c't Desinfec't

Das Rettungssystem bei Virenbefall

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

- Entfernt Trojaner und Viren unter Windows
- Mit 4 Scannern: ClamAV, ESET, IKARUS, WithSecure
- Signatur-Updates gratis bis Oktober 2026

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 nicht mehr startenden PCs bergen

Zusatz-Werkzeuge für Profis nutzen

Malware-Analyse mit mehreren Expertentools

Zwei Extra-Scanner selbst konfigurieren

Schnelleres Desinfec't von USB-SSD

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

4 197665 616908 03

Editorial

Liebe Leserin, lieber Leser,

verhält sich Ihr Windows-PC verdächtig und befürchten Sie eine Virusinfektion? Damit Schadcode nicht noch mehr Schaden anrichten kann, sollten Sie den Computer nicht mehr einschalten. Moment, auf Ihrer Festplatte liegen wichtige Daten, auf die Sie dringend zugreifen müssen? Keine Sorge, genau für solche Fälle gibt es das c't-Sicherheitstool Desinfec't.

Um einen möglicherweise verseuchten PC aus einer sicheren Entfernung zu untersuchen, bringt Desinfec't sein eigenes Live-Betriebssystem mit. Das startet direkt von einem USB-Stick statt Windows. So untersuchen Sie Ihr System mit Virenscannern von unter anderem Eset und Ikarus. Damit auch aktuelle Schädlinge entdeckt werden, sind ein Jahr lang gratis Signaturupdates für die Scanner inklusive. Das Sicherheitstool hilft, mögliche Fehlalarme einzugrenzen, es kann Bedrohungen aber auch unschädlich machen.

Nach dem Start von Desinfec't können Sie auf Windows-Festplatten zugreifen, um so Ihre wichtigsten Daten in Sicherheit zu bringen. Dafür kopieren Sie sie einfach auf den Desinfec't-Stick. Mit einem speziellen Tool können Sie mit etwas Glück sogar versehentlich gelöschte Daten wiederherstellen.

Auch wenn sich Desinfec't primär an PC-Einsteiger richtet, profitieren auch Malwareprofis davon. Mit dem Open Threat Scanner und dem Thor Lite Scanner erstellen sie auf bestimmte IT-Sicherheitsvorfälle maßgeschneiderte Scanregeln. Mit weiteren Tools ist zudem die Schadcodeanalyse von etwa Office-Dokumenten möglich.

Mit Desinfec't haben Sie ein mächtiges Werkzeug in Ihren Händen, um Ihren PC und Ihre Daten zu retten. Dabei wünschen wir Ihnen viel Erfolg!

Dennis Schirrmacher

Inhalt

Direkt loslegen!

Viren jagen mit Desinfec't

Mit dem c't-Sicherheitstool Desinfec't 2025/26 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 2025/26 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

Viren aufspüren, Daten retten

Das c't-Sicherheitstool Desinfec't macht Malware unschädlich und ermöglicht den sicheren Zugriff auf infizierte Windows-PCs. Das Tool richtet sich neben Computereinsteigern auch an Malware-Experten, die mit ausgewählten Profiwerkzeugen IT-Sicherheitsvorfälle analysieren. Die 2025/26er-Version bringt nun vier Virenscanner mit.

Von **Dennis Schirrmacher**

Wenn in Windows sprichwörtlich der Wurm drin ist, sollten Sie den Computer aus Sicherheitsgründen nicht mehr einschalten. Falls Sie das doch tun, richtet ein Schadprogramm mit sehr hoher Wahrscheinlichkeit noch mehr Unheil an und nimmt etwa Ihre Daten gegen eine Lösegeldzahlung in Beschlag. Doch wie gehen Sie am besten vor, wenn auf der Festplatte gespeicherte vertrauliche Dateien dringend benötigt werden? Hier bietet sich Desinfec't 2025/26 als Rettungsanker an.

Desinfec't ist eigentlich ein Linux-System; damit jedoch auch Computereinsteiger mit dem Sicherheitstool zurechtkommen, haben wir das Interface bewusst simpel gehalten und es orientiert sich optisch am Windows-Desktop. Die Icons sind verständlich beschriftet, sodass es keine Missverständnisse geben sollte.

Um die Untersuchung von Problem-PCs mit so wenig Risiko wie möglich zu ermöglichen, ist Desinfec't keine Windows-Anwendung, sondern bringt ein eigenes Linux-Livesystem mit und startet direkt von einem USB-Stick statt des regulär installierten Windows. So greifen Sie aus sicherer Entfernung auf eine inaktive Windows-Installation zu. In diesem

Zustand ist nämlich auch ein möglicher Virus zur Untätigkeit verdonnert.

Für die Überprüfung des Systems sind mehrere Virenscanner von unter anderem ESET, IKARUS und WithSecure mit dabei. Zusätzlich bringen Sie mit dem Sicherheitstool Ihre persönlichen Daten in Sicherheit. Malware-Experten unterstützt Desinfec't mit diversen Profi-Analysetools wie Capa und FLOSS. Wer die Kernfunktionen von Desinfec't bereits kennt, kann direkt zum Praxisartikel (Seite 14) springen, der Schritt für Schritt zeigt, wie man es am effektivsten nutzt.

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

Downloaden und installieren

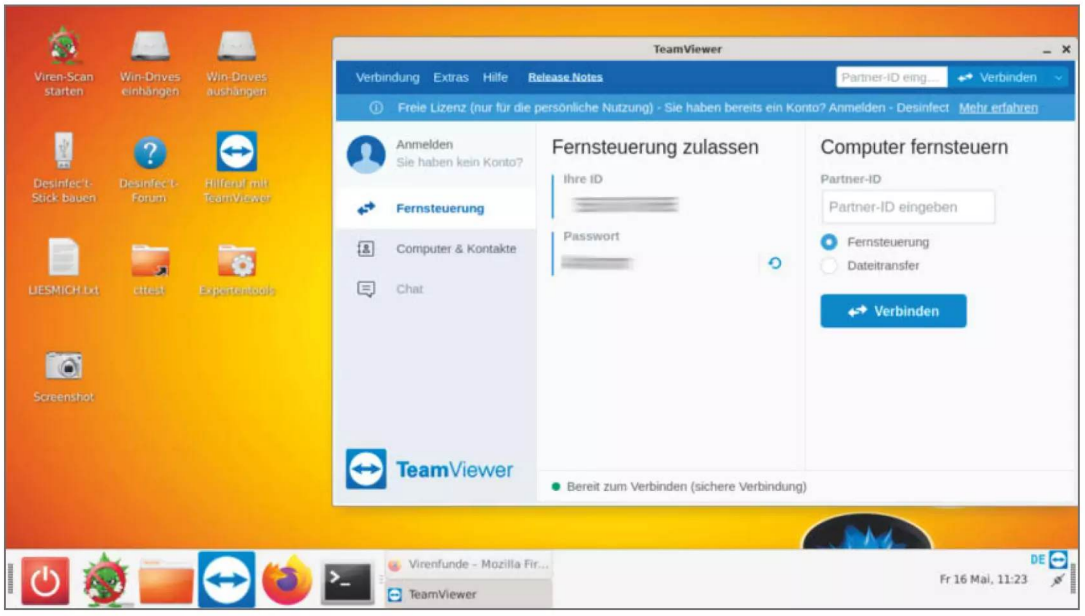
Um einen Windows-Computer zu untersuchen, müssen Sie Desinfec't 2025/26 zuerst herunterladen und dann auf einem USB-Stick mit mindestens 16 Gigabyte installieren. Das dafür benötigte Installationstool Desinfect2USB ist im Download enthalten. Das reine Kopieren der ISO-Datei auf einen USB-Stick klappt nicht. Auch Tools zum Erzeugen von bootfähigen Sticks wie Rufus funktionieren nicht. Nur mit unserem Installationstool erhalten Sie nach wenigen Minuten einen funktionsfähigen Desinfec't-Stick.

Theoretisch startet Desinfec't auch von einer DVD. Das ist aber aus mehreren Gründen nicht zu empfehlen: So läuft das System nämlich fühlbar langsamer und die Bedienung wird zur Geduldsprobe. Noch schwerer wiegt, dass Signaturupdates nicht auf der DVD gespeichert werden können. Demzufolge muss man alle Signaturen wieder und wieder herunterladen. Nur auf einem USB-Stick bleiben aktualisierte Virensignaturen auch nach einem Neustart erhalten.

Zum Starten von Desinfec't müssen Sie Ihren PC noch so einstellen, dass er nicht Windows von der Festplatte, sondern Desinfec't vom USB-Stick bootet. Das ist zum Glück keine Raketenwissenschaft, und der Kasten „Desinfec't starten“ auf Seite 10 zeigt kompakt, wie das geht.

Wir haben das System auf PCs verschiedenen Alters erfolgreich gestartet und konnten es problemlos nutzen. Weil es aber unzählige Hardwarekonstellationen gibt, bootet Desinfec't leider nicht auf

Damit auch Computereinsteiger mit Desinfec't 2025/26 klarkommen, orientiert sich die Desktopdarstellung an Windows und die Icons sind prägnant beschriftet.



Wer nicht weiterkommt, holt sich den Familien-Admin über TeamViewer zu Hilfe. Der greift dann über das Internet auf den Problem-PC zu und hilft bei der Analyse.

allen Computern aus dem Stand. Im Praxisartikelartikel ab Seite 14 finden sich Tipps für Problem-PCs, damit es mit dem Start trotzdem klappt.

Damit das System stabil läuft, muss der zu untersuchende PC mindestens über 8 GByte RAM verfügen. Das ist nötig, weil das Live-System komplett aus dem Arbeitsspeicher läuft. Dort machen sich auch die Virenscanner breit. Vor allem im Zuge der Signaturaktualisierung beanspruchen sie einige Ressourcen.

Direkt loslegen

Wenn das Desinfec't-Startmenü erscheint, haben Sie die erste Hürde erfolgreich überwunden. Hier können Sie mit dem Easyscan direkt ohne Umwege eine Untersuchung der Windows-Festplatten einleiten. In diesem Modus startet der Scanner von ESET direkt mit einer Analyse der gesamten Windows-Installation. Für den vollen Funktionsumfang wählen Sie den Menüpunkt „Desinfec't starten" aus.

In diesem Modus haben Sie die Wahl aus mehreren Scannern von unter anderem ESET und IKARUS. Zusätzlich sind mehrere Expertentools enthalten, die sich aber ausdrücklich an Malware-Profis richten. Schließlich ist die Bedienung dieser Tools komplexer, und schon für die korrekte Deutung der Ergebnisse muss man über Kenntnisse zu Schadsoftware verfügen.

Vor einem Scan aktualisieren sich die Scanner bei einer aktiven Internetverbindung automatisch. Das ist wichtig, damit ESET & Co. auch aktuelle Bedrohungen erkennen. Signaturupdates sind ein Jahr lang gratis. In der Regel reicht es für einen ersten Überblick aus, nur einen Scanner von der Leine zu lassen. Nach der Aktualisierung startet der Scan umgehend.

Standardmäßig schauen sich die Scanner auf der gesamten Windows-Festplatte um. Auf Wunsch können Sie aber auch nur einzelne Ordner untersuchen oder eine am PC angeschlossene USB-Festplatte. Nach dem Scan öffnet sich im integrierten Firefox-Browser eine Ergebnisliste. Über darin enthaltene Links können Sie unter anderem entdeckte Malware unschädlich machen. Dabei löscht Desinfec't die verdächtigte Datei nicht, sondern benennt sie um, sodass Windows sie nicht mehr ausführen kann. Das lässt sich im Zweifelsfall später auch einfach wieder rückgängig machen. Außerdem stehen Hilfsmittel bereit, um mögliche Fehlalarme besser einschätzen zu können.

Wir haben dafür gesorgt, dass man in Desinfec't auch Laufwerke scannen kann, die mit Microsofts BitLocker und VeraCrypt verschlüsselt sind. Das

klappt auch mit vollständig verschlüsselten Windows-Installationen.

Profis können sich mit dem Open Threat Scanner und dem Thor Lite Scanner sogar eigene Scanregeln erstellen, umso individuell und zielgenau raffinierten Schädlingen nachzuspüren. Mehr Informationen dazu und zu den weiteren Expertentools finden Sie in einem Praxisartikel (siehe Seite 32).

Daten retten

Eins muss aber jedem klar sein: Desinfec't ist kein Wundertool, das auf Knopfdruck automatisch PCs bereinigt, rettet und dabei womöglich auch noch verschlüsselte Daten wiederherstellt. Vielmehr ist es ein mächtiges Diagnosetool, das beim Eingrenzen von Schäden hilft. Zusätzlich fungiert es als Notfallsystem und ermöglicht so den Zugriff auf nicht mehr startende PCs.

Das ist hilfreich, wenn Windows mit Schadcode verseucht ist oder überhaupt nicht mehr startet. Weil Windows-Viren unter Linux nicht ausgeführt werden können, besteht für Desinfec't keine Infektionsgefahr. Außerdem setzt sich das Sicherheitstool nach jedem Neustart in den Ausgangszustand zurück. Eine Sicherheitsmaßnahme, damit sich nichts im System einnistet.

So können Sie in Ruhe auf persönliche Daten zugreifen und etwa Bewerbungen und Fotos in Sicherheit bringen, indem Sie die Dateien auf dem Desinfec't-Stick speichern. Mit dem Expertentool Photorec besteht außerdem die Chance, dass Sie versehentlich gelöschte Daten wiederherstellen können.

Dank des integrierten TeamViewer-Clients greifen Familien-Admins über das Internet auf Problem-PCs von Familie und Bekannten zu und helfen bei der Diagnose.

Hilfe in Sicht

Um die Funktionsweise von Desinfec't 2025/26 zu verstehen und das volle Potenzial des Sicherheitstools auszuloten, sollten Sie die folgenden Artikel genau studieren. Dort steht unter anderem ausführlich, wie Sie das Sicherheitstool installieren, booten und einen Virenscan starten. Zusätzlich gibt es Tipps, um verschiedene Probleme zu lösen. Aus der Erfahrung heraus beantwortet der Artikel viele Fragen, die uns Leser immer wieder stellen.

Außerdem finden Sie im Desinfec't-Forum Hilfe (siehe ct.de/wsnb). Dort tauschen sich Nutzer über Probleme aus und präsentieren oft Lösungen. Um Bugs auszubügeln, etwa wenn Microsoft, wie schon öfter in der Vergangenheit passiert, an BitLocker dreht, können wir Desinfec't-Updates bereitstellen, die sich bei einer bestehenden Internetverbindung in der Regel automatisch installieren. (des) ct

Desinfec't-Forum:
ct.de/wsnb

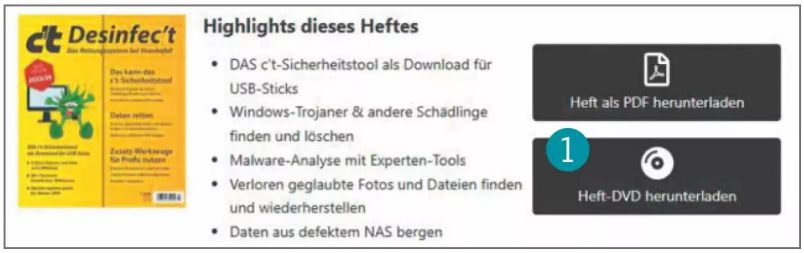
Desinfec’t 2025/26 im Nu einsetzen

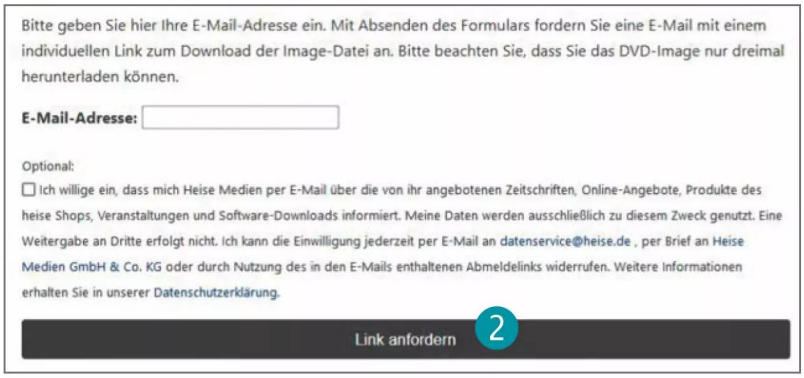
Um mit dem c’t-Sicherheitstool einen PC zu untersuchen, müssen Sie es nur herunterladen und auf einem USB-Stick installieren. Mit dieser Anleitung ist das gar nicht schwer und in wenigen Minuten erledigt.

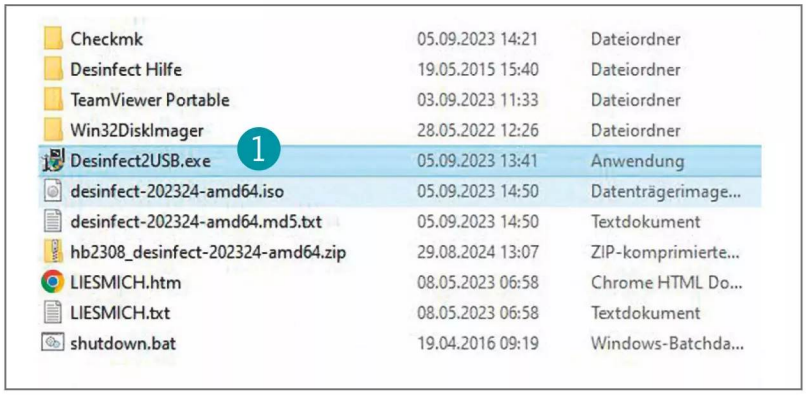
Von **Dennis Schirrmacher**

Herunterladen, entpacken, installieren und starten. Das sind die grundlegenden Schritte, die Sie vor dem Scan eines Windows-Computers erledigen müssen. Läuft Desinfec’t 2025/26, 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 2025/26 noch nicht final und die Downloadseite war noch offline. Deswegen stammen die Bilder aus einer Vorgängerversion. Die Schritte sind aber alle gleich geblieben. (des) *c't*

Desinfec't 2025/26 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 2025/26. 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.

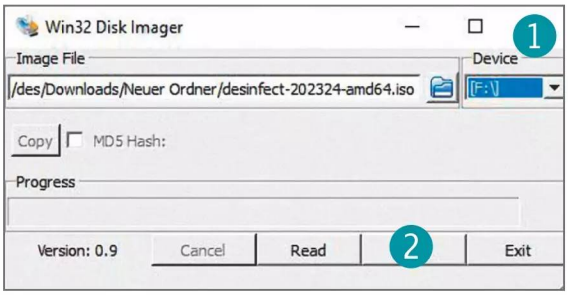


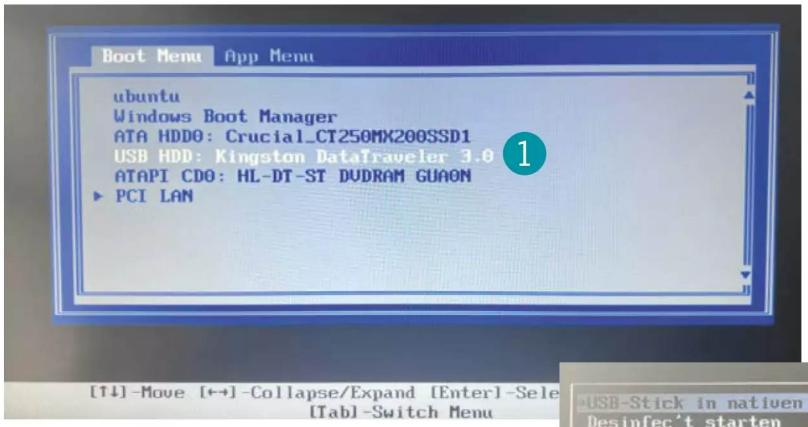




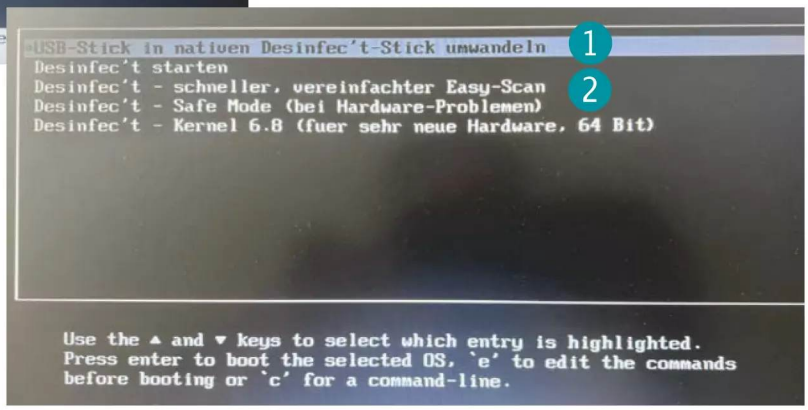
Installationsassistent starten: Ist der Download des circa 4 GB großen Archivs mit Desinfec't 2025/26 abgeschlossen, entpacken Sie es. Um nach dem Entpacken mit der Installation auf einem USB-Stick zu beginnen, starten Sie unser Installationstool „Desinfect2USB" mit einem Doppelklick (1). Im Anschluss 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 2025/26 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.

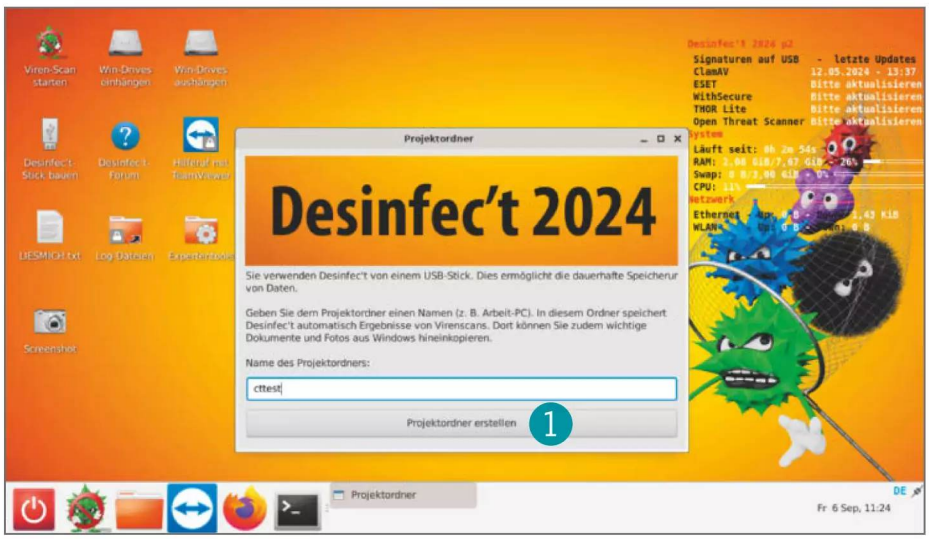




Desinfec't 2025/26 starten: Welche Möglichkeiten es gibt, Ihren PC vom Desinfec't-Stick anstatt Windows zu starten, steht im Artikel auf Seite 16. Hier sehen Sie den sichersten Weg über das BIOS-Bootmenü, bei dem ein möglicherweise verseuchtes Windows nicht laufen muss. Wählen Sie an dieser Stelle den 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.

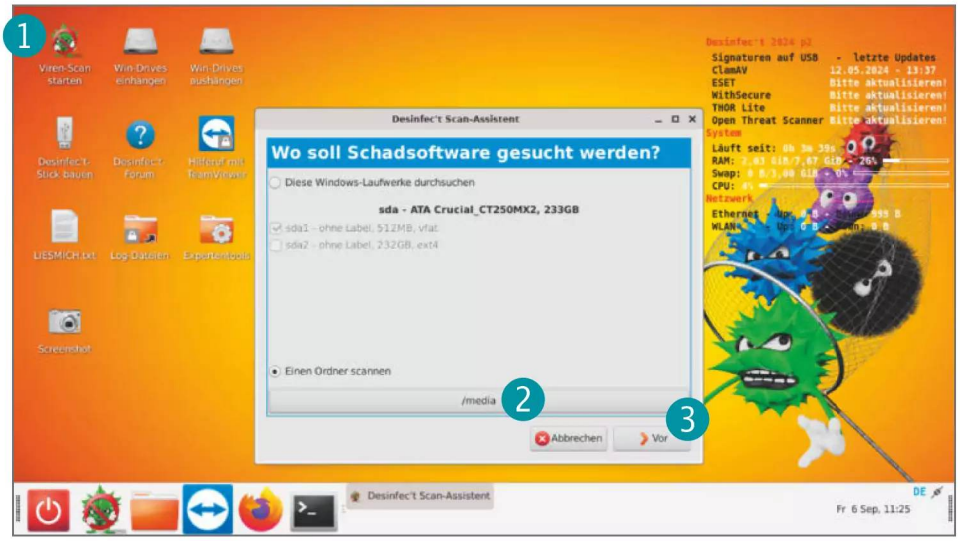


Desinfec't-Stick einmalig umwandlen: Damit sich ein Desinfec't-Stick auch aktualisierte Virensignaturen merkt, müssen Sie ihn einmalig umwandeln. Wählen Sie dafür den ersten Punkt aus (1). Ist dieser Vorgang abgeschlossen, wählen Sie in Zukunft stets den Punkt „Desinfec't starten" aus. Alternativ können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

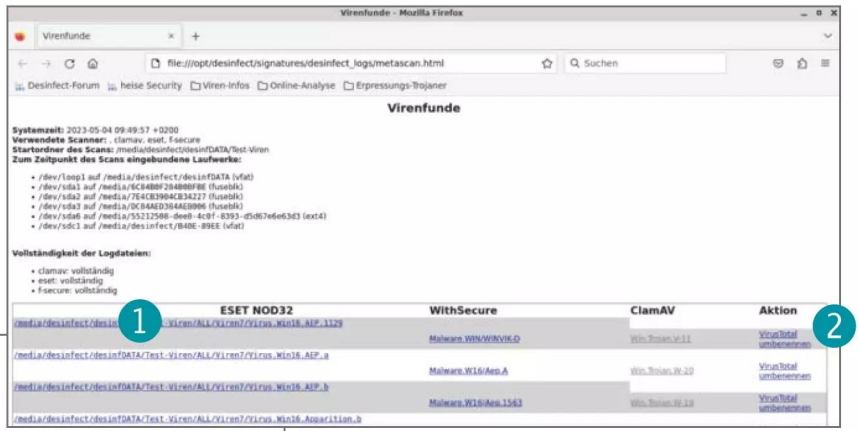


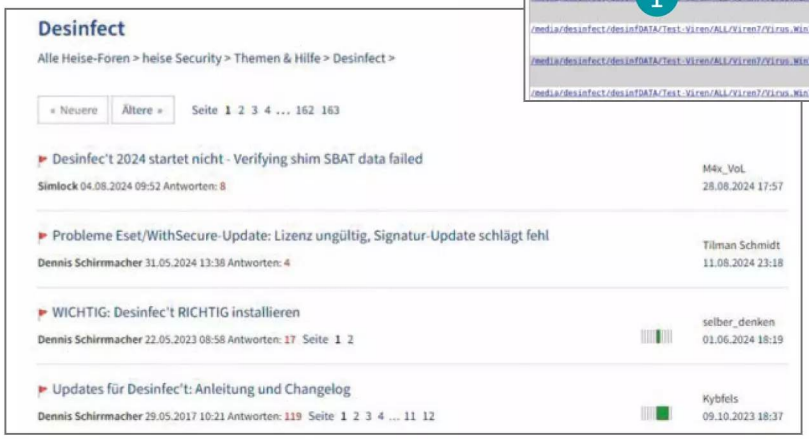
Nach dem ersten Start: Booten Sie Desinfec't auf einem Computer das erste Mal, müssen Sie einen Projektordner anlegen (1). Das ist praktisch, wenn Sie den Stick an verschiedenen PCs benutzen. Mit Projektordner-Namen wie „Spiele-PC" oder „Arbeitscomputer" verlieren Sie nicht den Überblick. In diesem Ordner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

Desinfec’t 2025/26 voll ausschöpfen

Desinfec’t ist ein mächtiges Sicherheitstool, das Ihnen beim Auffinden von Schadcode hilft und den Zugriff auf verunfallte und nicht mehr startende Windows-PCs ermöglicht. Dieser Artikel zeigt, wie das am einfachsten und schnellsten geht und welche Analysetools für Malware-Experten enthalten sind.

Von **Dennis Schirrmacher**

Über Computer verwalten wir unsere Onlineidentität, managen unter anderem Passwörter und erledigen Bankgeschäfte. Außerdem speichern wir unser Leben auf Massenspeichern und neben unersetzbaren privaten Fotos liegen dort auch wichtige Dokumente. Diese Kronjuwelen befinden sich im Visier von Cyberkriminellen: Mittels kopierter Log-in-Daten kapern sie Benutzerkonten, und verschlüsselte Daten dienen als Druckmittel zum Erpressen von Lösegeld.

Weil betrügerische Mails mit Schadcode im Anhang immer glaubwürdiger werden, kann man es Opfern kaum vorwerfen, wenn sie auf eine etwa im Namen eines Freundes verschickte gefälschte Mail hereinfallen, den Dateianhang mit Schadcode öffnen und sich einen Virus einfangen. Wenn das passiert, steigt der Stresslevel natürlich rasant. Versuchen Sie in so einem Fall erst mal Ruhe zu bewahren, denn mit Desinfec’t 2025/26 ist Hilfe in greifbarer Nähe. Die Anleitung zeigt, wie Sie dabei vorgehen.

Das c’t Sicherheitstool stützt sich auf die Linux-Distribution Ubuntu 22.04 LTS und wird als Live-System auf einem USB-Stick installiert. Davon startet es direkt, um eine inaktive Windows-Installation aus sicherer Entfernung zu untersuchen. Dafür sind Virenscanner von ClamAV, ESET, IKARUS und WithSecure auf dem Stick. Mit ESET und IKARUS haben wir uns bewusst für zwei Scanner aus Europa entschieden, die sich bei der Datenverarbeitung an die Datenschutz-Grundverordnung (DSGVO) halten müssen. Der Scanner von IKARUS hat in unseren Tests mit einer hohen Erkennungsrate gepunktet. Außerdem finden alle Analysen lokal statt und es gibt keine Datei-Uploads in die Cloud. Vor einem Scan mit IKARUS erscheint ein Fenster, in dem Sie die Teilnahme am Signature-Quality-Assurance-Programm (SigQA) bestätigen oder ablehnen können. Über dieses Telemetriesystem analysiert IKARUS neue Bedrohungen, um die Erkennungsrate zu verbessern. Die Übermittlung der Daten an die IKARUS-Server erfolgt verschlüsselt und anonymisiert. Mit seinem Open-Source-Ansatz ist ClamAV als Ergänzung zu den Closed-Source-Scannern der namhaften Hersteller mit an Bord.

Das ist neu in Desinfec’t 2025/26

- Gratis Signaturupdates bis Oktober 2026
- Kernel 6.8 (optional 6.16 für neue Hardware)
- Neue Malware-Analysetools wie QPDF
- Überarbeiteter BTRFS-Installer für SSDs

Wie Sie Desinfec't 2025/26 herunterladen

Käufer der digitalen Einzelausgabe bekommen mit ihrer Auftragsbestätigung via E-Mail einen Downloadlink für die Zip-Datei mit Desinfec't 2025/26.

Auch Kioskkäufer können Desinfec't herunterladen. Dafür müssen Sie lediglich die Website ct.de/desinfect2025-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.

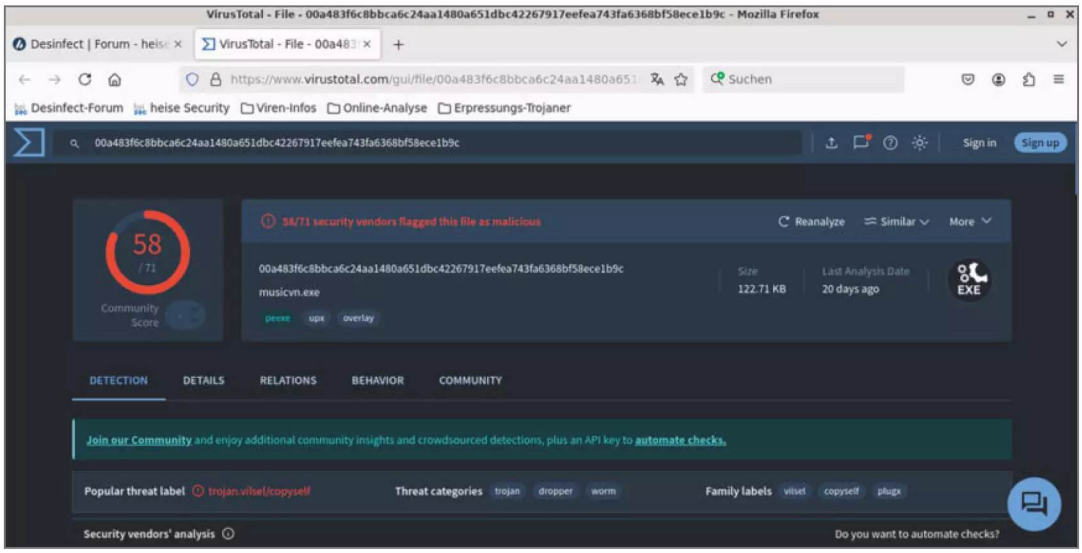
Außerdem sind der Open Threat Scanner (OTS) und der Thor Lite Scanner dabei (siehe Seite 32). Letztere sind vor allem bei brandaktuellen Bedrohungen, die noch kein Virenscanner erkennt, sehr hilfreich. Doch diese beiden Scanner und weitere Expertentools richten sich vor allem an Malware-Profis, die bereits Erfahrung in der Behandlung von Security-Vorfällen mitbringen.

Herunterladen und installieren

Desinfec't 2025/26 ist für jeden Käufer dieser Ausgabe kostenlos. Damit Sie für die oben beschriebene Stresssituation gewappnet sind, sollten Sie am besten jetzt gleich einen Desinfec't-Stick erstellen. Den legen Sie sich dann in die Schublade und sind somit auf den Ernstfall einer Computerattacke vorbereitet.

Haben Sie nicht vorgesorgt und Ihr PC ist bereits von Schadcode durchlöchert, können Sie Ihr Windows-System zum Erstellen eines Sticks selbstverständlich nicht starten. In so einem Fall erstellen Sie den Stick auf einem anderen Computer, etwa am Arbeitsplatz oder bei einem Freund. Das geht auch, wie später beschrieben, unter Linux.

Um mit der Installation zu beginnen, benötigen Sie einen USB-Stick mit mindestens 16 GByte



Um Fehlalarme einzugrenzen, laden Sie verdächtige Dateien zum Onlineanalyseservice VirusTotal hoch. Dort schauen 70 Scanner drauf und helfen Ihnen bei der Einschätzung.

Speicherplatz und das Zip-Archiv mit Desinfec't 2025/26. Greifen Sie am besten zu einem flinken USB-3.0-Stick von einem Markenhersteller, damit das Speichern von aktualisierten Virensignaturen schnell und verlässlich funktioniert. In der Vergangenheit haben uns oft Leseranfragen erreicht, die Probleme mit dem Start oder Signaturupdates hatten, und in vielen Fällen war der Grund ein lahmer USB-Stick. Damit Sie dafür einen Anhaltspunkt haben, prüft ein Skript vor der Installation, ob ein Stick schnell genug ist. Ist er zu lahm, erscheint eine Warnung und die Installation bricht ab. Neuerdings kann man Desinfec't auf einer USB-SSD installieren, was mehrere Vorteile mitsichbringt (siehe Seite 88).

Haben Sie den Stick, folgt der Download von Desinfec't 2025/26. Wie das funktioniert, steht im nachfolgenden Kasten „Wie Sie Desinfec't 2025/26 herunterladen". Im Archiv befindet sich unter anderem die ISO-Datei von Desinfec't 2025/26 und das Installationstool „Desinfect2USB". Bitte nutzen Sie zur Installation ausschließlich Desinfect2USB. Nur unser Tool stellt sicher, dass Desinfec't 2025/26 korrekt installiert wird.

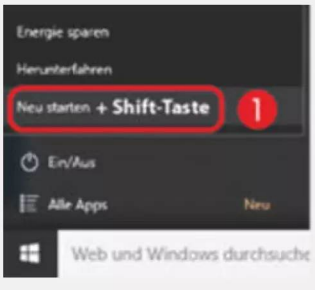
Hintergrund ist: Desinfec't benötigt auf dem Stick ein bestimmtes Partitionslayout, das unser Installer Desinfect2USB dynamisch und passend zu Ihrem Stick erzeugt. Desinfec't besteht aus mehreren Bereichen. Das System befindet sich auf einer Partition, die sich nach jedem Neustart aus Sicherheitsgründen wieder in den Werkszustand zurückversetzt. Virensignaturen liegen wiederum auf einer anderen Partition, die Daten persistent speichert.

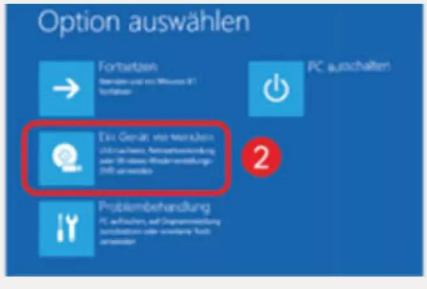
Desinfec't starten

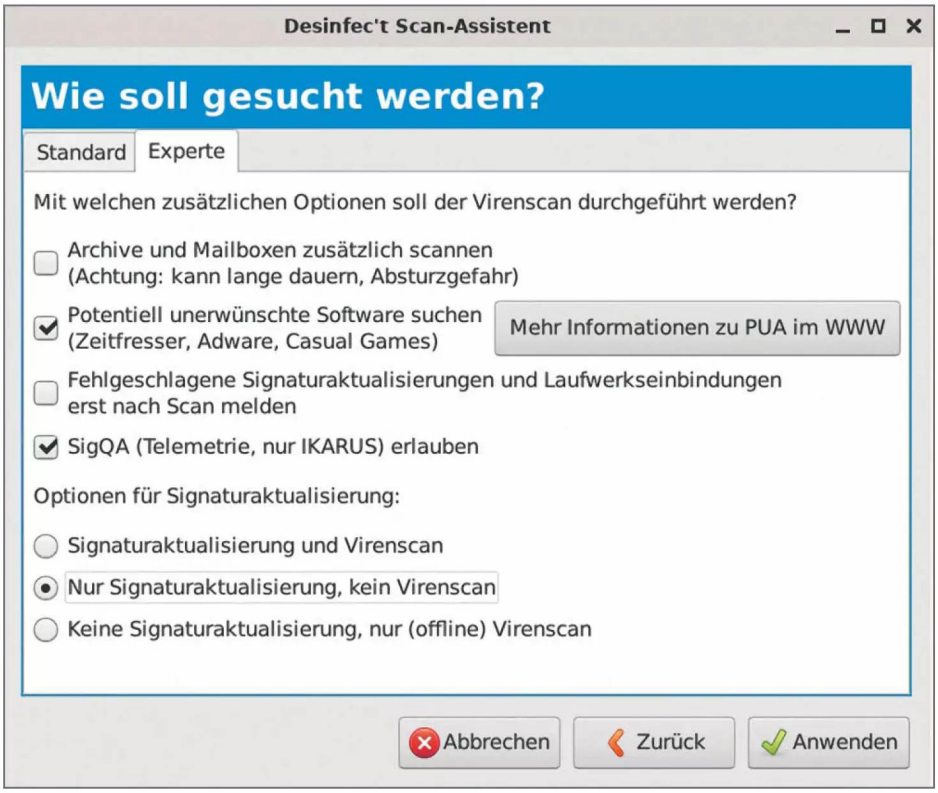
Vermuten Sie, dass ein Schädling sein Unwesen auf Ihrem Windows-PC treibt, fackeln Sie nicht lange und fahren Sie den Computer herunter. Schließen Sie dann den Desinfec't-Stick an. Schalten Sie den PC wieder ein und drücken sofort entweder F8, F10, F11 oder F12, damit das BIOS-Bootmenü erscheint. Bei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

Erscheint das BIOS-Menü, wählen Sie im Anschluss das Medium mit Desinfec't aus und starten Sie davon. Funktioniert das nicht, ist ein Umweg über das vollständige BIOS-Menü nötig. 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. Dafür halten Sie die Umschalttaste (Shift-Taste) gedrückt (1) und klicken im Startmenü auf Neustart. Im nächsten Bildschirm bestätigen Sie den dort aufgeführten Punkt „Ein Gerät verwenden" (2). Danach wählen Sie das Medium mit Desinfec't aus (3). Nun fährt Windows herunter und bootet automatisch das Notfallsystem. Will der Start partout nicht klappen, wählen Sie im Desinfec't-Bootmenü die Option „Safe Mode" aus. Dann sollte alles funktionieren.







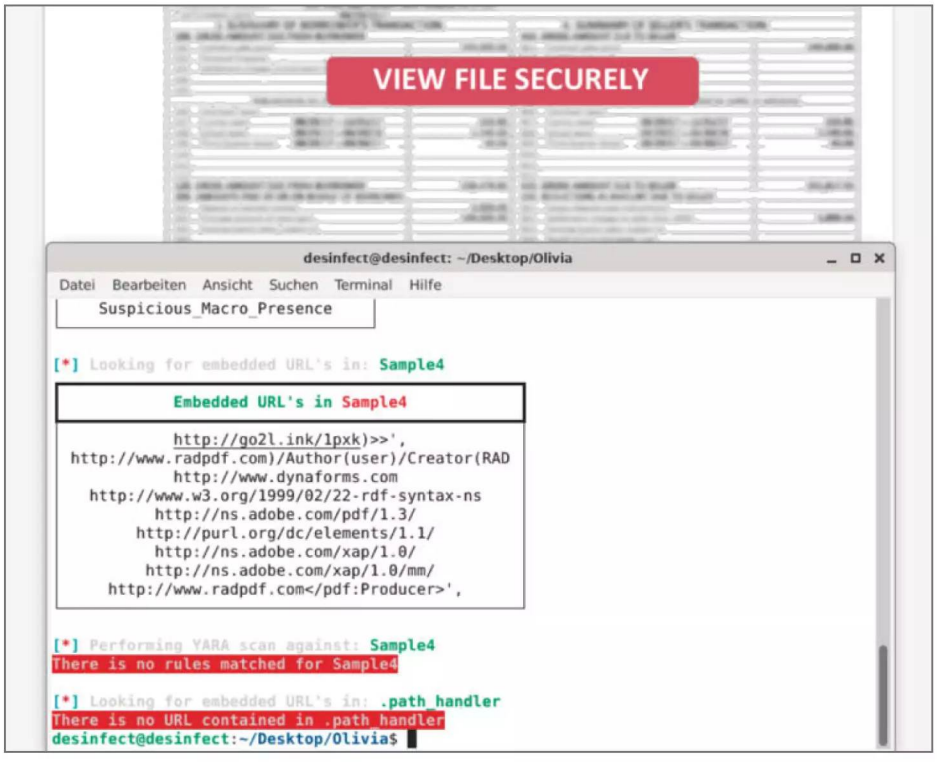
Wer möchte, kann auch nur die Virensignaturen aktualisieren, ohne den PC zu scannen. Im Anschluss können Sie den Desinfec't-Stick mit aktuellen Signaturen an einem Offline-PC nutzen.

Die Installation mit Etcher oder Rufus funktioniert deshalb nicht. Auch wenn es auf den ersten Blick so aussieht und auch ein bootfähiger Stick dabei herauskommt, von dem Desinfec't startet, kommt es spätestens im Betrieb zu schwerwiegenden Problemen. So stürzt das System oft ab und aktualisierte Virensignaturen werden nicht dauerhaft gespeichert.

Stöpseln Sie zur Installation den USB-Stick am PC ein und starten Sie unter Windows Desinfect-2USB. Taucht an dieser Stelle eine Fehlermeldung mit der Beschreibung „Error 5“ auf, funkt ein übereifriger Virenscanner dazwischen und will den Zugriff auf den USB-Stick verhindern. Ist das der Fall, schalten Sie Ihren Echtzeitscanner für die Dauer der Installation aus.

Nach einem Doppelklick auf Desinfect2USB öffnet sich das Tool Win32 Disk Imager und die ISO-Datei des Sicherheitstools ist vorausgewählt. Prüfen Sie danach unbedingt, ob der ausgewählte Laufwerksbuchstabe unter „Device“ dem des USB-Sticks entspricht. Das ist wichtig, weil das Installationstool den ausgewählten Stick ohne weitere Nachfrage vollständig löscht. Um auf Nummer sicher zu gehen, prüfen Sie im Explorer von Windows, welcher Laufwerksbuchstabe dem Stick zugeordnet ist. Sind Sie sich vollkommen sicher, klicken Sie zum Start der Installation auf „Write“. Mit einem flinken Stick ist die Installation nach wenigen Minuten abgeschlossen. Nicht wundern: Nach der Installation ist es normal, dass der Stick im Explorer von Windows nicht angezeigt wird. Beim ersten Start müssen Sie den Stick nämlich noch für den vollen Funktionsumfang einmalig konvertieren. Doch dazu später mehr.

Alternativ können Sie Desinfec't auch unter Linux herunterladen und mit dem Konsolenbefehl `dd if=desinfect-202526-amd64.iso of=/dev/sdx status=progress` installieren. Wenn Sie bereits einen USB-Stick mit Desinfec't 2025/26 besitzen, können Sie aus dem laufenden System weitere Sticks erstellen. Praktisch: Dabei werden auch aktualisierte Virensignaturen direkt übernommen. Um die Installation auf diesem Weg zu starten, klicken Sie auf dem Desktop auf das



Mit dem Expertentool Qu1cksc0pe entlocken Sie etwa PDF-Dateien Geheimnisse, ohne die Datei zu öffnen.

Icon „Desinfec't-Stick bauen“. Für einen Stick mit üblichem Funktionsumfang belassen Sie es bei den Standardoptionen und klicken auf „Anwenden“. Wenn Sie für Familienmitglieder einen Stick erstellen wollen, können Sie die Option „Easy Scan“ auswählen. So ein Stick startet ohne Umwege direkt in den Scanmodus.

Wer sich mit Linux auskennt und den Desinfec't-Stick mit weiteren Anwendungen und Tools aufmotzen möchte, wählt die Btrfs-Option aus (siehe Seite 48). Wegen der Snapshotfunktion des Btrfs-Dateisystems bleibt installierte Software auch nach einem Neustart erhalten.

Die Starthürde

Das kniffligste ist das Booten von Desinfec't. Es ist wichtig zu verstehen, dass Desinfec't keine Anwendung ist, die Sie unter Windows starten. Vielmehr starten Sie Ihren Computer vom USB-Stick mit Desinfec't anstatt vom Windows-System auf der Platte. Wie Sie das bewerkstelligen, erklärt der Kasten „Desinfec't starten“ Schritt für Schritt (siehe unten).

Doch leider läuft das Sicherheitstool nicht auf allen Computern. Dabei ist inkompatible Hardware das Hauptproblem. Wir haben Desinfec't 2025/26 erfolgreich auf vielen PC-Modellen der vergangenen Jahren erfolgreich gestartet, konnten damit eine Netzwerkverbindung aufbauen, Signaturen aktualisieren und sie scannen, doch es wird immer Systeme geben, auf denen das Sicherheitstool nicht läuft. Das ist vor allem auf älteren PCs der Fall. Aus Ressourcengründen können wir nicht alle jemals erschienenen Treiber testen und unterstützen.

Klappt der Start nicht, wählen Sie im Desinfec't-Startmenü den alternativen Kernel 6.16 aus. Funktioniert es damit auch nicht, können Sie mit einem Safe-Start-Punkt versuchen, zumindest ein rudimentäres System auf die Beine zu bekommen.

Festplatten untersuchen

Auf jedem PC will Desinfec't nach dem ersten Start einen individuellen Projektordner anlegen. Vergeben Sie dafür einen prägnanten Namen wie „Homeoffice-PC“. Das ist besonders praktisch, um nicht den Über-

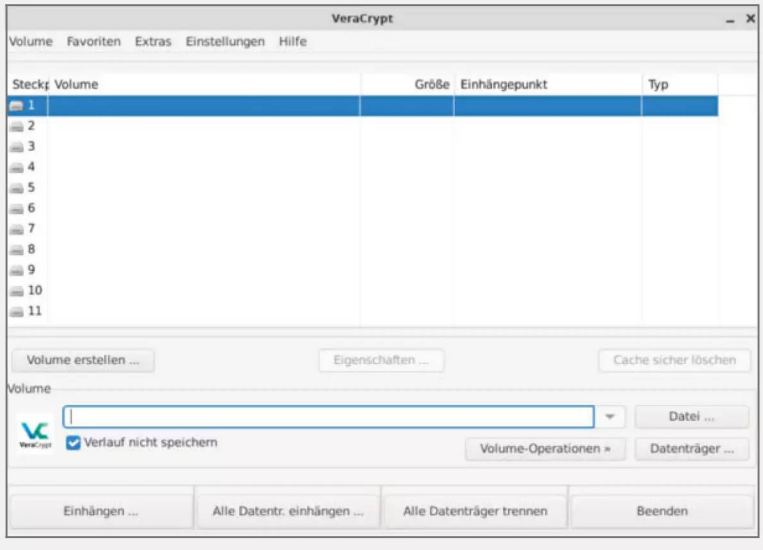
Verschlüsselte Festplatten scannen

Wer seine Festplatte mit Microsofts Bitlocker verschlüsselt hat, kann das Laufwerk direkt aus dem Scanassistenten heraus einbinden. Dafür wählen Sie es lediglich aus und geben nach den Scannerupdates das Bitlocker-Passwort ein. Das klappt auch, wenn Sie den PC via TPM entsperren und den 48-stelligen Wiederherstellungsschlüssel eingeben. Diesen finden Sie in Ihrem Microsoft-Konto. In Desinfec't loggen Sie sich mithilfe des Firefox-Browsers in Ihr Microsoft-Konto ein, um darauf zuzugreifen.

Bei Tests in der Redaktion hat die Entschlüsselung über Desinfec't problemlos mit Systempartitionen, die unter aktuellen Windows 10 und 11 verschlüsselt wurden, 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 den Bitlocker-Schrauben dreht und die Entwickler der Mount-Tools unter Linux erst mal nachziehen müssen. Wann immer das erfolgt, bringen wir Desinfec't auf den aktuellen Stand.

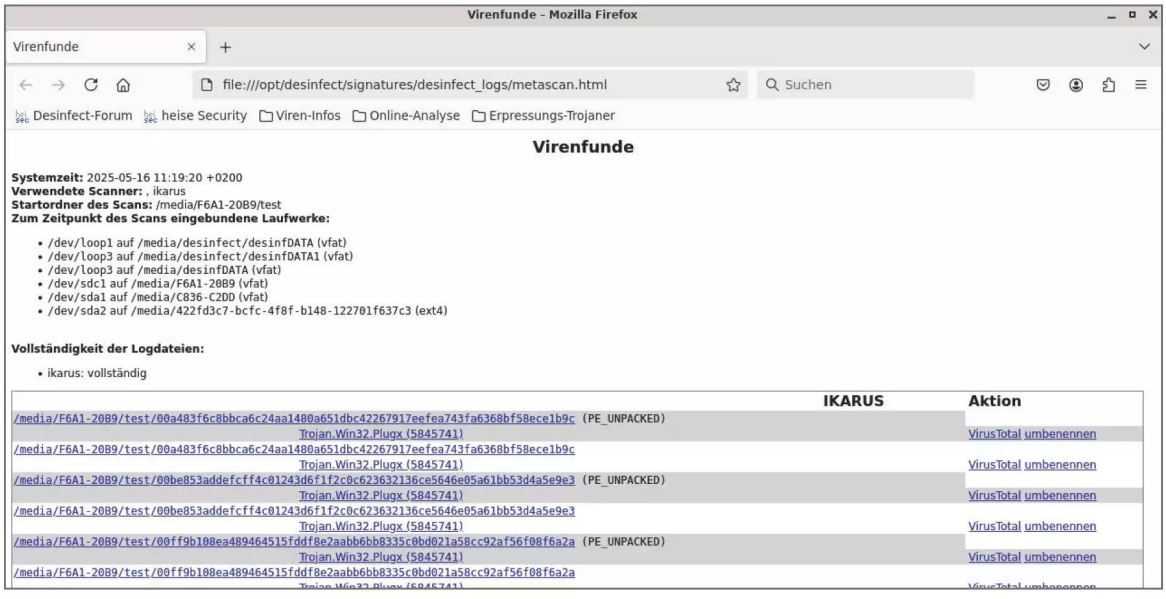
Seit Windows 11 23H2 gibt es die Verschlüsselung auch für Windows Home. Erfüllt ein Desktop-PC oder Notebook Microsofts Voraussetzungen für Windows 11, wird die Festplatte automatisch verschlüsselt. Doch erst, wenn Sie Ihren PC mit einem Microsoft-Konto verbinden, erhalten Sie ein Passwort/Wiederherstellungsschlüssel. Unter Windows greifen Sie aber auch ohne Microsoft-Konto auf die nicht mit einem Passwort geschützte, aber trotzdem verschlüsselte Festplatte zu. Dank eines Kniffs klappt das auch unter Desinfec't. Wollen Sie in diesem Fall ein BitLocker-Laufwerk mounten, lassen Sie das Passwortfeld einfach frei und drücken Sie die Eingabetaste.

Wer mit VeraCrypt verschlüsselte Daten scannen möchte, muss die Container beziehungsweise Laufwerke über den VeraCrypt-Client im Expertentools-Ordner einbinden. Wählen Sie den verschlüsselten Datenträger aus und mounten diesen. Die Festplatte taucht dann im Scanassistenten zur Auswahl auf. Haben Sie Ihre Systemplatte komplett verschlüsselt, wählen Sie noch die Option „Partition mithilfe der Systemverschlüsselung einhängen (Pre-Boot Authentifizierung)“ aus. Im Scanassistenten taucht die Festplatte nicht als Windows-Partition auf, sondern erst nach Auswahl von „einen Ordner scannen“ auswählen.



blick zu verlieren, wenn Sie mit dem Sicherheitstool auf dem Stick mehrere Computer untersuchen wollen. In diesem Ordner landen neben den Scanergebnissen auch in Sicherheit gebrachte Dateien.

Damit die Scanner ihre Virensignaturen aktualisieren können, benötigt Ihr PC eine Internetverbindung. Dafür schließen Sie einfach ein Ethernetkabel an. Natürlich funktioniert eine Verbindung auch kabellos via WLAN, dann benötigen Sie aber Zugangsdaten dafür. Für eine WLAN-Verbindung klicken Sie auf das WLAN-Symbol unten rechts in der Taskleiste. Wenn sich Desinfec't Ihr WLAN-Kennwort merken soll, starten Sie den Scanassistenten über das Icon „Viren-Scan starten“. Nun taucht zuerst ein Verbindungsassistent auf. Geben Sie das WLAN-Passwort für das ausgewählte Netz ein und speichern es. Fortan verbindet sich Desinfec't automatisch mit diesem WLAN. Doch Vorsicht: Das Kennwort liegt unverschlüsselt



Nach einem Scan öffnet sich automatisch die Ergebnisliste in Firefox. Von dort aus können Sie Funde zur weiteren Analyse auf VirusTotal hochladen oder Trojaner direkt unschädlich machen.

auf dem Stick. Gerät dieser in falsche Hände, kennt der Finder ihr WLAN-Passwort. Sie können, wenn verfügbar, natürlich von vornherein auch ein Gäste-WLAN nutzen, das von Ihrem Haupt-WLAN entkoppelt ist. Klappen Signaturupdates nicht, setzen Sie die Signaturen mithilfe eines Skripts aus dem Expertentools-Ordner auf dem Desinfec't-Desktop zurück und probieren es dann noch einmal.

Im Anschluss wählen Sie die zu untersuchenden Partitionen und die Scanner aus. Die erweiterten Optionen können Sie unverändert belassen. Vorsicht: Aktivieren Sie den Punkt „verschlüsselte Archive scannen", erhöht das die Scanzeit immens und außerdem können PCs mit wenig Speicher abstürzen, weil das Entpacken im Arbeitsspeicher geschieht, der je nach Größe eines Archivs überlaufen kann.

Schlagen die Scanner Alarm, bewahren Sie erst mal Ruhe! Vor allem ClamAV neigt zu Fehlalarmen. Dennoch halten wir ihn für eine gute Ergänzung zu den kommerziellen Scannern. Sie sollten also alle Funde analysieren. Um das Risiko eingrenzen zu können, laden Sie einen verdächtigen Fund zur Onlineanalyseplattform VirusTotal hoch. Das klappt direkt aus der Ergebnisliste über den entsprechenden Menüpunkt. Bei diesem Service untersuchen rund 70 Onlinescanner die Datei und zudem finden sich dort oft Kommentare von anderen Nutzern, die bei der Einschätzung helfen können, ob es vielleicht ein Fehlalarm war.

Ist es aber wirklich ein Virus, machen Sie den durch einen Klick auf „umbenennen" unschädlich. Weil aus Trojaner.exe Trojaner.exe.VIRUS wird, kann Windows die Datei nicht mehr ausführen. Wenn Sie damit versehentlich eine legitime Datei behandelt haben, können Sie das Umbenennen rückgängig machen. Das klappt auch im großen Stil für mehrere Dateien mit dem Skript „Umbenennung rückgängig machen" im Expertentools-Ordner auf dem Desktop.

Werkzeuge für Profis

Außer OTS und Thor Lite Scanner bringt Desinfec't weitere Malware-Analysetools mit. Mit Werkzeugen wie Capa, Detect It Easy, FLOSS Qu1cksc0pe und QPDF analysieren Malware-Profis Dateien auf Schadcode und werten die Ergebnisse aus (siehe S. 40 und 72). Somit eignet sich Desinfec't 2025/26 außer zum einfachen Virenscan auch für Incident-Response-Tätigkeiten und Datenforensik. (des) c't

CLC25

19. und 20. November 2025 • Mannheim

Die Konferenz für Developer Experience, Platform Engineering und mehr

Highlights aus dem Programm:

- **Platform Engineering:** Der goldene Pfad zur eigenen Developer-Plattform
- **KI in Software Development und Delivery:** Hilfreiche Agenten
- **Stabile Systeme:** Mit Observability den Überblick behalten
- **Sichere Supply Chain:** Images, Dependencies, Authentifizierung
- **Erfahrungsberichte:** KI, IT-Grundschutz, Multi Tenancy & Co.

Jetzt **Frühbucher-tickets** sichern!

Workshops am 18. November

clc-conference.eu

Gold-Sponsor: CloudBees

Silber-Sponsor: ;-) Plus.line

Veranstalter: iX Magazin für professionelle IT; dpunkt.verlag

FAQ Desinfec't 2025/26

Das c't-Sicherheitstool hilft bei der Analyse von möglicherweise mit Schadcode infizierten Windows-PCs. Außerdem bringen Sie damit Ihre Daten von nicht mehr startenden Computern in Sicherheit. Dabei tauchen gelegentlich Probleme auf, die aber in der Regel schnell gelöst sind.

Von **Dennis Schirrmacher**

Stick-Konvertierung klappt nicht

? Ich habe Desinfec't wie im Heft beschrieben unter Windows mit dem offiziellen Installationstool Desinfect2USB installiert. Dann habe ich den Stick, wie im Artikel erwähnt, beim ersten Start in einen nativen Stick konvertiert. Das hat aber, glaube ich, nicht richtig geklappt, denn wenn ich den PC jetzt vom Stick starte, taucht der Punkt zum Umwandeln wieder im Desinfec't-Bootmenü auf. Was mache ich falsch?

! Sie haben gar nichts falsch gemacht, und der Stick ist vollständig konvertiert. Dabei handelt es sich um einen Bug im Grand Unified Bootloader (GRUB) zum Starten von Linux-Systemen, der in Verbindung mit Desinfec't auf manchen Computern auftaucht. Leider sind wir diesem Fehler bislang nicht auf die Spur gekommen und konnten ihn deshalb bisher nicht bereinigen. Wählen Sie einfach den Punkt „Desinfec't starten" aus. Im Anschluss sollte der Eintrag nicht mehr auftauchen.

Keine WLAN-Verbindung möglich

? Ich habe einen brandneuen Laptop mit einem Wi-Fi-7-Modul. Leider findet Desinfec't mein WLAN nicht und ich kann keine Internetverbindung herstellen. Haben Sie einen Tipp für mich?

! Das klingt so, als würde der Treiber für das WLAN-Modul fehlen. Desinfec't hat für solche Fälle den

alternativen Kernel 6.16 implementiert, der Treiber für sehr neue Hardware mitbringt. Um das System damit zu starten, wählen Sie einfach den entsprechenden Eintrag im Desinfec't-Bootmenü aus. Bei einem Testsystem mit Wi-Fi 7 hat das bei uns geklappt.

Upgrade möglich?

? Ich habe noch den Stick mit Desinfec't 2024/25 in der Schublade liegen. Kann ich den irgendwie auf die aktuelle Version upgraden?

! Nein, das ist nicht möglich. Bitte installieren Sie neue Desinfec't-Versionen nicht auf Sticks mit älteren Ausgaben, da es sonst zu massiven Fehlern im Betrieb kommt. Sie können den alten Stick aber wie unter „Desinfec't-Stick löschen" beschrieben formatieren und dann das neue Desinfec't 2025/26 darauf installieren.

Desinfec't-Stick löschen

? Ich möchte gerne meinen alten Desinfec't-Stick löschen und wieder als normalen USB-Stick nutzen. Leider steht nach der Formatierung nur ein Bruchteil des eigentlichen Speicherplatzes zur Verfügung. Ist der Stick jetzt kaputt?

! Nein, der Stick ist nicht kaputt. Das Problem ist, dass Desinfec't auf mehreren Linux-Partitionen liegt, die Windows nicht alle sieht. Deshalb können Sie diese Partitionen mit den herkömmlichen Festplatten-Werkzeugen in Windows nicht ändern oder löschen. Dafür gibt es aber eine Lösung: Geben Sie unter Windows 10/11 im Suchfeld `cmd` ein und öffnen so die Eingabeaufforderung. Starten Sie dann das Windows-Dienstprogramm zum Verwalten von Laufwerken, indem Sie `diskpart` eintippen und die Eingabetaste drücken. Geben Sie `list disk` ein, um die am Computer angeschlossenen Laufwerke anzuzeigen. Mit dem Befehl `select disk ?` wählen Sie den Stick mit Desinfec't aus. Das Fragezeichen steht für die Nummer des Datenträgers. Stellen Sie unbedingt sicher, dass Sie den korrekten Stick ausgewählt haben: Der nächste Schritt löscht alle Daten unwiderruflich. Nun tippen Sie den Befehl `clean` ein. Mit `create partition primary` erzeugen Sie eine Partition auf dem Speicherstick. Anschließend formatieren Sie den Datenträger wie gewohnt über den Windows-Explorer und einem Rechtsklick auf „Formatieren". Dann steht er wieder mit seiner vollen Kapazität zur Verfügung.

Zu wenig RAM?

? Ich habe hier noch einen sehr alten PC mit 4 GByte Arbeitsspeicher. Desinfec't startet zwar, ein Scan friert aber immer reproduzierbar ein. Ist Desinfec't 2025/26 mit meinem Computer nicht kompatiblel?

! Jein. Desinfec't basiert auf einem Linux-Livesystem, das direkt von einem USB-Stick startet. Deshalb läuft das gesamte Betriebssystem aus dem RAM und belegt entsprechend Platz. Wenn dann noch die Scanner ihre Signaturen aktualisieren und der Scanvorgang startet, belegt das in der Regel mehr als 4 GByte. Für den Betrieb sind demzufolge mehr als 4 GByte RAM notwendig. Mit 8 GByte sind auf jeden Fall genügend Reserven vorhanden.

Fehler 105 und 122

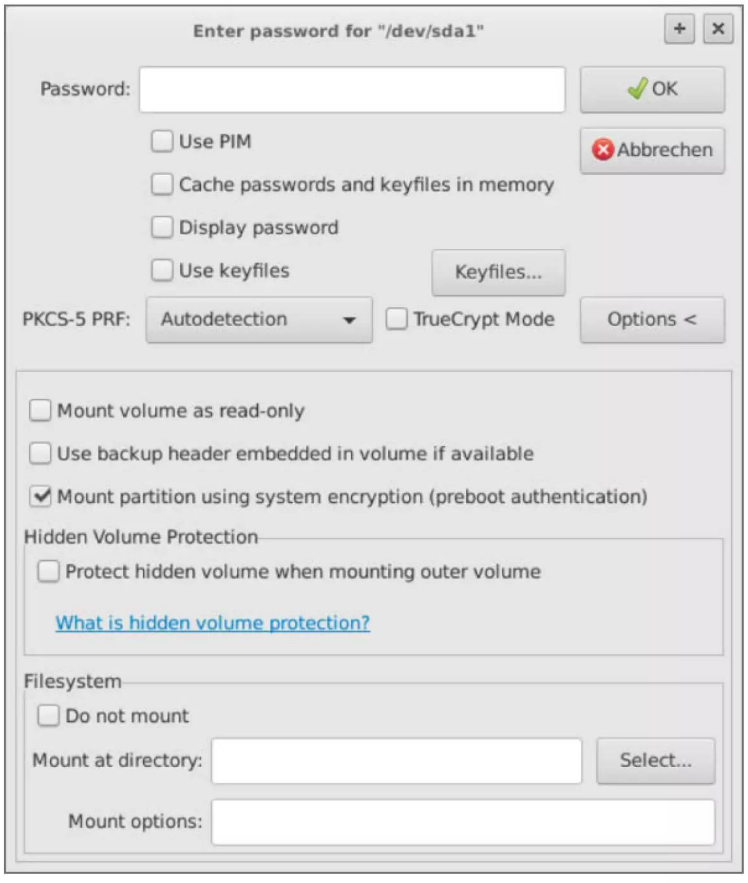
? Ich halte mich penibel an die Installationsanleitung unter Windows im Heft, aber es taucht immer wieder die Fehlermeldung 122 auf und ich kann die Installation nicht abschließen. Was läuft da schief? Im Internet habe ich übrigens auch etwas über Fehler 105 gelesen, aber das scheint ein anderes Problem zu sein.

! Den Fehler 122 konnten wir bislang nicht reproduzieren. Aber im Desinfec't-Forum haben wir Einträge dazu gefunden, in denen Nutzer das Problem mit der Deaktivierung der Google-Drive-Software gelöst haben. Im Anschluss war die Installation möglich. Beim Fehler 105 verhindert ein Virenscanner den Zugriff auf einen USB-Stick, sodass die Installation nicht gestartet werden kann. In diesem Fall pausieren Sie bitte Ihren Virenwächter temporär für die Installation. Vergessen Sie aber danach nicht, den Virenschutz wieder einzuschalten.

Virensignaturen werden nicht gespeichert

? Ich habe den Stick mit Rufus erstellt. Desinfec't startet auch, aber aktualisierte Virensignaturen sind nach einem Neustart wieder verschwunden. Ist mein Stick defekt?

! Der Stick ist fehlerhaft. Die Installation funktioniert nur mit unserem Tool Desinfect2USB korrekt. Dieses Installationstool finden Sie im heruntergeladenen Zip-Archiv. Nur Desinfect2USB stellt sicher,



Damit der VeraCrypt-Client auch vollverschlüsselte Windowsinstallationen erkennt, müssen Sie den Haken wie im Screenshot zu sehen setzen.

dass alle für den reibungslosen Betrieb notwendigen Partitionen erzeugt werden. Das Betriebssystem ist etwa auf einer Partition, die sich nach jedem Neustart aus Sicherheitsgründen komplett zurücksetzt, damit sich dort nichts einnisten kann. Die Virensignaturen liegen wiederum auf einer persistenten Partition, damit sie einen Neustart überleben. Demzufolge sind Installationen mit Etcher, Rufus & Co. unvollständig und es kommt zu Abstürzen und Fehlern.

Windows mit VeraCrypt wverschlüsselt

? Ich habe meine Windows-Installation komplett mit VeraCrypt verschlüsselt. Desinfec't kann über den integrierten Client ja auf damit verschlüsselte Laufwerke zugreifen. Aber irgendwie klappt das bei mir nicht. Was mache ich falsch?

! Verschlüsselte Container oder Laufwerke binden Sie wie gewohnt über den VeryCrypt-Client in Desinfec't ein. Wenn aber das gesamte Windowssystem verschlüsselt ist, müssen Sie im VeraCrypt-Client die Option „Mount partition using system encryption (preboot authentication)" aktivieren. Dann klappt das Scannen auch mit einem vollverschlüsselten Windows.

Weitere Hilfe

Antworten auf weitere Fragen und Hilfe zu Problemen finden Sie im offiziellen Desinfec't-Forum (siehe ct.de/wdzm). Dort können Sie auch gerne selbst gefundene Lösungen für Probleme abladen. Neben Nutzern helfen dort auch zum Launch von neuen Desinfec't-Versionen die Redaktion und unser Entwickler aus. (des) *c't*

Desinfec't-Forum:
ct.de/wdzm

Aktuelle IT-Bedrohungstrends

Welche Malware ist derzeit besonders gefährlich, welche aktuellen Angriffswege sollte man kennen und wie kann man sich schützen? Dieser Artikel liefert Antworten und gibt Tipps zur Prävention und leistet Erste Hilfe.

Von **Olivia von Westernhagen**

Das digitale Böse ist nicht totzukriegen: Wann immer Strafverfolger bestehende Cybercrimegangs zerschlagen, formieren sich die verbleibenden Akteure im Untergrund neu. Sie ändern ihre Strategien und satteln auf neue, oft noch raffiniertere Angriffsmethoden um.

Entsprechend wichtig ist es, gegenwärtige Bedrohungstrends zu kennen. Anhand aktueller Veröffentlichungen und Statements von Behörden und Sicherheitssoftwareherstellern haben wir die wichtigsten Entwicklungen aufgeschlüsselt und zeigen, wie Sie sich schützen können. Dabei geht es unter anderem um Ransomware-Erpressung ganz ohne Verschlüsselung, zunehmenden Informationsdiebstahl und eine besonders fiese Social-Engineering-Masche namens „ClickFix“.

Ransomware-Business in Bewegung

Eine zentrale Rolle in der derzeitigen Bedrohungslandschaft nehmen die schon seit Jahren dominie-

renden Verschlüsselungstrojaner ein. Daran hat auch die Tatsache nichts geändert, dass die Erpresserszene im vergangenen Jahr massive Umwälzungen durchlief: Gleich zwei etablierte Gangs, nämlich Lockbit und Blackcat/ALPHV, mussten ihre Posten als Platzhirsche im Ransomwarebusiness räumen.

Lockbit, die bis dahin erfolgreichste und aktivste Gruppe, fiel Anfang 2024 der „Operation Cronos“ internationaler Strafverfolger zum Opfer. Mit dezimiertem Personal und geschwächter Infrastruktur spielt sie seither eine eher untergeordnete Rolle. Die Blackcat-Gang nutzte kurze Zeit später die günstige Gelegenheit für einen „Exit Scam“: Unter dem Vorwand eines Website-Takedowns machte sie sich mit Lösegeldern in Millionenhöhe aus dem Staub und hinterließ geprellte Partner, denen eigentlich ein Anteil zugestanden hätte.

Das alles sorgte aber nicht etwa für einen dauerhaften Rückgang erpresserischer Aktivitäten. Andere Gangs, die sich zuvor nicht gegen die großen Konkurrenten durchsetzen konnten, haben die entstandene Lücke schnell gefüllt. Viele von ihnen verfolgen wie Lockbit und Blackcat ein Ransomware-as-a-Service-Modell (RaaS): Sie vermieten ihre Erpresser-Infrastrukturen und streichen von den Mietern (Affiliates) eine Provision ein.

Erbitterte Konkurrenz

Eine klare und vor allem dauerhafte Vormachtstellung im Ransomware-Business hat indes noch keine der nachgerückten Gangs übernehmen können. Je nach Sicherheitssoftwarehersteller und Statistik werden als neue Spitzenreiter unter anderem RansomHub, Qilin, Akira und Cl0p gehandelt. Alle vier sind laut einer Liste aktiver Cybercrime-Gruppen des Bundesamts für Sicherheit in der Informationstechnik (BSI) auch in Deutschland aktiv.

Gemäß Statistiken von Palo Altos Unit 42 war RansomHub mit weltweit über 250 Erpressungen die aktivste Gruppe im ersten Quartal 2025. Einen möglichen Grund für diesen Erfolg liefert die Vermutung von Sicherheitsforschern, dass hinter RansomHub ein Rebranding von Blackcat steckt oder dass zumindest einige ehemalige Mitglieder beteiligt sein könnten. Das dürfte auch viele Ex-Blackcat-Affiliates auf der Suche nach einem „neuen“ und doch schon erprobten Erpresserwerkzeug angezogen haben.

Trend Micro wiederum hält Qilin, auch bekannt als Agenda, für die derzeit stärkste Kraft im RaaS-Geschäft. In England sorgte diese Gang im laufenden Jahr für den ersten offiziell anerkannten Todesfall

„This domain has been seized“: Dank des verstärkten Einsatzes internationaler Strafverfolger zieren solche Banner immer häufiger die Darknet-Websites von Crimeware-Gangs.

infolge eines Cyberangriffs: In einem attackierten Krankenhaus starb ein Patient, der aufgrund der IT-Störung zu spät versorgt werden konnte.

Zu den genannten Gruppen, die teilweise schon seit mehreren Jahren im Geschäft sind, gesellen sich laufend neue, die angesichts der Szene-Umwälzungen Morgenluft wittern. So etwa die Interlock-Gang, vor der US-Behörden im Juli 2025 warnten und die auch in Europa aktiv sein soll. Zugleich bringen regelmäßige Ermittlungserfolge unter internationaler Beteiligung etablierte wie auch neue Gruppen immer öfter ins Straucheln. So legte etwa im Juli dieses Jahres „Operation Checkmate“ die Darknet-Infrastruktur der Ransomware-Gang Blacksuit lahm. Rund zwei Monate zuvor hatten Strafverfolger im Rahmen der „Operation Endgame 2.0“ gar Hunderte Server vom Netz genommen – ein erfolgreicher Schlag gegen das gesamte Crimeware-Ökosystem.

Datenklau im Fokus

Und noch ein Umstand macht der stark fluktuierenden Szene das (Über-)Leben schwer: Offenbar wird es immer schwieriger, Ransomwareopfer zu einer Zahlung zu bewegen. So zahlten laut Statistiken des IT-Sicherheitsdienstleisters Coveware im zweiten Quartal 2025 nur 26 Prozent der Opfer ein Lösegeld; im zweiten Quartal des Vorjahres waren es noch 36 Prozent.

Statt mögliche finanzielle Einbußen mit breit gestreuten Angriffen zu kompensieren, setzen die derzeit erfolgreichsten Gangs weiterhin vor allem auf „High Profile“-Targets. Große Konzerne und Organisationen sowie kritische Infrastrukturen also, denen sie immer höhere Lösegelder abzupressen versuchen.

Im zweiten Quartal 2025 hat Coveware einen sprunghaften Anstieg durchschnittlich gezahlter Beträge um mehr als 100 Prozent verzeichnet – von zuvor 552.777 US-Dollar im ersten Quartal auf nun durchschnittlich 1.130.070 US-Dollar. Spannend dabei: Coveware schreibt die heftige Spitze aktuellen „data-exfiltration-only incidents“ bei einzelnen großen Organisationen zu. Dabei handelt es sich um Erpressungen, bei denen komplett auf die sonst übliche, zusätzliche Verschlüsselung der Systeme („Double Extortion“) verzichtet wurde.

Ganz neu ist dieses Konzept nicht. Die ClOp-Gang setzte schon im Herbst 2023 auf eine Sicherheitslücke in MoveIT-File-Sharing-Servern, schöpfte wertvolle Unternehmensdaten ab, drohte mit einer Veröffentlichung und verlangte – ganz ohne Verschlüsselung – Lösegelder in Millionenhöhe. Nachdem dieser Plan aufgegangen war, verfolgt ClOp den eingeschlagenen Pfad des Schwachstellen-Missbrauchs bis heute weiter: Die Leaksite der Gang listet regelmäßig neue, teils prominente Opfer wie HP oder HPE.

Richard Werner, Security Advisor bei Trend Micro, bestätigt die Entwicklung gegenüber c’t: Die Verschlüsselung werde „in vielen Fällen gar nicht mehr durchgeführt“ – möglicherweise um die Opfer „darüber im Unklaren zu lassen, was bereits alles infiziert ist“. Weitere Vorteile der Vorgehensweise für die Kriminellen: Sie lässt sich deutlich schneller und unauffälliger bewerkstelligen und spart den Gangs viel Aufwand bezüglich der Verwaltung von Entschlüsselungskeys nebst zugehörigem Kundenservice.

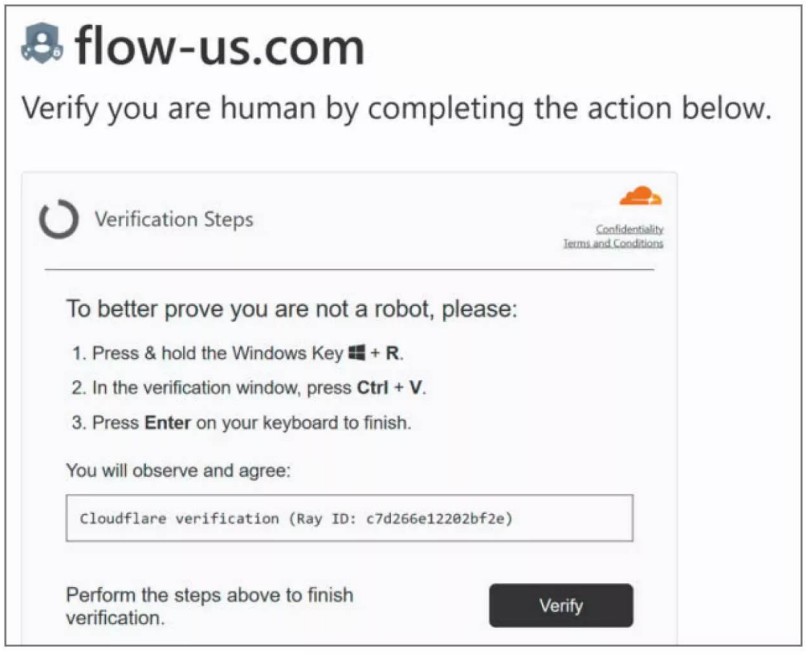
Ob das Konzept des „data-exfiltration-only“-Ansatzes irgendwann zum Standard wird oder ob es sich eher als alternative Variante zur „Double Extortion“ hinzugesellt, bleibt abzuwarten. In dem dramatischen Anstieg der durchschnittlich gezahlten Lösegelder will Coveware jedenfalls noch keinen grundsätzlichen Trend sehen. „Ausreißer nach oben“ zwischen zwei Quartalen habe es auch in der Vergangenheit schon gegeben, beteuert der Dienstleister in einem Blogeintrag.

Trotz des aktuellem Ransomware-Fokus auf große Unternehmen sollten sich Privatpersonen nicht allzu sehr in Sicherheit wiegen. Denn auch sie können weiterhin jederzeit ins Visier von Ransomware geraten. Wichtig in diesem Zusammenhang: Aktuelle Ransomware-Familien bedrohen längst nicht mehr nur Windows. RansomHub beispielsweise kann sich auch auf Linux-, NAS- und ESXi-Systemen einnisten.

Informationsdiebstahl im Aufwind

Auf die Frage, welcher Malware-Typ ihnen abseits von Ransomware in den vergangenen Monaten besonders häufig begegnet sei, antworteten Experten von G Data, Mandiant, OPSWAT und Trend Micro gegenüber c’t einhellig: Infostealer. Schadcode also, der infizierte Systeme nach wertvollen Informationen wie Log-in-Daten durchforstet.

Ebenso wie Ransomware- sind auch Infostealer-Angriffe oft finanziell motiviert und finden im Kontext eines Crimeware-as-a-Service-Modells statt. Gestohlene Daten werden unter anderem in Untergrundforen zum Verkauf angeboten oder unmittelbar von den Dieben für Identitätsklau oder sonstige Betrügereien missbraucht.



Vorsicht vor „ClickFix“-Angriffen: Gefälschte Captchas bringen ahnungslose Nutzer zum proaktiven Ausführen von Schadcode auf ihren Rechnern.

Der mittlerweile weltweit verbreitetste Infostealer heißt Lumma. Er hat es auf Windows-PCs abgesehen und sammelt dort unter anderem Browserdaten, Krypto-Wallets, VPN-Konfigurationen und Dokumente etwa im PDF- oder Word-Format. Abschließend schickt er seine Funde an die Command-and-Control-Server seiner Gebieter.

Mitunter beobachten Experten Infostealer und Ransomware auch im Doppelpack. Ein aktuelles Beispiel: Die Interlock-Gang schleust im Zuge einer Ransomware-Infektion wahlweise Lumma oder den Stealer Berserk ein. Diese sammeln Login-Daten, um den Gangstern erweiterte Zugriffsrechte zu bescheren und ihnen den Weg durchs Netzwerk zu bahnen (Privilege Escalation, Lateral Movement). Das sind perfekte Voraussetzungen für die anschließende Erpressung.

Auch Infostealer bedrohen nicht nur Windows-Systeme. Derzeit versuchen sie auch verstärkt, sich auf Macs breitzumachen. So verbarg etwa im Juni dieses Jahres eine speziell präparierte Website entsprechenden Schadcode hinter angeblichen Tipps zum macOS-Troubleshooting. Und auch im mobilen Bereich dominiert Malware, die es auf wertvolle Informationen abgesehen hat: Laut Analysten von G Data sind Trojaner, die Online-Bankingdaten ausspähen, weiterhin die verbreitetste Bedrohung auf Android-Smartphones.

Zum Schutz vor Informationsdiebstahl sollte man einen mit einem starken Masterpasswort abgesicherten Passwortmanager nutzen und keinesfalls Kennwörter unverschlüsselt im Webbrowser speichern. Multifaktor-Authentifizierung (MFA) sorgt für zusätzliche Sicherheit.

IoT-Geräte als Propaganda-Kanal

Neben finanziell motivierten spielen auch immer wieder politisch motivierte Angriffe eine tragende Rolle in der Bedrohungslandschaft – oft in Gestalt sogenannter Distributed-Denial-of-Service-Angriffe (DDoS).In den vergangenen Monaten legten Gruppen wie etwa die prorussische Gang „NoName-057(16)“ vielfach Websites von Unternehmen und Behörden auch in Deutschland zeitweise lahm.

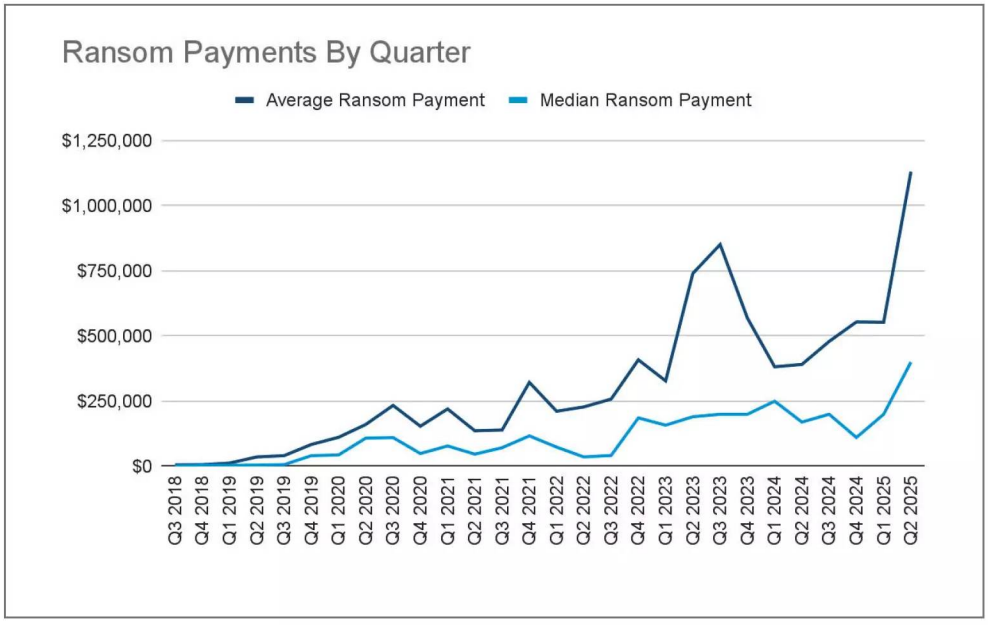
Das Unternehmen Link11, Anbieter von DDoS-Schutzlösungen, sieht vor dem Hintergrund geopolitischer Konflikte ein steigendes Risiko auch für Privatpersonen in Deutschland. Denn häufig setzen die Angreifer auf Botnetz-Strukturen aus infizierten PCs, IoT- und anderen Endgeräten.

„Im ersten Halbjahr 2025 haben wir im Vergleich zu den Vorjahreszahlen eine Zunahme der DDoS-Angriffe auf Ziele in der DACH-Region im Link11-Netzwerk verzeichnen können“, teilte ein Sprecher gegenüber c’t mit. In diesem Zuge habe sich auch die Verbreitung Botnetz-bildender Malware über IoT-Geräte wie Router, Kameras und Smart-TVs weiter beschleunigt. Neben dem Missbrauch für DDoS-Attacken seien mittels modularer Malware etwa auch Klickbetrug oder Account-Takeover-Angriffe, also massenhafte automatisierte Login-Versuche möglich.

Generell gilt: „Smarte“ Geräte sollte man immer auf dem aktuellen Stand halten und Billigprodukte lieber meiden – denn häufig bekommen die keine Updates. Im Zweifel ist es besser, unsichere Produkte zu entsorgen oder sie zumindest vom Netz zu nehmen“.

Phishing nimmt zu

Bevor erpresserischer, datenklauender oder sonstiger Schadcode Systeme infizieren kann, muss er erst einmal dorthin gelangen. Häufig geschieht dies im Zuge einer Phishing-Kampagne: Laut Bundeskrimi-



Bildquelle: Coveware

Die Höhe der Lösegeldzahlungen bei Ransomware-Erpressungen steigt seit Jahren – und hat unlängst einen großen Satz nach oben gemacht.

nalamt (BKA) ist das Aufkommen registrierter Phishing-Mails 2024 gegenüber 2023 um fast 70 Prozent gestiegen.

Dabei bezieht sich das BKA auf Zahlen der Verbraucherzentrale Nordrhein-Westfalen. Die betreibt einen „Phishing-Radar“, an den Betroffene im vergangenen Jahr insgesamt 424.328 Phishing-Mails weiterleiteten. Das Angriffsniveau sei auch im ersten Halbjahr 2025 hoch geblieben, teilte die Verbraucherzentrale auf Nachfrage von c’t mit: knapp 205.000 Mails seien bislang eingegangen.

Natürlich hat längst nicht jede Phishing-Kampagne das unmittelbare Ziel, Schadcode auszuliefern. Doch nicht selten dient etwa das Einsammeln von Zugangsdaten über eine in der Mail verlinkte Phishingsite späteren Malware-Angriffen. Die Sites seien zunehmend kurzlebig und enthielten bewusst wenige Elemente, berichtet ein Experte des Unternehmens OPSWAT gegenüber c’t. Die Angreifer versuchten damit, klassische Reputationsfilter auszutricksen – Schutzmechanismen, die die Seriosität von Websites bewerten sollen.

Für Endnutzer bedeutet das, dass sie noch aufmerksamer gegenüber vermeintlich seriösen Mails etwa von Kreditinstituten, Zahlungsdienstleistern oder Onlinehändlern sein sollten. Im Zweifel lohnt es sich, telefonisch nachzuhaken, statt vorschnell auf verdächtige Links zu klicken oder gar persönliche Daten einzugeben.

Einen Überblick über aktuelle Phishing-Kampagnen bietet die Verbraucherzentrale NRW auf ihrer Website. Dort finden Sie bei Bedarf auch die E-Mail-Adresse für die Weiterleitung von Verdachtsfällen an den Phishing-Radar.

ClickFix: Erst denken, dann (nicht) klicken

Erhöhte Vorsicht ist auch gegenüber anderen Betrugsmaschen geboten, die darauf bauen, das Vertrauen potenzieller Opfer zu erschleichen. Sicherheitsforscher beobachten derzeit eine starke Zunahme von Social-Engineering-Angriffen. Besonders verbreitet ist dabei die sogenannte „ClickFix“-Masche. Dabei sollen Nutzer unter einem Vorwand davon überzeugt werden, auf Websites Interaktionen auszuführen, die in Wirklichkeit eine Schadcode-Ausführung auf dem betreffenden System zur Folge haben.

Häufig passiert das im Kontext eines gefälschten Captchas: Website-Besucher sollen zum Beweis ihres „Menschseins“ beispielsweise bestimmte Tastenkombinationen eingeben. Statt einer Authentifizie-

rung kopieren sie dabei unbewusst Code in ihre Zwischenablage, starten diesen etwa über den „Ausführen“-Dialog von Windows – und holen sich letzten Endes aktiv Lumma, Qakbot oder anderen Schadcode auf ihre Systeme. Auch von dieser Masche sind neben Windows- derzeit häufig auch macOS-Systeme betroffen.

Wer einschlägige Tastenkombinationen wie etwa „Win+R“ oder „Strg+V“ kennt, kann den Betrug leicht durchschauen. Zudem hilft auch schon eine gewisse Skepsis gegenüber ungewöhnlichen Captcha-Modellen.

Aktuelle KI-Trends

Während KI-generierter Schadcode weiterhin eine Randerscheinung darstellt und sich meist auf einfache Skripte beschränkt, sehen Experten im Bereich des Social Engineering eine deutliche Bedrohungszunahme der KI-Nutzung.

Mit selbstlernenden Sprachmodellen (LLM) wie ChatGPT lassen sich Angriffe teilweise automatisieren, was Kriminellen Zeitaufwand erspart. Unter anderem lassen sie darüber Inhalte für vermeintlich vertrauenswürdige Websites generieren, um diese dann zur Schadcode-Verbreitung zu nutzen. Ebenfalls brandgefährlich: KI-gestützte Phishing-Kampagnen, die den Schreibstil eines Vorgesetzten zu imitieren versuchen. Oder im Zuge eines Vishing-Angriffs (Voice Phishing) dessen Stimme.

Im Mai dieses Jahres waren mutmaßlich KI-generierte Videos Teil einer Social-Engineering-Kampagne via TikTok. Die kurzen Clips sollten angeblich Schritte zur Aktivierung gecrackter Software oder zur Freischaltung von Premium-Funktionen vorführen. In Wirklichkeit handelte es sich auch hier um eine ClickFix-Variante: Wer der Anleitung folgte, führte PowerShell-Befehle aus und fing sich als „Belohnung“ einen Infostealer ein.

Das Beispiel ist nur eines von vielen aus den vergangenen Monaten, in deren Rahmen soziale Medien zum Angriffsvektor wurden – ein Ort, an dem viele Nutzer besonders empfänglich für Social-Engineering-Taktiken sind.

Im Notfall hilft Desinfec’t

Mit unseren Tipps und einer gesunden Portion Misstrauen gegenüber potenziellen Social-Engineering-Versuchen sind Sie schon recht gut gegen aktuelle Bedrohungen gewappnet. Unverzichtbar sind außerdem regelmäßige Sicherheitsupdates - denn auch Softwareschwachstellen zählen weiterhin zu den wichtigsten Einfallstoren der Angreifer.

Vor allem auf Windows-PCs sollte immer ein Virenschutz laufen. Sofern man die Signaturen aktuell hält, bietet der standardmäßig aktive Defender schon einen ausreichenden Grundschutz.

Falls es dennoch einmal zum erfolgreichen Angriff kommen sollte, hilft Desinfec’t, private PCs wie auch Firmenrechner zu bereinigen. Das Live-System startet direkt vom USB-Stick, spürt Malware auf Windows-Rechnern mithilfe mehrerer AV-Scanner auf und bringt Ihre persönlichen Daten in Sicherheit. Außerdem bringt es mehrere Expertentools zur Malwareanalyse mit. (des) c't

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

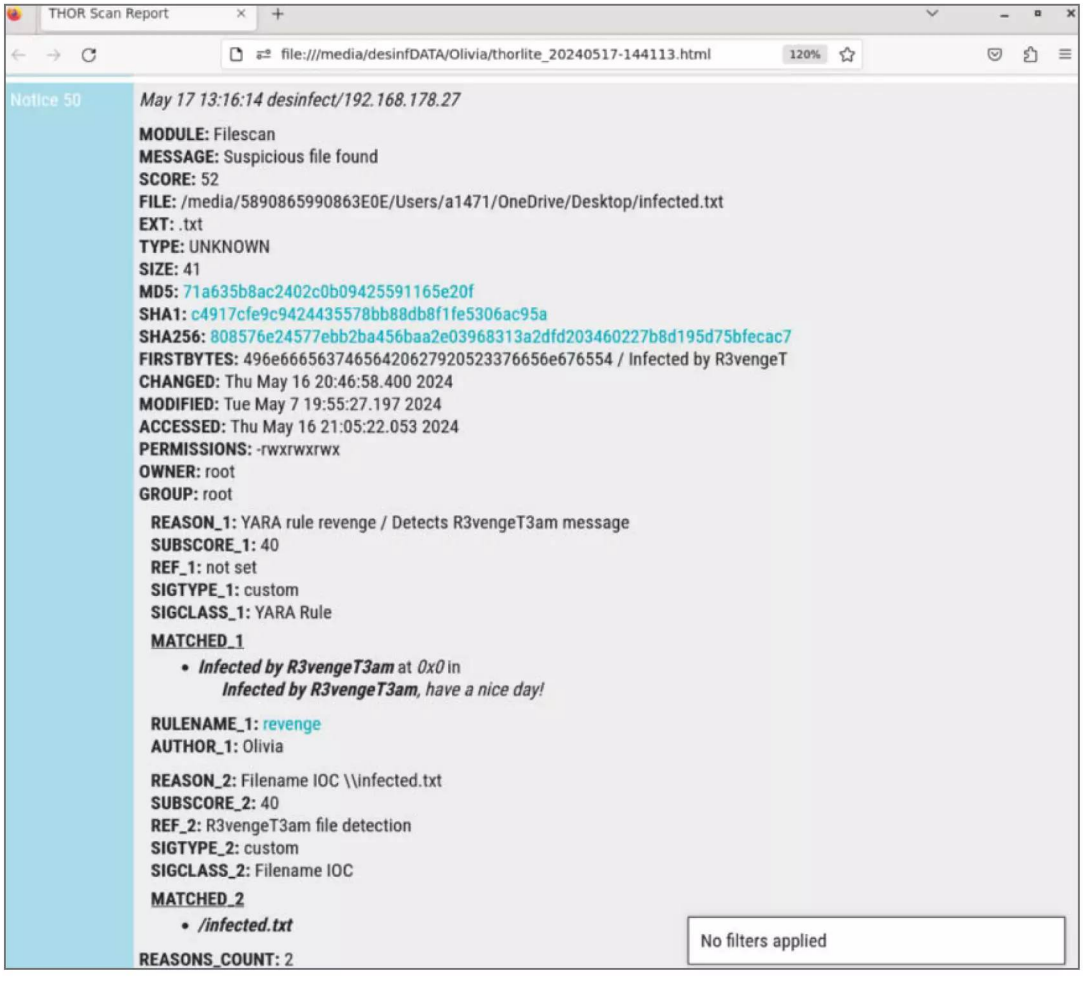
Nach mehrstufigen Hackerangriffen wie auch bei Infektionen mit komplexer, tief im System verborgener Malware ist die Sachlage oft erst einmal undurchsichtig. „Was ist überhaupt passiert?“, lautet die initiale Frage, bei deren Klärung Thor Lite helfen kann.

Beim Scannen stehen eine Vielzahl potenzieller Einbruchsspuren, sogenannter Kompromittierungsindikatoren (Indicators of Compromise, IoCs) auf der

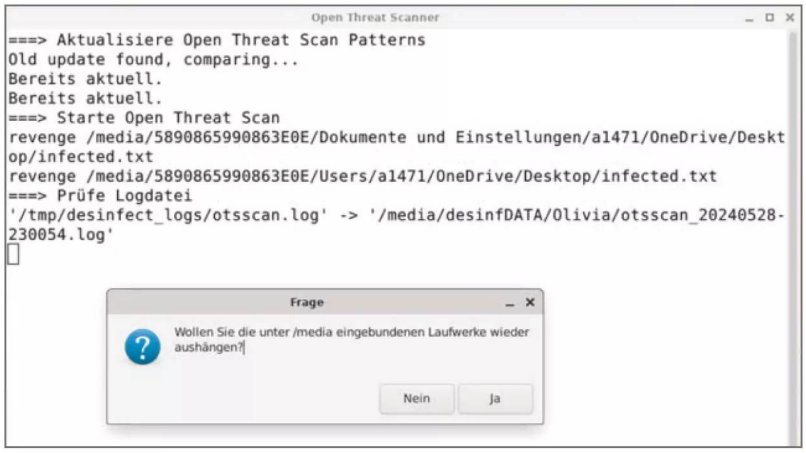
Fahndungsliste des Werkzeugs. Das können etwa verdächtige IP-Adressen, bestimmte Dateinamen oder Strings wie im „R3vengeT3am“-Beispiel sein. Zudem erkennt Thor Lite von Haus aus zahlreiche Hackertools, die als potenzielle Angriffswerkzeuge nur bedingt die Aufmerksamkeit klassischer AV-Scanner erregen.

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
```

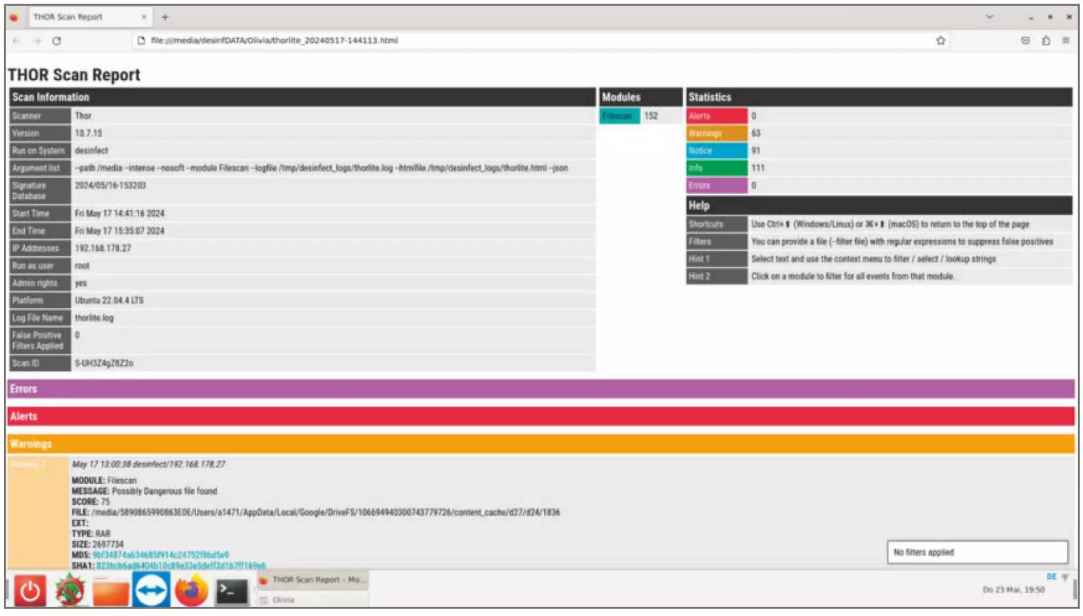
Thor Lites Filename-IoC-Dateien arbeiten mit regulären Ausdrücken. Wer sich damit auskennt, kann unter anderem zu berücksichtigende Pfade eingrenzen oder Dateien finden, deren Namensgebung in Teilen variieren. Dies ist keine Seltenheit bei Schadcode, der zur Laufzeit extrahierte Komponenten vor Scanprozessen 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.

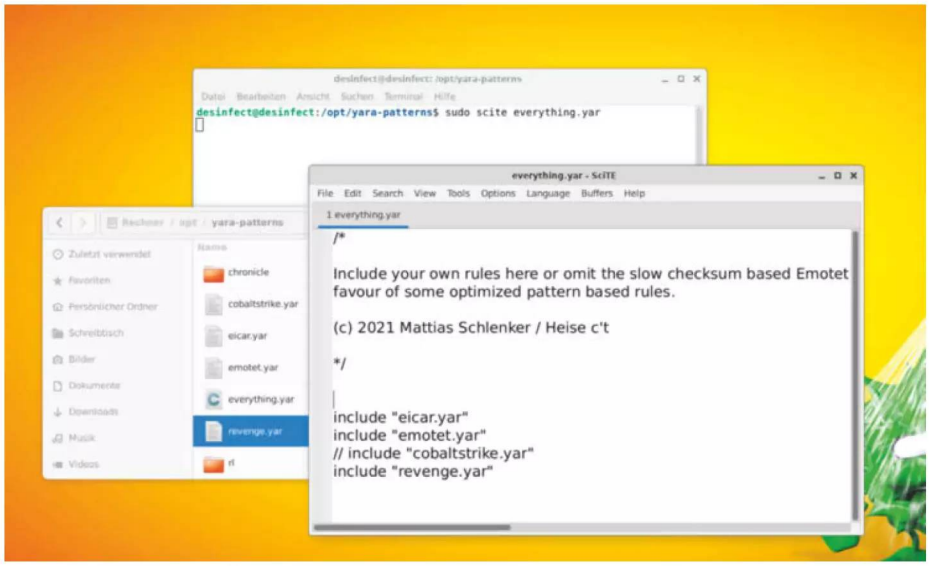
Einbruchsspuren aufgeschlüsselt

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

WIR TEILEN KEIN HALBWISSEN.
WIR SCHAFFEN FACHWISSEN.

Webinar · 16. Oktober

Wärmepumpentechnik für Einsteiger

Wir erklären die Arbeitsweise der verschiedenen Wärmepumpen-Typen und liefern Anhaltspunkte für eine erste Machbarkeitsabschätzung in der eigenen Immobilie.

Webinar · 21. Oktober

Sicher online bezahlen

Das Webinar stellt praxisnah verschiedene gängige Angriffe auf Onlinebanking und digitale Zahlungsmittel wie Kreditkarten vor.

Webinar · 6. November

Sprach-KI produktiv einsetzen

c't-Redakteure geben einen Überblick über die gängigen Sprachmodelle. Sie erläutern Kosten, Ressourcenbedarf und Einsatzmöglichkeiten.

Workshop · 3. Dezember

Microsoft 365 im Griff: Teams & Tools produktiv im Team einsetzen

Sie entwickeln praxisnahe Strukturen für eine konsistente, teamorientierte Nutzung. Im Mittelpunkt steht nicht die Technik, sondern die Zusammenarbeit.

Mehr anzeigen ▲

heise.de/ct/Events

Malware-Analysetools für Profis

Zusätzliche mächtige und vielseitige Werkzeuge in Desinfec't 2025/26 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 2025/26 bringt im „Expertentools"-Ordner auf dem Desktop hilfreiche Profitools zur tiefgehenden Malwareanalyse verdächtiger Dateien

mit. 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.

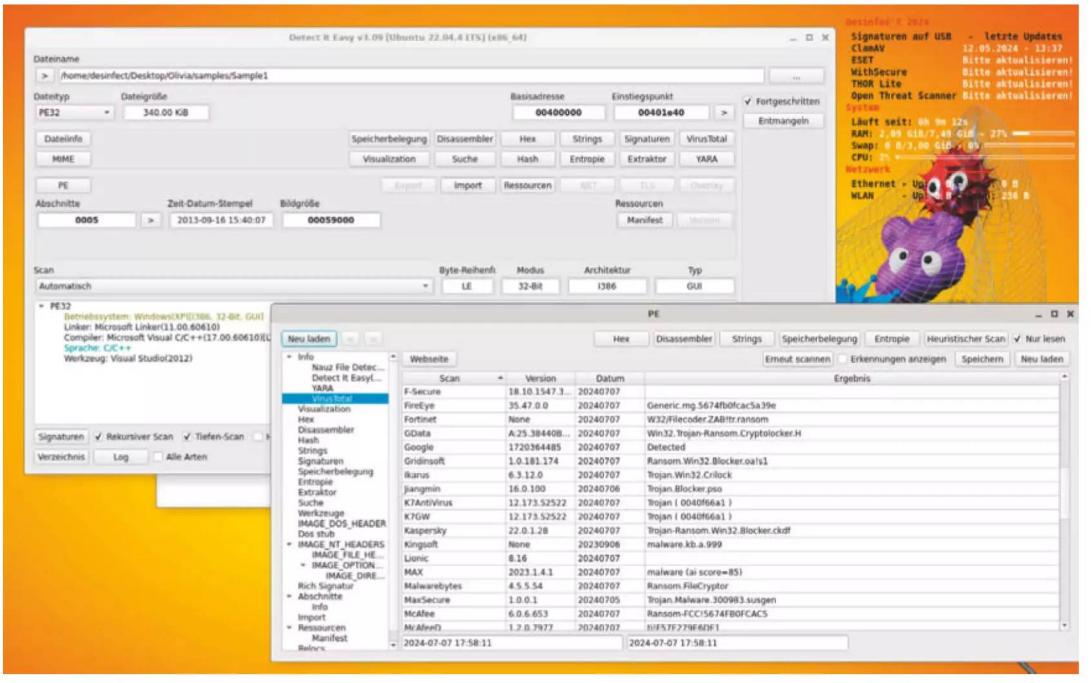
Für den Fall, dass Sie grundsätzlich lieber auf der Kommandozeile arbeiten, finden Sie die benötigten Befehle für die anderen Tools ebenfalls in diesem Artikel. Dabei gehen wir der Einfachheit halber jeweils davon aus, dass das Terminal bereits im Verzeichnis mit den Samples geöffnet wurde. Ansonsten 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 Bilddateien, Skripte und vieles mehr.

Malware-Tools in Desinfec't 2025/26

- 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.

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

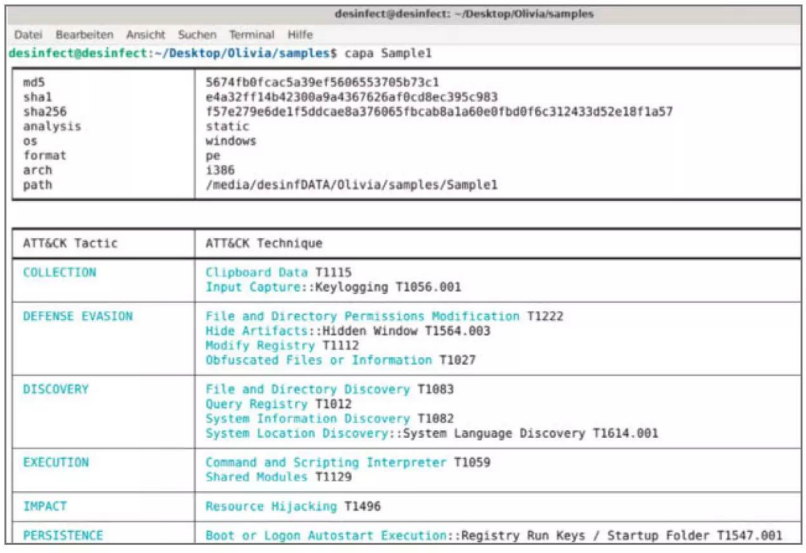
Auch Capa kann Experten bei der Analyse ausführbarer Windows-Dateien ein großes Stück Arbeit abnehmen – allerdings auf abstrakterer Ebene. Das wie FLOSS vom Mandiant-Team entwickelte Tool bestimmt im Rahmen eines Scans die spezifischen Fähigkeiten (Capabilities) einer Malware. Es kann beispielsweise 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



```
desinfect@desinfect: ~/Desktop/Olivia/samples
Datei  Bearbeiten  Ansicht  Suchen  Terminal  Hilfe
desinfect@desinfect:~/Desktop/Olivia/samples$ capa Sample1
```

md5	5674fb0fcac5a39ef5606553705b73c1
sha1	e4a32ff14b42300a9a4367626af0cd8ec395c983
sha256	f57e279e6de1f5ddcae8a376065fbcab8a1a60e0fbd0f6c312433d52e18f1a57
analysis	static
os	windows
format	pe
arch	i386
path	/media/desinfDATA/Olivia/samples/Sample1

ATT&CK Tactic	ATT&CK Technique
COLLECTION	Clipboard Data T1115 Input Capture::Keylogging T1056.001
DEFENSE EVASION	File and Directory Permissions Modification T1222 Hide Artifacts::Hidden Window T1564.003 Modify Registry T1112 Obfuscated Files or Information T1027
DISCOVERY	File and Directory Discovery T1083 Query Registry T1012 System Information Discovery T1082 System Location Discovery::System Language Discovery T1614.001
EXECUTION	Command and Scripting Interpreter T1059 Shared Modules T1129
IMPACT	Resource Hijacking T1496
PERSISTENCE	Boot or Logon Autostart Execution::Registry Run Keys / Startup Folder T1547.001

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.

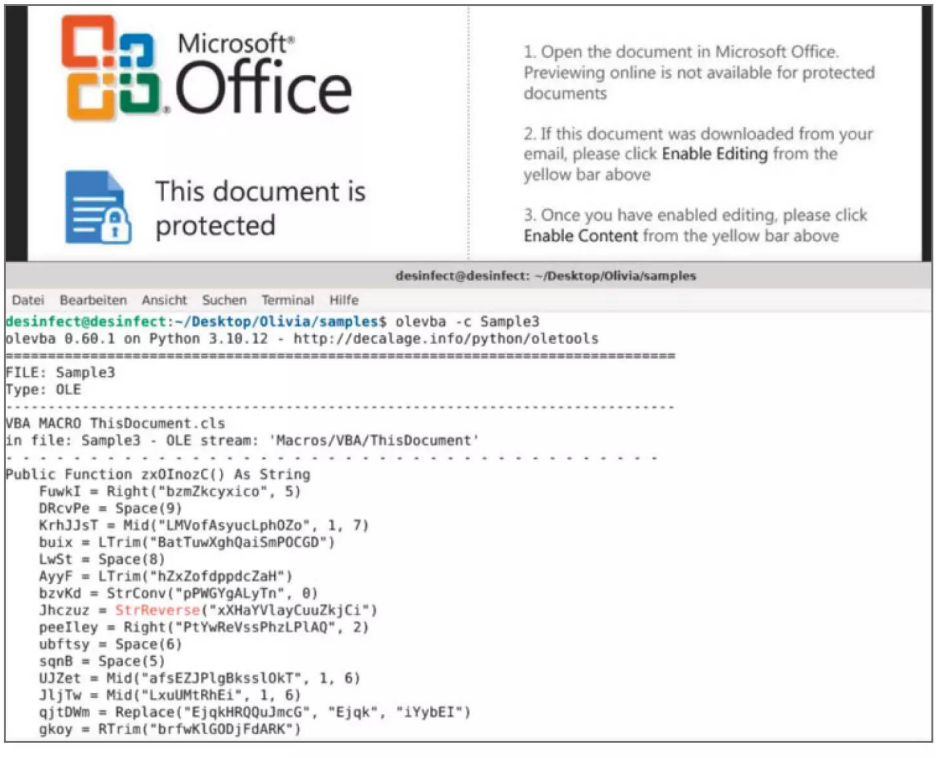
Um den Verdacht zu bestätigen, rufen Sie die oletools-Komponente „oleid“ auf: `oleid Sample3`. Oleid untersucht das Format des Word-Dokuments – in diesem Fall „MS Word 97-2003 Document or template“ – und schätzt das Risiko anhand verschiedener Kriterien wie etwa vorhandener Verschlüsselung und enthaltener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

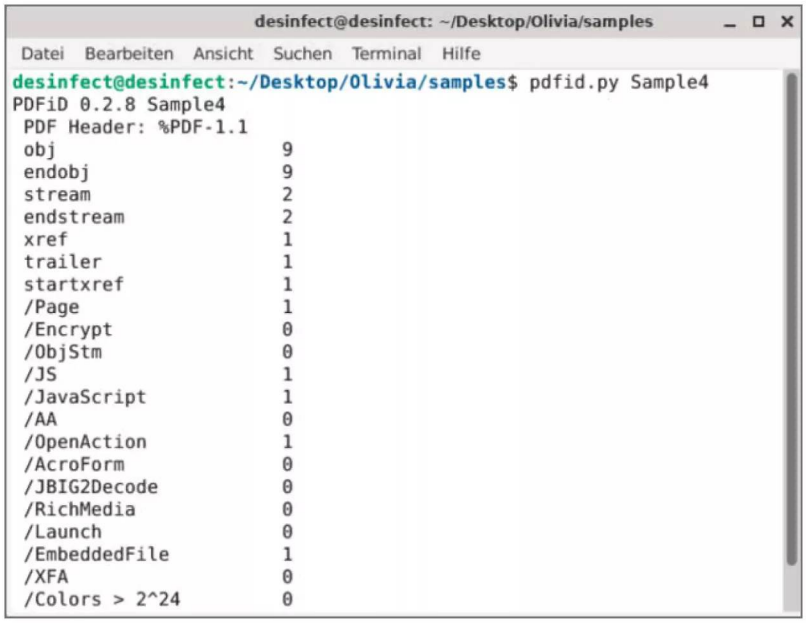
Auch mraptor hält den Makro-Code für verdächtig, nachdem es ihn mithilfe von Keywords unter die Lupe genommen hat. Offenbar wird er beim Öffnen des Word-Dokuments automatisch gestartet und führt anschließend Dateien oder Befehle außerhalb des VBA-Kontexts aus.

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:

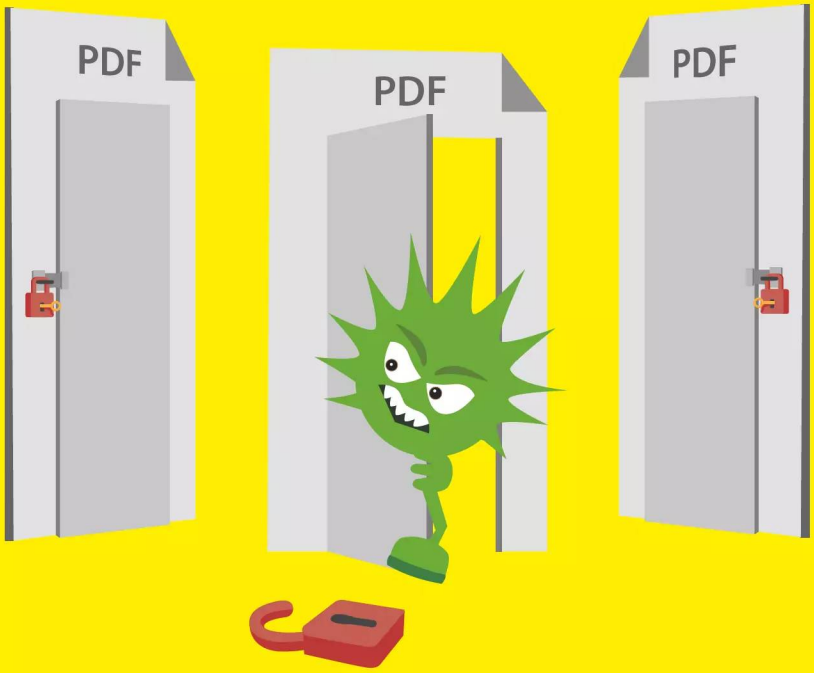
```
this.exportDataObject({cName: ↵
↳"eicar-dropper.doc", nLaunch: 2});
```

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 Expertentools zur Malware-Analyse 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



PDF-Dokumente mit QPDF entschlüsseln

Viele Malware-Analysewerkzeuge kapitulieren vor passwortgeschützten PDFs. Der Desinfec't-Neuzugang QPDF räumt dieses Hindernis mit wenigen Handgriffen aus dem Weg.

Von **Olivia von Westernhagen**

Um im Rahmen von Phishing-Kampagnen Empfänger, Spamfilter und Antivirensoftware gleichermaßen auszutricksen, müssen sich Cybergangster stetig etwas Neues einfallen lassen. Folgerichtig beobachteten Sicherheitsforscher auch in den vergangenen Monaten wieder clevere Kombinationen verschiedener Verschleierungstechniken, in denen präparierte PDF-Dokumente als Köder dienen. Zum Beispiel können PDFs mit einem Zugangsschutz versehen werden, der nicht nur für Malware-Analysten ein Ärgernis darstellt. Wir beschreiben, wie man den erkennt und in vielen Fällen dann auch entfernen kann, um das Dokument danach untersuchen zu können oder es wie gewohnt zu benutzen.

In aktuellen Cybercrime-Fällen tarnten Angreifer Links zu Phishing-Websites als QR-Codes („Quishing“)

und versteckten diese in passwortgeschützten PDF-Dateien. Als vermeintliche Hotelrechnungen oder Geschäftsberichte verschickten sie die Dokumente anschließend per E-Mail. Das benötigte PDF-Passwort fügten sie als Bild in die Nachricht ein – lesbar für Menschen, nicht aber ohne Weiteres für automatische Erkennungsmechanismen.

Geschützte PDFs analysieren

Ein solcher Passwortschutz schlägt mehrere Fliegen mit einer Klappe: Während er beim Empfänger den Anschein von Vertraulichkeit und Seriosität erweckt, erhöht die mit ihm einhergehende Dokumentverschlüsselung zugleich die Wahrscheinlichkeit, dass Schutzlösungen scheitern und die gefährliche Mail ungehindert ihr Ziel erreicht. Auch Werkzeuge zur manuellen Schadcode-Analyse werden von verschlüsselten PDFs auf eine harte Probe gestellt: Sie spucken Kauderwelsch aus oder kapitulieren gar vollständig.

Seit Desinfec't 2024/25 hat das Livesystem eine Ergänzung des Profi-Werkzeugkastens im Gepäck, mit dem die Analyse trotzdem gelingt: QPDF. Eigentlich dient das Tool primär zur Bearbeitung von PDF-Dateien. Doch da man damit auch PDFs entschlüsseln kann, ermöglicht QPDF eine Analyse durch verschiedene in Desinfec't enthaltene Expertentools wie pdfid.py zum Untersuchen von PDF-Dateien. QPDF funktioniert übrigens auch mit anderen Linux-Distributionen und unter Windows.

Dieser Artikel erklärt die Verwendung von QPDF anhand konkreter Beispieldateien (Download siehe ct.de/wcn8) und geht kurz auf das Herausfinden beziehungsweise Knacken verloren gegangener PDF-Passwörter ein. Außerdem erläutert er in Grundzügen, wie Sie die QPDF-Funktionen mit bereits in Desinfec't vorhandenen Profiwerkzeugen kombinieren können (siehe Seite 40). So spüren Sie etwa Schadcode oder Phishing-Links in Dokumenten auf.

Gefahrlos ausprobieren

Wie die übrigen Tools im Profi-Werkzeugkasten des Livesystems richtet sich QPDF primär an fachkundige Experten, die etwa im Zuge einer Incident Response Verdachtsfälle einkreisen und anschließend eingehend untersuchen wollen. Doch im Unterschied zu manch anderen Expertentools in Desinfec't kann die unsachgemäße Nutzung des PDF-Tools keinen Schaden auf dem System anrichten; somit können auch Laien gefahrlos mit QPDF experimentieren. Wohl aber könnten Dokumente beim Herumprobieren kaputt gehen. Nutzen Sie dafür dementsprechend keine wichtigen PDF-Dateien und wenn doch, lieber ausschließlich Kopien.

Entsprechend einsteigerfreundlich sind auch die von uns gewählten Beispiele: zwei PDFs identischen, harmlosen Inhalts mit unterschiedlichem Passwortschutz. Da die Dokumente statt Malware nur Bild und Text enthalten, können Sie sie bedenkenlos auch außerhalb von Desinfec't herunterladen. Damit die Dateien unter Desinfec't einen Neustart überleben, müssen Sie die Dateien im persistenten Projektordner speichern.

Verschlüsselung erkennen

Dass es sich bei unseren Beispielen um passwortgeschützte Dokumente handelt, wissen Sie bereits. Sieht man sich jedoch in der Realität mit einem verschlüsselten PDF konfrontiert, muss man erst einmal zu dieser Erkenntnis gelangen: Schließlich gehört ein Doppelklick auf das potenziell gefährliche Fundstück nicht gerade zu den Best Practices eines Schadcode-Analysten. Im Idealfall will man das sogar automatisiert entdecken können.

Doch wie erkennt man eigentlich verschlüsselte PDFs? In Desinfec't gelingt dies schnell und einfach mit dem enthaltenen Python-Skript pdfid.py von Didier Stevens: Es sucht nach bestimmten Strings, die formatbedingt häufig in PDF-Dokumenten vorkommen und die deren spezifische Eigenschaften beschreiben. Suchtreffer gibt pdfid.py auf der Kommandozeile zurück.

Navigieren Sie zum Ausprobieren in Ihren Desinfec't-Projektordner mit den heruntergeladenen und entpackten Beispielen. Öffnen Sie dort ein Terminalfenster und tippen Sie `pdfid.py Beispiel1.pdf` ein. Im konkreten Fall erkennt das Tool unter anderem, dass unser Beispiel eine Seite umfasst (`/Page 1`); vor allem aber bestätigt `/Encrypt 1` die vorhandene Verschlüsselung.

Dass diese tatsächlich ein Analysehindernis darstellt, verdeutlicht ein Aufruf des Allround-Analyse-Werkzeugs Qu1cksc0pe. Das Kommandozeilentool kann neben anderen Formaten auch die Struktur von PDF-Dateien unter die Lupe nehmen, sie nach verdächtigen URLs durchsuchen und anhand von YARA-Regeln als schädlich identifizieren. Geben Sie dafür im bereits für pdfid verwendeten Terminalfenster folgenden Befehl ein:

```
qu1cksc0pe --file Beispiel1.pdf --docs
```

Erwartungsgemäß gibt Qu1cksc0pe eine Fehlermeldung zurück: Es kann das PDF aufgrund der Verschlüsselung nicht analysieren. Abhilfe schafft im nächsten Schritt QPDF.

Showtime für QPDF

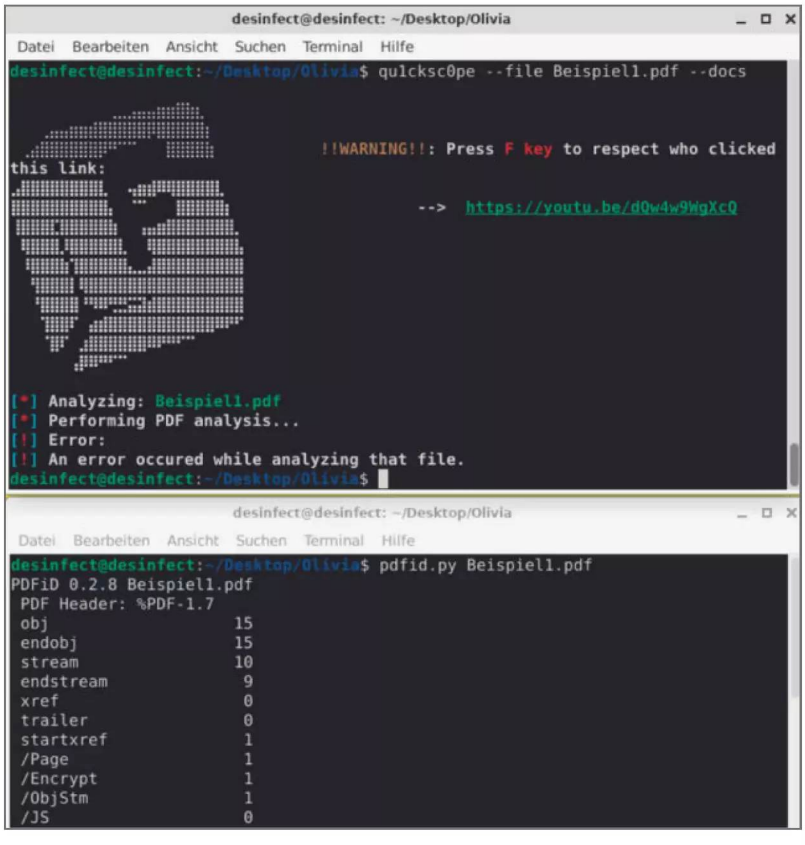
Wie die zuvor genannten Werkzeuge finden Sie auch QPDF im Expertentools-Ordner auf dem Desinfec't-Desktop. Ein Klick auf das entsprechende Icon öffnet ein Fenster mit der Hilfefunktion des Tools. Über die Kommandozeile starten Sie QPDF nebst Hilfe am bequemsten, indem Sie direkt in das Verzeichnis mit den Beispiel-PDFs navigieren, dort ein Terminalfenster öffnen und `qpdf --help` eintippen. Auf diese Weise erübrigen sich Pfadangaben zu den Ordnern und Dateien, die Sie scannen möchten.

Dass QPDF nicht primär der Malware-Analyse dient, sondern vor allem sehr vielfältige Funktionen zur PDF-Bearbeitung bereitstellt, verdeutlichen die zahlreichen in der Hilfe aufgelisteten Befehle. Diese Optionen reichen vom Hinzufügen oder Entfernen von PDF-Seiten und -Overlays über Rotationsmöglichkeiten, Linearisierung bis hin zur aufwendigen Verschlüsselung.

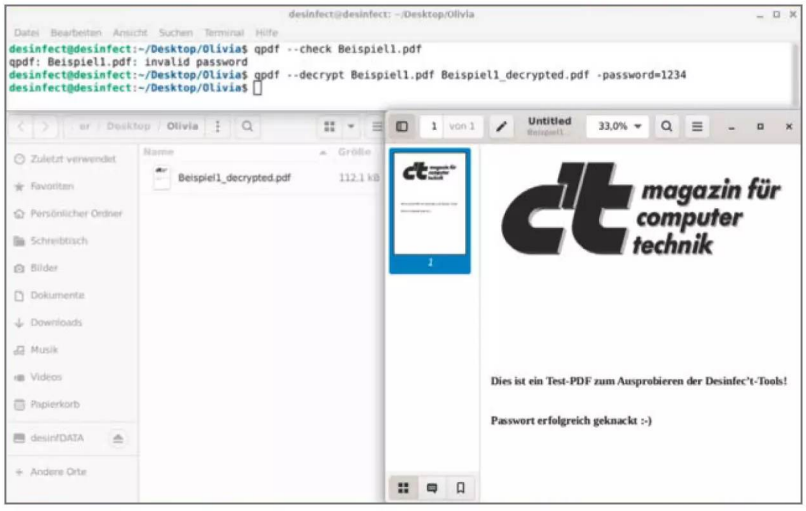
Im Rahmen dieses Artikels nutzen wir das Werkzeug, um Informationen zur bereits vorhandenen Verschlüsselung zu sammeln und diese anschließend aufzuheben. Schritt eins übernimmt die Befehlszeile `qpdf --check Beispiel1.pdf`.

Die Rückgabe `Beispiel1.pdf: invalid password` gibt Ihnen auf etwas umständliche Art zu verstehen, dass Sie zum Entsperren ein Passwort eingeben müssen. Unsere Beispieldateien haben wir der Einfachheit halber mit dem Kennwort „1234“ geschützt.

Mit dem folgenden Befehl übergeben Sie das Passwort an QPDF und speichern zugleich eine entschlüsselte PDF-Kopie im aktuellen Verzeichnis:



Qu1cksc0pe (oben) scheitert an der Analyse des ersten Beispiels. Das Analysetool pdfid.py (unten) erkennt den Grund: die Verschlüsselung.



Nach der Passwortübergabe lässt sich unser Testdokument problemlos öffnen.

```
qpdf --decrypt Beispiel1.pdf ↵
↳Beispiel1_decrypted.pdf ↵
↳-password=1234
```

Geschafft: Das erste Beispiel ist entschlüsselt! Vom Erfolg können Sie sich überzeugen, indem Sie den „`--check`-Parameter, pdfid.py oder auch Qu1cksc0pe auf Beispiel1_decrypted.pdf loslassen. Die Resultate sind die Meldung `file is not encrypted` (QPDF), `/Encrypt 0`(pdfid) sowie ein problemloser Qu1cksc0pe-Scan.

User vs. Owner

Während der Sachverhalt bei Beispiel1.pdf recht klar ist, birgt Beispiel2.pdf ein Rätsel, das es zu knacken gilt. Zwar kann man das Dokument nämlich ohne jegliche Abfrage problemlos in Desinfec't's PDF-Viewer öffnen. Zugleich lassen Scans mit pdfid und Qu1cksc0pe aber dennoch auf eine Verschlüsselung schließen, die einer Analyse im Weg steht.

Wie passt das zusammen? Des Rätsels Lösung: Während Beispiel1.pdf mit einem sogenannten User- oder Document Open-Passwort vor dem unbefugten Öffnen geschützt ist, nutzt Beispiel2.pdf lediglich ein Owner-Passwort, auch Permissions-Passwort genannt. Das User-Passwort, das den Inhalt vor neugierigen Blicken schützt, ist also leer.

Die Owner-Passwort-Variante kann man in gängigen PDF-Programmen separat vergeben. Sie unterbindet nicht das Öffnen mit einem Viewer, sondern dient der Rechtebeschränkung zum Bearbeiten, Kopieren oder Drucken der Dokumentinhalte.

Technisch gesehen verwendet der PDF-Standard 2.0 eine symmetrische (AES-)Verschlüsselung, nutzt also zum Ver- und Entschlüsseln denselben Masterkey. Der steht nicht etwa im Klartext im Dokument, sondern wird seinerseits unter Verwendung der gesetzten User- und Owner-Passwörter – oder aber, wenn ein Passwort leer ist: mit Defaultwerten – verschlüsselt. In einem sogenannten Encryption Dictionary speichert das PDF je nach gesetzten Passwörtern eine oder mehrere Ciphertext-Varianten des Keys. Dort landen auch, ebenfalls aufwendig verschlüsselt, Informationen zum Rekonstruieren der Passwörter und zum Validieren von Passworteingaben durch die Nutzer.

Bei einem leeren User-Passwort benötigt das PDF-Programm zum Entschlüsseln keine Eingabe. Die Verschlüsselung wird beim Öffnen des Dokuments aufgehoben – und mit ihr die gesamte Schutzwirkung des Owner-Passworts. Mit dem nachfolgenden Befehl stellt das Tool den Vorgang des Öffnens – gefahrlos und ohne PDF-Anzeige – nach, um eine Kopie des entschlüsselten Dokuments zu erstellen:

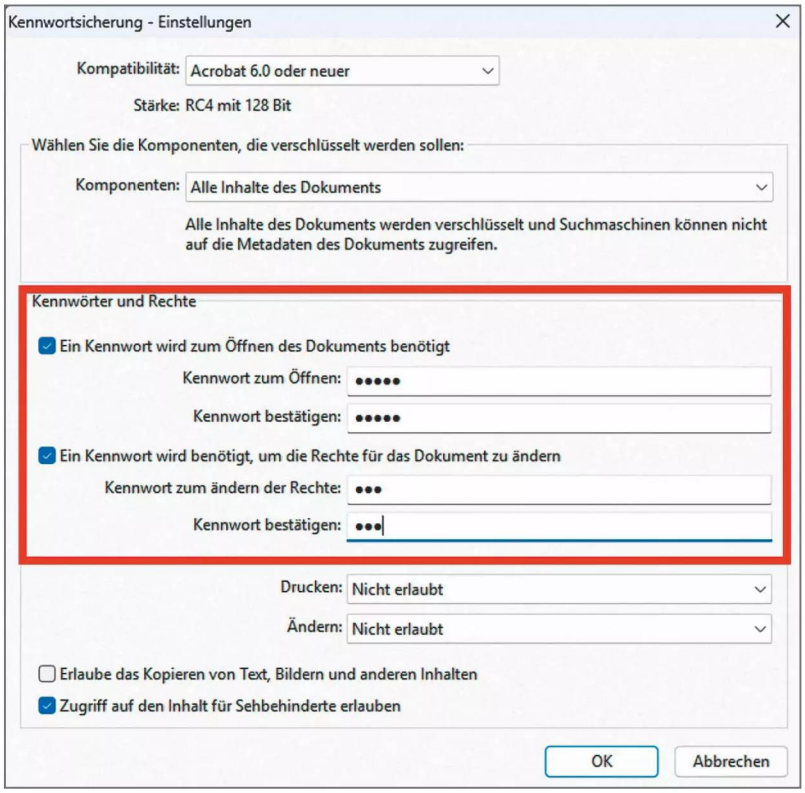
```
qpdf --decrypt Beispiel2.pdf ↵
↳Beispiel2_decrypted.pdf
```

„Ist das Owner-Passwort nicht eigentlich eine Farce, wenn man es so einfach aushebeln kann?“, könnte man nun fragen. Die Antwort lautet: „Ja“. In der PDF-Dateiformatspezifikation erläutert der Formatentwickler Adobe diesbezüglich: „Once the document has been opened and decrypted successfully, a conforming reader technically has access to the entire contents of the document.“

Das Owner-Passwort selbst besitzt also keinerlei Schutzwirkung, und es liegt in der Verantwortung der PDF-verarbeitenden Software, den vom Dokumentersteller beabsichtigten Zugriffsschutz umzusetzen. Salopp ausgedrückt pfeift QPDF auf diese Verantwortung und nutzt den unbeschränkten Zugriff zum Entfernen des Passworts.

User-Passwort ausgraben

Es kann vorkommen, dass User-Passwörter verdächtiger PDF-Dateien nicht mehr auffindbar sind. Etwa dann, wenn ein Mitarbeiter nach dem Öffnen des



Gängige PDF-Programme wie die Freeware PDF-Xchange Viewer erlauben die separate Vergabe von User- und Owner-Passwörtern.

heruntergeladenen Dokuments die Mail mit den zugehörigen Informationen in Panik gelöscht hat und sich partout nicht erinnern kann, was er eingegeben hat. Will man dennoch das Passwort oder zumindest mehr über den potenziell verursachten Schaden herausfinden, gibt es primär zwei Möglichkeiten: eine Online-Recherche oder den Versuch, das Passwort über ein Tool zu knacken.

Ein erfolgversprechender erster Schritt beim Nachforschen im Web besteht im Hochladen des PDFs zum Malware-Analysedienst VirusTotal. Aus dem Desinfec't-Kontext heraus können Sie den Upload beispielsweise via „Detect It Easy“ (DIE) anwerfen. Das per Doppelklick auf das entsprechende Icon im Expertentools-Ordner aufrufbare Werkzeug identifiziert neben vielen anderen Dateiformaten auch PDFs und liefert wertvolle statische Informationen zum Dokument. Der „VirusTotal“-Button befindet sich gut sichtbar auf der grafischen Oberfläche von DIE.

Basierend auf dem Datei-Hash überprüft der Service, ob das schädliche Dokument bereits bekannt und ein Online-Report verfügbar ist. Ist dies der Fall, so liefert der darin befindliche Reiter „Community“ oftmals Hintergrundinformationen, die bei der weiteren Recherche helfen können. Dazu gehören zum Beispiel Links zu Beschreibungen der betreffenden Schadcode-Kampagne oder der Name einer Cybercrime-Gruppe als Drahtzieher.

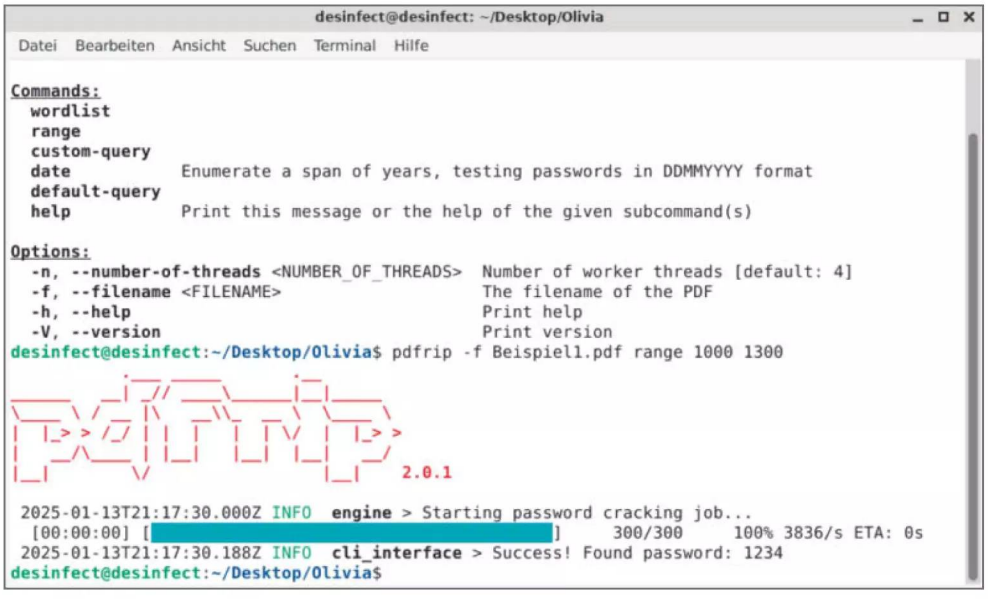
Eine vielversprechende Anlaufstelle zum anschließenden Weiterforschen ist die Malpedia des Fraunhofer-Instituts *(siehe ct.de/wcn8)*.

Bruteforce mit PDFRip

Wenn die Suche erfolglos bleibt, hilft möglicherweise PDFRip weiter (siehe ct.de/wcn8). Das quelloffene, kostenlose Kommandozeilentool versucht, verloren gegangene PDF-Passwörter per Bruteforce, also automatisiertem Durchprobieren, zu knacken.

PDFRip ist plattformübergreifend verwendbar: Der in der Readme.MD im GitHub-Repository gut erklärte Installationsvorgang klappte bei unserem

Bruteforce-Tool: PDFRip hilft im Notfall beim Knacken verlorener Passwörter.



kurzen Testlauf unter Windows wie auch Linux problemlos. Im Ubuntu-basierten Desinfec't ist PDFRip nicht vorinstalliert, bei akutem Bedarf jedoch – wenn auch nicht persistent – nachrüstbar. Hierfür installieren Sie zunächst die Programmiersprache Rust mittels folgenden Kommandozeilenbefehls:

```
curl --proto '=https' --tlsv1.2 -sSf ↵
↳https://sh.rustup.rs | sh
```

Wählen Sie im Terminal-Dialog die Standardinstallation. Danach folgt die eigentliche PDFRip-Installation mit Rusts Paketmanager cargo in einem neuen Terminal-fenster.

```
cargo install --git ↵
↳https://github.com/mufeedvh/↵
↳pdfrip.git
```

Der Aufruf pdfrip -h listet nun die verfügbaren Optionen auf; konkrete Anwendungsbeispiele liefert wiederum die Readme.MD. Die Kehrseite des Bruteforce-Ansatzes: Schon das Knacken eines alphanumerischen Passworts mit vier Stellen (`default-query -max-length 4`) kann bei nur durchschnittlich leistungsfähiger Hardware einige Stunden beanspruchen. Für längere Passwörter oder Ausgangssituationen, in denen man sich beispielsweise noch an die Struktur des Passworts erinnert, bietet PDFRip glücklicherweise passende Modi – etwa mit vorgefertigten Wortlisten, Jahreszahlen oder unter Vorgabe eines spezifischen Formats wie `DOC-ID{0-99}-FILE`.

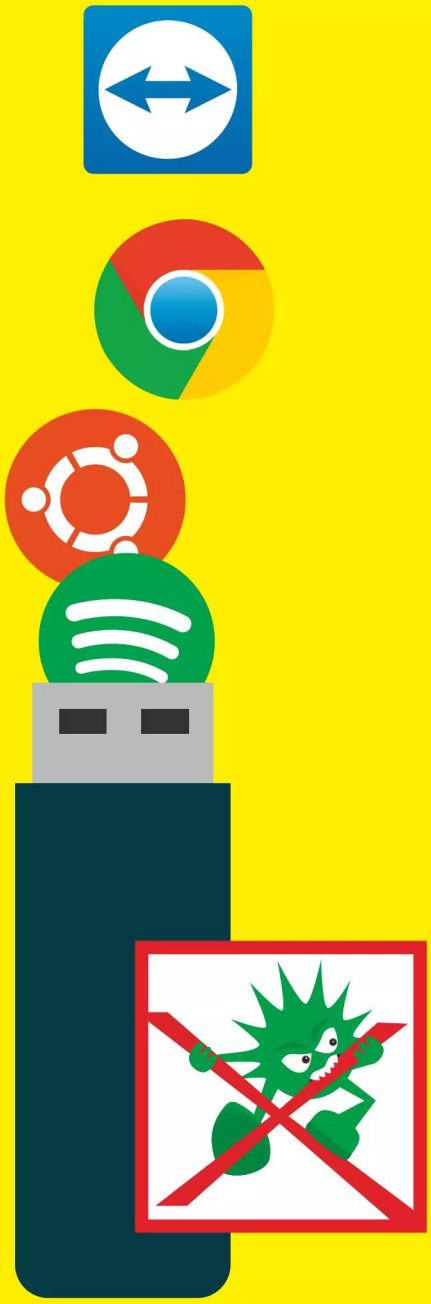
Ein extrem zeitsparender Bruteforce-Aufruf für Beispiel1.pdf, der lediglich alle Ziffernkombinationen von 1000 bis einschließlich 1300 durchprobiert, sieht folgendermaßen aus:

```
pdfrip -f Beispiel1.pdf range 1000 ↵
↳1300
```

Gut gerüstet loslegen

Mit QPDF, pdfid.py, Qu1cksc0pe und DIE steht Ihnen in Desinfec't eine leistungsfähige Toolkombination zur Verfügung, um PDFs und ihre Verschlüsselung initial zu identifizieren, zu entsperren und anschließend eingehend zu untersuchen. Das bis hierhin noch nicht genannte, ebenfalls von Didier Stevens stammende Skript pdf-parser.py – ebenfalls Bestandteil des Desinfec't-Arsenals – rundet die Sammlung ab, indem es etwa schädliche Skripte in PDF-Dokumenten aufzuspüren hilft.Eine Übersicht über alle Malwareanalysewerkzeuge nebst kurzer Beschreibungen zeigt die Textdatei 01_Tool_Liste_.txt im Expertentools-Ordner. (des) c't

Weiterführende Infos zu verwendeten Tools:
ct.de/wcn8



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.

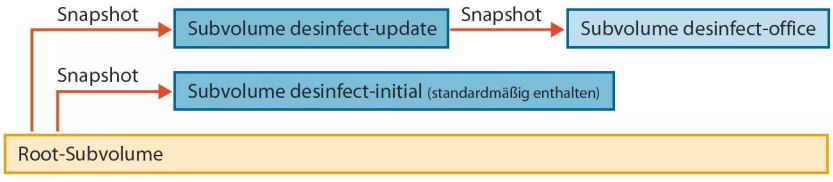
Los gehts!

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 2025/26 p1", hat es geklappt. Steht dort nur „Desinfec't 2025/26", 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:

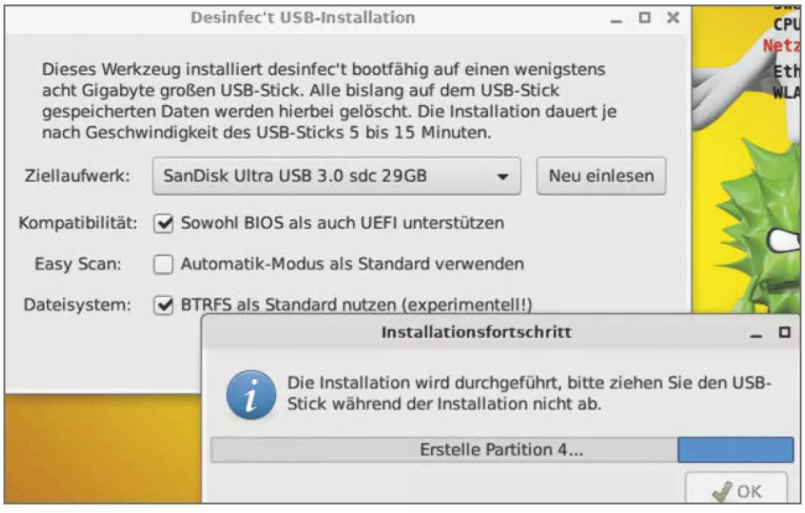
```
sudo chroot /cdrom/desinfect-update/↴
↳.casper/filesystem.dir
dpkg -i /var/cache/apt/archives/↴
↳.desinfect-meta*.deb
```

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 Anwen-

dungen 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 wechseln

Desinfec't, Btrfs und Windows

Bei Desinfec't 2025/26 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 2025/26 arbeitet mit versteckten Partitionen. Bisher konnten wir dieses Schema allerdings nicht für einen Btrfs-Stick anwenden – aber wir arbeiten daran.

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

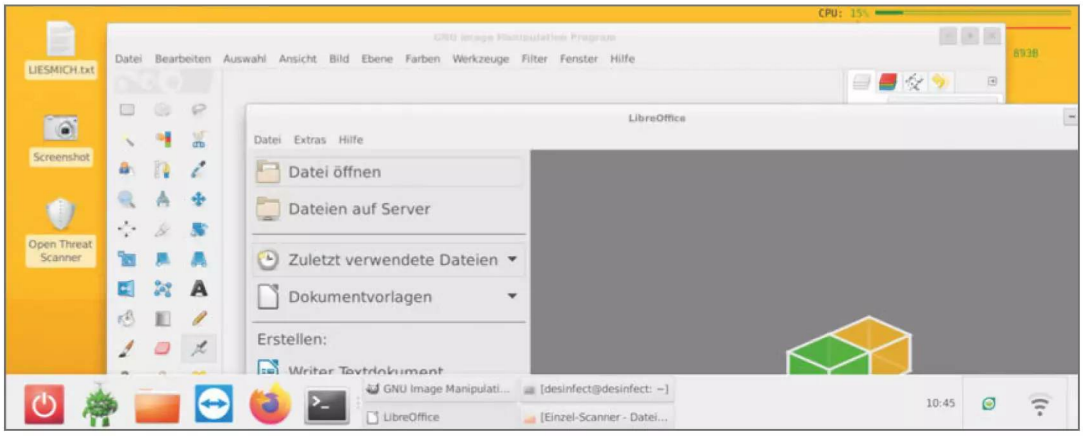
```
sudo rm $CHROOT/usr/sbin/policy-rc.d
```

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 6.16 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

Superschnelles Desinfec‘t dank USB-SSD

Ein USB-Stick mit Desinfec’t gehört schon lange an den Schlüsselbund jedes Admins. Doch von einer USB-SSD läuft Desinfec’t noch flüssiger und verlässlicher. Mit ein wenig Vorbereitung geht so eine Installation schnell von der Hand. Ein erster Ausblick.

Von **Mattias Schlenker**

Erinnern Sie sich noch, als Desinfec’t 2011 erstmals auf einer DVD dem Heft beilag? Seitdem konnte man das c’t-Sicherheitstool auch auf einem USB-Stick installieren.

Ab sofort gibt es eine neue Option für Experimentierfreudige: Installieren Sie Desinfec’t auf einer USB-SSD und profitieren Sie so von essenziellen Vorteilen. Dieses Projekt ist aber bislang nicht final. Auch die zur Installation nötige Prozedur wird sich noch vereinfachen. Dieser Artikel gibt einen Einblick in die Zukunft von Desinfec’t.

SSD statt Stick

USB-Sticks bieten zwar reichlich Speicherplatz zu überschaubaren Preisen und dank kompakter Ge-

häuse hat man sie immer in der Hosentasche dabei. Doch es fehlen Funktionen von SSDs wie das Wear-Leveling oder die Trim-Unterstützung zur Verlängerung der Lebensdauer von Flash-Speichern. Dazu kommen oft noch unterirdische Lese- und Schreibgeschwindigkeiten. Spätestens einmalig komplett überschriebene Sticks bringen selten mehr als 10 Megabyte pro Sekunde. Damit dauert das Laden großer Signaturbestände der Virenscanner gefühlt ewig.

SSDs unterstützen dagegen die lebensverlängernden Maßnahmen für Flash-Speicher und außerdem sind sie im Vergleich zu Sticks pfeilschnell. Für Desinfec't eignen sich neben SATA- auch NVME-Modelle. Damit Desinfec't von allen Vorzügen profitiert, empfehlen wir eine SSD mit mindestens 120 Gigabyte Speicherplatz. So ein SATA-Modell ist neu schon ab 10 Euro erhältlich. Bitte beachten Sie, dass der Datenträger für die Installation komplett gelöscht werden muss. Im Anschluss können Sie wieder Daten darauf speichern.

Für den Umzug benötigen Sie außerdem ein passendes SSD-USB-Gehäuse, das schlägt typischerweise mit 5 bis 15 Euro zu Buche. Obacht: Sehr günstige Platinen unterstützen oft die SMART-Funktion zur Überwachung des Flash-Speichers nicht; diese Funktion will man aber nicht missen. Je nachdem, welche Schnittstellen Ihr Computer hat, greifen Sie zu einem Gehäuse mit USB-A- oder USB-C-Anschluss. Haben Sie sich für ein Modell entschieden, stecken Sie die SSD ein und schrauben Sie das Gehäuse zu.

Und nun zur Software: Als Installationsmedium erstellen Sie zum letzten Mal einen Desinfec't-Stick mit der Standardprozedur. Unter Windows nutzen Sie dafür unser Installationstool Desinfect2USB. Unter Linux gelingt es mit dd. Im Anschluss starten Sie Ihren Computer vom Stick. Weil für die Installation auf einer SSD kein konvertierter Stick nötig ist, überspringen Sie diesen Punkt im Desinfec't-Bootmenü und wählen direkt den Punkt „Desinfec't starten“ aus. Die SSD-Installation klappt aber auch von einem bereits konvertierten Stick.

Schließen Sie die USB-SSD erst an, wenn der Desktop vollständig aufgebaut ist. Klicken Sie anschließend doppelt auf das Icon „Desinfec't Stick bauen“. Nach ein paar Sekunden erscheint der Installationsassistent. Prüfen Sie unbedingt zweimal, ob das richtige Laufwerk mit der SSD vorausgewählt ist. Setzen Sie das Häkchen bei der Option „Auf SSD installieren“. Starten Sie die Installation. Der Vorgang sollte innerhalb weniger Minuten abgeschlossen sein.

Im Anschluss fahren Sie Desinfec't herunter, ziehen den USB-Stick ab und starten Ihren PC direkt von der USB-SSD. Das funktioniert genauso wie bei einem USB-Stick über das BIOS-Bootmenü. Im Folgenden gibt es noch ein paar Tipps.

Swap oder kein Swap?

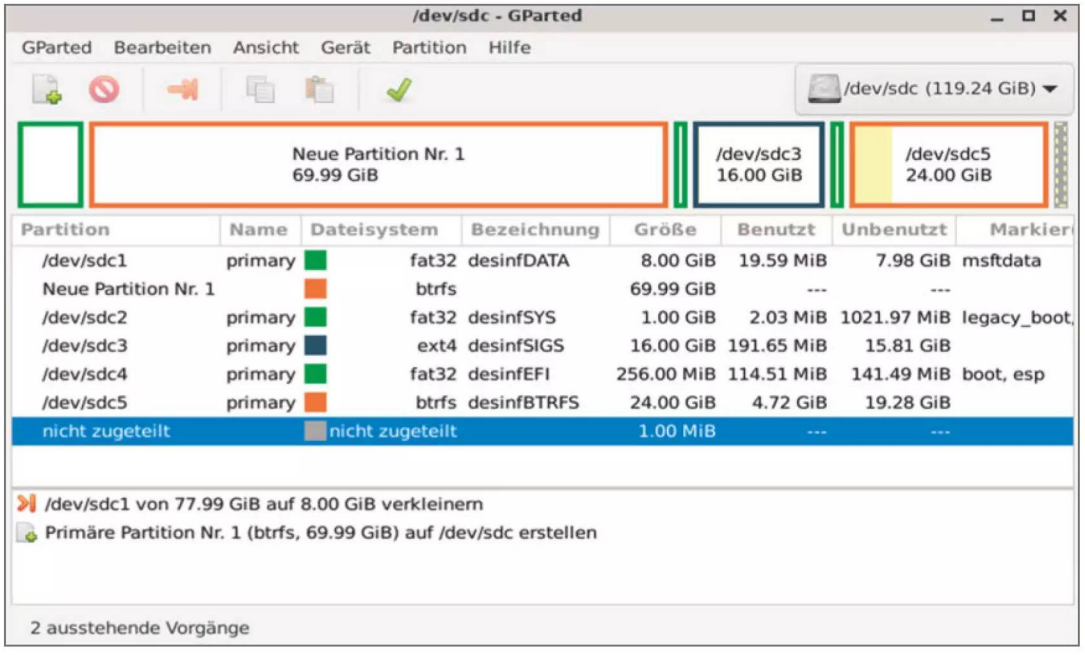
Als wir die USB-Stick-Installation implementiert haben, verfügten viele PCs nur über 4 GByte RAM. Doch schon damals waren Virenscanner speicherhungrig und haben den Arbeitsspeicher mitunter komplett für sich beansprucht. Da bleibt für das Live-System von Desinfec't nichts übrig, die Bedienung wird zäh und es kann sogar zu Abstürzen kommen.

Daher haben wir bei der USB-Installation den Auslagerungsspeicher (Swap) aktiviert. Linux lagert aber manchmal Speicherseiten aus, um Platz für Block-Devices – also Festplatten und SSDs – zu schaffen. Problematisch dabei ist, dass jeder Virenscan mit mehreren Scannern wiederholt auf dieselben Blöcke zugreift. Das wiederum führt dazu, dass Speicherseiten ausgelagert werden, um schneller auf Festplatten und SSDs zugreifen zu können.

Leider geht Linux dabei davon aus, dass das Lesen und Schreiben aus dem Swap etwa so schnell ist wie das Lesen und Beschreiben der Laufwerke, die zwischengespeichert werden. Bei USB-Sticks ist das aber nicht der Fall und der Swap auf einem Stick ist bis zu hundertmal langsamer als ein direkter SSD-Zugriff. Das führt zu Verzögerungen oder sogar Abstürzen.

Weil selbst aktuelle SSDs immer noch langsamere Zugriffszeiten als RAM haben, bremst das Auslagern von Daten den Betrieb. Für Desinfec't 2025/26 und für Desinfec't 2026 (erscheint voraussichtlich im Mai 2026) werden wir daher den Umgang mit dem Swap ändern: Beim Start auf Computern ab 8 GByte RAM wird der Auslagerungsspeicher bei Desinfec't auf USB-Sticks und SSDs grundsätzlich deaktiviert sein. Auf PCs mit weniger Arbeitsspeicher bleibt der Swap hingegen aktiv. In beiden Fällen läuft das System von einer SSD spürbar flotter.

Damit auch Nutzer von Desinfec't 2025 davon profitieren, stellen wir das p2-Update mit einer Zwischenlösung bereit. Um den Swap zu deaktivieren, öffnen Sie die Datei grub.cfg im Ordner boot/grub/. Tragen Sie dort den Bootparameter `noswap` ein. Das können Sie etwa unter Windows direkt aus dem Explorer mit der gerade erzeugten Desinfec't-SSD ausprobieren.



Bei unserer Test-SSD mit 120 GByte belegt Desinfec't standardmäßig rund 80 GByte. Auf Wunsch können Sie diese Partition verkleinern und wie in unserem Beispiel eine zusätzliche Partition mit 70 GByte zum Speichern Ihrer Daten anlegen.

Ohne Swap und aufgrund der im Vergleich zu einem USB-Stick deutlich flinkeren Lese- und Schreibraten läuft Desinfec't fühlbar schneller. Damit das auch auf Dauer so bleibt, ist es ratsam, unbelegten Speicher auf der SSD wieder als verfügbar zu markieren, damit schneller in freie Speicherzellen geschrieben werden kann. Das erledigt der Trim-Befehl. Stellen Sie dazu sicher, dass alle Partitionen gemountet sind, und führen Sie dann im Terminal als Root den Befehl `fstrim --all` aus.

Darf es eine Partition mehr sein?

In unseren Versuchen haben wir das Sicherheitstool auf einer SSD mit 120 GByte installiert. Wie auf einem USB-Stick setzt sich Desinfec't auch auf einer SSD aus mehreren Partitionen zusammen, etwa für das System und zum Speichern aktualisierter Virensignaturen. In unserem Beispiel ist die erste Partition, die unter anderem Desinfec't-Daten enthält, mit rund 80 GByte mit Abstand die größte. Sie ist standardmäßig mit FAT32 formatiert und damit universell verwendbar, aber auch eingeschränkt, weil Sie darauf keine Dateien größer als 4 GByte speichern können. Doch es gibt Abhilfe: Da die Partition keinerlei Bootdateien enthält, können Sie sie mit einem beliebigen anderen Dateisystem formatieren. Wenn Sie primär unter Linux arbeiten, bietet sich BTRFS an. Für Windows-Nutzer eignet sich NTFS.

Um Partitionen zu verändern und Abschnitte mit einem bestimmten Dateisystem zu formatieren, starten Sie Desinfec't von einem Stick und stecken die USB-SSD erst an, wenn der Desktop komplett geladen ist. Starten Sie dann über das Terminal mit dem Befehl `gparted` das Partitionierungswerkzeug. Unter dem Reiter „Partitionen" können Sie Bereiche vergrößern oder löschen. Mithilfe von GParted werden Sie Desinfec't auch wieder los, wenn die SSD anderweitig gebraucht wird: Löschen Sie dafür einfach alle Partitionen.

Bootprobleme?

Ein Datenträger mit Desinfec't setzt statt einer GPT- auf eine MBR-Partitionierung. Das mutet altertümlich an, früher konnten wir darüber aber eine höhere Kompatibilität gewährleisten. Diesen Hack schleppt das Sicherheitstool bis heute mit.

In der Theorie ist dieser Fall in den UEFI-Bootspezifikationen eigentlich abgedeckt, und durch einen MBR-Fallback sollte Desinfec't problemlos starten. Doch leider gehen viele Hardwarehersteller bei der Implementierung der Spezifikationen in ihre Motherboards lax vor und Desinfec't bootet nicht. Der Grund ist, dass das System einen GPT-partitionierten Datenträger mit einer EFI-Systempartition nach dem Schema eines Windows-Installationsmediums erwartet. Doch es gibt zwei Workarounds, um eine Desinfec't-SSD trotzdem zu starten. Der einfachste Weg ist es, in den UEFI-Einstellungen den Legacy-Modus zu aktivieren, der sich mit der MBR-Partitionierung zufriedengibt.

Ist das auf Ihrem PC nicht möglich, müssen Sie mit einem USB-Stick ein Windows-Installationsmedium simulieren; für diese Boot-Krücke reicht ein Stick mit 1 GByte. Starten Sie zur Vorbereitung der Boot-Hilfe Desinfec't von einem Stick und legen Sie auf dem künftigen Boot-Stick mit GParted eine FAT32-Partition an. Kopieren Sie dann den Inhalt (Bootloader, Grub, Kernel und initramfs) der EFI-System-Partition der Desinfec't-SSD auf den Stick und versehen Sie die Partition mit den Flags „boot“ und „esp“ (siehe Screenshot).

Fahren Sie den PC herunter. Schließen Sie dann den Boot-Stick an und wählen ihn als Startmedium aus. Sobald das Desinfec't-Bootmenü erscheint, stöpseln Sie die USB-SSD an und starten dann das Sicherheitstool. Wenn die Boot-Animation erscheint, sind Kernel und Initramfs geladen und Sie können den Boot-Stick abziehen. Das müssen Sie dann bei jedem Start von Desinfec't so machen.

Ausblick

Von einer SSD läuft das Sicherheitstool deutlich schneller und stabiler, doch es geht noch mehr: Desinfec't benutzt viele Hacks. Das liegt an den Anforderungen eines USB-Sticks. Das führt so weit, dass wir Virenscanner bei jedem Systemstart neu installieren müssen, damit sie zuverlässig funktionieren. Davon wollen wir zukünftig weg. Eine feste Installation auf einer SSD ist der Weg dorthin. Dies ist ein erster Ausblick, wie Desinfec't künftig von einer SSD laufen wird.

Desinfec't 2025/26 ermöglicht erstmals eine experimentelle USB-SSD-Installation, die weitgehend Ubuntus Festplatteninstallation entspricht. Damit fällt unter anderem der genannte Hack weg und das System ist schneller einsatzbereit. In Zukunft planen wir auf Basis dieser Installationsmethode und der in BTRFS enthaltenen Snapshot-Funktion das System noch einfacher modifizierbar zu machen, sodass Sie etwa Anwendungen und Treiber dauerhaft installieren können. (des) c't

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 2025/26 voll ausschöpfen“ (Seite 14) 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.

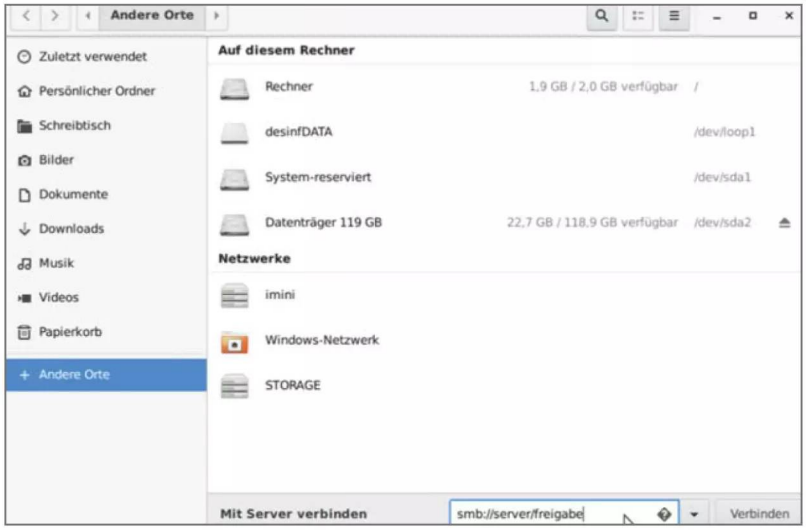
Wenn Sie sich im Dateibaum eines Windows-Systemlaufwerks umsehen, fällt auf, dass die Ordner englische Namen in Desinfec't tragen; der Windows-Explorer zeigt normalerweise deutsche Bezeichnungen. Anders als unter Windows ist auch: Sie können sich frei in allen Verzeichnissen bewegen. Desinfec't schert 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-

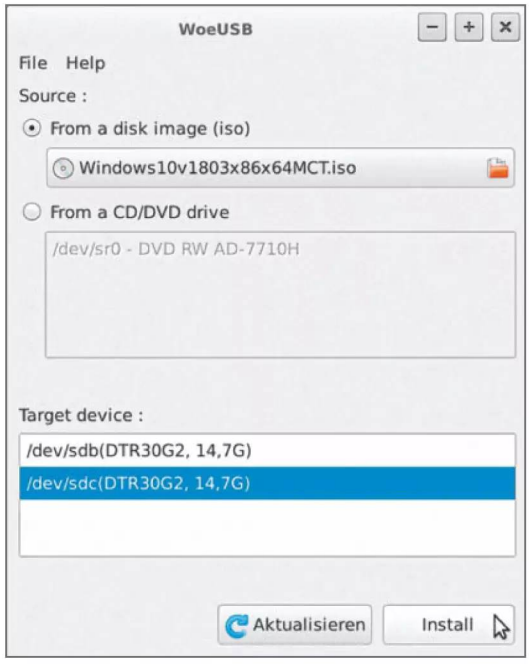
Weitere Hinweise
ct.de/w9ax

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.

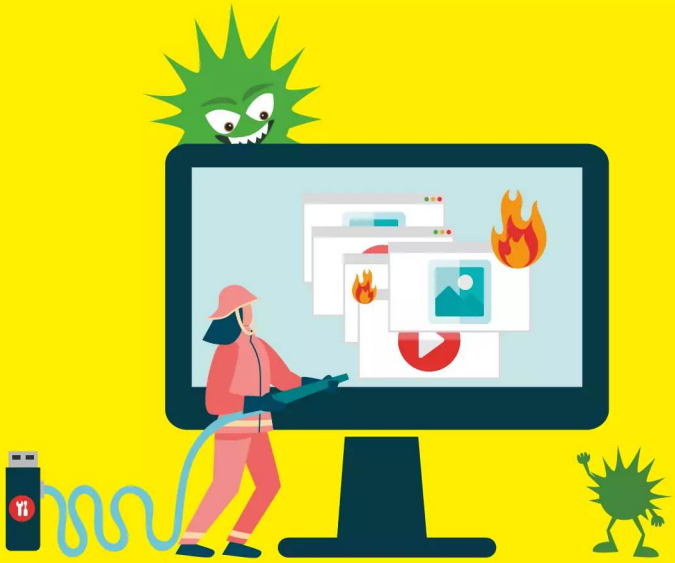
Die Änderung der Paketquellen und die anschließend hinzugefügten Pakete gehen verloren, wenn Sie Desinfec’t herunterfahren. Die Paketeinrichtung können Sie erhalten, indem Sie nach der Installation die Pakete in einem Terminalfenster auf den Stick kopieren:

```
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

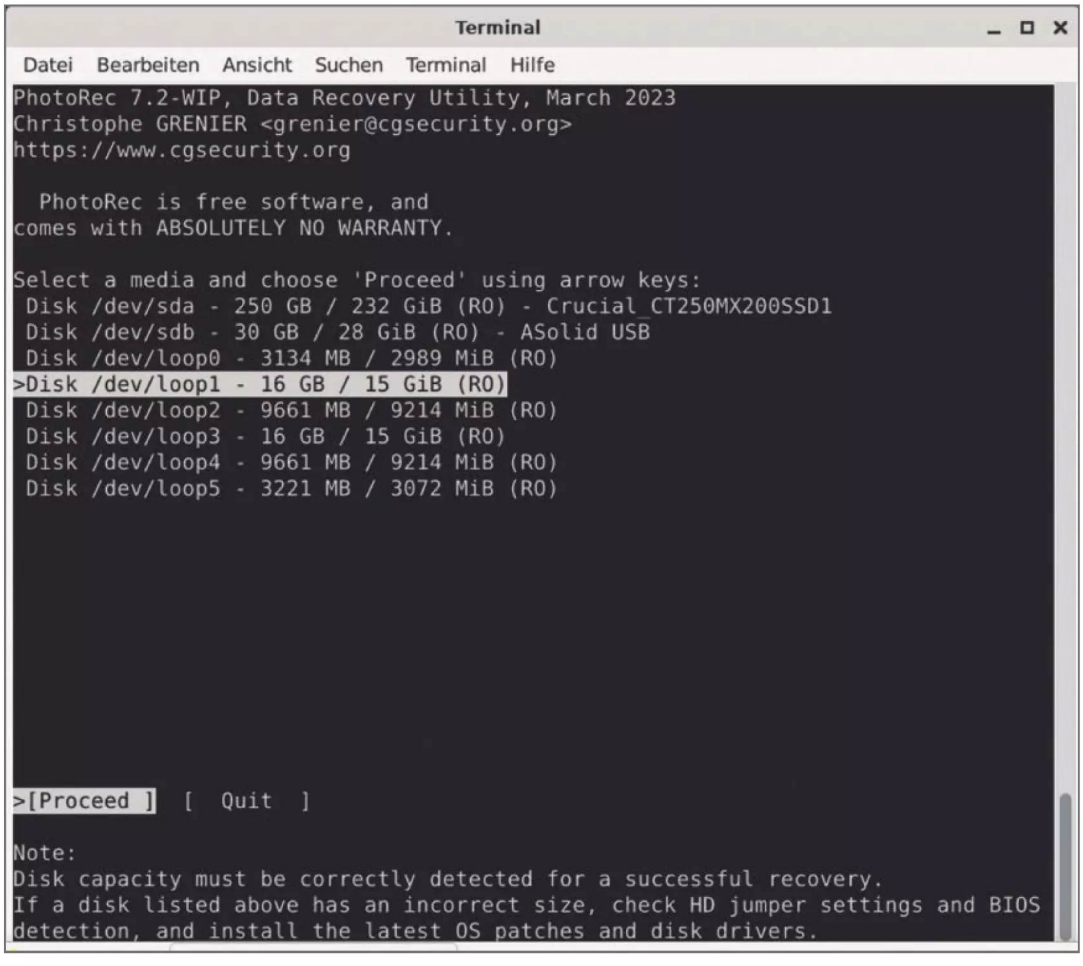
Bei größeren Defekten oder logischen Fehlern, wo etwa ein Absturz des Treibers oder Rechners das Dateisystem beschädigt hat, lassen sich die Dateisysteme nicht mehr einbinden oder es fehlen ganze Verzeichnisse, weil die Verzeichnisstruktur fehlerhaft ist. Selbst wenn Sie das Medium versehentlich (schnell-)formatiert 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:

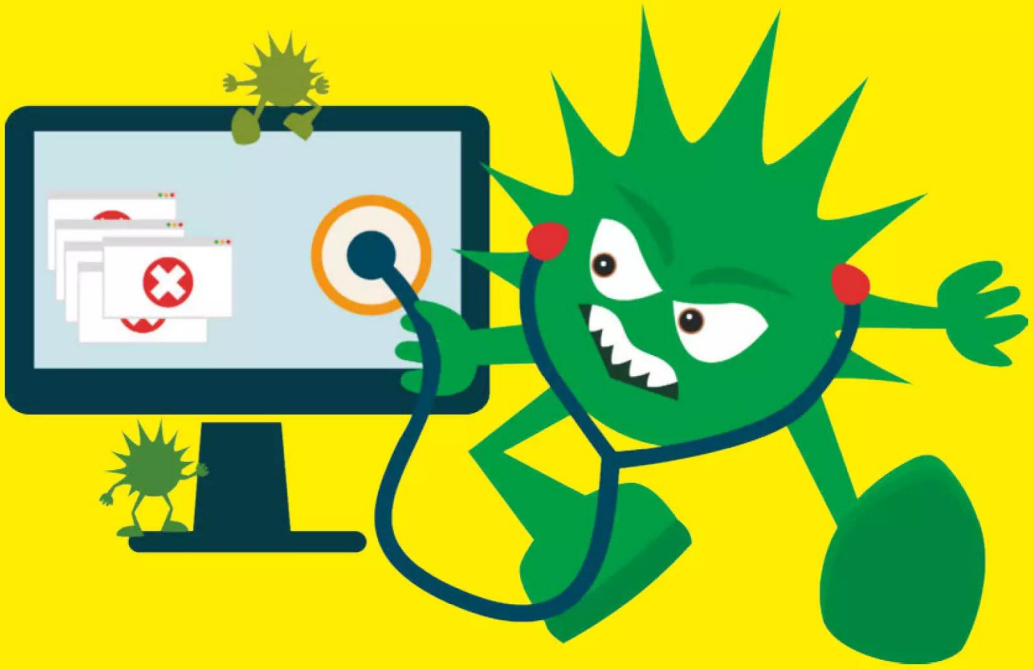
```
eml n 20000000 \x0aMessage-ID:\s
```

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

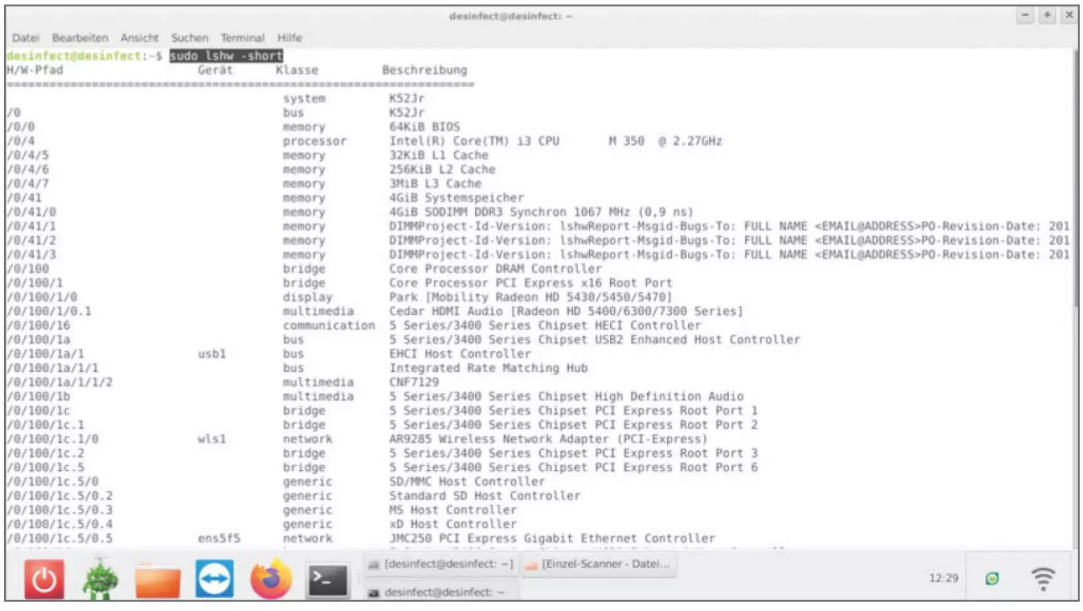
Eines davon ist `dmidecode`, das vom BIOS generierte DMI-Tabellen mit der Selbstbeschreibung des Systems anzeigt. Der Befehl

```
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/*
```

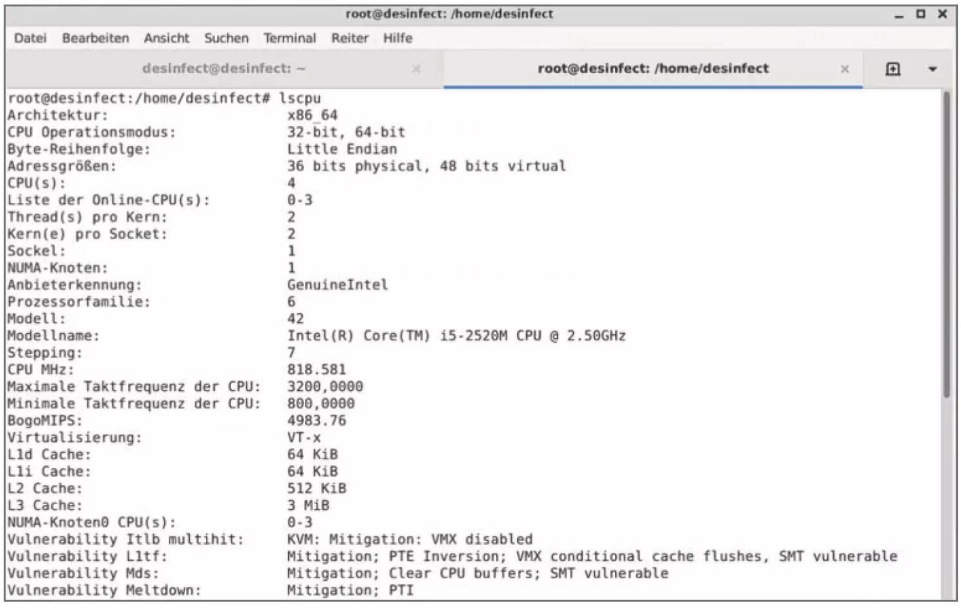
Bei Desinfec't zeigt das den Inhalt von Dateien zu vielen Sicherheitslücken, die seit Anfang 2018 bekannt wurden. Findet sich in den Dateien ein mit „Vulnerable“ oder „Mitigation“ beginnender Text, dann ist Ihr Prozessor für die im Dateinamen genannte Sicherheitslücke anfällig.

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.

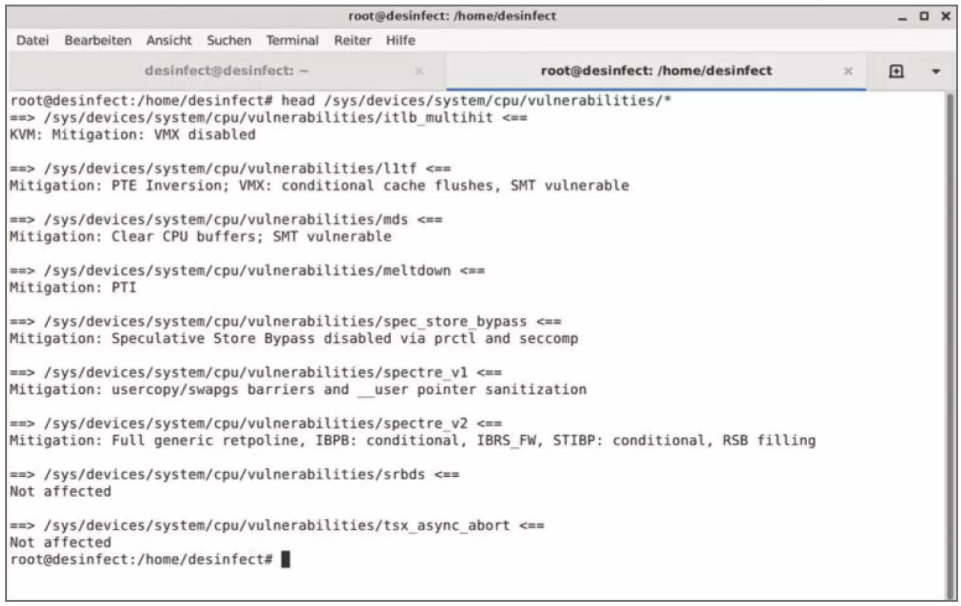
PCI- und USB-Geräte

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

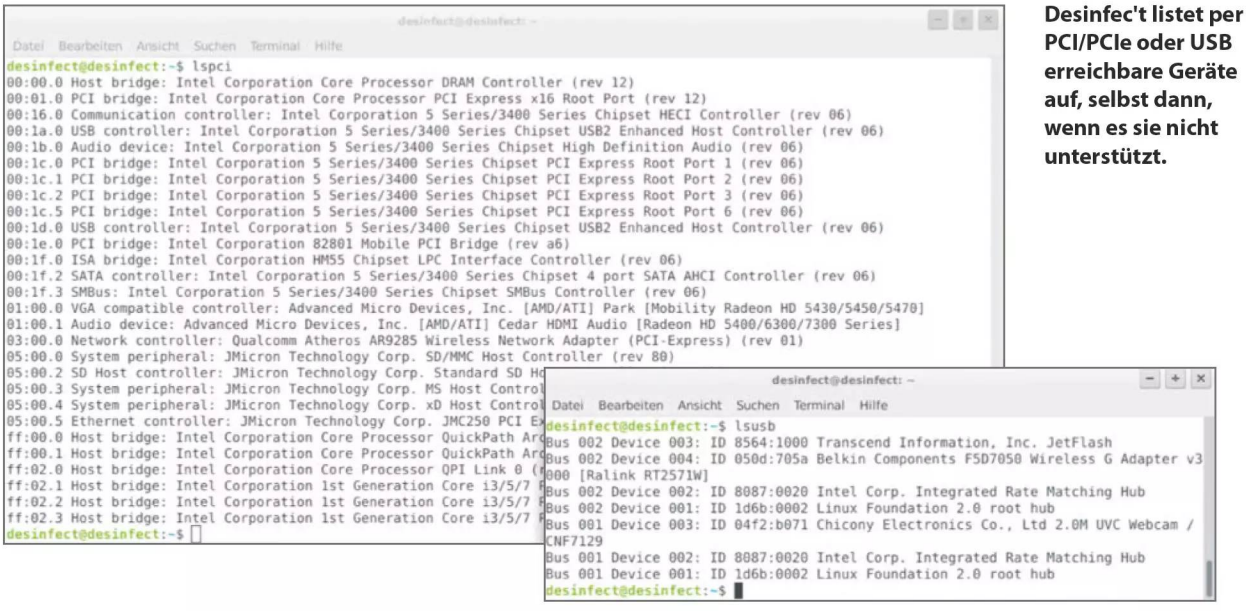
Das Werkzeug lscpu nennt die Zahl der CPU-Kerne sowie Minimal- und Turbo-Taktfrequenz.



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:

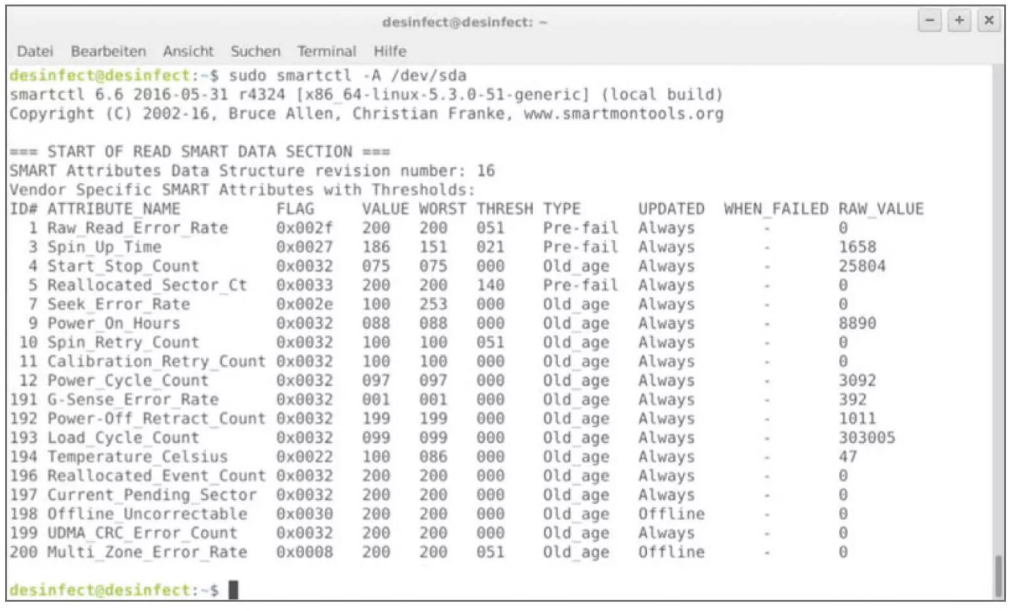
```
sudo hdparm -I /dev/sda
```

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

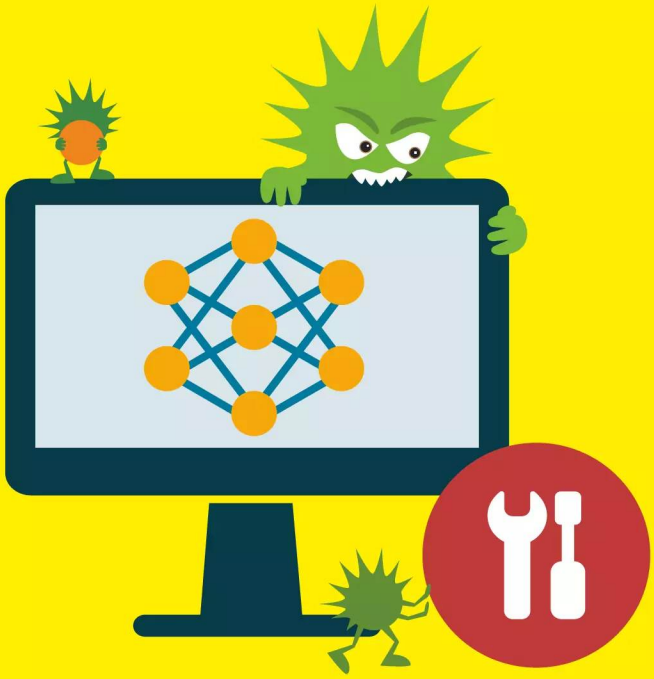
Viele der erwähnten Programme bieten Optionen, mit denen sie mehr Ausgaben liefern oder weitere Aufgaben erledigen. `lspci` gibt bei Angabe des Parameters `-k` etwa umfangreichere Informationen aus, die auch den vom Kernel verwendeten Treiber nennen. Noch viel mehr Details zu PCI/PCIe-Geräten und ihrer 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



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**

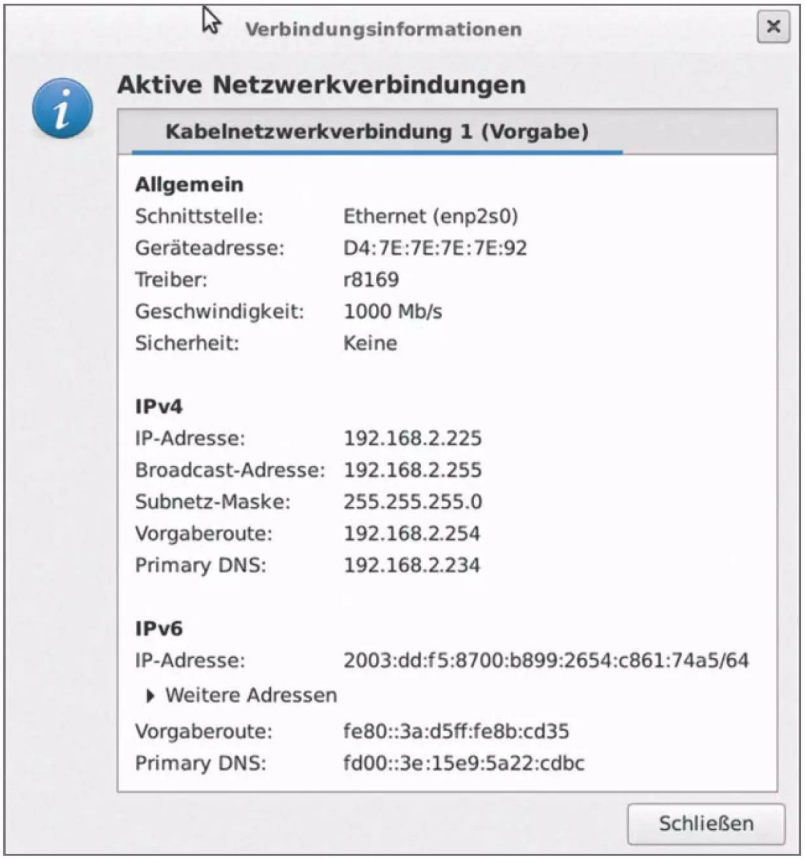
Netzwerkprobleme gibt es reichlich. Die kann man am OSI-Schichtenmodell durchdeklinieren, muss man aber nicht. Mit dem folgenden Know-how und den Werkzeugen in Desinfec't setzen Sie gleich an den neuralgischen Stellen an, um Probleme im Netzwerk aufzuspüren und zu lösen. Wie in vielen anderen Praxisartikeln 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 24.04 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/24.04/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

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.

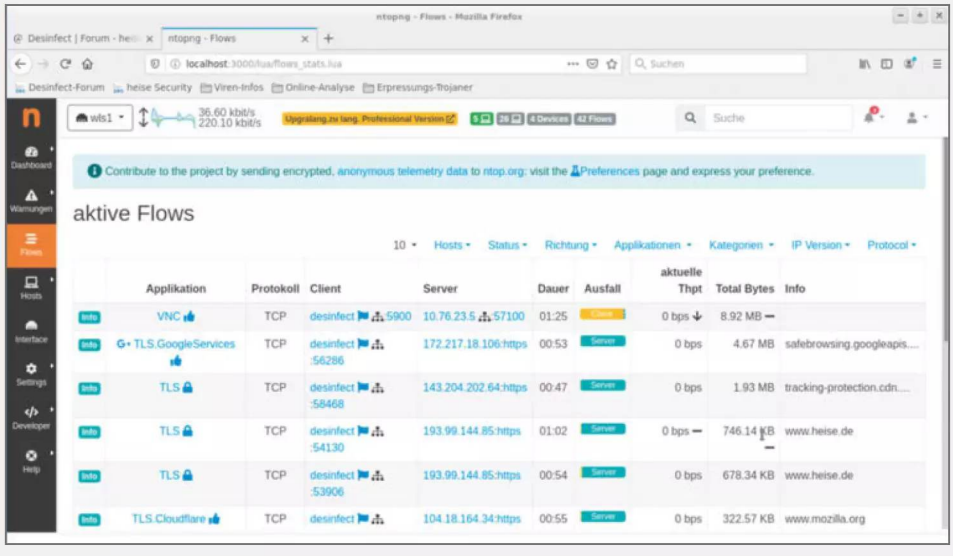
Hält das Problem an, starten Sie den Router neu. Hilft auch das nicht, prüfen Sie mit einem weiteren Gerät, ob vielleicht nur der PC ein Problem hat. Surfen Sie aus dem WLAN die Lieblingswebsites mit einem Smartphone an. Besser wäre ein zweiter PC. Er sollte idealerweise nicht baugleich mit dem ersten 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

auf die 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.

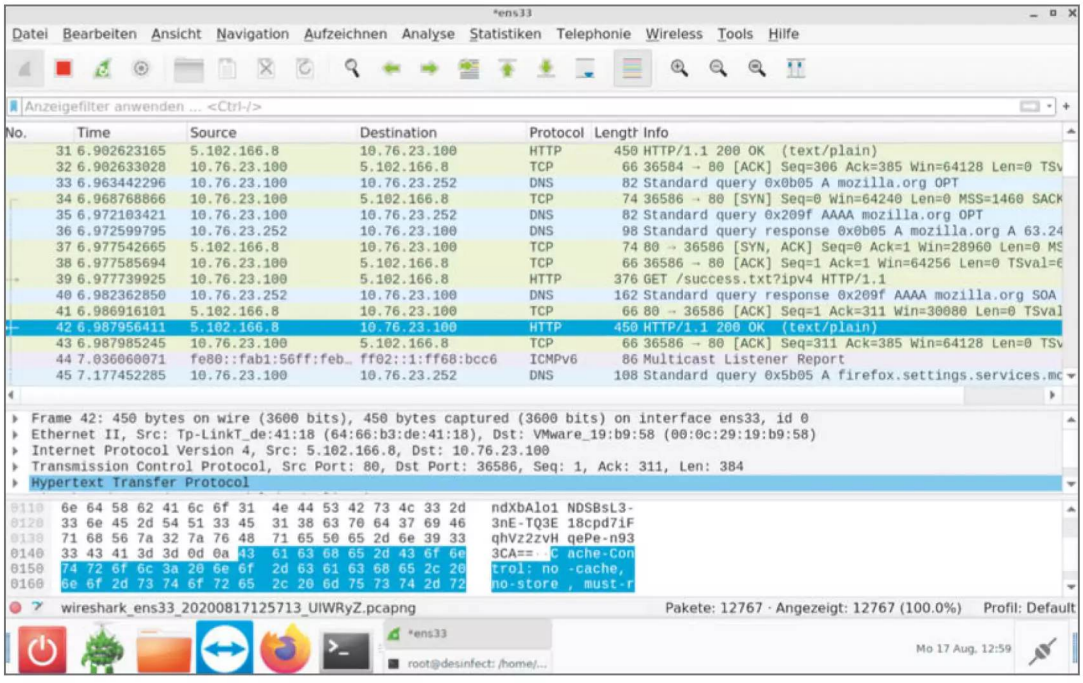
müssen Sie meist mit Betätigen der Tasten `Strg+C` abbrechen.

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



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.

durchexerzierten 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.

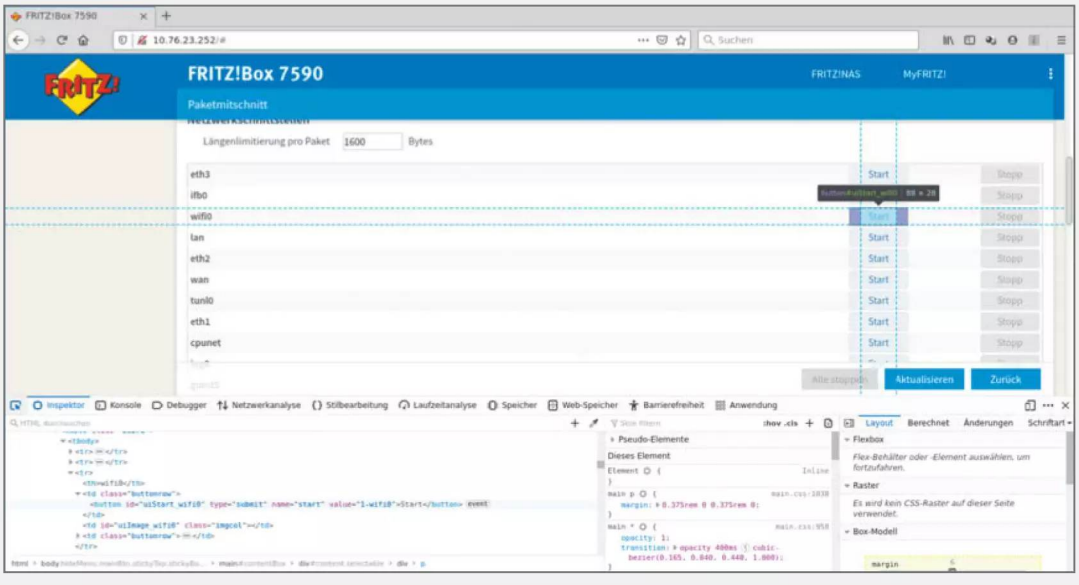
Fritzbox als Horchposten für Wireshark & Co.

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

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)

Redaktion: Thorsten Leemhuis, Mattias Schlenker, Olivia von Westernhagen

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

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

DTP-Produktion: Vanessa Bahr, Dörte Bluhm, Lara Bögner, Beatrix Dedek, Laura-Sophie Gruhn, Madlen Grunert, Cathrin Kapell, Steffi Martens, Marei Stade, Matthias Timm, Christiane Tümmler, Nicole Wesche

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

Illustration, Fotografie: Steffi Martens, Ninett Wagner, Melissa Ramson, Andreas Wodrich, www.freepik.de

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: 26.09.2025

Vorschau: c't KI-Wissen 2/2025

Ab dem 24. Oktober im Handel und auf shop.heise.de

Kritische Analysen & Kreative Praxis

KI durchdringt mittlerweile alle Bereiche der Gesellschaft. Von der Softwareentwicklung über medizinische Neuentwicklungen, Musik- und Bildergenerierung bis zu neuen staatlichen Überwachungsmethoden. Im Sonderheft KI-Wissen beleuchten wir die aktuelle Entwicklung. Wir analysieren, wie aktuelle KI-Modelle funktionieren, und zeigen, wie man KI-Agenten praktisch nutzen kann.

KI-Dienste ermöglichen neue Verfahren in der Medizin, helfen bei der Erkennung von Hautkrebs und anderen Krankheiten. Die Digitalisierung hat aber auch ihre Tücken, etwa wenn Sprachmodelle als billiger Ersatz für Psychotherapeuten herhalten sollen oder zweifelhafte Angebote Verstorbene digitalisieren, um den Verlust der Angehörigen zu lindern. Auch smarte Brillen, die mithilfe von KI Informationen über die Umwelt einblenden, sind längst keine Zukunftsmusik mehr, wie unsere Tests aktueller Modelle zeigen.

Eng verknüpft mit der Frage nach dem Nutzen der KI ist aber auch der kritische Blick auf die Risiken, wenn Dienstleister sich mithilfe von KI Musikstücke, Stimmen und Bilder aneignen, ohne die Urheber adäquat zu bezahlen. Hier regt sich Widerstand, den wir in verschiedenen Bereichen der Kreativbranche genauer beleuchten.

Schließlich blicken wir auf die wirtschaftlichen und ökologischen Auswirkungen: Was passiert, wenn die KI von einer Handvoll US-Unternehmen kontrolliert wird, die andere Firmen, Angestellte und Nutzer auf ihre Plattformen zwingen und immer höhere Gebühren für ihre KI-Dienste verlangen? Das Rennen um die stärksten KI-Modelle hat inzwischen Dimensionen erreicht, die massive Auswirkungen auf die Wirtschaft, Energieversorgung und Umwelt haben. Da fällt es schwer, in Europa Alternativen aufzubauen und die mächtigen Konzerne adäquat zu regulieren. Zur Gefahr für Demokratien werden selbst einzelne Unternehmen wie Palantir, die riesige Datenbanken miteinander verknüpfen und auch Deutschland zu einem Überwachungsstaat hochrüsten.

So zeigen wir im Sonderheft KI nicht nur die technisch neuen Möglichkeiten durch KI auf, sondern beleuchten ebenso die Schattenseiten der neuen Technik, damit die Leserinnen und Leser besser verstehen, was in den sonst so undurchsichtigen Algorithmen passiert.

Themenschwerpunkte

KI-Modelle & Agenten
- Vergleichstest von Reasoning-Modellen
- Wo verlaufen die Grenzen aktueller Sprachmodelle im Vergleich zu menschlichen Gehirnen?
- Feintuning: Chatbots verbessern mittels RAG
- Lokale Modelle: LLMs komprimieren für schwächere Hardware
- Agenten: So steuern KI-Modelle Apps und Dienste
- MCP: Eigene Server aufsetzen und auf dem Desktop einsetzen, Sicherheitsprobleme erkennen

Forschung & Medizin
- KI in der Science Fiction: Das können wir aus Star Trek lernen
- Smart Glasses: Das leisten die neuen smarten Brillen, Tipps für Brillenträger
- Smart Glasses: Test neuer Modelle von Ray-Ban und Even G1
- Doktor ChatGPT: Das taugen LLMs als billige Psychologen
- Stimmanalyse: KI erkennt Krankheiten am Tonfall
- Krebsvorsorge: Das taugen Hautkrebsscanner
- Trauerkultur: Wie verändern KI und Technik den Umgang der Hinterbliebenen

Medien & Urheberrecht
- Musik-Generatoren: Was passiert mit Musikern und Labels, wenn alle nur noch KI-Muzak hören?
- Musik-Generatoren: Vier Dienste im Vergleich
- KI-Musik: Vorsicht vor dem Kleingedruckten – Anbieter sichern sich weitgehende Rechte
- KI-Stimmen: Sprecherverband fordert Regulierung, Spieleproduzenten üben Druck aus
- KI-Bildverwaltung: Fotos und Videos mithilfe von KI ordnen und verwalten
- Urheberrecht: Kennzeichnungspflicht für KI-Bilder

Regulierung & Datenschutz
- Technik-Monopole: Welche Gefahren von den „Magnificent 7" ausgehen und welche Rolle KI dabei spielt
- Ressourcenbedarf: Wie die riesigen Server-Center die Umwelt gefährden
- Suche nach Alternativen: Wie Europa sich von den US-Anbietern emanzipieren kann
- Orwell lässt grüßen: Wie Palantir den Überwachungsstaat aufrüstet
- Supermarktkassen: So funktionieren Kundenüberwachung und Datenanalyse im Einzelhandel
- EU-Regulierung: Das bringt die KI-Verordnung

Datenkraken verstehen!

Schwachstellen aufdecken wie die Profis!

JETZT Tools + Taktiken kennenlernen

Mittlerweile arbeiten Profi-Hacker als Pentester, um Sicherheitslücken aufzudecken. Wir blicken ihnen im c't Sonderheft über die Schulter:

- Trainingsmaterial für angehende Hacker
- Live-Pentest: Cyberangriffe zu Fuß
- Mit dem Raspi Angriffe simulieren
- Interview: Über das Hacken einer PS5

shop.heise.de/ct-hacking25

im heise shop!

Generell portofreie Lieferung für Heise Medien- oder Maker Media Zeitschriften-Abonnenten oder ab einem Einkaufswert von 20 € (innerhalb Deutschlands). Nur solange der Vorrat reicht. Preisänderungen vorbehalten.

heise shop

SUPPORT ME

🙏 Hope my post useful for you, if you want support me please following one of the ways:

Buy or Renew Premium Account

👉 Rapidgator: https://rapidgator.net/account/registration/ref/49023

👉 Nitroflare: https://nitroflare.com/payment?webmaster=194862

⚠ Note: Please DON'T turn on VPN when making payment.

Donate Directly

USDT (TRC20):

TFniVipHpFsPVrUHBLsvkZJV4Mjj1MUz96

DOGE (Doge Network):

DCfVVnvNaVtxQbWyfpWsihbGnvpkuYdtJS

Every little support helps me to keep going and create more content.

THANK YOU SO MUCH!