Wie schützt macOS vor Malware?

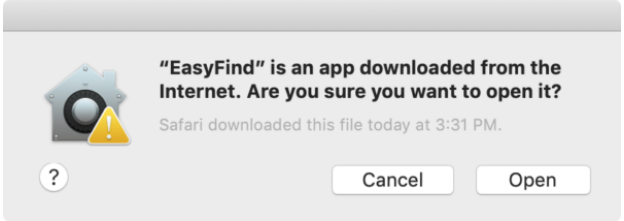
von Thomas Reed (Malwarebytes), Übersetzung KJM

Mac-Anwendern wird oft gesagt, dass „Macs keine Viren bekommen“. Das ist natürlich nicht wirklich wahr. Macs können und werden infiziert. Es ist jedoch richtig, dass macOS einen gewissen grundlegenden Schutz vor Malware bietet. Dieser Schutz kann in mancher Hinsicht sehr effektiv sein, aber leider auch in anderen Bereichen ziemlich wirkungslos. Lassen Sie uns einen Blick darauf werfen, wie macOS-Funktionen Sie vor Malware schützen und wie Malware diese Funktionen überwinden kann.

Quarantäne

macOS hat eine Funktion, die als Quarantäne bezeichnet wird. Jedes Mal, wenn eine Datei aus dem Internet heruntergeladen wird, wird sie mit einem Quarantäne-*Flag* „markiert“. Wenn Sie versuchen, eine heruntergeladene App mit diesem Flag-Set zu öffnen, wird macOS eine ganze Reihe von Prüfungen starten.

Wenn diese Prüfungen erfolgreich sind, zeigt macOS eine Meldung an, die Sie darüber informiert, dass Sie eine aus dem Internet heruntergeladene Anwendung öffnen, die Sie zulassen müssen, wenn Sie die Datei verwenden möchten. (macOS zeigt diese Meldung dem Benutzer an, um die wahre Natur der Datei anzuzeigen, falls sie als ein anderer Typ getarnt war, z.B. eine als Dokument getarnte App.)



Sobald die App zum ersten Mal erfolgreich geöffnet wurde, wird das Quarantäne-*Flag* entfernt und diese Prüfungen werden nicht mehr wiederholt.

Einige der anderen Schutzfunktionen in macOS hängen von der Quarantäne ab, und leider gibt es einige Möglichkeiten, wie Anwendungen auf Ihre Festplatte gelangen können, ohne mit einem Quarantäne-*Flag* markiert zu sein. Einige Beispiele:

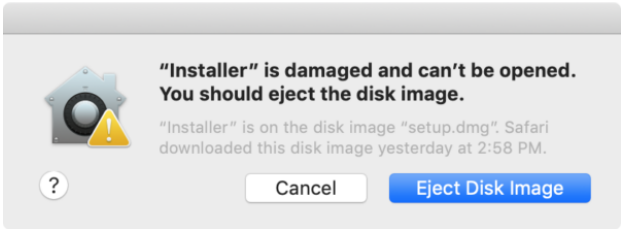
- Nicht alle Apps setzen ordnungsgemäß ein Quarantäne-*Flag* für Dateien, die sie herunterladen; Torrent-Apps und bösartige Downloader sind zwei Beispiele dafür.
- Das Kopieren einer Anwendung auf einen anderen Mac, nachdem das Quarantäne-*Flag* entfernt wurde, führt dazu, dass die Anwendung auf dem zweiten Mac nicht unter Quarantäne gestellt wird.
- Das Kopieren einer Datei auf eine Nicht-Mac-Dateifreigabe oder einen USB-Stick, der nicht Mac-formatiert ist, führt zum Verlust des Quarantäne-*Flags*.
- Schwachstellen, die die Erstellung von Dateien ermöglichen, ohne legitime Download-Methoden zu durchlaufen, ermöglichen *flag*lose Anwendungen auf der Festplatte.

Gatekeeper

Kehren wir zurück dahin, wo eine App aus dem Internet heruntergeladen wird und ein Quarantäne-*Flag* gesetzt wurde. Die erste der Prüfungen, die bei einer unter Quarantäne stehenden Anwendung durchgeführt werden, ist die Überprüfung der Code-Signatur der Anwendung.

Eine Codesignatur ist ein Stück kryptographischer Daten, die den Ersteller der App identifiziert und dazu verwendet werden kann, festzustellen, ob die App manipuliert wurde. Sie hängt von einem Zertifikat ab, das von Apple als Teil eines 99-Dollar-Entwicklerkontos erhalten wurde.

Wenn die Codesignatur anzeigt, dass die App manipuliert wurde oder dass das Zertifikat, mit dem die Signatur erstellt wurde, von Apple widerrufen wurde, lässt macOS die App überhaupt nicht laufen.



Leider ist der Gatekeeper nicht unfehlbar, und seine größte Schwäche ist die Quarantäne selbst. Gatekeeper-Checks finden nicht für Anwendungen statt, die nicht unter Quarantäne stehen, d.h. auch für Anwendungen, die unter Quarantäne gestellt wurden, aber bereits mindestens einmal geöffnet wurden und somit nicht mehr unter Quarantäne stehen.

Das bedeutet, dass eine unschuldig aussehende App nach der Installation alle Arten von bösartigen Prozessen im Hintergrund herunterladen könnte, und diese Prozesse würden nicht der Gatekeeper-Prüfung unterliegen. Ähnlich würde, wenn Sie eine bösartige Anwendung auf Ihrem Computer ausgeführt hätten und Apple einige Zeit später das für die Code-Signatur verwendete Entwicklerzertifikat widerrufen hätte, die Anwendung weiterhin auf Ihrem Mac ausgeführt, da Code-Signaturprüfungen nur für isolierte Anwendungen als Teil von Gatekeeper durchgeführt werden.

Dies bedeutet auch, dass Malware Anwendungen auf Ihrem Mac böswillig modifizieren könnte, was die Auffindbarkeit und Entfernung der Malware teuflisch erschweren würde.

XProtect

XProtect ist eine versteckte Funktion des Systems, von der Sie nie wissen würden, dass sie vorhanden ist. XProtect ist eine grundlegende Anti-Malware-Funktion, die ebenfalls mit der Quarantäne verbunden ist. XProtect hat eine relativ geringe Anzahl von Regeln zur Identifizierung bekannter bösartiger Anwendungen, und jede isolierte Anwendung, die Sie zu öffnen versuchen, wird zuerst über XProtect hinaus ausgeführt. Wenn sie mit einer der Regeln übereinstimmt, wird macOS es nicht erlauben, sie zu öffnen.

XProtect leidet unter den gleichen Problemen wie Gatekeeper, da es sich nicht gegen etwas schützen kann, das kein Quarantäne-Flag hat. Es gibt jedoch ein größeres Problem: Zum Zeitpunkt dieses Schreibens war die letzte Regel, die XProtect hinzugefügt wurde, der 13. März 2018. Es fehlen also Regeln für fast ein ganzes Jahr neuer Malware! Die Zukunft von XProtect ist unklar, aber es schützt Sie definitiv nicht vor aktuellen Bedrohungen.

Tool zur Entfernung von Malware

2012 führten eine Reihe von Angriffen auf macOS durch Schwachstellen in Java dazu, dass Malware einfach durch den Besuch einer Website installiert wurde. Da dies die Quarantäne umging, war das nichts, für das die damaligen Sicherheitsmaßnahmen in macOS gerüstet waren. So erstellte Apple im Hintergrund das Malware Removal Tool, kurz MRT.

Das MRT ist eine Blackbox. Niemand weiß wirklich genau, wie oder wann es funktioniert, und es läuft leise, ohne Benachrichtigung der Person, die den Computer benutzt. Sein einziger Zweck ist es, bekannte Malware zu entfernen, die auf den Computer gelangt ist.

Wie XProtect erkennt auch MRT nur bekannte Malware über scheinbar fest programmierte Regeln im MRT-Code. Niemand weiß wirklich, wie diese Regeln funktionieren, und in letzter Zeit hat Apple es sich zur Aufgabe gemacht, die Zeichenketten für Malware-Namen im MRT-Code zu verschleiern, so dass wir auch nicht sagen können, was sie erkennen können.

```
mov     qword [rbp+var_80], rax
call    imp___stubs__swift_retain          ; swift_retain
lea     rdi, qword [a0sx28a9883a]          ; "OSX.28a9883.A"
mov     r10d, 0xd
mov     esi, r10d
```

Es gibt keine Malware namens OSX.28a9883.A, aber so nennt Apple sie.

Leider hat MRT in letzter Zeit nicht viele Updates gesehen, die leicht zu identifizieren sind. Weil es sich um eine solche Blackbox handelt, ist es unmöglich zu wissen, aber es sieht sicherlich nicht so aus, als ob es in der Lage wäre, viele aktuelle Malware zu erkennen.

Schutz der Systemintegrität

Diese Funktion wird als **SIP** abgekürzt und schützt die Kernsystemdateien vor Änderungen. Dieses SIP, das auch als *„rootless"* bezeichnet wird, verhindert, dass alle Benutzer, einschließlich des allmächtigen root-Benutzers, eine große Anzahl von eingeschränkten Dateien auf dem System ändern. Nur bestimmte Teile der Apple Software können Änderungen an diesen Dateien vornehmen. Diese Funktion kann nur durch einen Neustart des Computers in den Wiederherstellungsmodus und die Eingabe eines altertümlichen Befehls im Terminal deaktiviert werden, was für den Durchschnittsbürger nicht möglich ist.

Obwohl SIP für einige Software zum Zeitpunkt ihrer Einführung Probleme verursachte, hat es sich als eine ausgezeichnete Sicherheitsmaßnahme erwiesen, die sicherstellt, dass die Systemdateien nicht manipuliert werden können.

```
thomas$ sudo mkdir /System/blah
Passwort:
mkdir: /System/blah: Betrieb nicht zulässig
```

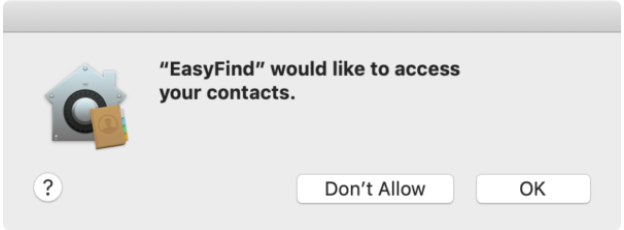
Infolgedessen glauben einige Leute, dass SIP eine Rolle spielt, um zu verhindern, dass Malware Macs infiziert. Leider ist das nicht der Fall. Noch vor SIP hat nur einige Malware Änderungen an den Dateien vorgenommen, die jetzt durch SIP geschützt sind. Malware kann einen Mac ganz einfach infizieren, ohne dies zu tun und sogar ohne Root-Rechte zu benötigen. Das bedeutet, dass SIP nichts tut, um zu verhindern, dass Malware Ihren Mac unsichtbar infiziert, wenn Sie den Fehler machen, die falsche App zu öffnen.

Transparenz, Zustimmung und Kontrolle

Dieser Bissen wird einfach auf **TCC** *(Transparency, Consent, and Control)* verkürzt und ist ein neues Feature von macOS 10.14 (Mojave). TCC schützt bestimmte Benutzerdaten vor dem Zugriff von außen, mit dem Ziel, zu verhindern, dass Apps heimlich Dinge tun, wie z.B. den Verlauf Ihres Webbrowsers zu verschleiern.

Dies ist ein edles Ziel, aber trotz seiner kurzen Lebensdauer hatte TCC schon einige Probleme. Diese

reichen in ihrer Schwere von einer Vielzahl von Erlaubnis-Anfrage-Dialogen, die „Dialogmüdigkeit“ verursachen können, bis hin zu Schwachstellen, die es Apps ermöglichen könnten, direkt an TCC vorbeizugehen und trotzdem Zugriff auf die Daten zu erhalten.



Ein Beispiel für einen TCC-Dialog. Viele Leute werden einfach auf OK klicken, um es verschwinden zu lassen.

TCC verhindert selbst keine Malware-Infektion. Wenn es jedoch korrekt funktioniert, verhindert es, dass Malware Zugriff auf einige Ihrer Daten erhält. Machen Sie es sich jedoch nicht zu bequem, da Malware immer noch ungeschützte Daten wie Passwörter und Kreditkarten verschlingt, die in Chrome's Autofill gespeichert sind, das nicht von TCC abgedeckt wird.

Mein Gehirn explodiert! Was bedeutet das alles?

Die gute Nachricht ist, dass Apple ständig daran arbeitet, macOS zu einem sichereren Ort zu machen. Obwohl Sicherheitsexperten schnell auf Lücken in den Schutzfunktionen von macOS hinweisen, ist Ihr Mac damit definitiv sicherer als ohne sie.

Es ist jedoch wichtig zu bedenken, dass jeder einzelne dieser Schutzmaßnahmen Löcher aufweist. Malware-Autoren wissen genau, wo sich diese Löcher befinden, und sind (zumindest einige von ihnen) geschickt darin, sie auszunutzen. Also lasst Eure Deckung nicht fallen!

In der Sicherheitswelt sprechen wir gerne über Schutzebenen. Mehrere Ebenen zu haben, ist eine gute Vorgehensweise, denn wenn Malware über ein oder zwei hinauskommt, kann sie immer noch von einer anderen Ebene blockiert werden. Angesichts der verschiedenen Löcher in den aktuellen Schutzfunktionen ist es sinnvoll, Ihrem Mac eine weitere Schutzebene hinzuzufügen, wie z.B. Antivirensoftware.

Malwarebytes für Mac zum Beispiel kann helfen, Löcher zu schließen, indem es aktuelle Bedrohungen erkennt, die XProtect und MRT nicht erkennen. Mit der neu eingeführten App Block Funktion kann es auch helfen, die Löcher in Gatekeeper zu stopfen.

Wenn Sie also wissen, wovor Ihr Mac allein schützen kann und wo er Hilfe benötigt, können Sie sich sicherer fühlen, egal ob Sie Anwendungen aus dem Internet herunterladen oder sich einfach eine zusätzliche Sekunde Zeit nehmen, um diese Dialogfelder durchzulesen.

Wie man in macOS Mojave PDFs ohne zusätzliche Software erstellt

von William Gallagher (OSXdaily), Übersetzung KJM

Seit Jahren können Sie aus jedem Dokument auf Macs ein PDF erstellen. Wir nehmen es jedoch so selbstverständlich, dass wir nicht wissen, welche zusätzlichen Optionen wir haben — und auch nicht bemerkt haben, wie Apple versucht, die Art und Weise, wie wir PDFs erstellen sollen, zu ändern. AppleInsider führt Sie durch die Erstellung eines PDFs ausschließlich mit Bordmitteln, die mit macOS ausgeliefert werden.

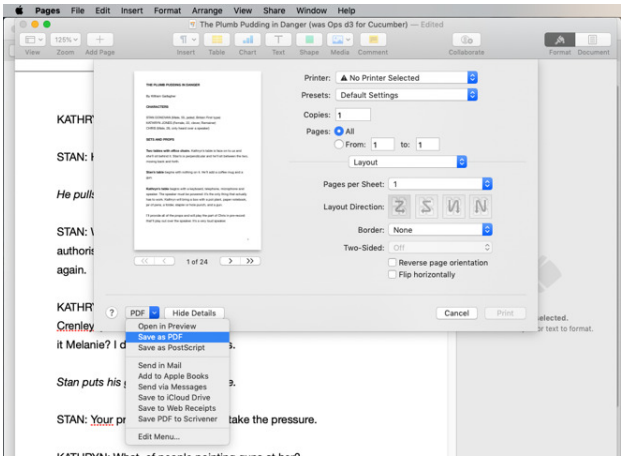
Wir wissen einfach nicht zu schätzen, was wir haben. Nach einer kurzen Zeit in den 90er Jahren, in der PDFs nur mit aufwändiger Software erzeugt werden konnten, wurde das Dokumentenformat als Kernfunktion zu macOS hinzugefügt. Für eine Weile danach wurde einem erst dann klar, wie integral PDFs für Macs sind, wie einfach sie zu bedienen sind, wenn man den PC eines Kunden benutzen musste. Und wie ärgerlich war es, dass man, um ein PDF unter Windows auszudrucken, zusätzliche Software kaufen musste — wenn die IT-Abteilung des Kunden es überhaupt zuließ.

Die Dinge haben sich geändert, und jetzt hat Windows 10 einige der PDF-Funktionen, die wir am Mac gewohnt sind. Dennoch bedeutet unsere Vertrautheit, dass wir einige der feineren PDF-Details und Funktionen verpassen könnten, die unsere Macs für uns leisten können.

Es gibt Tools von Drittanbietern mit Funktionen, die Macs — und insbesondere die Vorschau-App — nicht haben. Aber die überwiegende Mehrheit dessen, wofür Sie ein PDF verwenden können, ist direkt dort in Mojave abgedeckt.

Erstellung von PDFs

Jahrelang war die Art und Weise, wie man aus jedem Dokument in jeder Anwendung auf dem Mac ein PDF macht, genau die gleiche. Du hast es gedruckt. Gehen Sie zu Datei, Drucken und klicken Sie auf die PDF-Schaltfläche unten links im Druckdialog. Es sieht aus wie eine Schaltfläche, ist aber ein Dropdown-Menü. Wählen Sie Als PDF speichern aus der Liste und dann wird Ihnen ein normaler Speicherdialog angezeigt, in dem Sie auswählen können, wohin Sie das PDF-Dokument legen möchten.

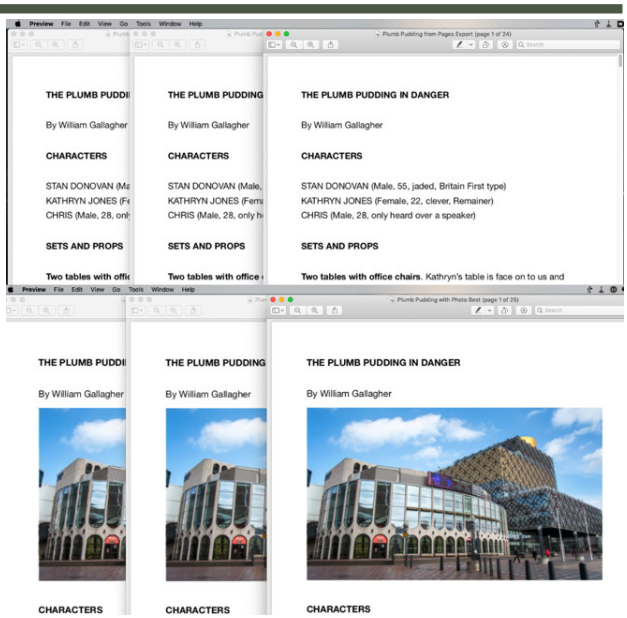


Es ist leicht zu übersehen, aber jeder Druckdialog hat ein PDF-Dropdown-Menü.

Das ist es. Das ist alles. Bevor Sie die Option Als PDF speichern wählen, können Sie im Druckdialog einige kleinere Anpassungen vornehmen. Sie können es so einstellen, dass das PDF beispielsweise nur aus den Seiten 10-15 besteht. Oder ändern Sie es von Hoch- auf Querformat. Alles, was Sie für einen Dokumentendruck auf Papier einstellen können, können Sie hier für das PDF anpassen, aber das ist alles.

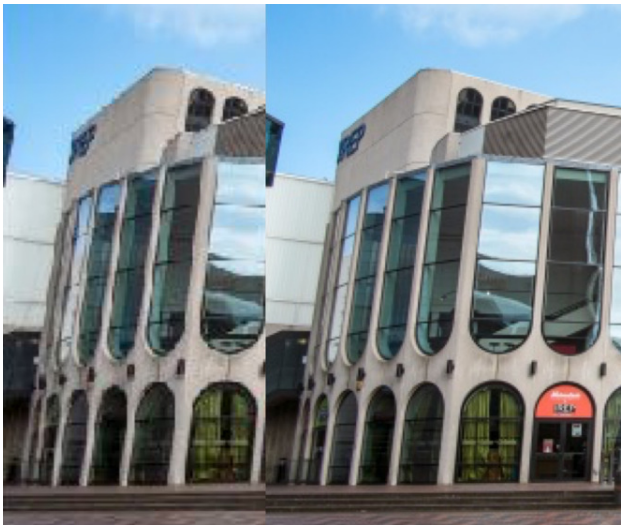
Apple würde es jedoch vorziehen, wenn man das anders machen würde. Das Unternehmen würde es vorziehen, dass Ihre Apps Ihnen so etwas wie die Option Datei > Export nach PDF anbieten, die Pages, Numbers und andere Apple Apps haben.

Im Moment kann man nur Vermutungen anstellen, ob eine bestimmte App dies jemals übernehmen wird oder nicht. Microsoft Office ignoriert es zum Beispiel und hält sich an den alten Weg — aber es gibt Zeiten, in denen dieser Exportansatz sinnvoll ist. Das liegt zum Teil daran, dass Sie dadurch keinen Schritt bei der Suche durch den Druckdialog machen müssen, aber es gibt Ihnen auch die Möglichkeit, das PDF in verschiedenen Qualitäten zu speichern. Es ist kein präzises Werkzeug, aber Apple gibt Ihnen die Wahl zwischen Gut, Besser und Am besten, damit Sie eine deutlich unterschiedliche Qualität und Dateigröße des resultierenden PDF erhalten.



Oben von links-nach rechts: ein gutes, besseres, bestes Text-PDF. Unten: das Gleiche mit einem Foto

Sie können sich schwer tun, einen Unterschied im Text zu erkennen, wenn Sie Gute, Bessere oder Beste Qualität beim Export nach PDF gewählt haben. Es ist nicht immer ein dramatischer Unterschied, wenn das PDF auch Fotos enthält, aber es kann sein. In diesem Beispiel hat die gute Qualität die Wände des Theaters im ersten Bild leicht verzerrt.



Machen Sie sich ein Bild vom Unterschied zwischen guter und bester Qualität. Beachten Sie, wie das Mauerwerk zwischen den Fenstern verformt ist.

Ebenso werden Sie, wenn das PDF Diagramme oder Illustrationen enthält, Unterschiede feststellen, die jedoch klein sein können. Bei Stift- und Tuschedarstellungen sehen Sie zum Beispiel, dass Bereiche mit Kreuzschraffuren weniger ausgeprägt aussehen.

Es gibt keine Möglichkeit zu messen, wie viel Unterschied es geben wird, und tatsächlich gibt es nicht einmal eine Möglichkeit, im Voraus zu wissen, wie viel

kleiner Ihre Dateigröße sein wird. Es hängt von der Länge Ihres PDF-Dokuments und der Anzahl der Fotos oder Illustrationen ab. Zum Beispiel ist das PDF-Dokument im obigen Bild 115KB bei guter Qualität, 168KB bei besserer Qualität und 197KB bei bester Qualität.

Das ist kein Unterschied, der dich betreffen wird. Doch bei einem viel größeren und komplexeren Dokument könnte eine Verringerung der Dateigröße der Unterschied sein, ob man es in einen Dienst wie MailChimp hochladen kann oder nicht.

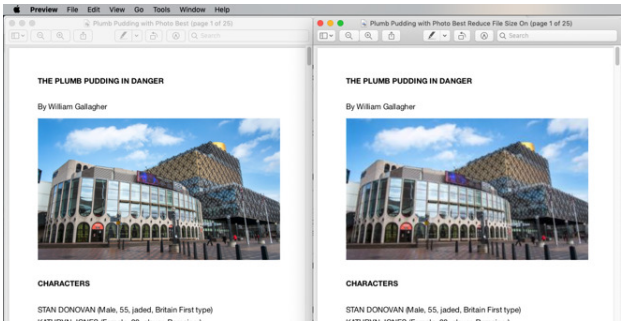
Die Vorschau ist nicht nur zum Ansehen gedacht.

Das Dokument in den obigen Beispielen wurde in Pages erstellt, als PDF exportiert und dann in der Vorschau geöffnet. Die Vorschau-App ist ein hervorragender PDF-Reader — aber sie ist auch viel mehr als das.

Die Vorschau hat zwei seltsam ähnliche, aber wichtig unterschiedliche Optionen. Im Menü Datei sehen Sie sowohl Export… als auch Export nach PDF.

Mit dem ersten Export… können Sie ein PDF erstellen, genau wie mit der zweiten Option, aber es gibt Ihnen mehr Kontrolle auf dem Weg dorthin. Wählen Sie Export… und Vorschau zeigt einen regulären Dialog Speichern unter mit bestimmten automatischen Einstellungen an. Es gibt zum Beispiel eine Formateinstellung. So können Sie jedes Dokument als PDF, JPEG, PNG usw. speichern.

Darunter gibt es jedoch Einstellungen, die je nachdem, welches Format Sie gewählt haben, variieren. Für PDF erhalten Sie eine Option namens Quarzfilter. Der Name Quartz kommt von den internen Core Graphics-Funktionen von macOS und was Sie hier wirklich einstellen, ist, wie der Mac das PDF rendert. Sie können ein monochromes PDF erstellen, die Bilder aufhellen und die Dateigröße reduzieren.

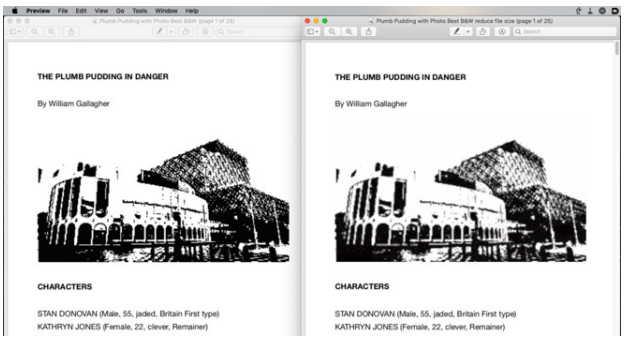


Links: das PDF-Dokument in Originalgröße. Rechts: das Gleiche nach Verwendung von Preview's Reduzieren der Dateigröße

Sie erhalten jedoch keine Optionen für die Festlegung der Reduzierung, Sie können die Option Dateigröße reduzieren nur ein- oder ausschalten. Man kann auch nicht zwei der Quart Filter Optionen wählen oder zumindest nicht gleichzeitig. Man könnte ein PDF erzeugen, das beispielsweise schwarz-weiß wäre. Dann kann man es öffnen und mit dem Befehl Dateigröße reduzieren erneut exportieren.

Auch hier gibt es keine Möglichkeit, den Unterschied zwischen all dem, was die Größe Ihres PDF-Dokuments ausmacht, vorherzusagen. Wenn Sie jedoch beispielsweise das gleiche Pages-Dokument mit einem Foto aufnehmen und die Dateigröße reduzieren, wird das 197KB-Original zu einem 92KB-PDF.

Als ich zu den PDF-Seiten zurückging und mich entschied, eine Schwarz-Weiß-Version in der Vorschau zu erstellen, entstand eine 86KB-Datei. Die folgende Reduzierung der Dateigröße dieser Version ergab dann ein 87KB Dokument.



Sie können das Leben aus Ihrem PDF herausquetschen. Links: eine monochrome Version. Rechts: Diese Version hat auch die Funktion Dateigröße reduzieren durchgesetzt.

So haben wir das Dokument so schlecht wie möglich gemacht und auch noch seine Größe erhöht, wenn auch nur ein bisschen. Vielleicht ist das der Grund, warum Apple es nur erlaubt, jeweils einen Quarzfilter zu wählen.

Dennoch, auch wenn Sie ein wenig herumfummeln müssen, um eine Kombination aus kleiner Dateigröße und einem Dokument zu erhalten, das lesbar ist, können Sie dies tun. Sie haben mehr Möglichkeiten für PDFs auf dem Mac, bevor Sie Anwendungen von Drittanbietern berücksichtigen.

Genauso ist es mit dem nächsten Thema. Meistens werden Sie nur PDFs lesen und nur manchmal werden Sie sie erstellen. Und dann bleibt noch etwas weniger Zeit, um die PDFs anstelle des Originaldokuments zu bearbeiten.

Sie können einige umfangreiche Bearbeitungen auf Ihrem Mac durchführen, wie z.B. das Hinzufügen und Entfernen ganzer Seiten. Und Sie können jedes PDF innerhalb weniger Sekunden mit den Funktionen von Mojave kommentieren oder markieren.