Bild: Albert Hulm, Illustrator

Startinspektion

Mit Autoruns prüfen, was mit Windows alles startet

Hin und wieder möchte man genau wissen, was Windows alles beim Systemstart lädt – etwa bei einem Virenverdacht oder wenn beim Booten immer wieder eine lästige Fehlermeldung auftaucht. Das Programm Sysinternals Autoruns hilft Ihnen, die Ursache zu finden.

Von Jan Schüßler

Wenn Windows sich beim Starten nicht so verhält, wie Sie es erwarten, kann das verschiedene Ursachen haben – recht häufig ist, dass das System versucht, irgendetwas zu laden, das inkompatiblel ist, abstürzt oder schlicht gar nicht vorhanden ist. Das Programm Autoruns aus Microsofts Tool-Sammlung Sysinternals listet auf, was Windows beim Starten alles lädt, schaltet einzelne Autostart-Einträge per Klick ab und bietet zudem eine Schnellprüfung auf Malware.

Autoruns laden Sie direkt bei Microsoft herunter (siehe ct.de/yf71). Nach dem Entpacken des Programmpakets autoruns.zip finden Sie vier ausführbare Dateien im Programmordner. Autoruns.exe und Autoruns64.exe sind die 32- und die 64-Bit-Ausgaben des Programms. Nehmen Sie einfach die, die zu Ihrer Windows-Architektur passt – die ermitteln Sie aus den „Basisinformationen über den Computer“, die Sie per Windows+Pause öffnen.

Etwas anderes ist es bei Autorunsc.exe und Autorunsc64.exe: Dies sind spezielle Kommandozeilen-Versionen, die rein textbasiert in einer Eingabeaufforderung oder PowerShell bedient werden müssen. Sinnvoll ist das in erster Linie für den Einsatz auf Windows-Servern, die keine grafische Bedienoberfläche bieten, sondern komplett per PowerShell administriert werden. Einen Überblick über alle Schalter dieser Programmversionen finden Sie in der Autoruns-Dokumentation (siehe ct.de/yf71).

Offline-Modus

Autoruns ist auch im c’t-Notfall-Windows enthalten. In dieser Form eignet es sich sehr gut zur Offline-Analyse, also für Windows-Installationen, die gerade nicht laufen – etwa, weil sie es wegen einer kaputten Autostart-Konfiguration nicht können, oder zum Zweck der Virensuche.

Um eine Windows-Installation für eine solche Offline-Untersuchung einzubinden, starten Sie Autoruns und rufen dann im Menü „File“ die Funktion „Analyze Offline

System“ auf. Nun geben Sie das Windows-Verzeichnis und das üblicherweise verwendete Benutzerverzeichnis der zu prüfenden Installation an, also beispielsweise `f:\windows` und `f:\users\benutzername`.

Zur Offline-Analyse muss Autoruns übrigens nicht zwingend aus einem Notfallsystem heraus laufen. Sie können auch die Festplatte aus dem betroffenen Rechner ausbauen und an einen anderen Windows-PC anklemmen – entscheidend ist der Zugriff auf die Systempartition.

Anders als viele andere System-Tools braucht Autoruns nicht sofort Administratorrechte. Sobald es sie doch braucht, etwa für Eingriffe in die Startkonfiguration, fordert es sie automatisch an.

Eine Warnung ist unerlässlich: Wenn Sie aus reinem Spaß am Herumprobieren irgendwelche Treiber-Autostarts lahmlegen, nimmt Windows das mit etwas Pech sehr übel und bootet danach nicht mehr. Erstellen Sie also stets ein Backup, bevor Sie mit Autoruns experimentieren.

Überblick verschaffen

Autoruns durchsucht die Orte der Registry, die dafür bekannt sind, Windows mitzuteilen, was es bei Systemstart und Benutzerlogin laden soll. In der Standardansicht wirft es alle gefundenen Einträge in eine einzelne Liste, gruppiert nach Fundort, auf der Registerkarte „Everything“. Zudem kategorisiert es alle Einträge in weitere Registerkarten. So finden sich Gerätetreiber unter „Drivers“, Windows-Dienste unter „Services“ und so weiter.

Auf der Registerkarte „Logon“ erscheinen die Elemente, die erst bei der Anmeldung des gerade angemeldeten Benutzers geladen werden. Sie können sich auch die Autostarts anderer Benutzer anzeigen lassen. Dazu muss Autoruns mit Administratorrechten laufen. Tut es das noch nicht, klicken Sie zunächst im Menü „File“ auf „Run as Administrator“ und bestätigen Sie die Abfrage der Benutzerkontensteuerung. Nun können Sie über das Menü „User“ ein anderes Benutzerprofil auswählen.

Was ist was?

Die linke Spalte mit dem Namen „Autorun Entry“ gibt an, wo sich in der Windows-Konfiguration die Anweisung zum automatischen Start eines Elements befindet – also Name und Pfad des Registry-Schlüssels oder, auf der Registerkarte „Scheduled Tasks“, Name und Pfad in der Windows-Aufgabenplanung. In seltenen Fällen kann sich ein Autorun-Eintrag auch direkt im Dateisystem befinden, nämlich dann, wenn etwas im „Autostart“-Ordner des Startmenüs liegt.

Autostart-Einträge können Sie übrigens aus Autoruns heraus per Doppelklick öffnen (oder per Rechtsklick und „Jump to Entry“). Je nach Art des Eintrags öffnet sich dann der Registry-Editor, die Aufgabenplanung oder der Datei-Explorer. Die Aufgabenplanung zeigt den gewünschten Eintrag allerdings nicht direkt an – möchten Sie etwas an einer Aufgabe ändern, müssen Sie sich über den linken Navigationsbereich zum passenden Eintrag hangeln.

In der Spalte „Image Path“ zeigt Autoruns Pfad und Namen der Datei, die ein Eintrag startet. Im Regelfall sind das ausführbare Dateien mit der Endung .exe sowie Programmbibliotheken, Treiber und Codecs. Doch Obacht: Was unter „Image Path“ steht, ist nur die halbe Wahrheit. Mit welchen Parametern, Schaltern oder sonstigen Argumenten ein Programm ausgeführt wird, steht erst im Detailbereich unterhalb der Liste, wenn Sie einen Eintrag per Klick markieren.

Das ist vor allem bei der Virensuche wichtig zu wissen. Angreifer verschleiern den Autostart ihrer Schädlinge gerne, indem sie ihnen nicht einen direkten Autostart-Eintrag geben, sondern dafür sorgen, dass ein vertrauenswürdiger Windows-Bestandteil die Malware lädt. So könnten Angreifer etwa den Windows-Hostprozess rundll32.exe auffordern, die Programmbibliothek shell32.dll zu laden, die wiederum den Schädling startet. Beispiele für solche Fälle hat Microsoft-Mitarbeiter Moti Bani in einem Blogeintrag zusammengetragen (siehe ct.de/yf71).

Sinnvoll filtern

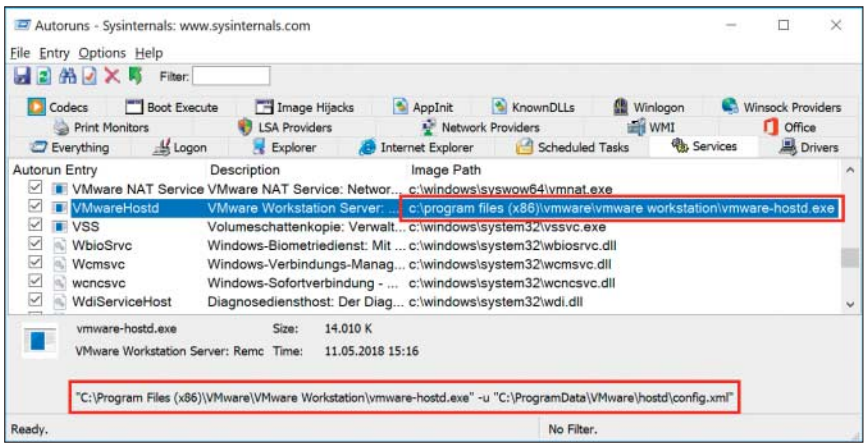
Wie lang die Liste ist, die Autoruns Ihnen anzeigt, können Sie über das Menü „Options“ steuern. Vieles ist uninteressant, allen voran Orte, an denen Autoruns gar keine Autostart-Einträge findet. Die Option „Hide Empty Locations“ können Sie also getrost aktiv lassen.

Mit den Optionen „Hide Windows Entries“ und „Hide Microsoft Entries“ blendet Autoruns Einträge aus, die zu Windows selbst beziehungsweise zu anderen Microsoft-Produkten gehören, also etwa zu Office, Outlook & Co.

Wie Autoruns das ermittelt, hängt davon ab, ob Sie unter „Scan Options“ ein Häkchen vor „Verify Code Signatures“ gesetzt haben. In der Standardeinstellung ist das nicht der Fall. So blendet „Hide Microsoft Entries“ alle Einträge aus, die im Image Path auf Dateien verweisen, die in ihren Eigenschaften Microsoft als Hersteller nennen. „Hide Windows Entries“ begrenzt diese Filterfunktion auf Einträge, die ins Windows-Verzeichnis verweisen.

Haben Sie in den Scan-Optionen das Verifizieren der Codesignaturen eingeschaltet, funktioniert der Filter etwas anders: „Hide Windows Entries“ blendet dann Einträge aus, die im Image Path auf Dateien mit einer gültigen Signatur des Betriebssystems zeigen. „Hide Microsoft Entries“ blendet zudem alles aus, was eine gültige Signatur der Microsoft Corporation aufweist.

Schalten Sie die Signatur-Verifizierung stets ein. Spätestens dann, wenn Sie die Autostarts nach Viren absuchen, ist es sowieso unerlässlich: Für Kriminelle ist es ein Leichtes, in den Dateieigenschaften ihrer Schädlinge einfach „Microsoft“ als Herausgeber einzutragen. Eine gültige



Im unteren Infobereich zeigt Autoruns, mit welchen Argumenten ein Eintrag startet.

Signatur vorzugaukeln, ist dagegen ungleich komplizierter.

Manche Einträge lassen sich übrigens nicht ausblenden, obwohl sie zu Windows gehören: Systemprozesse wie rundll32.exe und cmd.exe, hinter denen Kriminelle gerne ihre Schädlinge verstecken (siehe oben), bekommen Sie immer zu sehen.

Virencheck

Für die Prüfung, ob Windows beim Booten Viren mitlädt, bietet Autoruns einen komfortablen Mechanismus. Die verlässlichsten Ergebnisse sind bei einem Offline-Scan zu erwarten – in einem laufenden System versuchen manche Schädlinge, sich vor der Entdeckung zu tarnen.

Für die Virenprüfung bedient sich Autoruns des kostenlosen Online-Virenscan-Dienstes VirusTotal.com. Der lässt sich per Upload übers Netz mit Dateien füttern, die er auf rund 70 Antivirenprogrammen auf Schädlichkeit prüft. Um Bandbreite zu sparen, akzeptiert VirusTotal auch Hash-Werte – einzigartige Prüfsummen, die sich der Dienst für jede gescannte Datei merkt.

Um die Virenprüfung zu verwenden, klicken Sie im Menü „Options“ auf „Scan Options“. Setzen Sie Häkchen vor „Verify Code Signatures“, „Check VirusTotal.com“ und „Submit Unknown Images“. Sobald Sie den Dialog mit „Rescan“ bestätigen, bittet Autoruns Sie, die Nutzungsbedingungen von VirusTotal abzunicken.

Autoruns ermittelt nun zunächst die Hash-Werte aller Autostart-Elemente und schickt sie an VirusTotal. Sobald der Dienst das Scan-Ergebnis zurückmeldet, taucht es in der Tabellenspalte „VirusTotal“ auf. „2/68“ bedeutet: 2 von 68 Scannern stufen die Datei als schädlich ein. Ein Klick auf das Ergebnis führt Sie zum ausführlichen Bericht bei VirusTotal.com. Kennt VirusTotal einen Hash-Wert nicht, wird Autoruns es für diesen Eintrag nicht beim Übermitteln des Hashes belassen, sondern automatisch die ganze Datei zur Überprüfung zu VirusTotal hochladen.

Um einen guten Überblick über die Scan-Ergebnisse zu bekommen, aktiveren Sie die Optionen „Hide Windows Entries“ und „Hide VirusTotal Clean Entries“. Was jetzt noch angezeigt wird, hat mindestens einen Virenscanner bei VirusTotal Alarm schlagen lassen.

Locker bleiben

Lassen Sie sich nicht ins Bockshorn jagen, wenn einer von siebzig Scannern glaubt, einen Schädling gefunden zu haben. Bei VirusTotal sind immer wieder Scanner mit von der Partie, die diverse harmlose Windows-Bestandteile für Malware halten, weil sie zu einem bestimmten Verhaltensmuster passen. Hellhörig sollten Sie werden, wenn drei oder mehr Scanner einen Fund melden – vor allem, wenn auch renommierte Scanner dabei sind, wie etwa Avira, BitDefender, Kaspersky oder Norton.

Ein Tipp, falls Sie einen Schädling vermuten, der so neu ist, dass nur wenige Scanner ihn erkennen: Warten Sie ein bisschen ab! Bei tatsächlicher Malware steigt die Erkennungsquote meist nach ein paar Minuten bis Stunden rapide an. Schicken Sie einen Verdachtsfall also eine Stunde später einfach nochmal zur Prüfung ein. Klicken Sie dazu mit der rechten Maustaste auf den Listeneintrag und wählen Sie „Resubmit to VirusTotal“. Per Klick auf „Scanning file...“ in der Tabellenspalte „VirusTotal“ öffnet sich ein Browserfenster, in dem Sie den Scan-Status live überwachen können. Wenn nun nicht mehr zwei, sondern zehn oder zwanzig Scanner Alarm schlagen, haben Sie tatsächlich einen Befall, dem Sie zum Beispiel mit Desinfec’t zu Leibe rücken können (siehe c’t 12/2018 ab S. 80).

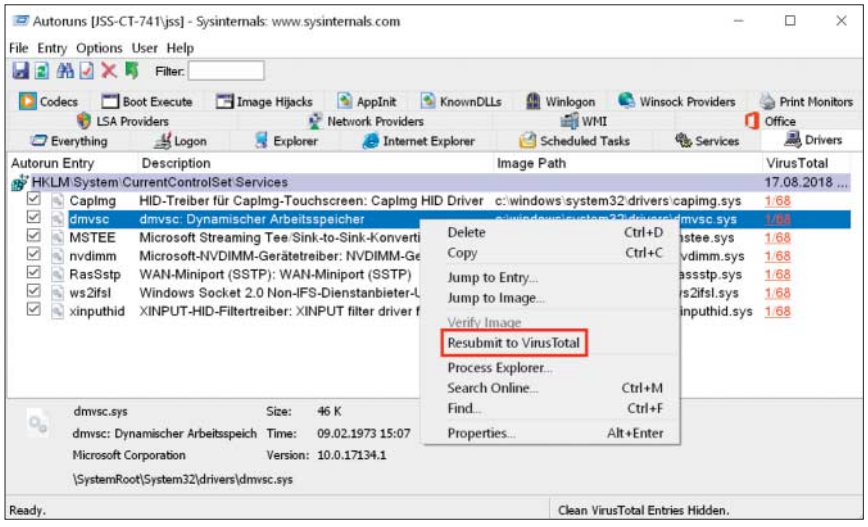
Was nervt da?

Andere Anwendungsfälle für Autoruns haben nichts mit Viren zu tun: wenn Windows etwa bei jedem Systemstart meckert, weil es eine Komponente, DLL oder Treiberdatei nicht finden kann. Die Ursache ist oft eine längst deinstallierte Software oder ein unsauber entfernter Treiber für ein Gerät, das gar nicht mehr existiert.

Bekommen Sie eine solche Fehlermeldung, ist es eine gute Idee, in Autoruns danach zu suchen. Setzen Sie im Optionen-Menü den Filter „Hide Windows Entries“ und durchforsten Sie die Autostart-Liste – ruhig in der Registerkarte „Everything“. Im besten Fall erkennen Sie den Namen der Treiberdatei vom Fehlerdialog wieder. Falls nicht, können die Beschreibungen in den Spalten „Description“ und „Publisher“ hilfreich sein. Hier steht in den meisten Fällen, wofür der Eintrag gut ist und wie der Hersteller des Treibers heißt. Entfernen Sie das Häkchen vor dem passenden Eintrag; beim nächsten Neustart sollte die Fehlermeldung verschwunden sein.

Auf ähnliche Weise könnten Sie auch den Autostart diverser Software samt ihrer Symbole im Infobereich der Taskleiste unterdrücken – sei es bei Grafik- und Soundkarten-Treibern oder bei Programmen wie Spotify, OneDrive, Steam und ähnliches. Wir raten aber stets dazu, in solchen Fällen den vom Anbieter vorgegebenen Weg zu gehen: Den allermeisten Programmen und Tools können Sie den automatischen Start auch in ihren Einstellungen abgewöhnen; und auch in den Tools von Grafiktreibern lassen sich Taskleistensymbole und Kontextmenü-Erweiterungen meist irgendwo abschalten. Ein Eingriff mittels Autoruns birgt hingegen stets das Risiko, dass Sie zu viel abschalten und Funktionen lahmlegen.

(jss@ct.de) c't



Ist eine Datei verdächtig, schicken Sie sie später einfach noch mal zum Prüfen ein. Schlägt nach wie vor nur ein Scanner an, ist sie ziemlich sicher harmlos.

Autoruns und Beispiele: ***ct.de/yf71***