Desinfec’t, reanimiert

Workaround startet Desinfec’t 2022 wieder auf Windows-PCs

Der Bootloader von Desinfec’t ist unter die Räder eines Windows-Updates gekommen, seit Mitte August startete das Sicherheitstool deswegen nicht mehr. Wir haben das Problem analysiert und zeigen, wie Sie es lösen.

Von Dennis Schirrmacher

Eigentlich ist die Sicherheitsfunktion UEFI Secure Boot eine gute Sache. Sie verhindert durch Überprüfungen, dass Computer manipulierte Betriebssysteme starten. Das ist besonders gefährlich, weil sich Angreifer so von Nutzern unbemerkt tief in PCs verankern und Schindluder treiben können. Um mit Schadcode präparierte Systeme vor dem Start zu enttarnen, prüft Secure Boot die Signatur von jedem Bootloader. Ist er nicht von Microsoft signiert, verweigert der Computer den Systemstart.

Das Problem

Microsoft hat kürzlich ein Windows-Sicherheitsupdate (9. August 2022 KB5012170) veröffentlicht, um Secure Boot sicherer zu machen [1]. In den Standardeinstellungen installiert sich der Patch automatisch und spielt eine sogenannte Revocation List ins UEFI-BIOS, die diverse Bootloader mit bekannten Sicherheitslücken sperrt. Darunter befindet sich auch der Bootloader von Ubuntu 20.04 LTS, den Desinfec’t nutzt. Seitdem startet das Sicherheitstool auf Computern mit aktiviertem Secure Boot nicht mehr.

Wer seinen PC damit scannen will, müsste die Funktion für den Start von Desinfec’t temporär deaktivieren. Aus Sicherheitsgründen sollte man das aber nicht tun. Außerdem könnte das zu Problemen mit via Bitlocker verschlüsselten Festplatten führen und Sie könnten sich im schlimmsten Fall vom Zugriff auf Ihre eigenen Daten aussperren. Die Deinstallation des Updates hilft in diesem Fall übrigens nicht, da die Revocation List im Flash-Speicher des Motherboards liegt.

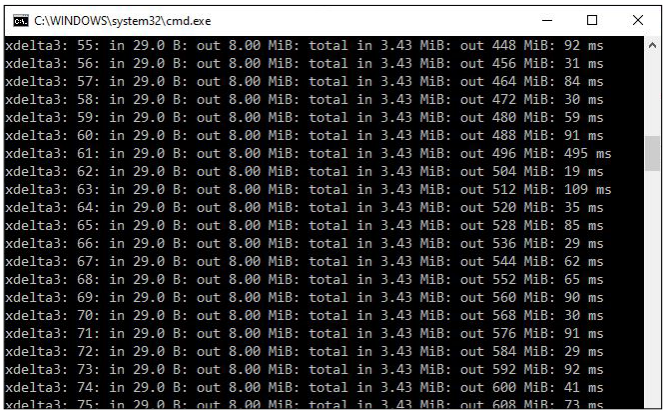
Ende August machte uns ein Thread im offiziellen Desinfec’t-Forum auf das Problem aufmerksam und wir setzten unseren Entwickler darauf an. Die Lösung war schnell klar: Der Bootloader muss getauscht werden. Doch das ist leichter gesagt als getan.

Das liegt am komplexen Aufbau eines Desinfec’t-Sticks. Er besteht aus mehreren Partitionen, darunter die System-Partition, die sich nach jedem Neustart aus Sicherheitsgründen in den Ausgangszustand zurückversetzt, und eine Partition für aktualisierte Virensignaturen, die dauerhaft gespeichert werden. Ganz am Anfang des Sticks befindet sich das ISO mit dem inkompatiblen Bootloader. An die Boot-Partition kommt man aber nicht ohne Weiteres dran. Da wir den aktualisierten Bootloader in der Dateistruktur bildlich gesprochen nur hinter dem inkompatiblen Bootloader platzieren konnten, klappte der Tausch auch nach mehreren Anläufen nicht. Aufgrund der beschriebenen Anordnung sah unser Test-PC beim Booten vom Stick stets den inkompatiblen Bootloader als Erstes, mit dem der Start weiterhin fehlschlug. Eine Reparatur bestehender Desinfec’t-Sticks ist also nicht möglich.

Mit dieser Erkenntnis entschieden wir uns dazu, die ISO-Datei von Desinfec’t 2022 zu überarbeiten; die neue Version steht inzwischen zum Download bereit (siehe Seite 53). Erstellen Sie damit einen

neuen Stick, startet Desinfec't 2022 wieder mit aktiviertem Secure Boot.

Im Folgenden zeigen wir auf, wie der Patchvorgang funktioniert. Wer die alte ISO-Datei noch auf der Festplatte gespeichert hat und sich den 4 GByte umfassenden Download des aktualisierten ISO-Image sparen möchte, kann das als Anleitung nutzen, um Desinfec't 2022 selbst mit dem kompatiblen Bootloader auszustatten und es auf einem USB-Stick zu installieren. Das im c't-Sonderheft enthaltene Desinfec't 2022/23 bringt den aktualisierten Bootloader übrigens ab Werk mit.



Das Tool Xdelta3 übernimmt den Patch-Prozess und bessert nur an den nötigen Stellen nach. Der Prozess dauerte bei uns mit einem USB-3.0-Stick nur rund eine halbe Minute.

Workaround unter Windows

Um loszulegen, benötigen Sie neben der alten ISO-Datei und einem USB-Stick, der an Ihren Rechner gesteckt ist, noch ein kleines Tool, das Sie direkt vom Server unseres Desinfec't-Entwicklers herunterladen können (ct.de/yfhp). Damit statten Sie das ISO-Image mit dem kompatiblen Bootloader Grub 2.06 aus Ubuntu 22.04.1 aus, sodass Desinfec't mit aktivem Secure Boot wieder startet. Der Workaround funktioniert unter Linux und Windows.

Binden Sie als Nächstes die alte ISO-Datei von Desinfec't 2022 als Laufwerk ein. Unter Windows 10/11 gelingt das in den Standardeinstellungen mit einem Doppelklick. An dieser Stelle kann aber ein DVD-Brennprogramm dazwischenfunken. In diesem Fall klicken Sie mit der rechten Maustaste auf die ISO-Datei und wählen die Option „Öffnen" oder „Öffnen mit/Windows Explorer". Hat das geklappt, kopieren Sie den kompletten Inhalt des virtuellen DVD-Laufwerks in einen neuen Ordner auf der Festplatte.

Im Anschluss laden Sie den Boot-Patch (siehe ct.de/yfhp) herunter. Entpacken Sie alle Dateien aus dem BootPatch-Archiv in den Ordner mit den Desinfec't-Dateien. Nun starten Sie den Patchprozess durch einen Doppelklick auf „BootPatch.bat". Erschrecken Sie nicht vor der auftauchenden Warnmeldung: Dabei handelt es sich um Windows Smart Screen. Das ist ein Cloud-basierter Schutzmechanismus, der Windows vor dem Ausführen unbekannter Dateien schützen soll. In diesem Fall ist es ein Fehlalarm. Über einen Klick auf „Weitere Informationen" können Sie die Option „Trotzdem ausführen" auswählen.

Nun beginnt der Patchvorgang, der die neue ISO-Datei „desinfect-202200-amd64-grub206.iso" mit aktualisiertem Bootloader erzeugt. Um den Prozess so effizient und den Patch so klein wie möglich zu halten, kommt das Befehlszeilenprogramm Xdelta3 zum Einsatz. Das Tool erstellt Differenzabbilder von zwei verschiedenen Versionen einer Binärdatei. Dafür analysiert es die alte ISO-Datei und verändert ausschließlich die Passagen, die den Bootloader betreffen. Die anderen Teile der Datei bleiben auch im neuen ISO-Image identisch. Das Befehlszeilenprogramm Xdelta3 macht diesen Prozess besonders effizient, und auch der Patch bleibt so klein, wie es geht.

Im Anschluss fragt ein Warnfenster der Benutzerkontensteuerung, ob Sie „Win32-DiskImager" öffnen wollen. Bestätigen Sie diese Abfrage, damit sich das Tool öffnet und die aktualisierte Version von Desinfec't 2022 auf dem angeschlossenen USB-Stick installieren kann. Dafür müssen Sie unter „Device" sicherstellen, dass der richtige Stick ausgewählt ist. Das erkennen Sie am Laufwerksbuchstaben. Klicken Sie auf „Write", wird der ausgewählte Datenträger ohne weitere Nachfrage überschrieben.

Ist der Schreibvorgang abgeschlossen, taucht der Stick unter Windows noch nicht auf. Das ist normal, keine Sorge. Nun müssen Sie den Computer vom Desinfec't-Stick starten. Im Desinfec't-Bootmenü wählen Sie einmalig den vorausgewählten Punk „in nativen Desinfec't-Stick umwandeln" aus. Erst dann halten Sie einen vollwertigen Desinfec't-Stick in der Hand, der auch Daten wie aktualisierte Virensignaturen speichert. Ohne die Umwandlung läuft Desinfec't im schreibgeschützten Modus und kann keine Daten speichern. Erst nach der Umwandlung taucht der Stick unter Windows auf und Sie können auf die Datenpartition zugreifen. Taucht der Punkt „in nativen Desinfec't-Stick umwandeln" nach der Konvertierung und einem Neustart noch mal im Desinfec't-Bootmenü auf, ignorieren Sie den Eintrag und starten Sie Desinfec't. Leider haben wir bislang keinen Weg gefunden, das abzustellen.

ISO-Patch unter Linux

Auch unter Linux kopieren Sie als Erstes den kompletten Inhalt vom ISO-Image von Desinfec't 2022 in einen neuen Ordner. Aus dem Archiv „BootPatch.zip" Entpacken Sie die Datei „BootPatch.sh" in den Ordner mit den Desinfec't-Dateien.

Nun rufen Sie das Terminal auf und installieren Xdelta3 via `sudo apt-get install xdelta3`. Jetzt wechseln Sie im Terminal in den zuvor erstellten Ordner und starten den Patchvorgang mit `bash BootPatch.sh`. Nun kopieren Sie das neue Image „desinfect-202200-amd64-grub206.iso" mit dem Befehl `dd if=desinfect-202200-amd64-grub206.iso of=/dev/sdx status=progress` auf einen USB-Stick. Sdx müssen Sie mit der Kennzeichnung Ihres Sticks anpassen. Alternativ können Sie auch ein Tool zum Schreiben von Imagedateien auf Sticks wie Etcher dafür nutzen. Das eignet sich vor allem für Linux-Einsteiger, da es eine grafische Oberfläche mitbringt und der USB-Stick vorausgewählt ist, sodass Sie nicht versehentlich eine Festplatte überschreiben.

Im Anschluss startet Desinfec't 2022 wieder problemlos auf PCs mit dem Windows Update und aktivem Secure Boot. So steht der Virenjagd nichts im Wege und Sie können Computer auf Trojaner absuchen und Daten von nicht mehr startenden Windows-Systemen auf dem Desinfec't-Stick in Sicherheit bringen. *(des@ct.de)* c't

Literatur

[1] Mirko Dölle, Ausgebootet, Microsoft schaltet Linux-Bootloader ab, c't 20/2022, S. 14

Dateien Desinfec't-Bootproblem:
ct.de/yfhp