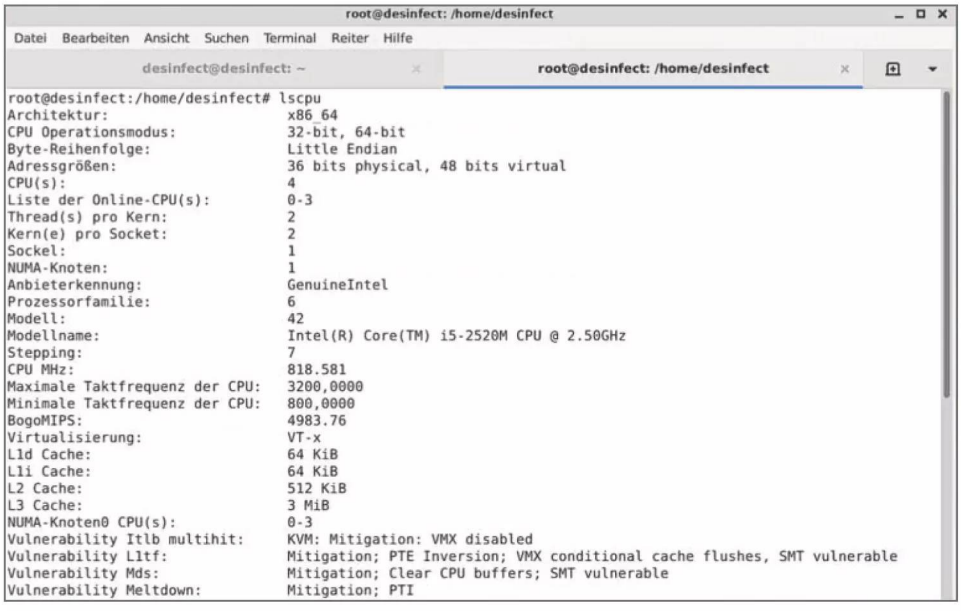
Bei Desinfec't zeigt das den Inhalt von Dateien zu vielen Sicherheitslücken, die seit Anfang 2018 bekannt wurden. Findet sich in den Dateien ein mit „Vulnerable“ oder „Mitigation“ beginnender Text, dann ist Ihr Prozessor für die im Dateinamen genannte Sicherheitslücke anfällig.

Die erwähnten Dateien unterhalb von /sys/ erzeugt der Kernel von Desinfec't dynamisch selbst. Dort finden sich daher nur Angaben zu Schwachstellen, die er kennt. Daher fehlen Infos zu Prozessorlücken, die erst nach Fertigstellung von Desinfec't bekannt wurden.

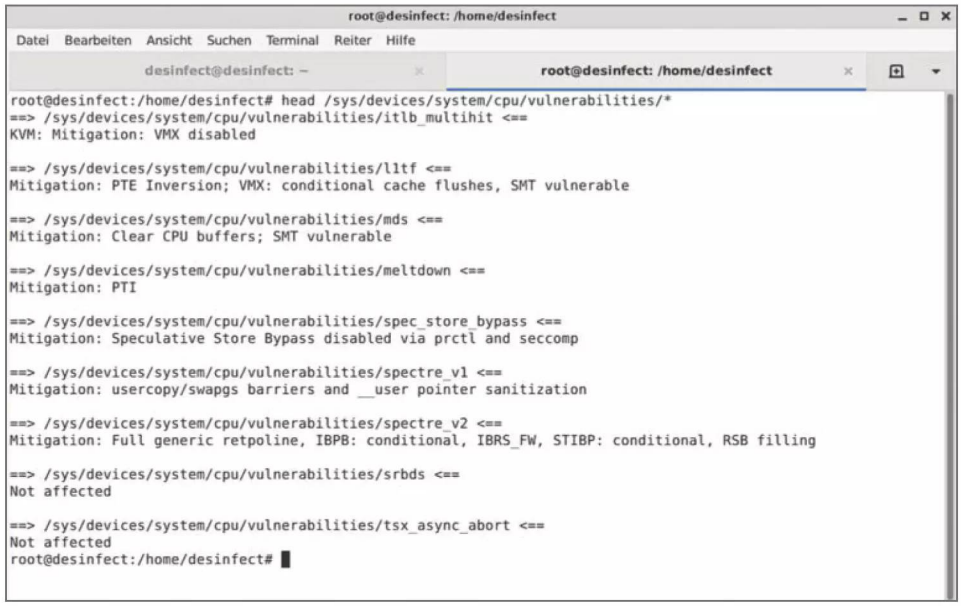
## PCI- und USB-Geräte

Für die meisten Funktionen eines Systems sind PCI- und PCIe-Chips zuständig, die auf dem Mainboard oder Erweiterungskarten sitzen. Diese fragen Sie mittels `lspci` ab. In der meist ein oder zwei Dutzend Einträge langen Liste finden sich oft die Grafik- und Netzwerkprozessoren, die Klassenbezeichnungen wie „VGA compatible controller“ oder „Ethernet controller“ kennzeichnen. Die dahinter stehenden Bezeichnungen erhält das Diagnosewerkzeug nicht von der Hardware, sondern aus einer lokalen Datei, die einige falsche oder irreführende Informationen enthält. Das liegt an Hardware-Herstellern, die dieselben oder eng verwandte Chips

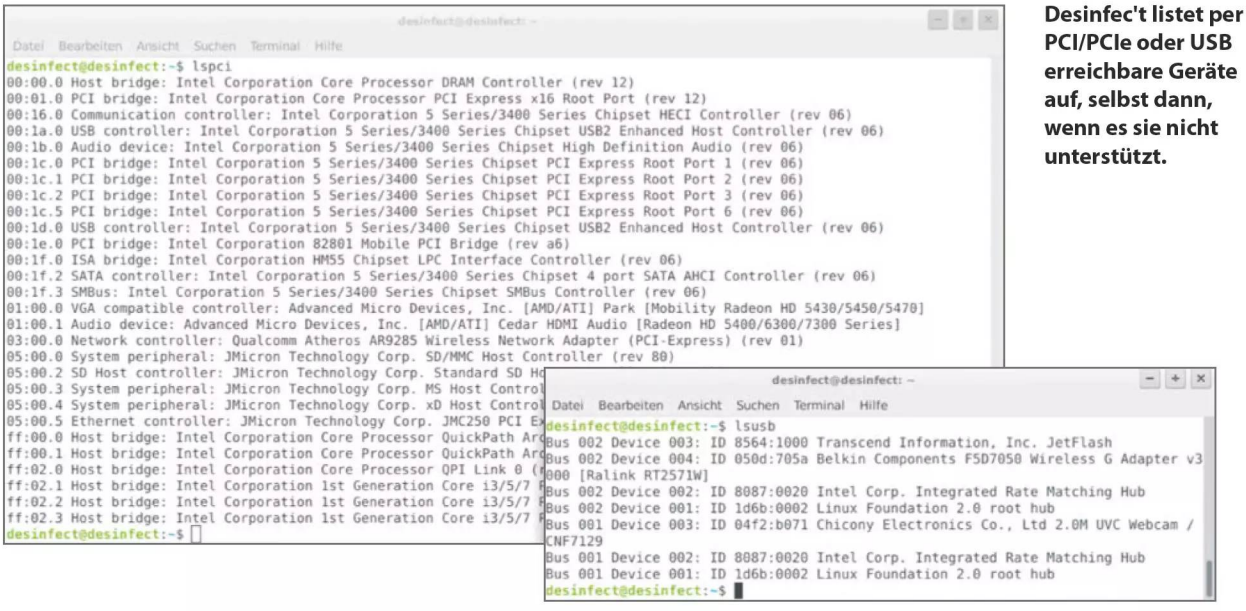
Das Werkzeug lscpu nennt die Zahl der CPU-Kerne sowie Minimal- und Turbo-Taktfrequenz.




manchmal unter ganz unterschiedlichen Bezeichnungen vertreiben – der Grafikkern eines Intel-Core-i-Prozessors wird daher vielleicht als GPU eines Xeon dargestellt. Da auch das eingangs erwähnte `lshw` auf solche Daten zurückgreift, sollten Sie dessen Ausgaben ebenfalls mit Vorsicht begegnen. Oft lassen sich Unklarheiten ausräumen, indem Sie im Internet nach den Hersteller- und Gerätebezeichnern des Bausteins suchen. Diese Device- und Vendor-IDs wirft `lspci` bei Angabe von




Desinfec't klärt, ob Ihr Prozessor für die Sicherheitslücken Meltdown und Spectre anfällig ist.




**Desinfec't listet per PCI/PCIe oder USB erreichbare Geräte auf, selbst dann, wenn es sie nicht unterstützt.**

`-mm` aus; bei einer Radeon HD 6450 lautete die Kombination etwa „1002:6779“.

Eine Liste der USB-Geräte erhalten Sie mittels `lsusb`. Hier liegen die angezeigten Gerätebezeichnungen aus den erwähnten Gründen manchmal auch daneben, sodass Sie die numerischen Bezeichner im Zweifel auch hier zu Hilfe nehmen sollten.

Die Liste der PCI/PCIe- und USB-Geräte beziehen `lscpi` und `lsusb` direkt vom Mainboard und den jeweiligen Hardware-Komponenten. In den Aufstellungen tauchen daher auch Komponenten auf, die der von Desinfec't verwendete Linux-Kernel nicht unterstützt. Ausgeschaltete Hardware kann in den Listen allerdings fehlen. Das kann etwa bei Notebooks passieren, bei denen Bluetooth- und WLAN-Chips per USB angebunden sind: Die tauchen womöglich erst auf, wenn Sie den Flugmodus per Schalter oder Funktionstaste deaktivieren. Letztere arbeiten unter Desinfec't aber in Einzelfällen nicht – das ist einer von mehreren Gründen, warum Desinfec't hin und wieder mal eine Hardware-Komponente nicht sieht.

## Datenträger

Das Werkzeug `lsblk` zeigt die von Linux erkannten Datenträger an; dabei liefert es auch den Mount-Punkt mit, sofern das System die darauf befindlichen Partitionen eingehängt hat. Durch Angeben der Option `--fs` erhalten Sie auch Informationen zum Dateisystem, deren Bezeichnung (Label) und dem normalerweise eindeutigen Bezeichner (UUID/Universally Unique Identifier).

Sie wollen lediglich Datenträger samt Ihrer Modellbezeichnung auflisten? Dann verwenden Sie `lsblk --nodeps -o +MODEL`, damit das Werkzeug alle Volumes ignoriert. Dabei zeigt es in der ersten Spalte die von Linux vergebene Gerätebezeichnung. Der zuerst entdeckte Datenträger bekommt beispielsweise „sda“, der zweite „sdb“. Bei ATA-Datenträgern kann man diese Device-Angaben nutzen, um weitere Informationen abzurufen:

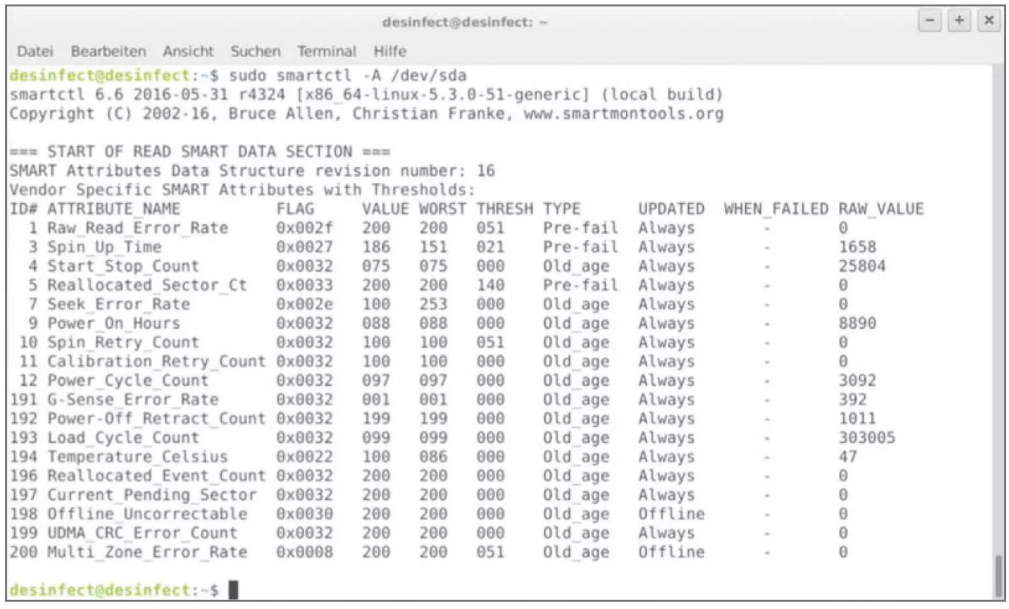
```
sudo hdparm -I /dev/sda
```

Das nennt etwa die Seriennummer, die unterstützten Übertragungsstandards und vieles andere. Die Gerätebezeichnung brauchen Sie auch, um mit der Self-Monitoring, Analysis and Reporting Technology (SMART) von SSDs und Festplatten zu interagieren. Diese liefert unter anderem Informationen zu Nutzungsdauer und Gesundheitszustand des Datenträgers:

```
sudo smartctl -A /dev/sda
```

Die zweite Spalte erwähnt dabei die kryptisch anmutenden Namen der unterstützten SMART-Attribute,

**Die SMART-Daten dieser Festplatte zeigen, dass bislang keine defekten Sektoren gefunden wurden, für die Reservesektoren einspringen mussten.**




die letzte deren aktuellen Wert. Hier finden Sie etwa Angaben zu Fehlern, die Anzahl der Betriebsstunden, die Temperatur oder die Menge der geschriebenen und gelesenen Daten. Der Wert in der Zeile mit der ID 5 (meist „Reallocated Sector Count“) ist einer der wichtigsten: Er zeigt, wie viele schlechte Sektoren bereits gegen Reservesektoren ausgetauscht wurden. Falls das schon vorgekommen ist, sollten Sie den Wert fortan im Auge behalten; steigt er stetig oder gar sprunghaft, sollten Sie zügig ein Vollbackup anlegen und einen Ersatzdatenträger beschaffen.

Einige der Attribute finden sich bei allen Datenträgern, manche sind aber optional oder herstellerspezifisch; darunter leider auch jene, die Informationen zur Abnutzung der SSD liefern.

Ersetzen Sie das `-A` durch ein `--all`, um noch mehr SMART-Informationen abzurufen. Via

```
sudo smartctl -t short /dev/sda
```

## SMART-Attribute bei Festplatten und SSDs (Auswahl)

| Attribut | Bedeutung |
|---|---|
| Raw Read Error Rate | Häufigkeit von Lesefehlern |
| Reallocated Sector Count | Anzahl der bereits genutzten Reservesektoren |
| Seek Error Rate | Anzahl von Positionierungsfehlern der Festplattenköpfe (nur HDD) |
| Program Fail Count | Flash-Programmierfehler (nur SSD) |
| Erase Fail Count | Flash-Löschfehler (nur SSD) |
| Spin Up Time | Zeit für das Hochfahren der Festplatte |
| CRC Error Count | aufgetretene SATA-Schnittstellenfehler |
| Media Wearout Indicator/SSD Life Left | Indikator für Flash-Abnutzung (nur SSD) |
| Power On Hours | Gesamtbetriebszeit des Laufwerks |
| Power Cycle Count | Anzahl der Einschaltvorgänge |
| Host Writes/Total LBAs Written | geschriebene Gesamtdatenmenge in Sektoren |
| Host Reads/Total LBAs Read | gelesene Gesamtdatenmenge in Sektoren |
| Temperature | Betriebstemperatur |

können Sie den Datenträger auffordern, einen kurzen Selbsttest auszuführen, der meist nur einige Minuten dauert und keine Daten gefährdet; der längere Test, für den Sie `short` in `long` ändern müssen, prüft den ganzen Speicherbereich; bei großen Festplatten kann das daher leicht eine Stunde oder länger dauern. Beide Aufrufe starten den Selbsttest im Hintergrund und beenden sich gleich wieder. Dabei nennen sie die geschätzte Testzeit. Währenddessen arbeitet der PC nahezu normal weiter, denn bei Zugriffen unterbricht der Datenträger seinen Selbsttest automatisch für einen kurzen Moment. Das Testergebnis erfahren Sie über folgenden Befehl:

```
sudo smartctl -l selftest /dev/sda
```

Der jeweils neueste Test hat die niedrigste Nummer; falls er noch im Gange ist, zeigt die Spalte „Remaining“ den prozentualen Fortschritt. Bei einem Lesefehler bricht das Laufwerk den Test ab und nennt den beschädigten Sektor im Testergebnis. Dieser wird gegen einen Reservesektor ausgetauscht, sobald der angeschlagene Sektor das nächste Mal überschrieben wird. Details zur Lösung solcher Probleme und weitere SMART-Tricks erläutern [1] und der Artikel „Fotos und Dateien retten“.

## UEFI-Bootdiagnose

Falls Ihr System die installierten Betriebssysteme per UEFI startet, können Sie folgenden Befehl nutzen, um sich die beim BIOS hinterlegte UEFI-Boot-Einträge anzuzeigen:

```
sudo efibootmgr
```

Das klappt aber nur, wenn Sie auch Desinfec’t über UEFI-Mechanismen booten; Sie dürfen es daher nicht mit den Methoden eines klassischen BIOS starten („Legacy Boot“), wie es viele moderne BIOSe per CSM (Compatibility Support Module) ermöglichen.

Sie können `efibootmgr` mit dem Schalter `-v` aufrufen, um neben den Bezeichnungen auch etwas kryptisch wirkende Details zu den Boot-Einträgen auszugeben. Über die darin stehenden Datenträger- und Pfadangaben findet das BIOS beim Systemstart den Boot-Loader, die Betriebssysteme bei der UEFI-Installation auf der ESP (EFI System Partition) ablegen. Diese meist 100 bis 500 MByte große FAT-Partition können Sie mit Linux auch einhängen und durchstöbern. Wenn Sie hier einen EFI-Boot-Loader finden, für den kein UEFI-Boot-Eintrag mehr existiert, können Sie den mit `efibootmgr` anlegen:

```
sudo efibootmgr --create ↵
↳--disk /dev/sda --part 1 ↵
↳--loader '\EFI\ubuntu\shimx64.efi' ↵
↳--label 'Mein Ubuntu'
```

Dieser Befehl funktioniert bei einem System, bei dem die ESP über die Gerätebezeichnung /dev/sda1 erreichbar ist; falls die ESP bei Ihrem System woanders liegt, müssen Sie die Angaben hinter `--disk` und `--part` anpassen. Das gilt auch für den Pfad zum Bootloader, den Sie durch einfache Anführungszeichen schützen müssen, denn sonst gehen die Backslashes verloren.

Ob UEFI Secure Boot aktiv ist, zeigt das folgende Kommando:

```
sudo dmesg | grep -i 'Secure boot'
```

Der Befehl durchsucht das Log des Kernels nach einer Statusausgabe.

Die Kernel-Meldungen enthalten noch eine ganze Menge anderer Details zur Hardware und deren Verwendung durch Linux. Durch `sudo dmesg --human` wird die Ausgabe etwas übersichtlicher, denn dann verwendet das Programm verschiedene Farben und relative Zeitangaben.

## Netzwerkgeräte

Ein `ip link show` liefert Ihnen eine Liste der Netzwerkschnittstellen, die neben Netzwerkchips auch virtuelle Geräte wie das Loopback-Device enthält. Naturgemäß klappt das nur bei Netzwerkhardware, für die Desinfec’t einen Treiber mitbringt. Bei Ethernet-Hardware ist das meist der Fall; bei WLAN-Chips passiert es aber hin und wieder, dass ein Treiber fehlt oder er die Hardware nur rudimentär unterstützt. Über das Werkzeug `ethtool` können Sie die Übertragungsgeschwindigkeit und andere Details zur Netzwerkverbindung abrufen. Die wesentlichen Attribute können Sie aber auch den Verbindungsinformationen entnehmen, die das grafische Netzwerkkonfigurationstool von Desinfec’t anzeigt.

## Thermometer

Der Befehl `gnome-power-statistics` liefert Details zu Notebook-Akkus. Das Kommando `sensors` zeigt die Temperaturdaten an, die vom Kernel automatisch

erkannte Sensoren liefern. Meist enthalten die einen Abschnitt, der „coretemp“ (Intel) oder „k10temp“ (AMD) im Namen enthält: Dort findet sich die Temperatur des Prozessors und oft auch die der einzelnen Kerne. Falls es einen Abschnitt „acpitz“ gibt, stehen hier via ACPI abgefragte Werte der Thermal Zones des Mainboards; meist sitzt einer der darüber abfragbaren Sensoren in der Nähe des Prozessorsockels. PCs mit Radeon-Grafik geben manchmal auch ein mit „radeon“ oder „amdgpu“ betitelten Abschnitt mit der Temperatur des Grafikchips aus. Es gibt aber auch PCs, wo das Programm keinerlei Informationen liefert: Manchmal unterstützt Desinfec’t die Monitoring-Chips gar nicht, manchmal erst nach der eher mühsamen Konfiguration über `sudo sensors-detect`. Die ist bei vielen PCs leider nötig, um Lüfterdrehzahlen abzufragen oder die Spannungsversorgung zu überprüfen.

## Befeuern

Nutzen Sie den Speedtest von OpenSSL, um Lüfterdrehzahlen und Prozessortemperatur versuchsweise nach oben zu treiben, indem sie allen CPU-Kernen etwas zu tun geben:

```
openssl speed -multi $(nproc --all)
```

Desinfec’t bringt kein Programm mit, um die Grafikkarte zu belasten. Für diese Aufgabe können Sie den Furmark von GpuTest nutzen. Laden Sie dessen Linux-Version via ct.de/wjjr herunter, um es dann wie folgt zu starten:

```
cd Downloads
unzip GpuTest_Linux_x64_0.7.0.zip
cd GpuTest_Linux_x64_0.7.0/
./GpuTest /test=fur
```

Achtung: Sie sollten die beiden zuletzt genannten Lasttests nicht als einhundert Prozent stichhaltigen Stabilitätstest betrachten, denn Desinfec’t konfiguriert und nutzt Ihre Hardware womöglich anders als Ihr regulär genutztes Betriebssystem. Stürzen sowohl letzteres als auch Desinfec’t sporadisch ab, heißt das daher keineswegs, dass die Schuld bei der Hardware liegt. Die kann trotzdem beim Betriebssystem oder seinen Treibern liegen. Das gilt insbesondere bei Systemen mit GeForce-Grafikchips, denn Nvidias proprietärer Linux-Grafiktreiber liegt Desinfec’t aus Lizenzgründen nicht bei. Stattdessen kommt ein Treiber zum Einsatz, der ohne nennenswerte Unterstützung von Nvidia entwickelt wird. Er kann daher oft nur einen Bruchteil des Leistungspotenzials von GeForce-GPUs ausschöpfen. Naturgemäß brauchen diese daher bei einem Lasttest weniger Strom, wodurch beispielsweise Probleme bei der Spannungsversorgung nicht zutage treten, aber im dümmsten Fall halt zu anderen Fehlern führen. Das Gleiche gilt auch für Grafikchips, für die Desinfec’t keine 3D-Treiber mitbringt.

Auch Interrupts (IRQs), Stromsparmechanismen und viele andere Hardware-Parameter konfiguriert Desinfec’t womöglich nicht so wie Ihr reguläres Betriebssystem. Das ist ganz normal; Ähnliches kann auch passieren, wenn Sie das altbackene Windows 7 auf einem modernen und mit Windows 10 ausgelieferten System einrichten. Wenn es für Reklamationen um die Klärung von Instabilitäten geht, sind Sie daher mit dem Betriebssystem am besten bedient, für das der Hersteller die Hardware ausgelegt hat. Falls Sie das nutzen, aber die Ursache bei der verwendeten Installation vermuten, sollten Sie das Betriebssystem ein zweites Mal parallel installieren und damit testen.

## Detaillierter

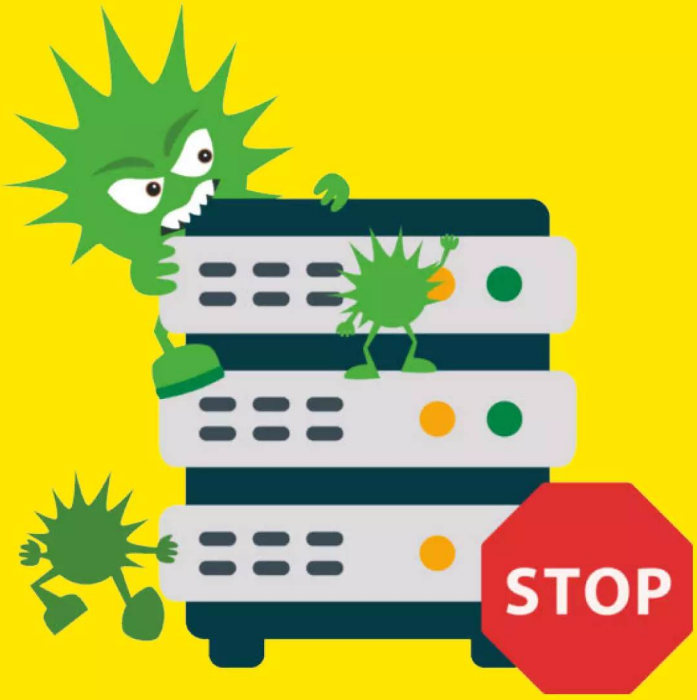
Viele der erwähnten Programme bieten Optionen, mit denen sie mehr Ausgaben liefern oder weitere Aufgaben erledigen. `lspci` gibt bei Angabe des Parameters `-k` etwa umfangreichere Informationen aus, die auch den vom Kernel verwendeten Treiber nennen. Noch viel mehr Details zu PCI/PCIe-Geräten und ihrer Konfiguration spuckt das Programm aus, wenn Sie es via `sudo lspci -v` aufrufen; mit `-vv` oder `-vvv` sind es sogar noch mehr. Auch `lsusb` gibt durch ein `-v` mehr Informationen aus. Der Schalter `-t` bewegt beide Programme dazu, die Hardware in einer Baumstruktur darzustellen. Bei PCs mit USB-2- und USB-3-Controllern können Sie dort sehen, an welchem der beiden ein USB-Gerät hängt.

Das sind einige Möglichkeiten, die die erwähnten Programme bieten. Diese liefern oft selbst eine Übersicht, wenn man sie mit `--help` aufruft. Noch ausführlicher sind die Handbuchseiten, die man mit Befehlen wie `man lspci` aufruft und durch Drücken von Q wieder verlässt. Achtung: Detaillierte Diagnoseaufgaben erfordern manchmal Systemverwalterrechte, worauf die Ausgaben meist hinweisen; starten Sie die Programme dann mit einem vorangestellten `sudo` Desinfec’t bietet noch einen anderen Vorteil: Es ermöglicht eine Problemrecherche im Internet, wenn das installierte Betriebssystem zickt. (des) c't

### Literatur

[1] Boi Feddern, **Gucken kost' nix**, SSD-Diagnose mit SMART, c’t 15/2013, S. 152

**GpuTest herunterladen**
ct.de/wgrz



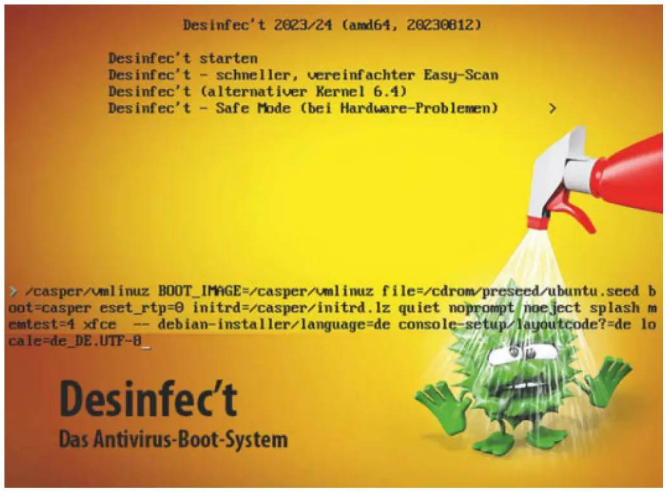

# Daten von NAS-Platten kratzen

**In den meisten Netzwerkspeichern steckt ein mehr oder minder umfrisiertes Linux. Streikt die Hardware, sind die Daten deshalb nicht verloren. Ein Live-System wie unser Desinfec't, das wir dafür ein wenig aufgebrezelt haben, genügt meist, um sie mit überschaubarem Aufwand zu bergen.**

Von **Peter Siering**

Ein NAS stellt im Netzwerk Speicherplatz bereit. Selbst 08/15-NAS-Geräte vom Lebensmitteldiscounter mit Platz für zwei Festplatten bemühen in der Regel die Standardtechniken des Linux-Kernels, um sie zu einer großen zusammenzufassen (RAID0) oder die Daten redundant darauf abzulegen (RAID1). Als Dateisystem kommt oft das gängige ext4 zum Einsatz. Größere Geräte variieren: Sie nutzen andere RAID-Techniken, etwa RAID5 mit mehr als zwei Platten, oder greifen auf Dateisysteme zurück, die selbst auch die Plattenverwaltung übernehmen. So findet sich zunehmend Btrfs auf NAS-Platten. Auf Selbstbau-NAS-Systemen mit FreeNAS ist außerdem ZFS anzutreffen.

Linux, wenn es denn mit passenden Treibern wie unser Desinfec't ausgestattet ist, stellt das Lesen solcher Festplatten vor keine schwierige Aufgabe – schwieriger ist es, überhaupt herauszufinden, was ein NAS nutzt, und dann schließlich die Daten so auszulesen, dass die Platten möglichst unverändert blieben, worauf dieser Artikel besonderen Wert legt. Die folgenden Hinweise taugen begrenzt auch dann, wenn es zu einer Datenhavarie gekommen




**Sicher ist sicher: Das Blacklisten der RAID-Module im Bootmanager verhindert, dass Desinfec't solche Platten voreilig schon konfiguriert. Auf das Hinzufügen der eingekreisten Optionen kommt es an. Die vorgegebenen Parameter variieren je nach Boot-Medium und Methode.**

ist, die NAS-Hardware also noch lebt, es aber nicht schafft, die gespeicherten Daten bereitzustellen. Falls Sie Daten von Platten kratzen müssen, die an einem (Hardware-)RAID-Controller hingen: Das ist ein anderes Kapitel, auf das wir hier nicht weiter eingehen.

## Entdeckungsreisen

Unverzichtbar, um Dateninhalte eines nicht mehr funktionstüchtigen NAS in Sicherheit zu bringen, ist ein PC, den Sie als Rettungssystem verwenden. An den schließen Sie eine hinreichend große leere Festplatte an, um drauf die wiederhergestellten Daten zu sichern. Hilfreich ist es, wenn diese Rettungsplatte deutlich mehr Platz bereithält, dann passt gegebenenfalls auch ein Image für Experimente darauf, sodass Sie die Originalplatten nicht verändern, falls doch ein professioneller Datenretter helfen soll.

Idealerweise handelt es sich um einen vollwertigen PC mit vielen freien SATA-Anschlüssen. So können Sie alle Platten des NAS gleichzeitig an den PC anschließen. Nutzen Sie dafür SATA- oder eSATA-Ports. Eine USB-Dockingstation oder ein USB-Adapter führt eine zusätzliche Ebene ein, die gern mal Ärger macht: Bei unseren Experimenten für diesen Artikel kappten ältere USB-Dockingstationen die Kapazität großer Festplatten. Oft handelt man sich mit USB auch unnötige Performance-Nachteile ein, wenn es um große Datenmengen geht.

Wenn Sie alle Komponenten zusammengestöpselt haben und den PC einschalten, sollten Sie unbedingt Desinfec't daran hindern, automatisch Festplatten aus RAID-Verbunden einzubinden. Das geht, indem Sie im Bootmanager spezielle Startparameter eingeben. Die vom Kernel dafür vorgesehenen Parameter `raid=noautodetect` oder `md_mod.start_ro=1` bewähren sich aus unserer Sicht bei Desinfec't nicht: Der erste greift dort offenbar nicht und der zweite hat den Nachteil, dass nur anfängliche Schreibzugriffe auf einen RAID-Verbund verhindert werden. Nachhaltig funktioniert das zeitweise Deaktivieren sämtlicher RAID-Module.

Die nötigen Handgriffe variieren, je nachdem, wie der PC startet. Auf dem grafischen Bootscreen drücken Sie die Tab-Taste und tippen die Ergänzung direkt am Ende der Startparameter ein. Auf UEFI-Systemen bearbeiten Sie die vorselektierte Boot-Auswahl durch Drücken der Taste E, springen mit dem Cursor in die zweite Zeile und mit End ans Ende der Zeile. Fügen Sie in beiden Fällen mit einem Leerzeichen an: `modprobe.blacklist=raid0, raid1, raid456, raid10`. Starten Sie die Auswahl jetzt mit Return im grafischen Bootscreen oder mit F10 im UEFI-Grub.

Wenn der Desinfec't-Desktop zu sehen ist, öffnen Sie ein Terminal-Fenster und geben als Befehl erst einmal `sudo su` ein. Das hat den Vorteil, dass Sie im Folgenden nicht jedem Befehl ein `sudo` voranstellen müssen. Anders als sonst in c't üblich zeigen in diesem Artikel die grauen Kästen die Ausgaben der empfohlenen Befehle. Mit `lsblk` können Sie sich einen kompakten Überblick über die vorhandenen Datenträger verschaffen:

```
NAME   MAJ:MIN RM   SIZE RO TYPE MOUNTPOINT
loop1    7:1    0   5,5G  0 loop
sdb      8:16   0 232,9G  0 disk
+-sdb2   8:18   0   231G  0 part
\-sdb1   8:17   0     2G  0 part
loop2    7:2    0     7G  0 loop /opt/.../signatures
loop0    7:0    0   1,7G  1 loop /rofs
sdc      8:32   1  14,7G  0 disk /cdrom
\-sdc1   8:33   1   5,5G  0 part
sda      8:0    0 894,3G  0 disk
\-sda1   8:1    0 894,3G  0 part
loop3    7:3    0     2G  0 loop [SWAP]
```

Benutzen Sie die SIZE-Spalte, um sich zu orientieren. Das Gerät „sdc“ ist der Desinfec't-Stick. Die Geräte mit „loop“ im Namen sind Hilfsgeräte, die Desinfec't benötigt. Bei „sda“ handelt es sich um eine zusätzlich angeschlossene Rettungsfestplatte. Aus einem einfachen 2-Bay-NAS von Allnet stammt das Gerät „sdb“. Die Festplatte bildete darin zusammen mit einer weiteren redundanten Verbund (RAID1).

Obwohl Sie die RAID-Module durch die Boot-Option abgeklemmt haben, läuft die automatische Erkennung derselben. Die Ergebnisse können Sie mit `cat /proc/mdstat` anzeigen lassen.

```
Personalities : [linear] [multipath]
md126 : inactive sdb2[1](S)
      242149440 blocks
md127 : inactive sdb1[1](S)
      2047936 blocks
unused devices: <none>
```

Die Platte enthält augenscheinlich zwei RAID-Verbunde, „md126“ und „md127“. Um etwas über deren Beschaffenheit herauszufinden, befragen Sie mit dem Linux-eigenen Kommando für den Umgang mit Software-RAID idealerweise die in einem Verbund sichtbaren Partitionen oder Geräte, hier etwa „sdb2“: `mdadm -Evv /dev/sdb2:`

```
/dev/sdb2:
          Magic : a92b4efc
        Version : 0.90.00
           UUID : a945e406:6ce45545:0284e52d:87b2d038
  Creation Time : Thu Jan 1 01:13:39 1970
     Raid Level : raid1
  Used Dev Size : 242149440
                  (230.93 GiB 247.96 GB)
     Array Size : 242149440
                  (230.93 GiB 247.96 GB)
   Raid Devices : 2
  Total Devices : 2
Preferred Minor : 0
    Update Time : Wed Jul 4 14:54:20 2018
          State : clean
 Active Devices : 2
Working Devices : 2
 Failed Devices : 0
  Spare Devices : 0
       Checksum : b338ed83 - correct
         Events : 23
Number Major Minor RaidDevice State
this 1     8    18     1      active sync/dev/sdb2
0    0     8     2     0      active sync
1    1     8    18     1      active sync/dev/sdb2
```

Die Ausgabe zeigt die Daten einer speziellen Datenstruktur namens Superblock, die RAID-Geräte beschreibt, und bedarf nicht vieler Kommentare: Sie sehen, dass es sich um ein RAID1 handelt, wie viele Platten zum Verbund gehören (2), und, dass /dev/sdb2 als eine von zwei Platten im Verbund vorhanden ist.

Ein ähnlicher Befehl auf das RAID-Gerät selbst angewendet, nämlich `mdadm --detail /dev/md126`, liefert übrigens mitunter irreführende Erkenntnisse – lassen Sie sich davon nicht verwirren. Er weist manchmal solche als „inactive“ geführten Geräte als Mitglied eines RAID0-Verbunds aus. Lassen Sie sich davon nicht täuschen. Erst wenn ein RAID-Gerät als „active“ geführt wird, passt dann die Angabe zu den realen Verhältnissen.

## Zwiebeliges QNAP

Unsere Erwartung bei der Vorbereitung des Artikels war, dass es recht einfach sein sollte, die Daten von den Festplatten Linux-basierter NAS-System herunterzukratzen. Die Produkte der Firma QNAP haben die nicht erfüllt: Die 2018 aktuellen Geräte packen die Platten in ein RAID-Array, legen auf dieses RAID-Array ein DRBD-Volume (Distributed Replicated Block Device, eine Art RAID1 fürs Netz), fügen dieses Volume als physisches Volume dem Logical Volume Management zu, um es dann mithilfe des Device Mappers mit einem optionalen SSD-Cache zu versehen, gegebenenfalls mit LUKS zu verschlüsseln und schließlich als Laufwerk zugänglich zu machen. Das ist alles durchaus plausibel, wenn auch nur schwer zu durchdringen. Manches ist sogar geschickt, etwa der Einsatz von DRBD, um NAS-Inhalte übers Netz direkt auf ein anderes NAS zu replizieren.

Leider hat QNAP aber das Logical Volume Management von Linux modifiziert, sodass man die Volumes nicht mit einer herkömmlichen Linux-Distribution erreicht – ob das der Fall ist, hängt auch davon ab, wie das NAS eingerichtet wurde beziehungsweise sein Speicherplatz provisioniert worden ist (thick oder thin). Obendrein gibt es wohl noch eine Legacy-Konfiguration, die kompatibel zu regulären Linux-Techniken bleibt. Ob Ihre QNAP-Platten von einer regulären Linux-Distribution lesbar sind oder nicht, finden Sie beim Suchen nach physischen Volumes heraus (pvscan). Kann der Befehl einem Volume keine Volume Group zuordnen und gibt er als Fehlermeldung Hinweise zur Provisionierung aus, haben Sie am eigenen Leib erfahren, was ein Vendor-Lock ist. QNAP bestätigte diese Sonderlocken und wollte sie vorerst beibehalten. Andere Hersteller hingegen werben sogar damit, dass man die Platten ihrer Geräte mit regulären Linux-Distributionen auslesen kann.

## Sicherheitsumstand

Ein RAID muss, bevor man es als Dateisystem in den Dateibaum einhängen kann, zunächst aktiviert werden. Das ist nach dem zwangsweisen Auslassen der RAID-Module beim Systemstart etwas umständlich. Zunächst laden Sie die Module mit:

```
echo raid0 raid1 raid456 raid10 | xargs modprobe
```

Anschließend werfen Sie die im Device-Mapper beim Start ermittelten Erkenntnisse zu dem jeweiligen Gerät weg, indem Sie das RAID-Gerät stoppen: `mdadm -S /dev/md126`. Anschließend „starten" Sie es erneut:

```
mdadm --assemble --readonly --run /dev/md126 /dev/sdb2
```

Vorsicht, hier müssen Sie achtsam vorgehen, damit Sie nicht Geräte ins falsche Array stecken. Dadurch würden Sie im unglücklichen Fall Daten verlieren. Oft fängt `mdadm` solche Eseleien aber ab. Bei einem inkonsistenten Verbund kann es nötig sein, den Aufruf zusätzlich mit der Option `-f` zu versehen, um die Inbetriebnahme zu erzwingen. Damit steigern Sie allerdings auch das Risiko, Daten zu verlieren.

Ob der Verbund läuft, können Sie überprüfen, indem Sie erneut den Status mit `cat /proc/mdstat` abfragen:

```
md126 : active (read-only) raid1 sdb2[1]
      242149440 blocks [2/1] [_U]
```

Das Starten hat geklappt („active (read-only)"). Sie können die enthaltenen Daten jetzt eventuell schon als nur lesbares Dateisystem einhängen, etwa mit `mount /dev/md126 /mnt -o ro`. Die Wahrscheinlichkeit ist aber groß, dass der mount-Befehl meckert, weil die wenigsten NAS-Geräte direkt auf dem Verbund Daten speichern.

Klüger ist es deshalb zu untersuchen, was auf dem RAID-Gerät eigentlich liegt. `wipefs /dev/md126` liefert für unsere Testplatte:

```
offset               type
----------------------------------------------------------
0x218                LVM2_member [raid]
                     UUID: V6vY1Q-…-21L4-7QFs-hVRgX3
```

Keine Bange: `wipefs` löscht erst auf explizite Anforderung per Parameter. Ohne zeigt es nur an, was es löschen könnte. Mit `file -s /dev/md126` können Sie eine zweite Meinung einholen, die im konkreten Beispiel der ersten entspricht:

```
/dev/md126: LVM2 PV (Linux Logical Volume Manager),
UUID: V6vY1Q-…-21L4-7QFs-hVRgX3, size: 247961026560
```

Die Erkenntnis ist, dass der NAS-Hersteller den RAID-Verbund mit dem Logical Volume Management weiter aufteilt. Der RAID-Verbund ist ein physisches Volume, das Sie Desinfec't erkennen lassen müssen, `pvscan` erledigt das, sollte es nicht bereits automatisch passiert sein:

```
PV /dev/md126 VG vg0 lvm2 [230,93 GiB / 11,93 GiB free]
Total: 1 [… GiB]/in use: 1 [… GiB] / in no VG: 0 [0 ]
```

Mit `vgs` können Sie sich vergewissern, dass die Automatik beziehungsweise der vorangehende Befehl gleich eine passende Volume Group eingerichtet hat:

```
VG   #PV #LV #SN Attr   VSize   VFree
vg0    1   1   0 wz--n- 230,93g 11,93g
```

Das ist in der Regel der Fall. Wenn nicht, kann man analog zu `pvscan` mit `vgscan` eine Suche starten. Unter Umständen (siehe Kasten „Zwiebeliges QNAP") geben die Befehle Fehlermeldungen aus, denen man dann hinterherrecherchieren kann – eventuell ist das aber auch der Moment, wo man aufgeben und andere Wege suchen sollte, weil man ansonsten anfangen muss, Kernel-Patches zu lesen und anzupassen.

Mit einer aktiven Volume Group müssen Sie im nächsten Schritt ermitteln, welche logischen Volumes das NAS angelegt hat, `lvs` hilft dabei:

```
LV   VG   Attr       LSize   Pool Origin Data%  Meta% …
lv0  vg0  -wi-a---- 219,00g
```

Bei einfachen Geräten sind Sie jetzt fast am Ziel, `wipefs /dev/vg0/lv0` verrät, was auf dem logischen Volume gespeichert ist; `file` meckert über den Gerätenamen, der nur ein symbolischer Link ist, und verweist Sie an die „echte“ Gerätedatei, etwa /dev/dm-4, rufen Sie `wipefs` mit diesem Namen erneut auf:

```
offset               type
-------------------------------------------------------------
0x0                xfs   [filesystem]
                   UUID:  978f3d2a-…-5e0c4248fabd
```

Mit `mount /dev/vg0/lv0 -t xfs -o ro /mnt/` können Sie das offenbar enthaltene XFS-Dateisystem nun unter /mnt einhängen und auch mit dem Desinfec't-Dateimanager ansehen. Je nach NAS werden Sie nicht nur Ihre Dateien dort vorfinden, sondern auch Systemdateien, die das Gerät benötigt. Sie sollten dort also nicht anfangen aufzuräumen, wenn die Chance besteht, die Platten etwa in einem Ersatzgerät wieder in Betrieb zu nehmen.

## Image nutzen

Um Images von NAS-Platten anzufertigen und nicht das Original zu verhunzen, brauchen Sie einen hinreichend großen Rettungsdatenträger. Bezogen auf die bisherigen Beispiele, also der NAS-Platte als „sdb“ und dann als /target eingehängtem Rettungsdatenträger, erstellen Sie 1:1-Kopien auf folgende Weise:

```
dd if=/dev/sdb of=/target/mein.img bs=1M status=progress
```

Wenn die NAS-Platte nicht mehr vollständig lesbar ist, verwenden Sie stattdessen `ddrescue` – je nach Beschädigungsgrad läuft das deutlich länger, weil es beim Lesen defekte Sektoren umschifft. Die Parameter unterscheiden sich vom einfachen dd. Details zu ddrescue und das Retten von Dateien führen wir im Artikel „Fotos und Dateien retten“ aus.

Anschließend fahren Sie Desinfec't herunter, trennen die echte RAID-Platte von Ihrem PC und starten es erneut. Das Ausschließen der RAID-Module im Bootmanager per `modprobe.blacklist` ist bei diesem Start nicht mehr nötig. Die zuvor als Rettungsdatenträger formatierte Platte müssen Sie erneut einhängen (Desinfec't merkt sich so etwas nicht). Prüfen Sie zuvor mit `lsblk`, ob die Gerätenamen durch das Entfernen der einen Platte eventuell versprungen sind, etwa von sda auf sdb.

Nach dem Einhängen der Rettungsplatte (etwa mit `mount /dev/sda1 /target`) müssen Sie jetzt dafür sorgen, dass Desinfec't die Image-Datei mit den Partitionen des RAID-Mitglieds auch als solche behandelt. Dabei hilft ein weiterer Befehl, `kpartx -av /target/mein.img`:

```
add map loop4p1 (253:0): 0 4096000 linear 7:4 2048
add map loop4p2 (253:1): 0 484299087 linear 7:4 4098048
```

Alle Partitionen, die in der Image-Datei enthalten sind, bindet `kpartx` in einem Rutsch über ein Loop-Device und den Device-Mapper als Partitionen ein. Sie sind dann im Gerätebaum unter /dev/mapper als Geräte zu sehen. (Sollten Sie das eingebundene Image in der laufenden Sitzung wieder loswerden wollen, wiederholen Sie den `kpartx`-Aufruf und ersetzen Sie dabei die Option `-a` durch `-d`.)

Die eingangs zur Orientierung empfohlenen Befehle wie `lsblk`, `wipefs` und `file` liefern nun auch Informationen für das eingebundene Image unter dem Namen des loop-Device /dev/loop4 beziehungsweise seiner Partitionen /dev/mapper/loop4p1). Die automatische RAID-Erkennung erfolgt im aktualisierten Desinfec't, sodass die in einem Image enthaltenen RAID-Geräte in /proc/mdstat sichtbar sind. Stoppen Sie diese zunächst mit `mdadm -S /dev/<md>`.

Detailinformationen zu den einzelnen RAID-Mitgliedern erhalten Sie aber über die bereits bekannten Befehle wie `mdadm -Evv /`

### Rettungsplatte vorbereiten

In der ersten Ausgabe von `lsblk` ganz zu Anfang des Artikels taucht eine Festplatte mit der Bezeichnung „sda“ auf. Das ist die Rettungsplatte unseres PC. Der Gerätenamen können bei Ihnen variieren. Eine fabrikfrische Platte, die Desinfec't als „sda“ erkennt, bereiten Sie mit folgenden Schritten für den Einsatz unter Linux vor: Starten Sie im Terminal nach einem `sudo su` mit `cfdisk /dev/sda` die Partitionierung. Legen Sie eine GPT-Partition neu an und lassen Sie die Änderung auf die Festplatte schreiben. Beenden Sie cfdisk. Formatieren Sie die Partition mit dem ext4-Dateisystem: `mkfs.ext4 /dev/sda1`. Anschließend erstellen Sie ein Verzeichnis und hängen Sie das Dateisystem dort ein `mkdir /target; mount /dev/sda1 /target`. Desinfec't kann auch andere Dateisysteme einrichten, etwa FAT32. Das eignet sich aber nur dann, wenn Sie lediglich kleine Dateien auf die Rettungsplatte spielen wollen (kleiner als vier GByte). Für größere ist ext4 die bessere Wahl. Ein als Ersatz beschafftes neues NAS sollte eine ext4-formatierte Platte eigentlich immer lesen können.

dev/mapper/loop4p2 und wipefs /dev/mapper/loop4p2. Mit mdadm --assemble --readonly --run md9 /dev/mapper/loop4p2 können Sie den Verbund starten. Als Verbundnamen nimmt man einen bisher freien – im Zweifel schauen Sie in /proc/mdstat, was dort bisher nicht auftaucht. Anschließend können Sie fortfahren, wie der Artikel es am Beispiel physischer Geräte zuvor gezeigt hat.

## Schutzschirm

In besonders verzwickten Fällen, in denen man Schreibzugriffe auf die Daten braucht, etwa um ein Dateisystem zu reparieren, könnte xmount helfen. Das Programm kann Geräte oder Image-Dateien so einhängen, dass Linux alle daran ausgeführten Änderungen in eine Cache-Datei umleitet. Das heißt, das Original bleibt unverändert, es sind aber trotzdem Änderungen möglich. xmount müssen Sie in Desinfec't nachinstallieren: Entfernen Sie dazu alle Kommentarzeichen (#) am Beginn der Zeile in /etc/apt/sources.list. Lassen Sie anschließend neue Paketlisten holen und xmount installieren:

```
apt-get update; apt-get install xmount
```

Soll das Programm dauerhaft auf Ihren Desinfec't-Stick, kopieren Sie es in das dafür reservierte Verzeichnis:

```
cp /var/cache/apt/archives/*.deb ↵
↳/opt/desinfect/signatures/deb
```

Ein vollständiger Aufruf von xmount sieht so aus:

```
xmount --in raw /dev/sdb --cache ↵
↳/target/sdbcache --out raw/fakedev/
```

Er bindet das physische Gerät /dev/sdb als neues Gerät unter dem Pfad /fakedev/sdb.dd ein. Daten aus schreibenden Zugriffen, die auf dieses virtuelle Gerät erfolgen, landen in der Datei /target/sdbcache und nicht auf /dev/sdb. Gesetzt den Fall, /dev/sdb enthält wie in den bisherigen Beispielen zwei Partitionen, die je in einem RAID1-Verbund stecken (erkannt als md126 und md127) und logische Volumes enthalten, würde man den md126-Teil des Ensembles mit folgender Befehlsfolge beschreibbar mounten:

```
mdadm -S /dev/md126
mdadm -S /dev/md127
mkdir /fakedev
xmount --in raw /dev/sdb --cache ↵
↳/target/sdbcache --out raw/fakedev/
kpartx -av /fakedev/sdb.dd
mdadm --assemble --run /dev/md126 /dev/mapper/loop4p2
pvscan
mount /dev/vg0/lv0 -t xfs /mnt
```

Dabei sind md126 und 127 die automatisch erkannten RAID-Verbunde auf /dev/sdb. Das Verzeichnis fakedev nimmt das von xmount erstellte Gerät auf. Der Aufruf von kpartx hat /dev/map per/loop4p2 als beschreibbare Partition aus dem von xmount erstellten Gerät zugänglich gemacht. Scheitert der letzte Aufruf, kann man mit fsck /dev/vg0/lv0 das Dateisystem reparieren lassen, ohne dass dabei auf der Originalplatte Daten verändert werden. So wäre es

bei einer misslungenen Rettungsaktion immer noch möglich, das Original einem Datenretter zu überantworten.

## Dateisystem-RAID

Auf verschiedenen NAS-Geräten findet man einen bunten Mix von Dateisystemen wieder: Neben XFS und ext3/4 sind wir auf Synology-Geräten auf Btrfs gestoßen. Obwohl das Dateisystem viele Möglichkeiten bietet, auch die Festplatten selbst zu verwalten und Redundanz herzustellen, setzt der Hersteller dafür bisher weiterhin auf das bewährte Linux-Software-RAID. Btrfs ist dann nur das Sahnehäubchen auf dem Storage-Stack. Entsprechend wenig gibt es deshalb zum Einbinden solcher RAID-Verbunde über die so weit erklärten Handgriffe hinaus zu sagen.

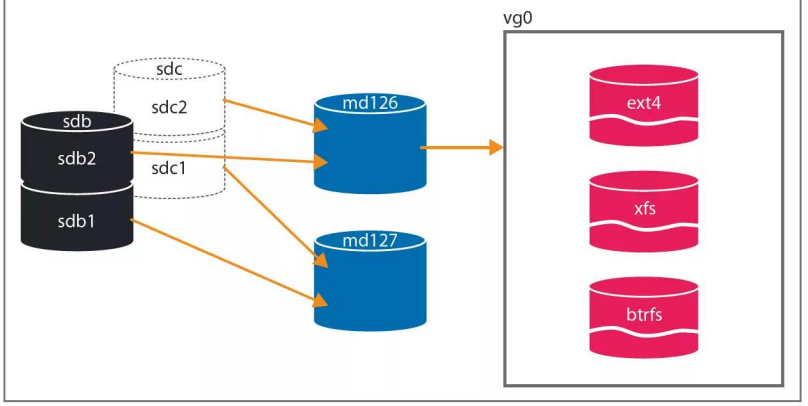
Einfacher ist das Auslesen von NAS-Daten, wenn die Platten direkt mit einem Dateisystem bespielt sind. Das ist etwa bei Platten aus einem Selbstbau-NAS mit FreeNAS als Software der Fall. Die kann Desinfec't von sich aus lesen (dank integriertem ZFS on Linux). ZFS kennt zwar unterschiedliche Feature-Sets, ist aber abwärtskompatibel; eine moderne Version soll immer ältere Versionen lesen können. Anders als einen Linux-eigenen RAID-Verbund erkennt Desinfec't einen ZFS-Pool nicht, aber mit `zpool import` kann man Pools sehen, auf deren Platten Desinfec't zugreifen kann:

```
   pool: pstest
     id: 11197401931174254511
  state: UNAVAIL
status: The pool was last accessed by another system.
action: The pool cannot be imported due to damaged …
   see: http://zfsonlinux.org/msg/ZFS-8000-EY
config:
        pstest           UNAVAIL unsupported feature(s)
          mirror-0                              ONLINE
            usb-Inateck_FE2005_00A1234595FF-0:0  ONLINE
          usb-Inateck_FE2005_00A123459600-0:0  ONLINE
```

Wenn der Pool aus dem blühenden Leben geschieden ist, dann kann man den Import forcieren: `zpool import -f pstest -o readonly=on`. Wenn die Features nicht passen, dann empfiehlt ZFS einen schreibgeschützten Import (readonly) – was beim Wiederherstellen von NAS-Daten generell eine gute Idee ist. Mit der Option `-F` kann man ZFS auch dazu animieren, den Pool zu reparieren. Das sollte man idealerweise nur tun, wenn man ein Backup oder Image hat. Anders als Linux-Software-RAID arbeitet ZFS mit Namen für die Pools und benötigt zum Import, also zur Wiederinbetriebnahme, keine Gerätenamen.

## So strukturieren NAS-Geräte Festplatten

Beim Einrichten eines NAS entstehen aus physischen Platten (/dev/sdb, …) oder Partitionen (/dev/sdb1, …) RAID-Verbunde (/dev/md126, /dev/md127 …). Oft stecken sie einen RAID-Verbund als physisches Volume in eine Volume Group (/dev/vg0, …). Aus dem Speicher einer Volume Group bilden sie logische Volumes. Die kann man in ihrer Größe verändern. Die logischen Volumes versehen sie mit einem Datei-system (ext4, xfs, …), auf denen die Dateien landen. Verschlüsselung oder Caching kann an verschiedenen Stellen zusätzliche Ebenen einführen. Wie viele Partitionen, Verbunde und Volume Groups ein NAS anlegt, hängt von der gewünschten Redundanz und den Herstellervorgaben ab. Dieses Bild gibt die Verhältnisse des im Artikel beispielhaft behandelten Allnet ALL NAS 200 wieder.




## Komplikationen

Die Beispiele haben wir bewusst einfach gehalten. Wenn man die Platten aktueller Geräte untersucht, findet man in einem 2-Bay-NAS durchaus fünf oder mehr Partitionen, die nach einem Desinfec't-Start dann als md123 bis md127 sichtbar sind. Das ist normal, selbst wenn Sie auf dem NAS eine große, redundant ausgelegte Datenplatte eingerichtet haben. Die Hersteller nutzen die zusätzlichen RAID-Verbunde, um dort ihre Software und Konfigurationsdaten abzulegen. Bei einer Standardkonfiguration dürften Sie Ihre Daten auf dem größten RAID-Verbund finden.

Die einzelnen RAIDs sind dabei durchaus anders aufgebaut: So enthalten QNAP-Geräte zwei RAID-Verbunde, die bis zu 32 Platten aufnehmen können, obwohl als Redundanzstufe nur RAID1 gewählt ist. Womöglich macht es sich der Hersteller an dieser Stelle einfacher, die Betriebssoftware auch für Geräte anderer Ausstattungsklassen gleich mit abzuhandeln. Normalerweise sind solche Entdeckungen kein Grund zur Besorgnis.

Viele NAS-Geräte bieten an, die Festplatten zu verschlüsseln. Normalerweise greifen sie dabei ebenfalls auf bewährte Linux-Technik zurück, die auch unter dem Namen LUKS gehandelt wird. Sie erkennen eine Partition, einen RAID-Verbund oder ein logisches Volume daran, dass `file`, `wipefs` & Co. „LUKS“ nebst weiteren Attributen ausgeben. In einem solchen Fall brauchen Sie das Kennwort oder den Schlüssel, um das Gerät zu entsperren und auf Daten zugreifen zu können. Das kann, muss aber nicht das Kennwort sein, das Sie beim Einrichten vergeben haben.

QNAP beispielsweise salzt das in der Weboberfläche eingegebene Kennwort. Über ct.de/wrgv finden Sie eine Hilfe zum Berechnen solcher Kennwörter. Bei anderen NAS-Geräten bleibt nur Probieren und Forschen. Das Prinzip ist simpel: Mit

```
cryptsetup luksOpen /dev/sdb1 decrypted
```

weisen Sie Desinfec’t an, die verschlüsselte Partition /dev/sdb1 entschlüsselt als /dev/mapper/decrypted bereitzustellen. Das Kennwort fragt `cryptsetup` ab. Alternativ kann man das Programm auch mit Schlüsseldateien füttern (`--key-file`).

Generell berücksichtigt dieser Artikel Erfahrungen der letzten Jahre mit Linux-Software-RAIDs [1] und Experimente mit ausgewählten Geräten. Wir können nicht ausschließen, dass in freier Wildbahn andere Techniken in NAS-Geräten zum Einsatz kommen oder dass Hersteller von gängigen Praktiken abweichen. Mit den so weit geschilderten Methoden sollte es möglich sein, solche Fälle bis zu der Grenze zu erkunden, an der es schließlich gefährlich wird. Mithilfe der mit `xmount` aufgezeigten Arbeitsweise kann ein erfahrener Linux-Nutzer diese Grenze sogar hinter sich lassen, ohne Daten zu zerstören.

Der Vollständigkeit halber noch folgender Hinweis: Sollten Sie Platten aus einem sehr, sehr alten NAS geborgen haben, kann es sein, dass dessen Prozessor nicht mit der heute verbreiteten Byte-Folge „Little-Endian“ arbeitet. `mdadm` kennt beim Zusammenbauen eines RAID-Verbunds die Option `--update=byteorder`, um solche Unterschiede auszugleichen. Ob das nötig ist und was passiert, wenn man es versäumt, konnten wir mangels geeigneter Hardware nicht probieren. Vielleicht ist der Hinweis aber für Ihren Fall eine nützliche Fährte.

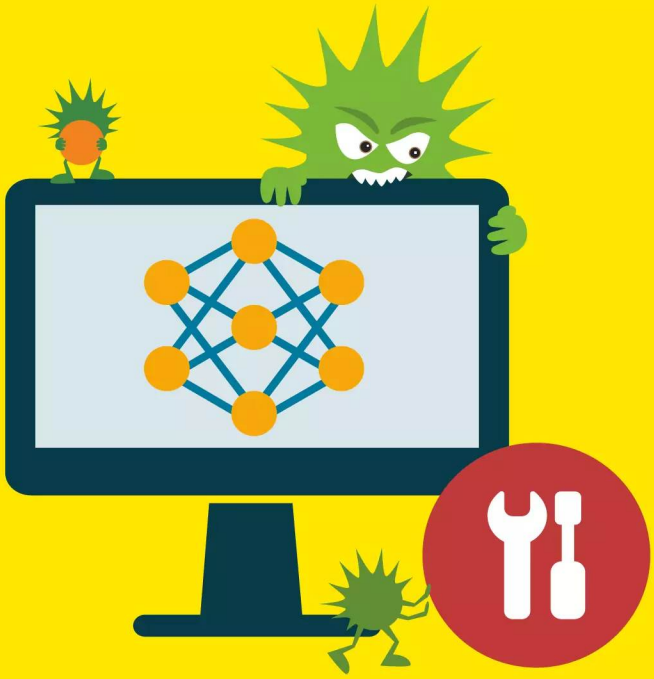
Sollten die geschilderten Schritte bei Ihren NAS-Platten keine Daten fördern, die NAS-Hardware aber reif für die Elektroschrottsammlung sein, hilft ein gebrauchtes Ersatzgerät. In der jeweiligen Gerätefamilie lassen sich die Platten oft einfach umbauen oder nach Inbetriebnahme mit einer fabrikfrischen Festplatte zumindest auslesen. Außerdem gibt es natürlich professionelle Datenretter. Manch einer hat sich sogar auf die NAS-Geräte ausgewählter Hersteller spezialisiert, weil die das mit der Offenheit von Linux nicht so ernst nehmen und eben mehr als nur die Frisur ändern. (ps) **c't**

## Literatur


[1] Peter Siering, **Festplattenpuzzles,** Tipps und Tricks rund um Linux-Software-RAID, c’t 6/2013, S. 184


**Ergänzende Hinweise**

ct.de/wx8z



# Netzwerkprobleme lösen

**Unser Live-Notfallsystem auf Linux-Basis hilft nicht nur bei der Schädlingsjagd, sondern auch dann, wenn das Netzwerk in Unordnung geraten ist. Sei es, dass der Browser streikt, der DNS-Malwarefilter mehr bremst als schützt oder dass die NAS-Freigabe sich nicht zeigt – mit Desinfec't kommen Sie den Ursachen auf die Spur.**

Von **Peter Siering**

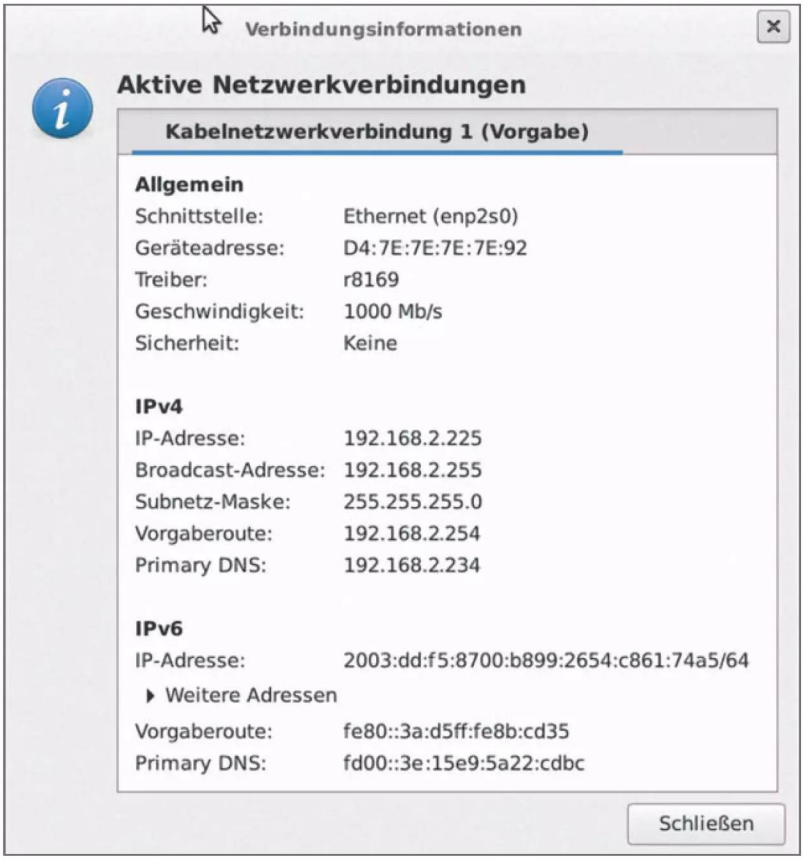
Netzwerkprobleme gibt es reichlich. Die kann man am OSI-Schichtenmodell durchdeklinieren, muss man aber nicht. Mit dem folgenden Know-how und den Werkzeugen in Desinfec't setzen Sie gleich an den neuralgischen Stellen an, um Probleme im Netzwerk aufzuspüren und zu lösen. Wie in vielen anderen Praxisartikeln spielt sich dabei viel auf der Kommandozeile ab. Oft brauchen Sie root-Rechte, das dazu dem Befehl voranzustellende `sudo` führen wir hier nicht ständig auf.

## Surf-Test

Auf den ersten Blick scheint es absurd, ein Live-System für die Diagnose im Netzwerk einzuspannen, doch das ist es nicht: Desinfec't ist dafür ausgerüstet, einen lokalen PC müssten Sie erst mit den Werkzeugen ausstatten. Einige davon gibt es für Windows gar nicht. Ein Live-System fällt keinem virtuellen Verschleiß anheim, der einer schon länger genutzten Betriebssysteminstallation nun mal zusetzt, etwa in Form von unerwünschten Browser-Plug-ins, Schädlingen …

Insofern können Sie Desinfec't auch benutzen, um alltägliche Aufgaben zu erledigen und es in die Fußstapfen seiner nicht mehr weiterentwickelten Geschwister Surfix und Bankix zu setzen: Es eignet sich, um mal eben eine Überweisung im Browser abzuschicken, mal eben zu surfen et cetera – von der DVD gebootet, muss man keine Änderung an Desinfec't selbst befürchten. Anders als seine ixigen Geschwister unternimmt Desinfec't jedoch keine Anstrengungen, Schreibzugriffe auf die Datenträger des PC zu unterbinden, auf dem Sie es starten!

In einem 1-PC-1-Router-Haushalt können Sie sich durch Starten von Desinfec't und dem testweisen Besuchen Ihrer Lieblingswebsites auch vergewissern, ob der Internet-Zugang und -Router einwandfrei arbeiten – dann hat offenbar Ihr PC ein Problem mit dem Netzzugang. Kommt auch Desinfec't nicht an die Websites heran, muss die Suche beim Router ansetzen. Schnell sind Sie dann bei den Klassikern der Netzwerkdiagnose.




**Der Knopf unten rechts in der Task-Leiste des Desinfec't-Desktop führt in die Netzwerkkonfiguration. Dort lassen sich die aktuellen Konfigurationsdaten einsehen und ändern sowie Schnittstellen ein- und ausschalten.**

## ntopng verrät, was im Netzwerk abgeht

Ist es der Sohn, der beim Update der Spiele-Konsole dem Rest der Familie die Bandbreite raubt, oder doch der Gastschüler, der mit Bild nach Hause telefoniert und nebenher Serien schaut? Der faule Familienadmin geht dieser Frage nicht per Pedes nach, sondern mit ntopng. Die Software frisst fortlaufend Netzwerkpakete, um sie zu analysieren und grafisch zusammenzufassen. So sieht man auf einen Blick, wer der größte Paketsauger im Netz ist, findet heraus, dass ein Gerät nicht nur mit den erwartbaren Servern spricht, und lernt dabei allerhand über das eigene Netz.

Desinfec't lässt sich nachträglich mit ntopng versorgen. Es empfiehlt sich, nicht die Version aus Ubuntu 22.04 zu nehmen, sondern gleich auf die Pakete zu setzen, die die ntopng-Macher bereitstellen (siehe auch ct.de/we5w). Die sind aktuell allerdings nur für die 64-Bit-Ausgabe von Desinfec't zu haben. Dazu sind nur wenige Handgriffe nötig: Aktivieren Sie in /etc/apt/sources.list die auskommentierten Zeilen, damit Desinfec't fehlende Pakete gegebenenfalls aus den Ubuntu-Repositories nachinstallieren kann, und rufen Sie dann folgende Befehle auf (stellen Sie ggf. sudo voran):

```
wget http://apt-stable.ntop.org/22.04/all/apt-ntop-stable.deb
dpkg -i apt-ntop-stable.deb
apt-get update
apt-get install ntopng ntopng-data
```

Die fügen das ntopng-Paket-Repository hinzu, aktualisieren die Paketlisten und installieren die für den Einsatz auf Desinfec't hilfreichen Pakete (für stationäre, dauerhafte Installationen von ntopng würde man weitere einrichten). Standardmäßig lauscht ntopng sodann an allen lokalen Schnittstellen. Wenn Sie gezielt nur Ihr WLAN überwachen oder die Daten an Ihrer Fritzbox abzweigen wollen, beenden Sie das Programm mit `killall ntopng` und starten Sie es dann entweder unter Angabe der Netzwerkschnittstelle mit `ntopng -i wls1` oder mit dem im Kasten „Fritzbox als Horchposten für Wireshark & Co." weiter hinten im Artikel vorgeschlagenen Skript.

ntopng analysiert die Pakete im Hintergrund. Um die Auswertung zu sehen und Details betrachten zu können, verbinden Sie sich mit dem Web-Browser mit ntopng. Die URL lautet `localhost:3000`. Beim ersten Anmelden mit Benutzernamen und Passwort admin fordert Sie die Oberfläche auf, das Passwort zu ändern. Anschließend sehen Sie das Dashboard, in dem ntopng eine Zusammenfassung seiner Erkenntnisse zeigt. Nach jedem Start läuft ntopng zehn Minuten lang in der Enterprise-Ausgabe mit allen Funktionen.

Danach wechselt es in den abgespeckten Community-Modus – doch für die eingangs geschilderte Aufgabe eignet sich die ebenso gut: Ausgehend vom Traffic-Dashboard können Sie sich die „Top Hosts" ansehen oder unter „Hosts" den gleichnamigen Menüpunkt wählen. Der Host im Netz mit dem höchsten Traffic-Aufkommen steht standardmäßig oben. Wenn Sie auf die

Desinfec't prüft nach dem Booten, ob es das Internet erreichen kann. Wenn das nicht der Fall ist, erscheint eine entsprechende Warnung. Eventuell kann es nötig sein, dass Sie zunächst die Zugangsdaten für Ihr WLAN eintragen. Fruchtet das nicht, so sehen Sie sich im Detail um. Prüfen Sie, ob Desinfec't eine gültige IP-Adresse erhalten hat. APIPA-Adressen, die mit „169." beginnen, sucht sich ein System selbst. Sie sind ein Hinweis auf Probleme mit der automatischen Vergabe (DHCP). Wenn Desinfec't keine gültige Adresse erhalten hat, wechseln Sie wenn möglich das Medium, also von WLAN zu Kabel oder umgekehrt.

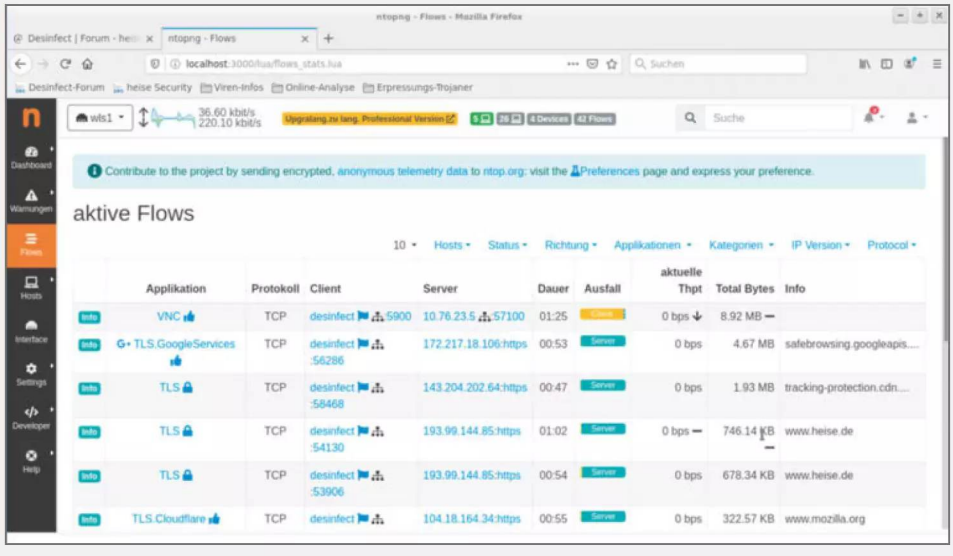
Hält das Problem an, starten Sie den Router neu. Hilft auch das nicht, prüfen Sie mit einem weiteren Gerät, ob vielleicht nur der PC ein Problem hat. Surfen Sie aus dem WLAN die Lieblingswebsites mit einem Smartphone an. Besser wäre ein zweiter PC. Er sollte idealerweise nicht baugleich mit dem ersten sein – Desinfec't bringt zwar viele Treiber mit, aber sicher nicht für jedes Gerät.

### IPv4 und IPv6 richten

Hat Desinfec't eine gültige IP-Adresse erhalten und klappt es trotzdem nicht, per Browser Systeme im Internet zu erreichen, müssen Sie genauer nachsehen: Gelingt es, Namen in IP-Adressen zu verwandeln? Öffnen Sie ein Terminalfenster. Der Aufruf von `ping heise.de` dort sollte fortlaufend ausgeben, dass Antworten von unserem Server eingehen. ping

IP-Adresse klicken, gelangen Sie in eine Detailansicht für den Host, die ein weiteres Aufschlüsseln der Erkenntnisse etwa nach Traffic-Art erlaubt. Spannend ist die Ansicht Peers, sie verrät, mit wem sich der Host wie unterhält.

Die Möglichkeiten, die ntopng bietet, gehen wesentlich weiter. In einer regulären Installation kann man Nutzer einrichten, lokale Netze definieren et cetera. Beim Betrieb aus Desinfec't heraus ergibt das wenig Sinn, weil diese Daten nach einem Reboot weg sind. Für einfache Auswertungen genügt aber schon das Werkzeug, das ohne Detailkonfiguration zugänglich ist. Gegebenenfalls können Sie unter Einstellungen im Expertenmodus die Zeitspannen verlängern, für die ntopng Daten in einer Sitzung aufbewahrt.




**Mit wenigen Klicks in der ntopng-Weboberfläche erhält man Einsicht ins eigene Netzwerk, sei es zu Fehlersuche oder zum Überprüfen von Geräten, die man der Datenschleuderei verdächtigt.**

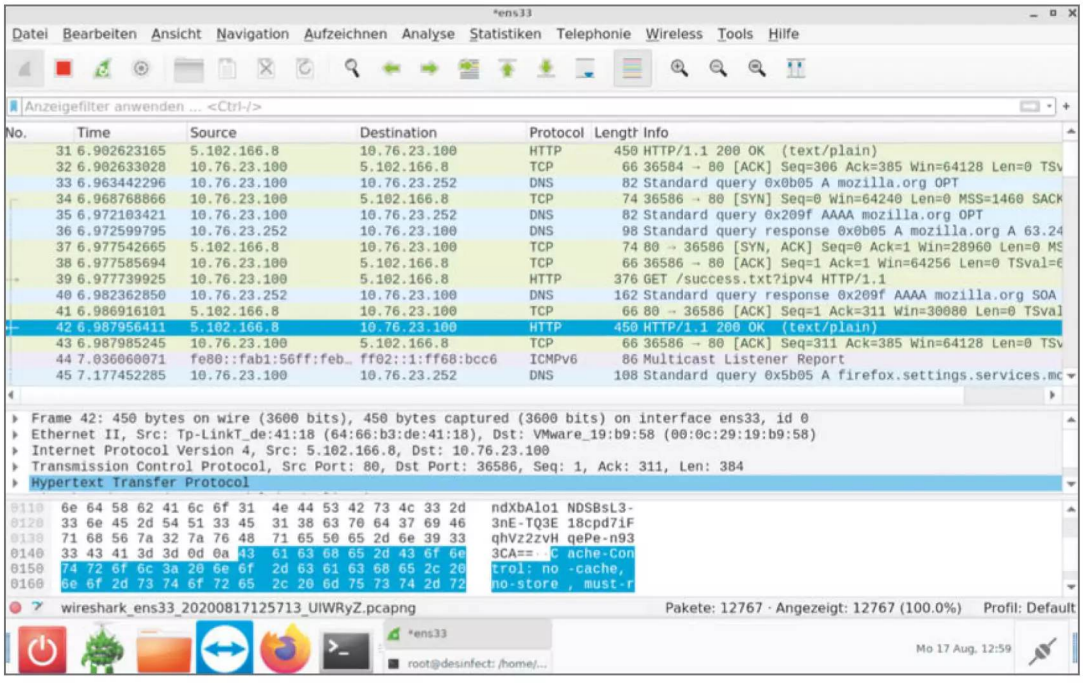
müssen Sie meist mit Betätigen der Tasten `Strg+C` abbrechen.

Kommt als Antwort „Unknown Host“, so klappt die Namensauflösung nicht. Prüfen Sie, welchen „Primary DNS“ Desinfec't für die „Aktive Netzwerkverbindung“ anzeigt. Erhalten Sie eine Antwort, wenn Sie diese IP-Adresse mit `ping 192.168.2.234` ansprechen? (Ersetzen Sie die Adresse durch die Ihres DNS-Servers.) Wenn nach einiger Zeit „Destination Host Unreachable“ erscheint, sind Sie wahrscheinlich auf der richtigen Spur.

Antwortet der DNS-Server nicht, probieren Sie einen öffentlichen DNS-Server wie den von Google aus. Wenn Sie ihn mit `ping 8.8.8.8` ansprechen, sollte eine Antwort kommen. Tragen Sie diesen Server ersatzweise in die Konfiguration von Desinfec't ein. Jetzt sollte auch `ping heise.de` die erwarteten Antworten liefern und Surfen möglich sein.

Wenn Ihre Netzwerkanbindung selbst gestört ist, wird all das nicht fruchten. Versuchen Sie direkt die IP-Adresse unseres Servers oder die des Google-Nameservers anzusprechen: 193.99.144.80 oder 8.8.8.8. Kommt hier keine Antwort der Gegenseite, probieren Sie es mit der von Desinfec't als „Vorgaberoute“ ausgegebenen Adresse. Das ist das Standard-Gateway Ihres Netzes, das alle Pakete weiterleiten soll – mithin der Router. Antwortet der nicht, müssen Sie sich seiner Konfiguration widmen.

Beachten Sie auch, dass viele Router und Provider von sich aus IPv6 aktivieren. Die so weit durchexer-




**Ohne Monitoring-Port am Switch oder eine Fritzbox als Horchposten zeigt Wireshark nahezu ausschließlich den Desinfec't-eigenen Netzwerkverkehr. Um Konfigurationsprobleme im LAN oder WLAN zu erkennen, ist das oft schon genug.**

zierten Beispiele stellen aber nur sicher, dass IPv4-Verkehr reibungslos läuft. Wenn in Ihrem Netz IPv6 aktiv ist, sollten Sie dieselben Schritte mit dem Pendant `ping6` durchlaufen. Es kommt vor, dass Störungen im Netzwerk durch schlecht konfiguriertes IPv6 entstehen, etwa bei einem unzureichend eingerichteten Pi-Hole.

## Gehemmte Freigaben

Die Außenanbindung, die Sie mit den so weit gegebenen Hinweisen überprüfen können, sagt noch wenig über Verhältnisse im lokalen Netz aus. Klappt dort die Namensauflösung nicht, etwa beim Zugriff auf eine Freigabe, so hat das nichts zu tun mit dem DNS-Server des Providers, den Ihr Router befragt.

Die Server- und Freigabenamen von Windows-PCs werden in kleinen Netzen per Broadcast aufgelöst. Falsche Subnetzmasken garantieren Probleme. Was helfen kann: akribisch die IP-Konfigurationen aller beteiligten Rechner daraufhin zu überprüfen, ob gemeinsame Informationen wie die Netzmasken identisch eingerichtet sind, und konsequent die Namen setzen, sodass auch der Router die beteiligten Geräte unter denselben Namen kennt.

Scheitern Zugriffe auf die Freigaben des NAS oder eines anderen Rechners, so kann Desinfec't eine zweite Meinung liefern. SMB-Zugriffe beherrscht es aus seinem Dateimanager heraus. Geben Sie in der Adresszeile den Namen des Servers und der Freigabe mit vorangestelltem SMB:// ein. Wenn das fehlschlägt, Probieren Sie es mit der IP-Adresse statt des Servernamens. Klappt der Zugriff mit Desinfec't, nicht jedoch mit Windows, müssen Sie dort nach den Ursachen fahnden. Eventuell hat sich in Windows ein falsches Passwort festgesetzt. Die zeigt `cmdkey /list` und `cmdkey /delete` tilgt sie gegebenenfalls.

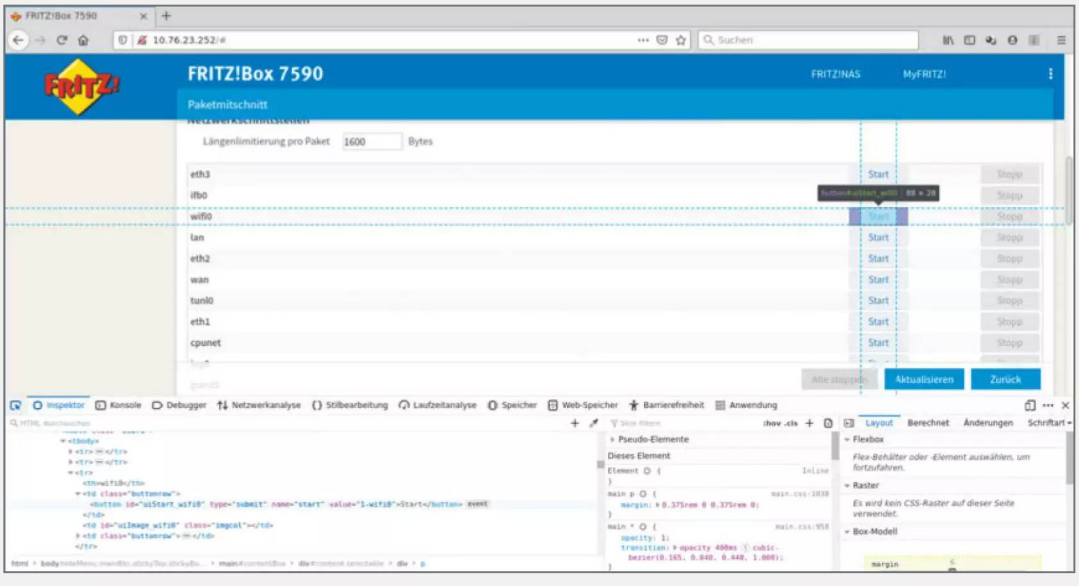
# Fritzbox als Horchposten für Wireshark & Co.

AVM hat seinen Fritzboxen eine Funktion für den Paketmitschnitt spendiert. Die lässt sich leicht ansteuern, wenn man an den Namen oder die IP-Adresse der Box in der Adresszeile des Browser „support.lua“ anhängt, also dort fritz.box/support.lua eingibt. Nach dem Überprüfen des Passworts zeigt die Box eine lange Liste von Optionen an, die vor allem für den Hersteller im Supportfall nützlich sind. Unter „Paketmitschnitte“ gibt eine Fritzbox eine Tabelle von Schnittstellen aus, die sich belauschen lassen. Per Knopfdruck lässt sich ein solcher Mitschnitt starten und beenden. Er landet dann als Datei auf der Festplatte des PC. Die Daten haben das gängige PCAP-Format, das fast jeder Sniffer lesen kann, etwa Wireshark und tcpdump.

Das Shell-Skript fritzdump.sh automatisiert diese Handgriffe, indem es die Ausgaben direkt an ein Programm weiterleitet, das diese anzeigt – man muss also den Zwischenschritt über eine Datei nicht gehen. Das Skript stammt übrigens von den ntopng-Machern (siehe Kasten „ntopng verrät, was im Netzwerk abgeht“ weiter vorne im Artikel). Nach dem Herunterladen des Skripts und dem Setzen des Execute-Bits mit `chmod +x fritzdump.sh` müssen Sie im Skript die Adresse Ihrer Fritzbox und den Namen der Schnittstelle eintragen, an der Sie lauschen wollen. Beim Aufruf erwartet das Skript als Parameter das Zugangspasswort Ihrer Fritzbox.

Am Ende des Skripts steht das Programm, das aufgerufen werden soll. Sie können das Programm (ntopng) zum Beispiel durch wireshark ersetzen. Löschen Sie dazu ntopng am Ende und schreiben Sie wireshark hin. Wenn Sie jetzt das Skript mit `./fritzdump.sh <Passwort>` starten (passendes Passwort vorausgesetzt), sollte sich Wireshark öffnen und bereits den von der Fritzbox gelieferten Paketmitschnitt live anzeigen. Wenn Sie währenddessen ein Browser-Fenster mit der Paketmitschnittseite der Fritzbox offen haben, sehen Sie dort, dass ein Mitschnitt läuft.

Diese Seite hilft auch dabei, den richtigen Namen der Netzwerkschnittstelle für Ihr Analysevorhaben zu finden. Aktivieren Sie einfach bei geöffneter Mitschnittseite die Entwicklerwerkzeuge im Browser, klicken Sie auf das Fadenkreuz und dann auf den Button der jeweiligen Netzwerkschnittstelle. Der Inspektor der Entwicklerkonsole zeigt dann in der hervorgehobenen Zeile den Namen der Schnittstelle als Wert in value="". Experimentieren Sie gegebenenfalls, bis Sie die richtige Schnittstelle erwischt haben.




**Fritzboxen bieten auf den Supportseiten ihrer Weboberfläche Funktionen, um Paketmitschnitte anzufertigen. Die lassen sich nicht nur speichern, sondern direkt weiterverarbeiten. Beim Herauspicken der Namen der richtigen Schnittstelle helfen die Entwicklerfunktionen des Browsers.**

## Paketverlust

Unangenehme Fehler sind solche, die nur sporadisch auftreten. Ganz besonders lästig sind die beim Streamen, weil hier große Puffer im Spiel sind, die sogar eine Trennung der DSL-Verbindung überleben können, ohne dass Sie davon überhaupt Notiz nehmen. Schließen Sie in solchen Fällen zunächst technische Fehler aus.

Sehen Sie sich dazu in Desinfec't im Terminal mit `ifconfig` die Statistiken für die Netzwerkschnittstellen an. Die Zähler für Übertragungsfehler (Fehler, Verloren, Überläufe) sollten bei 0 stehen. Laufen die in kurzen Zeitabständen hoch, müssen Sie die Ursache dafür finden.

Das gleiche gilt dann, wenn die Schnittstelle häufig zwischen Betriebsmodi wechselt, etwa zwischen Halb- und Vollduplex- oder 10- und 100 Bit/s-Betrieb umschaltet. Die letzten Zeilen solcher Kernel-Meldungen bekommen Sie mit `dmesg | tail` zu sehen.

Bei drahtgebundenen Netzwerken ist ein vom Hamster angefressenes oder vom Bürostuhl plattgewalztes Patch-Kabel dann oft die Ursache. Tauschen Sie es aus. Wechseln Sie Netzwerkdosen und Switchports nacheinander durch, bis Sie die matschige Komponente isoliert haben. Markieren Sie offenbar defekte Dosen oder Ports und führen Sie kaputte Kabel sofort dem Recycling zu.

Auch Funknetzwerke sind von Haustieren bedroht, jedenfalls wärmte im Winter die Katze eines Kollegen ihren Pelz auf dem Router und schaltete dabei das WLAN ab. Normalerweise aber sind andere WLANs der größere Feind: Wenn mehrere WLANs denselben Frequenzbereich nutzen, bleibt für jedes einzelne entsprechend weniger Bandbreite über. Die Automatiken der Router zum Finden eines wenig frequentierten oder besser noch freien Kanals funktionieren meist gut. In Problemfällen ergibt es Sinn, den Router fest auf einen Kanal zu konfigurieren. Packen Sie Ihr WLAN dorthin, wo der Nachbar funkt, der selten daheim ist.

Einen Überblick, welches Netz auf welchem Kanal mit welcher Stärke aktiv ist, verschaffen Sie sich unter Desinfec't zum Beispiel mit LinSSID. Das Programm müssen Sie nachinstallieren: Entfernen Sie die Kommentarzeichen (#) am Anfang der Zeilen in /etc/apt/sources.list und lassen Sie die Paketlisten aktualisieren: `apt-get update`. Jetzt können Sie mit `apt-get install linssid` das Paket für die WLAN-Anzeige-Software einrichten und mit `linssid` aufrufen.

## Profi-Werkzeuge

Desinfec't hat viele Werkzeuge an Bord, die auch passionierte Netzwerkbetreuer schätzen. Mit `curl` kann man Web-Dienste und -Seiten ansteuern, um die Erreichbarkeit zu prüfen, Status-Codes abzufragen oder auch nur um Dateien herunterzuladen. `curl` beherrscht alle wesentlichen Zugriffstechniken (POST, GET), kann mit Zertifikaten umgehen und liefert detaillierte Rückmeldungen. Ein paar Beispiele:

`curl -I heise.de` gibt normalerweise nicht sichtbare Informationen aus dem Header bei HTTP-Zugriffen aus. `curl -O example.com/test.zip` würde die Datei test.zip von example.com herunterladen (example.com ist nur ein Beispiel). `curl -X POST https://example.com/example.cgi?example=test` würde per Post-Request Daten an ein CGI-Skript auf dem Server senden.

Weniger spezialisiert, dafür aber universeller ist netcat (`nc`). Es kann sowohl als Client als auch als Server fungieren, verbindet nahezu beliebige Ports per TCP oder UDP und kann sogar Unix-Domain-Sockets verwenden. Will man etwa die Erreichbarkeit eines Mail-Servers prüfen, so kann man mit `nc <servername> 25` seinen TCP-Port 25 ansprechen.

Mit der zusätzlichen Option `-l` können Sie netcat anweisen, auf dem lokalen PC den TCP-Port 25 zu öffnen, sodass er Verbindungen von außen entgegennimmt. Wenn Sie dann mit netcat auf einem entfernten Host darauf zugreifen, wissen Sie, dass das untersuchte Netzwerk für Zugriffe über Port 25 in dieser Richtung durchlässig ist.

Der Netzwerkschnüffler Wireshark ist ebenfalls an Bord. Üblicherweise zeigt der nur den eigenen Verkehr und an alle Knoten im Netz adressierten Pakete an. Für die Fehlersuche auf dem eigenen System ist das ausreichend. Wer mehr sehen möchte, braucht in einem drahtgebundenen Netz einen Switch-Port, der allen Netzwerkverkehr oder den anderer Ports auf den Desinfec't-PC spiegelt. In einem – wie heute üblich verschlüsselten – Funknetz sind zusätzliche Verrenkungen nötig.

Wer eine Fritzbox als Router verwendet, kann hingegen bequem schnüffeln: Die Web-Oberfläche von AVMs Routern bietet Funktionen für Paketmitschnitte an. Die kann Desinfec't einsammeln und als Eingaben an Wireshark weitergeben. Das geht ebenso im Zusammenspiel mit anderen Netzwerkwerkzeugen, mehr dazu im Kasten „ntopng verrät, was im Netzwerk abgeht“. Schnüffeln muss nicht unbedingt heißen, die Unterhaltung von Geräten zu debuggen, sondern kann auch helfen, statistische Daten aufzubereiten, um unkooperative Mitbenutzer zu finden. (ps) **c't**

**Skripte, Software**
**ct.de/we5w**

# Vorschau: c't Security-Einstieg

**Ab dem 25. Oktober im Handel und auf shop.heise.de**

**Mehr Sicherheit mit wenigen Handgriffen**

Im neuen Sonderheft zeigt die c't-Redaktion anhand von Security-Checklisten für verschiedenste Bereiche, wie Sie Punkt für Punkt die Sicherheit Ihrer Geräte und Accounts verbessern. Speziell für Ihren Windows-Rechner zeigt das Sonderheft ausführlich, wie Sie mit Bordmitteln und mit zusätzlicher Open-Source-Software dem System eine Extraportion Sicherheit verpassen. Außerdem erklärt die c't-Redaktion, wie und warum Sie auf die Passwortalternative Passkeys umsatteln sollten, um Phishern und Hackern einen Strich durch die Rechnung zu machen. Zudem liefert das Sonderheft Hintergrundwissen zu den Tricks und dem Vorgehen von typischen Angreifern, damit Sie stets gewappnet sind.

**Weitere Infos: ct.de/wwzk**

## Themenschwerpunkte

- 14 Security Checklisten für alle Fälle
- Passkeys gegen Phishing und Leaks
- Passkeys unter Linux nutzen
- TOTP-Generator und -Tresor selbst hosten
- Extra-Sicherheit für Windows
- Windows App-Installationsquellen einschränken
- Cybercrime verstehen und bekämpfen
- Online-Betrugsschutz
- Industrialisierung des Cybercrime
- Scammer bekämpfen
- Angriffe auf Bankkunden

# Desinfec’t 2024/25 vom Server booten

**Nie mehr nach Desinfec’t-USB-Sticks suchen, stattdessen den Virenjäger bequem aus dem Netzwerk starten? Ein Bootserver mit dem Sicherheitstool fürs Heim- oder Büronetz machts möglich. Das funktioniert sogar mit einem Raspberry Pi.**

Von **Mattias Schlenker**

Nicht nur für Admins in Unternehmen, auch im Privathaushalt ist ein eigener Bootserver mit Desinfec’t praktisch: Damit überprüfen Sie etwa Notebooks von Schulkindern bequem auf Viren, ohne nach einem Desinfec’t-Stick kramen zu müssen. Zu scannende Clients müssen lediglich über eine aktive Netzwerkverbindung verfügen und schon können sie das Sicherheitstool direkt über das Netzwerk starten.

Für das Einrichten benötigt man nur einen als Bootserver konfigurierten und dauerhaft eingeschalteten Computer, von dem Clients im Netzwerk, die man scannen will, die 64-Bit-Version von Desinfec’t beziehen. Realisieren lässt sich das Ganze über Preboot Execution Environment (PXE).

Unter PXE versteht man ein Bündel von Verfahren, mit denen ein PC Startdateien statt von einer lokalen Festplatte aus dem Netzwerk lädt. So kann ein Server beispielsweise eine vollständige Betriebssystemumgebung bereitstellen, an der sich ein Client bedient. Heutzutage beherrschen im Grunde alle Onboard-Ethernet-Karten PXE.

## Drei Netzwerkserver

Damit Desinfec’t aus dem Netzwerk startet, benötigt man drei Serverdienste: einen DHCP-Server zur Konfiguration von unter anderem IP-Adressen, einen TFTP-Server zum Übertragen der Bootdateien und einen NFS-Server zum Bereitstellen der

Systemdateien. Die Dateien für die Einrichtung finden Sie im Archiv, welches Sie über den Download-Link am Ende des Artikels herunterladen können. Doch Vorsicht: Das Einrichten eines DHCP-Servers in einem bestehenden Netzwerk ist nur etwas für Leute, die wissen, was sie tun. Alle drei Server können auf einem Linux-Computer im lokalen Netz laufen. Man kann sie aber auch auf mehrere Geräte verteilen.

In diesem Artikel konzentrieren wir uns auf das Setup mit Debian-basierten Systemen, wie Raspberry Pi OS und Ubuntu. Kommt als Bootserver ein Raspberry Pi zum Einsatz, müssen Sie ein paar Dinge beachten: Im Grunde reicht sogar ein Raspi 1 aus, um Desinfec't im Netzwerk an Clients zu verteilen. Mit dieser Version des Einplatinencomputers gestaltet sich das Starten des Bootservers jedoch als sehr langwierig und Desinfec't wird nur zäh an Clients ausgeliefert. Damit beides schneller vonstatten geht, sollte ein Raspi 3 in Kombination mit einer flinken SD-Karte zum Einsatz kommen. Falls Sie einen OpenWrt-Router zum Bootserver machen wollen, müssen Sie die DHCP- und TFTP-Konfigurationseinstellungen für den dort verwendeten Serverdienst dnsmasq konvertieren (siehe ct.de/wp9u).

Für ein besseres Verständnis empfehlen wir aber, zunächst unsere Musterkonfiguration auf Computern mit Ubuntu, Debian oder Raspberry Pi OS nachzustellen und erst dann die Server auf beispielsweise NAS und Router zu verteilen. Unter ct.de/wp9u finden Sie einen Link, wie man zum Beispiel auf einem mit OpenWrt laufenden DSL-Router und einem 4-GByte-Speicherstick eine PXE-Bootumgebung aufsetzt, die Desinfec't serviert.

Am Anfang steht die Einrichtung des DHCP-Servers. Die folgende Konfiguration ist für das in Debian enthaltene isc-dhcp-server-Paket geschrieben. Zunächst müssen Sie in der Datei /etc/default/isc-dhcp-server die Netzwerkinterfaces eintragen, an denen der Server lauschen soll. Das sieht beispielsweise wie folgt aus:

```
INTERFACES="enp2s0"
```

Danach bearbeiten Sie die Konfigurationsdatei /etc/dhcp/dhcpd.conf::

```
ddns-update-style none;
option domain-name "meinnetz.test";
option domain-name-servers ↵
                        ↳10.76.23.252;
option routers 10.76.23.252;
default-lease-time 600;
max-lease-time 7200;
authoritative;
subnet 10.76.23.0 ↵
↳netmask 255.255.255.0 {
  range 10.76.23.80 10.76.23.220;
  use-host-decl-names on;
  option subnet-mask 255.255.255.0;
  option broadcast-address ↵
  ↳10.76.23.255;
  next-server 10.76.23.250;
}
class "pxeclient" {
  match if substring (option ↵
  ↳vendor-class-identifier, 0, 9) = ↵
  ↳"PXEClient";
  if substring (option ↵
  ↳vendor-class-identifier, 15, 5) = ↵
  ↳"00000" {
    # BIOS client
    filename "pxelinux.0";
  }
  else {
    # default to EFI 64 bit
    filename "bootx64.efi";
  }
}
```

Damit setzen Sie einen DHCP-Server auf, der das Netz 10.76.23.0/24 bedient; der Bootserver hat die Adresse 10.76.23.250. Gateway und Nameserver sind mit 10.76.23.252 ansprechbar. Der Parameter 0 sorgt dafür, dass dieser DHCP-Server maßgeblich für dieses Netzwerk ist.

Starten Sie jetzt den DHCP-Server neu:

```
service isc-dhcp-server restart
```

Nun kann man prüfen, ob der DHCP-Server via PXE-Boot sichtbar ist. Stellen Sie dafür beim PC, auf dem Desinfec't aus dem Netzwerk starten soll, die Bootreihenfolge auf „Network Boot“. Das gelingt temporär über das BIOS-Bootmenü oder dauerhaft im BIOS – oft heißt der Punkt mit dieser Option „Startup“. Läuft der DHCP-Server korrekt, sollten nun auf dem Client beim Booten die MAC-Adresse, die UUID des BIOS und die vom DHCP-Server erhaltenen Parameter zu sehen sein. Der Computer versucht nun per TFTP die Datei pxelinux.0 vom Server 10.76.23.250 zu laden. Da aber noch kein TFTP-Server läuft, bricht der Bootvorgang nach einigen Minuten ab.

## TFTP für den Bootloader

Für den TFTP-Server kommt der „Anvins TFTP-Server“ aus dem zu installierenden Paket tftpd-hpa zum Einsatz. Geben Sie dafür `apt install tftpd-hpa` ein. Die Konfiguration gelingt über die Datei /etc/default/tftpd-hpa. Passen Sie die IP-Adressen an die in Ihrem Netz verwendeten an und ändern Sie gegebenenfalls den Pfad des Ordners mit den Bootdateien:

```
TFTP_USERNAME="tftp"
TFTP_DIRECTORY="/opt/tftpboot"
TFTP_ADDRESS=":69"
TFTP_OPTIONS="--secure"
```

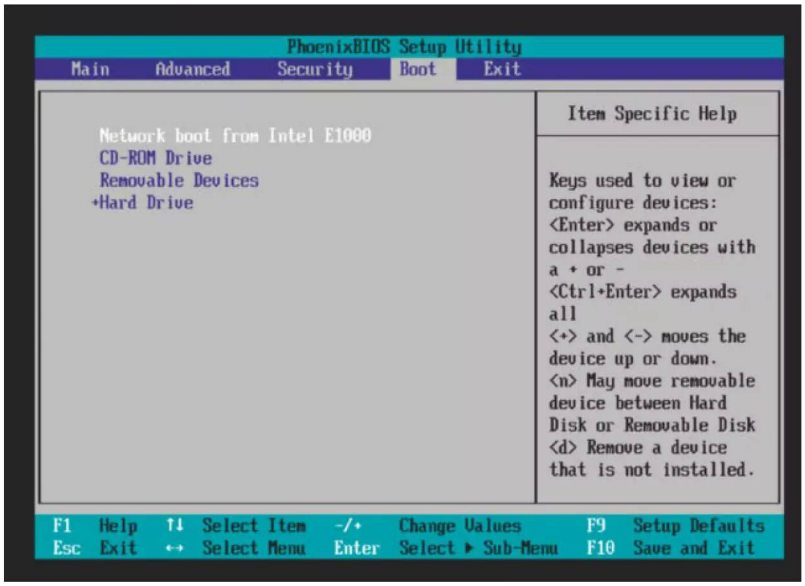
In diesem Schritt befüllen Sie das Bootverzeichnis /opt/tftpboot. Alle benötigten Dateien finden Sie im tftpboot.tgz-Archiv. Sie können diese einfach in Ihren Ordner /opt/tftpboot kopieren. Wenn Sie gerade kein Desinfec’t 2024/25 zur Hand haben, können Sie die Bootdateien auch herunterladen (siehe ct.de/wp9u). Wenn Sie mit UEFI-Clients arbeiten, müssen Sie das Paket zwingend herunterladen, da die benötigten Dateien im ISO-Image fehlen.

Zur Erläuterung: Ein BIOS-Client wird am Vendor-String „00000“ erkannt und erhält die Bootdatei „pxelinux.cfg“, bei allen anderen Clients wird angenommen, dass es sich um einen UEFI64-Client handelt, diese bekommen das EFI-Modul „bootx64.efi“. Falls Sie in Ihrem Netzwerk exotische Architekturen wie SPARC, Itanium oder alte UEFI32-Nettops übers Netz booten, ist die Differenzierung der Klasse „pxeclient“ detaillierter vorzunehmen. Der Client holt sich im Falle des BIOS-Clients die COM32-Module und die Konfigurationsdatei pxelinux.cfg/default via TFTP vom Server. Sie können nun erste Tests mit einer minimalen Version fahren:

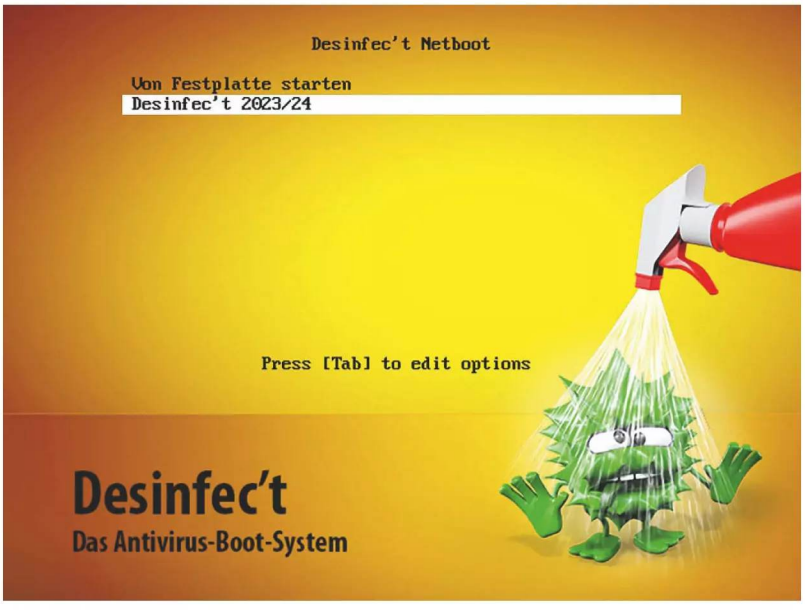
```
DEFAULT /menu.c32
TIMEOUT 300
MENU TITLE Desinfec't Netboot
LABEL local
MENU LABEL Von Festplatte starten
MENU DEFAULT
LOCALBOOT 0I
```

Im Falle von UEFI-GRUB gilt die Konfigurationsdatei grub/grub.cfg mit der folgenden minimalen Konfiguration:

```
set default=0
set timeout=10
```




**Im BIOS-Setup können Sie PXE als bevorzugte Bootmethode dauerhaft aktivieren. Ist mal kein Server im Netz aktiv, startet nach einigen Sekunden das auf der Festplatte installierte System.**




**Neben verschiedenen Desinfec't-Versionen kann man über ein modifiziertes Netboot-Menü auch andere Linux-Distributionen via PXE starten.**

```
menuentry "Start von Festplatte" {
  exit
}
```

In beiden Fällen wird der Computer lediglich angewiesen, die PXE-Boot-Umgebung nach 10 Sekunden zu verlassen und mit dem nächsten Bootmedium in der festgelegten Reihenfolge fortzufahren. Sind die Konfigurationsdateien abgelegt, können Sie Ihre Clients bereits testen: Sobald der PXE-fähige Client Antwort vom DHCP-Server erhalten hat, lädt er das Menü.

## Desinfec't-Bootdateien ablegen

Kopieren Sie nun noch Kernel (vmlinuz) und Ramdisk (initrd.lz) aus dem Ordner /casper im Desinfec't-ISO-Image in den TFTP-Boot-Ordner und passen Sie die IP-Adressen in den Konfigurationsdateien im Archiv tftpboot.tgz an. Mit dieser Änderung können Sie in die initiale Ramdisk booten.

Falls Sie planen, TFTP-Boot langfristig auch fürs Deployment von Images oder zur Installation von Linux-Servern einzusetzen, haben Sie die Möglichkeit, in der DHCP-Konfiguration pro MAC-Adresse zu bestimmen, ob und wenn ja welche Bootdatei verwendet werden soll. Mit der Option, die Bootdatei per MAC-Adresse zu überschreiben, booten Sie auch exotische Hardware wie ARM SBC mit uBoot, alte SPARC-Maschinen oder PowerPC-Macs ohne Konflikte übers Netz.

Der Bootloader PXELINUX erlaubt Konfigurationsdateien für MAC- oder IP-Adressen, die vor „default“ gesucht werden, mehr Details zeigt das Syslinux-Wiki (siehe ct.de/wp9u). Im Falle von GRUB empfehlen viele Tutorials, während des Bootvorgangs auf das HTTP-Protokoll zu wechseln, dann nämlich kann ein Skript auf dem Webserver anhand der IP-Adresse bestimmen, welche Konfiguration ausgeliefert wird.

## Der NFS-Server

Nun installieren Sie das Paket nfs-kernel-server und setzen damit den NFS-Server auf. Die Konfiguration geschieht in der Datei /etc/exports. An dieser Stelle müssen Sie folgende Zeile hinzufügen:

```
/opt/nfsboot/desinfect202425 ↵
↳10.76.23.0/24(ro,insecure,↵
↳no_subtree_check,async,↵
↳no_root_squash)
```

```
mkdir -p /opt/nfsboot/desinfect202425
mkdir /tmp/desinfect202425
mount -o loop desinfect202425-↵
↳amd64.iso /tmp/desinfect202425
rsync -avHP /tmp/desinfect202425/ ↵
↳/opt/nfsboot/desinfect202425/
umount /tmp/desinfect202425
```

Starten Sie jetzt den NFS-Server neu:

```
service nfs-kernel-server restart
```

Anschließend können Sie Ihren PXE-Client resetten und Desinfec't starten.

## Signaturen speichern?

Die Speicherung von aktualisierten Signaturen auf NFS-Freigaben ist möglich, hat aber Tücken und wird daher von uns nur eingeschränkt unterstützt. So dürfen zum Beispiel keine zwei Clients gleichzeitig Signaturupdates durchführen. Zudem können die numerischen User IDs von Linux für Verwirrung sorgen: Eset und WithSecure legen beim ersten Start - und damit bei der ersten Signaturaktualisierung - eigene Nutzer an, die jeweils die niedrigsten freien User IDs nutzen. Ist die Reihenfolge der Signaturaktualisierung bei zwei Clients oder bei einem erneuten Bootvorgang auf einem PC unterschiedlich, passt die Eigentümerschaft von Signaturen und Konfiguration nicht und keiner der Virenscanner kann genutzt werden.

Wenn Sie Signaturen auf einer NFS-Freigabe nutzen wollen um beispielsweise mit Yara/OTS und eigenen Erkennungsroutinen oder Thor Lite scannen wollen, können Sie das auch ohne tief gehende Linux-Kenntnisse NFS-Signaturen umsetzen. Für alles, was darüber hinaus geht, sollten Sie sich sehr gut mit Linux auskennen.

Zur „Erstbefüllung" nehmen Sie einen Stick zur Hand, auf dem Desinfec't persistent installiert ist. Kopieren Sie den kompletten Inhalt der Signaturpartition in einen Ordner auf dem NFS-Server, den Sie zuvor angelegt haben. Im Beispiel verwenden wir „/mnt/archiv/desinfect-signatures". Hier kopieren wir mit „rsync" unter Beibehaltung numerischer User IDs. IP-Adressen sind natürlich anzupassen, achten Sie auf die abschließenden Slashes:

```
rsync --avHP --numeric-ids /opt/desinfect/↵
↳signatures/ 10.76.23.250:/mnt/archiv/desinfect-↵
↳signatures/
```

Dieser Ordner bekommt jetzt den folgenden Eintrag in der Konfigurationsdatei /etc/exports:

```
/mnt/archiv/desinfect-signatures ↵
↳10.76.23.0/24(rw,no_subtree_check,no_root_squash)
```

Anschließend ergänzen Sie die PXELINUX-Konfiguration um den Parameter nfssigs:

```
nfssigs=10.76.23.250:/mnt/archiv/desinfect-↵
↳signatures
```

Nach dem Start eines Clients zeigt der Systemmonitor rechts oben „Signaturen auf NFS" und Updates überleben den Neustart.

Wenn Sie Desinfec't 2024/25 auf einem BtrfsStick mit Änderungen versehen haben, können Sie das modifizierte Rootverzeichnis der Btrfs-Partition in den Ordner casper/filesystem.dir/ des exportierten Desinfec't kopieren (rsync -avHP –delete-after quelle/ ziel/) und anschließend das komprimierte Dateisystem casper/filesystem.squashfs einfach löschen. Beim Netzwerkboot wird nun dieser Ordner als Root-Dateisystem genommen, spätere Anpassungen wie der Austausch von Grafiken oder Anpassungen der Starter auf dem Desktop (/etc/skel/ Desktop) sind dann mit geringem Aufwand auf dem Server möglich.

## Debugging

Falls mal etwas nicht funktioniert, schauen Sie noch einmal ganz genau hin: Mit dieser Schritt-für-Schritt-Anleitung sollten Konfigurationsprobleme schnell auffallen. Zusätzlich können sich erfahrene Linuxer beispielsweise mit einem TFTP-Client auf die Suche nach falsch gesetzten Berechtigungen für Dateien machen, die man per TFTP übertragen will. Problemen beim NFS-Mount kann man in der BusyBox-Shell eines unvollständig gestarteten Desinfec't auf den Grund gehen, beispielsweise indem man das Share manuell einbindet und dabei auf Fehlerausgaben achtet:

```
mount -t nfs server://share /cdrom
```

Klappt der Mount ohne Fehler, prüfen Sie, ob das richtige Verzeichnis exportiert wurde. Der Inhalt von /cdrom muss exakt wie bei einem von DVD gebooteten Desinfec't aussehen. Läuft alles, kann man die Optik noch etwas schicker machen: Im Syslinux-Wiki finden Sie viele Hinweise, um das PXE-Bootmenü aufzuhübschen (siehe ct.de/wp9u). (des) **c't**

**Bootloader, PXE-Bootmenü aufhübschen, PXE-Bootumgebung auf DSL-Router**
**ct.de/wp9u**

heise academy

# Schützen Sie Ihre Unternehmens-Daten

Webinar-Serie: „Verschlüsselung, digitale Signaturen & Zertifikate für Unternehmen“

*2. Oktober*
Passwortstrategien für Unternehmen & Selbstständige

*9. Oktober*
Einführung in die Verschlüsselung

*16. Oktober*
Symmetrische & hybride Verfahren in der Praxis

*23. Oktober*
Digitale Signaturen für eine verlässliche Kommunikation

*30. Oktober*
Digitale Zertifikate verstehen & anwenden

**Jetzt Tickets sichern:**
heise-academy.de/webinare/encrypt