Desinfec’t 2022

Die Fähigkeiten von Desinfec't 2022 im Überblick

Das kann Desinfec’t ..... **Seite 20**
Die Virenjäger schlagen zu ..... **Seite 24**

Bild: Andreas MArtini

Das Sicherheitstool der c't-Redaktion ist in einer neuen Fassung erschienen. Damit jagen Sie Windows-Trojaner und erlegen sie - auch Einsteiger schaffen das. Desinfec't kann aber noch viel mehr.

Von Dennis Schirrmacher

Sie haben einmal nicht aufgepasst, vorschnell einen verdächtigen Mailanhang geöffnet und der Virenscanner in Windows hat bereits Alarm geschlagen? Das System verhält sich seltsam oder verweigert gar den Start? Sie wollen einfach auf Nummer sicher gehen? Dann schlägt die Stunde von Desinfec't.

Das kann Desinfec't

Das Sicherheitstool bringt mehrere Virenscanner und weitere Komponenten mit, um verdächtigen Aktivitäten in Windows auf die Spur zu kommen. Das Besondere von Desinfec't ist, dass es sein eigenes Betriebssystem auf Linux-Basis mitbringt und direkt von einem USB-Stick oder einer DVD bootet.

Deshalb müssen Sie ein möglicherweise verseuchtes Windows zur Analyse nicht starten, was dem Trojaner die Gelegenheit geben würde, noch mehr Schaden anzurichten. Stattdessen schauen Sie mit Desinfec't aus einer sicheren Entfernung auf die inaktive Windows-Installation. Von dort können Sie sich in Ruhe einen Überblick verschaffen. Damit Windows-Nutzer sich in Desinfec't sofort zurechtfinden, orientiert sich seine Desktop-Umgebung am Aussehen des Microsoft-Betriebssystems. Außerdem haben wir Unnötiges aus dem Linux-System geworfen, damit nichts vom Einsatz als Sicherheitstool ablenkt. So starten Sie bereits nach kurzer Zeit den ersten Virenscan.

Wenn Windows gar nicht mehr startet, fungiert Desinfec't sogar als Notfallsystem und gewährt Ihnen Zugriff auf die eigenen Dateien. So bringen Sie etwa Fotos direkt auf dem Desinfec't-Stick oder auf einer USB-Festplatte in Sicherheit.

Start vorbereiten

Damit Desinfec't optimal läuft, sollten Sie es von einem USB-Stick starten. Nachdem Sie die ISO-Datei heruntergeladen haben, können Sie diese direkt unter Windows auf einem mindestens 16 GByte großen Stick installieren – das ist in wenigen Minuten erledigt. Im Anschluss müssen Sie dem Computer lediglich sagen, dass er statt von der Festplatte vom USB-Stick starten soll. Wie das alles funktioniert, beschreibt der Folgeartikel. Nur auf einem USB-Stick läuft Desinfec't zur Höchstform auf: Es startet nicht nur schneller und läuft flüssiger, sondern es merkt sich auch Daten wie aktualisierte Virensignaturen und in Sicherheit gebrachte persönliche Daten. Damit das System optimal läuft, sollte der PC über mindestens 4 GByte Arbeitsspeicher verfügen.

Wer das System hingegen auf eine DVD brennt und davon startet, muss die Virenscanner nach jedem Neustart aktualisieren, denn auf diesem Medium kann Desinfec't keine Daten speichern. Aus Sicherheitsgründen wird das System aber auch auf einem USB-Stick nach jedem Reboot, bis auf die Signaturen und geretteten Daten, in den Ausgangszustand zurückversetzt. So ist sichergestellt, dass sich kein Schädling einnisten kann. Windows-Trojaner können aber ohnehin nicht auf Desinfec't überspringen, da der Malware-Code unter Linux schlicht nicht läuft. Bislang ist uns auch kein Fall bekannt, in dem ein Linux-Trojaner das Sicherheitstool befallen hat.

Viren aufspüren

Für die Virenjagd bringt Desinfec't standardmäßig Virenscanner von ClamAV, Eset und WithSecure (ehemals F-Secure) mit. Profis können noch den Scanner Microsoft Defender nachinstallieren oder mit dem konfigurierbaren Open Threat Scanner (OTS) und Thor Scanner tiefer eintauchen, um hoch entwickelte Malware vom Schlage Emotet aufzuspüren.

Damit den Scannern keine aktuellen Schädlinge durchrutschen, sind kostenlose Signatur-Updates für ein Jahr inklusive. Starten Sie einen Virenscan, aktualisieren sich die Scanner bei einer aktiven Internetverbindung automatisch. Standardmäßig untersuchen die Virenjäger die gesamte Festplatte. Auf Wunsch scannen Sie ausgewählte Ordner auf Festplatten oder angeschlossene USB-Sticks. Dank integrierter Tools funktioniert das auch mit via Bitlocker und VeraCrypt verschlüsselten Datenträgern. Für einen ersten Überblick genügt es in der Regel, nur den voreingestellten Scanner von Eset auf die Windows-Installation loszulassen.

Damit auch Computerneulinge mit Desinfec't Trojaner beseitigen können, orientiert sich die Darstellung an Windows.

Wer sich überhaupt nicht mit Computern auskennt, wählt einfach den Easy-Scan-Modus. Hier startet der Scanner nach der automatischen Aktualisierung ohne Umschweife mit der Untersuchung und Sie müssen nichts weiter einstellen.

Trojaner einschätzen

Ist ein Scan beendet, öffnet sich automatisch die Ergebnisliste im integrierten Webbrowser Firefox. Die Datei mit den Ergebnissen landet auch auf dem USB-Stick, sodass Sie die Liste an einem anderen Computer analysieren können. In der Liste sehen Sie auf einen Blick, welcher Scanner eine Datei für einen Virus hält. Doch keine Panik: Nicht alle Funde sind in allen Fällen mit echten Trojanern gleichzusetzen. Fehlalarme sind durchaus an der Tagesordnung. Um das besser einschätzen zu können, bringt Desinfec't Hilfe mit. So laden Sie beispielsweise verdächtige Dateien direkt aus der Ergebnisliste zum kostenlosen Online-Analysedienst Virustotal hoch. Dort schauen 60 bis 70 Scanner auf die Datei und helfen bei der Einschätzung.

Wenn Sie das nicht weiterbringt oder wenn Sie mit der Bedienung von Desinfec't überfordert sind, rufen Sie einfach über den integrierten Fernwartungsclient TeamViewer den Familien-Admin zur Hilfe. Dann kann dieser die Kontrolle über den Problem-PC übernehmen und nach dem Rechten sehen. Dafür benötigen beide Parteien lediglich eine aktive Internetverbindung und den im Privatbereich kostenlos nutzbaren und in Desinfec't integrierten TeamViewer-Client. Die Gegenseite lädt den Client kostenlos herunter.

Viren beseitigen

Wenn sich der Verdacht erhärtet und alle Zeichen auf Trojaner stehen, hilft Desinfec't bei der Beseitigung. Im Anschluss ist der Schädling zwar noch da, aber Windows kann ihn nicht mehr ausführen. Das funktioniert mit wenigen Klicks und lässt sich bei Bedarf auch wieder rückgängig machen, etwa wenn doch mal eine legitime Datei außer Gefecht gesetzt wurde. Da Desinfec't standardmäßig nur lesend auf die Windows-Festplatte zugreift, ist es sehr unwahrscheinlich, dass das Tool etwas kaputt macht. Den Schreibzugriff muss man explizit aktivieren.

Doch eines muss jedem klar sein: Auch mit aktuellen Signaturen können die Scanner brandneue Schädlinge übersehen. Das Katz-und-Maus-Spiel zwischen Malware-Entwicklern und Herstellern von Anti-Viren-Software ist nach wie vor im Gange und es kommt immer wieder vor, dass sich Trojaner an Scannern vorbeischleichen. Außerdem kann Desinfec't keine von Schadcode manipulierte Systemeinstellungen reparieren. Vor allem Schädlinge wie Emotet richten nicht nur auf einzelnen Computern, sondern in ganzen Netzwerken flächendeckenden Schaden an.

Mit Desinfec't lassen Sie mehrere Virenscanner auf Windows los.

Absolute Sicherheit bekommen Sie in der Regel nur, wenn Sie das komplette System löschen und Windows neu installieren. Desinfec't ist kein Allheilmittel, sondern eher der wichtige erste Helfer in der Not, um sich einen Überblick zu verschaffen und wichtige Dateien zu retten.

Werkzeuge für Profis

Neben dem OTS und Thor Scanner bringt Desinfec't für Experten noch weitere Tools mit. Hier müssen Sie wirklich wissen, was Sie damit anstellen. Ansonsten könnte etwas in Windows kaputtgehen, und im schlimmsten Fall startet das System nicht mehr.

Doch wer weiß, was er tut, kann mit den Werkzeugen beispielsweise verloren geglaubte Daten retten. Das ist hilfreich, wenn man zum Beispiel aus Versehen die SD-Karte einer Digitalkamera gelöscht hat. Außerdem ist es möglich, ganze Festplatten zu klonen und so etwa eine Windows-Installation auf eine neue SSD umzuziehen. Außerdem greifen Sie auf die Windows-Registry zu und ändern Werte. Besonders an dieser Stelle gilt die vorangegangene Warnung: Hier operieren Sie quasi am offenen Patienten – nur erfahrene Windows-Chirurgen sollten zu diesen Werkzeugen greifen.

Probleme sind lösbar

Wenn Desinfec't nicht startet, Scanner sich nicht aktualisieren oder Sie andere Probleme mit dem System haben, gibt es Hilfe. Im folgenden Praxisartikel lesen Sie Tipps zur größten Hürde, dem Start des Sicherheitstools. So gibt es etwa alternative Startoptionen, um das System auf besonders aktueller Hardware zu booten. Unser offizielles Forum ist eine bewährte Anlaufstelle, um Probleme zu lösen. Dort sind zahlreiche Nutzer mit hilfreichen Tipps aktiv. In der Regel lassen sich viele Schwierigkeiten mit überschaubarem Zeitaufwand lösen. Doch auch wenn wir das System auf vielen Computern erfolgreich getestet haben, wird es immer PCs geben, auf denen es schlicht nicht startet.

In den ersten Wochen nach der Veröffentlichung von Desinfec't sind der Entwickler und die Redaktion im Forum aktiv (siehe ct.de/y8xc). Wenn alle Stricke reißen, können Sie uns auch direkt eine E-Mail schreiben. Hat sich ein Fehler in das System eingeschlichen, versuchen wir, diesen zügig zu beseitigen und ein Update zu veröffentlichen. Das sollte sich bei einer aktiven Internetverbindung automatisch installieren. *(des@ct.de)* **ct**

Desinfec't-Forum: ct.de/y8xc