



Schädlingsjäger

Virensuche mit dem c't-Notfall-Windows 2026

Zentrale Aufgabe unseres Notfallsystems ist die Jagd nach Schädlingen. Erledigt wird sie von gleich fünf Virenscannern und zwei Schnelltests.

Von Axel Vahldiek

Wenn Windows von einem Schädling befallen wurde, gilt der Patient der reinen Lehre zufolge als tot: Setzen Sie das Betriebssystem komplett neu auf und installieren Sie alle Anwendungen erneut. Wer gut vorbereitet ist, spielt einfach ein Image der Installation zurück, das erstellt wurde, als sie noch als sauber galt. Doch selbst wenn Sie ein solches Image haben, sieht es bei Freunden und Verwandten oft anders aus. Und gemäß der reinen Lehre ist dann eine Neuinstallation fällig. Denn selbst wenn Sie alle internen Datenträger noch so gründlich prüfen und reinigen, bleibt doch ein

Restrisiko, dass vom Schädling etwas übrig bleibt.

In solchen Fällen schlägt die Stunde unseres Rettungssystems. Im Vergleich zu Desinfec't hat das c't-Notfall-Windows einen gewichtigen Vorteil: Windows-Nutzer brauchen sich im Ernstfall nicht auch noch mit einem neuen Betriebssystem vertraut zu machen. Damit durchsuchen Sie die Installation gründlich nach Schadsoftware. Bestätigt sich dabei der Virenverdacht, wissen Sie, dass eine Neuinstallation tatsächlich angebracht ist. Dritten gegenüber mag diese Bestätigung als Argumentationshilfe dienen. Für jene Fälle,

in denen eine Neuinstallation partout nicht infrage kommt, bieten die Werkzeuge des Notfall-Windows das Entfernen der Schadsoftware an. Eine Garantie dafür, dass das klappt, gibt es zwar nicht, aber falls die Reinigungsversuche scheitern, haben Sie noch ein Argument mehr für die Neuinstallation.

Die Suchprogramme, die nach dem Booten des Notfallsystems vom Stick starten, können vom Virus auf der SSD/Festplatte nicht befallen werden. Denn er läuft ja in diesem Moment nicht, sondern liegt einfach nur als inaktiver Datenhaufen auf dem Datenträger.

Eines aber ist und bleibt lästig an der Suche nach Viren: Weil die Scanner dabei viele Gigabyte an Daten gründlich durchforsten müssen, können die Suchläufe dauern und zwar je nach Leistungsfähigkeit der Hardware durchaus viele Stunden. Eine Abkürzung können unsere Schnelltests bieten: Damit erfahren Sie zwar nicht, ob die gesamte Installation sauber ist. Es stellt sich aber vielleicht ruckzuck heraus, dass tatsächlich ein Schädling vorhanden ist. Dann wissen Sie, dass die gründlichen Suchläufe lohnen.

Weil bei einem Virenbefall schon genug Alarm im Oberstübchen herrscht, liefern wir für alle in diesem Betrag erwähnten Werkzeuge zur Virensuche wieder unsere bewährten Schritt-für-Schritt-Anleitungen. Falls Ihnen die bekannt vorkommen, täuschen Sie sich nicht, denn sie basieren auf den Texten der vorangegangenen Version. Wir haben sie für die aktuelle Ausgabe gründlich überprüft und überarbeitet. Verwenden Sie also nur die aktuellen Versionen.

Schnelltests

Vorab noch ein paar Details zu den Schnelltests. Der erste steckt im Sysinternals-Programm „Autoruns“ (Einführung in [1]). Es kann alle Autostart-Einträge der Windows-Installation durchforsten und die gefundenen Programme auf einen Schlag von über 70 Scannern prüfen lassen. Das gelingt im Idealfall sogar rasend schnell, denn Autoruns lädt dazu Hashes der ausführbaren Dateien bei [VirusTotal.com](https://www.virustotal.com) hoch. Das ist ein von Google betriebener Dienst. Nur bei dort unbekannten Hashes ist der Upload der zu prüfenden Datei selbst erforderlich.

Auch beliebige einzelne Dateien können Sie mit dem Notfall-Windows einem Schnelltest unterziehen. Klicken Sie dazu im Kontextmenü einer verdächtigen Datei

auf „Senden an/Sigcheck“. Sigcheck ist ebenfalls ein Programm von Sysinternals. Es prüft erstens die Signatur der Datei, bildet zweitens diverse Prüfsummen (MD5, SHA1, SHA256 ...) und lädt drittens ebenfalls einen Hash bei VirusTotal hoch. Das Ergebnis erscheint in einer zwar hässlichen, aber funktionalen Eingabeaufforderung.

Was die Interpretation der Ergebnisse betrifft, gilt für beide Schnelltests im Wesentlichen dasselbe wie bei einer Ampel: Zeigt sie Rot, sollten Sie auf jeden Fall stehen bleiben, doch bei Grün können Sie trotzdem überfahren werden. Anders formuliert: Sofern eine Datei von einem bekannten Anbieter signiert ist und kein Virens Scanner etwas zu meckern hat, ist sie wahrscheinlich harmlos – obwohl es eben keine Garantie gibt. Wenn hingegen die Signatur fehlt oder Seltsamkeiten aufweist, sollten Sie vorsichtig sein.

Beachten Sie: Microsoft hat entschieden, dass zwar so ziemlich alle Windows-eigenen ausführbaren Dateien signiert sind, die Signaturen aber nicht in den Dateien selbst stecken (sondern tief unterhalb des Windows-Ordners versteckt sind). Als Folge erscheinen viele Windows-eigene Dateien unter dem Notfall-Windows als nicht signiert. Das ist normal und erst mal kein Grund zur Sorge. Dasselbe passiert übrigens auch, wenn Sie von einer Parallelinstallation ausgehend die Signatur prüfen.

Vorbereitungen

1. Falls im normalen Betrieb auch nur der geringste Verdacht auf einen Erpressungstrojaner aufkommt: Rechner so-

fort hart ausschalten! Anschließend Notfall-Windows booten und alles an Daten retten, was noch unverschlüsselt ist.

2. Sonst das auf der Platte installierte Windows laufen lassen, aber alle Netzwerkverbindungen kappen.
3. Explorer öffnen, im Kontextmenü der Windows-Partition (üblicherweise C:) „Eigenschaften“ auswählen, auf „Bereinigen“ klicken, um die Datenträgerbereinigung zu starten. Dort „Systemdateien bereinigen“ anklicken, Nachfrage bestätigen, alle Häkchen setzen, Nachfragen bestätigen.
4. Browser-Cache leeren. Firefox: „Einstellungen/Datenschutz und Sicherheit/Chronik löschen“. Edge: im Dreipunkte-Menü klicken auf „Einstellungen/Datenschutz, Suche und Dienste/Browserdaten löschen/Zeitbereich „Gesamte Zeit““. Chrome: Strg+Umschalt+Entf drücken, den „Zeitraum“ auf „Gesamte Zeit“ umstellen, „Daten löschen“ anklicken.
5. Im Mailclient Papierkorb und Spam-Ordner leeren.

Schnelltest mit Autoruns

1. Notfall-Windows booten, Netzwerkverbindung herstellen, Windows-Partition auf der Festplatte identifizieren, bei Bedarf BitLocker entsperren.
2. Aus dem Startmenü „Autoruns“ aufrufen.
3. Den initialen System-Scan von Autoruns bei Eile durch Drücken der Esc-Taste abbrechen.
4. In der Menüleiste unter „Options“ auf „Scan Options“ klicken. Häkchen vor

```
X:\windows\system32\cmd.exe
C:\>sigcheck -v X:\users\default\downloads\eicar.com:
Verified: Unsigned
File date: 12:05 08.12.2025
Publisher: n/a
Company: n/a
Description: n/a
Product: n/a
Prod version: n/a
File version: n/a
MachineType: n/a
MD5: 44D88612FEA8A8F36DE82E1278ABB02F
SHA1: 3395856CE81F2B7382DEE72602F798B642F14140
PESH1: 3395856CE81F2B7382DEE72602F798B642F14140
PE256: 275A021B8FB6489E54D471899F7D89D1663FC695EC2FE2A2C4538AABF651FD0F
SHA256: 275A021B8FB6489E54D471899F7D89D1663FC695EC2FE2A2C4538AABF651FD0F
IMP: n/a
VT detection: 65/77
VT link: https://www.virustotal.com/gui/file/275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f/detection
Drücken Sie eine beliebige Taste . . .
```

SigCheck sieht bescheiden aus, prüft aber eine Datei auf einen Schlag mit über 70 Virenscannern, hier beispielhaft mit der harmlosen Testdatei Eicar.

„Check VirusTotal.com“ setzen. Auf „Rescan“ klicken.

5. In der Menüleiste auf „File“ und „Analyze Offline System“ klicken. Im Dialog hinter „System Root“ den Pfad zum Windows-Ordner eintragen (üblicherweise C:\Windows), hinter „User Profile“ den Pfad des Nutzerprofils (C:\Users\<Kontoname>).
6. Nach dem Scan in der Spalte „Virus Total“ nachschauen (Anzeige dazu eventuell nach rechts scrollen): Steht hier hinter einem Autostart-Eintrag „0/77“, hat kein Scanner etwas gefunden.

Die Zahl hinter dem Schrägstrich ist die Anzahl der prüfenden Scanner und variiert, entscheidend ist die Zahl vor dem Schrägstrich. Steht hier eine andere Zahl als 0, kommt es drauf an: Ist es nur eine 1, handelt es sich vermutlich um einen Fehlalarm, bei 2 oder 3 womöglich auch. Spätestens bei höheren Zahlen ist eine gründliche Recherche angebracht.

7. Sollten auf dem PC verschiedene Nutzerkonten verwendet werden, Vorgang mit deren Nutzerprofilen wiederholen.
8. Bei Windows-Parallelinstallationen bitte beachten: Jede Windows-Installation muss vom Notfall-Windows mit dem Laufwerksbuchstaben eingebunden sein, den sie selbst zu haben glaubt. Wenn sich also beide Installationen jeweils auf C: wöhnen, wird sie das Notfall-Windows trotzdem als C: und D: einbinden, und dann müssen Sie vor der Prüfung von D: mit Autoruns die Buchstaben D: und C: in der Datenträgerverwaltung tauschen [2]. Sonst zeigt Autoruns falsche Ergebnisse.

Virenschnelltest mit Sigcheck

1. Notfall-Windows booten, Netzwerkverbindung herstellen, Windows-Partition auf der Festplatte identifizieren.
2. Im Explorer verdächtige Datei auswählen, in ihrem Kontextmenü auf „Senden an“ und „Sigcheck“ klicken. Die Ausgabe erscheint in einer Eingabeaufforderung.
3. Zeile „Verified“ prüfen: „Signed“ deutet auf Vertrauenswürdigkeit hin. Alles andere ist ein Alarmsignal, vor allem wenn die Datei angeblich von einer großen Firma wie Microsoft oder Google stammt. Das gilt für „Unsigned“ ebenso wie für eine vorhandene, aber als nicht vertrauenswürdig eingestufte Signatur (beispielsweise: „Die digitale

Signatur des Objekts konnte nicht bestätigt werden“, „Ein Zertifikat wurde explizit durch den Aussteller gesperrt“ oder „Eine Zertifikatskette zu einer vertrauenswürdigen Stammzertifizierungsstelle konnte nicht aufgebaut werden“).

4. Steht ziemlich weit unten in der Zeile „VT detection“ als Ergebnis „0/77“, hat keiner der auf VirusTotal versammelten Scanner etwas Verdächtiges gefunden. Die Zahl hinter dem Schrägstrich ist die Anzahl der beteiligten Scanner und variiert, entscheidend ist die Zahl vor dem Schrägstrich. Der Link zur Ergebnisseite der Prüfung steht eine Zeile tiefer. Sie können ihn wie gewohnt mit der Maus markieren, per Strg+C in die Zwischenablage kopieren und in Firefox in die Adresszeile einfügen.

Virensuche mit ...

1. Notfall-Windows booten, Windows-Partition auf der Festplatte identifizieren.
2. Wichtig: Vor dem Start eines Scanners Netzwerkverbindung herstellen.
3. Scanner **nacheinander** laufen lassen (siehe folgende Anleitungen). Die Reihenfolge ist egal. Vor jedem weiteren Suchlauf das Notfallsystem neu starten und wieder bei der Anleitung „Virensuche ...“ beginnen.

... Defender Offline

1. Der Defender kann nur 64-Bit-Windows-Installationen prüfen. Falls bei Ihnen ein 32-Bit-Windows installiert ist: weiter beim nächsten Scanner. Dasselbe gilt, wenn Microsofts Virens Scanner Fehlermeldungen auswirft (er verwendet Systemdateien von C:, was nicht immer klappt).

2. Aus dem Startmenü „Defender“ aufrufen. Das Programm beginnt sofort mit der Virensuche, brechen Sie diese durch einen Klick auf „Cancel scan“ ab.
3. Im Reiter „Update“ auf „Update definitions“ klicken. Warten, bis die frischen Virendefinitionen geladen sind.
4. Im Reiter „Home“ unter „Scan Options“ „Custom“ auswählen, auf „Scan now“ klicken.
5. Laufwerke auswählen, auf „OK“ klicken, die Virensuche beginnt.

... Emsisoft Emergency Kit

1. Aus dem Startmenü „Emsisoft“ aufrufen.
2. Update abwarten.
3. Lizenzvereinbarung annehmen.
4. Updates laden automatisch, sonst auf den Link „Jetzt aktualisieren“ klicken
5. Im Feld „Scannen“ auf „Eigener Scan“ klicken.
6. Die Laufwerke des Notfall-Windows (B:, X: und Y:) durch Klick auf das rote Kreuz daneben aus der Auswahl entfernen.
7. Optionen unter „Scan-Einstellungen“ nach Wunsch aktivieren.
8. Auf „Weiter“ klicken (dazu je nach Display-Auflösung erst etwas nach unten scrollen). Das Programm überprüft nun die Laufwerke.

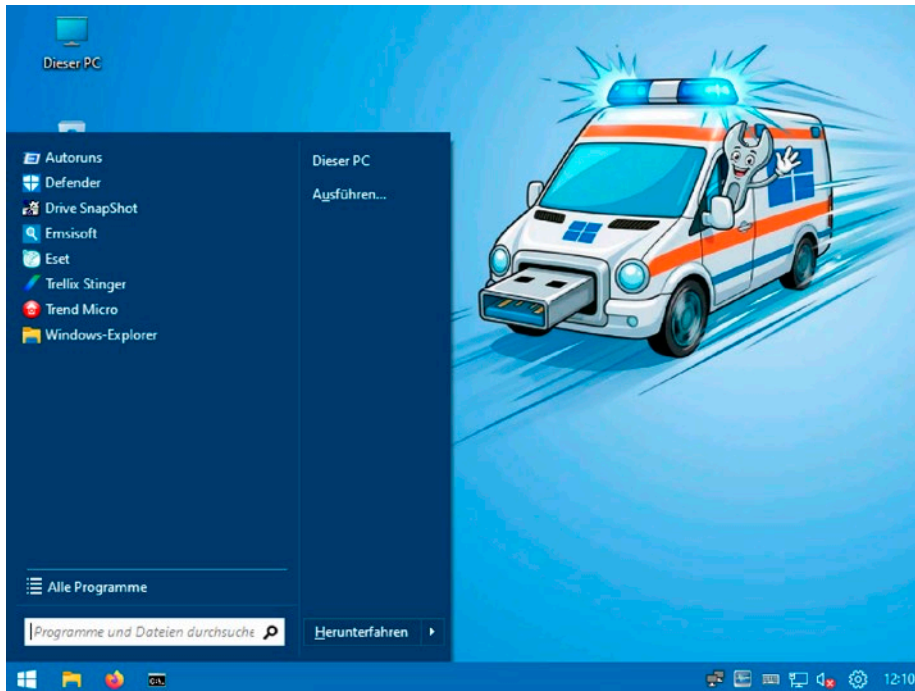
... Eset Online Scanner

1. Nach dem Start des Notfall-Windows einige Sekunden warten. Dann aus dem Startmenü „Eset“ aufrufen, auf „Erste Schritte“ klicken, Nutzungsbedingungen akzeptieren.
2. Falls die Software jetzt eine neue Produktversion herunterlädt und sich dann beendet: Wie sich die künftige Version verhalten wird, lässt sich nicht

Signatur-Update abkürzen

Beim Bauen landen aktuelle Signaturen für den Windows Defender und Emsisoft im Notfallsystem – die übrigen Scanner beziehen diese erst beim Start über eine bestehende Internetverbindung. Wenn Sie mit dem c't-Notfall-Windows offline arbeiten, also ohne Internet, helfen nur die erstgenannten Scanner.

Damit Sie zum Aktualisieren der Signaturen nicht den Bauvorgang erneut starten müssen, haben wir eine Abkürzung vorgesehen: In PEBakery finden Sie im Projektbaum unter Extras das Skript „Signatur-Aktualisierung“. Es erledigt alle nötigen Schritte. Das funktioniert, solange Sie die Dateien des letzten erfolgreichen Bauablaufs nicht gelöscht haben. (ps@ct.de)



Defender, Emsisoft, Eset, Trellix Stinger und Trend Micro: Gleich fünf Virens Scanner finden Sie im Startmenü des Notfallsystems.

vorhersagen, aber falls es wie bisher läuft, starten Sie das Programm einfach erneut und entfernen das Häkchen vor „Neueste Produktversion herunterladen“.

3. Im Dialog „Bevor wir beginnen“ nach Wunsch entscheiden.
4. „Benutzerdefinierter Scan“ anklicken, Laufwerke auswählen und dann auf „Speichern und Fortfahren“ klicken.
5. Über Quarantäne von potenziell unerwünschten Anwendungen entscheiden (Vorsicht, alle Dateien in der Quarantäne liegen in der RAM-Disk, gehen also beim Beenden des Notfall-Windows verloren!). Unten links auf den blauen Link „Erweiterte Einstellungen“ klicken, Einstellungen prüfen, auf den Zurück-Knopf oben klicken.
6. Auf „Prüfung starten“ klicken. Frische Virensignaturen werden heruntergeladen, die Virensuche beginnt.

... Trellix Stinger

1. Aus dem Startmenü „Trellix Stinger“ aufrufen. Nutzungsbedingungen akzeptieren. Programm aktualisiert sich.
2. Oben rechts auf „Advanced“ und dann auf „Settings“ klicken. Unterhalb von „Scan Targets“ und „Scan Options“ alles anhaken. Unterhalb von „On threat detection“ (Was tun bei Viren-

fund?) wählen: „Remove“ verschiebt in Quarantäne, „Report“ weist nur auf den Fund hin. Letzteres ist für eine weitere Analyse sinnvoll (siehe Schritt-für-Schritt-Anleitung „Virenfund“). Pull-down-Menü „GTI settings – Sensitivity“ auf „Very High“ ändern, also die höchste Heuristik-Stufe. „Save“ anklicken.

3. Unterhalb der Schaltfläche „Scan“ auf den Link „Customize my scan“ klicken. Laufwerke auswählen, „Scan“ anklicken, Virensuche startet.

... Trend Micro HouseCall

1. Aus dem Startmenü „Trend Micro“ aufrufen. Update abwarten. Im nächsten Dialog die Lizenzbestimmungen bestätigen („Accept and Continue“).
2. Auf den Link „Settings“ klicken. Im Reiter „Smart Feedback“ auf Wunsch das Häkchen vor „Turn on Trend Micro Smart Feedback“ entfernen, sonst schickt die Software Informationen zu Ihren Dateien an den Hersteller.
3. In den Settings im Reiter „Scan Type“ „Custom Scan“ auswählen, Häkchen vor den zu prüfenden Laufwerken setzen, mit „OK“ bestätigen.
4. Auf „Scan now“ klicken. Die Virensuche beginnt.

Virenfund

1. Vorab: Wenn Sie das Notfall-Windows selbst auf Viren untersuchen, werden die Scanner immer fündig. Hintergründe dazu finden Sie auf der Projektseite (ct.de/-11072902). Entscheiden Sie, ob die infizierten Dateien in Quarantäne geschoben, gelöscht oder ignoriert werden sollen. Obacht: Der Quarantäne-Ordner liegt auf der RAM-Disk, wird also beim Beenden des Notfall-Windows gelöscht!
2. Infizierte Datei für genauere Analyse mit Firefox bei VirusTotal.com hochladen. Den Link finden Sie auf der Startseite des Browsers.
3. Auf Wunsch: Infizierte Datei für weitere Recherche an einen sicheren Ort kopieren, am besten per kennwortgeschütztem Zip-Archiv, welches Sie mit 7-Zip erstellen (im Startmenü unter „Alle Programme/Utilities“).
4. Infizierte Datei löschen.

Nacharbeiten bei Virenfund

1. Noch unter dem Notfallsystem die Hosts-Datei kontrollieren (in C:\Windows\System32\Drivers\etc): per Rechtsklick mit Notepad öffnen, dann unbekannte Zeilen mit # auskommentieren oder löschen.
2. Auf 64-Bit-Systemen auch prüfen, ob es unter „C:\Windows\Syswow64\Drivers\etc“ eine weitere Datei namens „hosts“ gibt; die dann genauso behandeln.
3. Installiertes Windows starten.
4. Kontrollieren: Firewall, Virens Scanner, Plug-ins von Browser und Mail-Client, Proxy-Einstellungen von Windows, Browser und Mailclient.
5. Erst danach Netzwerkverbindung wieder herstellen.
6. Aktualisieren: Windows Update, Virens Scanner, Browser, Mailclient, PDF-Reader.
7. Falls aus historischen Gründen immer noch vorhanden: Löschen Sie Flash. Sofern Java verzichtbar ist: ebenfalls löschen.
8. Möglichst noch prüfen: Netzwerkfreigaben, Autostarts, laufende Prozesse. (axv@ct.de) **ct**

Literatur

- [1] Jan Schüßler, Startinspektion, Mit Autoruns prüfen, was mit Windows alles startet, c't 19/2018, S. 174
- [2] Axel Vahldiek, Plattenteiler, Partitionieren mit Windows-Bordmitteln - Teil 1: Datenträgerverwaltung, c't 2/2018, S. 154