c't Desinfec't

Das Rettungssystem bei Virenbefall

NEUE VERSION 2026 / 27



Komplett überarbeitet: einfacher, schneller, zuverlässiger

- Windows prüfen, Schädlinge entfernen, Daten retten
- Mit Virenscannern von ESET, IKARUS und WithSecure
- Signaturupdates bis November 2027

Vireninfektion! Das müssen Sie tun

Das kann das c't-Sicherheitstool

So funktioniert's: Trojaner aufspüren und unschädlich machen

Daten retten

Auf nicht mehr startende PCs zugreifen

Persönliche Dateien in Sicherheit bringen

Für Einsteiger und Profis

Installieren, starten, scannen: Funktionsweise Schritt für Schritt erklärt

Profi-Werkzeuge zur Malwareanalyse

So holen Sie alles aus Desinfec't heraus

€ 16,90
CH CHF 29.90
AT € 18,50
LUX € 19,50

4 195957 616902 04

FÜR ALLE, DIE ES GENAU WISSEN WOLLEN



Lesen Sie 5 Ausgaben c't mit 30 % Rabatt – als Heft oder digital in der App, im Browser oder PDF. Erhalten Sie dazu noch ein Geschenk Ihrer Wahl.

Ansgar Kossowski
und Steffen Herget
c't Redaktion



Jetzt 5 × c't lesen
für 26,75 € statt ~~36,25 €~~

30 % Rabatt!

Jetzt bestellen:
ct.de/wissen

ct.de/wissen | 0511 / 647 22 888 | leserservice@heise.de

Editorial

Liebe Leserin, lieber Leser,

wenn ein PC Anzeichen einer Vireninfektion zeigt, fällt es schwer, ruhig zu bleiben. Schließlich sind persönliche Daten in Gefahr, und Kriminelle könnten mit Ihrer Kreditkarte bezahlen oder Ihre Dokumente und Fotos verschlüsseln, sodass Sie nicht mehr darauf zugreifen können. Hier kommt Desinfec't als Retter in der Not ins Spiel. Es hilft bei der Analyse und Bereinigung Ihres Computers. Zusätzlich können Sie Ihre wichtigsten Daten auf einem Desinfec't-Datenträger in Sicherheit bringen.

Damit im Ernstfall alles glatt verläuft, haben wir das brandneue Desinfec't 2026/27 von Grund auf überarbeitet. Die neue Version sieht nicht nur anders aus, auch die zugrunde liegende Technik haben wir generalüberholt. Dadurch startet das System zuverlässiger, und Signaturupdates und Scans laufen wesentlich stabiler.

Nach wie vor richtet sich Desinfec't vor allem an Windows-Nutzer, die ihr System auf Viren untersuchen wollen. Als technische Basis dienen Ubuntu 26.04 LTS und KDE. Mithilfe des Btrfs-Dateisystems können Sie das System bei Problemen auf den Werkszustand zurücksetzen. Anstelle von Windows startet Desinfec't direkt von einem USB-Datenträger wie einem Stick oder einer SSD in einem USB-Gehäuse. So untersuchen Sie Ihr inaktives Windows-System aus sicherer Entfernung.

Der neue Scanassistent AVRunner steuert die drei enthaltenen Virenscanner ESET Server Security, IKARUS cmd.scan und WithSecure ATLANT. Damit den Scannern keine frisch entschlüpften Viren durchrutschen, sind ein Jahr lang kostenlose Signaturupdates inklusive.

Wie Sie Desinfec't einrichten und loslegen, lesen Sie ab Seite 20. Wir hoffen, dass Desinfec't Ihnen hilft, infizierte PCs zu heilen und Ihre Daten zu retten.



Dennis Schirrmacher

Inhalt

6 **Desinfec't 2026/27** Das Notfallsystem Desinfec't kann die letzte Rettung für ein verseuchtes Windows sein. Um Trojanern auf die Spur zu kommen und Windows zu säubern, schickt es mehrere Virenscanner von unter anderem ESET und WithSecure los.

10 **Im Einsatz** Lernen Sie die Funktionsweise und den Funktionsumfang des c't-Sicherheitstools kennen. Der Artikel zeigt im Detail, wie Sie damit am effektivsten eine Virenjagd starten.

20 **Schritt für Schritt starten** So laden Sie Desinfec't 2026/27 herunter, installieren es auf einem USB-Datenträger und starten Ihren PC davon.

24 **Bilderstrecke Virenscan** So aktualisieren Sie Virensignaturen, starten einen Scan und werten Ergebnisse aus.

30 **FAQ** Antworten auf die häufigsten Fragen.

36 **Netzscan** Damit Desinfec't auf Windows-PCs mit ARM-CPU läuft, müssen Sie es übers Netzwerk starten. Das ist gar nicht schwer.

40 **Status quo Malware** Dieser Artikel zeigt, welche Trojaner gerade in Umlauf sind und auf welche Taktiken Angreifer derzeit setzen, um Computer zu kompromittieren. So schützen Sie sich vor solchen Attacken.

46 **VirusTotal ausreizen** Mit dem Gratis-Tool vt-cli zapfen Sie VirusTotal über die Kommandozeile an. So starten Sie etwa Batch-Scans mehrerer verdächtiger Dateien und stoßen im Zuge der Incident Response passgenaue Malware-Recherchen an.

Direkt loslegen!

Viren jagen mit Desinfec't

Mit dem c't-Sicherheitstool Desinfec't 2026/27 untersuchen Sie Windows aus sicherer Entfernung auf PC-Schädlinge. Das Live-System startet von einem USB-Datenträger und schaut mit mehreren Virenscannern von unter anderem ESET, IKARUS 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.

Zusätzlich bringen Sie mit Desinfec't Ihre persönlichen Daten von einem nicht mehr startenden PC in Sicherheit. Um Desinfec't zu nutzen, laden Sie zuerst das Image von Desinfec't 2026/27 herunter. Anschließend erstellen Sie einen USB-Datenträger und starten es von dort. Weitere Informationen dazu finden Sie in der Schritt-für-Schritt-Anleitung ab Seite 20.

52 **Dokumentenanalyse** Desinfec't bringt mehrere Tools mit, mit denen Sie verdächtige PDF- und Word-Dokumente durchleuchten können.

60 **Trojaner aufspüren** Ein leistungsstarkes und kostenloses Profi-Toolkit unterzieht Schadcode und andere Bedrohungen einer Bestandsaufnahme – auch Einsteiger können mit den flexiblen Befehlen auf der Kommandozeile erste Schritte wagen.

66 **Exe-Dateien analysieren** Anhand des Erpressungstrojaners WannaCry zeigen wir, wie Sie Schadcode tiefgreifend analysieren.

74 **Maßgeschneiderter Virenscanner** Auf der Basis von YARA-Regeln können Sie gezielt auf die Suche nach Schadcode gehen.

82 **Die Technik von Desinfec't** Wir haben unser Live-System zur Schädlingsjagd auf Windows-PCs erneuert. Dieser Artikel blickt technisch auf die Neuerungen und die Auswirkungen für Nutzer.

92 **Entwicklung mit KI** KI sollte helfen, Ideen an einem Prototyp früh zu beurteilen. Es wuchs sich zu einer mehrmonatigen Chat-Session aus. Das Resultat: Desinfec't 2026/27.



ZUM HEFT

3 Editorial
91 Impressum
98 Vorschau c't Lokale KI

Die neue Desinfec't-Ära beginnt

Wir haben unser bewährtes Sicherheitstool dieses Jahr auf eine komplett neue Basis umgestellt. Die Kernfunktionen bleiben natürlich erhalten.

Von **Dennis Schirrmacher und Peter Siering**

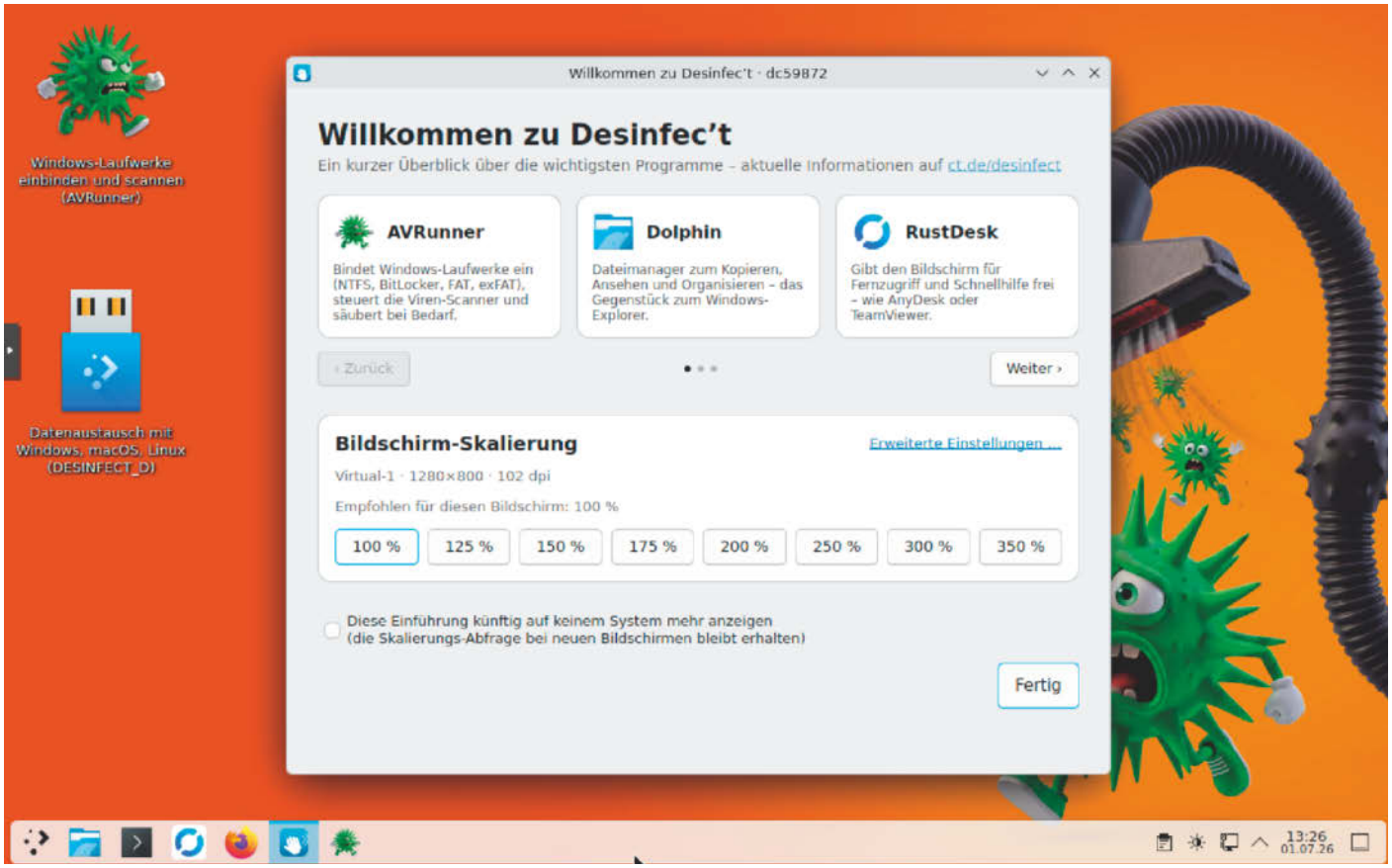


Bild: Martina Bruns / KI / heise medien

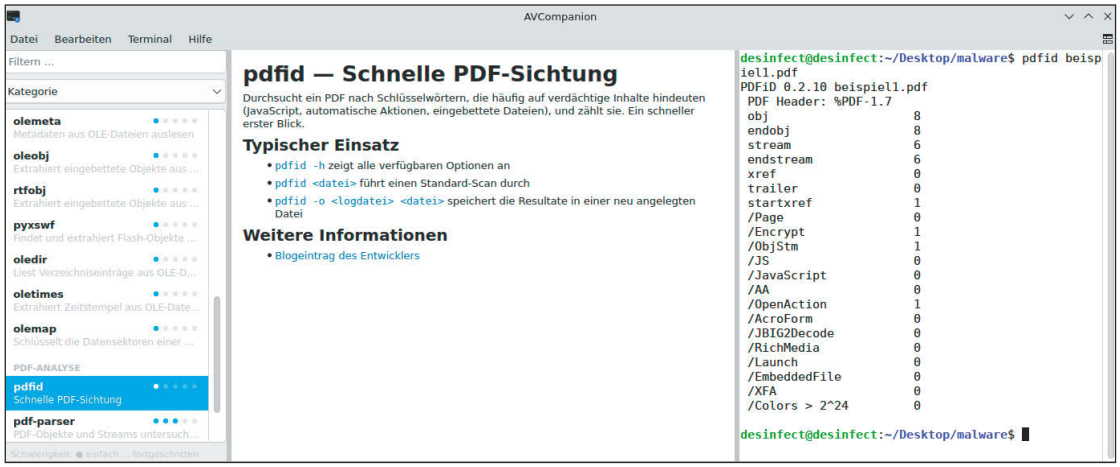
Desinfec't 2026/27 richtet sich vor allem an Windows-Nutzer und scannt Computer auf Schädlinge jeder Art. Es verwendet als Grundlage ein spezielles Linux-System, das direkt von einem transportablen Datenträger wie USB-Stick, externe SSD oder USB-SD-Card-Adapter startet. Da Windows inaktiv ist, schläft auch der Schadcode und kann kein weiteres Unheil anrichten. In diesem sicheren Zustand untersuchen Sie dann Ihren Computer.

Um PC-Schädlingen auf die Schliche zu kommen, sind mehrere Virenscanner dabei. Ein Jahr lang Gratis-Signaturupdates sorgen dafür, dass die Scanner auch aktuelle Bedrohungen erkennen. Zusätzlich sind für erfahrene Malware-Analysten Tools wie Capa und FLOSS dabei. Der Desinfec't-Datenträger bietet Platz, um darauf Dateien eines nicht mehr startenden PCs in Sicherheit zu bringen.

Damit auch Computereinsteiger mit den Grundfunktionen zurechtkommen, halten wir die Bedienung so simpel wie möglich. Weil mit der Neufassung beim ersten Booten keine Umwandlung des Sticks mehr nötig ist, verläuft der Start des Sicherheitstools einfacher und es gibt einen Stolperstein weniger. Vor allem im Betrieb hat sich einiges getan und etwa Signaturupdates laufen stabiler. Damit Sie bei der Schädlingssuche nicht im Dunkeln tappen, liefert der komplett neue Scanassistent „AVRunner" nun hilfreiche Statusinformationen. Doch was haben wir überhaupt verändert?



Nicht nur die Technik ist neu, auch die Oberfläche haben wir aufgeräumt: Viele bisher über mehrere Werkzeuge verstreute Funktionen bündelt der Scanassistent AVRunner.



!Desinfec't bringt neben den Scannern von ESET, IKARUS und WithSecure auch viele Profitools für die Malwareanalyse mit. Diese sind im AVCompanion zusammengefasst.

Das hat sich getan

Im Grunde hat Desinfec't 2026/27 mit seinen Vorläufern vor allem den Namen und einige Zutaten gemein. Den Rest haben wir stark überarbeitet. Die Implikation für Desinfec't-Kenner: Sie müssen etwas umdenken und sollten unbedingt den direkt auf Seite 10 folgenden Artikel zum Erstellen eines Boot-Mediums und zur Nutzung der überarbeiteten Werkzeuge lesen. Eine Zusammenfassung der wichtigsten Schritte finden Sie auf Seite 20.

Was bleibt: Sie müssen das Desinfec't-Image herunterladen. Um das Image auf einen USB-Wechseldatenträger zu übertragen, haben wir die Software Imagewriter geschrieben. Sie läuft unter Windows oder macOS und überträgt direkt das komprimierte Image auf den Datenträger. Der sollte 32 GByte oder mehr Platz bereithalten. Davon nimmt sich Desinfec't 16 GByte. Den übrigen freien Platz können Sie verwenden, um Dateien aus der Desinfec't-Welt mitzunehmen, etwa um Ergebnisse eines Scans mit den gewohnten Werkzeugen unter Windows oder macOS in Ruhe zu analysieren.

Die Neuerungen in aller Kürze: Als Betriebssystemgrundlage verwenden wir Ubuntu 26.04 LTS. Anders als früher ist der Bootdatenträger beschreibbar, also keine nicht beschreibbare ISO-Datei als Basis mehr. Das Linux-Dateisystem auf dem Stick ist Btrfs. Ein beim Erstellen des Images erstellter Snapshot erlaubt, beim Booten den Ausgangszustand wiederherzustellen. Das schützt vor vermurksten Sticks und hilft als Sicherheitswaschgang bei schmuddeligen Scanzielen.

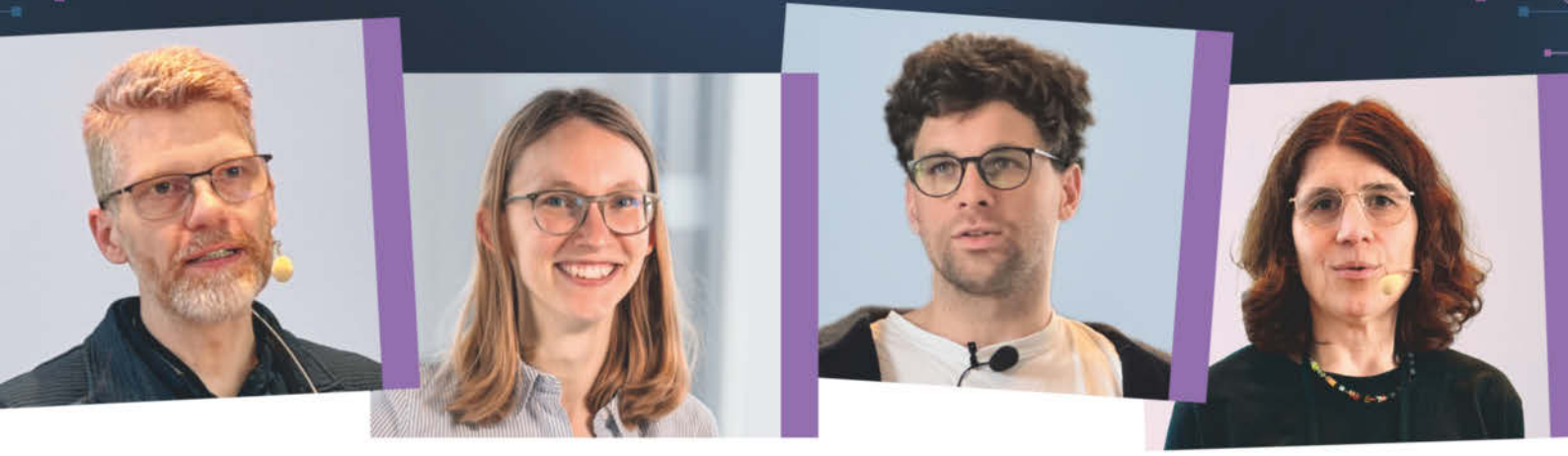
Der neue Scanassistent „AVRunner" steuert die enthaltenen Virenscanner, ESET Server Security, IKARUS cmd.scan, WithSecure ATLANT und ClamAV. Er versucht einen Balanceakt zwischen Übersichtlichkeit nebst einfacher Bedienung und lässt Sie als Nutzer nicht im Dunklen stehen, was gerade passiert: Es ermittelt und optimiert den Scanumfang, zeigt den Fortschritt an und bemerkt auch, wenn sich ein Scanner in die ewigen Jagdgründe begeben haben sollte. AVRunner kümmert sich selbst darum, Windows-Datenträger einzubinden – ohne Aufforderung fasst Desinfec't keine FAT-, exFAT- oder NTFS-/Bitlocker-Partitionen des Nutzers an.

Sie können Desinfec't nicht nur im privaten Umfeld, sondern auch im Büro, in Unternehmen und Universitäten nutzen. Wer mehrere Sticks braucht, etwa um das Unternehmen einzudecken oder die Uni-Rechner zu scannen, erhält im heise shop Sonderkonditionen (service@shop.heise.de). Für direkte Fragen an die Redaktion zu Desinfec't schreiben Sie gern eine E-Mail an desinfect@ct.de. Support-Anfragen bitten wir möglichst detaillierte Informationen beizulegen, etwa Logs oder Bildschirmfotos. (des) c't

betterCode()

Agentic AI Summit

1. und 2. Juni 2027 • München



Die Konferenz zu KI-gestützter Softwareentwicklung

Der Agentic AI Summit zeigt dir, wie du KI-Tools gewinnbringend einsetzt und wie sich deine Arbeitsweise dadurch verändert. Er zeigt den Weg zur **AI Software Factory.**

Auf dem GenAI Summit tauschst du dich mit Gleichgesinnten über **alle Aspekte** von KI in der Softwareentwicklung aus.

Call for Proposals
bis 28.12.2026

agenticai-summit.bettercode.eu

Veranstalter

iX MAGAZIN FÜR PROFESSIONELLE IT



Bild: Martina Bruns / KI / heise medien

Desinfec’t 2026/27: So legen Sie los

Herunterladen, einrichten, Trojaner jagen: So gehen Sie mit dem komplett überarbeiteten Desinfec’t 2026/27 auf Virenjagd.

Von **Dennis Schirrmacher und Peter Siering**

Die neue Desinfec’t-Version sieht nicht nur anders aus, auch unter der Haube hat sich einiges getan. Es ist weiterhin einfach zu nutzen, führt die eingebauten Scanner an einer kürzeren Leine und sollte Updatezyklen zuverlässiger als früher bewältigen. Eine modernisierte technische Basis aufbauend auf Ubuntu 26.04 LTS und eine grafische Oberfläche mit KDE als Grundlage verbessern die Kompatibilität. Davon profitieren nicht nur Computereinsteiger, sondern auch Malwareprofis.

Obwohl gerade auf den ersten Blick vieles ungewohnt wirken mag, hat sich an der Bedienung und Funktionsweise gar nicht so viel verändert. Dieser Artikel zeigt, wie Sie Desinfec’t 2026/27 herunterladen, betriebsbereit machen und die neue Bedienoberfläche für die Scanner verwenden. Zusätzlich

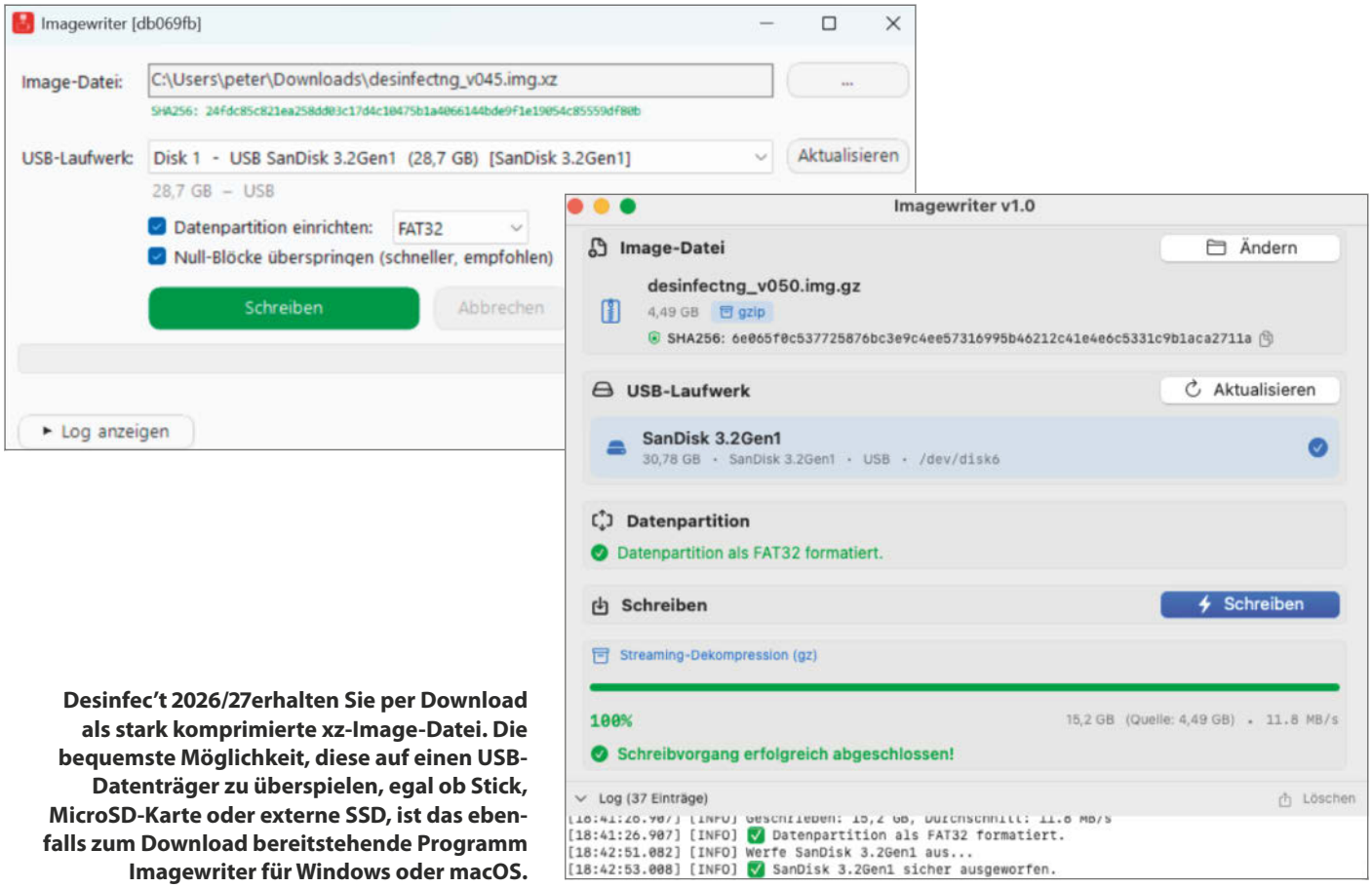
liefert er Tipps, wie Sie von hinzugekommenen Funktionen profitieren und gewährt einen Ausblick darauf, was professionelle Datenforensiker und Malwareanalysten damit anstellen können.

Download

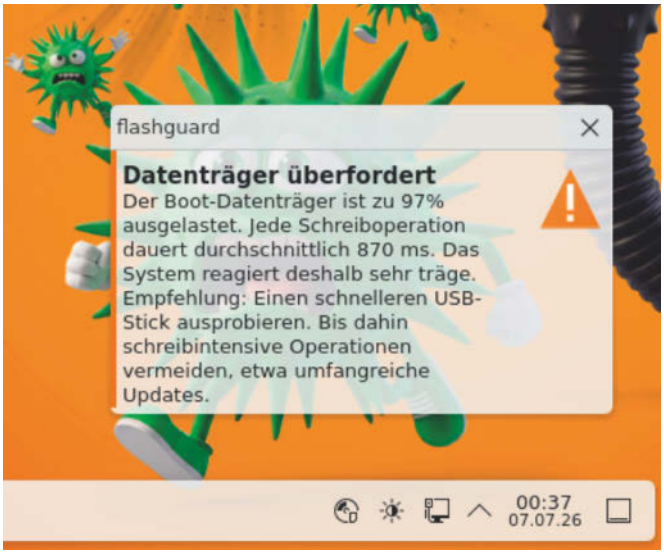
Desinfec't hat erstmals eine eigene Projektseite auf heise online: https://ct.de/desinfect. Dort finden Sie die passenden Download-Links für das Image und den zusätzlich notwendigen „Imagewriter" für Windows oder macOS. Das eigens für Desinfec't entwickelte Programm überträgt das heruntergeladene Image auf USB-Sticks und andere Wechseldatenträger. Danach ist Desinfec't sofort einsatzbereit. Die Projektseite hält obendrein aktuelle Hinweise zu Desinfec't.

Wie daraus schon abzulesen ist: Desinfec't ist keine Anwendung, die Sie unter Windows installieren und starten. Im Image steckt ein spezialisiertes Linux-System, das statt Windows von einem angesteckten Datenträger wie einem USB-Stick bootet. Das bringt den Vorteil mit sich, dass Sie die inaktive Windows-Installation aus einer sicheren Entfernung begutachten können.

Damit Desinfec't optimal läuft, empfehlen wir dringend einen Marken-USB-3.0-Stick oder noch besser eine externe SSD. Der Datenträger sollte mindestens 16 GByte Kapazität haben, besser 32 GByte, weil Desinfec't selbst rund 12 GByte beansprucht. Er sollte flink lesen, vor allem aber muss er parallel ausgeführten Schreibzugriffen gewachsen sein. Gerade bei Billigsticks und Werbegeschenken ist das nur selten der Fall.



Desinfec't 2026/27erhalten Sie per Download als stark komprimierte xz-Image-Datei. Die bequemste Möglichkeit, diese auf einen USB-Datenträger zu überspielen, egal ob Stick, MicroSD-Karte oder externe SSD, ist das ebenfalls zum Download bereitstehende Programm Imagewriter für Windows oder macOS.



Die Achillesferse eines Livesystems ist der Datenträger: Ein kleiner Daemon wacht deswegen permanent über das Wohlbefinden des Datenträgers, von dem Desinfec't gestartet ist. Bei steigenden Fehlerraten oder sich anhäufenden Schreibzugriffen warnt es. Dann sollten Sie den Datenträger gegen ein besseres Exemplar austauschen.

Wenn Sie dieser Empfehlung nicht folgen, müssen Sie damit rechnen, dass Desinfec't gar nicht erst startet oder sich anfühlt, als würde der Computer demnächst einschlafen. Wenn Desinfec't gestartet ist, wacht ein kleines Programm „Flashguard" über das Wohlergehen des Bootdatenträgers und warnt, wenn ihm Schreibzugriffe über den Kopf wachsen oder sich Fehler häufen. Erscheinen fortwährend solche Warnungen, sollten Sie den Stick austauschen.

Desinfec't lässt sich auf 64-Bit-x86-Systemen mit nur 4 GByte RAM starten und benutzen, aber ihm geht dort schnell die Puste aus: Sämtliche Log- und temporären Dateien landen in einem vom Hauptspeicher abgezwackten Bereich, um USB-Sticks nicht mit der Schreiblast zu quälen. Dieser Datenbestand wächst mit umfangreichen Scans. Einen alternativenn Weg Desinfec't auf solchen Rechnern und Windows-PCs mit ARM-CPU einzusetzen, stellt der Artikel auf Seite 36 vor.

Auf heute gängigen PCs mit 8 GByte RAM und mehr fängt das System an, sich wohlzufühlen. Scans, auch mit mehreren Scannern parallel, sind möglich. AVRunner beobachtet, während es Scanner laufen lässt, die wichtigsten Systemressourcen und warnt bei Knappheit – treten solche Meldungen wiederholt auf, haben Sie dem System womöglich doch zu viel zugemutet. Reduzieren Sie die Last. Bedenken Sie, dass auch große Archivdateien problematisch sein können, weil sie im Hauptspeicher entpackt werden müssen.

Einrichten

Das Einrichten eines Desinfec't-Datenträgers mit Imagewriter löscht alle darauf vorhandenen Daten endgültig und ist mit wenigen Klicks erledigt. Das Programm fragt vorher nach und fordert je nach Betriebssystem zusätzliche Rechte an. Gewähren Sie ihm die. Machen Sie es sich einfach und starten Sie das Programm aus dem Ordner, in dem auch das Desinfec't-Image liegt. Imagewriter schlägt dann direkt vor, dieses Image zu verwenden. Andernfalls müssen Sie die Image-Datei von Hand auswählen.

Vergleichen Sie die von Imagewriter automatisch berechnete SHA256-Prüfsumme mit der von uns angegebenen. Das stellt sicher, dass der Download der knapp 4 GByte großen Image-Datei geklappt hat. Prüfen Sie, ob der richtige Datenträger als Ziel gewählt ist. Wenn Sie ihn nach Programmstart angesteckt haben, können Sie das Programm erneut nach solchen Geräten suchen lassen. Alle anderen Optionen belegt Imagewriter passend vor. Sie brauchen nichts zu ändern. Bevor Sie den Datenträger beschreiben, prüfen Sie noch mal, ob es der richtige ist!

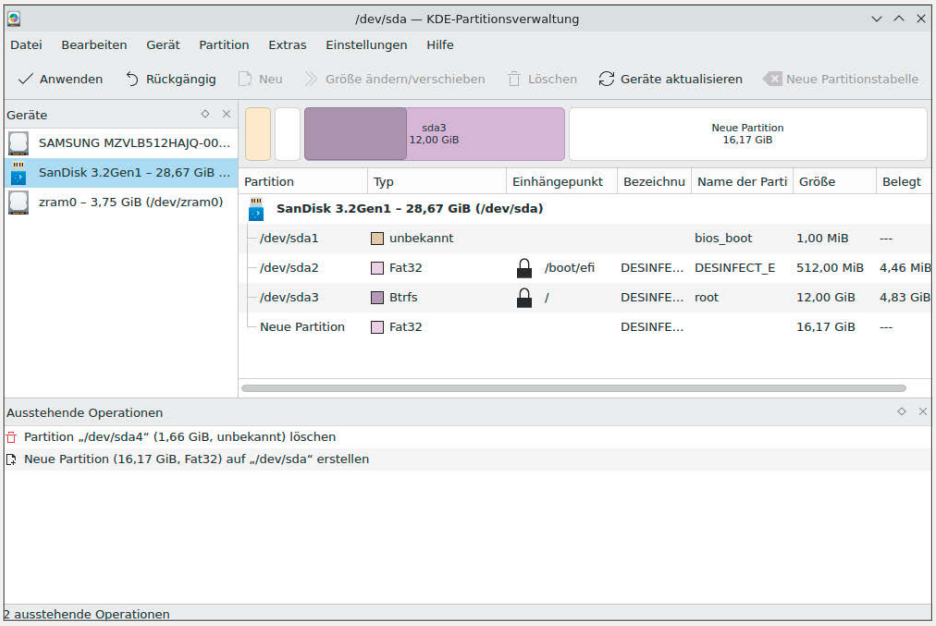
Alternative Methoden, Datenträger mit Desinfec’t einzurichten

Unser Programm Imagewriter nimmt das komprimierte Desinfec’t-Image und schreibt es auf einen USB-Stick, ohne dass Sie es dafür erst dekomprimieren müssen. Es erkennt das Desinfec’t-Image, weil das Image eine Platzhalterpartition namens DESINFECT_D enthält. Findet es die Platzhalterpartition vor, löscht es sie nach dem Schreiben des Images und erstellt über den freien Platz des Datenträgers eine Partition mit FAT-, exFAT- oder NTFS-Dateisystem mit dem Label „DESINFECT_D“ für den Datenaustausch.

Sie können unser Image mit anderen Werkzeugen auf Ihren Datenträger überspielen, solange sie die Daten 1:1 übertragen. Aktuelle Versionen des Gnome Disk Utility (Disks/Laufwerke) schreiben wie Imagewriter direkt die xz-komprimierte Datei. Wenn Sie dd oder andere Tools bevorzugen, müssen Sie die Datei ggf. dekomprimieren. Da die anderen Tools nichts von der Platzhalterpartition wissen, müssen Sie sich selbst darum kümmern, die anzulegen.

Das geht am einfachsten direkt nach dem ersten Booten von Desinfec’t: Starten Sie über das Startmenü unter System als Erstes die KDE-Partitionsverwaltung. Löschen Sie dort die Platzhalterpartition und fügen Sie anschließend eine neue Partition hinzu. Geben Sie ihr den Volumenamen DESINFECT_D. Die Änderungen müssen Sie dabei explizit bei der Partitionsverwaltung mit „Anwenden“ ausführen lassen. Erst beim nächsten Reboot ist die Partition dann automatisch zugänglich.

Sie müssen nicht den gesamten freien Platz dem Datenaustausch widmen. Die KDE-Partitionsverwaltung kann nach dem Löschen der Platzhalterpartition auch zunächst das Desinfec’t-Btrfs (/dev/sda3) im laufenden Betrieb vergrößern – das bietet sich an, wenn Sie das System häufiger nutzen, es selbst erweitern wollen und ohnehin auf einer SSD am USB-Adapter einrichten, die mehr Speicherplatz als ein typischer USB-Stick bereithält.



Das Desinfec’t-Image lässt sich auch mit gängigen Programmen auf einen USB-Datenträger schreiben, das die Daten 1:1 überträgt, etwa dem Gnome Disk Utility. Nach dem Booten hilft dann die KDE-Partitionsverwaltung, den Bereich für den Datenaustausch einzurichten.

Imagewriter richtet automatisch den freien Platz eines Datenträgers für den Datenträgeraustausch ein (DESINFECT_D). Dort können Sie Scanergebnisse ablegen, falls nötig Logs sichern und Dateien ablegen, die Sie von einem verseuchten Rechner retten. Unter Windows wählt Imagewriter statt FAT32 als Dateisystem exFAT, sobald der Datenträgeraustauschbereich größer als 32 GByte wäre; eine alternative Auswahl von NTFS ist möglich, falls Sie das bevorzugen.

Mit handelsüblichen USB-Sticks dauert das Beschreiben mehrere Minuten. Haben Sie etwas Geduld. Grundsätzlich ist das Schreiben von Wechseldatenträgern unter Windows eine wackelige Angelegenheit. Windows lässt, je nachdem, was es auf dem Datenträger beim Anstecken vorgefunden hat, nur ungern die Finger davon – es zeigt womöglich Formatierdialoge an, ignorieren Sie diese. Im Zweifel probieren Sie das Beschreiben ein weiteres Mal oder bemühen Sie nötigenfalls versuchsweise einen anderen PC. Details zu eventuellen Schreibfehlern können Sie im Log finden und uns gern übermitteln.

Eine Warnung am Schluss: Auch Sticks, die den eingangs geschilderten Anforderungen gar nicht genügen, zeigen durchaus brauchbare Schreibraten im Imagewriter. Ein Schreiberfolg garantiert entsprechend keinen erfolgreichen Start. Erst wenn Desinfec't zügig vom Datenträger bootet und anschließend auch rund läuft, können Sie sicher sein, dass Sie ein ordentliches Exemplar erwischt haben.

Starten

Bevor Sie Desinfec't auf einem PC starten, eine wichtige Warnung: Es kann sein, dass allein der Versuch vom PC beziehungsweise vom installierten Windows als Einbruchsversuch registriert wird. Dann werden Sie beim nächsten regulären Start aufgefordert, Wiederherstellungsschlüssel oder Passwörter für BitLocker einzugeben. Diese müssen Sie also vor eventuellen Experimenten unbedingt so gesichert haben, dass Sie ohne Hilfe der Windows-Installation herankommen!

Um das frisch erstellte Desinfec't zu booten, gibt es zwei Wege. Aus dem laufenden Windows heraus oder über die Bootweiche, die die meisten PCs über eine spezielle Tastenkombination zugänglich machen. Auf dem zum Erstellen des Sticks verwendeten Windows-PC können Sie den Start direkt aus dem laufenden System einleiten. Lassen Sie den Desinfec't-Datenträger stecken.

Öffnen Sie dann das Windows-Startmenü, halten Sie die Umschalt-Taste gedrückt, klicken Sie auf „Ein / Aus“ und dann auf „Neu starten“. Nach einiger Zeit landen Sie in einem Menü. Wählen Sie dort den Punkt „Ein Gerät verwenden“ und dann das Medium mit Desinfec't aus (meist „USB HDD“). Nun startet der Computer vom externen Datenträger neu und das Desinfec't-Bootmenü (Grub) erscheint.

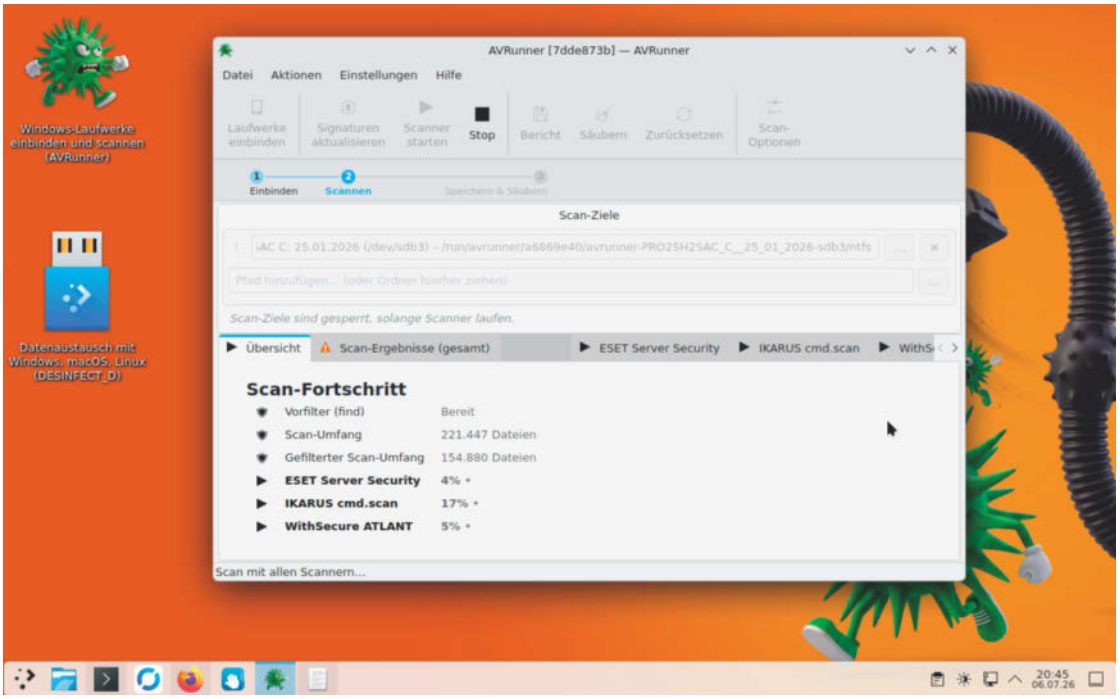
Bei PCs mit Verdacht auf Schadcodeinfektion sollten Sie nicht den Weg über Windows gehen, sondern den Stick vor dem Einschalten anstecken und als Bootgerät auswählen. Die Auswahl erscheint meist, wenn Sie nach dem Einschalten eine spezielle Taste wie F9, F11 oder F12 drücken – idealerweise finden Sie die richtige Taste für einen PC über eine Internetsuche. Widerborstigen Geräten helfen Sie auf die Sprünge, indem Sie Wechseldatenträgern im BIOS/UEFI-Setup Vorrang einräumen. Wenn Sie Erfolg haben, erscheint auch hier das Desinfec't-Bootmenü.

Klappt der Start vom Stick, sehen Sie das Desinfec't-Bootmenü mit vier Einträgen: Der oberste Punkt „Desinfec't GNU/Linux“ ist der richtige. Er startet das System nach wenigen Sekunden auch automatisch. Die anderen Optionen sind für die Fehlersuche oder um den Stick in den Zustand zurückzuversetzen, in dem er sich direkt nach dem Bespielen befand – der Artikel kommt später darauf zurück und auch die FAQ auf Seite 30 enthält weitere Tipps, falls sich Desinfec't komisch benimmt oder nicht startet.

Wenn Sie das Desinfec't-Menü nicht zu Gesicht bekommen, probieren Sie an Ihrem PC weitere USB-Ports durch. Bevorzugen Sie dabei USB-Anschlüsse, die direkt auf der Hauptplatine liegen (meist an der Gehäuserückseite). Vergewissern Sie sich gegebenenfalls an einem anderen PC der Funktionstüchtigkeit Ihres frisch bespielten Datenträgers. Probieren Sie auch USB2-Ports aus, die zwar langsamer, oft aber zuverlässiger funktionieren. Experimentieren Sie gegebenenfalls mit anderen Datenträgern.

Scanhelfer

Beim ersten Start begrüßt Sie der Desinfec't-Desktop mit einem Willkommensbildschirm. Dort können Sie unter anderem die Skalierung der Bildschirmauflösung anpassen, damit Icons auf einem 4K-Monitor nicht winzig erscheinen, und bei mehreren Displays das primäre auswählen. Diese Abfragen erscheinen immer wieder, wenn Desinfec't andere Monitore erkennt, auch wenn Sie die Willkommensbotschaft deaktivieren. Alle dort ausführlicher beschriebenen Programme finden Sie auch im KDE-Startmenü und die wichtigen auch in der Startleiste.



AVRunner bindet Windows-Laufwerke ein und steuert die Scanner in Desinfec't 2026/27. Dabei wirft das Programm nicht nur ein Auge darauf, ob die Scanner das Livesystem zu stark belasten, sondern zeigt immer auch an, wie groß der Scan-Fortschritt ist. Sie können erkennen, ob noch Zeit zum Kaffeekochen oder für andere Unternehmungen bleibt.

Das zentrale Programm ist „AVRunner". Es steuert die integrierten Virenscanner und bindet Windows-Laufwerke nur auf Ihre explizite Anforderung hin ein. Von sich aus macht Desinfec't FAT, exFAT, NTFS und BitLocker-Volumes nicht zugänglich; es verhält sich hier bewusst anders als übliche Linux-Distributionen. Wenn eine Festplatte mit BitLocker verschlüsselt ist, fragt das Programm das BitLocker-Passwort oder den Wiederherstellungsschlüssel ab, sofern diese nötig sind.

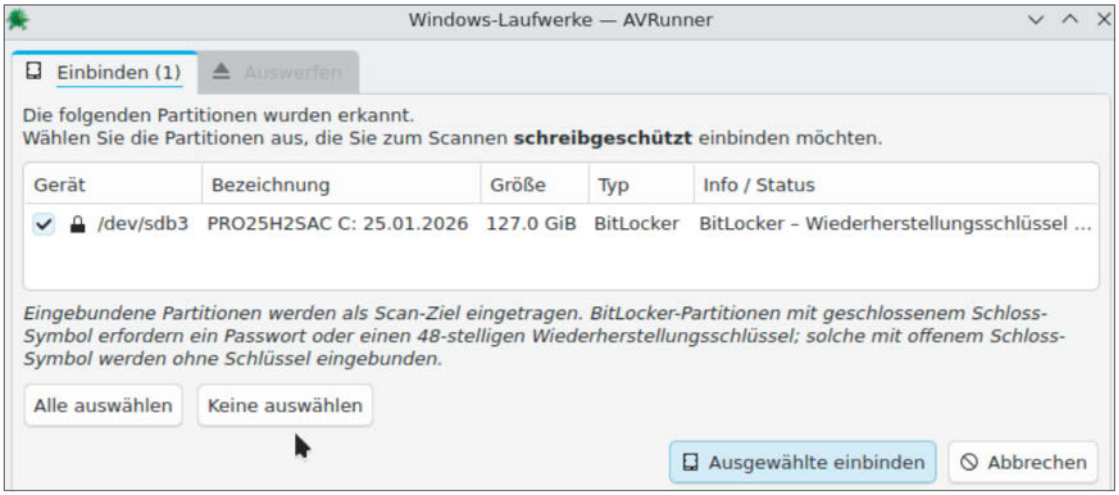
Eingebundene Windows-Laufwerke trägt AVRunner automatisch als Scanziel ein. Sobald mindestens ein Scanziel festgelegt ist, können Sie Scanner einzeln starten oder gleich alle aktiven Scanner loslegen lassen – einige Scanner sind voreingestellt bewusst pausiert, THOR Lite und Yara sind Spezialscanner, die man üblicherweise nicht über ganze Dateibäume jagt, sondern gezielt für die Suche nach bestimmten Dateien nach Verdacht einsetzt. ClamAV als Open-Source-Vertreter ist langsam und neigt zu Fehlalarmen. Aktiv sind ESET Server Security, IKARUS cmd.scan und WithSecure ATLANT.

Im Tab „Übersicht" zeigt AVRunner die Gesamtaktivitäten an und in „Scan-Ergebnisse (gesamt)" fasst das Programm die Ergebnisse über alle Scanner zusammen. Jeder Scanner hat einen eigenen Tab. Dort können Sie im Aktivitätsprotokoll die Ausgaben des Scanners verfolgen und sehen auch Tätigkeitshinweise von AVRunner den Scanner betreffend.

Der pro Scanner vorhandene zweite Tab „Scan-Ergebnisse" zeigt die aus Sicht des Scanners relevanten Ereignisse. Das können Funde infizierter Dateien sein oder auch Hinweise zu Dateien, die der Scanner nicht angefasst hat, etwa weil ihm ein Passwort für verschlüsselte Archive fehlte oder Dateien zu groß waren. Die Tabs zeigen auch das aktuelle Alter der Signaturen an.

Scantipps

Apropos Signaturen: Diese Datenbanken, denen die Scanner Merkmale von Schädlingen entnehmen, sollten bei ernsten Scanläufen aktuell sein. Das stellt ein Klick auf „Signaturen aktualisieren" sicher – Sie können das für einen (im jeweiligen Tab) oder für alle Scanner erledigen lassen (in der Toolbar). Da die Scanner hinter den Kulissen sehr unterschiedlich arbeiten: haben Sie Geduld, bis das Update durch



Um Windows-Laufwerke unter Linux geordnet für Scans zugänglich zu machen, krallt sich AVRunner alle erkennbaren FAT-, exFAT-, NTFS- oder Bitlocker-Partitionen. Wiederherstellungsschlüssel oder Passwörter für letztere erfragt es bei Bedarf.

ist und rechnen Sie nicht damit, hier immer minutenaktuelle Signaturen zu erhalten. Tagesaktualität ist erstrebenswert.

Mit „Scanner starten“ lassen Sie alle nicht pausierten Scanner von der Leine. Die werden nacheinander in der Tab-Reihenfolge die gewählten Scanziele durchsuchen. Pausierte Scanner können Sie einzeln starten, ohne dass Sie deren Pause aktiv beenden müssen. In den Einstellungen unter „Scanner verwalten“ können Sie die Reihenfolge und das Pausieren konfigurieren – dasselbe gelingt über Rechtsklicks auf die Tabs. Ein Scan über große Datenbestände kann Stunden dauern. Um Desinfec’t erst mal kennenzulernen, genügen kleinere Aufgaben.

Dafür ein paar schnelle Tipps: Der unserer Erfahrung nach flinkste Scanner ist IKARUS. Sie müssen nicht alle Dateien, die auf einem eingebundenen Windows-Laufwerk liegen, scannen lassen – ein Klick auf die drei Punkte in der jeweiligen Zeile des Scanziels erlaubt die Auswahl eines Ordners. In den Optionen schlummern weitere Abkürzungen: Über Vorfilter kann AVRunner den Scannern einen gefilterten Ausschnitt der Scanziele vorspielen, um zum Beispiel nur ausführbare Dateien, jüngst geänderte Dateien oder nur Dateien bis zu einer gewissen Größe zu scannen.

Bevor AVRunner die Scanner auf Windows-Laufwerke loslässt, filtert es Hardlinks aus. So werden Dateien nicht unnötig oft gescannt. Außerdem ermittelt das Programm, wie viele Dateien zu bearbeiten sind. Ein spezieller Monitorprozess kann so beobachten, wie weit ein Scanner mit der Arbeit ist. Für Sie als Nutzer ist so abschätzbar, wie lang ein umfangreicher Scan wohl noch dauern wird.

Diese Extraarbeit vor dem Scan zahlt sich an mehreren Stellen aus: Sie sehen als Nutzer den Fortschritt. Die Zählung respektive den Fortschritt zeigt AVRunner in den Scanner-Tabs für den aktiven Scanner und auf der Übersichtsseite für alle beauftragten Scanjobs. Am Ende kann AVRunner prüfen, ob ein Scanner unerwartet viele Dateien nicht angeschaut hat – in der aktuellen Implementierung kann es zu geringen Abweichungen kommen, grobe Abweichungen von mehreren Hundert Dateien deuten auf ein technisches Problem hin.

Scanoptionen

Die Optionen verdienen einen ausführlicheren Kommentar: „Scans mit erhöhten Rechten ausführen“ ist nur nötig, wenn Sie mit Desinfec’t auf Linux-Dateisysteme losgehen – AVRunner wählt die Zugriffsrechte für Windows-Laufwerke passend. Wenn Sie VeraCrypt-Volumes scannen wollen, die das Programm von sich aus in den Linux-Dateibaum einbindet, müssen Sie diese Option setzen, und den Mountpunkt von Hand als Scanziel über den Knopf mit den drei Punkten auswählen.

„Ausführliches Protokoll“ sollten Sie nur aktivieren, um einen Scanner genauer zu beobachten, etwa wenn der aussteigt, um der Ursache auf die Schliche zu kommen – idealerweise nur auf einem Teilverzeichnisbaum, um das Log nicht stark anschwellen zu lassen. „Scanner parallel ausführen“ kann auf üppig ausgestatteten PCs die Gesamt-Scanzeit reduzieren. „Alle Partitionen anzeigen“ sollten Sie nur bei Verdacht auf Schädlinge im frühen Bootprozess aktivieren.

Wir haben uns entschieden, keine Beschränkung der Dateigröße für alle Scanner vorzugeben: IKARUS schaut nur Dateien mit einer Größe von bis zu 64 MByte an, die anderen Scanner machen hier keine Vorschriften. Alle lassen wir Archive durchsuchen. PUA-Optionen sind voreingestellt nicht aktiv – weil sie oft nur Fehlalarme produzieren. Auch „Alternate Datastreams (ADS) sichtbar machen“, ist nicht aktiv. Für einen gründlichen Scan eines verdächtigen PCs mit NTFS-Laufwerken würden wir das einschalten und keine weiteren Filter hier aktivieren. Die benutzerdefinierten Vorfilter haben wir bereits erwähnt.

Scanergebnisse

Wenn ein oder mehrere Scanner ihr Werk getan haben, sollten sich die Scanergebnis-Tabs gefüllt haben – dort landen infizierte Dateien oder auch übersprungene und von den Scannern gemeldete Dateien. Die Ergebnislisten enthalten einige nützliche Funktionen: Per Rechtsklick auf eine Datei können Sie diese in der Dateiverwaltung (dem KDE-Explorer) anzeigen lassen und an andere Programme zur weiteren Beurteilung weiterleiten, etwa einen Hex-Editor oder Kommando-Editor oder Kommandozeilenprogramme für die Malwareanalyse in einem Spezialterminal mit Bedienhilfen (AVCompanion). Dort finden Sie auch viele Experten-Tools, die die Artikel ab 46 beschreiben.

Die Ergebnislisten lassen sich nach Dateinamen und Signaturen filtern. Die Filter lassen sich umkehren, sodass Sie sich nach Eingabe von „file too big“ mit einem Klick auf das Symbol hinter dem Suchfeld alle nicht unter diesem Begriff aufgeführten Dateien anzeigen lassen können. Für alle Funde berechnet AVRunner SHA256-Prüfsummen. Ein Doppelklick auf die Prüfsumme öffnet den Onlinedienst VirusTotal im Browser und zeigt eventuell dort über die Datei vorliegende Informationen. AVRunner lädt keine Dateien zu VirusTotal hoch, das müssen Sie bei Bedarf selbst erledigen; Tipps dazu liefert der Artikel auf Seite 40.

Um die Ergebnisse von Scanläufen zu konservieren, können Sie AVRunner mit dem Button „Bericht“ anweisen, eine Zusammenfassung als Datei zu speichern. Es schlägt als Format dafür HTML vor, Sie können aber auch JSON verlangen, um Berichte mit eigenen Tools später weiterzuverarbeiten oder anders aufzubereiten.

Die Berichte landen standardmäßig auf dem DESINFECT_D-Datenaustauschbereich des Sticks, wenn der unseren Empfehlungen folgend angelegt worden ist. Wenn Sie AVRunner nach einem Scan beenden und dabei Schädlinge gefunden oder Dateien übersprungen worden sind, ohne einen Bericht zu speichern, warnt das Programm. Mit „Zurücksetzen“ können Sie die Ergebnisse verwerfen und andere Scanziele für weitere Läufe eintragen.

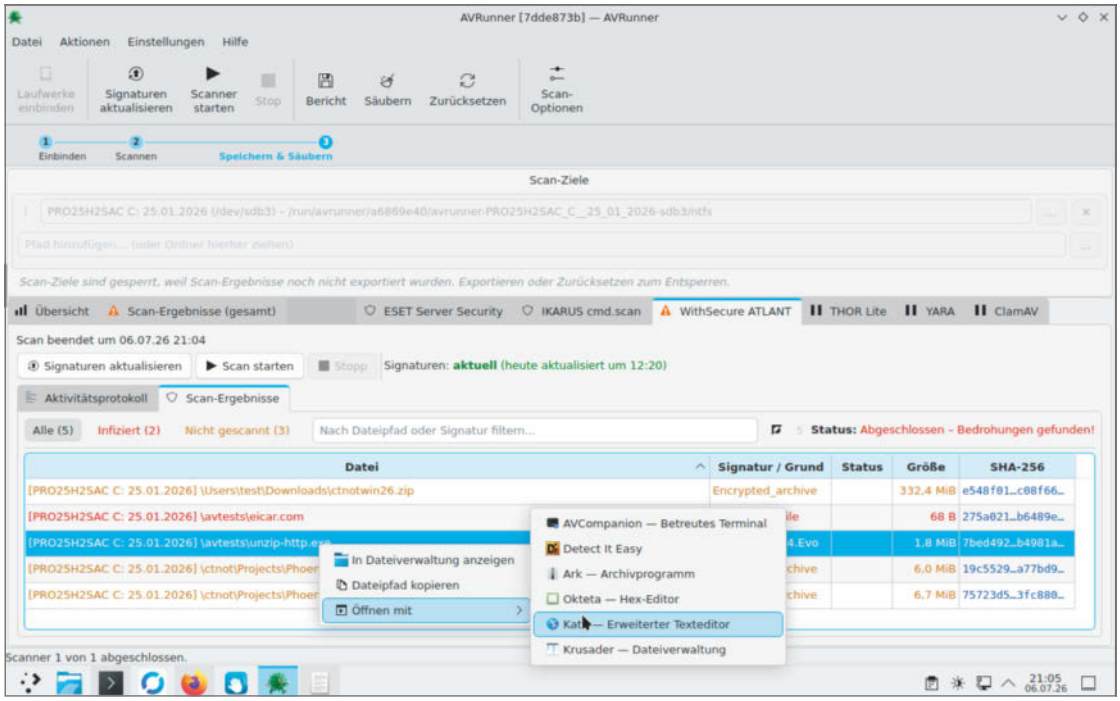
Wir haben für die erste Veröffentlichung den Kampf gegen KDE und Ubuntu verloren, um zuverlässig Stromsparmaßnahmen und Bildschirmabschaltung aus AVRunner heraus zu steuern – immer wieder gerieten gesperrte Desktops in den Weg. Desinfec’t schaltet deshalb all diese Maßnahmen systemweit ab.

Für Scans, deren Ende Sie nicht abwarten wollen, gibt es im „Aktionen“-Menü die Funktion „Scanner starten und herunterfahren“. Sie startet die Scanner nacheinander oder parallel auf den konfigurierten Scanzielen, speichert die Ergebnisse, als hätten Sie selbst einen „Bericht“ verlangt und fährt den PC herunter. Im Fall eines Fehlers unterwegs bleibt der PC eingeschaltet.

Scannachlese

Bei umfangreichen Scans mit mehreren Scannern kann es vorkommen, dass das in der Übersicht als Fazit angezeigte Ergebnis von den Einschätzungen einzelner Scanner abweicht. WithSecure ATLANT weist übersprungene Dateien in seiner Ausgabe als „infiziert“ aus. AVRunner differenziert in seiner Bewertung über alle Scanner und meldet solche Funde lediglich als „übersprungen“. Das gleicht das Verhalten an das der anderen Scanner an. Ansonsten meldet AVRunner die Dinge, wie sie sind.

Sollten die Scanner Schädlinge gefunden haben, kann AVRunner helfen, diese unschädlich zu machen. Der Säubern-Button in der Toolbar öffnet einen Dialog, in dem Sie für jede Datei entscheiden können, ob an ihren Dateinamen „_desinfected“ angehängt werden soll. So verhindert Desinfec’t minimalinvasiv, dass die Windows-Installation die Datei ausführt, etwa weil sie in einem der zahlreichen



Nach einem Scanlauf fasst AVRunner die Ergebnisse zusammen. Laufen mehrere Scanner, ohne etwas zu beanstanden, dürfte ein System sauber sein. Wenn es zu Funden kommt, können Sie per Kontextmenü detaillierte Informationen einholen. Optional sind das Speichern eines Berichtes und das Säubern durch Umbenennen von infizierten Dateien.

Winkel von Windows automatisch gestartet wird. Das ist allerdings keine gründliche Reinigung, sondern eher ein Notbehelf, um eine Windows-Installation noch mal starten zu können, ohne dass die Schädlinge gleich wieder aktiv werden können.

AVRunner bindet sämtliche Windows-Datenträger für Scans ausschließlich lesbar ein. Nur während des Säuberns macht es sie kurzzeitig schreibbar zugänglich, sonst wäre das Umbenennen nicht möglich. Nehmen Sie eventuelle Warnungen dabei ernst: Nicht jedes NTFS-Laufwerk lässt sich sicher beschreiben, wenn Windows nur im Schnellstart steckt oder im Ruhezustand beendet wurde. Bei Warnungen sollten Sie diese Operation also nicht leichtfertig, sondern nur dann ausführen, wenn Sie es wirklich mit einem infizierten System zu tun haben und keine andere Wahl bleibt.

Scan-Orientierung

Im neuen Desinfec't ist AVRunner die zentrale und einzige komfortable Stelle, um Windows-Datenträger mit FAT, exFAT, NTFS und BitLocker einzubinden. Das in vielen Linux-Distributionen aktive automatische Einbinden haben wir bewusst stillgelegt. AVRunner bemüht sich, den Datenträgern in seiner Oberfläche sprechende Namen zu verpassen. Das klappt besonders gut, wenn diese in Windows klare Bezeichnungen erhalten haben. Die Laufwerksbuchstaben zeigt Desinfec't nicht an – das würde spätestens bei mehreren Windows-Installationen auf den Datenträgern uneindeutig sein.

Von AVRunner eingebundene Windows-Datenträger sind in der grafischen Oberfläche KDE als Ort unter demselben Namen sichtbar, wie er in den Scanzielen verwendet wird. Sie können AVRunner beim Verlassen anweisen, die Laufwerke über das Programmende hinaus eingebunden zu lassen: im Dateimenü gibt es dazu „Beenden, Laufwerke eingebunden lassen“ und eine zweite Option, um das sogar beschreibbar zu tun. Beim nächsten Start räumt AVRunner solche eingebundenen gebliebenen Laufwerke von sich aus ab. Achtung: Was Linux-Tools bei schreibenden Zugriffen auf Windows-Laufwerke anrichten, liegt in Ihrer Verantwortung. Nutzen Sie das nur mit äußerster Vorsicht!

Das neue Desinfec't zieht nur Updates aus unseren Paketquellen. Sie können aber per Klick in Discover (der Bedienoberfläche für Paketinstallationen) die Ubuntu- und Mozilla-Quellen aktivieren. Beachten Sie aber, dass umfangreiche Updates schwache Sticks stark strapazieren und bei wahlloser Paketinstallation durchaus Kernfunktionen von Desinfec't leiden könnten – mit dem im Folgenden noch beschriebenen Zurücksetzen auf Werkseinstellungen können Sie ein mit Paketinstallationen verkonfiguriertes Desinfec't in den Zustand beim Bespielen des Sticks zurückversetzen, freilich unter Verlust Ihrer Änderungen.

Für den Fernzugriff auf Desinfec't steckt jetzt RustDesk im Paket. Das passende Gegenstück ist für macOS, Windows und Linux zu haben. Der Wechsel schien angezeigt, weil RustDesks Support für Wayland bereits nutzbar ist und es als Open-Source entwickelt wird. Auf Seite des Helfenden ist es inzwischen nötig, eine Anmeldung bei Google, Microsoft oder GitHub vorzunehmen, um die öffentlichen RustDesk-Server zu verwenden. Für Kommandozeilenfans ist ein SSH-Server eingebaut. Da weder die Konten für „root" noch „desinfect" ein Passwort haben, ist der Zugang in einem frischen, unveränderten Image erst nach Setzen ebensolcher möglich.

Fehlerhelfer

Für den Fall, dass das Starten vom eingerichteten Datenträger nicht klappt, enthält das Bootmenü einige Helfer. Besonders nützlich sind die unter „Desinfec't-Helfer". Die beiden Optionen, die mit „Schreibschutz" beginnen, starten das System so, dass sämtliche Schreibzugriffe nicht auf dem Datenträger landen, sondern im RAM (technisch via OverlayFS). Das heißt, dass Änderungen beim Neustart vergessen werden. Sie helfen auch herauszufinden, ob die Schreibleistung eines Sticks nicht genügt. Klappt ein Boot mit Schreibschutz, aber kein regulärer, haben Sie es mit einem schreibschwachen Stick zu tun.

Der Schreibschutz ist auch auf PCs nützlich, die so schmuddelig sind, dass Sie Übergriffe auf Desinfec't ausschließen wollen, oder wenn Sie Dinge ausprobieren wollen, ohne dass Desinfec't Schaden nimmt. Zwei Ausgangspunkte bieten sich für solche Boots an: „Werkseinstellungen" entspricht dem Zustand direkt nach dem Beschreiben des Datenträgers. „Aktueller Zustand" enthält alle Änderungen, die Sie beim letzten regulären Start vorgenommen haben, wie etwaige Signaturupdates und Updateinstallationen.

Die Option „Wiederherstellen: Werkseinstellungen" setzt den Stick auf den Zustand direkt nach dem Bespielen mit dem Image zurück. Achtung: Dabei gehen sämtliche Änderungen, die Sie an der Konfiguration gemacht haben, alle nachinstallierten Pakete und Signaturupdates verloren. Unter der Haube wird auf einen Btrfs-Snapshot zurückgeschaltet. Die Partition für den Datenaustausch (DESINFECT_D) bleibt dabei unangetastet.

Die mit „Experte:" eingeleiteten Optionen sind für Linux-Flüsterer hilfreich, um Fehler beim Starten zu diagnostizieren oder den Start des GUI zu verhindern. „Erweiterte Optionen" bringt jedes Ubuntu mit. Sie tauchen nach Kernel-Updates ohnehin auf. Deswegen haben wir sie nicht herausoperiert – beide dürften für Desinfec't-Nutzer eher uninteressant sein.

Wie erwähnt, landen Systemlogs und auch die Protokolle der Scans nur in temporärem Speicher. Das heißt, dass sie nach einem Neustart von Desinfec't nicht mehr vorhanden sind. Für die Hauptaufgabe, nämlich das Scannen von Windows-PCs, erzeugt AVRunner auf Wunsch Berichte im HTML- oder JSON-Format – der „Bericht"-Button oder der gleichnamigen Menüeintrag initiieren das. Diese landen auf dem Datenaustauschbereich des Sticks (DESINFECT_D) und überleben Neustarts. Das gilt auch für alle Dateien, die Sie dort selbst ablegen.

Wenn Sie zum Beispiel für Bugreports an uns oder eigene Experimente Logdateien des Systems aufbewahren wollen, bietet AVRunner im Hilfemenü die Funktion „Log-Export" an. Sie haben die Wahl, ob Sie nur die Logs der Scanner und des Scan-Vorgangs unter /var/log/avrunner sichern lassen oder einen ausführlichen Debug-Bericht, der auch Absturz-Backtraces von AVRunner einschließen kann. Achtung: Diese Berichte können persönliche Daten enthalten. Die Exporte landen als Zip-Archiv auf dem Datenaustauschbereich des Sticks.

Aussichten

Was technisch hinter dem neuen Desinfec't steckt, welche Entscheidungen wir bei der Neuentwicklung zu treffen und welche Probleme zu lösen hatten, beschreiben die Artikel auf Seite 82 und 92 detaillierter. Wenn Ihnen etwas auffällt, wenn Sie etwas vermissen oder etwas nicht funktioniert, freuen wir uns über Feedback. Sie finden über die Projektseite ein Forum, einiges Feedback dort ist bereits in die Version 2026/27 eingeflossen. Gern können Sie auch per E-Mail mit uns Kontakt aufnehmen: desinfect@ct.de.

(des) c't

Desinfec't:
ct.de/wmzt



Desinfec’t 2026/27 im Nu einsetzen

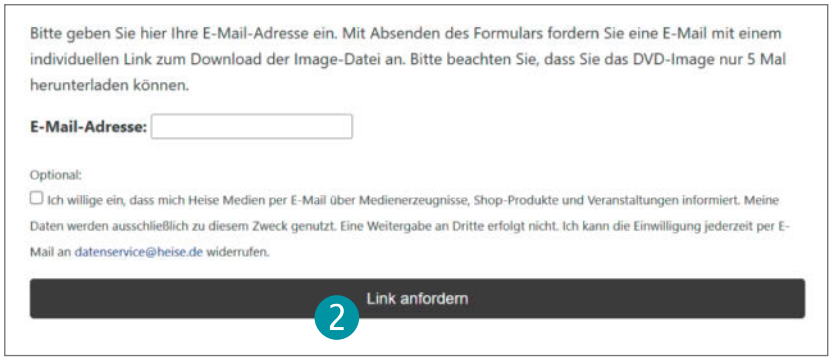
Um mit dem c’t-Sicherheitstool einen PC zu untersuchen, müssen Sie es nur herunterladen und auf einem USB-Datenträger installieren. Mit dieser Anleitung ist das gar nicht schwer und in wenigen Minuten erledigt.

Von **Dennis Schirrmacher**

Herunterladen, entpacken, installieren und starten. Das sind die grundlegenden Schritte, die Sie vor dem eigentlichen Scan eines Windows-Computers erledigen müssen. 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 2026/27 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 2026/27 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 2026/27. Wenn Sie das Heft am Kiosk gekauft haben, tippen Sie einfach die URL ct.de/desinfect 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 wie die Kioskkäufer 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.





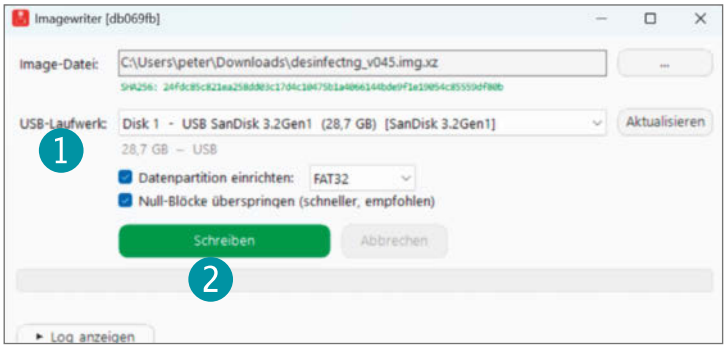
Imagewriter erhalten Sie für Windows und für macOS. Die Programme sind signiert. Sie fordern beim Ausführen erhöhte Rechte an, um Datenträger wie USB-Sticks zu beschreiben. Sie berechnen die auf der Download-Seite angezeigte SHA256-Prüfsumme des Desinfec't-Images automatisch und zeigen sie an.

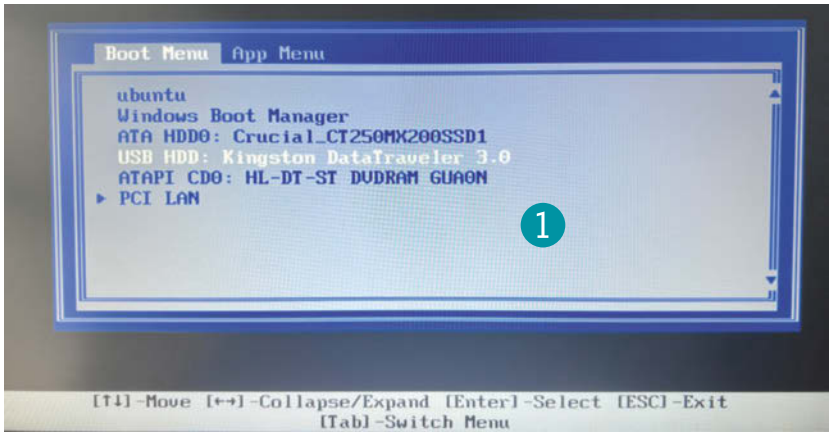
Imagewriter für Windows (EXE, 1,1 MByte, SHA256: 1
654c0dcc6ac9577c82aa890e3c5219fdaf6cae6c6e106f4067a34090a11db6c3, das ist die neue Fassung, die im Forum als imagewriter101.exe-Testversion bereitgestellt wurde)

Imagewriter für macOS (DMG, 600 KByte, SHA256:
a10f67f17c45fca91de3164ada15195310d3213dcbf000dc603e59bbf5945488)

Installationsassistent downloaden: Nun müssen Sie noch den Installer „ImageWriter" unter ct.de/desinfect herunterladen (1). Kopieren Sie ImageWriter in den gleichen Ordner, in dem auch das Image von Desinfec't 2026/27 liegt. Denn nur dann ist das Image vorausgewählt, wenn Sie den Installer starten.

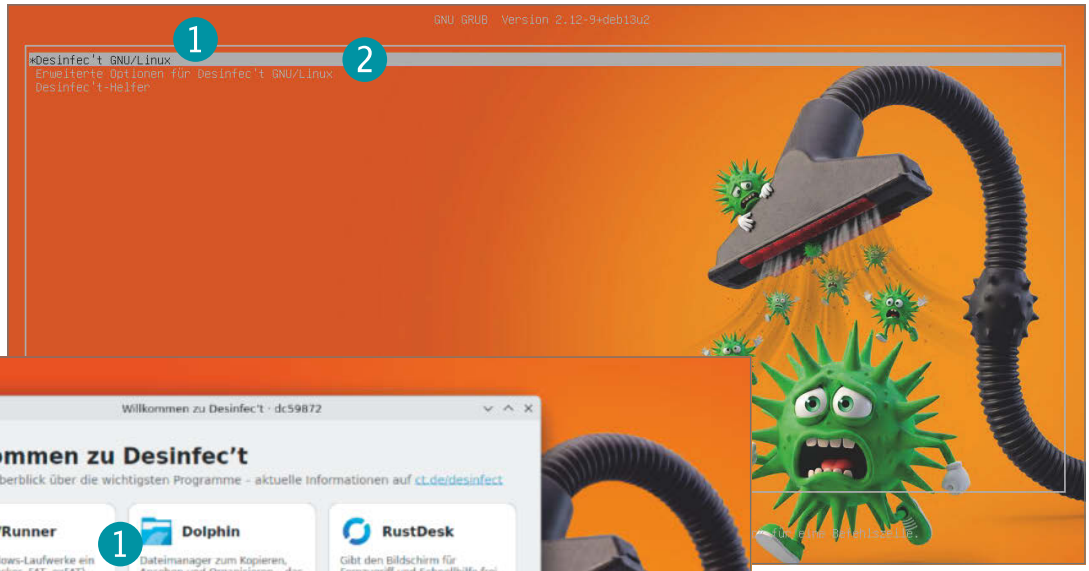
Desinfec't 2026/27 auf USB-Datenträger installieren: Unter „USB-Laufwerk" müssen Sie sicherstellen (1), dass der korrekte Stick, die richtige SSD oder SD-Karte ausgewählt ist. Stimmt alles, müssen Sie nur noch auf „Schreiben" klicken (2), damit die Installation startet.





Boot-Datenträger auswählen: Welche Möglichkeiten es gibt, Ihren PC vom Desinfec't-Stick anstatt Windows zu starten, steht im Artikel auf Seite 10. 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-Datenträger 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 2026/27 starten: Um das System zu booten, wählen Sie den Punkt „Desinfec't GNU/Linux" aus (1). Gibt es beim Start Probleme, können Sie unter „Erweiterte Optionen für Desinfec't GNU/Linux" (2) das Booten im RecoverModus ausprobieren.





Nach dem ersten Start: Um direkt mit einem Virenscan loszulegen, klicken Sie auf „AVRunner" (1), um den Scanassistenten zu starten. Wie es dann weitergeht, zeigt die Bilderstrecke ab Seite 24.

heise academy heise security PRO



Die nächste Angriffswelle kommt mit KI

Wie du dich nicht davon überrollen lässt.

KI verkürzt Reaktionszeiten auf ein Minimum. Lerne, wie moderne Prozesse Risiken deutlich reduzieren.

> Zum kostenlosen Whitepaper
heise-academy.de/hacker-ki



Viren finden und säubern

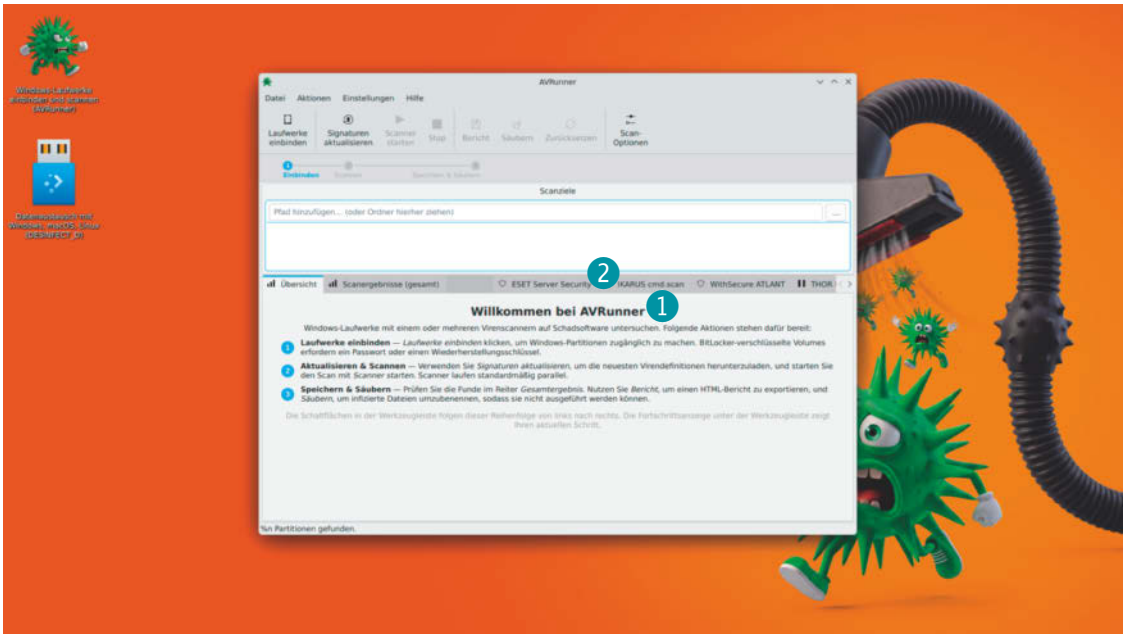
Irgendetwas stimmt mit dem Rechner nicht. War es vielleicht der kürzliche Download? Zeit, der Sache Schritt für Schritt mit Desinfec't auf den Grund zu gehen.

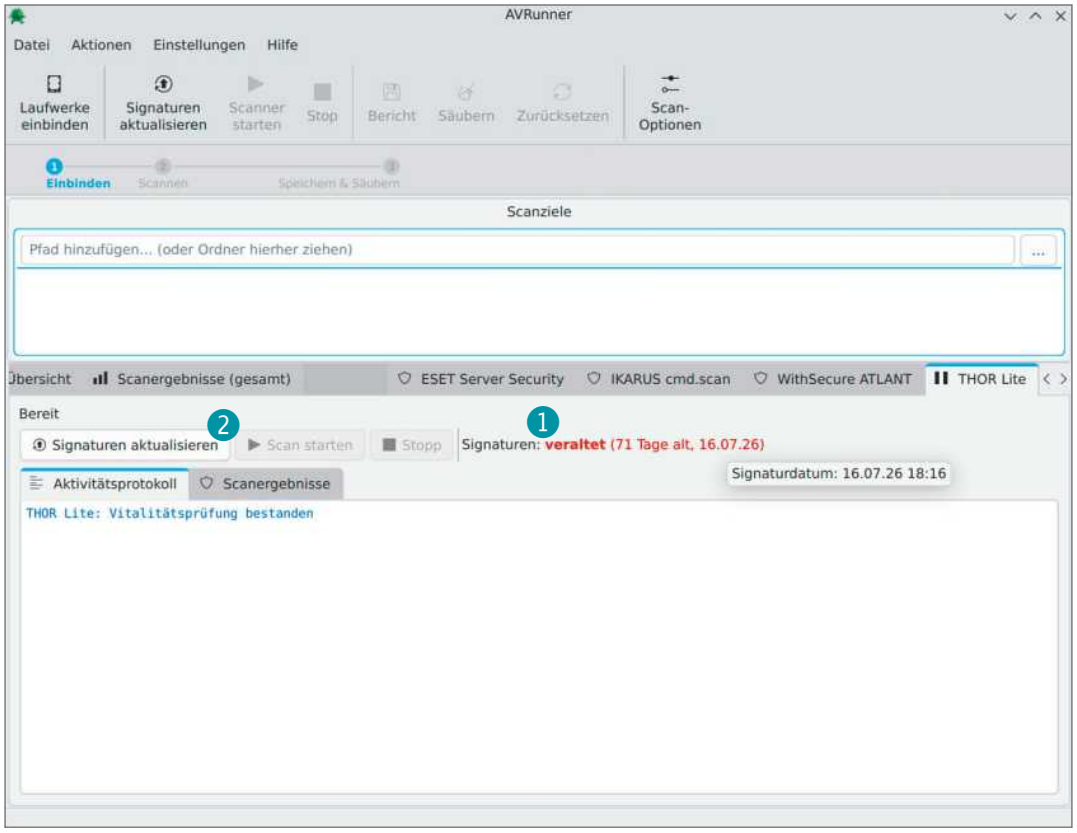
Von **Wilhelm Drehling**

Ein falscher Klick auf einen Mail-Anhang und prompt lädt man eine suspekte Datei herunter. War das vielleicht ein Virus? Zum bereits vorhandenen Bauchweh über diese Missgeschick gesellt sich ein ungewohntes Verhalten des PCs. Der Schreck sitzt tief, doch die Devise heißt ruhig zu bleiben: Schalten Sie den Computer erstmal aus, damit der Schadcode nicht noch mehr Schaden anrichten kann.

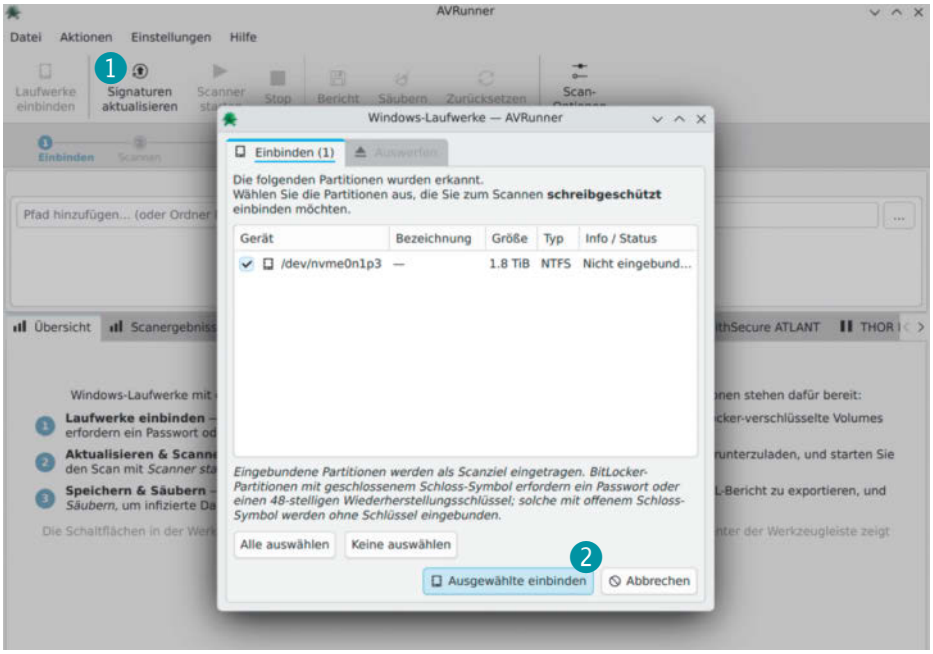
Am sichersten ist es nun, Windows schlafen zu lassen und die Arbeit dem Diagnosetool Desinfec't zu überlassen. Sollten Sie noch keinen Desinfect-Stick haben, müssen Sie einen über einen gesunden Computer erstellen, so wie in der Bilderstrecke ab Seite 20 und ausführlicher im Artikel ab Seite 10 beschrieben. Dort steht auch, wie Sie das Sicherheitstool starten. Läuft Desinfec't auf Ihrem Rechner, kann es losgehen. (wid) c't

Der richtige Ort, um Schädlinge aufzustöbern und Viren außer Gefecht zu setzen, ist der Scanassistent AVRunner (1). Es bringt mehrere Scanner von unter anderem ESET und IKARUS mit, die Ihren PC nach unerwünschten Eindringlingen durchforsten (2).

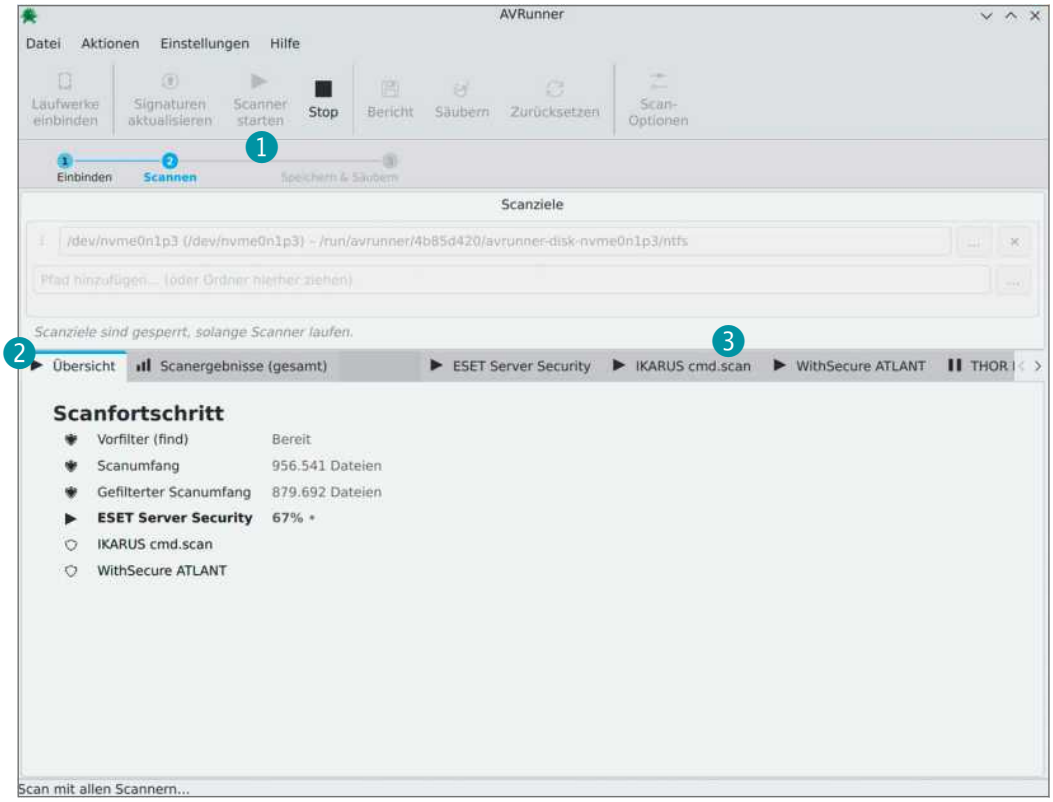




Als nächstes sollten Sie sicherstellen, dass die Scanner auf dem aktuellen Stand sind (1): Mit einem Klick auf „Signaturen aktualisieren“ (2), lädt AVRunner aktuelle Signaturen nach, auf deren Basis die Scanner Viren und schadhafte Dateien erkennen. Das ist wichtig, weil ESET & Co. sonst brandneue Schädlinge übersehen würden.

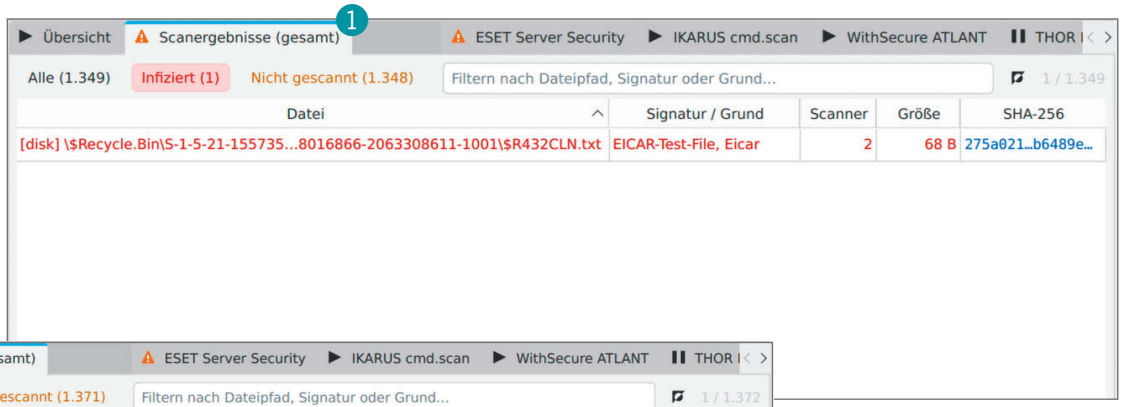


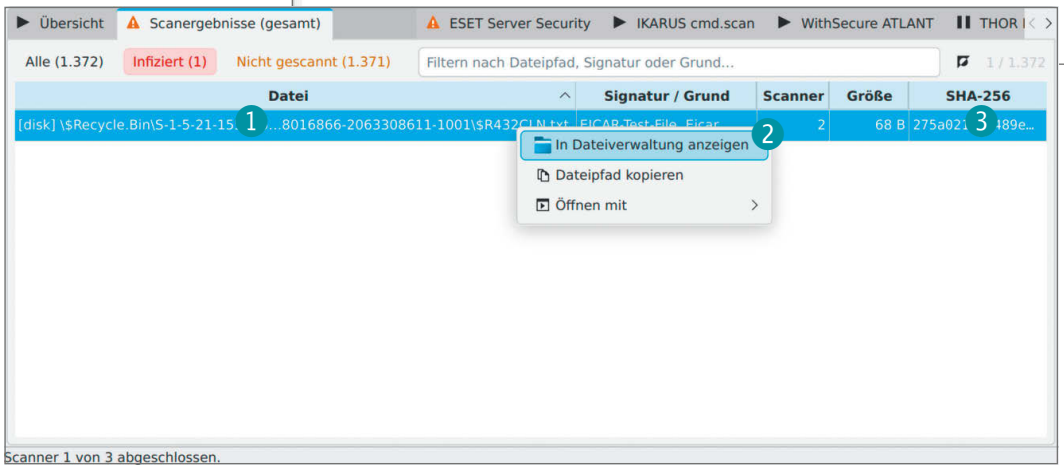
Bevor Sie jedoch die Scanner auf Virenjagd schicken, müssen Sie Ihre Laufwerke einbinden (1), damit die Virenscanner wissen, was sie durchsuchen sollen. Es öffnet sich ein neues Fenster, in dem Ihre Festplatte bereits vorausgewählt ist. Wenn alles stimmt, bestätigen Sie die Auswahl mit „Ausgewählte einbinden“ (2). Verwenden Sie BitLocker als Festplattenverschlüsselung, müssen Sie zum Einbinden der Laufwerke den BitLocker-Schlüssel eingeben.



Nun ist AVRunner bereit, um Ihren PC zu analysieren: Mit Klick auf „Scanner starten“ (1) legen die Scanner los. Dies kann nun je nach der Menge von Dateien und der Schnelligkeit Ihres Computers zwischen einigen Minuten bis hin zu mehreren Stunden dauern. In der Übersicht (2) blendet AVRunner den aktuellen Fortschritt ein, mehr Informationen zu den einzelnen Scans erhalten Sie in den Tabs zu den einzelnen Scannern (3).

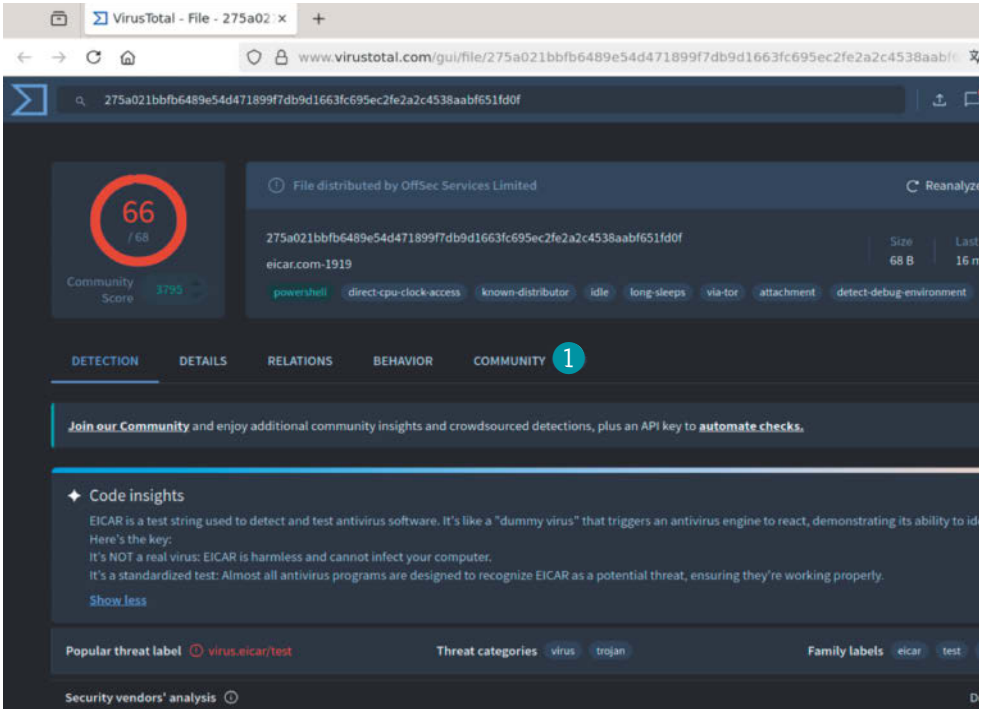
Wenn einer der Scanner einen Fund verzeichnet, so finden Sie diesen unter „Scanergebnisse (gesamt)“ rot hinterlegt (1). Nun können Sie den Fund analysieren und Gegenmaßnahmen ergreifen.

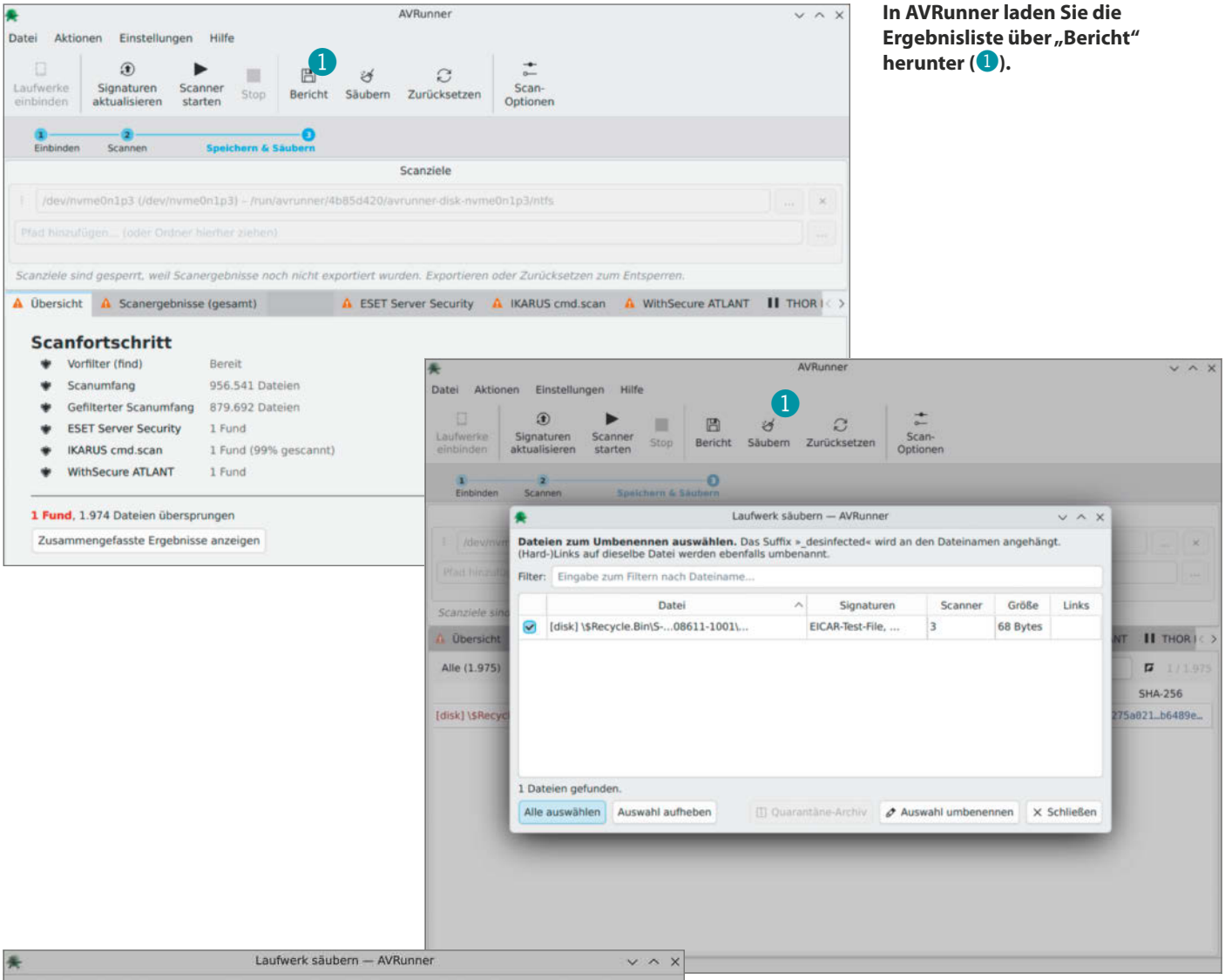




Mit einem Rechtsklick auf den Fund in der Datei-Zeile (1) sehen Sie sich den Ort an (2), wo die Datei liegt. Handelt es sich etwa um eine jüngst von Ihnen aus einem offiziellen Downloadportal heruntergeladene legitime Datei im Download-Ordner, handelt es sich mit hoher Wahrscheinlichkeit um einen Fehlalarm.

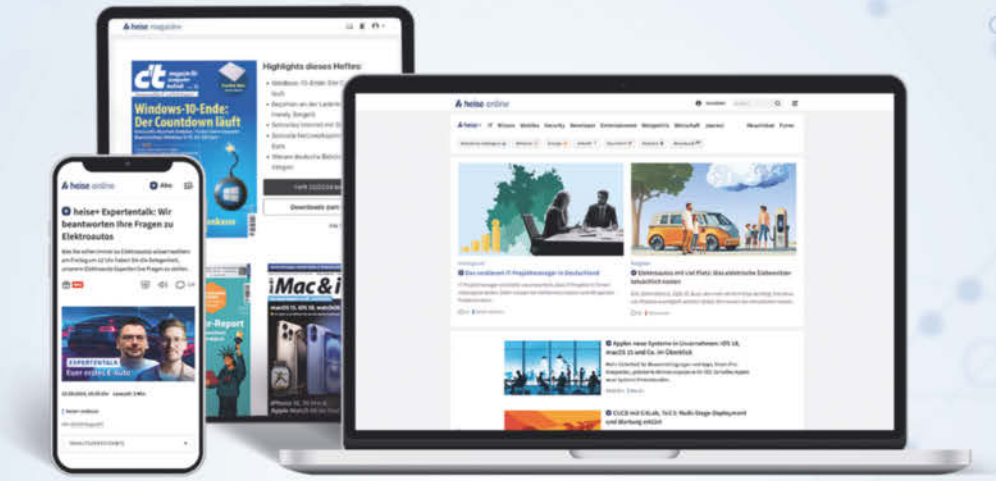
Über den Onlineanalysedienst Virustotal grenzen Sie einen möglichen Fehlalarm weiter ein: Wenn Sie mit einem Doppelklick den Hash-Wert anklicken (Oberer Screenshot 3), öffnet sich die Virustotal-Website mit weiterführenden Informationen zum Fund. Virustotal prüft Dateien mit rund 70 Onlinescannern, so lassen sich fehlerhaft angemerkte Dateien gegenprüfen, als auch Funde bestätigen. Noch ein Tipp: Manchmal sind die Analysen der Schädlinge schwer zu verstehen, häufig hilft ein Blick in die Nutzerkommentare (1), um die Situation besser einschätzen zu können.





In AVRunner laden Sie die Ergebnisliste über „Bericht“ herunter (1).

Viren entschärfen Sie minimal invasiv, indem Sie auf Säubern (1) klicken. Im Hintergrund bleibt die Datei erhalten, sie wird jedoch von AVRunner umbenannt („Auswahl umbenennen“, 2), um sie effektiv unausführbar zu machen. Damit ist die Gefahr aber nur zum Teil gebannt: Desinfec't kann zwar das Ausführen von Viren verhindern, von Schadcode beeinflusste Systemeinstellungen kann es aber nicht auf Knopfdruck wieder geradebiegen. Dementsprechend sollten Sie zur Sicherheit Ihre wichtigsten Dokumente auf dem Desinfec't-Stick sichern und Windows neu aufsetzen. Nur dann ist garantiert, dass wirklich alles sauber ist.



c't Mac&i iX Make: c't Fotografie

Magazin-Abonnenten lesen mehr als 65 % günstiger

heise+

Das digitale Abo für IT und Technik.

Exklusiver Sonderrabatt für Magazin-Abonnenten:

- ✓ Zugriff auf alle kostenpflichtigen Artikel auf heise.de und in der App
- ✓ Alle Ausgaben der Magazine c't, iX, Mac & i, Make und c't Fotografie digital und als PDF verfügbar
- ✓ Wöchentlicher Newsletter mit allen Highlights und Empfehlungen
- ✓ Weniger Werbung für mehr Lesekomfort

Jetzt bestellen unter

heiseplus.de/upgraden

Oder einfach QR-Code scannen

leserservice@heise.de 0511 / 647 22 888

Ein Angebot von: Heise Medien GmbH & Co. KG • Karl-Wiechert-Allee 10 • 30625 Hannover

Desinfec't 2026/27

Die FAQ bündelt die Antworten auf häufig gestellte Fragen.

Von **Dennis Schirrmacher**



Stick bleibt leer

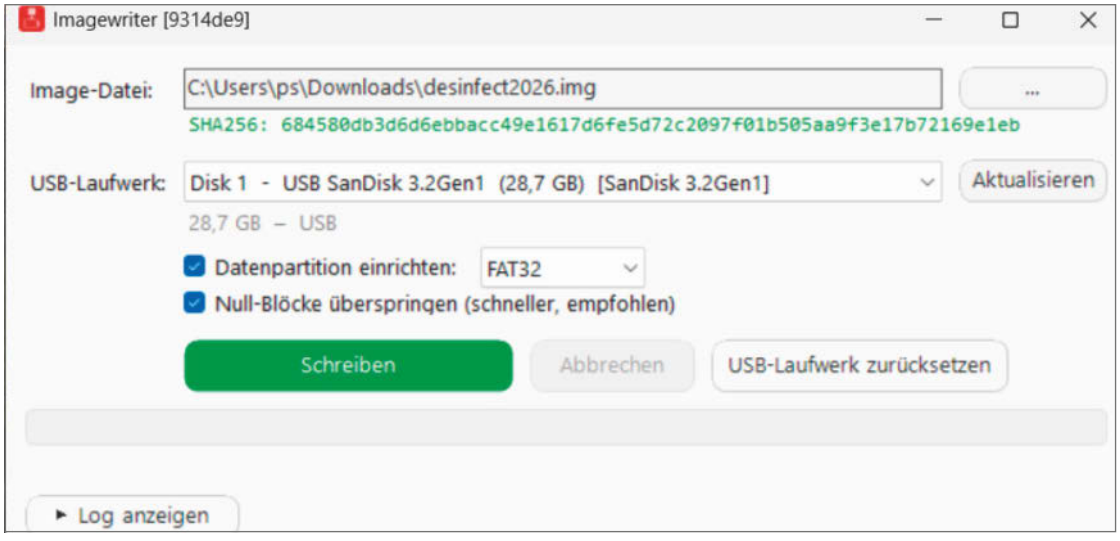
? Ich habe mit dem Imagewriter das heruntergeladene Image auf einen Stick überspielt. Aber der Stick ist hinterher leer. Die Prüfsumme stimmt. Was mache ich falsch?

! Sie machen gar nichts falsch: Das ist das erwartete Verhalten. Imagewriter teilt den Stick in mehrere Partitionen auf. Die, aus denen Desinfec't schließlich bootet, sind nicht sichtbar. Windows und macOS zeigen beim Anstecken beziehungsweise nach dem Beschreiben des Sticks nur die Partition für den Datenaustausch (DESINFECT_D) und die enthält keine Daten, sondern nur eine Datei mit entsprechendem Hinweis.

Stick ruiniert

? Mein mit Desinfec't bespielter Stick ist ruiniert. Er zeigt nur noch einen Teil der Kapazität an und alle Versuche, die volle Kapazität wiederherzustellen, scheitern. Wie repariere ich meinen Stick?

! Wahrscheinlich ist der Stick nicht kaputt, sondern wie unter „Stick bleibt leer" erklärt sind nur Teile nicht sichtbar. Unser Imagewriter bietet die Funktion „USB-Laufwerk zurücksetzen", die die volle



Desinfec't frisst USB-Sticks nicht, es partitioniert nur so, dass sie mit manchen Tools kaputt aussehen. Unser Imagewriter hat deshalb mit „USB-Laufwerk zurücksetzen" eine Funktion, um den Gesamtplatz wieder als eine leere Partition einzurichten.

Kapazität eines Sticks wieder zugänglich macht. Achtung: Dadurch gehen sämtliche Daten auf dem Stick verloren!

Dubioser Imagewriter?

? Woher kommt das Programm Imagewriter, das Sie zum Bespielen der Datenträger mit Desinfec't empfehlen?

! Wir haben das Programm eigens für Desinfec't erstellt. Es kann ohne Dekomprimierung das Image direkt verarbeiten und erkennt eine DESINFECT_D-Platzhalterpartition darin. In diesem Fall vergrößert es die am Ende angelegte Datenaustauschpartition auf die Gesamtkapazität des Datenträgers. Das Programm gibt es für macOS und Windows.

Es gab mal ein Windows-Programm selben Namens, das seit vielen Jahren nicht mehr gepflegt wird und in der Versenkung verschwunden ist. Das gilt auch für das gleichnamige Werkzeug aus dem SUSE-Distributionsbaukasten. Diese älteren Imagewriter sind nicht mit dem Desinfec't-Image kompatibel.

Imagewriter scheitert

? Mir gelingt es auf keinem meiner PCs mit Windows 10 und eurem Imagewriter einen Desinfec't-Stick zu erstellen. Gibt es Alternativen?

! Sie können jedes Programm verwenden, das direkt komprimierte Images auf einen Datenträger schreiben kann. Es eignet sich zum Beispiel Rufus. Wenn Sie andere Programme verwenden wollen, müssen Sie das Image unter Umständen vorher dekomprimieren. Beachten Sie bitte, dass Sie anschließend zu Fuß auf dem Datenträger den Bereich für den Datenaustausch (DESINFECT_D) einrichten müssen. Der Artikel auf Seite 10 erklärt im Kasten „Alternative Methoden, Datenträger mit Desinfec't einzurichten“ die nötigen Schritte im laufenden Desinfec't.

Auswahl beim Booten

? Wenn ich meinen PC boote und per Hotkey das BIOS-Bootmenü aufrufe, zeigt der beim neuen Desinfec't zwei Partitionen zur Auswahl. Welche ist die richtige?

! Viele UEFI-BIOS-Implementierungen bieten alle FAT32-Partitionen eines USB-Datenträgers an, auch wenn nur eine davon die für den EFI-Boot interessanten Daten – das Verzeichnis „EFI“ – enthält. Im Fall eines Standarddatenträgers mit Desinfec't 2026/27 ist die als „Partition 2“ beschriebene Auswahl die richtige zum Starten. „Partition 4“ enthält den für den Datenaustausch eingerichteten Bereich mit dem Namen DESINFECT_D.

Abbruch beim Booten

? Ich habe das Image auf meinen Stick aufgespielt, die Prüfsumme hat gepasst und beim Schreiben gab es keine Fehler. Trotzdem hagelt es beim Booten vom frischen Stick kryptische Fehlermeldungen, die sehr nach Linux riechen. Was läuft verkehrt?

! Die wahrscheinlichste Ursache ist, dass Sie einen USB-Stick verwenden, dessen Zuverlässigkeit zu wünschen übrig lässt. Das gilt vor allem dann, wenn die Meldung von Start zu Start variiert. Testen Sie andere USB-Ports, besonders die direkt am Mainboard, versuchen Sie bewusst auch „langsame“ USB-2.0-Ports (die nicht blau sind). Wenn das alles nicht hilft, probieren Sie bitte einen anderen Stick.

Stick überlastet

? Nach dem Start von Desinfec't erhalte ich immer wieder Warnungen eines Programms „Flashguard“, der Stick sei überlastet. Ich habe einen riesen großen 128-GByte-Markenstick, das kann doch nicht sein.

! Eine verbreitete Marke ist bei Sticks leider kein Garant für eine gute Qualität. Die Speicherkapazität spielt keine Rolle. Auch sagen hohe Schreib- und Leseraten nichts darüber aus, ob ein Stick mit Desinfec't gut funktioniert. Letztlich ist die Anzahl andauernder kleinteiliger Schreibzugriffe das entscheidende Kriterium – IOPS kommen dem nahe, doch wir haben auch Sticks gehabt, die in dieser Disziplin sehr gut ablieferten, aber trotzdem nicht gut liefen. Deswegen gilt: ausprobieren. Tendenziell warnt Flashguard zu früh. Das heißt, seltene Warnungen sind kein Problem. Die Einschätzungen, die Flashguard mit den Meldungen anzeigt, geben Empfehlungen.

Ein paar Tipps, die sich aus dem Feedback ergeben haben: Tendenziell lieber kleine Sticks mit 16 oder 32 GByte zuerst probieren. Je neuer und größer,



Desinfec't ist wählerisch, was den USB-Datenträger angeht. Bei uns haben sich SanDisk Ultra 32 GB, MicroSD-Karten der Klasse A2 im USB-Adapter, ausgemusterte SSDs oder Billig-SSDs bewährt. Leser berichten auch, dass sogar aus Notebooks ausgeschlachtete Magnetplatten gut funktionieren.

umso eher eignen sich Sticks nicht. Wenn ohnehin eine alte SSD herumliegt, ist die mit USB-Adapter meist besser. Neu gab es solche bei Redaktionsschluss für rund 35 Euro zusammen für Adapter und eine 128 GByte große Billig-SSD. Wir nutzen auch MicroSD-Karten in einem USB-Stick-artigen Adapter – für diese Speichermedien gibt es Qualitätskriterien, A2 ist zu bevorzugen, aber auch A1 ist schon besser als viele USB-Sticks. Qualitätskriterien für die MicroSD-Karten-Adapter gibt es leider keine. Hier hat sich Markenware bei uns bewährt.

Ein Leser wies im Desinfec't-Forum darauf hin, dass er Desinfec't erfolgreich auch mit einer 2,5-Zoll-Magnetfestplatte verwendet. Auf die Idee waren wir nicht gekommen und haben es ausprobiert: Es klappte bei uns auch mit einer 5400-U/min-Magnetfestplatte am USB-Adapter, den wir für SATA-SSDs verwenden. Allerdings genügte die Stromversorgung nicht für alle Platten, die wir in der Schublade fanden.

Läuft super lahm

? Ich habe länger einen Stick gesucht, mit dem Desinfec't bootet. Jetzt schlägt „Flashguard" an und das System bedient sich super zäh. Wieso läuft das so langsam?

! Desinfec't 2026/27 lässt sich bei einem gesunden Datenträger im Rahmen der Möglichkeiten der Hardware „normal" bedienen. Auf Systemen mit wenig Hauptspeicher (unter 16 GByte RAM) kommt es natürlich an seine Grenzen, wenn Sie während der Scans munter durchs Web surfen, Tabs im Browser stapeln und gleichzeitig drei Scanner laufen. Wenn hingegen jeder Klick zur Geduldsprobe wird, ohne dass Scanner arbeiten, haben Sie noch keinen brauchbaren Stick gefunden.

Stick testen

? Sie schreiben die ganze Zeit, dass die Sticks zu lahm sind. Wie kann ich denn testen, ob es am Stick oder an irgendwas anderem liegt?

! Desinfec't bietet im kurz nach dem Systemstart angezeigten Grub-Menü Optionen an, die dabei helfen. Sie haben rund 30 Sekunden Zeit, wenn das Menü erscheint. Drücken Sie eine der Tasten, um den Cursor hoch oder runter zu bewegen, damit unterbrechen Sie den automatischen Start. Unter „Desinfec't-Helfer" finden Sie die passenden Optionen für einen Start mit anderen Parametern.

Die erste, „Systemschreibschutz: aktueller Zustand“ ist die richtige. Sie lässt Desinfec’t normal starten, es führt aber keine Schreibzugriffe auf den Stick aus, sondern leitet die vollständig in den Hauptspeicher um. Wenn Ihr PC so annehmbar schnell den Desinfec’t-Desktop zeigt und sich dort auch einige Minuten benutzen lässt, haben Sie die Gewissheit, dass der Stick das bremsende Element ist.

Alten Desinfec’t-Stick verwenden

? Wie passen die Anforderungen des neuen Desinfec’t zu den von heise vertriebenen Sticks für frühere Versionen. Eignen sich die?

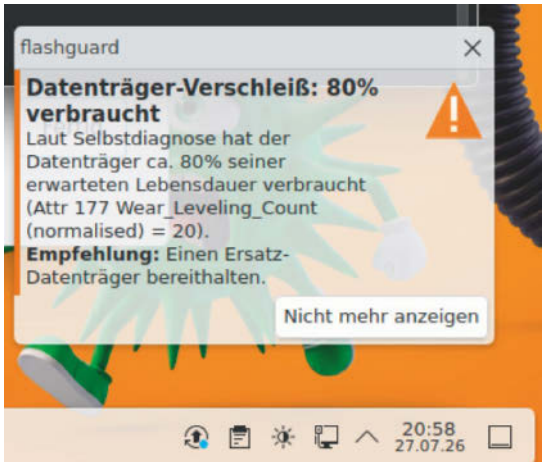
! Teils, teils. Wir testen die angebotenen Sticks selbstverständlich mit der jeweils aktuellen Desinfec’t-Version. Im Lauf der Jahre haben die Kollegen des heise shop diverse Chargen ausgeliefert, sodass es keine einfache Antwort gibt. Die Ansprüche, die das System an die Sticks gestellt hat, waren im Vergleich mit der aktuellen Fassung moderater. Die letztjährigen Sticks scheinen sich unserer Erfahrung nach leider schlecht zu eignen. Ältere Sticks haben in unseren Stichproben besser funktioniert.

Stürzt ab

? Ich habe die Tipps nachvollzogen, um einen nutzbaren Stick zu finden, aber Desinfec’t stürzt auf meinem PC ständig ab. Gibt es Optionen?

! Wenn ein Problem mit dem Stick ausgeschlossen ist, idealerweise Ihr Stick an anderen PCs tadellos funktioniert, könnte eine Unverträglichkeit von Desinfec’t mit bestimmten Hardwarekomponenten ursächlich sein. Wir sichten eingehende Fehler auf Komponenten, die mehrfach genannt werden, und versuchen solchen Problemen nachzugehen. Im Desinfec’t-Forum finden Sie entsprechende Nachfragen der Redaktion. Sollten wir Lösungen finden, werden wir dort und auf der Projektseite Hinweise dazu veröffentlichen (siehe ct.de/wjps).

Sie können eine weitere Bootoption ausprobieren, die verhindert, dass Desinfec’t für moderne Grafikkarten passende Treiber lädt. Sie finden dort „Test: ohne Graffikkartensupport“. Wenn sich das System nun normal bedienen lässt, bleibt für solche Systeme – dem Feedback anderer Leser nach oft mit Nvidia-Grafikkarte – leider nur diese Startmethode übrig.



Flashguard wacht über den Gesundheitszustand des Desinfec’t-Boot-Datenträgers. Tendenziell warnt es früh. Wenn sich das System zäh bedient, sollten Sie die Empfehlungen ernst nehmen.

Image ansehen

? Nach dem Download habe ich die Image-Datei entpackt und wollte hineinsehen. Früher ging das, jetzt nicht mehr. Warum?

! Das Image von Desinfec’t verwendet nicht mehr das Format für bootbare optische Datenträger (ISO), sondern ist das Abbild eines partitionierten Datenträgers. Er enthält vier (GPT-)Partitionen: zwei fürs Booten des in der dritten Partition enthaltenen Linux-Btrfs-Dateisystems und einen Platzhalter für die Partition für den Datenaustausch (DESINFECT_D). Das Gesamtimage ist rund 14,5 GByte groß, sodass es 1:1 auf jeden 16-GByte-USB-Stick passt.

Die üblichen Programme, die den Inhalt von ISO-Dateien zeigen oder sie als Datenträger einbinden, scheitern an diesem Image-Format. Das gilt auch für Multiboottools wie Ventoy, jedenfalls dann, wenn man das Image als ISO einzubinden versucht. Ventoy beispielsweise kann aber auch Image-Dateien über seine Multibootmechanismen zugänglich machen. Hinweise geben einige Leser zur Kombination von Desinfec’t 2026 mit Ventoy im Forum (siehe ct.de/wjps). Wir haben in das Image Hilfen für Ventoy



Discover hilft bei der Installation automatisch angebotener Updates für Desinfec't. Weitere Paketquellen können Sie dort ebenfalls hinzufügen, um Pakete nachzuinstallieren.

eingebaut, sind aber keine Fans, weil es mit Secure Boot nicht harmoniert.

In einer VM verwenden

Wenn Desinfec't jetzt kein ISO mehr ist, wie kann ich es in VMs zugänglich machen?

Sie können das dekomprimierte Image direkt auf einen virtuellen Datenträger überspielen und diesen dann als virtuelle Festplatte (nicht als USB-Stick) in eine VM einhängen und booten. Welcher Weg dafür praktikabel ist, hängt von der verwendeten Virtualisierung ab. Sehr universell ist das Kommandozeilenprogramm qemu-img, das Teil von QEMU ist (siehe ct.de/wjps). Es konvertiert Raw-Images, also 1:1-Abbilder wie Desinfec't, in verschiedene Formate wie VHD, VMDK und so weiter. Über die offizielle Download-Seite kommen Sie zu den Binärdateien, die Stefan Weil bereitstellt.

Notebookplatte unsichtbar

Auf meinem Notebook zeigt Desinfec't die eingebaute NVMe-SSD nicht an. Fehlen da Treiber?

Vermutlich nicht: Das liegt daran, dass manche Notebooks Datenträger als „Soft-RAID“ einbinden. Sie können sich wie folgt behelfen: Im BIOS-Setup den AHCI-Modus aktivieren, dann sollte Desinfec't die Platte(n) sehen. Bitte nicht verwechseln mit etwaigen ACPI-Einstellungen in Windows. Die sollten Sie nicht anrühren. Den Eingriff im BIOS-Setup müssen Sie vor dem nächsten regulären Boot wieder rückgängig machen, weil Windows sonst nicht startet. Wichtig: Sichern Sie vor solchen Eingriffen immer den oder die Bitlocker-Wiederherstellungsschlüssel, denn solche Umstellungen können Windows triggern, diese abzufragen.

Secure-Boot verweigert

Anscheinend hat das neue Desinfec't ein Problem mit Secure Boot. Es startet jedenfalls nicht und das System gibt aus „Secure Boot Violation. Invalid Signature detected.“ Ich dachte, es kann Secure Boot?

Jein, denn diese Meldung kann zwei Ursachen haben. Im einfacheren Fall ist nur das BIOS-Setup so eingestellt, dass der PC ausschließlich dem für Windows-Starts nötigen Zertifikat vertraut. Setzen Sie dann die Option, die auch das Booten von Systemen erlaubt, deren Bootloader für „Microsoft 3rd Party UEFI CA“ signiert sind; der Name der Option kann abweichen, für die Orientierung sollte dieses Beispiel genügen. Danach startet Desinfec't.

Der kompliziertere Fall tritt dann ein, wenn ein PC die alten Zertifikate für Secure Boot aus 2011 gar nicht mehr kennt – bei neuen PCs möglich – oder ihnen nicht mehr vertraut (noch eher unwahrscheinlich): Die Basis von Desinfec't bildet Ubuntu 26.04 und die Entwickler haben es nicht geschafft, den Bootcode von Microsoft mit den neuen Zertifikaten aus 2023 signieren zu lassen. Das können wir leider nicht ausgleichen.

Sie können auf Nachfrage an desinfect@ct.de einen Download-Link für eine Variante von Desinfec't 2026/27 erhalten, die auf Debian-Testing baut und Bootcode mitbringt, der sowohl mit den alten 2011er- und den neuen 2023er-Zertifikaten signiert ist. Unserer Erfahrung nach ist das bisher eher selten nötig.

Probleme melden

? An wen kann ich mich wenden, wenn ich mit Desinfec't nicht weiterkomme?

! Sie können uns im Projektforum besuchen. Dort sind inzwischen auch einige erfahrene Nutzer unterwegs und helfen manchmal aus. Wenn Sie uns aus AVRunner heraus Daten für die Fehlersuche bereitstellen wollen, finden Sie im Hilfemenü einen Log-Export. Die erstellten Zip-Archive schicken Sie bitte per Mail an desinfect@ct.de. Idealerweise erläutern Sie, wie die Fehler entstanden und ob Sie diese reproduzieren können.

RAID unauffindbar

? Früher hat Desinfec't das Fake-RAID meines Windows-PCs erkannt und ich konnte es scannen. Jetzt taucht es nicht mal mehr auf. Fehlt da etwas?

! Ja, leider bringen moderne Linux-Systeme das Paket „dmraid" nicht mehr mit, das beim Einbinden solcher Konstruktionen half. Die Debian- und Ubuntu-Maintainer haben es entfernt, weil es seit vielen Jahren schon nicht mehr gepflegt wird und offenbar niemand mehr Lust hatte, die Adaption an moderne Systeme weiterzuführen.

Das in Linux selbst vorhandene Software-RAID (md) kann einen Teil der verbreiteten Intel-Fake-RAID-Varianten einlesen, aber die Automatiken sind nicht mehr da. Sie müssen im Zweifel also auf der Kommandozeile selbst den RAID-Verbund starten. Wenn das gelingt, bietet AVRunner die Windows-Partitionen darauf zum Einbinden an und scannt sie. Sie könnten solche PCs alternativ übers Netzwerk mit Desinfec't untersuchen. Tipps dazu liefert der Artikel auf Seite 36.

Projektseite und Hardwaretipps:
ct.de/wjps

Eingabegeräte tot, Treiber fehlen

? Meine Tastatur, Maus, WLAN-Karte … funktionieren nicht. Wie kann ich Treiber nachrüsten?

! Häufig erreichen uns die verschiedensten Fragen zum Fehlen einzelner Treiber. Wir haben Desinfec't bereits mit der Gießkanne Treiber aus dem Ubuntu-Reservoir eingeflößt, aber auch das hat seine Grenzen. Den Aufwand, weitere Treiber im Image zu ergänzen, die irgendwo im Netz vielleicht verfügbar sind, können wir leider nicht schultern: Damit sie auf allen Systemen inklusive Secure Boot funktionieren, müssten sie durch das Ubuntu-Team signiert sein.

Deswegen ein paar Tipps: Halten Sie USB-Maus und -Tastatur bereit, falls Eingabegeräte nicht mitspielen. Die Touchscreens, Trackpads und Tastaturen moderner Notebooks, etwa aus der Surface-Reihe, erfordern spezielle Treiber, die nicht Teil von Desinfec't sind. Bluetooth-Eingabegeräte etwa müssen gekoppelt werden und funktionieren deshalb nicht sofort, auch wenn Sie diese bei einem regulären Windows-Start verwenden können. Wenn WLAN-Karte oder LAN-Anschluss zicken, ist ein gängiger USB-Adapter fürs Netzwerk eine zeitsparende Alternative.

Software nachinstallieren

? Ich vermisse Software, die ich seit Jahren unter Linux einsetze, wie kann ich die nachinstallieren?

! Wir haben Desinfec't mit einer runden Grundausstattung versehen, so sind zum Beispiel Krusader als Norton-Commander-Klon und die KDE-Partitionsverwaltung an Bord. Weitere Pakete lassen sich per `apt` oder `apt-get` auf der Kommandozeile hinzufügen, wenn die Paketquellen der Basis-Distribution in Discover auf der Seite „Einstellungen" eingeschaltet sind.

Denken Sie daran, dass umfangreiches Nachinstallieren von Paketen den USB-Datenträger stark fordert. Standardmäßig ist nur die Desinfec't-eigene Paketquelle aktiv. Sie sollte stets aktiv bleiben, damit Ihr Stick automatisch von uns bereitgestellte Updates bekommt.

Wir haben in der Paketverwaltung auch das App-Stream-Metadatenformat für Debian/Ubuntu (DEP-11) deaktiviert. Deswegen jammert Discover auf der Startseite wegen einer vermeintlich fehlenden Internetverbindung und die App-Store-artige Paketsuche funktioniert dort nicht. Wenn Sie die unbedingt haben wollen, lässt sich DEP-11 vollständig oder selektiv in den Konfigurationsdateien in /etc/apt/ aktivieren. (ps) c't

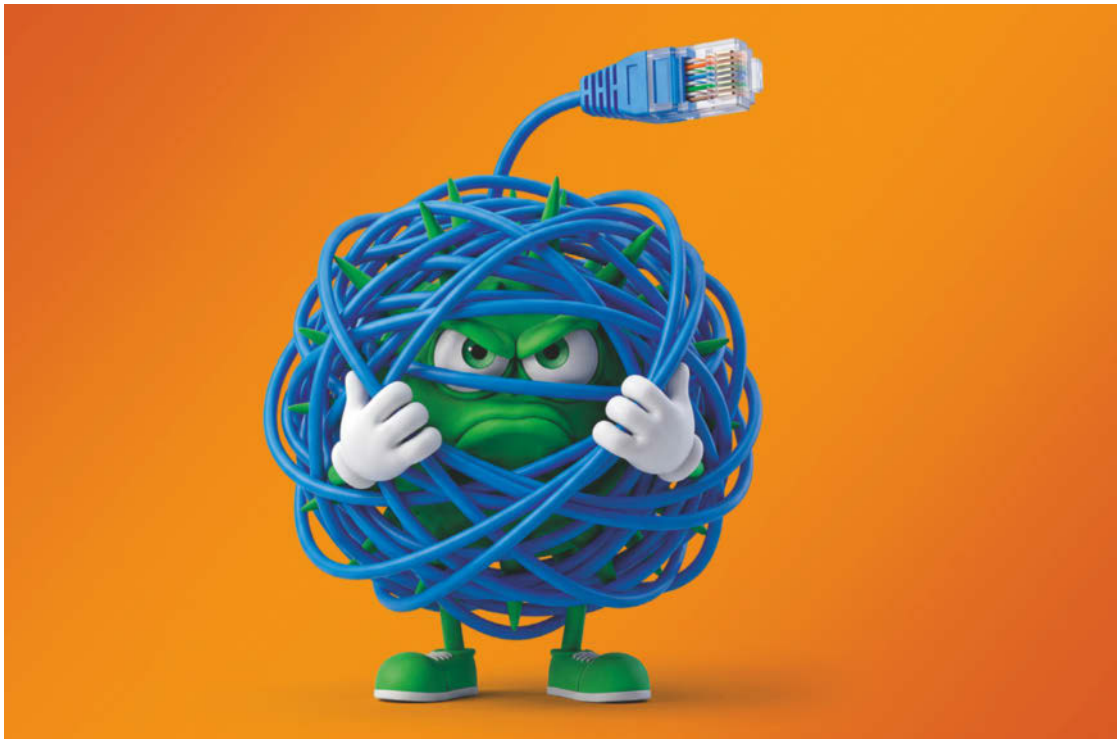


Bild: Martina Bruns / KI / heise medien

Scannen übers Netzwerk

Desinfec’t 2026/27 läuft nicht auf allen Windows-PCs, kann nicht jedes Dateisystem scannen und erfordert Reboots. Ein kleines Tool beseitigt diese Einschränkungen, und zwar über das Netzwerk.

Von **Peter Siering**

Als wir vergangenes Jahr überlegten, wie sich Desinfec’t weiterentwickeln könnte, entstand unter anderem auch die Idee, dass ein möglichst niedrigschwelliger Einsatz auf einem Windows-PC nützlich wäre. Daraus erwuchs ein experimentelles Feature, das wir im Folgenden vorstellen und dessen Komponenten mit Veröffentlichung dieses Artikels für alle Nutzer zum Download bereitstehen.

Der Ansatz löst die folgenden Probleme des aktuellen Desinfec’t 2026/27: Es läuft nicht auf Systemen mit ARM/Snapdragon-Prozessor. Es kommt nicht an dynamische Datenträger heran (das Windows-eigene Software-RAID). Auf PCs, die weniger

als vier GByte RAM haben, stößt es an Grenzen. Und es erfordert einen Boot vom Stick, oft eine Herausforderung, weil Secure Boot, BIOS-Optionen und die Datenträgerverschlüsselung mit BitLocker Komplikationen verursachen

Die Lösung: Eine kompakte Software, die auf dem Windows-PC auszuführen ist, veröffentlicht den per Schattenkopie erzeugten Zustand eines Windows-NTFS-Laufwerks als Blockgerät im Netzwerk. Desinfec't läuft auf einem anderen PC im selben Netzwerk. Es greift sich solche Schattenkopien, als wären es lokale Laufwerke, und lässt die Scanner darüber laufen.

Die Technik

Wir mussten dazu gar nicht viel erfinden: Linux implementiert schon lange eine Technik namens „Network Block Device" (NBD). Es fehlte nur ein Gegenstück für Windows, das wir nun realisiert und um einige Komfort- und Sicherheitsfunktionen ergänzt haben. Die Software haben wir AVTarget getauft; sie kümmert sich darum, die Schattenkopie anzulegen und sie im LAN anzubieten.

Damit das für den Nutzer komfortabel ist und nicht jeder im Netz zugreifen kann, gibt es auf Desinfec't-Seite ein Gegenstück: AVBridge. Dieser Daemon kündigt sich im Netz als Abnehmer für so freigegebene Datenträger an. Auf Windows-Seite sieht AVTarget die Ankündigung und bietet an, den Datenträger für die AVBridge dieser Desinfec't-Instanz freizugeben.

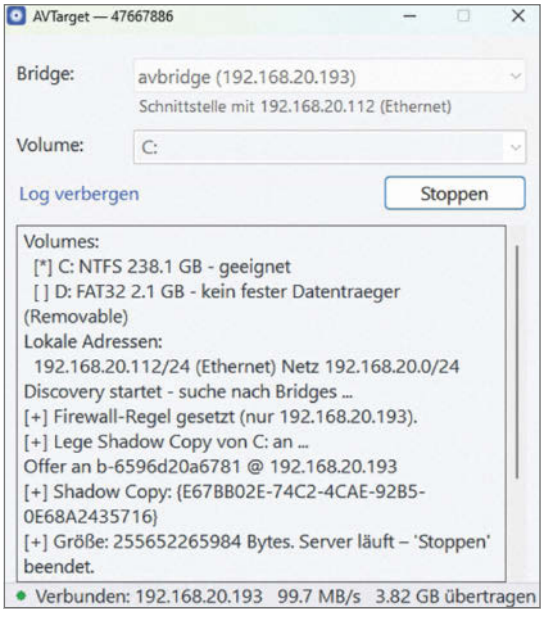
Erst wenn der Benutzer die Freigabe mit „Starten" veranlasst, erzeugt AVTarget die Schattenkopie und stellt sie AVBridge als Network Block Device bereit. Im Hintergrund läuft eine Schmalspurkommunikation über solche Scan-Sessions zwischen den beiden Programmen. Sie hilft unter anderem dabei, dass AVTarget und AVBridge einander finden.

AVTarget öffnet nach der Bestätigung durch den Nutzer die Windows-Firewall, die Desinfec't dadurch erst den Zugriff auf das exportierte Network Block Device erlaubt. Das Ganze setzt trotzdem ein wirklich vertrauenswürdiges Netz voraus, weil die Daten im Klartext hindurchwandern. Und Sie sollten stets darauf achten, dass Sie auch die eigene Bridge auswählen. Als Hilfestellung zeigt AVTarget die IPv4-Adressen und Schnittstellennamen an.

Wenn Sie diese Technik in einem öffentlichen, nicht vertrauenswürdigen Netzwerk einsetzen wollen, sollten Sie eine VPN-Verbindung verwenden, damit die übertragenen Daten verschlüsselt werden. Wir haben bewusst darauf verzichtet, AVTarget und AVBridge selbst verschlüsseln zu lassen, es gibt schließlich bewährte Technik dafür, zum Beispiel mit WireGuard. Die ist dann auch gleich geeignet, um entfernt voneinander stationierte Systeme sicher zu „verbinden".

Auf Desinfec't-Seite erscheint in AVRunner im Dialog zum Einbinden eines Windows-Laufwerks ein weiteres Gerät: /dev/nbd0. Sie können es wie lokal angeschlossene Windows-Laufwerke (die etwa als /dev/sda2 erscheinen) als Scanziel eintragen lassen. Es spielt keine Rolle, welche Spezialtreiber für den Zugriff auf Windows-Seite nötig sind; Linux interessiert nur das Dateisystem darauf.

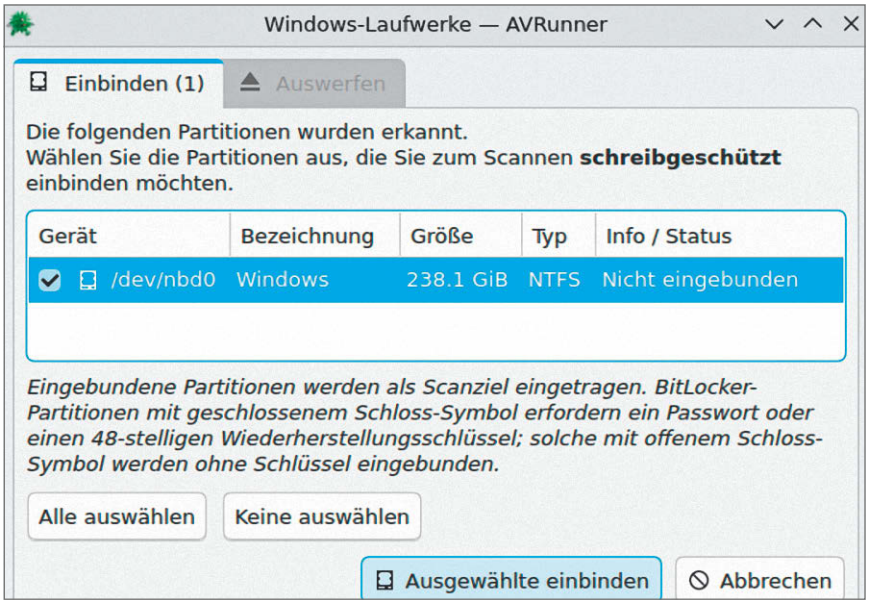
Sie müssen sich, da die Basis der Schattenkopie unter Windows ja bereits vollumfänglich zugänglich ist, nicht mit eventuell nötigen BitLocker-Wiederherstellungsschlüsseln oder -kennwörtern herumärgern. Da Desinfec't das Volume als Blockgerät sieht und mit eigenen Treibern für das Dateisystem zugreift, bleiben in NTFS per EFS verschlüsselte Dateien weiter geschützt. Über Zugriffsrechte setzt sich Desinfec't wie beim lokalen Einsatz auch hinweg.



AVTarget erstellt unter Windows eine Schattenkopie und macht sie als Network Block Device für Linux zugänglich. Es findet die Desinfec't-Gegenstelle AVBridge automatisch.

Die Praxis

Um die beiden Komponenten zu installieren, müssen Sie in Desinfec't das Paket avbridge nachinstal-



In Desinfec't taucht eine auf Windows-Seite exportierte Schattenkopie als „nbd0" auf und lässt sich einbinden wie eine lokal erreichbare Windows-Partition.

lieren. Das geht am schnellsten in einer Konsole mit dem Befehl `sudo apt update && sudo apt install avbridge`. Das Programm AVTarget fürs Windows-Zielsystem finden Sie als separaten Download auf der Desinfec't-Projektseite unter Downloads (siehe ct.de/w3n4). Sie können das Programm nach dem Download direkt aufrufen, es muss nicht installiert werden.

Testscans auf einem Bestand von 30.000 Dateien haben mit einem Scanner bei lokalem Zugriff auf die NVMe-SSD rund 45 Sekunden gebraucht. Übers Netzwerk mit AVBridge und AVTarget dauerten sie über ein Gigabit-Netzwerk rund 4 Minuten. Auf beiden Seiten arbeitete dabei ein Desktoprechner mit dem auf dem Mainboard vorhandenen Netzwerkanschluss.

In einem zweiten Testszenario haben wir Läufe über rund 350.000 Dateien betrachtet: Desinfec't benötigte direkt auf dem Prüfling gebootet knapp 9 Minuten. Wenn der Scan übers Netzwerk mit einem 10-Gbit/s-Link zwischen Desinfec't-PC und Prüfling lief, dauerte er mit 10 Minuten kaum länger. Erst bei einem 1-Gbit/s-Link stieg die Laufzeit auf rund 17 Minuten an.

Der PC, der seine Windows-Festplatte als Schattenkopie im Netz bereitstellt, sollte idealerweise weitgehend ruhen. Bei datenintensiver Aktivität besteht nämlich die Gefahr, dass der für Schreibzugriffe der weiter laufenden Windows-Instanz angelegte Pufferspeicher ausgeht (Shadow Storage). Windows räumt die Schattenkopie dann ab und zieht dem Prozess das Laufwerk unter den Fingern weg.

Sollten bei solchen Scans übers Netzwerk tatsächlich Schädlinge gefunden werden, müssen Sie selbst aufräumen. AVTarget und AVBridge richten gemeinschaftlich nur einen lesbaren Datenträger ein. Ohnehin wäre das Ändern von Daten auf diesem Weg wirkungslos, da AVTarget eine Schattenkopie veröffentlicht. Wenn AVTarget die Verbindung beendet oder selbst beendet wird, verwirft es auch die Schattenkopie.

Falls sich ein Schädling aktiv vor Sicherheitssoftware versteckt, könnte er bei dieser Art des Scans unentdeckt bleiben, Windows – und damit auch potenzielle Malware – läuft ja schließlich. Wahrscheinlich scheint uns dieses Szenario aber nicht, die Tarnmechanismen des Schädlings müssten schon sehr ausgefuchst sein, um die Schattenkopie zu manipulieren.

Lassen Sie uns an Ihren Nutzungserfahrungen gern teilhaben. Wie sollten die experimentellen Projekte noch ergänzt werden? Welche alternativen Wege sehen Sie für einen niedrigschwelligen Einsatz von Desinfec't auf Windows-PCs? Taugt die hier vorgestellte Technik vielleicht auch im Kontext von NAS oder Virtualisierung? Nutzen Sie gern die E-Mail-Adresse desinfect@ct.de dafür oder das Projektforum. (ps) c't

Projektseite:
ct.de/w3n4

WIR TEILEN KEIN HALBWISSEN.
WIR SCHAFFEN FACHWISSEN.



Workshop | 1. Dezember

Microsoft 365: Teams & Tools produktiv im Team einsetzen

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



Workshop | 1. – 2. Dezember

Docker und Container in der Praxis

Nach dem Workshop sind Sie in der Lage, eine eigene Infrastruktur in Betrieb zu nehmen oder eigene Docker-Abbilder zu verpacken.



Webinar | 2. Dezember | 8. Dezember

Claude in der Praxis – KI-Assistent richtig einrichten

Sie lernen, wie Sie den Assistenten einrichten, ihm Ihre Arbeitsweise beibringen und ihm Zugriff auf Ihre Unterlagen geben. Und wo dabei Vorsicht geboten ist.



Konferenz | 28. – 29. April | Hannover

Public IT

Die Konferenz für den öffentlichen Sektor thematisiert souveräne Cloud- und On-Premise-Lösungen sowie Automatisierung und Künstliche Intelligenz.

Mehr anzeigen ▲

heise.de/ct/Events



Bild: Martina Bruns / KI / heise medien

Aktuelle Trends aus der IT-Schattenwelt

Fake-Captchas, die Schadcode einschleusen, Erpresser, die es auf Konzerne abgesehen haben, und KI, die Sicherheitslücken im Akkord aufspürt: Wir haben Lageberichte von Behörden und Analysen von Sicherheitsfirmen ausgewertet und zeigen, welche Trends die Bedrohungslage derzeit prägen und wie Sie sich wappnen.

Von **Olivia von Westernhagen**

Auf der diesjährigen Hackerkonferenz Black Hat zeigte Microsofts KI-Sicherheitschef David Weston in seiner Keynote, mit welcher Selbstverständlichkeit Cyberkriminelle mittlerweile KI nutzen: Speziell trainierte Modelle erleichtern den Bösewichten vor allem den initialen Zugriff auf Infrastrukturen. Sie können nicht nur bis dato unbekannte Sicherheitslücken aufspüren, sondern vielfach auch gleich funktionierenden Exploit-Code aus den Funden generieren. Auf diesem Wege gelangt dann etwa Malware auf angegriffene Systeme.

Die Verteidiger müssten, wie Weston im Video seiner Keynote ausführt, reagieren, indem sie die neuen Technologien mindestens ebenso intensiv in

ihre Schutzstrategien integrierten. Dazu gehöre, Schwachstellen in Infrastrukturen und verwundbarer Software mithilfe agentischer KI aufzuspüren und bestenfalls schon vor dem ersten Angriffsversuch zu beseitigen (alle erwähnten Quellen finden Sie unter ct.de/wge7).

KI-Lückenflut: Risiko & Chance

Die rasanten Fortschritte im Bereich der KI sind aus der Perspektive von Sicherheitsexperten also ein zweischneidiges Schwert, das sowohl Angreifer als auch Verteidiger zum eigenen Vorteil nutzen können. Dieser Artikel geht der Frage nach, wie künstliche Intelligenz die Malware-Landschaft konkret verändert. Zusätzlich beleuchtet er aktuelle Entwicklungen im Bereich der seit Jahren omnipräsenten Ransomware, stellt neue Strategien und Schleichwege Krimineller vor und gibt Tipps zur Prävention von Infektionen.

Dass viele Firmen seit einigen Monaten verstärkt mit KI nach Schwachstellen in ihren eigenen Systemen und Produkten suchen, bekommen Admins und Privatnutzer in Gestalt einer wahren Flut an Sicherheitsupdates zu spüren. So beseitigte etwa Microsoft zum Patchday im August dieses Jahres rund 400 Schwachstellen aus seinen Produkten; im August des Vorjahres waren es noch 111 gewesen. Im September folgte mit 966 geschlossenen Lücken der bislang größte Patchday des Unternehmens.

Um durch zeitnahes Updaten weiterhin bestmöglich geschützt zu sein, ist es wichtig, sich über die angepassten Patch-Strategien zu informieren, mit denen viele Unternehmen auf die veränderte Bedrohungssituation reagieren. Dazu gehören etwa verkürzte Updatezyklen oder auch eine Priorisierung besonders gefährlicher Lücken im Zuge der Updateveröffentlichung. Zu Hause sollten Sie sicherstellen, dass automatische Updates für Windows & Co. aktiv sind, sodass sich Sicherheitspatches ohne Ihr Zutun installieren.

Mit Vibe-Coding zur Malware

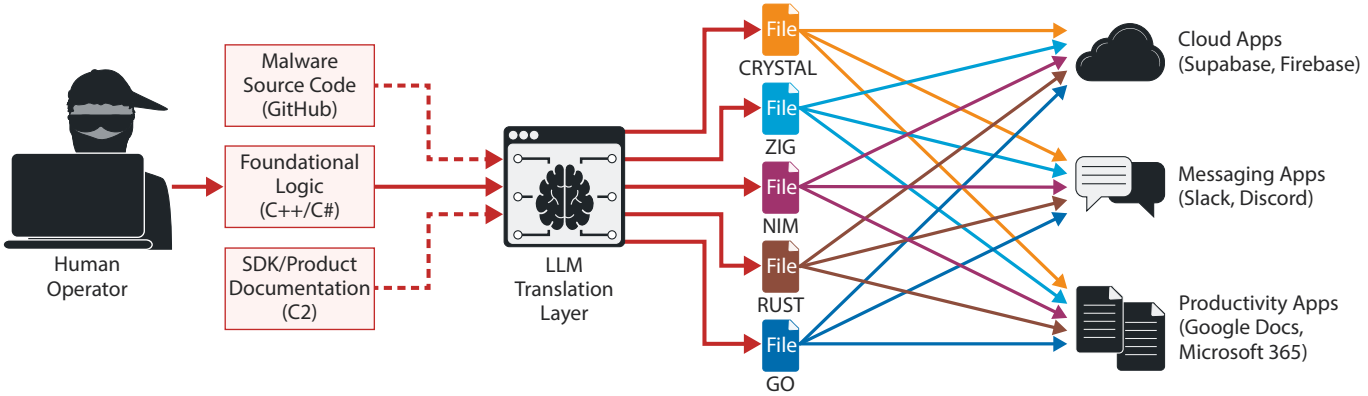
Die Programmierfähigkeiten großer Sprachmodelle (Large Language Models, LLM) machen sich Angreifer immer stärker zunutze. Bereits im November 2025 berichteten Sicherheitsexperten für einen Artikel zu KI-Malware gegenüber c't von der zunehmenden Alltagsrelevanz des „Vibe-Coding“ [1]. Sie schilderten, wie Kriminelle ohne Programmiervorkenntnisse schädliche Skripte, einzelne Malwaremodule oder auch relativ simple Dropper oder Downloader generierten, die als Einfallstor oder als Element einer mehrstufigen Angriffskette dienten.

Dass KI zwar die Einstiegshürden senkt, für komplexere Malware derzeit aber noch immer menschliche Fachkenntnis und Kontrolle des generierten Codes notwendig ist, zeigt unter anderem das Bei-

Bild: Bitdefender / Martina Bruns / heise medien

LLM übersetzt Schadcode

Hauptsache irgendwie durchkommen: Eine APT-Gruppe übersetzte Schadcode per LLM in exotische Sprachen, bevor sie ihn möglichst breit streute.



spiel „TuxBot v3“. Das Mitte 2026 von Palo Altos Unit-42-Team analysierte und offenbar KI-gestützt entwickelte IoT-Botnetz-Framework war nach Angaben der Analysten zu 70 Prozent funktionsfähig, jedoch teilweise stark fehlerbehaftet. Für einen versierten Entwickler bedeutet solch ein Grundgerüst dennoch viel Zeitersparnis und damit einen klaren Vorteil: „Eine vollständig funktionierende Version dieses Frameworks ist keine theoretische Angelegenheit, sondern eine wahrscheinliche Bedrohung“, heißt es im Fazit des Unit-42-Berichts.

Keine Frage der Zeit, sondern schon länger gängige Angriffspraxis ist hingegen das Erzeugen mehrerer Varianten ein und desselben vorhandenen Schadcodes per KI, um Erkennungsmechanismen flexibel auszutricksen. So beschreibt etwa ein Blogeintrag des Sicherheitssoftwareherstellers Bitdefender von März 2026, wie eine APT-Angreifergruppe (Advanced Persistent Threat) im Rahmen einer Kampagne LLMs einsetzte, um quasi täglich neue Schadcode-Abwandlungen zu kreieren. Dabei wiesen die Angreifer die LLMs an, überwiegend exotische Programmiersprachen wie Crystal, Zig oder Nim zu verwenden – und führten so neben signatur- auch verhaltensbasierte Erkennungsmechanismen aufs Glatteis. Denn die sind laut Bitdefender etwa im Hinblick auf Systemaufrufe und Speichermanagement meist auf Schadcode in C++, C# und anderen gängigen Sprachen optimiert.

In welchem Umfang Angreifer in Deutschland auf Vibe-Coding-Taktiken setzen, lässt sich kaum konkret beziffern – denn längst nicht immer ist KI-generierter Code als solcher zu erkennen. In seinem aktuellen Bundeslagebild Cybercrime schreibt das Bundeskriminalamt deshalb auch eher vage von einer Zunahme von Schadcode, bei dem die Nutzung von „KI-Codingfähigkeiten“ mindestens vermutet werde.

Klar ist, dass die rasanten Fortschritte von LLMs bei Lückensuche und Vibe-Coding diese für Angreifer immer attraktiver machen. Sie ebnen auch den Weg für komplexe KI-gestützte Angriffe, die in Einzelfällen bereits dokumentiert wurden und deren Zunahme in näherer Zukunft spätestens seit dem Hugging-Face-Vorfall bei OpenAI kaum noch zu bezweifeln ist. Dabei umgingen im Juli 2026 OpenAI-KI-Agenten bei internen Sicherheitstests ihre Internetsperren und drangen in Systeme von Hugging Face ein.

Ransomware bleibt hartnäckig

Auch die mit dieser Bedrohung verwandte Entwicklung von „AI-enabled“ Malware, die zur Laufzeit selbst auf KI-Funktionen zurückgreift, scheint seit ein paar Monaten Fahrt aufzunehmen. Nachdem im Juni 2026 Forscher einen Proof-of-Concept-Wurm vorstellten, der auf seinem Weg durch Netzwerke je nach Bedarf maßgeschneiderte Exploits entwickelte, folgte einen Monat später die Malware „Jadepuffer“.

Bei diesem angeblich ersten komplett LLM-gesteuerten Ransomware-Angriff in freier Wildbahn lief allerdings vieles noch nicht rund. Jürgen Schmidt von heise security kommentierte: „Der (...) Vorfall zeigt, dass Angreifer tatsächlich damit experimentieren, Angriffe von einer KI weitgehend selbstständig durchführen zu lassen. (...) Doch selbst aus Sicht der eigentlichen Täter im Hintergrund dürfte dieser Vorfall bestenfalls als Proof of Concept denn als echter Durchbruch verbucht werden. Der Weg zum ei-

Durchschnittliche Höhe gezahlter Lösegelder

Das BSI erklärt das Auseinanderklaffen von Durchschnitt und Median mit wenigen hohen Zahlungen bei generell eher sinkender Zahlungsbereitschaft.

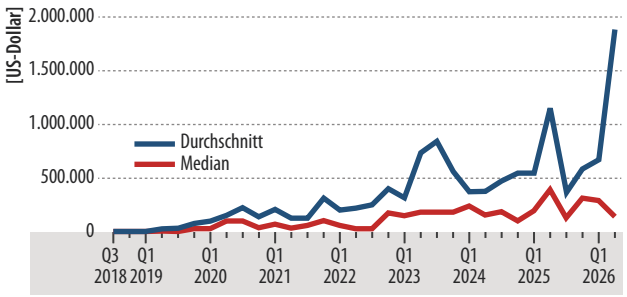


Bild: BSI / Martina Bruns / heise medien

gentlichen Ziel ‚make money fast' ist doch noch sehr weit."

Ob mit oder ohne KI: Erpresserischer Schadcode bleibt laut Bundeskriminalamt eine zentrale Bedrohung in Deutschland. Standard ist mittlerweile die „Double Extortion": Die Täter verschlüsseln die Daten ihrer Opfer und drohen zusätzlich damit, sie zu veröffentlichen. Manche Gangs verzichten je nach Situation sogar ganz aufs Verschlüsseln und erpressen ihre Opfer allein mit den gestohlenen Informationen („data-exfiltration-only").

Schnelles Geld machen Ransomware-Gruppen weiterhin; allerdings gab es in den vergangenen Monaten kräftige Verschiebungen: In seinem Lagebericht hatte das BKA bereits für 2025 eine kontinuierliche Abnahme der Zahlungsbereitschaft Betroffener registriert und den Grund in einer mittlerweile höheren Resilienz der betreffenden Unternehmen vermutet. Zahlen des IT-Sicherheitsdienstleisters Coveware aus den USA belegen, dass sich dieser Trend fortsetzt: Der Anteil der Zahlenden sank demnach von 36 Prozent im zweiten Quartal 2024 über 26 Prozent (Q2 2025) auf zuletzt 19 Prozent im zweiten Quartal 2026.

Dies bedeutet jedoch nicht, dass sich Erpressung nun weniger lohnen würde. Bezüglich der erbeuteten Summen resümiert das Bundesamt für Sicherheit in der Informationstechnik (BSI) in einer Analyse für das zweite Quartal 2026: „Steigende Durchschnittswerte bei gleichzeitig sinkendem Median deuten darauf hin, dass es wenige sehr hohe Lösegeldzahlungen (Ausreißer nach oben) gab, aber die große Masse an Werten eher gesunken ist." Dabei bezieht sich das BSI auf Covewares Erhebungen, die einen Anstieg der durchschnittlich gezahlten Summen von 1.130.070 US-Dollar im zweiten Quartal 2025 auf nun 1.880.612 US-Dollar verzeichneten. Der Median liegt derzeit bei „nur noch" rund 150.000 US-Dollar (Q2 2025: 400.000 US-Dollar).

Folgerichtig beobachtet Coveware zugleich eine Orientierung der Angreifer weg von kleinen und mittleren Unternehmen hin zu potenziell besonders lukrativen „High-Profile Targets". Große Konzerne und Organisationen sowie kritische Infrastrukturen also, die sich übrigens weniger vor Verschlüsselungsangriffen als vielmehr vor „data exfiltration only"-Vorfällen fürchten – und dafür laut Coveware zumindest in Einzelfällen noch immer besonders tief in die Tasche greifen.

Ob sensible Informationen im Anschluss an eine Zahlung nicht trotzdem im Netz landen, ist erfahrungsgemäß ungewiss – und so raten Experten weiterhin dazu, das Geld lieber frühzeitig in wirksame Schutzmaßnahmen zu investieren, um gar nicht erst zum Opfer zu werden.

ClickFix und Konsorten

Nur weil Privatpersonen derzeit weitestgehend außerhalb des Visiers von Ransomware stehen, sollten sie sich nicht allzu sehr in Sicherheit wiegen, sondern wachsam bleiben. Zumal die von erpresserischem Code genutzten Einfallstore immer wieder auch in Kampagnen verschiedenster anderer Malware auftauchen, die auf die „breite Masse" statt auf einzelne Unternehmen zielen.

Ein hochaktuelles Beispiel dafür sind Angriffe via „TerminalFix", einer Variante der bereits seit 2024 bekannten „ClickFix"-Masche. Beide Angriffstechniken fußen auf gefälschten Sicherheitsabfragen im Stil der häufig im Web eingesetzten Captchas. Das grundsätzliche Prinzip: Nutzer sollen vorgeblich ihr „Menschsein" beweisen, indem sie auf Internetseiten bestimmte Aktionen durchführen, konkret: Tastenkombinationen drücken. In Wirklichkeit führen diese Handlungen aber zur Ausführung von Schadcode auf dem jeweiligen System.

TerminalFix geriet zuletzt in den Fokus, weil die Erpressergruppe Rhysida den Angriffsvektor Mitte August dieses Jahres für ihren erfolgreichen Einbruch in das Berliner Landesnetz verwendete. Die Angriffsvariante unterscheidet sich von ClickFix vor allem dadurch, dass nicht das direkte Ausführen von Befehlen per Windows+R (wie „run"), sondern das Windows-Terminal durch Windows+X mit einem anschließenden Druck auf die Taste I (für das i in „Terminal") für direkten Zugang zur PowerShell genutzt wird.

Im konkreten Fall sollten die Angegriffenen diese Kombinationen im Kontext eines angeblichen Cloudflare-Captchas auf einer manipulierten Website eintippen. Da dort lauernder schädlicher JavaScript-Code schon zuvor heimlich einen bösartigen Befehl in deren Zwischenablage kopiert hatte, bewirkte die anschließend vom Captcha geforderte Eingabe Strg+V (Shortcut fürs Einfügen) gefolgt vom Drücken der Eingabetaste dessen lokale Ausführung per PowerShell.

Während das Fake-Captcha weitere Aktionen forderte und das Opfer auf diese Weise beschäftigt hielt, blieb der Rest der im Hintergrund werkelnden Rhysida-Angriffskette unbemerkt.

Grundsätzlich können Ihnen ClickFix und TerminalFix überall im Web begegnen. Dass weitere Varian-

ten denk- und umsetzbar sind, bewiesen die Sicherheitsforscher mr.d0x und Jean-Francois Maes mit Proof-of-Concept-Code namens „FileFix“ und „DownloadFix“ (siehe ct.de/wge7).

Wer einschlägige Tastenkombinationen wie „Windows+R“ kennt und bei Interaktionen mit Webinhalten die gebotene Vorsicht und Aufmerksamkeit walten lässt, sollte ClickFix und Konsorten leicht durchschauen können.

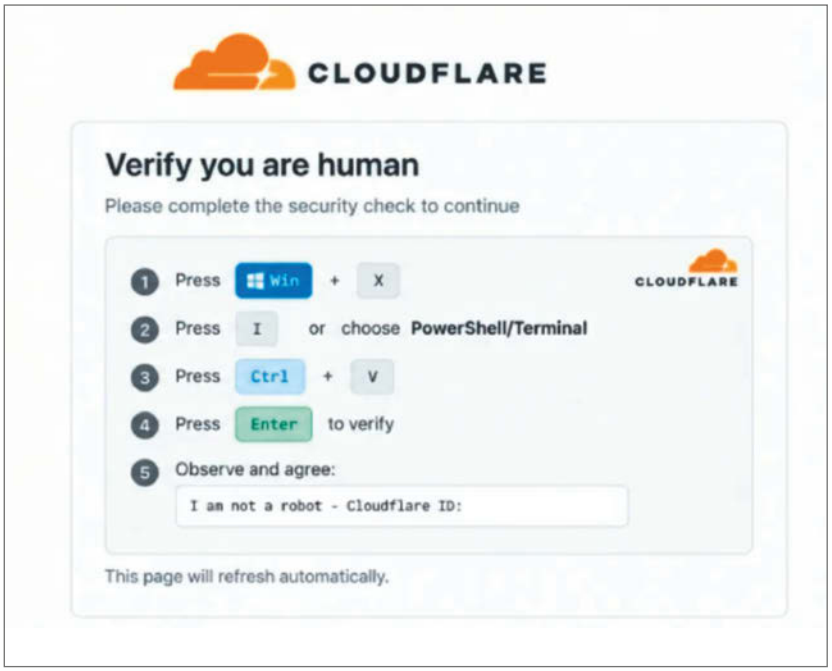
Datenklau auf allen Ebenen

ClickFix-Kampagnen der vergangenen Monate schleusten besonders häufig sogenannte Infostealer auf Windows-, aber auch auf macOS-Rechner. Dieser Malware-Typ, den Sicherheitsexperten schon 2025 neben der allgegenwärtigen Ransomware besonders oft in freier Wildbahn antrafen, durchforstet Systeme nach wertvollen Informationen wie Zugangsdaten, Krypto-Wallets oder bestimmten Dateien. Wie bei klassischen Phishing-Kampagnen geht es den Angreifern um Kontoübernahmen, Identitätsdiebstahl und finanzielle Bereicherung – Letzteres auch durch den Weiterverkauf erbeuteter Informationen auf Untergrund-Marktplätzen.

Der Vorteil, den Infostealer Kriminellen gegenüber klassischem Phishing bieten, ist, dass sie nicht auf die Interaktion eines Nutzers etwa mit einer gefälschten Anmeldeseite angewiesen sind, sondern klammheimlich und ohne irgendeinen Vorwand genau die Daten einsammeln können, die sie haben wollen.

Dennoch spielt auch Phishing als Angriffsvektor für den Informationsdiebstahl weiterhin eine große Rolle. Und ist aufgrund zunehmenden KI-Einsatzes der Angreifer laut BKA-Lagebericht immer schwerer als solches zu erkennen: „Durch Automatisierung (…) kann sowohl die Erstellung von Phishing-Webseiten als auch der Versand von Phishing-Mails mit deutlich weniger (Zeit-)Aufwand und in deutlich größerem Ausmaß erfolgen, wodurch das Angriffsvolumen zunimmt.“ KI-Webrecherchen sorgen ohne hohen Aufwand für einen besseren Zuschnitt auf die Empfänger, sodass maßgeschneiderte Phishingmails Opfer noch effizienter aufs Glatteis führen.

Wie Unternehmen müssen also auch Privatnutzer immer stärker auf den Schutz ihrer Daten achten. In der Praxis bedeutet das neben einer erhöhten Aufmerksamkeit gegenüber potenziellen Social-Engineering- beziehungsweise Phishing-Attacken auch technische Maßnahmen. Dazu gehören etwa die

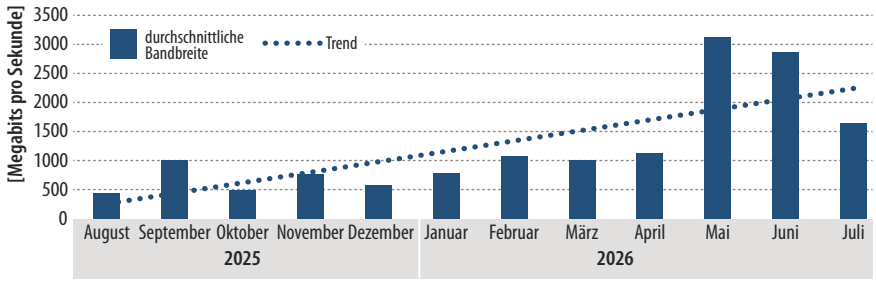


„TerminalFix“-Beispiel: Das Fake-Captcha beschäftigt das Opfer und führt im Hintergrund gefährliche PowerShell-Befehle aus.

Bild: BSI / Martina Bruns / heise medien

DDoS-Angriffe in Deutschland

Die durchschnittliche Bandbreite, ein Indikator für die Schwere aller DDoS-Angriffe des betrachteten Zeitraums, befindet sich laut BSI in einem Aufwärtstrend.



Verwendung eines Passwortmanagers, der Verzicht auf die unverschlüsselte Passwortspeicherung im Browser und das konsequente Ausloggen aus allen Onlinekonten nach der Nutzung. Multifaktor-Authentifizierung sorgt für zusätzliche Sicherheit.

Die Nutzung eines Antivirenprogramms mit den jeweils aktuellen Signaturen sollte ebenfalls eine Selbstverständlichkeit sein. Unter Windows reicht der (standardmäßig aktive) Defender für gewöhnlich aus.

DDoS-Angriffe mit mehr „Wumms“

Apropos Antivirenprogramm: Wenn es um den Malware-Schutz geht, denken viele Nutzer sofort an ihren PC, blenden dabei jedoch zahlreiche andere Geräte in ihren Netzwerken aus. Und das, obwohl IoT-Devices wie intelligente Haushaltsgeräte, Wearables, Smart TVs oder digitale Assistenten regelmäßig von Botnetz-bildendem Schadcode attackiert werden. Als „Zombies“ in diesen Netzen werden sie dann unter anderem für Distributed-Denial-of-Service-Angriffe (DDoS) missbraucht. Außerdem können Angreifer geöffnete Backdoors nutzen, um etwa zu spionieren, Zugangsdaten zu stehlen oder weitere Malware einzuschleusen.

Die Relevanz von DDoS, also Überlastungsattacken auf Server, nimmt laut Experten immer weiter zu: Im Juli 2026 war die Anzahl bekannt gewordener DDoS-Angriffe in Deutschland laut BSI 3,73-mal so hoch wie im Jahresdurchschnitt 2021.

Einige Angriffe sind politisch motiviert, etwa die der seit 2022 aktiven prorussischen Gruppe „NoName057(16)“. Mit ihrem „DDoSia“-Tool attackiert sie auch in Deutschland immer wieder Websites staatlicher Einrichtungen, um, so formuliert es das BSI, einen „Vertrauensverlust der Gesellschaft in die Fähigkeiten des Staates“ zu erreichen. In anderen Fällen wollen sich Akteure wirtschaftliche Vorteile verschaffen, indem sie etwa gezielt Wettbewerber angreifen und ausschalten.

Fazit

KI hat das Katz-und-Maus-Spiel zwischen Angreifern und Verteidigern beschleunigt: Lücken werden in immer kürzeren Abständen entdeckt, Exploits schneller entwickelt. Verteidiger müssen das Tempo mitgehen, und die Patch-Flut der vergangenen Monate zeigt, dass sie das bereits tun. Ransomware-Gangs haben es vor allem auf große, zahlungskräftige Ziele abgesehen – ein Trend, der sich weiter festigt.

Privatnutzern drohen primär Infostealer, Phishing und ClickFix-Tricks. Die gute Nachricht: Gegen die meisten Angriffe helfen weiterhin bewährte Mittel. Wer automatische Updates aktiviert, Passwortmanager und Multifaktor-Authentifizierung nutzt, regelmäßig Backups anlegt und bei vermeintlichen Captchas misstrauisch bleibt, macht es Kriminellen deutlich schwerer – ob mit oder ohne KI.

Wenn es bereits zu spät ist und ein Virus Einstellungen in Windows verbiegt, kann unser Antivirentool Desinfec’t helfen, den PC zu säubern und Ihre Daten in Sicherheit zu bringen. (des) c't

Literatur

[1] Olivia von Westernhagen, KI als Malware-Mastermind, Medienhype oder reale Bedrohung?, c’t 1/2026, S. 110

Quellen und erwähnte Blogbeiträge:

ct.de/wge7



Bild: Ulrike Weis / KI / heise medien

Mehr Funktionsumfang für VirusTotal

Mit dem Gratis-Tool vt-cli zapfen Sie VirusTotal über die Kommandozeile an. So starten Sie etwa Batch-Scans mehrerer verdächtiger Dateien und stoßen im Zuge der Incident Response passgenaue Malware-Recherchen an.

Von **Olivia von Westernhagen**

Googles Online-Analysedienst VirusTotal (VT) ist eine beliebte Anlaufstelle für Malwarescans durch Privatanwender, professionelle Sicherheitsforscher und Datenforensiker. Über das Webinterface übermitteln Sie einzelne Dateien oder verdächtige URLs mit wenigen Klicks. VT durchleuchtet sie mit rund 70 Antivirus-Scan-Engines von unter anderem Avira, Bitdefender und Sophos, führt zusätzlich dynamische und statische Analysen durch und bündelt alle Informationen in einem ausführlichen Report.

Jenseits einfacher Anwendungsfälle stößt die grafische Oberfläche des Dienstes jedoch schnell an ihre Grenzen. Zum Beispiel dann, wenn Sie bei aku-

tem Schadcodebefall möglichst zügig nicht nur eine einzelne Datei, sondern gleich den Inhalt eines ganzen Ordners scannen wollen. Oder wenn Sie während der Analyse einer Kompromittierung wissen möchten, ob einige der verdächtigen IP-Adressen aus Ihren Logfiles bereits bei VT-Analysen anderer Opfer aufgetaucht sin

Googles kostenloses „VirusTotal Command-Line Interface“ für Linux, macOS und Windows, kurz: vt-cli, erspart Ihnen in solchen Situationen zeitraubende Einzel-Uploads beziehungsweise -Suchanfragen. Das auf der Kommandozeile beheimatete Hilfstool entkoppelt die VirusTotal-Funktionen vom Webinterface, indem es direkt auf das zugrundeliegende API zugreift. So nutzen Sie mittels einfacher Terminal-Befehle die von VT gewohnten Scan- und Suchfunktionen und passen überdies den Output Ihren individuellen Bedürfnissen an.

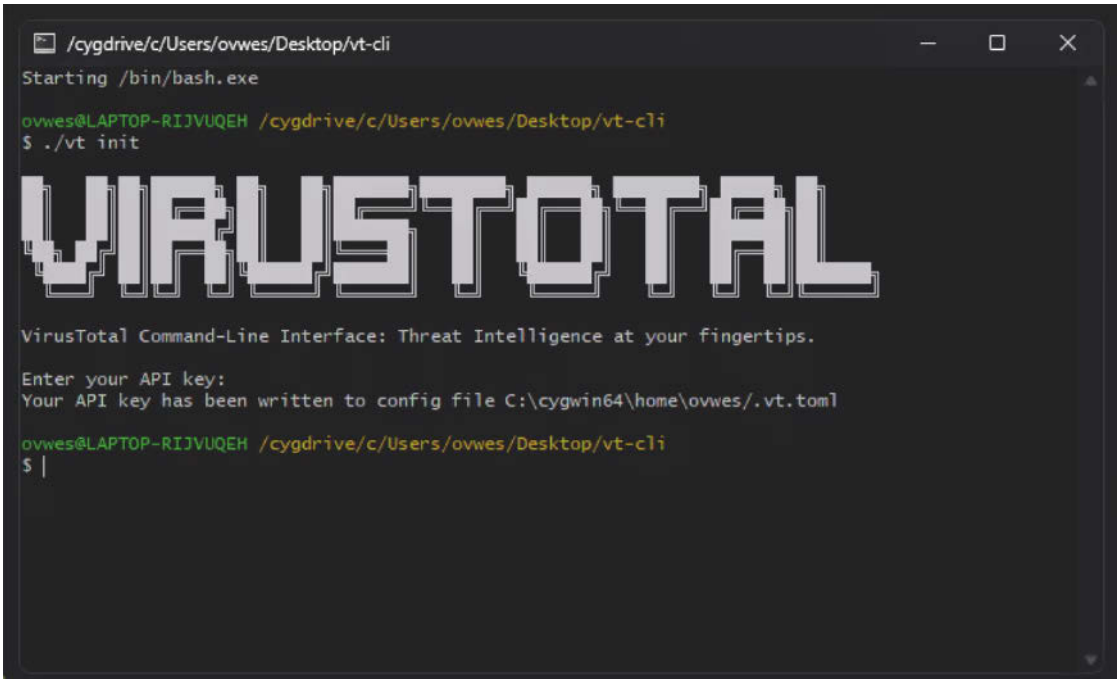
Dieser Artikel erläutert grundlegende Handgriffe mit vt-cli – von schnellen Batch-Scans über die Anwendung feingranularer Ergebnisfilter bis hin zur gezielten Suche nach relevanten Bedrohungsinformationen auf der VT-Plattform. Praktisch: Das Analysetool ist Bestandteil des Profi-Werkzeugkastens AVCompanion von Desinfec’t 2026/27. Dieser Artikel geht demzufolge auch kurz auf die Verwendung in dieser Distribution ein.

Herunterladen und einrichten

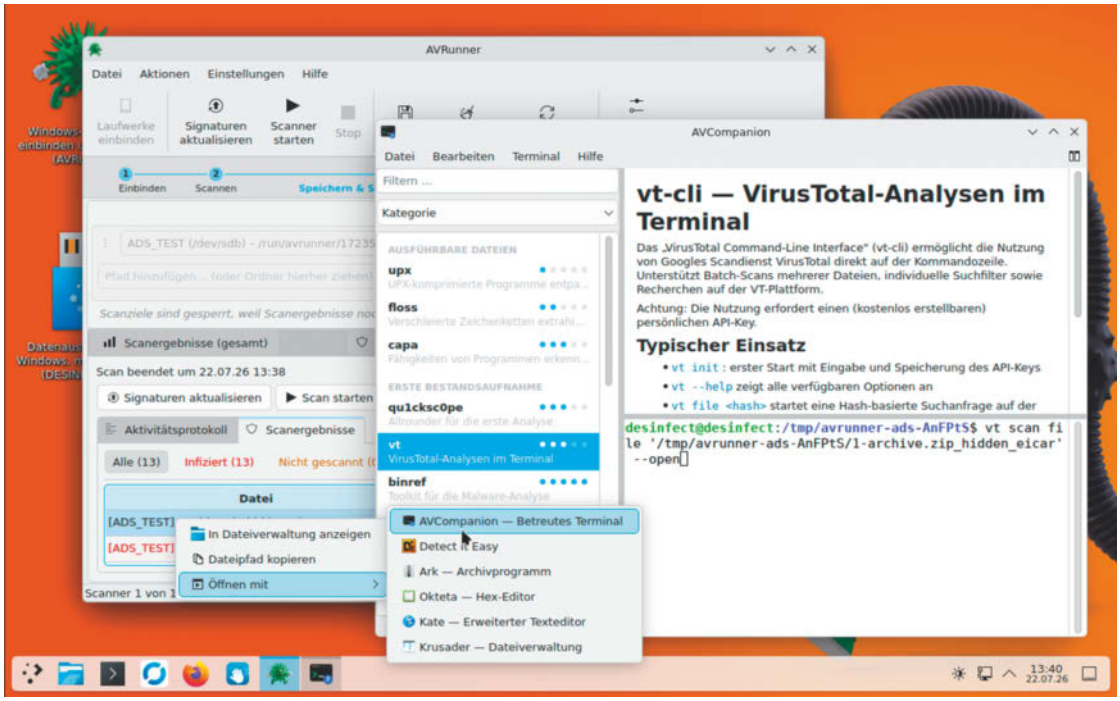
vt-cli ist ein offizielles VirusTotal-Projekt, dessen Quellcode bei GitHub gehostet wird. Am schnellsten bringt man es auf dem eigenen System zum Laufen, indem man auf die fertig kompilierten Binaries zurückgreift. Die stehen zum Veröffentlichungszeitpunkt dieses Artikels in Version 1.2.0 zum Download bereit. Neben vt-cli finden Sie alle in diesem Artikel erwähnten Tools und Verweise auf die VT-Doku über ct.de/wd9d.

Eine Installation ist nicht notwendig: Nach dem Extrahieren der Standalone-Anwendung „vt“ kopieren Sie diese einfach in ein beliebiges Verzeichnis, etwa mit verdächtigen Dateien, und starten Sie mit dem Kommandozeilenbefehl `vt init`. In unserem Testdurchlauf mit Windows 11 sowie mit einer frischen Installation des Debian-basierten Kali Linux in VirtualBox klappte das jeweils problemlos.

In der vt-cli-Dokumentation tummeln sich Anwendungsbeispiele, die die bereitgestellten VirusTotal-



Die Nutzung von vt-cli setzt einen kostenlosen API-Schlüssel voraus. Damit können Sie täglich maximal 500 Anfragen an VirusTotal stellen.



In Desinfec't 2026/27 nutzen Sie vt-cli bequem über die AVCompanion-Software.

Funktionen auf clevere und praktische Weise mit Unix-Befehlen wie `cat` oder `grep` kombinieren. Um diese Beispiele unverändert unter Windows übernehmen zu können, raten die vt-cli-Entwickler zur zusätzlichen Installation der freien Laufzeitumgebung Cygwin. Das Cygwin-Terminal versteht Unix-Befehle und bietet laut vt-cli-Team zudem Performancevorteile gegenüber der Standard-Windows-Konsole bei der Ausgabe großer Textmengen.

In Desinfec't 2026/27 nutzen Sie vt-cli am einfachsten über AVCompanion. Den Profiwerkzeugkasten starten Sie entweder über den „Willkommen"-Bildschirm nach dem Start von Desinfec't oder über das Startmenü. Alternativ können Sie auch nach einem Scan in der Ergebnisliste mit der rechten Maustaste auf einen Fund klicken, um AVCompanion zu öffnen.

Wählen Sie in der linken Seitenleiste „vt" aus. Nun können Sie im rechten Bereich des Fensters unter dem Punkt „Typischer Einsatz" direkt loslegen und etwa über die Option `vt scan file <datei> --open` eine verdächtige Datei direkt zur weiteren Analyse zu VT hochladen. In AVCompanion finden Sie auch Links zur Doku von vt-cli. Im Terminalfenster im unteren Bereich des AVCompanion-Fensters bedienen Sie das Tool über die gängigen Befehle. Alternativ arbeiten Sie mit vt-cli über das normale Terminal in Desinfec't.

Die Schlüssel, bitte!

Unabhängig davon, ob Sie vt-cli im Desinfec't-Kontext oder auf Ihrem Standard-System nutzen, fragt das Tool beim ersten Aufruf via `vt init` nach einem VirusTotal-API-Key. Einen solchen können Sie in der Ausführung „standard free public" kostenlos von der VT-Website beziehen. Dort legen Sie zunächst ein Konto an, loggen sich ein und klicken dann oben rechts auf Ihren Benutzernamen.

Über den Menüpunkt „API Key" sind der kostenlose Schlüssel wie auch Informationen zu den Nutzungsbedingungen und -beschränkungen abrufbar. Insbesondere die Aufforderung, den Schlüssel vor unbefugtem Zugriff zu schützen, sollten Sie dringend beherzigen: Bösewichte missbrauchen gestohlene Keys gern für massenhafte Anfragen, um etwa Verschleierungstaktiken ihres Schadcodes zu testen. Im schlimmsten Fall führt derlei Missbrauch zur Sperrung des Schlüssels.

Schnelle Suche vorab

Nach einmaliger Übergabe des Keys an vt-cli speichert das Tool diesen dauerhaft in einer Konfigurationsdatei im Home- beziehungsweise Benutzerverzeichnis Ihres Systems. Nun ist vt-cli startklar.

An dieser Stelle noch ein wichtiger Hinweis: Wenn Sie Dateien mit Ihrem kostenlosen API-Key zu VT hochladen, sind die Resultate, genau wie bei der Gratis-Nutzung im Browser, dauerhaft online abrufbar – und zwar für alle Nutzer. Achten Sie deshalb unbedingt darauf, keine Dokumente vertraulichen Inhalts zu übermitteln.

Falls Sie bei einer bestimmten verdächtigen Datei unsicher sind, ob Ihr Upload nicht doch ein Datenschutzproblem darstellen könnte, bietet sich ein Alternativweg an: Mit `vt file (Dateihash)` starten Sie eine Suchanfrage auf der VT-Plattform. Ist die Datei dort bereits bekannt und ein Report vorhanden, gibt Ihnen vt-cli dessen Inhalt im Terminal aus.

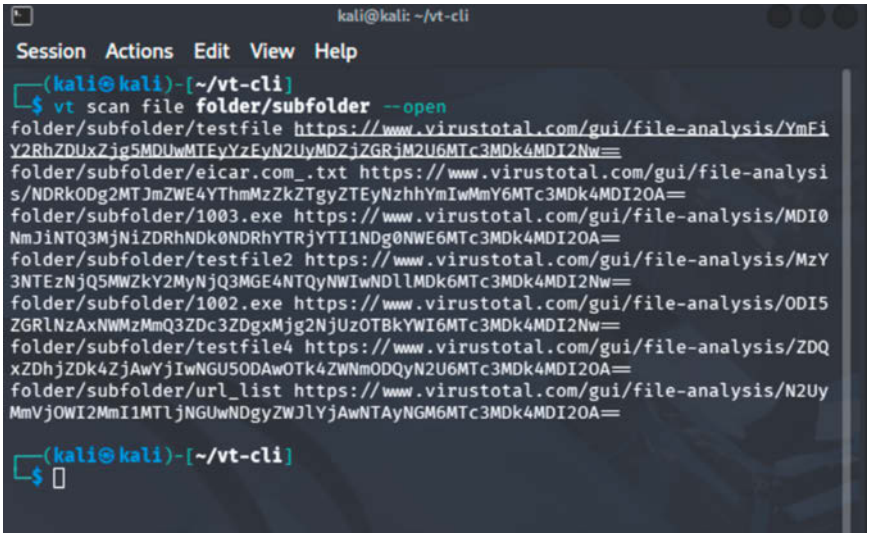
Für die Anfrage benötigen Sie den SHA-256-, SHA-1- oder MD5-Hash Ihrer verdächtigen Datei. Den ermitteln Sie unter Linux mit Kommandozeilentools wie `sha256sum`, `sha1sum` und `md5sum`. Unter Windows können Sie etwa das PowerShell-Cmdlet `Get-FileHash` nutzen. Wer grafische Oberflächen bevorzugt, konsultiert in Desinfec't mit dem Terminalbefehl `die` das Allround-Werkzeug „Detect it Easy" (DiE), hakt dort rechts außen „Fortgeschritten" an und klickt anschließend auf den „Hash"-Button.

Analysieren …

Um ein wenig mit via vt-cli verfügbaren Scan-Funktionen zu experimentieren, genügt es im Zweifel, schnell ein paar harmlose Testdateien zusammenzustellen oder alternativ auf die EICAR-Testdatei (Download siehe ct.de/wd9d) zurückzugreifen. Eine Analyse starten Sie ganz einfach mit `vt scan file (Pfadangabe/Dateiname) --open` beziehungsweise `vt scan url (URL) --open`. Dabei akzeptiert `vt scan` nicht nur URLs, sondern ebenso Domains und IP-Adressen.

Der Parameter `--open` sorgt dafür, dass vt-cli nach erfolgter Analyse Links zu den generierten VirusTotal-Reports auf der Kommandozeile ausgibt, sodass Sie sich in der gewohnten Webansicht durch die Ergebnisse klicken können. Alternativ dazu können Sie sich aber auch mit `--wait` alle Resultate direkt ins Terminal schreiben lassen, sobald die Analyse abgeschlossen ist.

Es lohnt in jedem Fall, sich näher mit den verfügbaren und teils auch kombinierbaren Scan-Parametern zu befassen: So schickt etwa `--password string (Passwort)` das benötigte Kennwort mit, wenn Sie ein geschütztes Schadcode-Archiv an VirusTotal senden. Eine Gesamtübersicht über alle verfügbaren



Im Webbrowser können Sie auf VirusTotal immer nur eine Datei hochladen und prüfen lassen. Erweiterter Funktionsumfang: vt-cli analysiert mehrere Dateien in einem Ordner in einem Rutsch.

Optionen bieten die vt-cli-Doku-Abschnitte zu `scan file` und zu `scan url`.

… in einem Rutsch

Nun aber zurück zu unserem eingangs beschriebenen Batch-Scan-Szenario: Für den Scan mehrerer Dateien oder auch URLs akzeptiert vt-cli Eingaben nach dem Schema `scan file (Datei1) (Datei2) (…)` und `scan url (URL1) (URL2) (…)`.

Noch einfacher lässt sich der Scan eines ganzen Ordners voller verdächtiger Dateien mit dem Einzeiler `vt scan file (Ordnerpfad) --open` abarbeiten.

Wollen Sie wiederum einen ganzen Schwung URLs nacheinander an VirusTotal übermitteln, speichern Sie diese zunächst in einer Textdatei mit einem Eintrag je Zeile. Das Abarbeiten dieser Liste gelingt dann mit vt-cli und dem Unix-Befehl `cat` folgendermaßen:

```
cat (Pfadangabe/URL-Liste)↵
↳ | vt scan url --open
```

Dabei schickt `vt scan url` den via `cat` ausgelesenen Dateiinhalt zeilenweise zur Analyse weiter. Im Anschluss liefert `--open` wie gewohnt zu jeder URL den erzeugten VT-Link zurück.

Kurze Einschätzung

Sie haben keine Zeit, umfangreiche Analyseberichte zu wälzen, und wünschen sich, etwa bei der Incident Response mit Desinfec't, einfach nur eine schnelle Bedrohungseinschätzung auf der Kommandozeile?

In diesem Fall verzichten Sie beim Aufruf von `vt scan` komplett auf Parameter wie `--open` oder `--wait`. Statt VT-Links oder Reports gibt vt-cli dann einfach nur eine Analyse-ID in Gestalt eines Hashes zurück. Diese reichen Sie an den Befehl `vt analysis (ID)` weiter. Der schreibt lediglich die Resultate der Scan-Engines ins Terminal und verzichtet auf Zusatzinformationen wie Verhaltensanalysen oder Community-Kommentare.

Kombiniert mit Unix-Befehlen lässt sich diese Ausgabe noch weiter filtern, etwa so:

```
vt analysis (Analyse-ID)↵
↳ | grep "category:" | sort
↳ | uniq -c
```

`grep` sucht in der Analyse alle Vorkommen des Begriffs „category“. VirusTotal nutzt diesen intern, um die Rückgaben der Scan-Engines in Kategorien wie „harmless“, „malicious“ und „undetected“ einzuordnen und Scanfehler zu protokollieren. Die Befehle `sort` und `uniq -c` sortieren die gefundenen Zeilen alphabetisch, zählen deren Vorkommen und entfernen Doppler vor der Ausgabe. Die könnte dann beispielsweise so aussehen:

– 1 category: "failure"
– 54 category: "malicious"
– 6 category: "timeout"
– 4 category: "type-unsupported"
– 11 category: "undetected"

Sie wissen jetzt, dass 54 Scanner die Datei oder URL für schädlich halten – eine recht klare Einschätzung. Auf ähnliche Weise gelingt übrigens auch eine schnelle Abfrage der herstellerspezifischen Malware-Aliases nach einem Dateiscan: Ersetzen Sie einfach `category:` durch `result:`.

Wissenswert für Entwickler: Über die Analyse-IDs sind Scan-Ergebnisse dauerhaft referenzierbar. Somit kann man die IDs auch verwenden, um etwa im Zuge umfangreicher Systemscans Resultate „zwischenzuspeichern“ und weiterzuverarbeiten, statt sie sofort auszugeben.

Hilfe bei der Aufklärung

Wenn ein System mit Schadsoftware infiziert wurde, stehen Sie vor größeren Problemen als nur einer einzelnen infizierten Datei. Es gilt dann, zahlreiche Einbruchspuren (Indicators of Compromise, IoCs, siehe ct.de/wd9d) systematisch auszuwerten und sie zueinander in Beziehung zu setzen, um das Geschehen zu rekonstruieren und adäquat darauf reagieren zu können.

Vorhandene VirusTotal-Reports können auch in diesem Zusammenhang eine wertvolle Recherchequelle darstellen. Mit vt-cli zapfen Sie diese ganz nach Bedarf an: via `vt file (Hash)`, alternativ aber auch mit den Befehlen `vt domain (Domain)`, `vt ip (IP-Adresse)` und `vt url (URL)`, sofern Ihnen etwa verdächtige Netzwerkaktivitäten oder Informationen aus Firewall-Logs als Ausgangspunkt dienen.

Die große Stärke von Anfragen via vt-cli gegenüber der Suchfunktion auf der VT-Website offenbart sich, wenn man die verfügbaren Befehlsergänzungen nutzt. Statt sich einfach komplette Reports zurückliefern zu lassen, kann man die Suche spezifizieren, um im Zuge der Incident Response wesentliche Fragen zu klären. Hier ein paar Beispiele:

- Auf welche konkreten Schädlinge weist von mir beobachteter beziehungsweise mitgeloggter Traffic hin? Die Befehle `vt domain reports`, `vt ip reports` und `vt url reports`, gefolgt von der jeweiligen Zieladresse, spüren alle VT-Analysen auf, in denen diese Adressen auftauchen.
- Umgekehrt kann man mit den Befehlen `vt file contacted_urls`, `vt file contacted_ips` und `vt file contacted_domains`, jeweils gefolgt vom Schadcode-Hash, herausfinden, mit welchen Gesprächspartnern im Web aufgespürte Malware kommuniziert.
- Hat mein ursprünglich analysierter Schadcode noch weitere Dateien aufs System geschleust? Sollte dem so sein, gibt `vt file dropped_files (Hash)` einen oder mehrere Hashes der gedroppten Malware aus der VT-Datenbank zurück. Mit erneuten `vt file`-Aufrufen können Sie dann direkt weiterrecherchieren.

Alle verfügbaren Befehlsergänzungen finden Sie in den Doku-Abschnitten zu `vt file`, `vt domain`, `vt ip` und `vt url`.

Ausprobieren lohnt sich

Kommandozeilenaffinität vorausgesetzt, ist vt-cli eine echte Bereicherung für alle, die die gewohnten VirusTotal-Funktionen flexibler und zielgerichteter nutzen wollen. Im Desinfec't-Kontext stellen VT-Reports eine nützliche Ergänzung zu den individuellen Resultaten der ins Live-System integrierten Scanner dar. Denn die VirusTotal-Multi-Scans ermöglichen, potenzielle Virenfunde – oder auch vermeintlich „saubere" Dateien – im Zweifel nochmals gegenzuchecken und so das Risiko von Fehlerkennungen zu reduzieren.

Die von vt-cli bereitgestellten Recherchemöglichkeiten lassen sich außerdem wunderbar mit Ergebnissen von weitere Analysetools kombinieren, sodass im besten Fall ein umfassendes Gesamtbild der analysierten Bedrohung entsteht. Ein Beispiel hierfür: Die in Desinfec't eingebauten Tools zum Durchleuchten potenzieller Phishing-PDFs wie pdfparser und pdfid von Didier Stevens finden unter anderem verdächtige Links in inspizierten Dokumenten. Ein PDF-Upload zu VT oder auch die gezielte Suche etwa via `vt url reports` könnte im nächsten Schritt Hinweise auf eine spezifische Phishing-Kampagne, verwandte Angriffsmaschen und bestenfalls auch konkrete kriminelle Akteure geben.

Last, but not least können auch Programmierer von vt-cli profitieren. Die verfügbaren Befehle erleichtern ihnen das Umsetzen eigener Projekte – von stark individualisierten Scans bis hin zu exakt zugeschnittenen Suchanfragen an VT als Wissensdatenbank.

Ein guter Ausgangspunkt, um sich mit den hier angesprochenen sowie weiteren Features vertraut zu machen, ist neben der ausführlichen vt-cli-Doku die via `vt help` auf der Kommandozeile abrufbare Übersicht über alle Befehle.

Grenzen setzt der Funktionsumfang des kostenlosen API-Keys, der Premium-Features wie etwa Malware-Downloads oder Zugriff auf den „VT Hunting"-Service ausklammert und die Zahl der täglichen VT-Anfragen auf 500 begrenzt. Diese recht großzügigen Beschränkungen lassen jedoch reichlich Raum für die maßgeschneiderte Malware-Jagd mit vt-cli. Viel Spaß beim Experimentieren! (des) c't

Downloads und Dokumentation:
ct.de/wd9d





Bild: Jessica Nachtigall / KI / heise medien

PDF- oder Word-Dateien untersuchen

Desinfec't 2026/27 eignet sich nicht nur für die Virenjagd, sondern hält auch nützliche Profiwerkzeuge bereit, um verdächtige Dokumente vor dem Öffnen zu analysieren oder dem Ursprung von Schadcode-Infektionen nachzuspüren. Oft handelt es sich dabei um harmlos wirkende Office- oder PDF-Dateien, die unter einem Vorwand im E-Mail-Postfach potenzieller Opfer lauern.

Von **Olivia von Westernhagen**

Werkzeuge wie QPDF, pdf-parser und die oletools-Sammlung helfen, die Funktionsweise dokumentenbasierter Malware- und Phishing-Angriffe aufzuschlüsseln. Wo man diese und weitere nützliche Helfer für die Dokumentenanalyse im neuen Desinfec't 2026/27 findet und wie man sie anwendet, erläutert dieser Artikel anhand zweier praktischer Beispiele. Diese können Sie – am besten direkt in der Desinfec't-Umgebung – herunterladen und selbst ausprobieren (Download siehe ct.de/wrka).

Wichtige Hinweise vorweg

Die hier vorgestellten Werkzeuge richten sich primär an Nutzer mit Expertenwissen in der Malwareanalyse, die potenzielle Infektionsherde untersuchen wollen. Doch auch interessierte Laien können damit experimentieren, da man mit ihnen, anders als mit manch anderen Profi-Tools aus dem Desinfec't-Werkzeugkasten wie dem Windows-Registryeditor FRED, keinerlei Schaden am System anrichten kann.

Das erste Beispiel (beispiel1.pdf) stammt aus einer echten Phishing-Kampagne und sollte daher mit angemessener Vorsicht seziert werden – trotz zum Zeitpunkt der Veröffentlichung inaktivem Phishing-Link. Demzufolge sollte die Analyse nicht auf Ihrem Produktiv-PC unter Windows, sondern unter Desinfec't stattfinden. Das zweite Beispiel (beispiel2.doc), ein von der Autorin dieses Artikels selbst erstelltes Word-Dokument mit eingebettetem Makro-Code, ist hingegen vollkommen harmlos.

Bei jedem Malware-Experiment gilt es im Hinterkopf zu behalten, dass das Desinfec't-System jetzt, anders als in früheren Versionen, vollständig persistent ist. Sämtliche vorgenommene Änderungen überdauern also unabhängig vom Speicherort den Reboot. Umso wichtiger ist es, sorgsam mit dem System umzugehen und sich Expertentools und Schadcode stets mit großem Respekt zu nähern. Wenn doch mal etwas schiefgeht, setzen Sie den Desinfec't-Datenträger im Menü „Desinfec't-Helfer" über die Option „Wiederherstellen: Werkseinstellungen" im Desinfec't Bootmenü zurück. Dabei gehen alle Änderungen verloren und Desinfec't befindet sich wieder im Urzustand.

Werkzeuge neu sortiert

Das Passwort für das Archiv mit den Beispieldateien lautet „infected". Entpacken Sie diese am besten in einem eigens dafür angelegten Ordner etwa auf dem Desinfec't-Desktop. Dabei hilft das Programm Ark zur Archivverwaltung (Rechtsklick auf den Download, „Mit Ark öffnen") .

Die kommandozeilenbasierten Expertentools sind in der aktuellen Desinfec't-Version umgezogen: Statt über einen speziellen Ordner sind sie nun zentral über den neuen „AVCompanion", einer Tool-Übersicht mit integriertem Terminal, aufrufbar.

In unserem speziellen Anwendungsfall starten Sie den sachkundigen Begleiter am bequemsten, indem Sie direkt in Ihrem neu angelegten Malware-Test-Verzeichnis ein Terminal öffnen und `avcompanion` eintippen. Alternativ können Sie den AVCompanion auch direkt beim Desinfec't-Start auf dem „Willkommen"-Bildschirm auswählen. Die dritte Option ist, ihn nach einem Scan in der Ergebnisliste per Rechtsklick auf einen Verdachtsfall zu starten.

Mit Programmbeschreibungen sowie per Klick direkt ins Terminal kopierbaren Kommandozeilenparametern („Typischer Einsatz") erleichtert AVCompanion das Auffinden und den Umgang mit den Tools. Die Nutzung ist jedoch optional, und sie können sämtliche Tools auch weiterhin über das Standard-Terminal starten und bedienen.

PDF-Beispiel seziert

AVCompanions Übersicht gliedert die verfügbaren Kommandozeilenwerkzeuge nach ihrem schwerpunktmäßigen Einsatzzweck. Für die Analyse des ersten Beispiels sind primär die Tools der Kategorie „PDF-Analyse" interessant.

Um einen ersten Überblick über die Eigenschaften des Dokuments zu erhalten, eignet sich insbesondere das Pythonskript pdfid von Sicherheitsforscher Didier Stevens: Es durchsucht PDF-Dateien nach



Über das integrierte Terminal des neuen AVCompanion sind alle enthaltenen Tools direkt auf verdächtige Dateien anwendbar.

spezifischen Strings, die Auskunft über zentrale Dokumenteigenschaften geben – so etwa über die Anzahl der Seiten („/Page“), aber auch über potenziell schädliche Inhalte wie ausführbaren JavaScript-Code („/JavaScript“) oder eingebettete Dateien („/EmbeddedFile“).

String-Funde werden mitsamt ihrer Anzahl im Terminal zurückgegeben. Wer mehr über die Bedeutung aller ausgewerteten Strings erfahren möchte, kann in den PDF-Dokumentspezifikationen nachschlagen (ct.de/wrka).

Der Befehl für den Aufruf lautet:

```
pdfid beispiel1.pdf
```

Das Tool findet unter anderem den String „/Encrypt 1“, der verrät, dass das Dokument mit einem Passwort verschlüsselt wurde. Derlei Verschlüsselungen wenden Angreifer im Rahmen von Phishing-Kampagnen bisweilen an, um zu verhindern, dass schädliche PDF-Anhänge in E-Mails von Schutzlösungen erkannt und abgefangen werden. Das zugehörige Passwort fügen die Kriminellen unter dem Vorwand vertraulicher Inhalte häufig als Bild in die Nachricht ein – lesbar für Menschen, nicht aber ohne Weiteres für automatische Erkennungsmechanismen.

Passwort entfernen mit QPDF

Werkzeuge zur manuellen Schadcode-Analyse werden von verschlüsselten PDFs auf eine harte Probe gestellt: Sie spucken Kauderwelsch aus oder kapitulieren gar vollständig. Aus diesem Grund muss im nächsten Schritt erst einmal das Passwort – und damit auch die Verschlüsselung – weichen. Für diesen Einsatzzweck hat Desinfec’t QPDF an Bord [1]. Das Tool stellt vielfältige Werkzeuge zur Bearbeitung von PDF-Dateien bereit; im Kontext der Dokumentenanalyse ist jedoch primär die Entschlüsselungsfunktion relevant. Um die zu nutzen, bedienen Sie sich folgender Terminal-Syntax:

```
qpdf --decrypt beispiel1.pdf↵
↳ beispiel1-decrypted.pdf↵
↳ --password=1234
```

QPDF legt die entschlüsselte Datei unter dem Namen „beispiel1-decrypted.pdf“ im selben Verzeichnis ab. Mit `qpdf --check beispiel1-decrypted.pdf` können Sie sich vom Erfolg der Entschlüsselung überzeugen: Lautet die Rückgabe „file is not encrypted“, hat alles geklappt.

In unserem Beispiel lautet das Kennwort einfachheitshalber schlicht „1234“. Leider funktioniert das Entschlüsseln mit QPDF grundsätzlich nur dann, wenn man das Passwort kennt. Ansonsten hilft es nur, das Dokument etwa mit einem Tool wie dem kostenlosen pdfrip zum automatisierten Durchprobieren von Passwörtern (Bruteforce) zu knacken.

Tiefer graben

Auch das Anwenden von pdfid auf beispiel1-decrypted.pdf bestätigt die erfolgreiche Entschlüsselung: Das Tool meldet „/Encrypt 0“. Nun ist es an der Zeit, sich mit den übrigen String-Funden auseinanderzusetzen. Interessant ist unter anderem die Zeile „/ObjStm 1“, die auf einen im PDF enthaltenen „Object Stream“ hindeutet. Solche Datenströme fassen mehrere Objekte in komprimierter Form zusammen. Die Idee dahinter ist, die PDF-Größe zu reduzieren – Angreifer können das Feature aber auch missbrauchen, um schädliche Inhalte vor neugierigen Blicken zu verbergen.

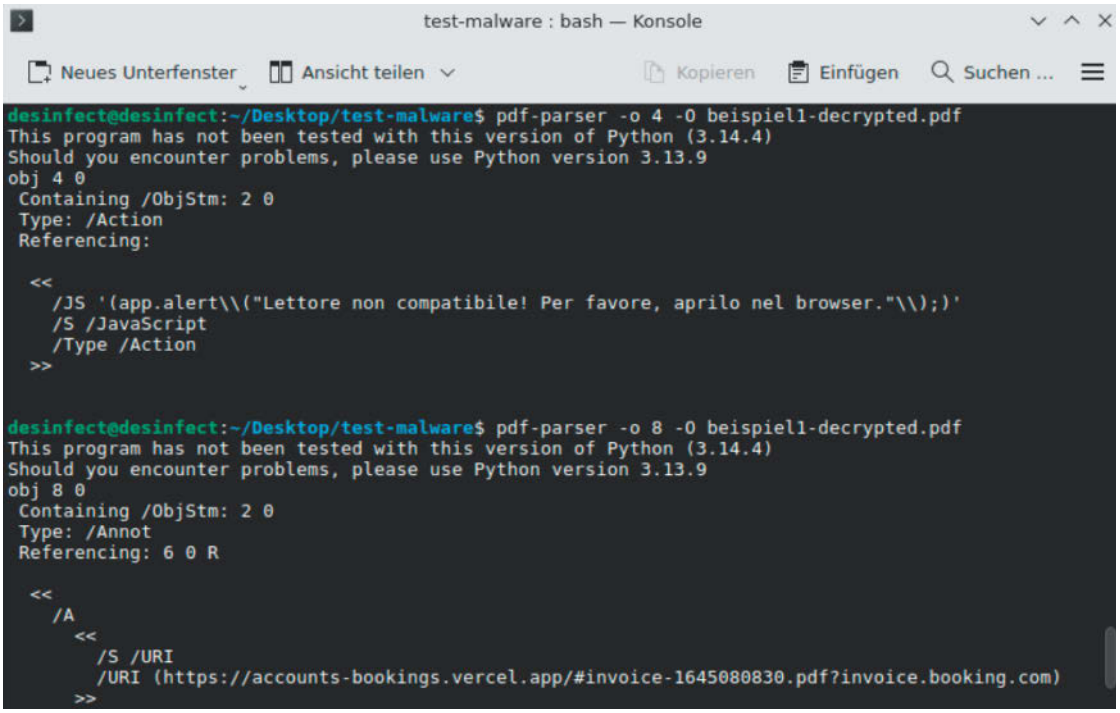
Ebenfalls verdächtig: Der „/OpenAction 1“-Eintrag verrät, dass beim Öffnen des PDFs eine automatisierte Aktion ausgeführt wird, die es in jedem Fall zu untersuchen gilt. Um weitere PDF-Geheimnisse ans Tageslicht zu holen, müssen Sie im nächsten Schritt die Datenströme analysieren. Dabei hilft pdf-parser, ein weiteres Tool von Didier Stevens, unter Verwendung folgender Terminal-Eingabe:

```
pdf-parser -a -O↵
↳ beispiel1-decrypted.pdf
```

Das Flag „-O“ parst die vorhandenen Streams, während „-a“, ähnlich wie in pdfid, gefundene Schlüsselbegriffe nebst nummerierter Verweise auf konkrete Objekte zurückgibt. Diese Objektnummern vergibt pdf-parser nicht selbst, sondern zieht sie direkt aus der Dokumentstruktur. Dort haben sie die Aufgabe, Objekte direkt referenzier-, also über die Nummer ansprechbar zu machen.

Besonders spannend sind in unserem konkreten Beispiel folgende vom pdf-parser gefundene Begriffe:

- /XObject verweist auf zwei Grafikobjekte im PDF.
- /JavaScript verrät uns, dass eines der gefundenen Objekte ein verborgenes Skript ist.
- /OpenAction verknüpft die bereits von pdfid erkannte Aktion beim Öffnen mit einer konkreten Objekt-



Beispiel 1 durchleuchtet: Der pdf-parser macht verborgene Inhalte wie JavaScript-Pop-ups oder schädliche Webadressen sichtbar.

nummer. Wie Sie beim Ausprobieren im Terminal sehen werden, ist das in unserem Beispiel die 1.
- /URI verweist auf eine Ressource aus dem Web.

Zum detaillierten Betrachten der einzelnen Objekte müssen Sie diese nach dem Schema

```
pdf-parser -o [Objektnummer] -O↵
↳ beispiel1-decrypted.pdf
```

parsen lassen, wobei auf „-o“ jeweils die dem Objekt zugeordnete Nummer folgt – in der Beispieldatei etwa die 4 für „/JavaScript“ oder die 8 für „/URI“.

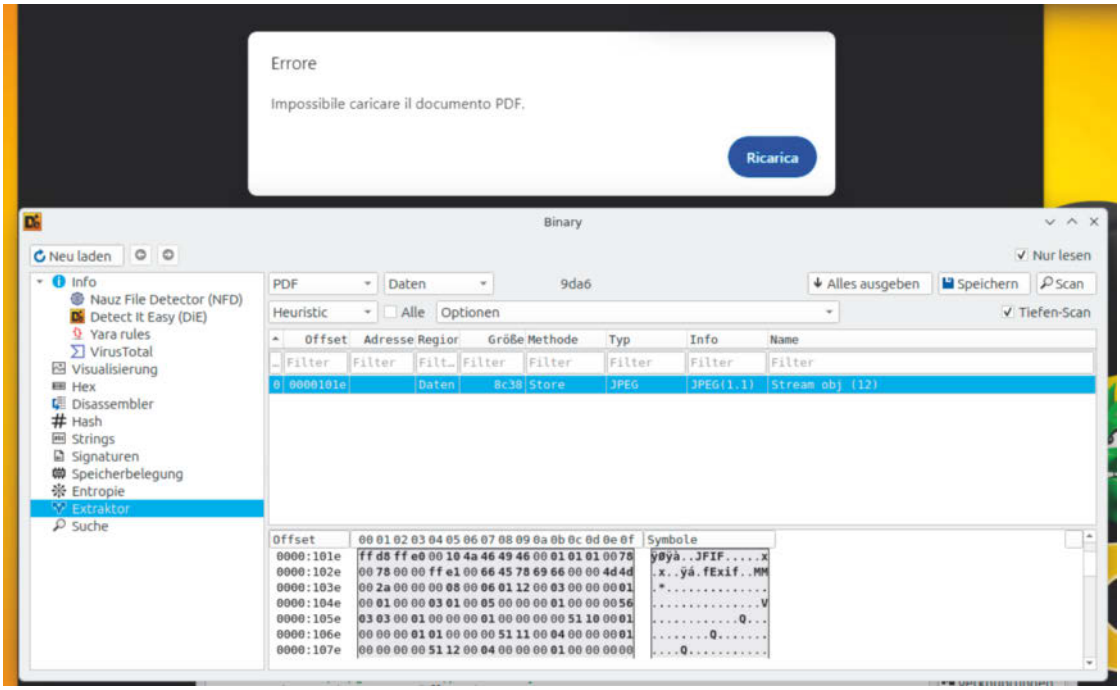
Die Analyse der zuvor genannten Objekte verrät Ihnen Folgendes:

- „OpenAction“ referenziert das JavaScript (4), ruft es also auf, wenn der Nutzer das PDF öffnet.
- Das Skript selbst gibt eine italienischsprachige Nachricht als Pop-up aus, die besagt, dass der PDF-Viewer nicht mit dem Dokument kompatibel sei und man es stattdessen im Browser öffnen solle.
- Ins PDF eingebunden sind außerdem eine Abbildung (eingebettet in ein „äußeres“, Koordinaten vorgebendes Grafikobjekt) sowie die bereits erwähnte URI.
- Letztere gibt offenbar vor, auf online abrufbare Rechnungsinformationen zu verweisen. Sie enthält die Strings „account-bookings“ und „booking.com“ – vermutlich, um den Anschein einer Hotelbuchung zu erwecken.

Das große Ganze

Um zu guter Letzt auch noch die Abbildung aus dem PDF zu extrahieren und anzusehen, verwenden Sie am bequemsten „Detect it Easy“(DiE). Das Allround-Werkzeug kann mit einer Vielzahl von Dateitypen umgehen, diese statisch analysieren und enthaltene Ressourcen extrahieren.

Als Tool mit grafischer Oberfläche ist DiE kein Bestandteil des AVCompanion. Stattdessen gehen Sie im konkreten Fall den Weg über die Kommandozeile: Nach Eingabe von `die beispiel1-decrypted.pdf`



Mit wenigen Klicks extrahiert „Detect it Easy“ (DiE) die gefälschte Fehlermeldung (oben im Bild) aus dem PDF-Beispiel.

öffnet sich das GUI. Alternativ ist DiE auch per Rechtsklick im Dateimanager („Öffnen mit“) sowie über den AVRunner auswählbar.

Setzen Sie rechts auf der grafischen Oberfläche den Haken „Fortgeschritten“ und klicken Sie anschließend auf den „Extraktor“-Button. Markieren Sie dann die Zeile mit der JPEG-Datei, welche DiE im PDF aufspürt, und klicken Sie auf „Alles ausgeben“.

Genau wie das zuvor mit dem pdf-parser aufgespürte JavaScript-Popup will das extrahierte Bild den Nutzer beim Öffnen des PDFs dazu bringen, eine dubiose Website aufzurufen: Es gebe Probleme beim Anzeigen des PDF-Inhalts, verkündet eine vermeintliche Fehlermeldung („Errore“). Ein blauer Fake-Button soll zum Klicken animieren. Er ist mit „Ricarica“ beschriftet, was auf Italienisch so viel „Neu laden“ bedeutet. Im PDF-Kontext führt er zum vermeintlichen Buchungslink, den Sie zuvor mit pdf-parser ausgegraben haben.

Eine VirusTotal-Analyse des PDFs (siehe ct.de/wrka) ergänzt noch fehlende Puzzleteile zum Verstehen der Phishing-Masche. So erfährt man etwa aus dem „Community“-Reiter des Reports, dass die Datei ursprünglich unter dem Namen invoice-1645080830.pdf kursierte. Offenbar sollten Empfänger dazu verleitet werden, im PDF nach Informationen zur angeblichen (Hotel-)Rechnung zu suchen – und letztlich auf den Link zu klicken. Weitere Report-Details verweisen auf beabsichtigten Datendiebstahl über die (mittlerweile inaktive) Phishing-Seite der Angreifer.

Abschließend noch ein Hinweis: Möglicherweise ist Ihnen beim Analysieren aufgefallen, dass der Dateihash von beispiel1.pdf von jenem aus der unter ct.de/wrka verlinkten VT-Analyse („Originaldatei“) abweicht. Das liegt daran, dass wir die Passwortverschlüsselung nachträglich ergänzt haben, um Ihnen die ganze Bandbreite der in Desinfec’t verfügbaren PDF-Analysetools an einem einzigen Beispiel zu demonstrieren.

Office-Dokument durchleuchtet

Ein weiteres seit Jahren unverändert beliebtes Einfallstor für Angreifer sind Office-Dokumente mit Endungen wie .doc, .docm oder auch .xls/.xlsm, in denen ausführbarer Code in Gestalt von Makros lauern kann.

Entsprechend unverzichtbar in Desinfec’t ist eine Toolsammlung zur Analyse solcher Dokumente. Sie heißt oletools und besteht derzeit aus rund einem

Dutzend Einzelwerkzeugen, die der AVCompanion in der Kategorie „Office-Dokumente“ aufschlüsselt. Die meisten der Tools durchleuchten Dateien des älteren OLE2-Formats mit den erwähnten Endungen. Einige Tools zielen aber auch auf das aktuellere Office-Open-XML-Format (z.B. .docx, .xlxs) sowie auf das Rich Text Format (.rtf) ab.

Unser „beispiel2.doc“ eignet sich perfekt, um insbesondere mit den folgenden Werkzeugen aus der oletools-Sammlung zu experimentieren:

- oleid analysiert OLE-Dateien im Hinblick auf typische Malware-Charakteristika.
- mraptor („MacroRaptor“) sucht speziell nach schädlichen VBA-Makros.
- olevba geht ins Detail: Es untersucht Makro-Code und versucht, verschleierte Funktionen und Strings zu entschlüsseln.

Spezifische Parameter benötigen die Werkzeuge (zunächst) nicht: der Aufruf erfolgt jeweils via [Toolname] beispiel2.doc.

Makro-Code aufgeschlüsselt

Im ersten Schritt liefert oleid Informationen etwa zu Dateiformat und Autor des Dokuments. Überdies entdeckt es auch den im Beispiel enthaltenen VBA-Makro-Code. An ihm führt es einen Abgleich mit potenziell verdächtigen Keywords durch, findet keine und stuft das potenzielle Risiko erst einmal vorsichtig als „Medium“ ein.

Im zweiten Schritt findet mraptor im Makro einen sogenannten „Auto-execution trigger“. Was das konkret bedeutet, kann olevba beantworten: Das Tool zeigt den Makro-Code direkt im Terminal an, ohne dass Sie das potenziell gefährliche Dokument öffnen müssen.

Der Methodenname „AutoOpen()“ sorgt dafür, dass das Makro beim Öffnen des Dokuments automatisch ausgeführt wird. Der enthaltene Code öffnet eine Messagebox (`MsgBox`). Vollständig in olevba lesbar ist deren Text allerdings nicht: Ein Hex-String sowie einzelne mittels `Chr()`-Funktion dargestellte ASCII-Zeichen stellen in unserem Beispiel den Versuch nach, einen Angriff zu verschleiern. Glücklicherweise identifiziert olevba derlei Standardtricks automatisch, gibt die entsprechenden Passagen in einer Tabelle aus und markiert sie als verdächtig.

Die zusätzlichen Switches `--decode` und `--deobf` machen den Text schließlich lesbar:

```
olevba --decode -deobf↵
↳ beispiel2.doc
```

Sofern sich nun aus olevbas Rückgaben die Nachricht „Alles entschluesselt!!“ zusammensetzt, haben Sie alles richtig gemacht.

Falls Sie Lust haben, können Sie an unserem Beispiel noch weitere oletools ausprobieren. So extra-

Literatur

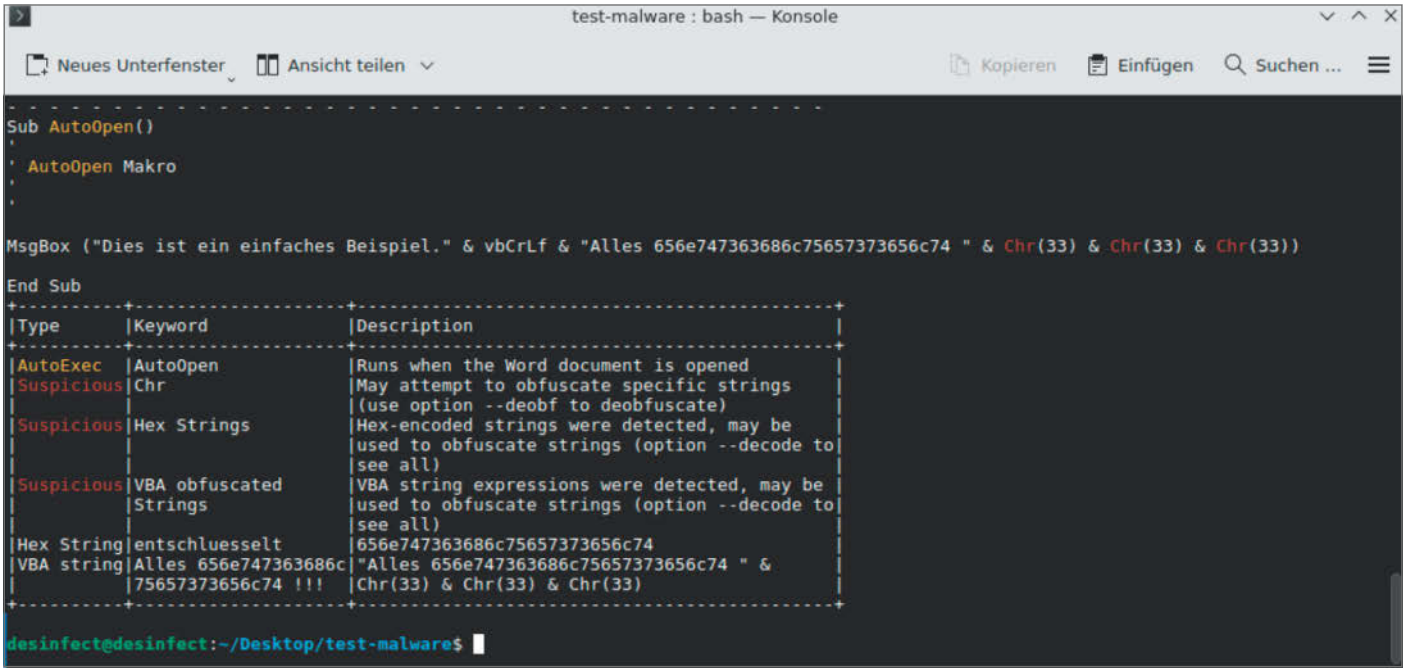
[1] Olivia von Westernhagen, PDF-Analyse statt Passwort, Desinfec’t: Potenziell gefährliche PDF-Dokumente mit QPDF entschlüsseln, c’t 6/2025, S. 140

[2] Olivia von Westernhagen, Schneller durchblicken, Qu1cksc0pe in Desinfec’t ermittelt Schadpotenzial von Dateien, c’t 26/2024, S. 158

Downloads und Dokumentation:

ct.de/wrka





Extrahiert und entschlüsselt: olevba aus der oletools-Sammlung macht verborgenen Makro-Code sicht- und vor allem auch lesbar.

hiert etwa olemeta sämtliche Metadaten aus dem Dokument. Mit olebrowse können Sie sich mittels GUI durch die Dateistruktur klicken und Datenströme in Hexadezimal-Ansicht betrachten.

Was leider keines der Werkzeuge aus der Sammlung kann, ist, die im Beispiel verborgene Abbildung zu extrahieren. Glücklicherweise wissen Sie ja jetzt bereits, wie sich dies ganz einfach mit DiE bewerkstelligen lässt.

Viele Wege zum Ziel

Anhand unserer Beispiele sollten Sie einen recht guten Eindruck von den Desinfec't-Tools gewonnen haben, die speziell für die Dokumentenanalyse gedacht sind. Unbedingt noch erwähnenswert ist, dass zwei Multifunktions-Tools aus der AVCompanion-Kategorie „Erste Bestandsaufnahme" ebenfalls entsprechende Funktionen mitbringen.

Zum einen stellt Qu1cksc0pe [2], ein Werkzeug mit vielfältigen Scanfunktionen, den Switch `--docs` zum Durchleuchten von Office-Dokumenten wie auch PDF-Dateien bereit. Es erkennt dabei sowohl die AutoExec-Funktion in unserem PDF als auch den Makro-Code in unserem .doc-Beispiel. Mit dem folgenden Aufruf

```
qu1cksc0pe --file (Dateiname) --docs
```

können Sie das ausprobieren. Außerdem bringt Binary Refinery (siehe S.60) gleich mehrere Module, sogenannte Units, mit, die Sie mit den beiden Dateien ausprobieren können.

Weiterhin nützlich ist die Unit pdfcrypt als QPDF-Alternative zur Passwortentfernung. Auf das verschlüsselte Beispiel-PDF wenden Sie sie an, indem Sie unter Eingabe von `refinery-shell` ins Terminal das Toolkit starten und anschließend eingeben:

```
emit beispiel1.pdf | pdfcrypt 1234↵
↳ | dump beispiel1-decrypted.pdf
```

Der Befehl entschlüsselt das PDF unter Verwendung des bekannten Passworts und speichert die entschlüsselte Kopie im selben Verzeichnis.

Sicherlich werden Sie noch auf weitere Wege und Möglichkeiten stoßen, verdächtigen Dokumenten ihre Geheimnisse zu entlocken. (des) c't



MEHR ALS EIN SWIPE – WISSEN DAS BLEIBT.

Mac & i

2× Mac & i mit 35 % Rabatt testen!

- Tipps & Praxiswissen für Apple-Insider
- Spannende Produkttests von Hard- und Software
- Workshops rund um die Apple-Produkte



\+ Geschenk nach Wahl

Adapter-Kabelbox oder Buch „Apple Junkies“



Jetzt bestellen:

www.mac-and-i.de/vorteil

leserservice@heise.de 0511 / 647 22 888

Mac & i. Das Apple-Magazin von c’t.

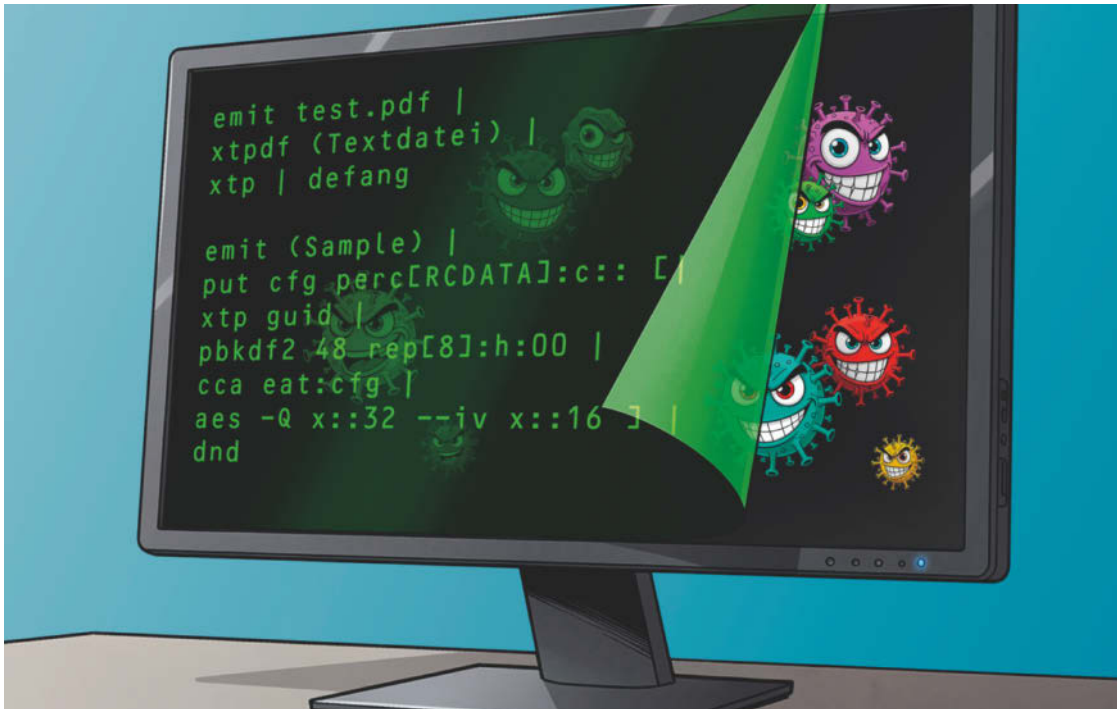


Bild: Ulrike Weis / KI / heise medien

Malware-Analyse mit Binary Refinery

Ein leistungsstarkes und kostenloses Profi-Toolkit unterzieht Schadcode und andere Bedrohungen einer Bestandsaufnahme – auch Einsteiger können mit den flexiblen Befehlen auf der Kommandozeile erste Schritte wagen.

Von **Olivia von Westernhagen**

Bei einer frisch entdeckten Infektion mit Malware kommt es buchstäblich auf jede Minute an: Je schneller die erste Bedrohungseinschätzung (Triage) gelingt, desto zeitnaher lassen sich geeignete Maßnahmen ableiten und ergreifen, um die Gefahr effektiv zu bekämpfen.

Da ist es hilfreich, wenn man typische Arbeitsabläufe der Analyse mit möglichst wenigen Tools erledigen kann. Oder, noch besser, mit nur einem einzigen: Binary Refinery. Das Projekt vereint zahlreiche nützliche Triagefunktionen und ermöglicht, diese auf der Kommandozeile flexibel zu kombinieren. So kann man etwa mit einem einzigen Befehl Schadcode aus einem Archiv extrahieren, ihn nach verschlüsselten Strings durchsuchen, die Funde dekodieren und sie schließlich in einer separaten Datei speichern.

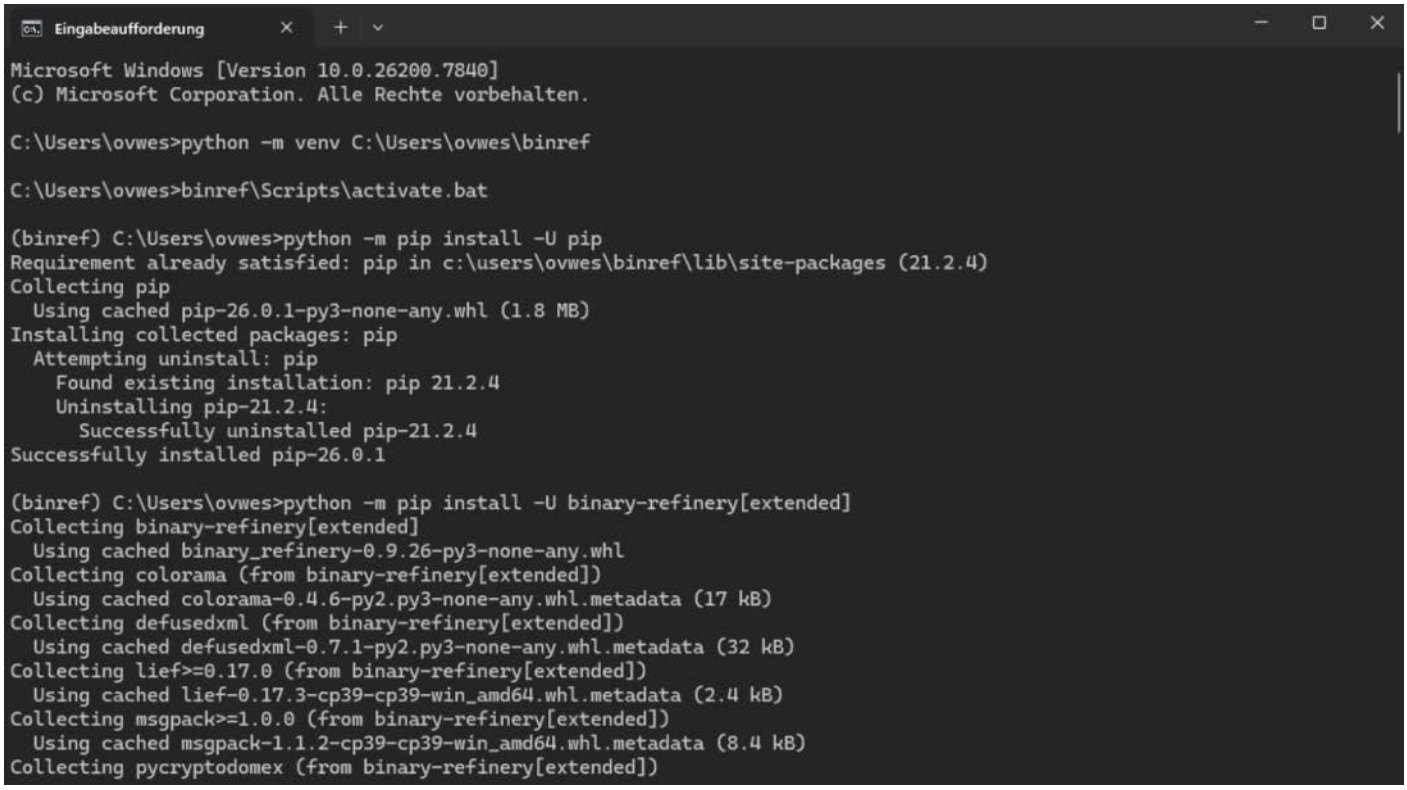
Derlei schnelle, maßgeschneiderte Untersuchungen lassen sich mit Binary Refinery auf unterschiedlichste Formate anwenden – von der Executable über Office-Dokumente und verschlüsselte Strings bis zum obfuskierten, also künstlich verkomplizierten und verschleierten Downloader-Skript.

Im Artikel stellen wir das kostenlose, auf einer umfangreichen Sammlung von Python-Skripten fußende Toolkit für Windows und Linux kurz vor. In Desinfec't 2026/27 finden Sie die Tools im Profiwerkzeugkasten AVCompanion. Dabei geben wir einfache Anwendungsbeispiele, die nicht nur für die detaillierte Analyse von Schadcode, sondern etwa im Zuge einer schnellen Suche nach möglichen Kompromittierungsindikatoren (Indicators of Compromise, IoCs) hilfreich sein können. Einige Anwendungsfälle wie etwa das Extrahieren von URLs oder IP-Adressen aus Text- oder Logdateien per simpler Befehlssequenz dürften auch für Nutzer spannend und praktisch sein, die mit Schadcode gar nichts am Hut haben.

Generell richtet sich Binary Refinery jedoch primär an Profis, die ihre Analyseabläufe optimieren und dabei von maximaler Flexibilität auf der Kommandozeile profitieren wollen. Wer ohne viel Einarbeitungszeit – und sogar ohne vorherige Installation – Lust hat, einfach mal mit kombinierten Datenoperationen zu experimentieren, kann sich stattdessen mit der Webversion von CyberChef austoben. Die Anwendung erlaubt das Kombinieren verschiedenster Operationen per Drag & Drop und gibt die Resultate direkt auf der GUI zurück.

Toolkit in Aktion

Um den Anwendungsfall aus dem ersten Absatz ganz ohne Malware gefahrlos nachzustellen, legen Sie eine Textdatei namens test.txt an. Tippen Sie ein



Schnell erledigt: Die Binary Refinery-Installation in einem isolierten Ordner mit venv, hier per Windows-Eingabeaufforderung.

wenig Text hinein und platzieren Sie dann den folgenden Base64-kodierten String dazwischen:

```
RXJmb2xncmVpY2ggZW5Oc2NobHVlc3NlbHQ=
```

Wenn Sie das Resultat nun noch in ein ZIP-Archiv verpacken (beispiel.zip), ist unser erstes Beispiel fertig. So lassen Sie Binary Refinery darauf los:

```
emit beispiel.zip | xtzip | b64 | dump↵
↳ output.txt
```

Wenn alles funktioniert hat, steht in der neu angelegten output.txt der dekodierte String. Ohne Pfadangabe landet diese im selben Verzeichnis wie beispiel.zip.

Mit vereinten Kräften

Zur Erklärung des Beispiels: Binary Refinery arbeitet mit sogenannten Units – Einheiten, die jeweils eine spezifische Aufgabe erledigen. Mit Pipe-Operatoren, die den Rückgabewert einer Unit von links als Eingabewert an die jeweils nächste nach rechts weiterreichen, lassen sich Teilaufgaben verketten:

- `emit` spezifiert in unserem Beispiel die von den übrigen Units weiter zu verarbeitende Datei, kann aber auch einzeln verwendet werden, um einfach nur deren Inhalt auf der Konsole auszugeben. Das funktioniert auch mit binären Daten. Tippt man nur emit ohne weitere Parameter ein, verarbeitet der Befehl den aktuellen Inhalt (z.B. einen kopierten String) aus der Zwischenablage des OS. Auch ein simples `emit Hello World!` oder die Übergabe à la `emit RXJmb2xncmVpY2ggZW5Oc2NobHVlc3NlbHQ= | b64` zum Dekodieren unseres Strings direkt im Terminal sind zulässig.
- `xtzip` extrahiert test.txt zur Weiterverarbeitung aus beispiel.zip. Mit dem Parameter `--pwd (Passwort)` öffnet das dazu auch passwortgeschützte Archive.
- `b64` spürt den Base64-kodierten String auf und dekodiert ihn, ist aber in anderen Zusammenhängen auch für die umgekehrte Operation verwendbar.
- `dump` schreibt das Resultat der vorangegangenen Operationen in output.txt. Lässt man diese Unit weg, landet der dekodierte String stattdessen im Terminal.

Phishing enttarnen

Eine weitere Nutzung von Binary Refinery, die Sie ganz ohne Schadcode selbst ausprobieren können, ist die Analyse verdächtiger Dokumente. Legen Sie dazu eine test.txt-Datei an und spicken Sie sie mit URLs, Domains und E-Mail-Adressen. Die Unit xtp

```
raw/Root/Pages/Kids/0/Resources/Properties/R17
raw/Root/Pages/Kids/0/Resources/Properties/R5
raw/Root/Pages/Kids/0/Resources/Properties
raw/Root/Pages/Kids/0/Resources/XObject/R18
raw/Root/Pages/Kids/0/Resources/XObject
raw/Root/Pages/Kids/0/Resources
raw/Root/Pages/Kids/0
raw/Root/Pages
raw/Root
raw
parsed/meta.json
parsed/page0.html
parsed/page0.json
parsed/page0.txt
parsed/page0/img1.jpg

┌──(binref)─(kali㉿kali)-[~]
└─$ emit test.pdf | xtpdf page0.txt | xtp | defang
http[:]//www.test123[.]com
//www[.]google[.]com
```

Nach dem Parsen der PDF-Dateistruktur durch xtpdf kann man sich die gewünschten Elemente extrahieren lassen – und sie, wenn man will, auch gleich weiter sezieren.

findet diese anhand ihrer Struktur, und die Unit defang entschärft die Treffer, indem sie eckige Klammern nach dem Schema `www[.]test[.]de` einbaut.

```
emit test.txt | xtp | defang
```

Das Resultat schreibt Binary Refinery in die Konsole.

Wie bereits erwähnt, lassen sich mit xtp neben Schadcodebestandteilen auch Logdateien im PCAP- oder in anderen Formaten schnell und einfach nach verdächtigem Traffic durchkämmen. Übrigens: Mit zusätzlichen Parametern kann xtp außer nach den genannten Default Patterns auch nach anderen typischen Mustern wie zum Beispiel IPv4/v6-Adressen, Hashes oder Pfaden suchen. Zudem versteht die Unit reguläre Ausdrücke. Um sie etwa gezielt für die Jagd nach Indicators of Compromise (IoCs) zu nutzen, lohnt es, sich die verfügbaren Optionen in der Doku anzuschauen. Wie und wo Sie die Recherche am besten angehen, verraten wir später.

Zurück zu den Beispielen: Besonders häufig lauern gefährliche Phishing- oder Download-Links in E-Mails, PDFs oder Office-Dokumenten. Um deren spezifische Struktur zu parsen und enthaltene Elemente zu extrahieren, bevor man sie etwa mit xtp weiter untersuchen kann, stellt Binary Refinery ebenfalls spezielle Units bereit. Dazu gehören xtmail, xtpdf, xtdoc und xtvba (Letztere zum Extrahieren von Makrocode).

Wenn Sie auch das ausprobieren möchten, erstellen Sie einfach eine PDF-Datei mit einem beliebigen Bild, etwas Text und einer URL. Speichern Sie diese und lassen Sie sich dann von Binary Refinery die darin enthaltenen Elemente nebst Pfaden ausgeben:

```
emit test.pdf | xtpdf -list
```

In der zurückgegebenen Elementauflistung enthaltene Bilder können Sie anhand ihrer Dateiendungen identifizieren. Ebenso taucht der eingebaute Text als Datei mit .txt-Endung (in unserem Testdurchlauf konkret: page0.txt) auf. Mit `emit test.pdf | xtpdf (Dateiname.Endung) | dump (Zieldatei)` extrahieren Sie die gewünschten Elemente nacheinander zur weiteren Analyse. Oder aber Sie nutzen das Kombinationspotenzial von Binary Refinery, um den extrahierten Text direkt mit xtp und defang weiterzuverarbeiten:

```
emit test.pdf | xtpdf (Textdatei)↵
↳ | xtp | defang
```

Recherchehelfer

Von Units wie blowfish, aes oder camellia für die Datenver- und Entschlüsselung über asm zum Disassemblieren von Code bis zu kramer oder xlmdeobf



Versand materieller Einzelprodukte nur nach Deutschland und Österreich. Portofreie Lieferung ab einem Einkaufswert von 40 €. Nur solange der Vorrat reicht. Preisänderungen vorbehalten.

heise shop

zum Lüften von Malwareverschleierungen: Sämtliche Möglichkeiten von Binary Refinery aufzuzählen, ist angesichts der Menge verfügbarer Units nebst Kombinationspotenzial weder machbar noch zielführend.

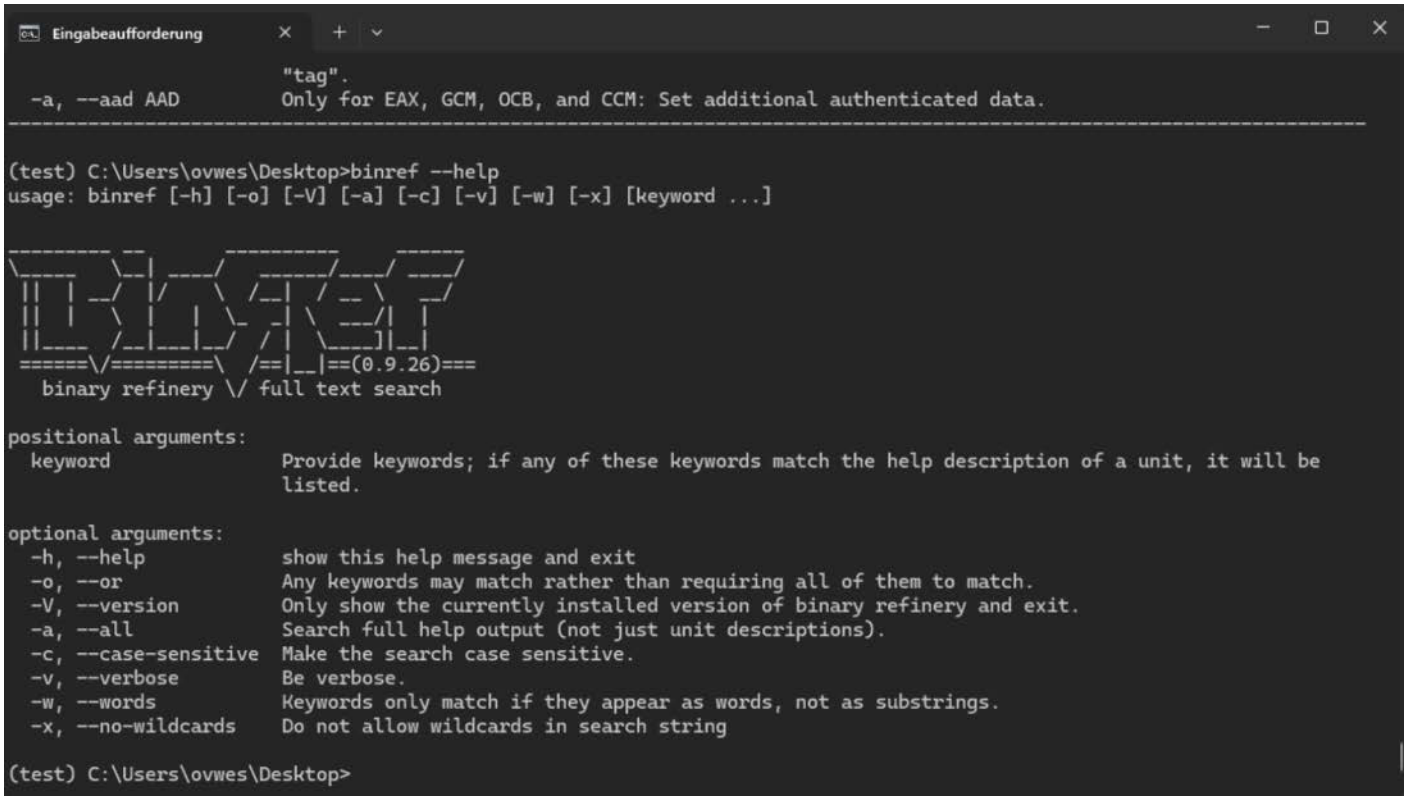
Nach dem Vorgeschmack dieses Artikels ist es deshalb an Ihnen, selbst mit dem Toolkit zu experimentieren und aus der Onlinedokumentation jeweils die Units nebst verfügbaren Parametern herauszusuchen, die Ihnen gerade nützlich sind. Sehr hilfreich zum Durchforsten der Doku ist die in Binary Refinery integrierte Suchfunktion, aufrufbar mit `binref --help`.

`binref (Keyword)` sucht nach einem oder auch mehreren Schlüsselwörtern und gibt anschließend die Kurzbeschreibungen aller Units aus, in deren Doku-Text der Begriff auftaucht. Der Parameter --all erweitert die Ausgabe der Units um deren vollständige Erläuterungen aus der Dokumentation. Ebenfalls sehr nützlich: `--words` verlangt, dass das Schlüsselwort für sich allein statt nur als Substring im durchsuchten Text auftaucht.

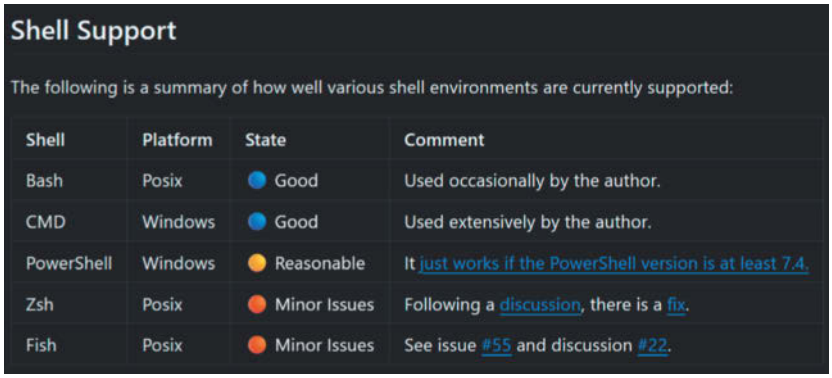
Tutorials und Howtos

Wenn Sie sich näher mit Binary Refinery vertraut machen, werden Ihnen bereits in der Readme.MD Anwendungsbeispiele begegnen, die deutlich komplexer sind als unsere Beispiele in diesem Artikel. Deren Funktionsweise erschließt sich selbst dann nicht unmittelbar, wenn man mal eben kurz in die Doku schaut. So soll etwa folgender Aufruf dazu dienen, eine Config-Datei aus einem Sample des HawkEye-Keyloggers zu extrahieren:

```
emit (Sample) | put cfg perc[RCDATA]↵
↳:c:: [| xtp guid | pbkdf2 48 rep[8]:h:↵
```



Die integrierte Volltextsuche ist unter anderem fürs Durchforsten der Doku praktisch.



Shell Support

The following is a summary of how well various shell environments are currently supported:

Shell	Platform	State	Comment
Bash	Posix	Good	Used occasionally by the author.
CMD	Windows	Good	Used extensively by the author.
PowerShell	Windows	Reasonable	It just works if the PowerShell version is at least 7.4.
Zsh	Posix	Minor Issues	Following a discussion, there is a fix.
Fish	Posix	Minor Issues	See issue #55 and discussion #22.

Gut zu wissen: In der Readme.MD gibt der Entwickler einen Überblick über den aktuellen Stand des Shell-Supports von Binary Refinery.

```
↳00 | cca eat:cfg | aes -Q x::32 -iv↲
↳ x::16 ] | dnd
```

Noch Fragen? – Vermutlich jede Menge.

Tutorials auf Basis praktischer Beispiele können dabei helfen, sich an derlei komplizierte Anwendungsfälle heranzutasten. Im GitHub-Repository von Binary Refinery stehen zahlreiche Tutorials zu verschiedenen Malwaretypen bereit – etwa zum NetWalker Dropper, Amadey Loader oder QakBot Config Decoder und ebenso die Malware-Samples, auf die sie sich beziehen.

Hilfreich kann es auch sein, Experten bei der Verwendung von Binary Refinery zuzuschauen: Bei YouTube gibt es eine nützliche Playlist zum Toolkit, inklusive eines aufgezeichneten Livestreams, in dem der Toolkit-Entwickler Jesko Hüttenhain einen Multi-Stage-Downloader auseinandernimmt.

Der Aufwand solchen Einarbeitens lohnt sich durchaus: Je tiefer Sie einsteigen, desto mehr Flexibilität und Möglichkeiten bietet Ihnen Binary Refinery bei der Analyse von Schadcode.

Aber auch ohne solch einen Deep Dive kann Ihnen das Toolkit einiges an Arbeit abnehmen, indem Sie es mit Teilaufgaben betrauen und mit weiteren Werkzeugen kombinieren. So könnten Sie zum Beispiel mit xtp und ähnlichen Units extrahierte IP-Adressen, E-Mail-Anhänge oder Schadcode im zweiten Schritt an weitere Tools wie Capa oder vt-cli weitergeben. Capa ermittelt spezifische Malwarefähigkeiten auf Basis der Wissensdatenbank von Angriffsmustern MITRE-ATT&CK-Frameworks. Das Tool vt-cli macht die Scan- und Recherchefunktionen der VirusTotal-Plattform von Google über die Kommandozeile verfügbar.

Dokumentation:
ct.de/wb4u

Tipps zur Installation

Wenn Sie nun Lust bekommen haben, Binary Refinery selbst auszuprobieren, folgen Sie einfach den Installationshinweisen aus der Readme.MD des GitHub-Repositories (siehe ct.de/yj1a). In Desinfec't ist die Toolsammlung direkt in AVCompanion integriert. In unserem Testdurchlauf gelang der Vorgang sowohl unter Windows als auch unter Linux schnell und problemlos. Doch eine Warnung: Wenn Sie das Toolkit auf echte Malware ansetzen wollen, sollten Sie es unbedingt in einer isolierten Umgebung wie einer Sandbox oder VM platzieren. Dafür eignet sich Desinfec't 2026/27 hervorragend.

Ebenfalls dringend zu beherzigen ist die Empfehlung des Entwicklers, Binary Refinery unter Verwendung des mitgelieferten Python-Moduls venv in einem isolierten Ordner („virtuelle Umgebung“) mit eigener Python-Installation einzurichten. Das soll unter anderem Versionskonflikten von Python-Bibliotheken vorbeugen und dafür sorgen, dass Toolkit-eigene Befehle nicht mit jenen anderer Programme auf dem System kollidieren.

Die Kommandozeilenbefehle zum Erzeugen und anschließenden Aktivieren der venv- Umgebung variieren je nach Betriebssystem und verwendeter Shell. Da die Readme.MD diese unterschiedlichen Fälle nicht aufschlüsselt, empfehlen wir, bei Bedarf einen zusätzlichen Blick in den venv-Abschnitt der Python-Dokumentation zu werfen. Abschließend noch ein Tipp für Nutzer der REMnux: Der sofort einsatzbereite Docker-Container spart die Installationsarbeit.

Aufwand, der sich lohnt

Binary Refinery verkörpert nahezu in Reinform die traditionelle Unix-Philosophie hochspezialisierter, aber mächtiger Tools, die man flexibel kombinieren kann, um komplexe Aufgaben zu meistern. Dementsprechend kann es einige Zeit erfordern, sich einzuarbeiten.

Doch wer regelmäßig Daten aus Dateien extrahieren muss, wird die investierte Zeit schnell wieder reinholen und auf Binary Refinery nicht mehr verzichten wollen. Nicht umsonst hat sich das Toolkit als feste Größe im Werkzeugkasten erfahrener Malwareanalysten etabliert. (des) c't

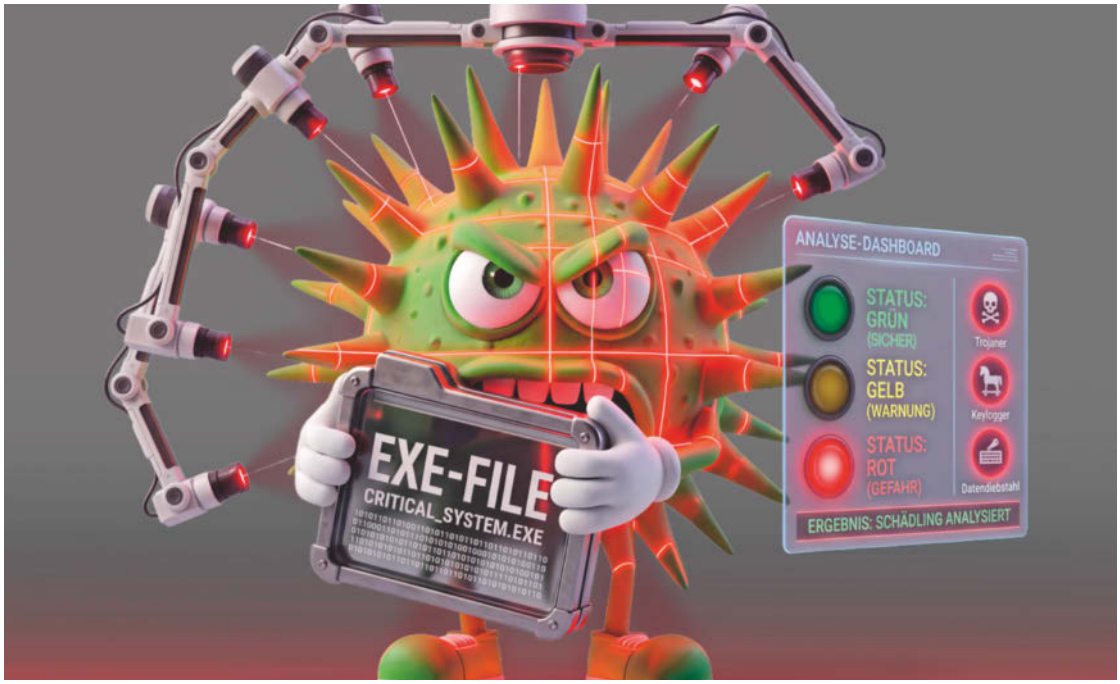


Bild: Martina Bruns / KI / heise medien

Exe-Dateien mit Desinfec’t analysieren

Sie möchten mit Desinfec’t 2026/27 Windows-Schadcode analysieren, um dessen Funktionsweise zu verstehen und angemessen auf einen potenziellen Virenfund zu reagieren? Kein Problem, genau dafür hält der Profi-Werkzeugkasten eine vielfältige Sammlung leistungsstarker Tools bereit. Anhand des Erpressungstrojaners WannaCry zeigen wir, wie es geht.

Von **Olivia von Westernhagen**

Ein unüberlegter Doppelklick auf eine via E-Mail zugeschickte Datei genügt, um PCs mit Schadcode zu verseuchen. Doch es gibt Wege, verdächtige Dateien zu untersuchen, ohne sie zu öffnen. Dieser Artikel erklärt, welche Werkzeuge sich speziell für die Analyse ausführbarer Dateien, aber auch für Schadcode-Komponenten etwa im Textformat eignen und wo Sie diese in Desinfec’t 2026/27 finden. Zum Ausprobieren dient ein konkretes Anwendungsbeispiel, das Sie herunterladen können (siehe ct.de/w1sz).

Bei unserer Beispiel-Malware handelt es sich um echten Windows-Schadcode, konkret: um die berühmt-berüchtigte WannaCry-Ransomware. Entpa-

cken Sie das mit dem Passwort `infected` gesicherte Archiv also keinesfalls in Ihrem Windows-System! Laden Sie es aus Sicherheitsgründen direkt in Desinfec't herunter. Im Linux-System kann der auf Windows zugeschnittene Schadcode kein Unheil anrichten.

Mit den nachfolgend vorgestellten Profi-Tools können Sie Ihr System in der Regel nicht beschädigen. Somit spricht grundsätzlich nichts dagegen, auch als Laie damit zu experimentieren und erste Erfahrungen in der Malware-Analyse zu sammeln.

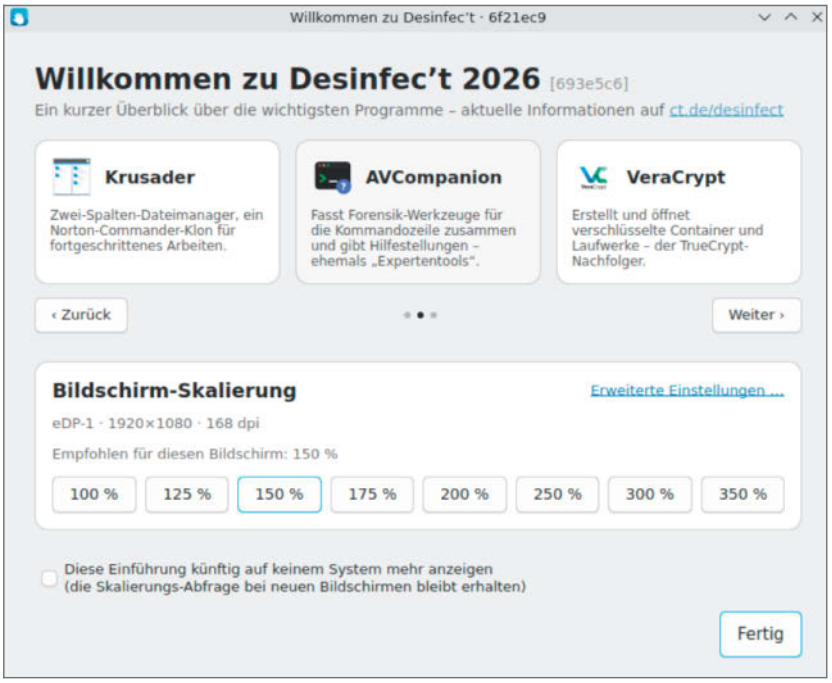
Falls Sie Desinfec't schon länger nutzen, ist Ihnen vermutlich bereits aufgefallen, dass die Expertentools umgezogen sind. Alle, die über die Kommandozeile bedienbar sind, stecken nun im neuen AVCompanion, übersichtlich nach Kategorien sortiert und mit kurzen Beschreibungen versehen. Dabei handelt es sich um eine Art erweitertes Terminal, das die enthaltenen Tools direkt aufrufbar macht. Um sich davon selbst ein Bild zu machen, öffnen Sie ein Standard-Terminal im frisch angelegten Malware-Testverzeichnis und starten den AVCompanion mit `avcompanion`.

Es gibt zwei weitere Wege zum Aufrufen des neuen Werkzeugkastens: Zum einen ist er über den Willkommen-Bildschirm auswählbar, zum anderen auch im Kontext eines Virenscans mit dem AVRunner, also der Scan-Komponente von Desinfec't. Im AVRunner rechtsklicken Sie einfach in der Ergebnisliste auf eine als verdächtig oder schädlich eingestufte Datei, um für eine tiefergehende Analyse direkt zum AVCompanion zu wechseln.

Erste Einblicke

Links im neuen Werkzeugkasten finden Sie die nach verschiedenen Kategorien sortierte Tool-Übersicht. Im Zuge unserer Beispiel-Analyse ist es sinnvoll, sich zunächst einen Überblick über die Eigenschaften von beispiel-ransom.exe zu verschaffen. Dafür wählen Sie in der dazu passenden AVCompanion-Kategorie „Erste Bestandsaufnahme“ das Tool Qu1cksc0pe aus (für Anleitungen und weitere Informationen zu den erwähnten Tools siehe ct.de/w1sz).

Wie der sich im Werkzeugkasten öffnende Beschreibungstext verrät, kombiniert Qu1cksc0pe im Zuge eines Dateiscans statische Analyseergebnisse mit Warnhinweisen zu verdächtigen Inhalten und potenziellen Schadfunktionen. Letztere Fähigkeit verdankt das Tool einem integrierten Satz spezieller



Der AVCompanion mit Expertentools zur Malware-Analyse ist in der aktuellen Desinfec't-Version direkt aus dem Willkommen-Bildschirm anwählbar.

Antiviren-Signaturen, den sogenannten YARA-Regeln.

Zum bequemen Bedienen fasst AVCompanion unter „Typischer Einsatz“ für jedes eingebaute Tool gebräuchliche Aufrufbeispiele zusammen, die sich per Mausklick direkt in das integrierte Terminal übertragen lassen. Probieren Sie das am besten einfach mal anhand des zweiten Punkts in der Qu1cksc0pe-Beschreibung aus und ersetzen dabei den Platzhalter durch den Dateinamen unseres Beispiels:

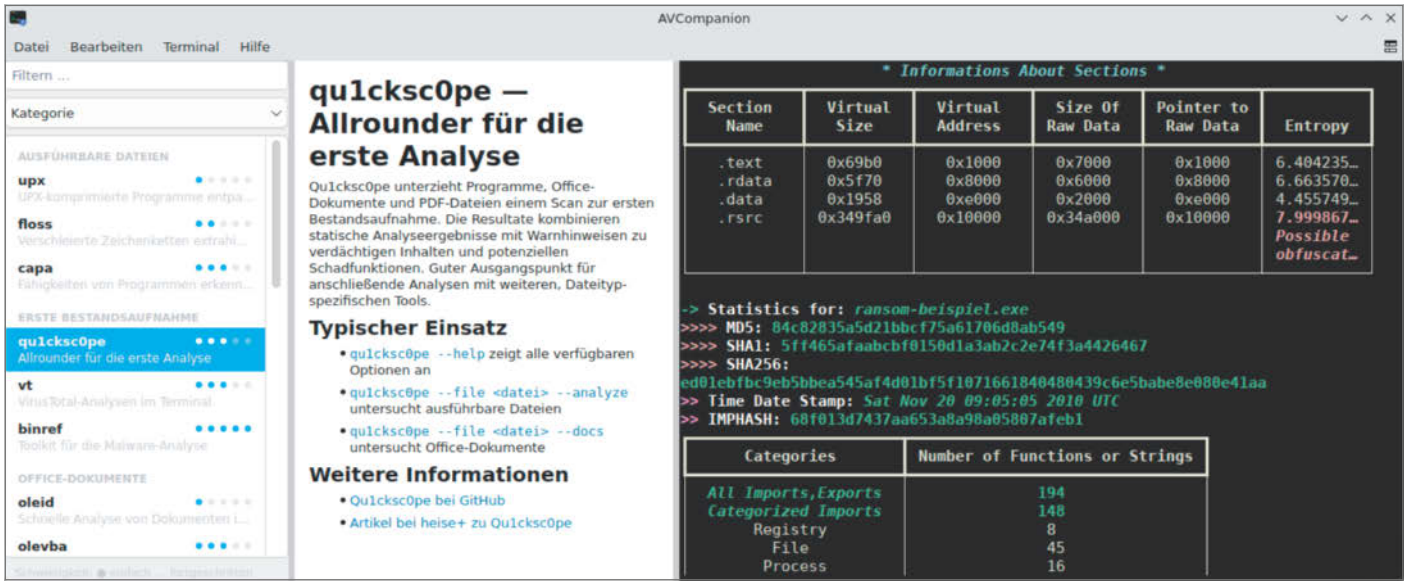
```
qu1cksc0pe --file beispiel-ransom.exe↵
                          ↳ --analyze
```

Interessante Erkenntnisse

Bevor Sie sich in Qu1cksc0pes Scanresultate vertiefen, sollten Sie die Ereignisse rund um WannaCry noch einmal kurz Revue passieren lassen: Im Mai 2017 richtete die verschlüsselnde Ransomware im Zuge eines Cyberangriffs Chaos an (siehe ct.de/w1sz). Der Schädling legte weltweit hunderttausende Windows-Rechner und mit ihnen die IT-Infrastruktur zahlreicher Unternehmen und öffentlicher Einrichtungen lahm, um Lösegeld zu erpressen. Aus heutiger Perspektive eignet sich WannaCry vor allem deshalb als Anschauungsbeispiel, weil die Autoren weitgehend auf eine Verschleierung ihres Codes verzichtet haben, anders als bei moderner Ransomware.

So kann Qu1cksc0pe diesen Schädling ungehindert durchkämmen und liefert Informationen, die vor dem bekannten WannaCry-Hintergrund teils erwartbar, teils aber auch spannend zum Weiterforschen sind. Unter anderem gruppiert das Tool importierte Windows-API-Funktionen im Code nach Kategorien. Es listet reichlich Hinweise auf lesende und schreibende Dateizugriffe in der File-Kategorie sowie unter Cryptography auf genutzte Verschlüsselungsoperationen. API-Funktionen der Kategorien Registry und System/Persistence untermauern die Fähigkeit der Ransomware, sich mittels neu installierter Dienste und dazu passender Autostart-Einträge dauerhaft im System einzunisten.

Ein weiterer Fund von Qu1cksc0pe gibt auf den ersten Blick Rätsel auf: Im Abschnitt „Interesting String Patterns“ listet das Werkzeug drei Dateinamen (tasksche.exe, taskdl.exe, taskse.exe), zu denen sich keine legitimen Windows-Programme zuordnen lassen. Ebenfalls ungewöhnlich ist die Tatsache, dass ein Segment der Datei (.rsrc) laut Qu1cksc0pes Analyse verschlüsselte Daten zu enthalten scheint.



Qu1cksc0pe in Aktion, aufgerufen aus dem AVCompanion. Über einen Rechtsklick passen Sie Farbschemata und Schriftgrößen an.

Tiefer bohren

Ein kleiner Spoiler an dieser Stelle: Beide Informationen – die ungewöhnlichen Dateinamen und das verdächtige Segment – hängen zusammen. In letzterem verbirgt die von uns betrachtete WannaCry-Komponente nämlich ein Zip-Archiv mit weiteren Komponenten, die sie zur Laufzeit extrahiert und unter Verwendung der jeweiligen Namen ausführt beziehungsweise strategisch auf dem System platziert.

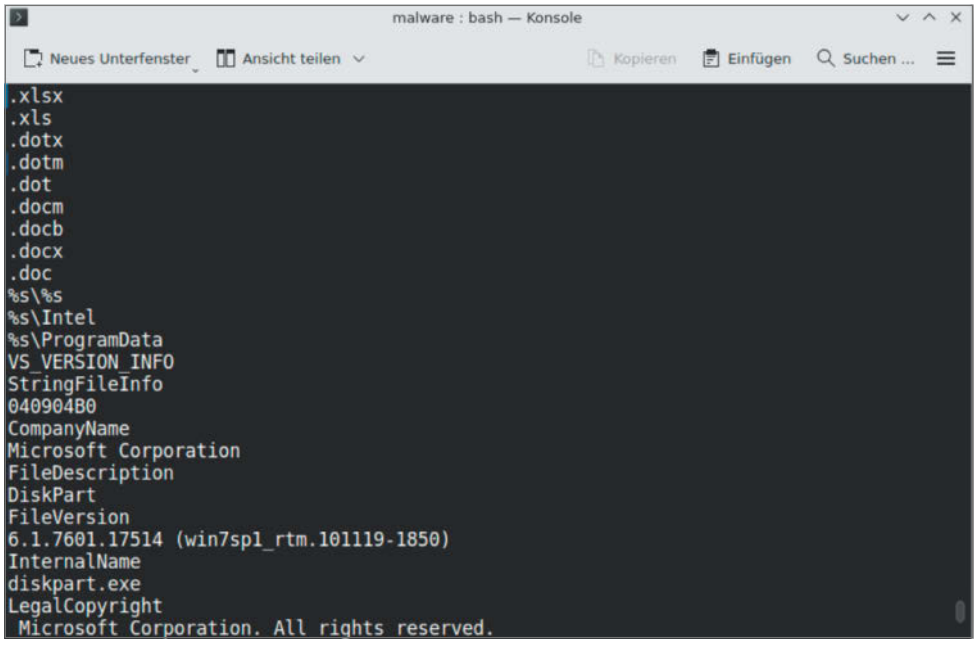
Vor dem Blick in dieses verborgene Archiv bietet es sich noch an, beispiel-ransom.exe mit zwei weiteren Werkzeugen aus dem Desinfec't-Fundus, nämlich Capa und FLOSS zu durchleuchten. Beide finden Sie in der AVCompanion-Kategorie „Ausführbare Dateien". Scans mit Capa dienen der Fähigkeiten-Analyse von Schadcode. Das funktioniert ähnlich wie bei YARA auf Basis von Regeln mit einer speziellen Syntax, die das vorinstallierte Werkzeug mitbringt.

Zur Beschreibung der in einem Sample entdeckten Fähigkeiten orientiert sich Capa am ATT&CK-Framework, einem in Security-Kreisen bewährten Werkzeug zum einheitlichen Klassifizieren von Angriffsstrategien, sowie am MBC (Malware Behavior Catalog). Beide Projekte betreut die Non-Profit-Organisation MITRE und beiden ist gemein, dass sie Angriffstaktiken und -techniken beschreiben und so durchnummerieren, dass die zugehörigen Erläuterungen ohne Verwechslungsgefahr online nachschlagbar sind (siehe ct.de/w1sz).

Fähigkeiten und versteckte Strings

Ein Aufruf von `capa beispiel-ransom.exe` liefert unter anderem Treffer zu den ATT&CK-Techniken „File and Directory Permissions Modification" (T1222), „Obfuscated Files or Information" (T1027) und „Query Registry" (T1012). WannaCrys Verschlüsselungsfähigkeiten bestätigen und konkretisieren etwa die MBC-Einträge „Encrypt Data::AES" (C0027.001) sowie „Generate Pseudo-Random Sequence" (C0021).

An dieser Stelle noch ein Pro-Tipp: Experten, die sich tief in den Programmcode hineinknien und einzelne Speicheradressen inspizieren wollen, ergänzen den Capa-Aufruf um den Schalter `-vv`. Das Tool spuckt dann Kombinationen aus konkreten Schadcodefähigkeiten (etwa „encrypt data using AES") nebst sämtlichen virtuellen Speicheradressen aus, an denen es entsprechende Programmfunktionen entdeckt haben will.



FLOSS findet Dateiendungen, nach denen WannaCry fahndet, und deckt nebenbei auch gleich dessen Tarnung als diskpart.exe auf.

Ein Scan mit FLOSS (FLARE Obfuscated String Solver) via `floss beispiel-ransom.exe` bringt weitere spannende Details ans Licht. FLOSS kann verschlüsselte Strings aus Executables extrahieren, ohne deren Code tatsächlich auszuführen. Dazu emuliert es die Assembler-Befehle potenzieller Entschlüsselungsfunktionen im Schadcode und gibt dem Nutzer dekodierte Zeichenketten zurück. Genauere technische Details zur Funktionsweise erklärt ein Dokument des Entwicklerteams (siehe ct.de/w1sz).

In unserem Beispiel findet FLOSS neben viel Schrott den String „WanaCrypt0r“ gefolgt von einer langen Liste mit Dateiendungen. Vielleicht können Sie es sich schon denken: Es handelt sich dabei um all jene Dateiformate, die WannaCry auf befallenen Systemen systematisch aufspürt und verschlüsselt.

Ebenfalls Teil von FLOSS' Funden: Metadaten aus der VS_VERSION_INFO-Struktur der PE-Datei. Das sind jene Informationen, die man unter Windows per Rechtsklick auf eine ausführbare Datei unter „Eigenschaften“ einsehen kann, darunter der ursprüngliche Dateiname (OriginalFilename), die Dateiversion (FileVersion) sowie der Name des Herausgebers (CompanyName).

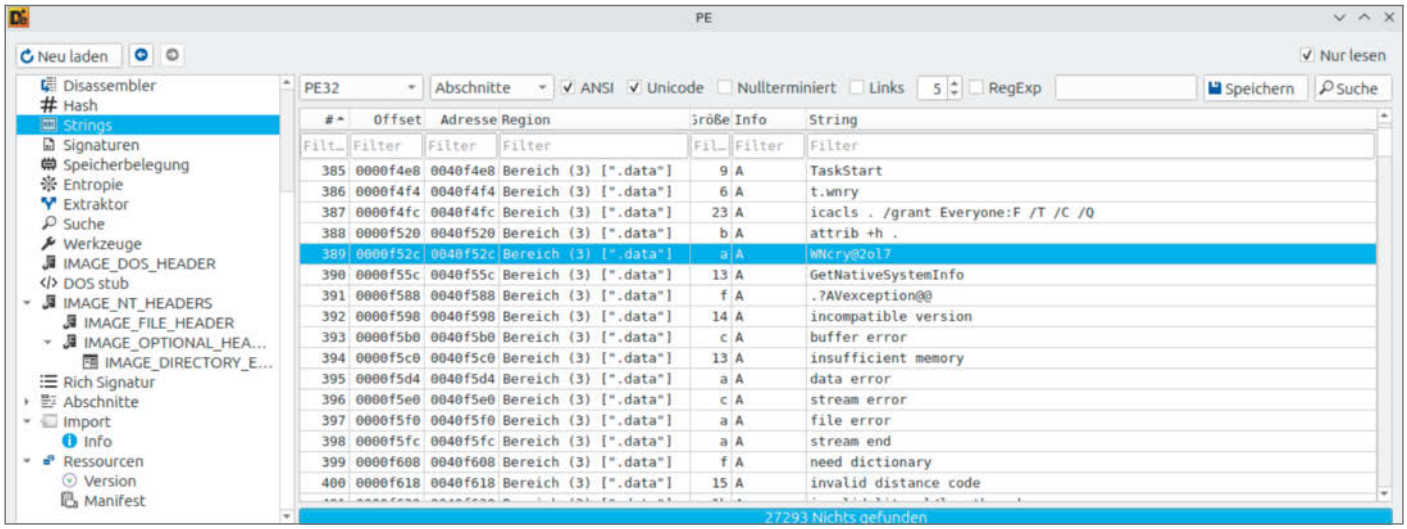
Mit diesen Informationen wird klar, dass sich die von uns umbenannte Datei ransom-beispiel.exe in freier Wildbahn als diskpart.exe von Microsoft tarnte. Als legitime Windows-Komponente dient besagtes Programm zur Festplatten- und Partitionsverwaltung und stellt somit für einen laufenden Ransomware-Prozess gleichen Namens eine naheliegende Tarnung dar.

Komponenten extrahieren

Nun ist es an der Zeit, die Geheimnisse der in unserem Beispiel verborgenen Zusatzkomponenten zu ergründen. Um an sie heranzukommen, nutzen Sie am einfachsten das Multifunktionswerkzeug Detect It Easy, kurz DiE.

Da DiE eine grafische Oberfläche hat, ist es nicht Bestandteil der AVCompanion-Übersicht. Sie können aber per Rechtsklick auf beispiel-ransom.exe im sich öffnenden Kontextmenü über „Mit Detect it Easy öffnen“ darauf zugreifen. Das klappt genauso übrigens auch bei Funden im AVRunner. Eine dritte Variante ist die schlichte Eingabe von `die` ins Terminal. In die sich daraufhin öffnende Oberfläche ziehen Sie verdächtige Dateien per Drag & Drop oder wählen alternativ einen Dateipfad über DiEs Suchleiste aus.

Eine zentrale Funktion von DiE ist, signaturbasiert eine große Zahl verschiedener Dateiformate zu erkennen. Diese und verwandte Informationen gibt das Tool in der unteren Hälfte seines Hauptfensters aus. Unsere beispiel-ransom.exe erkennt DiE als PE-Datei für Windows (Portable Executable); außerdem identifiziert es die Programmiersprache C/C++, kom-



Der Strings-Bereich von Detect It Easy enthüllt unter anderem das Archivpasswort des Schadcodes.

betterCode()

Agentic AI 2027

Die Konferenz zu KI-gestützter Softwareentwicklung

28. Januar 2027 • Online

Mit Agentic AI zum modernen Software-Stack

Die KI-gestützte Softwareentwicklung hat sich rasant entwickelt von Copilot für einfache Routinen zur **kompletten AI Software Factory.**
Für die Konferenz im Januar 2027 stehen zwei Themen im Fokus:

- **Context Engineering** für effiziente agentische Systeme
- **Verifikation und Testing** für stabilen und sicheren Code

Jetzt **Frühbucher-tickets** sichern!

agenticai.bettercode.eu

Veranstalter

iX MAGAZIN FÜR PROFESSIONELLE IT

piliert mit Microsoft Visual Studio. Wie zuvor Qu1cksc0pe bemerkt auch DiE im Zuge seiner Analysen die ungewöhnliche Struktur der .rsrc-Sektion und liefert dazu folgenden Output:

```
Archive: Zip (2.0) ↵
        ↳[encrypted, 55.8 %, 36 files]
```

Des Rätsels Lösung: Die .rsrc-Sektion beherbergt ein mit einem Passwort verschlüsseltes Zip-Archiv. Das wiederum enthält 36 Dateien, die auf 55,8 Prozent ihrer Ursprungsgröße zusammengestaucht wurden.

Wenn Sie den Fortgeschritten-Haken in der rechten Fensterhälfte setzen, erscheinen auf der Tool-Oberfläche zahlreiche zusätzliche Funktionen. Klicken Sie auf den Extraktor-Button und wählen Sie im sich öffnenden Fenster die Zip-Datei aus. Nach der Wahl eines Speicherorts – vorzugsweise des Testordners – genügt ein Klick auf „Alles ausgeben“.

Bevor es nun an die enthaltenen Dateien geht, können Sie noch einige DiE-Funktionen erkunden und sich mit der Oberfläche vertraut machen. Hierzu ein paar Tipps:

DiE stellt sowohl eine Hex- als auch eine Disassembler-Ansicht analysierter Executables bereit. Letztere können Sie etwa nutzen, um die zuvor von Capa als verdächtig markierten Speicheradressen zu inspizieren.

Unter „Strings“ fasst das Werkzeug sämtliche statischen String-Funde zusammen und verrät auch gleich, in welchem Dateisegment diese jeweils stecken.

Wer sich für Feinheiten der Dateistruktur interessiert, wirft einen Blick auf die aufgeschlüsselten Header-Daten, studiert die Speicherbelegung und schaut sich unter „Abschnitte“ alle Segmente im Detail an.

Dateiformate im Griff

Nun aber zurück zur Zip-Datei: Aus der DiE-Analyse wissen Sie bereits, dass diese passwortgeschützt ist – eine Anti-Analyse-Maßnahme der WannaCry-Entwickler. Das benötigte Passwort befindet sich als String in der untersuchten Programmdatei, die es zur Laufzeit zum Extrahieren der Dateien verwendet. Es lautet WNcry@2ol7 und steht, falls Sie selbst mit DiE nachforschen möchten, am Offset 0xf52c im .data-Segment.

Im Archiv stecken, wie von DiE bereits korrekt ausgewertet, insgesamt 36 Dateien. Als wäre die schiere Menge insbesondere für Analyse-Newbies nicht schon einschüchternd genug, kommt noch erschwerend hinzu, dass viele von ihnen die von den WannaCry-Entwicklern erdachte Fantasie-Endung „.wnry“ tragen. Mit dem Desinfec’t-Werkzeugkasten sind Sie für solche Fälle gut gerüstet. Beim Identifizieren von Dateiformaten hilft DiE, in dessen integrierter Hexadezimal-Ansicht Sie den Inhalt untersuchen können.

Noch komfortabler ist die Analyse mit dem Hex-Editor Okteta, den Sie unter anderem mit `okteta dateiname` über das Terminal starten können. Für das Inspizieren von Textdateien steht der KDE-Standard-Editor Kate zur Verfügung, via `kate dateiname` auf der Kommandozeile oder je nach Dateiendung (z. B. .txt) auch unmittelbar per Rechtsklick auf die Datei.

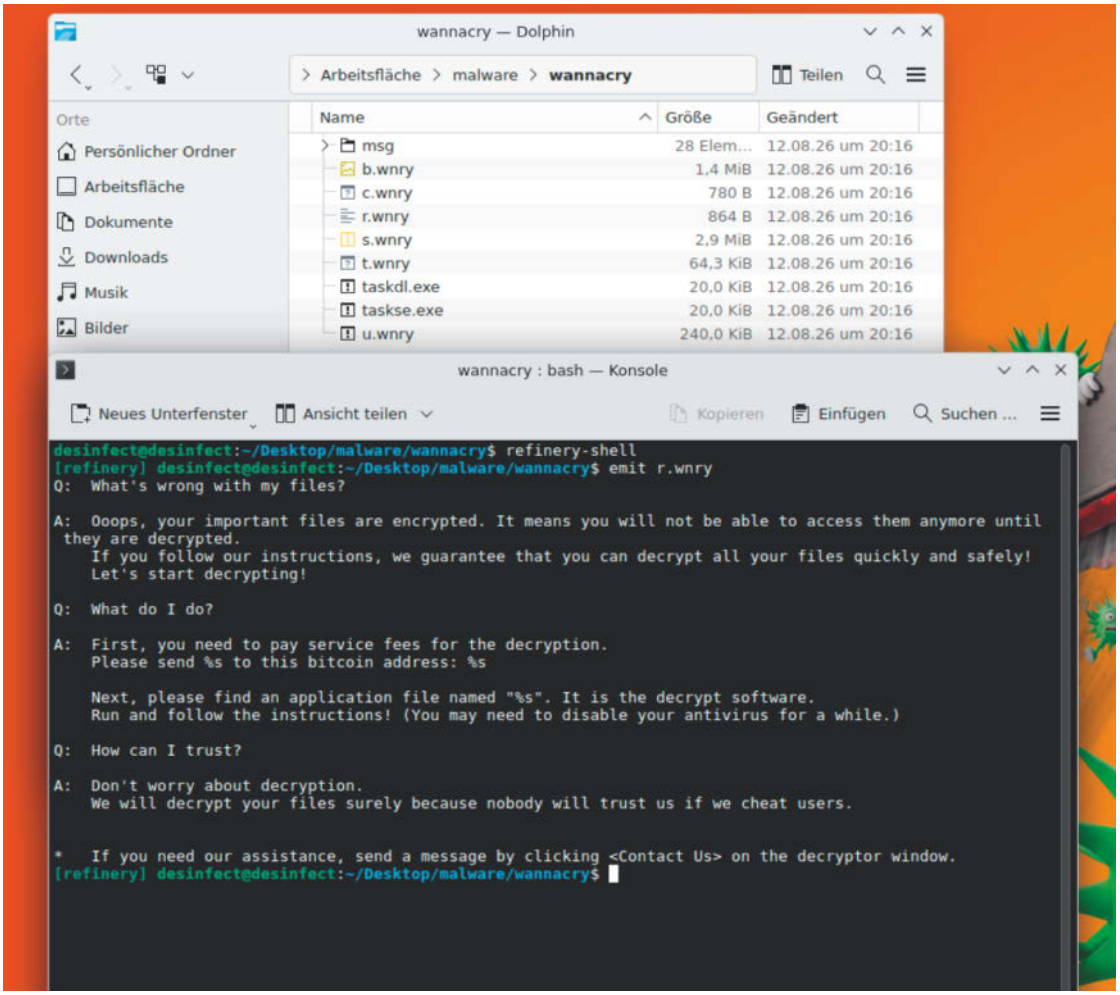
Geeignete Werkzeuge für die Binary-Analyse haben Sie in diesem Artikel bereits kennengelernt. Gut zu wissen ist, dass diese neben Windows-Executables noch weitere Formate analysieren können. So bringt Qu1cksc0pe einen `--docs`-Switch für Office- und PDF-Dokumente mit, auf den ein Artikel zur Dokumentenanalyse näher eingeht (siehe S. 52). Außerdem kann das Tool mit diversen Skriptsprachen, HTML- und EML-Dateien sowie ausführbaren Linux-Dateien umgehen. Eine vollständige Liste kompatibler Dateiformate finden Sie in der Qu1cksc0pe-Beschreibung bei GitHub.

FLOSS kann neben PE-Dateien auch Shellcode analysieren. Gleiches gilt für Capa, das zusätzlich das ELF-Format, .NET-Module sowie Reports verschiedener Sandbox-Projekte durchleuchtet. Achtung: Das dynamische Ausführen schädlicher Linux-Executables könnte Desinfec’t infizieren, weshalb Sie besser darauf verzichten sollten, im Live-System mit derlei Dateien zu hantieren.

Für das bis hierhin unerwähnte Allround-Tool für die Malware-Analyse Binary Refinery gibt es ebenfalls einen Praxisartikel (siehe S. 60). Darin erfahren Sie unter anderem, wie Sie das Werkzeug über den AVCompanion aufrufen und den Befehl `emit` nutzen, um sich den Inhalt beliebiger Dateien direkt im Terminal anzeigen zu lassen. Die Einarbeitung in komplexere Anwendungsszenarien erfordert einige Zeit, lohnt jedoch den Aufwand, wenn man regelmäßig vielschichtigem Schadcode zu Leibe rückt.

Weitere Ansatzpunkte

Eine ausführliche Analyse aller WannaCry-Komponenten würde hier den Rahmen sprengen. Folgende Hinweise sollen Ihnen das Sortieren der Dateien und das Ausprobieren jeweils passender Werkzeuge erleichtern:



Anwendungsbeispiel für Binary Refinery: Der Erpressertext aus r.wnry erscheint direkt im Terminal.

b.wnry: WannaCry-Desktophintergrund im BMP-Format (Windows Bitmap, unter Linux u. a. betrachtbar in Firefox)

c.wnry, r.wnry: Textdateien mit Erpresserbotschaft, Tor-C2-Adressen und anderen Informationen für die Lösegeldzahlung

s.wnry: Ein Zip-Archiv mit der Tor-Software

t.wnry: Verschlüsselte DLL mit Zusatzfunktionen für die Dateiverschlüsselung

u.wnry: Dient der Entschlüsselung (Decryptor)

taskdl.exe, taskse.exe: Hilfsanwendungen für WannaCrys Arbeitsabläufe

msg: Ordner mit Erpresserbotschaften in verschiedenen Sprachen im RTF-Format

Die Analyse der Secureworks Counter Threat Unit sowie eine detaillierte WannaCry-Untersuchung bei Medium helfen zusätzlich dabei, die Malware-Funktion in Gänze zu verstehen (siehe ct.de/w1sz). Für weitere Recherchen eignet sich die von Google betriebene Analyseplattform VirusTotal. Dafür sollten Sie vt-cli ausprobieren: Das im Artikel auf Seite 46 ausführlich beschriebene Werkzeug holt VirusTotal auf die Kommandozeile, einschließlich feingranularer Filterfunktionen für passgenaue Scans und Rechercheergebnisse. Im AVCompanion finden Sie vt-cli unter „Erste Bestandsaufnahme“.

Somit eignet sich Desinfec’t gut für die Malware-Analyse. Dank der Beschreibungen und Aufrufbeispiele im AVCompanion können damit auch Neulinge Trojaner inspizieren. (des) c't

Erwähnte Links:

ct.de/w1sz

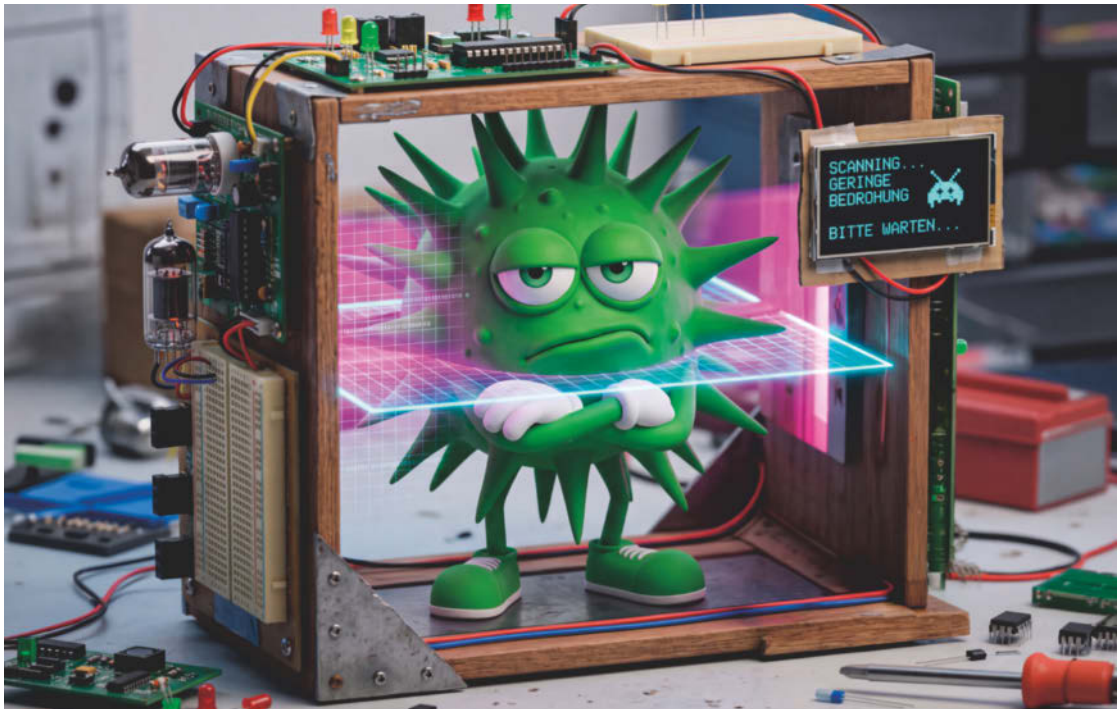


Bild: Martina Bruns / KI / heise medien

Zielgenaue Malware-Fahndung für Profis

Erfahrene Virenjäger verlassen sich nicht nur auf aktuelle Virensignaturen, sondern schreiben eigene Erkennungsregeln. Das klappt mit dieser Anleitung auch unter Desinfec't.

Von **Olivia von Westernhagen**

Desinfec't schafft mit Scannern von ESET, IKARUS & Co. in Kombination mit regelmäßigen Signaturupdates beste Voraussetzungen für eine erfolgreiche Malwaresuche. Und doch gibt es Situationen, in denen es hilfreich ist, ganz flexibel eigene Regeln für die Bedrohungssuche zu erstellen. Etwa dann, wenn ein verdächtiger E-Mail-Anhang oder nicht zuordenbare Dateien auf einem infizierten System auf ein brandneues Angriffsmuster deuten, das die klassischen AV-Scanner bislang nicht auf dem Radar haben.

Der Weg zum eigenen Scanner

Profis setzen zum zügigen Einkreisen solcher Gefahren gern auf YARA-Regeln. Das sind selbst ge-

schriebene, maßgeschneiderte Virensignaturen. Mit passenden Scannern kann man sie auf einzelne Rechner oder ganze Firmennetzwerke loslassen. So lässt sich die neue Bedrohung schnell aufspüren und unschädlich machen. YARA ist ein Open-Souce-Framework, das vom – mittlerweile zu Google gehörigen – VirusTotal-Team stammt.

Desinfec't 2026/27 stellt mit dem klassischen YARA-Tool sowie mit Thor Lite aus dem Hause Nextron Systems gleich zwei YARA-Werkzeuge über die grafische Oberfläche des Scan-Assistenten „AVRunner" bereit. Beide verarbeiten von Sicherheitsforschern handverlesene Signaturen und decken dabei jeweils unterschiedliche Einsatzzwecke ab: Der YARA-Scanner sucht gezielt nach bestimmten Schädlingen. Thor Lite durchsucht eingehängte Partitionen nach Spuren früherer Angriffe (Indicators of Compromise, IoC). So erfahren Sie, was vorgefallen ist, und können gezielt gegensteuern. Im Anschluss an eine kurze YARA-Einführung zeigt dieser Artikel, wie Sie den YARA-Scan und Thor Lite in der Desinfec't-Umgebung nutzen und um eigene Regeln aufrüsten. Ein einfaches Beispiel lädt zum Ausprobieren ein.

Achtung: Beide Tools richten sich an Admins und Malware-Experten, die Fehlalarme durch mitunter eilig gestrickte Regeln als solche interpretieren können. „Normale" Nutzer von Desinfec't, die nur mal schnell ihren Rechner überprüfen wollen, sind mit den Standard-Scannern von ESET, IKARUS und WithSecure besser beraten.

Regelbasierte Suche

YARA-Regeln folgen einer recht simplen, menschenlesbaren Syntax mit verbindlichen Elementen: Sie beginnen stets mit dem Schlüsselwort `rule`, gefolgt vom Namen der Regel sowie deren Inhalt in geschweiften Klammern. Zwischen den Klammern stehen meist Strings, nach denen YARA in den Zieldateien fahnden soll, sowie als verpflichtendes Element eine Bedingung, unter der die jeweilige Regel einen Suchtreffer ausgibt. Das Ganze sieht dann etwa wie folgt aus:

```
rule beispiel {
  strings:
    $a = "Diese Testregel" nocase
    $b = "ist" nocase
    $c = "ein einfaches Beispiel" ↴
                                ↳nocase
    $d = "nur" nocase
  condition:
    all of them
}
```

Diese sehr einfache Beispielregel greift, wenn in einer gescannten Datei jeder vordefinierte Suchstring mindestens einmal auftaucht. In welcher Reihenfolge das passiert, ist dabei egal. Auch das Vorkommen als Teilstrings in Kombination mit weiteren Buchstaben ist zulässig. Der Zusatz `nocase` weist YARA außerdem an, die standardmäßig aktive Unterscheidung von Groß- und Kleinschreibung zu ignorieren. „Diese Testregel ist nur ein einfaches Beispiel" triggert die Regel also ebenso wie „Ist diese testREgeL nur ein Einfaches beiSpiel, oder WAS?!".

Bei der Malware-Jagd bedeutet das: Kennt man einige markante Strings aus dem gesuchten Schadcode, kann man aus diesen eine eigene Regel für die zielgenaue Fahndung stricken. Dabei muss es sich nicht um lesbaren Text handeln: Mit Hexadezimal-Strings lassen sich etwa Bytesequenzen abbilden. Es sind, wie an folgendem Beispiel deutlich wird, auch Platzhalter zulässig:

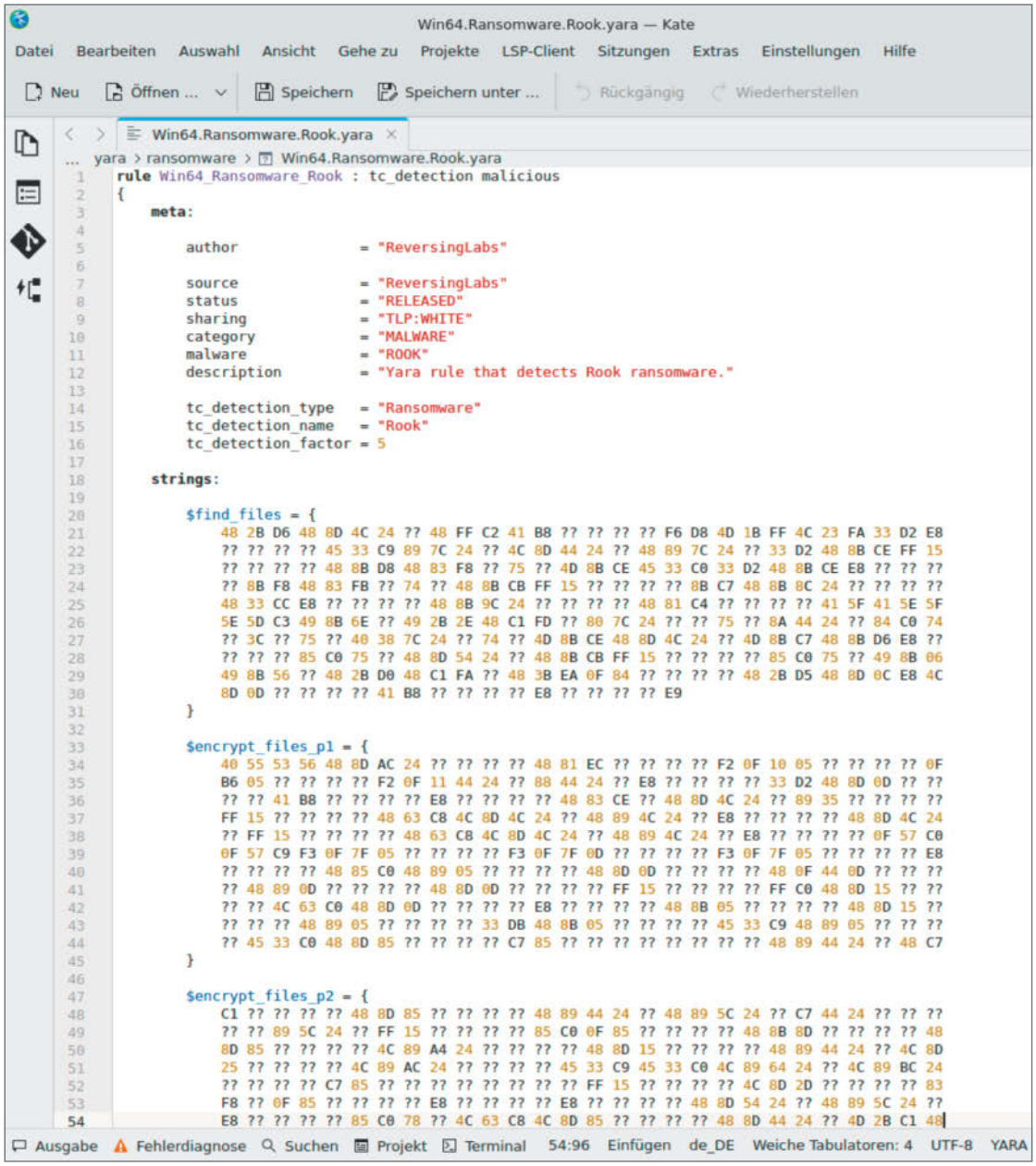
```
$hex_beispiel = { E2 34 ?? C8 A? FB }
```

Des Weiteren versteht YARA komplexe reguläre Ausdrücke und stellt neben `nocase` noch diverse andere Schlüsselwörter wie etwa `fullword`, `ascii` oder `wide` bereit, um String-Eigenschaften näher zu spezifizieren. Zum Weiterlesen haben wir Ihnen unter ct.de/wrux das online verfügbare YARA-Manual verlinkt.

Erster Testaufruf

Bevor es um den YARA-Einsatz im AVRunner geht, können Sie die Beispielregel zunächst selbst ausprobieren. Dabei erfahren Sie auch gleich, wie Sie eigene Signaturen in Desinfec't schreiben und lokal testen. Starten Sie Desinfec't und legen Sie als Testumgebung einen Ordner auf dem Desktop an. Erzeugen Sie darin per Rechtsklick eine leere Datei namens beispiel.yar. An der Endung .yar erkennen Programme, dass die Datei YARA-Regeln enthält.

Beim allerersten Öffnen und Bearbeiten der angelegten Datei kann es sein, dass Sie den Texteditor Kate manuell auswählen müssen (Rechtsklick, dann „Öffnen mit" wählen und „Kate" in das sich öffnende Suchfenster schreiben). Sobald Sie Text hinzugefügt haben, erkennt Kate die YARA-Regel als solche, nimmt sich ihrer als Standardprogramm an und verwendet zur besseren Lesbarkeit automatisch die passende Syntaxhervorhebung. Tippen Sie die wei-



Blick in eine komplexe YARA-Regel von ReversingLabs: Der Texteditor Kate sorgt in Desinfec't für eine gute Lesbarkeit.

ter oben genannte Beispielregel ein und speichern Sie die Datei.

Als „Köder" erstellen Sie anschließend eine Textdatei, etwa test.txt, die die Regelbedingungen erfüllt, also etwa den String „Ist diese Testregel nur ein einfaches Beispiel?" enthält.

Um zu testen, ob die ausgelegte Falle zuschnappt, wenden Sie Googles YARA-Tool in einem neuen Terminalfenster folgendermaßen auf die beiden Dateien an:

```
yara beispiel.yar test.txt
```

Wenn alles geklappt hat und der YARA-Scanner fündig wird, gibt er den Namen der Regel, gefolgt vom Namen des „Fundes“ im Terminal zurück: `beispiel test.txt`.

An dieser Stelle soll es bei dem einfachen Beispiel bleiben. Ihrer Experimentierfreude soll das jedoch keine Grenzen setzen. Zum Ausprobieren noch ein paar Anregungen: Entfernen Sie doch einmal das `nocase` aus der Regel, oder experimentieren Sie – natürlich bei angepasstem Köder – mit unterschiedlichen Bedingungen im `condition`-Abschnitt:

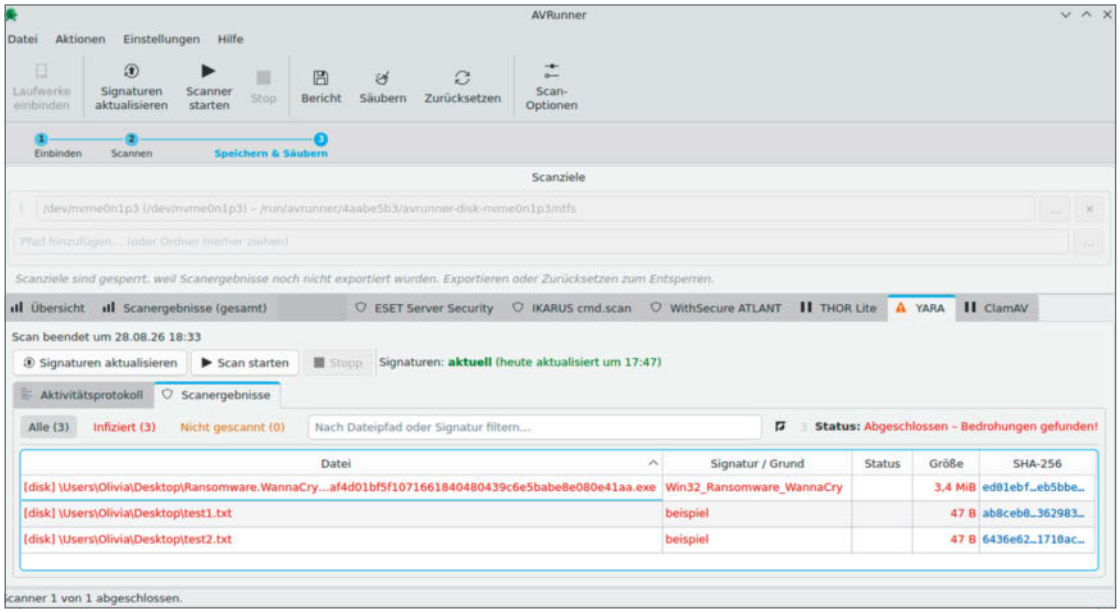
- `$a or $b`: `a` oder `b` müssen im Köder enthalten sein.
- `#a == 2 and #c > 3`: String `a` muss genau zweimal, String `c` mehr als dreimal vorkommen.
- `any of ($c, $d)`: Mindestens einer der beiden Strings muss vorkommen.
- `filesize <= 8KB`: Die Datei darf höchstens 8 KByte groß sein.

YARA-Scan im AVRunner

Wie eingangs erwähnt, ist Googles YARA-Scanner fester Bestandteil des Scan-Assistenten im neuen Desinfec’t. Er bringt einen Profi-Regelsatz mit, der regelmäßig aktualisiert wird. Anders als auf der Kommandozeile kann das Tool dort eingehängte Windows-Laufwerke „in einem Rutsch“ komplett scannen.

Den AVRunner starten Sie wahlweise über den „Willkommen“-Bildschirm oder über das grüne Virensymbol auf dem Desktop beziehungsweise in der Taskleiste. Sowohl der YARA-Scanner als auch Thor Lite sind auf der grafischen Oberfläche über eigene Tabs auswählbar. Anders als die integrierten Standard-Scanner von ESET, IKARUS und WithSecure sind beide nicht als Bestandteil von „Scanner starten“ vorkonfiguriert, weil es sich um Profi-Tools handelt, die nur Fachleute mit entsprechender Expertise ein-





Beim YARA-Scan eines Windows-Testsystems findet AVRunner die Ransomware WannaCry – und zwei „Köder", auf die die Beispielregel aus diesem Artikel anspringt.

setzen sollten. Nach dem Einbinden des zu untersuchenden Laufwerks (siehe S. 6) müssen Sie die Signaturupdates deshalb direkt über die entsprechenden Tabs anwerfen.

Im Folgenden geht es um einen klassischen YARA-Scan. Thor Lite ist später an der Reihe. Nach einem Klick auf „Signaturen aktualisieren" holt sich das Programm die aktuellen Regeln aus einem öffentlichen GitHub-Repository des Cybersecurity-Unternehmens ReversingLabs (siehe ct.de/wrux). Der Fokus der Signaturen liegt auf einer hohen Treffsicherheit bei zugleich möglichst geringer Fehlalarmquote. Im Fenster „Aktivitätsprotokoll" sowie unter „Signaturen" meldet Ihnen AVRunner zurück, ob die Aktualisierung erfolgreich war.

Im Anschluss klicken Sie einfach auf „Scan starten". Ausprobieren können Sie das entweder an einem potenziell infizierten Laufwerk, das Sie ohnehin überprüfen wollten, oder mittels der zuvor erstellten Beispieldatei nebst Köder.

Für letztere Variante legen Sie am besten gleich einen Ordner an, in dem der YARA-Scanner künftig aktualisierte Signaturen finden soll.

Wechseln Sie dazu in das Verzeichnis /opt/yara-patterns. Dort befindet sich bereits ein Unterordner, in dem die ReversingLabs-Regeln landen. Der Scanner bedient sich jedoch an allen Regeln in /opt/yara-patterns, sodass Sie hier beliebig viele Ergänzungen vornehmen können. Führen Sie also im Terminal `sudo mkdir (NeuerOrdner)` aus und kopieren Sie dann die Beispielregel hinein (`sudo cp`).

Nun müssen Sie noch den Köder im zu scannenden Windows platzieren. Starten Sie dafür Windows und erzeugen Sie auf dem dortigen Desktop die benötigte Testdatei nebst Suchstring. Auch hier können Sie natürlich wie im ersten Beispiel mit mehreren Varianten experimentieren.

Booten Sie jetzt Desinfec't. Nach dem Start eines YARA-Scans in AVRunner sollte der Köder-Fund in den Scanergebnissen auftauchen. Auf der Bedienoberfläche sind dazu jeweils Pfad und Dateiname des Fundes, die Bezeichnung der YARA-Regel (Überschrift: „Signatur"), die Dateigröße sowie der SHA-256-Hash aufgeführt.

Per Rechtsklick auf den Hash können Sie bei Bedarf bei VirusTotal (VT) nachschauen, ob ein Onlinereport zu dem Fund vorhanden ist. Googles Analyseplattform eignet sich an dieser Stelle wunderbar zum Weiterrecherchieren – zum Beispiel mit vt-cli, einem Tool aus dem Desinfec't-Werkzeugkasten, das VT-Funktionen komfortabel und passgenau auf der Kommandozeile verfügbar macht (siehe S. 46).

Einbruchsspuren finden

Thor Lite finden Sie im AVRunner-GUI links neben dem YARA-Scan. Zum Sammeln potenzieller IoCs nutzt die in Desinfec't enthaltene kostenlose Ausgabe des Thor-Scanners Tausende Regeln aus einem öffentlichen GitHub-Repository des Sicherheitsexperten und Nextron-Mitgründers Florian Roth (siehe ct.de/wrux). Solche IoCs können etwa bestimmte Dateinamen, verdächtige Strings oder auch Registry-Einträge sein, die eine bestimmte Malware-Familie nutzt, um sich dauerhaft im System einzunisten. Oder auch Logfile-Einträge, die etwa auf einen deaktivierten Virenschutz hinweisen.

Obacht: Die Funde von Thor Lite sind in der Regel nicht eindeutig, sondern müssen im Kontext der gescannten Umgebung und in Kombination miteinander betrachtet und von einem Profi eingeordnet werden. So erkennt Thor Lite standardmäßig zahlreiche „Hackertools", die einerseits zum Einbruch verwendbar sind, andererseits aber auf dem PC eines IT-Sicherheitsverantwortlichen zur Arbeitsausstattung gehören können.

Beim Einordnen der Verdachtsfälle hilft Thor Lites eingebautes Scoring-System, dessen Punktzahlen sich aus einer Kombination des Schweregrads des Fundes (Severity) und der Vertrauenswürdigkeit des Alarms (Confidence) errechnen. Ab 40 Punkten erzeugt der Scanner einen einfachen Hinweis („Notice") in seinem finalen Report; ab 60 Punkten wird eine Warnung („Warning") generiert. Punktzahlen über 80 bis zu 100 lösen einen „Alert" als höchstmögliche Gefahrenstufe aus. Wenn ein potenzieller IoC von gleich mehreren YARA-Regeln als solcher erkannt wird, erhöht das die Wahrscheinlichkeit eines berechtigten Alarms. Teilpunktzahlen können sich in solchen Fällen zu einem höheren Gesamt-Score nach einer festen Formel aufrechnen.

Die einzelnen Punktzahlen bezieht Thor Lite aus den jeweils getriggerten Regeln. Am besten veranschaulichen lässt sich das durch eine entsprechende Ergänzung unserer Beispielregel. Dazu bauen Sie vor dem `strings`-Abschnitt Folgendes ein:

```
rule beispiel {
  meta:
    author = "IhrName"
    description = "Regel zum ↵
          ↳Ausprobieren in Desinfec't"
    score = 60
  (...)
}
```

Das Schlüsselwort `meta` ist ein optionaler Bestandteil aller YARA-Regeln, der beliebige Zusatzinformationen enthalten kann. Der Bezeichner `score` wird speziell von Thor Lite erkannt und der zugewiesene Wert als Punktzahl interpretiert.

Ausprobieren

Zum Testen der angepassten Regel müssen Sie diese analog zum YARA-Scanner in den richtigen Thor-Lite-Ordner kopieren. Den finden Sie unter /opt/thorlite/custom-signatures/yara.

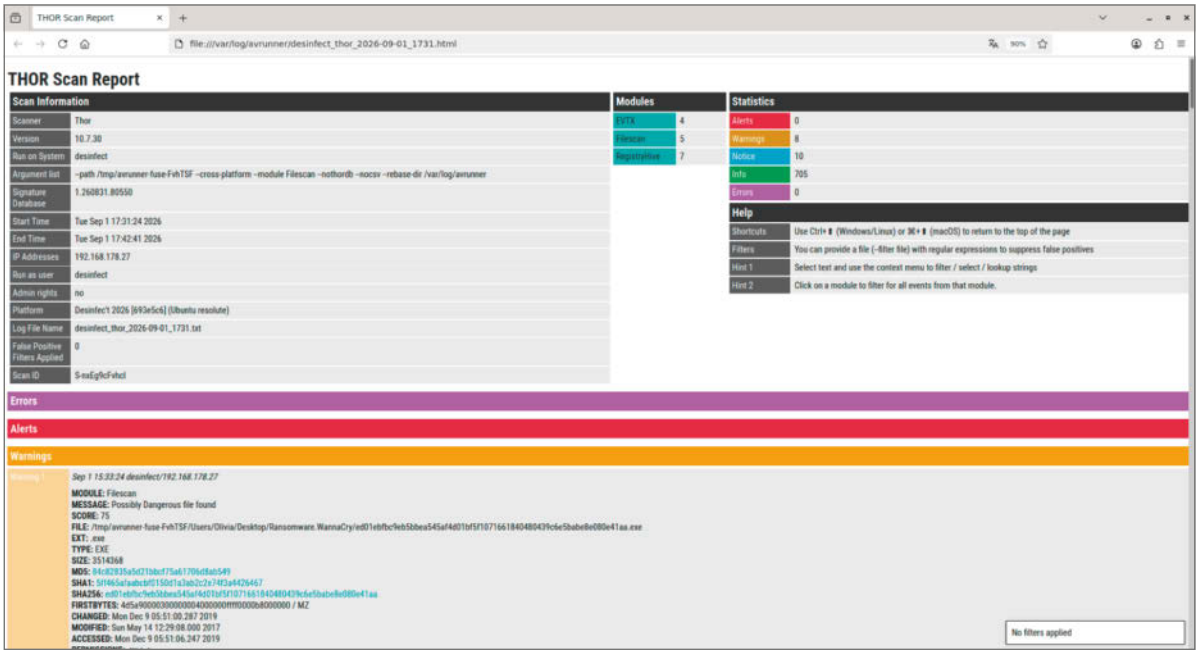
Vor dem Thor-Lite-Scan noch ein wichtiger Hinweis: Das Tool generiert bei jedem Suchdurchlauf einen HTML-Report, der je nach Zielsystem umfangreich ausfallen kann und Speicherplatz auf der Partition DESINFECT_D beansprucht. Zwar wird besagter Report beim nächsten Reboot gelöscht; dennoch empfiehlt es sich, zum Vermeiden von Speicherkrisen auf das Durchforsten riesiger Datenbestände zu verzichten.

Aber zurück zum Beispiel: Nach dem Scan der eingehängten Windows-Partition nebst Köderdatei sollten Sie im Thor-Lite-Tab des AVRunners den „Beispiel-Treffer" sehen. Die dargestellten Informationen entsprechen jenen, die Sie bereits im YARA-Scan-Tab gesehen haben. Ergänzend taucht in einer mit „Status" benannten Spalte zudem das Schlüsselwort „Warning" auf – basierend auf dem Score von 60, den Sie der Beispielregel zugewiesen haben.

Das AVRunner-GUI bietet einen ersten Überblick über potenzielle IoC-Funde, ist allerdings insofern limitiert, als etwa Details wie Teil- und Gesamtpunktzahlen nicht Bestandteil der Scanergebnisse sind. Zwar enthält das „Aktivitätsprotokoll" links neben den Resultaten einige dieser Zusatzinformationen, jedoch in sehr unübersichtlicher Form.

Um das Maximum aus der Spurensuche mit Thor Lite herauszuholen, sollten Sie sich deshalb den bereits erwähnten detaillierten HTML-Report anschauen, der nach jedem Scan in /var/log/avrunner landet. Er sortiert Alerts, Warnings, Notices, aber auch beim Scan aufgetretene allgemeine Informationen und schlüsselt sie jeweils farbig auf. Im Report erscheinen neben den bereits aus AVRunner bekannten Details etwa das Datum des letzten Zugriffs, die Metadaten aus den getriggerten Regeln – in unserem Fall `author` und `description` – sowie Teil- und Gesamtscores.

Wenn Sie den von Thor Lite generierten Report über den Neustart hinaus behalten und auch gleich



Thor Lites HTML-Report schlüsselt möglicheKompromittierungshinweise übersichtlich auf.

aus dem Live-System auf andere Systeme mitnehmen wollen, kopieren Sie ihn auf die Datenpartition DESINFECT_D eines Desinfec't-Sticks.

- Wenn Sie im horizontalen GUI-Menü „Hilfe/Logexport“ auswählen, landet nach dem Scanvorgang eine Zip-Datei mit allen Logdateien aus der aktuellen Sitzung in DESINFECT_D. Die erzeugten Debug-Logs können Sie hierbei explizit aussparen.
- Alternativ nutzen Sie die unter „Aktionen“ auswählbare Funktion „Scanner starten und herunterfahren“, die beim Herunterfahren ebenfalls ein automatisiertes Kopieren des HTML-Reports auslöst. Selektieren Sie gegebenenfalls vorab unter „Einstellungen/Scanner verwalten“ explizit Thor Lite und entfernen Sie die Haken bei den übrigen Scannern.

Lust auf mehr?

Die Grundlagen der YARA-Nutzung in Desinfec't haben Sie jetzt kennengelernt. Das ist jedoch nur der Anfang: Insbesondere das sichere Interpretieren von Thor-Lite-Reports erfordert Einarbeitungszeit und Übung anhand „echter“ Scans infizierter Systeme. Nextron Systems' Online-Handbuch zu Thor bietet wertvolle Hilfestellung, wenn Sie einmal nicht weiterwissen (siehe ct.de/wrux).

Wenn Sie Lust bekommen haben, eigene Regeln zu schreiben, um Schadcode aufzuspüren: Lesen Sie sich auch dafür gründlich ein. Denn unpräzise oder schlicht falsche YARA-Signaturen können Unmengen von Fehlerkennungen auslösen und den Scan-Assistenten zum Absturz bringen.

Testen und optimieren Sie Ihre YARA-Regeln, indem Sie sie etwa mit `yara regel.yar Ordnername` auf eine lokal gespeicherte Windows-Schadcodesammlung loslassen. Studieren Sie vorhandene Profi-Signaturen und lesen Sie im YARA-Handbuch nach, wie Sie ganze Regelsätze zwecks Zeitersparnis mit dem yarac-Tool kompilieren. Letzteres steht Ihnen in Desinfec't auf der Kommandozeile zur Verfügung; `yarac -h` bietet eine Übersicht über alle verfügbaren Parameter.

Tools für die Binary- und Dokumentenanalyse aus dem Desinfec't-Werkzeugkasten (siehe S. 60 und 52) helfen Ihnen bei Bedarf, verdächtigen Dateien passende YARA-Strings für die Erkennung zu entlocken.

(des) c't

Regelsammlungen und Dokumentationen:

ct.de/wrux

heise academy

Wissen, das weiterbringt

Entdecke praxisnahe Weiterbildungen zu Künstlicher Intelligenz, IT-Sicherheit und Regulatorik, die dich und dein Team auch in 2027 voranbringen. Mit erfahrenen Expertinnen und Experten und direkt anwendbarem Know-how seid ihr für die Herausforderungen von morgen gerüstet.



Unser Programm 2027: heise-academy.de/downloads

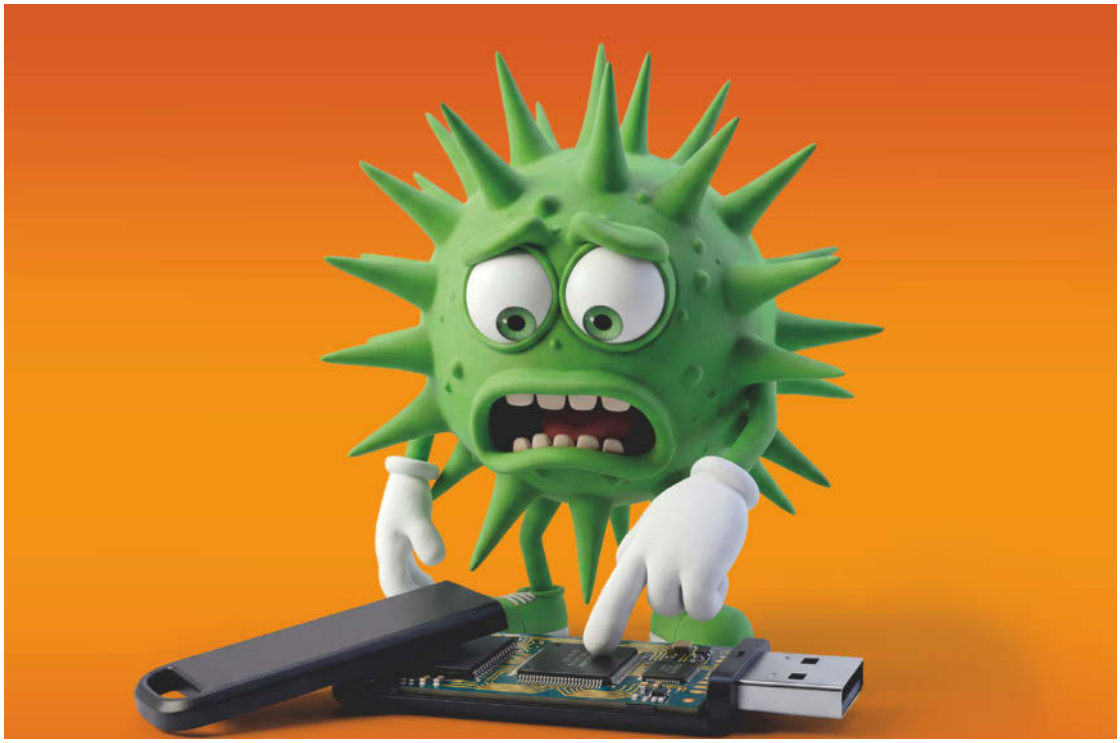


Bild: Martina Bruns / KI / heise medien

Entscheidungen zum neuen Desinfec’t

Wir haben unser Live-System zur Schädlingsjagd auf Windows-PCs erneuert. Dieser Artikel blickt technisch auf die Neuerungen und die Auswirkungen für Nutzer.

Von **Peter Siering**

Desinfec’t war über Jahre ein bootbares Image für optische Datenträger, das wir als ISO-Datei oder physische Heft-DVD herausgaben. Damit es überhaupt vom Stick startet und Änderungen dauerhaft speichert, waren viele Kunstgriffe nötig. Die jedoch erschwerten Updates und waren auch eine Bürde für die Weiterentwicklung. So entstand der Plan, die zugrundeliegende Technik von Desinfec’t zu erneuern.

Die Entstehung und welche Rolle dabei künstliche Intelligenz spielt, beschreibt der Artikel auf Seite 92. Im Folgenden soll es nicht um die Werkzeuge gehen, sondern darum, welche technische Finesse in Desinfec’t 2026/27 steckt und welche

Kompromisse wir für diese Runderneuerung des Werkzeugs eingegangen sind.

Die größte Änderung besteht wohl darin, dass Desinfec’t kein ISO-Image einer DVD mehr ist. Vielmehr handelt es sich um ein Abbild (Image) einer externen Festplatte mit mehreren GPT-Partitionen für moderne UEFI-Systeme. Es startet mit und ohne Secure Boot und auch an Rechnern noch mit einem klassischen BIOS. Eine der GPT-Partitionen enthält ein Btrfs-Dateisystem und damit das Herz der Linux-Distribution Desinfec't.

Btrfs-Blues

Die Wahl des Dateisystems lag nicht auf der Hand. Wir haben Btrfs ausgewählt, weil es seine Verwaltungsdaten mit Prüfsummen schützt und sich so Ausfallerscheinungen besonders von billigen und defekten Flash-Speichern schneller erkennen lassen sollten, als dies bei anderen Dateisystemen der Fall wäre. Außerdem kennt Btrfs das Konzept von Snapshots – so können Sie als Nutzer mit wenigen Handgriffen den Urzustand des Images wiederherstellen.

Wir handeln uns mit der Funktionsweise von Btrfs allerdings Nachteile ein. Es arbeitet nach dem Copy-on-Write-Prinzip. Schreibvorgänge fallen umfangreicher aus und strapazieren den Datenträger stärker als bei anderen Dateisystemen. Schwache USB-Sticks, die sonst unauffällig funktioniert haben, können die Schreiblast nicht schultern, und bremsen das System so stark, dass es unbenutzbar wird – oft startet das neue Desinfec’t dann nicht mal.

Wir haben einige Experimente mit Alternativen gemacht: Der erste Ansatz war ein Start mit einem OverlayFS, das sämtliche Schreibzugriffe in den Hauptspeicher umleitet. Das lässt Desinfec’t auch von schwächelnden Sticks zunächst zügig starten. Wenn jedoch später Signatur- und eventuelle Paketupdates wieder auf den Stick geschrieben werden, kommt es erneut zu kleinteiligen Schreibzugriffen, die solche Sticks überfordern.

Als zweite Alternative haben wir das in Linux enthaltene, auf Flash-Speicher optimierte f2fs ausprobiert. Hiermit startete unser Prototyp auch mit einem Overlay, schrieb aber Änderungen nicht kleinteilig, sondern in großen Blöcken zurück. Zu unserem Erstaunen versagten auch hierbei die schwachen Sticks. Aufgrund unzufriedener Nutzer haben wir schließlich auch ext4 noch als Alternative ausprobiert – das Ergebnis: auch ext4 funktionierte nicht besser.

Da es offenbar keine Rolle spielt, welches Dateisystem benutzt wird, sondern es allein auf die Qualität des USB-Sticks ankommt, stehen wir weiter zu



Im Bootloader Grub finden Sie eine Option, um einen Desinfec’t-Datenträger in die Werkseinstellungen, also den Ausgangszustand des Image, zurückzuversetzen.

unserer Entscheidung für Btrfs. Die Kombination seiner Vorteile überwiegt aus unserer Sicht deutlich etwaige Gewinne, die man mit anderen Dateisystemen erzielen könnte. Maßgeblich ist ein ordentlicher Stick.

Flash-Tücken

Bei der Auswahl des Datenträgers sollten Sie sich an den allgemeinen Qualitätskriterien für Flash-Speicher orientieren: USB-Sticks enthalten üblicherweise den qualitativ schlechtesten Flash-Speicher und simpelsten „Flash Translation Layer“ (FTL), der Blockoperationen auf Flash-Adressen übersetzt und die Speicherzellen verwaltet. Bessere Technik finden Sie bei MicroSD-Karten (nicht SD-Karten!). Am allerbesten fährt man mit einer (gern auch wegen der Kapazität ausgemusterten) SSD am USB-Adapter, idealerweise mit UAS-Unterstützung (USB Attached SCSI).

USB-Sticks sieht man ihre Qualitäten nicht an und die Hersteller nennen, wenn überhaupt, nur die kontinuierliche Leistung beim Lesen und Schreiben. Selten trifft man auch auf Angaben zu den Ein- und Ausgabeoperationen, die ein Stick pro Sekunde schafft (IOPS). Bei MicroSD-Karten hingegen gibt es technische Spezifikationen: Die nützlichste Angabe, um eine passende SD-Karte zu finden, ist die Application Performance. Dort verspricht das Siegel A2 die meisten IOPS. Bei den SSDs für den Desinfec’t-Einsatz braucht man sich darüber keine Gedanken zu machen.

Einen plausiblen, in endlicher Zeit laufenden Benchmark, der ein passendes Urteil über die Eignung von USB-Sticks für den Einsatz mit Desinfec’t ausspuckt, haben wir nicht gefunden. Der zuverlässigste Test ist schlicht Ausprobieren: Bespielen Sie Ihren Stick mit dem Image. Wenn das System in rund einer Minute startet und Signatur-Updates aller Scanner in endlicher Zeit erledigt, haben Sie einen brauchbaren Stick. Gute Sticks starten schneller.

Dass die Qualität des Datenträgers entscheidend ist, haben wir schon bei früheren Versionen von Desinfec’t festgestellt. Damit sich Nutzer nicht allein auf das Gefühl verlassen müssen, haben wir das Programm Flashguard geschrieben und eingebaut: Es wacht über die Vitaldaten des Boot-Datenträgers und warnt, wenn sich Fehler häufen. Das können Btrfs-Prüfsummenfehler sein, stark verzögerte Zugriffe oder auch Warnungen des Kernels, bei SSDs auch SMART-Fehler.

Nehmen Sie solche Warnungen im laufenden Betrieb ernst. Sie erscheinen als Nachrichten unten rechts auf dem Bildschirm und enthalten üblicherweise eine Handlungsempfehlung. Vereinzelt bei umfangreichen Paketinstallationen auftretende Warnungen können Sie ignorieren. Wenn Desinfec’t aber auch zäher reagiert und die Warnungen mehrfach auftreten, sollten Sie handeln. Einige Datenträger liefern vermeintliche SMART-Fehler, für die sich bei einer Recherche über die Bedeutung herausstellt, dass sie nur durch Missinterpretation zustande kommen. Die von Flashguard angezeigten Warnungen erlauben per Knopfdruck solche Warnungen dauerhaft zu unterdrücken.



Flashguard wacht über den Zustand des Bootdatenträgers und summiert die aufgelaufenen Lese- und Schreibdatenmengen.

NTFS-Lücken

Nicht nur das Dateisystem, das Desinfec’t selbst verwendet, hat uns beschäftigt, sondern auch die Windows-Dateisysteme, die untersucht werden sollen. Vor allem NTFS, also das Dateisystem, das Windows üblicherweise verwendet. Dafür existieren im Linux-Umfeld zurzeit zwei Implementierungen: im Kernel ntfs3, das von der Paragon-Implementierung abstammt, und im User-Mode ntfs-3g, das als langsamer gilt. Für eine dritte Implementierung,

die in jüngste Kernel-Versionen gerade Einzug hält, war es noch zu früh.

Unsere erste Wahl war der ntfs3-Treiber des Kernels, weil er als schneller gilt. Im Lauf der Evaluierung zeigten sich aber mehrere Nachteile: Er reagiert nicht gut, wenn viele Prozesse gleichzeitig bestimmte Strukturen des Dateisystems beharken. Außerdem kommt man damit nicht an die in NTFS gebräuchlichen Alternate Data Streams (ADS) heran. Das heißt, bei einer Prüfung des Dateisystems auf Schädlinge könnte Desinfec't dort versteckte Rootkits und Malware nicht finden.

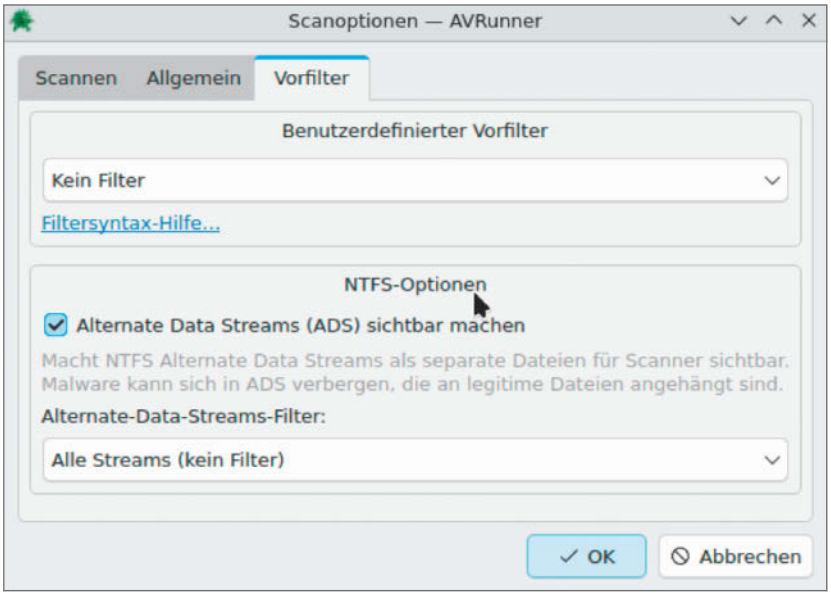
Auf den ersten Blick war auch ntfs-3g wenig geeignet, denn es hat ebenfalls einen blinden Fleck: Es setzt die mit Windows 10 eingeführte Technik „Windows Overlay Filter" (WOF) nicht um. Windows nutzt sie, um Speicherplatz zu sparen und Dateien zu komprimieren. Anders als die in NTFS vorgesehene transparente Kompression nutzt WOF Platzhalter im Dateisystem (Reparse Points), die Zugriffe auf solche Dateien auf einen speziellen Handler (Filter) umleiten.

Dieser Filter dekomprimiert die Datei und stellt sie transparent bereit. Microsoft nutzt diese Funktionen auch, um redundante Dateien in einer Windows-Installation nur ein einziges Mal zu speichern. Die Reparse Points können letztlich auf WIM-Dateien verweisen (so dedupliziert Windows dann auch den Datenbestand). Mit `compact` gibt es unter Windows im Terminal ein Programm, um mit WOF-Komprimaten zu arbeiten.

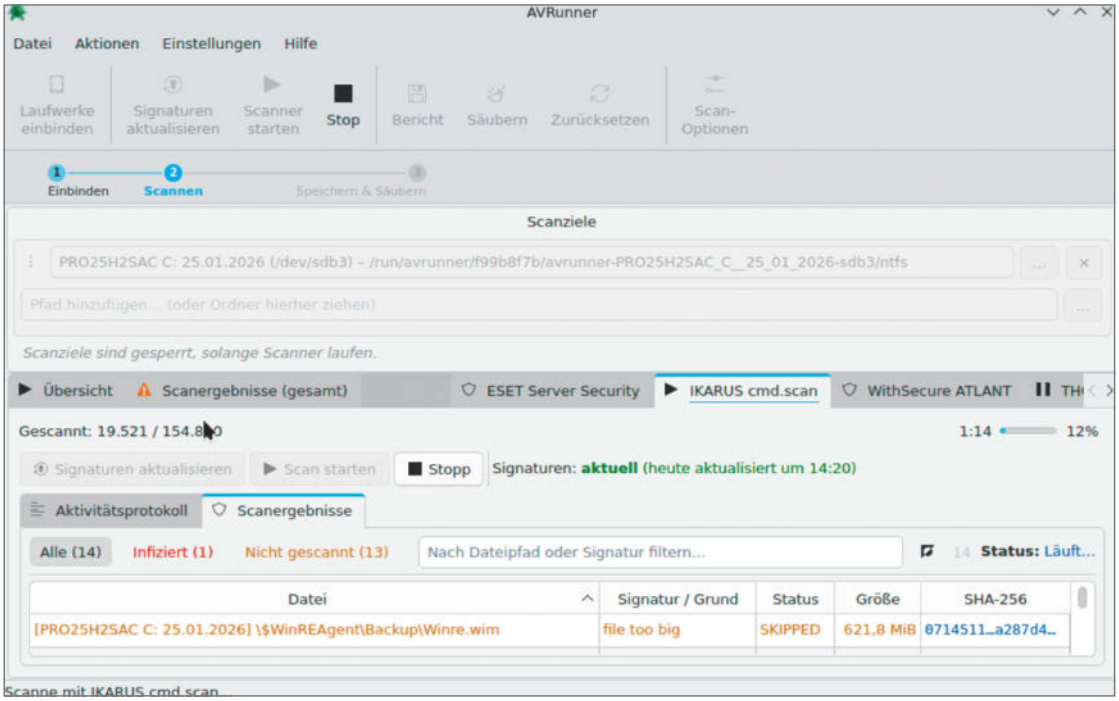
Glücklicherweise gibt es eine freie Implementierung der Funktionen als Bibliothek in ntfs-3g von Eric Biggers auf GitHub. Damit lassen sich solche Dateien zwar nur lesen, nicht schreiben, doch das genügt für die Zwecke von Desinfec't. So konnten wir diesen blinden Fleck in ntfs-3g beseitigen, sodass die Scanner in Desinfec't ein ziemlich vollständiges Bild der Inhalte eines NTFS-Dateisystems erhalten. Übrigens: Die erwähnten „bestimmten Strukturen", bei denen der ntfs3-Treiber des Kernels Probleme mit parallelen Zugriffen mehrerer Prozesse hat, sind ebendiese WOF-Daten.

Ein kleiner blinder Fleck bleibt bei NTFS, trotz aller Bemühungen: Der Inhalt von Dateien, die mit der nativen NTFS-Verschlüsselung (EFS) geschützt sind und die nur der angemeldete Nutzer unter Windows im Klartext sehen kann, bleibt Desinfec't verborgen. Der Vollständigkeit halber sei auch noch erwähnt: Die unter Windows mit Access Control Lists (ACL) gesetzten Zugriffsrechte interessieren unter Linux einen feuchten Kehricht. Desinfec't bindet Windows-eigene Dateisysteme so ein, dass es vollen Zugriff hat.

Desinfec't bindet NTFS-Laufwerke für die Scans nur lesend ein. Erst wenn Sie nach Schädlingsfun-



Alternate Data Streams in NTFS-Dateisystemen stellt nicht jede NTFS-Implementierung unter Linux bereit. Desinfec't wählt einen Sonderweg, um sie einzubinden.



Desinfec't hegt die Scanner mit allerlei Maßnahmen ein, damit der Schädlingsjäger einschätzen kann, wie lang er noch ansitzen muss.

den die Säuberung starten, die vermeintlich gefährliche Dateien umbenennt, muss Desinfec't auf NTFS schreiben. Dabei geht es mehrstufig zu Werke, weil NTFS-Volumes von Windows in einem nicht konsistenten Zustand hinterlassen werden.

Das kann mehrere Gründe haben: der Windows-Schnellstart, ein vom Nutzer gewünschter Ruhezustand oder ein technisches Problem. Wenn sich ein NTFS-Dateisystem in einem inkonsistenten Zustand befindet, warnt Desinfec't, bevor es schreibt. Sie sollten das Schreiben nur erzwingen, wenn das Kind schon im Brunnen liegt, nicht aber, wenn Sie Desinfec't nur ausprobieren.

Lässt sich ein NTFS-Dateisystem partout nicht einbinden, greift Desinfec't auf den Kernel-NTFS-Treiber (ntfs3) zurück. Der setzt sich großzügiger über den Zustand inkonsistenter NTFS-Dateisysteme hinweg und ermöglicht großzügig Schreibzugriffe mit eventuellen Nebenwirkungen. Das Steuerprogramm für die Scanner (AVRunner) warnt hiervor intensiv: Schlagen Sie diese Warnungen nicht leichtfertig in den Wind!

BitLocker-Locken

NTFS-Dateisysteme sind außerdem mitunter mit BitLocker verschlüsselt. Der Linux-Werkzeugkasten bietet auch hier zwei Varianten an, um den Zugriff zu realisieren: Dislocker und das für die Linux-Datenträgerverschlüsselung gebräuchliche Cryptsetup. Desinfec't verwendet Dislocker – es gilt momentan als das ausgereiftere Werkzeug.

Desinfec't kann BitLocker-Volumes in ganz unterschiedlichen Stadien vorfinden: Fertig verschlüsselte öffnet es, wenn der Nutzer einen Wiederherstellungsschlüssel oder das Passwort eingibt. Ein geschlossenes Schloss im Dialog zum Einbinden der Laufwerke ist der Hinweis darauf.

Bei Volumes, die durch die von Windows erzwungene Geräteverschlüsselung geschützt werden, gelten andere Regeln: Wenn diese Verschlüsselung noch nicht abgeschlossen ist, also Windows mittendrin unterbrochen wurde, kommt Desinfec't an das Laufwerk nicht ran. Windows muss sein Werk erst vollenden.

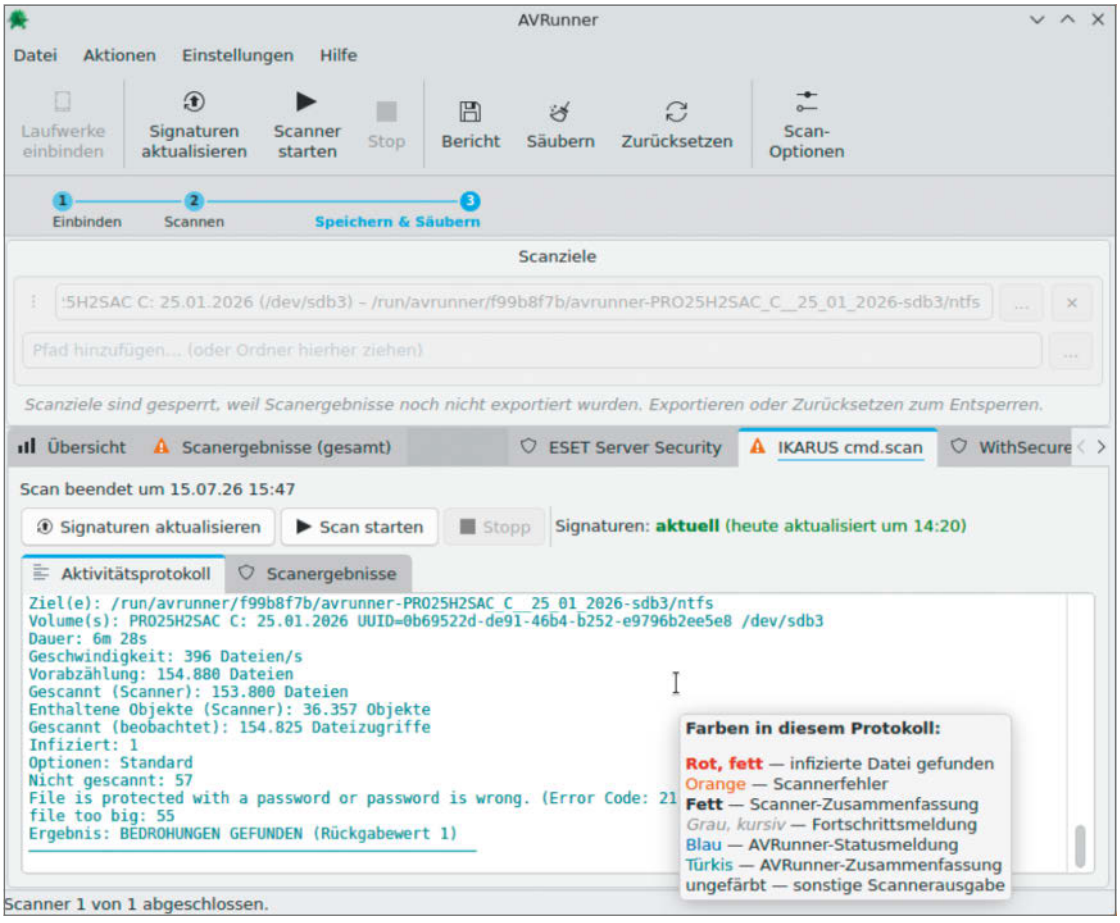
Außerdem kann ein Laufwerk zwar vollständig verschlüsselt sein, ohne den Wiederherstellungsschlüssel in einem Microsoft-Konto oder anderswo zu speichern oder zu notieren. Dann kann Desinfec't das Laufwerk direkt zugänglich machen. In beiden Fällen sehen Sie ein offenes Schloss im Dialog.

Datenträger mit BitLocker-To-Go behandelt Desinfec't wie fest installierte – es bindet sie nicht automatisch ein. VeraCrypt ist ein Sonderfall in Desinfec't: Solche Volumes werden unmittelbar in den Linux-Dateibaum eingebunden (Mounten). Damit die Scanner alle Dateien auf dem Datenträger sehen, müssen Sie aber in den Scanoptionen von AVRunner unter „Allgemein" die Option „Scans mit erhöhten Rechten ausführen" setzen.

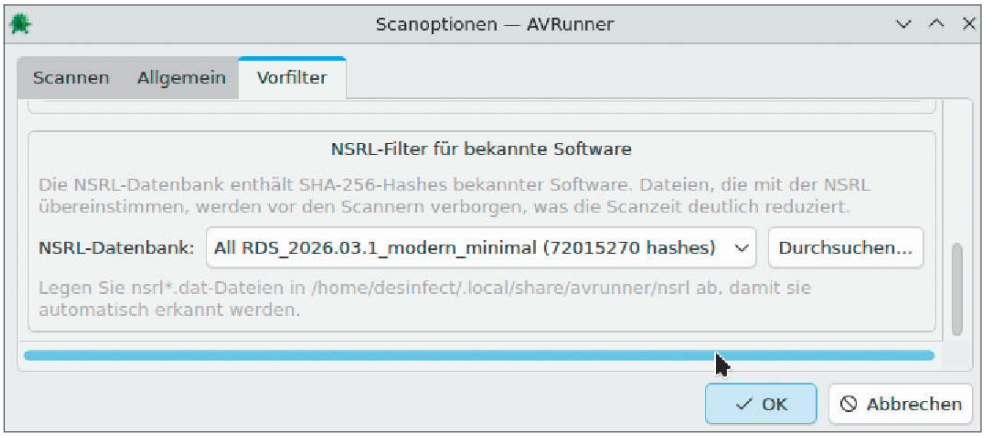
Scanner zähmen

Bei der Neuentwicklung von Desinfec't haben wir darauf geachtet, dass der Benutzer kontinuierlich darüber im Bilde ist, was das System gerade tut. Dazu gehören Informationen darüber, wie weit die Scanner bereits gekommen sind und etwaige Warnungen über hängen gebliebene Aufgaben und knapp werdende Systemressourcen. Im Idealfall sollen Sie als Nutzer bei Problemen erkennen, was Sie ändern können, um den PC doch noch erfolgreich zu untersuchen.

Nun haben die Hersteller der Scanner, die unser Projekt freundlicherweise mit einer Jahreslizenz unterstützen, andere Anforderungen an ihre Pro-



AVRunner liefert eine Zusammenfassung über den Scanumfang. Geringe Abweichungen sind in der aktuellen Implementierung erwartbar.



Eine experimentelle Idee: Vorfiltern des Scanziels nach wohlbekannten Dateien, um den Scanumfang zu reduzieren. Dateien mit bekannten SHA256-Prüfsummen werden ausgeblendet.

dukte. IKARUS cmd.scan passt am besten ins Desinfec't-Konzept: Ein Programm startet, um den Scanner einen Dateibaum untersuchen zu lassen. Es meldet dabei fortlaufend etwaige Befunde und zeigt auf Wunsch sogar jede angefasste Datei an.

ESET Server Security und WithSecure ATLANT gehen einen anderen Weg: Der Scanner steckt in einem Hintergrundprozess (Daemon), der kurz nach dem Booten startet und von einem Frontend mit Scanaufträgen gefüttert wird. Bei WithSecure gibt das Frontend die Ergebnisse direkt aus, bei ESET hingegen muss Desinfec't ein weiteres Programm bemühen, um die Ergebnisse einzusammeln.

Wie weit ein Scanvorgang fortgeschritten ist, kann Desinfec't keinem der Programme entlocken. Deshalb lassen wir das Steuerprogramm für die Scanner (AVRunner) die Systemaufrufe überwachen, mit denen die Scanner Dateien auf den zu untersuchenden Datenträgern öffnen. Dadurch, dass wir die Gesamtdateizahl vor dem Scan ermitteln, können wir daraus den Fortschritt ableiten und eventuelle Hänger erkennen.

Die Methode klingt einfach, ist aber kompliziert: Je nach Implementierung bei den Scannern mussten wir dafür zunächst die richtigen Prozesse finden. Die Herausforderung lag darin, mit AVRunner ganze Prozessgruppen zu beobachten und den Mechanismus so trennscharf zu gestalten, dass er auch mit parallel ausgeführten Scans zurechtkommt und die Zugriffe korrekt zuordnet.

Der Perfektionsgrad der Zählung ist für das Feedback an den Nutzer gut genug. Die Zahlen taugen für eine grobe Einschätzung, ob ein Scanner wirklich den vollständigen Satz der Dateien auf dem Scanziel bearbeitet hat. Wenn Ihnen in den von AVRunner ausgegebenen Zählern kleine Unterschiede im Verhältnis zur Gesamtdateizahl auffallen, ist das kein Grund zur Sorge. Auch bei sehr kleinen Scanumfängen können die Zahlen etwas pendeln.

Desinfec't gleicht auch noch allerlei andere Eigenarten der Scanner aus: So liefert IKARUS cmd.scan zum Beispiel verstümmelte Dateinamen zurück, Umlaute etwa fehlen vollständig. AVRunner versucht deshalb, in solchen Fällen die richtigen Dateinamen zu erraten. Möglich, dass das in Extremfällen auch mal misslingt.

IKARUS hat außerdem eine interne Längenbeschränkung beim Dateipfad. Die langen Namen der Verzeichnisse, unter denen Desinfec't die zu untersuchenden Dateisysteme einhängt, sind dabei kontraproduktiv. Das haben wir nicht auch noch eingefangen, sondern nehmen in Kauf, dass es so aussieht, als wären einzelne Dateien übersprungen worden. Bei den anderen Scannern haben wir kein solches Verhalten beobachtet. Bei WithSecure ATLANT fiel uns auf, dass das vom Hersteller für On-Demand-Scans mitgelieferte Programm den Daemon nicht optimal füttert und dessen Parallelverarbeitungspotenzial nicht ausschöpft. Desinfec't parallelisiert das deswegen selbst.

Filterfreuden

Mit den von den Scannern bereitgestellten Möglichkeiten, Scans auf bestimmte Dateigrößen oder -typen zu beschränken oder nur nach einem bestimmten Zeitpunkt geänderte Dateien zu unter-

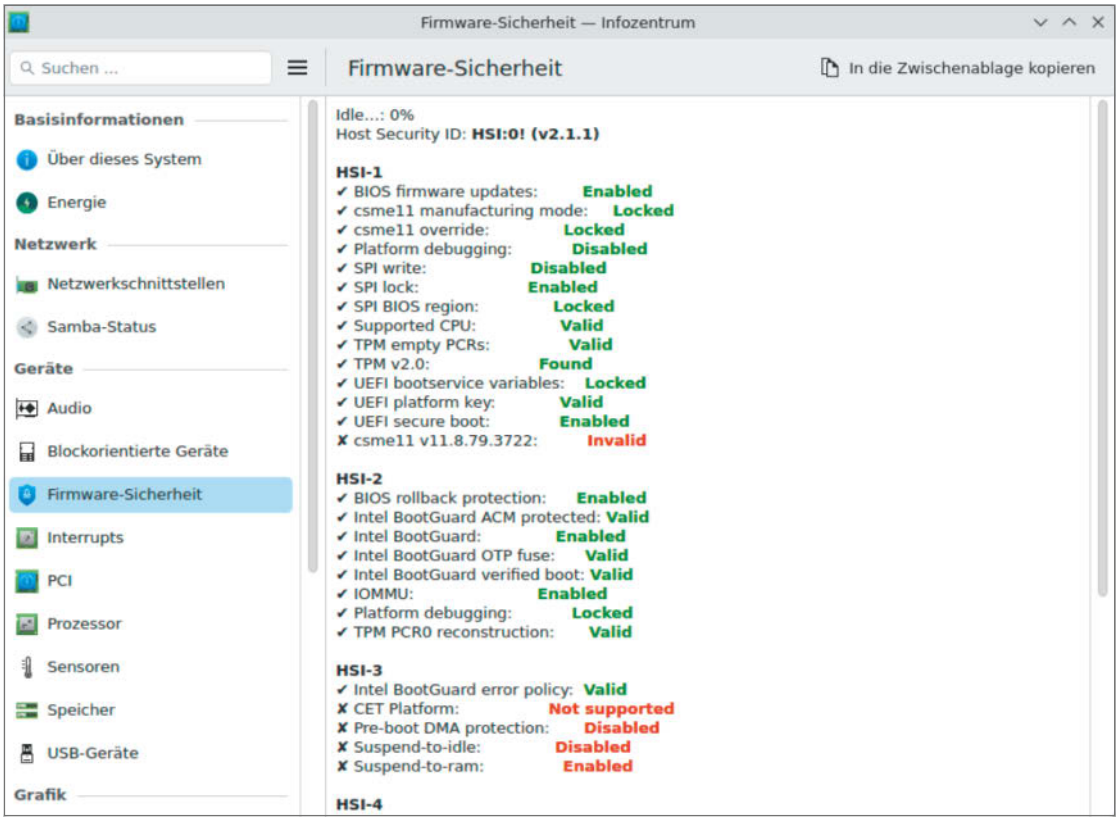
suchen, waren wir nicht zufrieden. Deshalb kamen wir auf die Idee, die Liste der zu scannenden Dateien selbst zu filtern und nur das Ergebnis an die Scanner weiterzugeben. Dafür bietet sich das (schon von ntfs-3g und Dislocker verwendete) Filesystem in Userspace (FUSE) an.

AVRunner startet zum Scannen von NTFS-Dateisystemen stets einen separaten Prozess „avrunner-fuse-proxy“: Der filtert dort alle Hardlinks, also redundant im Dateisystem referenzierte Dateien, aus dem für die Scanner sichtbaren Dateibaum aus. Das sind in regulären Windows-Installationen mehrere zehntausend Dateien und zahlt sich spätestens dann aus, wenn mehrere Scanner den Datenbestand durchforsten sollen.

Eine weitere wichtige Funktion des Proxys ist, auf NTFS-Dateisystemen Alternate Data Streams (ADS) für die Scanner sichtbar zu machen. Schließlich kann sich hier Malware verstecken. Der ntfs-3g-Treiber nutzt dafür erweiterte Attribute (xattrs) mit dem Präfix „user.“. Damit Sie die Streams leichter den Dateien zuordnen können, erzeugt der Proxy synthetische Dateinamen der Form „mein.txt:ads-data.dta:“ für alle Streams einer Datei und ahmt so die unter Windows gebräuchliche Schreibweise mit Doppelpunkt als Trennzeichen nach.

Wir haben außerdem ein experimentelles Feature in den Proxy eingebaut: Er kann zum Beispiel die vom US-amerikanischen National Institute of Standards and Technology (NIST) veröffentlichten Listen mit Prüfsummen für wohlbekannte Dateien als Filter verwenden und diese für die Scanner ausblenden, sofern die Prüfsumme der lokalen Datei stimmt. Das klappt genauso mit anderen Dateilisten mit SHA256-Prüfsummen, die Sie importieren. Details dazu finden Sie auf der Projektseite ct.de/desinfect.

Wir haben außerdem noch einen Vorfilter eingebaut, mit dem Sie gezielt nach bestimmten Dateien oder Dateitypen suchen können. Die Optionen orientieren sich dabei an denen des Kommando-



Desinfec’t 2026/27 beherrscht Secure Boot, aber nur, wenn der PC noch den alten Zertifikaten aus 2011 vertraut. Für die neuen Zertifikate aus 2023 ist es nicht gerüstet.

zeilenprogramms `find`. Beispiele für die Syntax zeigt AVRunner als Tooltipp, wenn Sie den Mauszeiger auf den eingebauten Filtern in den Scanoptionen ruhen lassen. Achtung: Optionen zur Größenangabe von Dateien, die die Scanner bieten, und die des Proxy addieren sich.

Skeptiker werden einwenden, dass die gestapelten FUSE-Schichten das Scannen verlangsamt. Zu Recht. Einiges davon fangen Caches im FUSE-Layer und der Page Cache des Kernels ab. Andererseits: Die Alternative wäre ein schnellerer, aber unvollständiger Zugriff, im Fall von Kernel-ntfs3 sogar ein fehlerhafter. Außerdem ist auf vielen Systemen FUSE ohnehin wegen BitLocker im Spiel.

Aus unserer Sicht sind die zusätzlichen Schichten mehr wert als ein schneller Scan. Indem Sie zum Beispiel gezielt nur die in den vergangenen 30 Tagen geänderten Dateien scannen lassen, sparen Sie eine Menge Zeit. Ohne den Proxy wäre das nicht so leichtfüßig für den Anwender realisierbar.

Rest vom Fest

Mancher, der bis hier den Erklärungen gefolgt ist, wird sich fragen, warum wir die Dateizählung und den Proxy nicht verheiratet haben. Glückwunsch. Dieses Lämpchen ist uns inzwischen auch aufgegangen – leider erst nach einigen Tests des nahezu fertigen Systems, sodass wir die Vereinheitlichung der beiden Komponenten auf eine spätere Generation verschoben haben.

Der Proxy ist momentan noch in Python implementiert. Eine Portierung auf C/C++, die mehr Geschwindigkeit verspricht, haben wir vertagt. Das bleibt einer kommenden Version vorbehalten, die auf die gleichzeitige Nutzung durch mehrere Scanner eingestellt ist, die Zählung integriert und detaillierte Daten liefert, ob die Scanner sämtliche Dateien bearbeitet haben.

Bis dahin können sich Nutzer mit Forscherdrang einer während der Entwicklung von Desinfec't eingesetzten Debug-Funktion bedienen. Setzen Sie unter /home/desinfect/.config in der avrunnerrc-Datei im Abschnitt `[Debug]` die Option `LogFileList=true`. Dann hält AVRunner eine Liste von zu scannenden Dateien vor und spuckt bei sequenziellen Scanläufen je Scanner eine zusätzliche Log-Datei der vom Proxy weggefilterten Dateien und vom Scanner übersprungene Dateien aus.

Das verlängert Scanläufe, strapaziert die Systemressourcen stärker (vor allem den knappen Hauptspeicher) und empfiehlt sich somit nur für die Fehlersuche, etwa weil Scanner offenbar nur einen Teil des Scanziels berücksichtigen. Es sollte nur als letztes Mittel dienen, dann, wenn sich sämtliche anderen Hilfsmittel erschöpft haben, etwa ausführlichere Scanaktivitätsprotokolle, die über die Scanoptionen zugänglich sind.

Zertifikatsroulette

Verzockt haben wir uns im Hinblick darauf, dass Desinfec't im großen Update-Jahr der Secure-Boot-Zertifikate 2026 für jeden Fall gerüstet ist. Wir hatten gehofft, dass die Ubuntu-Entwickler hier Lösungen für die Distribution erarbeiten und fertigstellen werden. Wir haben einen der zuständigen Entwickler mit Anfragen genervt, erhielten aber nur ausweichende Antworten.

Leider sieht es nicht so aus, als würde Ubuntu in endlicher Zeit überhaupt etwas anzubieten haben: Anstatt die für Secure Boot unter Linux übliche Zwischenschicht „shim“ von Microsoft mit den 2011er- und 2023er-Zertifikaten signieren zu lassen, haben die Ubuntu-Entwickler eine eigene Zwischenschicht entwickelt (sie heißt „stubble“) und zur Begutachtung eingereicht.

Für Desinfec't bedeutet das: Das veröffentlichte, auf Ubuntu aufbauende Image kann nur auf Systemen per Secure Boot starten, die noch dem alten Secure-Boot-Zertifikat von 2011 vertrauen – das dürfte für die meisten Rechner heute gelten. Neue PCs könnten nur noch dem neueren Zertifikat aus 2023 vertrauen, damit gelingt der Start nur mit abgeschaltetem Secure Boot. Bevor Sie das tun, müssen Sie aber unbedingt den BitLocker-Schlüssel Ihrer Windows-Partition auf Papier notieren – denn schlimmstenfalls müssen Sie den beim nächsten Start von Windows eingeben, um wieder an Ihre Daten heranzukommen.

Die Debian-Entwickler sind weiter: Sie haben einen Shim von Microsoft sowohl gegen die alten als auch die neuen Zertifikate für Secure Boot signieren lassen. Wir haben auch Desinfec't 2026/27 auf Basis von Debian Testing (Forky) gebaut: Mit dem neuen Shim startet es auch auf Systemen, die nur neuen Secure-Boot-Zertifikaten vertrauen. Wir stellen sie interessierten und Secure-Boot-geschädigten Lesern auf Anfrage gern zur Verfügung. Unserer Erfahrung nach sind die wenigsten Secure-Boot-Problem derzeit auf das Fehlen der 2011er-Zertifikate zurückzuführen. Meist ist das Problem, dass Geräte nur den Windows-Zertifikaten trauen, Details dazu in der FAQ auf Seite 30. (ps) c't

Desinfec't und NFTS-Implementierung:
ct.de/wnqg

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: Wilhelm Drehling (wid), Dennis Schirrmacher (des), Peter Siering (ps)

Mitarbeiter: Olivia von Westernhagen

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

DTP-Produktion: Vanessa Bahr, Martina Behncke, Beatrix Dedek, Laura-Sophie Gruhn, Madlen Grunert, Cathrin Kapell, Steffi Martens, Wolfgang Schwarz, Marei Stade, Matthias Timm, Christiane Tümmler, Nicole Wesche

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

Illustration, Fotografie: Thorsten Hübner, Albert Hulm, Moritz Reichartz

Titel: Steffi Martens, Martina Bruns / KI / heise medien

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

Mitglied der Geschäftsleitung: Jörg Mühle

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

Die kommerzielle Zweitvermarktung redaktioneller Inhalte der Heise Medien erfolgt exklusiv durch das F.A.Z.-Archiv. Anfragen zu Lizenzen, Nachdrucken, Datenbanknutzungen, Corporate- und institutionellen Mehrplatzlizenzen richten Sie bitte an das Team Rights Managment im F.A.Z.-Archiv per E-Mail an **syndikation@faz.de** oder Telefon unter **(069) 75 91-29 01**.

Einzelpreis: € 16,90; Schweiz CHF 29.90; Österreich € 18,50; Luxemburg € 19,50

Erstverkaufstag: 20.11.2026

Eine Haftung für die Richtigkeit der Veröffentlichungen kann trotz sorgfältiger Prüfung durch die Redaktion vom Herausgeber nicht übernommen werden. Kein Teil dieser Publikation darf ohne ausdrückliche schriftliche Genehmigung des Verlages in irgendeiner Form reproduziert oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden. Die Nutzung der Programme, Schaltpläne und gedruckten Schaltungen ist nur zum Zweck der Fortbildung und zum persönlichen Gebrauch des Lesers gestattet.

Für unverlangt eingesandte Manuskripte kann keine Haftung übernommen werden. Mit Übergabe der Manuskripte und Bilder an die Redaktion erteilt der Verfasser dem Verlag das Exklusivrecht zur Veröffentlichung. Honorierte Arbeiten gehen in das Verfügungsrecht des Verlages über. Sämtliche Veröffentlichungen erfolgen ohne Berücksichtigung eines eventuellen Patentschutzes.

Warennamen werden ohne Gewährleistung einer freien Verwendung benutzt.

Hergestellt und produziert mit Xpublisher: www.xpublisher.com

Printed in Germany.

Alle Rechte vorbehalten.

© Copyright 2026 by
Heise Medien GmbH & Co. KG



Bild: Martina Bruns / KI / heise medien

Per KI von der Idee zum Programm

KI sollte helfen, Ideen an einem Prototyp früh zu beurteilen. Es wuchs sich zu einer mehrmonatigen Chat-Session aus. Das Resultat: Desinfec't 2026/27.

Von **Peter Siering**

Das Linux-basierte Antiviren-System Desinfec't erscheint seit Jahren in c't. Es bedurfte dringend eines Neuanfangs: Die Basis war veraltet, viele technische Lösungen traten sich gegenseitig das Standbein weg und Updates gerieten zu einer peinvollen Aufgabe. Wir hatten in der Redaktion schon im vergangenen Jahr Pläne geschmiedet, was wir über Bord werfen und was wir weiterführen wollten.

Leider gab es Verzögerungen im Betriebsablauf und Anfang des Jahres musste ein Prototyp her, um zu prüfen, dass die Pläne praxistauglich sind. Mattias Schlenker, der das Projekt für c't über viele Jahre entwickelt und mitbetreut hat, gab dafür noch einige Impulse, hat sich aber aus der aktiven Mitarbeit zurückgezogen. Aufgrund guter Erfahrungen kam KI ins Spiel: Sie sollte zunächst nur die Fleißarbeit beim Prototypenbau beschleunigen.

Mit etwas Know-how zum Bau von Linux-Distributionen waren die ersten Schritte ein Klacks: Claude Opus 4.6 generierte binnen Stunden Skripte zum Erstellen bootfähiger Btrfs-Images auf Ubuntu-Basis.

Der Prototyp bewies, dass Btrfs und USB-Sticks im Team spielen. Der KI-Einsatz eskalierte: Aus einem Prototyp wuchs ein Dutzend Projekte. Wir skizzieren die KI-Programmierreise für ein zentrales Programm und ordnen die Ergebnisse ein.

Skepsis

Hätte man mir vor Monaten gesagt, dass ich einmal ein begeisterter KI-Flüsterer werde, ich hätte es nicht geglaubt. Seit KI sich in unser aller Leben drängelt, habe ich ihr immer mal wieder Aufgaben übertragen. Oft mit Erfolg entstanden kleine Skripte oder Programme. Manche Frage zu technischen Details beantwortete sie zielgerichteter als jede Suche in den Weiten des Internets. Doch umfangreiche Dinge? Ich war skeptisch.

Die Skepsis wich schon auf der ersten Etappe, zusammengefasst lautete der Auftrag: „Bau eine minimale Ubuntu-Distribution auf Basis der aktuellen Vorabversion von 26.04 LTS, die als Dateisystem Btrfs nutzt. Das Image soll direkt booten können. Es soll eine Desktop-Umgebung mitbringen und möglichst schlank sein. Der Bau soll aus einer GitLab-Umgebung heraus und lokal auf einem Debian oder Ubuntu laufen können."

Der Gesprächspartner Claude glänzt als neuer „Kollege": Er hat stets Zeit und inhaliert Stack Overflow, Bug-Tracker, Mailinglisten und Blogs wie der Roboter aus „Nummer 5 lebt!". Ein enormer Zeitfresser bei solchen Projekten sind die Recherchen. Statt alle Quellen einzeln anzusteuern und zu befragen, spuckt Claude die Antworten direkt aus, schließt meine Wissenslücken im Nu und unterbreitet Vorschläge.

Aber nicht nur das: Wenn ich eine Idee habe, schreibt Claude ratzfatz den Code dafür. Dabei spuckt er den langweiligen Kram, der stumpf enorm viel Zeit fürs fehlerfreie Hinschreiben kostet, binnen Sekunden aus. So ist eine Idee in der Praxis viel schneller ausprobiert, anstatt lange auf ihr herumzudenken. Erfahrene Entwickler wissen: Vieles ergibt sich erst, wenn man ein Programm benutzen kann.

Fast könnte man streiten, wer die Ideen hat. An vielen Stellen ergänzen sich meine Wünsche und der Wissensschatz der KI: Eine Ideenskizze genügt und Claude kommt daraufhin mit dazu passenden Techniken um die Ecke. Im Dialog schält sich dann heraus, welche wohl am besten geeignet wäre. Gefühlt entwickeln sich furchtbar fruchtbare fachliche Diskussionen.

Mein Hintergrundwissen hilft mir, dass Claude die Richtung hält: Oft kann ich angebotene Alternativen gleich ausschließen. Mitunter irrlichtert der „Gesprächspartner", lässt sich aber immer einfangen, wenn man denn mitbekommt, dass das so ist. Dass Claude fantasiert, wie KI-Skeptiker gern erzählen, erlebe ich vergleichsweise selten, dass er aber Vorurteile als Fakten ausgibt, immer wieder.

Organisation

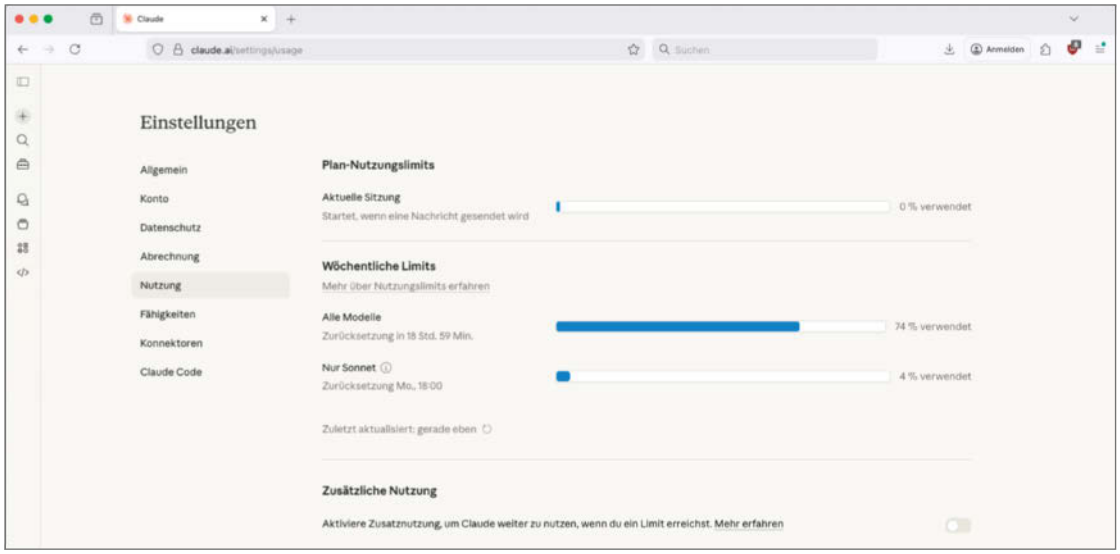
Eine Anforderung schon für den Prototyp war Reproduzierbarkeit: Von Anfang an soll Claude deshalb Git-Repositories für die im Chat entwickelten Projekte führen und Änderungen als Commits anlegen. Er stellt diese als Zip- oder tar.gz-Archiv bereit. Commits landen dann nach Sichtung und Test in eigenen Git-Repositories, an die die KI nicht herankommt. Theoretisch könnte ich eigene Repositories auch in Claude Code zugänglich machen, doch davor scheue ich mich.

Die Git-Repositories stellt eine private GitLab-Instanz bereit, die mit Runnern automatisiert übersetzt und auf Wunsch Installationspakete baut. Die dazu nötigen Anleitungen (.gitlab-ci.yml) hat samt und sonders ebenfalls Claude generiert. Erst das, was aus einem solchen Pipeline-Lauf herausfällt, wird überhaupt getestet. Eigene Änderungen am Code landen, sofern notwendig, in einem separaten Branch, um die Claude-Commits dort per Merge zu integrieren.

Die Commit-Messages von Claude sind ausführlich und direkt einzusortieren, etwa als Fix oder Feature. Kommentare im Code geraten geradezu ausschweifend, sodass der sich einladend lesen lässt. Aufgaben, von denen anzunehmen ist, dass sie vom eigentlichen Thema wegführen und größere Tiefe annehmen könnten, sind in separaten Chats besser aufgehoben. Das verseucht das Kontextfenster nicht ständig mit abseitigen Details.



Claude lernt unterwegs Dinge und gleicht sie mit inhaliertem Wisssen ab. Der Vorschlag verblüffte im ersten Moment doch. Dass es um Desinfec't geht, entnahm die KI dem Nutzernamen, den hochgeladene Debugging-Ausgaben enthielten.



Das Guthaben der Claude-Einstiegs-Abos frisst ein umfangreicheres Projekt so schnell weg, dass es gar nicht lohnt, die Kreditkarte wegzustecken.

Schon nach wenigen aktiven Tagen stoße ich an die Grenzen meines 20-Dollar-Abos. Vor allem das Limit für die „Aktuelle Sitzung“ beschränkt mein Tun. Das Zeitfenster startet mit der ersten Nachricht an die KI. Es wird erst nach mehreren Stunden zurückgesetzt. Oft erwischt mich die Pause, die sich Claude gönnt, zur Unzeit. Also zücke ich die Kreditkarte und stelle auf Max (5x) um. Ab jetzt kostet der Assistent rund 100 Euro pro Monat. Die „aktuelle Sitzung“ behindert mich nicht mehr. Das Wochenlimit reiße ich auch nicht mehr.

Allerdings ist meine Nutzungsweise etwas untypisch: Würde ich nicht nur den Chat, sondern Claude Code verwenden, fräße das mein Nutzungskontingent schneller weg. Ich lerne von anderen KI-Flüsterern, dass sie gern für triviale Fragen auf Sonnet als Modell ausweichen, das separat verrechnet wird, um so das Token-Guthaben für komplexe Aufgaben zu sparen. Ich habe mitunter das kostenlose ChatGPT als Lückenbüßer beschäftigt.

Transparent ist das alles nicht. Über die im Hintergrund verrechneten Token erfährt der Chat-Kunde bei den Claude-Flatrates nichts. Er kommt erst mit ihnen in Kontakt, wenn er „zusätzliche Nutzung“ bucht, bei der dann nicht mehr pauschal abgerechnet wird, sondern etwa bei Opus 4.7 dann tatsächlich über verbrauchte Token zu einem festen, durchaus stattlichen Preis.

Naheliegende Tendenz: je mächtiger ein neues Modell, desto mehr Token verschlingt es. Wie viele Token das Abo für ein Nutzungsmodell enthält, verrät Anthropic nicht. In Claude Code tauchen Token auf, aber man sieht nur den Verbrauch und nicht den Vorrat. Auch hier bleibt es bei Prozentangaben für den Nutzungsanteil der aktuellen Sitzung und Woche.

Review

Ich lade Kollegen mit Programmiererfahrungen zu einer Code-Review für ein großes Teilprojekt ein, das Claude nach meinen Vorgaben erzeugt hat: AVRunner ist die neue zentrale Steuerinstanz für im kommenden Desinfec’t integrierte Virenscanner (ClamAV, Eset, Ikarus und WithSecure). Es handelt sich um eine C++-Anwendung, die auf den Qt- und KDE-Frameworks aufbaut. Sie startet und stoppt die Scanner, beobachtet deren Tätigkeit, hält Ergebnisse fest und fasst sie zusammen, erlaubt das Säubern von Datenträgern und bindet sie auch interaktiv für den Nutzer ein.

Die Einschätzung des ersten Kollegen fällt wohlwollend aus. Er hat selbst schon mit Qt entwickelt und sieht sich gut strukturiertem Code gegenüber, der sich auf sprechend benannte Quelltextdateien verteilt. Er erwähnt positiv die detaillierten Kommentare, die er für viel nützlicher als menschengemachte hält: Sie erklären nicht, wie der Code etwas macht – was man ja sehen kann –, sondern warum dieser Weg gegangen wurde. Das hilft der KI bei der Orientierung, aber auch Menschen, die später damit weiterarbeiten sollen.

Ein zweiter Kollege, der bei heise Medien hauptamtlich programmiert, ist grundsätzlich skeptischer, was KI-generierten Code angeht. Und: Er steckt insgesamt tiefer in vielen der im Projekt verwendeten Techniken drin: Linux, Debian-Packaging, Qt und vor allem auch KDE. Auch ist seine Tauchtiefe eine andere, er nimmt sich mehrere Tage Zeit, den von Claude generierten Code zu inspizieren. Schnell fallen ihm Dinge auf, die seinem Arbeitsethos widerstreben.

Ein Teil ist Stilkritik: Er vermisst eine einheitliche Handschrift im Projekt, sieht variierende String-Typen und -Initialisierungen und nicht portable, aber weitverbreitete Guards in den Header-Dateien (Microsofts `#pragma once`). Konstanten sind nicht an einer Stelle definiert und sonst nur über einen sprechenden Namen zugänglich gemacht, sondern tauchen als Werte an mehreren Stellen auf. Rechenoperationen finden an einer Stelle als Mix aus Ganz- und Gleitkommazahlen statt.

Immer wieder packt ihn die Ungeduld, weil die KI Code generiert hat, den er selbst kürzer und knapper schreiben würde. Beispiele sind oft umständliche Initialisierungen von Variablen, unnötige Typumwandlungen und sinnfreie Zwischeninstanzen von Klassen – vor seinem geistigen Auge verplempert der Computer beim Ausführen des umständlichen Codes en masse Rechenleistung, vor allem verstellt die Umständlichkeit den Blick aufs Wesentliche für ihn. An vielen Ecken sieht er das Programm entgleisen, weil Fehler im Code nicht geprüft und behandelt werden.

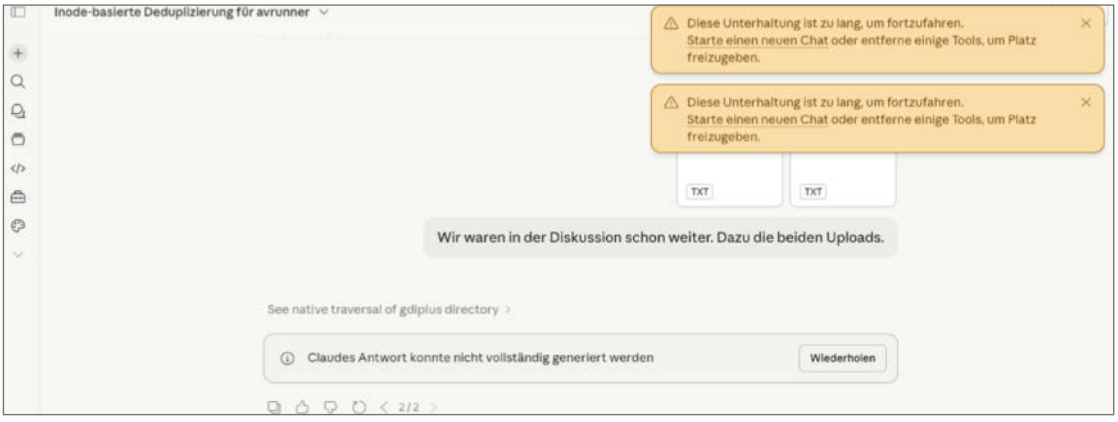
Aus jedem Winkel lachen ihn Framework-Fremdgänger an: Ein Hilfsprogramm zum Zählen von Dateizugriffen zerpflückt Optionen zu Fuß, anstatt `getopt()` zu verwenden. Er findet überall Fragmente, wo AV-Runner statt KDE-Funktionen solche von Qt verwendet und umgekehrt – hier müsste aus seiner Sicht eine Entscheidung gefällt werden. Den Aufruf externer Programme wie `find` würde er durch Funktionen des Frameworks ersetzen, um sich das fehleranfällige Parsen der Ausgaben und die Fehlerbehandlung hängengebliebener Prozesse zu sparen.

Mit seiner Empfehlung, der KI stilistisch und hinsichtlich der zu bevorzugenden Frameworks sehr konkrete Vorschriften zu machen, trifft er einen wunden Punkt: Das Projekt begann sein Leben als Prototyp und es gab Vorgaben, was die Funktionalität und Architektur betrifft, nicht aber zu den kritisierten Punkten. Claude hat zwar an mancher Stelle nachgefragt, mit welcher Technik er fortfahren soll – aber dazu gab es nur grobe Abstimmungen, etwa, dass ein Teilprojekt rein in C/C++ ohne Framework realisiert werden soll.

Schwache Seiten

Zu den anfänglichen Zweifeln, der Euphorie über große Fortschritte und den Bedenken erfahrener Programmierer gesellt sich irgendwann Ernüchterung. Claude wirkt blutdrucksteigernd, wenn er über eine Änderung räsoniert. Dann erinnert er an einen verwirrten Entwickler, der sich in einem komplizierten Gedankengeflecht verheddert hat und das wie ein Kleinkind ausplappert.

Den Claude-Chat kann man nicht unterbrechen, wenn er „denkt“, das muss man aushalten (Claude Code kennt einen Hotkey, um die KI abzuwürgen). Spätestens, wenn Claude den nächsten Auftrag erfragt, wird es Zeit, den Helfer aufzufordern, einen Schritt zurückzutreten und idealerweise mit inhalt-



Chats währen nicht ewig: Idealerweise startet man einen frischen Chat, bevor Claude die Puste ausgeht, weil der Kontext vollgelaufen ist.



Wenn der Kontext zu groß wird, fasst Claude den Gesprächsverlauf zusammen.

lichem Input für eine konstruktive Wende zu sorgen. Früher oder später werden Sie sich dabei erwischen, die KI zu beschimpfen, weil sie Mist verzapft. Denken Sie über die Anschaffung eines Sandsacks samt Boxhandschuhen nach.

Gerade weil Claude viel von der Fleißarbeit erledigt, braucht man hohe Aufmerksamkeit beim Testen der Ergebnisse. Das A und O ist aus meiner Sicht nicht, jede Codezeile zu prüfen, sondern vor allem die Gesamtzusammenhänge immer vor dem inneren Auge zu halten und Claudes Antworten daraufhin zu prüfen. Die Antworten fallen selbstsicher aus und schrauben trotzdem manchmal Mumpitz zusammen: Der Wunsch, bestimmte Fehler zusätzlich zu loggen, kann dazu führen, dass plötzlich jeder Furz auf stderr das Protokoll überschwemmt. Wer so etwas nicht gleich merkt, verschwendet mindestens die Zeit für einen weiteren Testzyklus.

Es lohnt sich, Dinge, die im Zusammenhang mit der gerade ausgeführten Aufgabe stehen, diszipliniert gleich zu testen und gegebenenfalls reparieren zu lassen. Der Chat hat dazu gerade den passenden Kontext. Wenn ein nervöser Nutzer von Chatnachricht zu Chatnachricht das Thema wechselt, etwa weil im Hintergrund das Erstellen der Testartefakte auf sich warten lässt, bezahlt er das mit abnehmender Antwortqualität.

KI braucht Schonung, wie der Kollege nebenan, der auch nicht ständig aus seiner Aufgabe herausgerissen werden möchte. Die technische Erklärung ist der Kontext, also der Inhalt der bisherigen Konversation, der mit jeder Anfrage an die KI geschickt wird – gewissermaßen das Kurzzeitgedächtnis des künstlichen Kollegen. Weicht man zwischendurch zu oft von der eigentlichen Aufgabe ab, fällt ihm das „Denken“ zunehmend schwerer.

Bei länger und länger werdenden Chats, bei denen die Qualität anhält, verschafft sich Claude Luft, indem er sie zwischendurch komprimiert. Dann wird der bisher Chatverlauf gegen eine eingekürzte Zusammenfassung ersetzt, weil das Kontextfenster eine bestimmte Größe nicht übersteigen darf. Bei Opus 4.7 passen immerhin eine Million Token rein, das entspricht Hunderten c’t-Seiten.

Das Einkürzen geschieht mitten in einer Ausarbeitung und manchmal hat man den Eindruck, dass Claude einen Filmriss hatte, weil er längst schon Erledigtes noch einmal versucht, nur um festzustellen, dass es bereits passiert ist. Meist fängt er sich, mitunter erst nach Knopfdruck des Chatpartners. Mein Eindruck ist, dass diese Aussetzer immer besser verarbeitet werden.

Im Grunde gehorcht das Coden mit Claude dem Prinzip „Führen durch Fragen“. Aber nach meinem Gefühl hat Anthropic mit dem Wechsel von Opus 4.6 auf Opus 4.7 den Spieß umgedreht: Ich war anfangs so genervt von den vielen Rückfragen, dass ich bei manchen Aufgaben auf Opus 4.6 zurückgeschaltet habe – Anfangs hatte mich bei dem Modell noch gestört, dass es nach anfänglicher Beratung zu schnell loskodiert, und ich musste immer wieder darum bitten, erst mal zu planen. Eine neue Modellversion ist wie ein neuer Kollege.

Claude ist vergesslich. Das gilt besonders für die Dat(ei)en, die in einem Chat erarbeitet worden sind. Er bewahrt sie eine Weile auf, aber nicht ewig. Ähnlich intransparent wie der Token-Verbrauch im Chat ist auch das. Während der intensiven Nutzung geschah es mehrfach, dass Claude das Git-Repository, an dem er vor wenigen Tagen noch gearbeitet hatte, nicht mehr erreichen konnte und einen Upload desselben erbat. Häufiger geschieht das, wenn in der Infrastruktur bei Anthropic mal wieder Server umgekippt sind.

Blick nach vorn

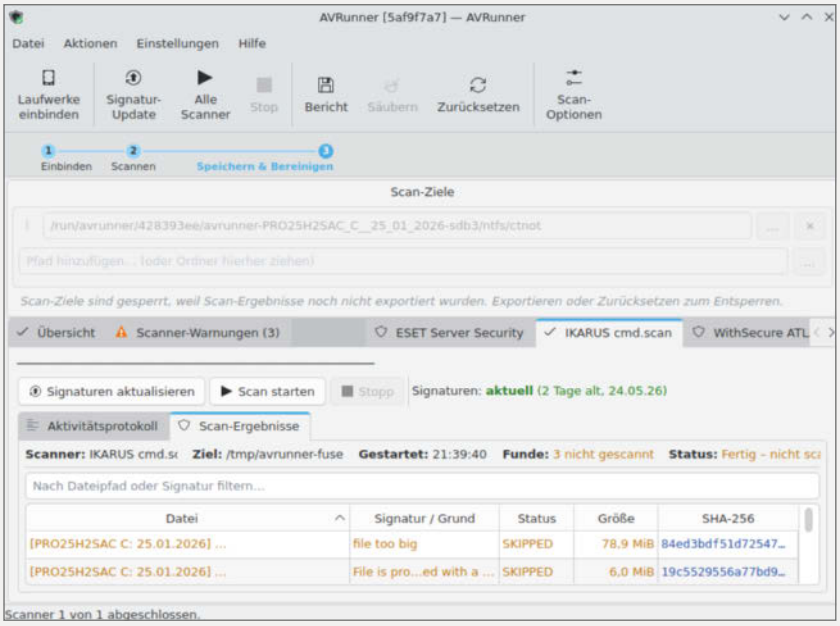
Streckenweise kommen Zweifel auf, ob wirklich eine Maschine am anderen Ende des Chatfensters die Nachrichten generiert und nicht eine fleißige Schar von vermutlich nicht ordentlich bezahlten Entwicklern irgendwo auf der Welt. Mitunter macht Claude Fehler und führt dabei sogar Gespräche mit sich selbst – zum Mitlesen. Da erhascht man dann den Blick darauf, dass `sed`-Befehle den Code bearbeiten sollen und straucheln, weil sie eine schließende Klammer an die falsche Stelle schreiben. Claude beschließt dann, andere Bearbeitungsoptionen einzusetzen. Welche verrät er nicht immer.

AVRunner im nächsten Desinfec’t

Die Anwendung AVRunner soll in der nächsten Version unseres Antiviren-Systems eine zentrale Rolle spielen. Sie wird Windows-Partitionen einbinden helfen sowie die Scanner steuern und deren Ergebnisse aufbereiten. Die Tabelle fasst einige Eckdaten des Projekts zusammen, das ohne KI-Hilfe niemals in diesem Zeitrahmen entstanden wäre. Was die Zahlen nicht wiedergeben: der Zeitaufwand für die Tüfteleien, die hinter so einem Projekt stehen und auf die wir im Rahmen der Veröffentlichung in c’t 16/2026 noch detaillierter eingehen wollen.

Projektmetriken

Dauer	2,5 Monate
C++-Zeilen	ca. 25.000
C++-Dateien	44
Header-Dateien	53
Klassen mit Qt-Code	36
i18n-Strings	516
Anzahl Commits	854
davon Fixes	54 %
davon neue Features	22 %
davon Refaktorierungen	5 %



Das typische Herauspuzzeln von Problemlösungen kann die KI viel besser als ein Mensch. Egal, ob ich im Lauf des Projekts Claude zu NTFS-Eigenarten befragt habe, ihm auftrug, langweiligen Code zu schreiben, um XML-Konfigurationen aus Kommandozeilenparametern zusammenzubauen und anzuwenden, oder ihn mit umfangreichen mit `bpftrace` erzeugten Log-Daten beworfen habe, meist brachte mich das um Größenordnungen schneller voran, als ich das allein hätte bewerkstelligen können.

Hierin liegt eine Gefahr: Dank des schnellen Vorankommens fühlt sich die KI wie eine Superkraft an. Erfolgserlebnisse, die früher manchmal Tage auf sich warten ließen, treten viel schneller ein und damit häufiger auf. Das Spaßniveau bleibt hoch. Das Aufhören fällt schwer. Fast wie Inspektor Columbo hat man nach einem langen Tag noch mindestens eine Frage, die man unbedingt stellen möchte – der Überraschungseffekt ist dabei aufseiten der KI: Mich hat Claude nicht nur einmal gefragt, ob es denn für heute nicht genug sei …

Dieses Menscheln der KI spricht den Nutzer auf subtile Weise an, obwohl heute fast jeder weiß, dass hier im Wesentlichen Statistik am Werk ist. Mich beschleicht mitunter das Gefühl, eine Büchse geöffnet zu haben, die ich nie wieder zubekomme. Vielleicht habe ich zu viele Jahre meines Arbeitslebens aus heutiger Sicht darauf verschwendet, Dinge zu erforschen, die Claude binnen Sekunden zu tun vermag. Andererseits: Ohne den Menschen als Filter macht die KI keinen Meter. (ps) c't

Vorschau c't Lokale KI

Ab dem 18. Dezember im Handel und auf shop.heise.de

Mehr Datenschutz mit der eigenen KI

Große Sprachmodelle helfen beim Schreiben, Programmieren und bei Alltagsarbeit und Anbieter wie Anthropic, OpenAI und Google gewöhnen Nutzer mit Einsteiger-Abomodellen an KI-Nutzung aus der Cloud. Die Probleme dieses Geschäftsmodells liegen auf der Hand: Einerseits fließen alle verarbeiteten Daten an die Betreiber, andererseits muss man als Kunde alle Preiserhöhungen erdulden.
Die Alternative: KI-Modelle auf der eigenen Hardware betreiben. Das Internet ist mittlerweile voll von kostenlos verfügbaren Modellen, die man herunterladen und selbst betreiben kann.

Doch lokale KI entwickelt sich rasant weiter, regelmäßig erscheinen neue Anwendungen, Modelle und bahnbrechende Ansätze – für Einsteiger nicht zu durchschauen.
Das Sonderheft Lokale KI liefert einen kompakten Einstieg ins Thema: von der passenden Hardware über empfehlenswerte Software bis hin zu Praxistipps, um mehr Token pro Zeit auf der eigenen Grafikkarte zu berechnen.

Weitere c't Sonderhefte: heise.de/s/00MxL

Themenschwerpunkte

Was Sie für den Einstieg wissen müssen

- Software für lokale KI
- Große KIs ohne High-End-Hardware betreiben

Die beste Software auswählen

- Lokale KI-Modelle mit aktuellen Fakten aus dem Internet anreichern
- Home Assistant und KI: Was der Home Generative Agent wirklich kann

KI-Hardware: von Raspi bis High-End-Workstation

- AMD Lemonade NPU
- Workstation mit viermal Intel Arc Pro B70







Videokurse für IT-Professionals jetzt entdecken: > heise-academy.de

Make:



Dann bist du bei uns genau richtig!

Jetzt bestellen:
make-magazin.de/miniabo

Für nur 19,90 €
statt 29 €

Make im Abo lesen und sparen:

- ✓ 2 Ausgaben als **Heft** und
- ✓ **Digital** im Browser, als PDF und in der App
- ✓ Zugriff auf das **Online-Artikel-Archiv**
- ✓ **Inkl. Geschenk** z. B. Make: Tasse

leserservice@make-magazin.de

0511/592 99 077


heise academy
Immer einen Skill weiter:
heise academy
Die IT verändert sich ständig – und mit ihr deine Chancen. Wir entwickeln deine IT-Skills weiter – mit praxisnaher Weiterbildung, die heute wirkt und morgen trägt. Für Menschen und Teams, die Technologie nicht nur nutzen, sondern verstehen und vorantreiben wollen. Entdecke Live-Trainings und On-Demand-Inhalte, die dich wirklich weiterbringen.
> IT-Weiterbildung entdecken unter heise-academy.de