DIETMAR **W**ALKER - **P**C-**B**LITZHELFER-**N**OTDIENST
Nationalgasse 14 • **7**2124 **P**liezhausen • ∅ **T**el. 07127 / 89194 - **F**ax 89118
Internet: http://www.pc-blitzhelfer.de – **M**obil 0172-882 79 55

Anleitung Grundlagen der manuellen Identifizierung und Entfernung von Malware

Wenn wir vom Kampf gegen Malware sprechen, geht es in der Regel hauptsächlich darum, wie gut Sicherheitssoftware Computer vor schädlicher Software schützt. Malware-Schutz (im Allgemeinen Antivirus- und Anti-Malware-Software) ist zweifelsohne einer der wichtigsten Verteidigungsmechanismen für Computer. Doch was, wenn Ihr Rechner infiziert wird, bevor Sie ein Sicherheitsprogramm installieren konnten?

Insbesondere bei der Reparatur oder Wartung von Computern kommt es häufig vor, dass die Rechner bereits infiziert sind. Dann ist das Installieren eines Sicherheitsprogramms nicht genug, um sämtliche Malware zu entfernen. Ratschläge zum Verhindern von Infektionen sind zwar unschätzbar, aber in dem Moment nicht wirklich eine Hilfe. Der erste Schritt wäre also das Herunterladen und Ausführen eines Malware-Scanners (etwa unser Emsisoft Emergency Kit). Im Idealfall findet dieser Scanner alle Schädlinge, aber das klappt aus verschiedenen Gründen leider nicht immer:

- Die Malware konnte sich bereits ungehindert installieren – ob nun die Sicherheitssoftware versagt hat oder gar keine erst auf dem Computer war, sei dahingestellt. Das bedeutet nun aber, dass sie sich eventuell auch vor dem Erkennen oder Entfernen schützt. Vielleicht ist es sogar eine bisher unbekannte oder ganz seltene Version, die noch gar nicht erkannt oder entfernt werden kann.
- Manche Malware ist zudem in der Lage, aktiv dafür zu sorgen, dass kein Sicherheitsprogramm installiert oder ausgeführt und damit auch kein Scan durchgeführt werden kann. Das ist zum Beispiel der Fall, wenn der Schädling schon läuft, aber noch kein Scanner.
- Viele Sicherheitsprodukte verlassen sich darüber hinaus zum Identifizieren von Schadprogrammen auf Verhaltens- oder heuristische Analysen. Dazu muss das Programm aber vor dem erstmaligen Ausführen der Malware schon laufen, um die Infektion verhindern zu können. Wird der Scan also erst danach durchgeführt, ist diese Funktionalität nur bedingt wirksam. Selbst wenn sich das System also erfolgreich scannen lässt, wird mitunter nur ein Teil oder gar nichts von der Malware erkannt.

Manuelle Malware-Entfernung

Ist der Computer also jetzt immer noch infiziert, hilft nur ein manuelles Entfernen der Malware. Das kann ganz schön tückisch sein – insbesondere, wenn Sie noch nie groß etwas mit der Identifizierung von Schadsoftware zu schaffen hatten, ganz zu schweigen von ihrer Entfernung. Wo sollen Sie anfangen? Und woher sollen Sie wissen, ob eine Datei, ein Ordner oder ein Registrierungseintrag bösartig ist oder nicht? Natürlich können Sie die Dateinamen im Internet suchen, aber für jede legitime Windows-Datei werden auch etliche Suchergebnisse auftauchen, nach denen sie bösartig sei.

Zum Glück gibt es verschiedene Tools, mit denen Sie sich einen Überblick verschaffen können, was auf Ihrem Computer vor sich geht. Wir haben uns entschieden, Ihnen die Malware-Entfernung mithilfe von Autoruns zu erklären. Das von Microsoft SysInternals entwickelte Programm ist kostenlos verfügbar und gehört zu den beliebtesten Tools für diesen Zweck.

Doch was ist der Unterschied zwischen einem automatisierten Scanner wie Emsisoft Emergency Kit und einer Analyseanwendung wie Autoruns? Ein automatisierter Scanner gleicht die Objekte im Dateisystem und in der Registrierung mit Malware-Definitionen ab und überprüft, ob es

Übereinstimmungen gibt. Eine Analyseanwendung hingegen zeigt an, welche Dateien wann genau beim Systemstart ausgeführt werden sollen. Bei einigen dieser Tools wird auch angezeigt, welche Prozesse liefen, als ein Scan durchgeführt wurde. Autoruns ist allerdings nur für die erstgenannte Funktion ausgelegt. Der Anwender des Tools muss also selbst entscheiden, ob die angezeigten Objekte gut- oder bösartig sind. (Hinweis: Viele Analyseanwendungen verfügen über Ausnahmelisten mit bekannten gutartigen Dateien, die nicht für schädliche Zwecke eingesetzt werden können.)

Malware identifizieren

Damit sind wir schon beim wichtigsten Schritt einer manuellen Malware-Entfernung angekommen: die Identifizierung. Es gibt leider keine magische Funktion, die alle verdächtigen Einträge mit einem Mausklick verschwinden lässt – zumindest noch nicht. Sie müssen also immer noch selbst herausfinden, was weg muss. Aber keine Bange. Sie brauchen keine komplizierten Analysen durchführen. Meistens reicht schon ein gutes Grundwissen über Windows und schlichtes logisches Denkvermögen. (Hinweis: Machen Sie sich spätestens jetzt unbedingt mit der Windows-Registrierung vertraut. Sollte Ihnen das Thema noch völlig fremd sein, finden Sie hier einen guten Einstiegspunkt.)

Wenn Malware auf ein System gelangt, wird sie sicherstellen, dass sie bei jedem Hochfahren des Computers gestartet wird. Bei der Suche nach Malware ist der erste Anlaufpunkt daher die sogenannte Ladeadresse. Wenn Sie diese finden, erhalten Sie meistens bereits einen Hinweis darauf, wo sich die Malware in Ihrem Dateisystem versteckt. Wie der Name schon andeutet, gibt Autoruns (also „automatisches Ausführen“) einen bequemen Überblick über die meisten Ladeadressen, die in Windows verwendet werden können.

Ein weiterer wichtiger Punkt zum Erkennen bösartiger Einträge ist das **Identifizieren von legitimen Objekten**. Das klingt leichter als es ist. Bevor wir uns mit einer einfachen Malware-Infektion befassen, werden wir uns daher zunächst einen Beispieleintrag in einer sauberen Windows-10-Installation ansehen. Abbildung 1 enthält einen Autoruns-Scan. Fangen wir oben an.

Abbildung 1: Autoruns-Scan – AlternateShell / cmd.exe

Die erste Datei in der Liste ist die cmd.exe unter dem Registrierungsschlüssel AlternateShell. Um zu erkennen, ob die Datei legitim ist oder nicht, sind zwei Punkte ausschlaggebend:

1. Ist die Datei vertrauenswürdig? Handelt es sich also um die echte cmd.exe von Windows oder ist es etwas anderes, das uns nur mit demselben Namen täuschen will?
2. Ist die Ladeadresse für die Datei gebräuchlich?

Wir können auch im Internet nach „cmd.exe“ suchen. Rechtsklicken Sie dazu einfach auf den Eintrag und wählen Sie „Search Online“ (Online suchen). Auf der ersten Seite der Suchergebnisse werden Ihnen Erläuterungen angezeigt, worum es sich bei der original cmd.exe handelt. Gleichzeitig gibt es jedoch Beispiele, wie sich Malware diesen Dateinamen zunutze macht. Sie erhalten also keine eindeutige Aussage zur Vertrauenswürdigkeit. Um sicherzustellen, dass es sich wirklich um eine echte Windows-Datei handelt, können wir stattdessen den Speicherort überprüfen (standardmäßig der System32-Ordner) oder die Datei über VirusTotal scannen. Rechtsklicken Sie dazu auf den Eintrag und wählen Sie „Check VirusTotal“ (Mit VirusTotal überprüfen). In diesem Fall ist die Datei legitim.

Auch das Suchen nach „AlternateShell“ kann nützlich sein. Laut einem Artikel von Microsoft dient AlternateShell zur Angabe der alternativen Umgebung, die bei Auswahl der Option „Abgesicherter Modus mit Eingabeaufforderung“ verwendet wird.

Wir können auch erkennen, dass die cmd.exe der Standardwert ist. Der Eintrag „cmd.exe“ unter „AlternateShell“ in unserem Autoruns-Bericht ist also rechtmäßig und kann hinsichtlich der Malware-Entfernung ignoriert werden. (Hinweis: Auch wenn das meistens der Fall ist, gibt es Ausnahmen, bei denen die legitime Datei in dem Eintrag durch eine bösartige Kopie ersetzt wurde. Aber das ist ein Thema für ein andermal.)

Schauen wir uns jetzt ein Beispiel für eine Malware-Infektion an. Hier haben wir ein Beispiel für einen Trojaner, der auf dem System installiert wurde. Der Autoruns-Bericht sieht dann wie folgt aus:

Abbildung 2: Autoruns-Scan – Trojaner-Beispiel

Das sieht auf den ersten Blick recht verwirrend aus. Autoruns sortiert die gesammelten Daten jedoch bequemerweise nach Ladeadresse. Es wird auch der Speicherort für jede Ladeadresse angezeigt, der sich in der Registrierung oder dem Dateisystem befinden kann. Wenn wir die Daten in dem Bericht jetzt analysieren (siehe Abbildung 2), stechen zwei Einträge hervor: Bei beiden handelt es sich um eine Zeichenfolge aus Buchstaben und Zahlen, während die anderen Objekte einigermaßen lesbare Namen haben. Laut Autoruns befinden sich die Einträge in:

- HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

Wie Sie sehen, handelt es sich bei dem ersten fragwürdigen Eintrag um einen Registrierungsschlüssel und bei dem zweiten um einen Ordner. Diesen beiden Speicherorte werden am häufigsten als Ladeadressen sowohl für reguläre Anwendungen als auch Malware genutzt. Möchten Sie sicherstellen, dass eine Anwendung beim Start von Windows ausgeführt wird, nutzen Sie einen dieser beiden Speicherorte.

Beginnen wir mit der einfachsten Speicheradresse: der Startup-Ordner. Laut Autoruns befindet sich die Datei „edf6e17148b3b3408342ac7be2e79536.exe“ in diesem Ordner. Zwei Punkte daran sind schon einmal suspekt:

1. Normalerweise sind im Startup-Ordner keine tatsächlich ausführbaren Dateien (.exe), sondern nur Verknüpfungen (.lnk) gespeichert, die dann beim Hochfahren eine Anwendung starten.
2. Der Dateiname ist nur eine zufällig aussehende Zeichenfolge ohne jeglichen Hinweis darauf, was hier geladen wird. Man würde erwarten, dass der Dateiname darauf hindeutet, welche Anwendung geladen wird … und natürlich, dass diese Anwendung dann auch tatsächlich auf Ihrem Computer vorhanden ist.

Um unseren Verdacht zu bestätigen, können wir in Autoruns einen Rechtsklick auf das Objekt machen und die Option „Check VirusTotal“ (Mit VirusTotal überprüfen) wählen. Ihnen wird dann ein Link zu den Scanergebnissen von VirusTotal angezeigt, die Ihnen bestätigen, dass die Datei tatsächlich bösartig ist und entfernt werden muss.

Sehen wir uns jetzt die andere Ladeadresse an, nämlich den Ausführungswert. Wir können diesen Eintrag direkt im Registrierungs-Editor öffnen, indem wir einen Rechtsklick darauf machen und „Jump to Entry …“ (Zum Eintrag springen) wählen. Das sieht dann wie folgt aus (siehe Abbildung 3):

Abbildung 3: Ausschnitt aus dem Registrierungs-Editor

Auch hier gibt es bereits einige Dateieigenschaften, die zur Vorsicht mahnen:

1. Der Dateiname ist wieder eine zufällige Zeichenfolge, ohne jeglichen Hinweis darauf, welches Programm ausgeführt wird.
2. Der Datenwert verweist auf eine Datei namens „svhost.exe“ in einem Temp-Ordner. Diese ist nicht mit der legitimen Windows-Datei „svhost.exe“ zu verwechseln, die sich normalerweise im Pfad \Windows\System32 befindet.

Als Nächstes können wir sehen, dass Autoruns zusätzliche Informationen bereitstellt und auch Metadaten der Datei erfasst hat. Diese können wir überprüfen, indem wir uns durch Rechtsklick auf die Datei und Auswählen von „Properties“ (Eigenschaften) die Eigenschaften anzeigen lassen (siehe Abbildung 4):

Abbildung 4: Metadaten – svchost.exe

Offensichtlich ist der Produktname der Datei „Windows Serivce“. Das klingt zunächst rechtmäßig, allerdings gibt es keine Windows-Datei mit diesem Produktnamen und darüber hinaus enthält die Bezeichnung einen Rechtschreibfehler: „Serivce“. Der Originaldateiname ist „Game.exe“, was in der Regel gar nichts mit der svchost.exe oder einem Windows-Dienst zu tun hat. Ein Scan über VirusTotal bestätigt schließlich, dass auch diese Datei schädlich ist.

Indem sie die beiden VirusTotal-Berichte vergleichen, können Sie außerdem überprüfen, ob beide Objekte zur selben Infektion gehören oder nicht. Öffnen Sie dazu in den VirusTotal-Ergebnissen das Register „Zusätzliche Informationen“, wo dann die Hash-Werte für diese beiden Dateien identisch sind.

Malware entfernen

Wir haben jetzt zwei Dateien und einen Registrierungseintrag identifiziert, die gelöscht werden sollen. Widmen wir uns also der eigentlichen Entfernung. Autoruns verfügt zwar über eine Löschfunktion („Delete“), aber die Malware könnte derzeit noch laufen (was sie auch tatsächlich tut). Wie bereits erwähnt, kann Malware sich nach der Entfernung wieder neu anlegen oder sogar den Löschversuch unterbinden. In diesem Fall kann Autoruns die Objekte nicht entfernen. Wir könnten versuchen, die Malware mithilfe des Windows Task-Managers zu beenden, was jedoch ebenfalls nur eine beschränkte Option ist. Die bessere Alternative – insbesondere bei der Malware-Entfernung – ist Process Explorer. Er bietet sich insbesondere deshalb besser an, weil er im Vergleich zum Task-Manager mehr Informationen liefert (wie hier zu sehen ist).

Die Malware haben wir schon einmal identifiziert. Jetzt müssen wir nur noch den zugehörigen Prozess finden.

Abbildung 5: Process Explorer

Wie Sie Abbildung 5 entnehmen können, passt nur ein Eintrag auf alle Einzelheiten des Schädlings: der Name svhost.exe, die Beschreibung „Windows Serivce“ und als Speicherort der Temp-Ordner (wird angezeigt, wenn Sie den Cursor auf die Zeile bewegen). Es ist extrem wichtig, dass alle Angaben übereinstimmen, da es sich bei der „svchost.exe“ auch um eine Windows-eigene Datei handeln kann.

Sobald dieser Prozess beendet wurde (Rechtsklick > Prozess abbrechen), können alle über Autoruns identifizierten Einträge problemlos gelöscht werden. Bitte beachten Sie, dass eine Datei eventuell noch manuell entfernt werden muss, selbst wenn Autoruns die Ladeadresse in der Registrierung nicht mehr anzeigt.

Alternativ können Sie den Computer auch im abgesicherten Modus neu starten. Dabei werden weder die Werte unter „Run“ noch die Dateien im Startup-Ordner geladen. Damit ersparen Sie sich das zusätzliche Herunterladen von Process Explorer.

Wir hoffen, dass Ihnen diese Einleitung zur Malware-Entfernung gefallen hat. Wir sind bald mit weiteren Beispielen zurück, um Ihnen zu zeigen, wie Sie bestimmte Infektionen loswerden (z. B. Ransomware, PUPs usw.). In der Zwischenzeit gilt natürlich weiterhin: Vorbeugen ist besser als heilen. Legen Sie sich also unbedingt ein zuverlässiges Antivirus- und Anti-Malware-Programm zu, um sich unnötige Kopfschmerzen zu sparen.

Quelle: https://blog.emsisoft.com/de/31201/grundlagen-manuellen-identifizierung-entfernung-von-malware/