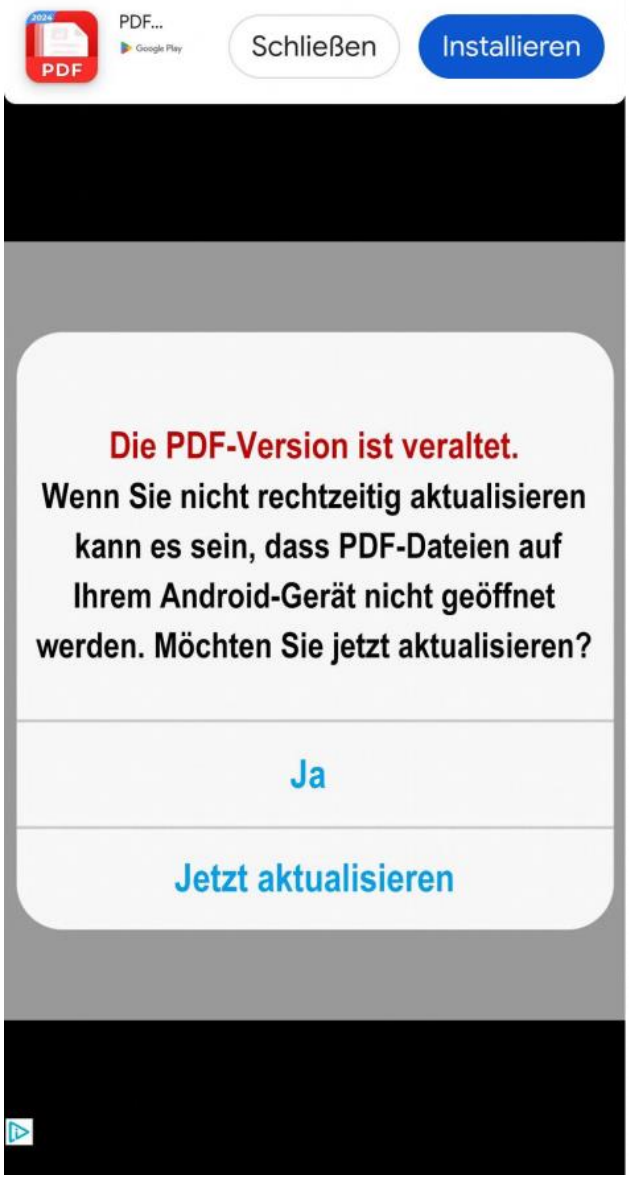
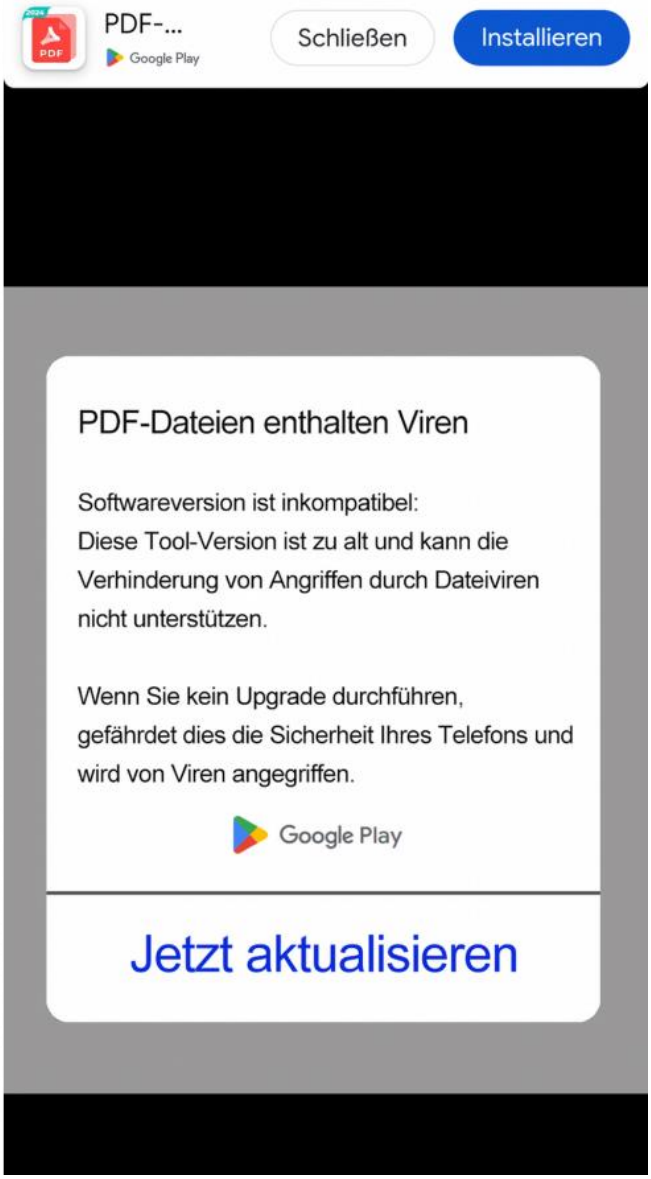
Neue Betrugsmasche am Smartphone

In letzter Zeit haben wir mehrere Zuschriften erhalten, in denen von sehr ähnlichen Betrugsversuchen am Smartphone berichtet wurde. Immer geht es dabei um **PDF-Dateien** und um Apps zum Anschauen von PDF-Dokumenten. Offenbar ist hier seit einigen Wochen eine neue Masche im Umlauf, die allerdings auf einem sehr alten und bekannten Vorgehen der Betrüger basiert: Es werden Werbeeinblendungen mit erfundenen Inhalten, die aussehen wie echte Handymeldungen, genutzt. Dieser Trick ist seit Jahren im Umlauf und hat immer wieder neue Auswüchse. In der aktuellen Welle geht es dabei um PDF-Dateien. Die Werbeanzeige erscheint bildschirmfüllend, was besonders ärgerlich ist. Dieses Problem tritt vor allem bei Android-Geräten auf.

Wir haben zwei Versionen dieses Betrugsversuchs zugeschickt bekommen:





Im ersten Fall wird behauptet, die PDF-Version sei veraltet. Damit soll suggeriert werden, unsere PDF-App, die wir zum Anschauen von PDF-Dateien verwenden, sei nicht mehr aktuell. Weiter heißt es: “Wenn Sie nicht rechtzeitig aktualisieren kann es sein, dass PDF-Dateien auf Ihrem Android-Gerät nicht geöffnet werden. Möchten Sie jetzt aktualisieren?” Zur Auswahl bekommt man “Ja” und “Jetzt aktualisieren”. Ein “Nein” oder “Später” gibt es nicht. All das zeigt bei genauerer

Betrachtung, dass es sich hierbei nicht um eine echte und seriöse Meldung handeln kann. Jede seriöse Meldung besitzt eine Option zum “Abbrechen” oder ein “Nein” zum Verhindern der Aktion. Mindestens ein “Später”, um den Vorgang zu verschieben, sollte vorhanden sein. Wenn diese Optionen fehlen, dann sind das klare Anzeichen eines Betrugs.
Am oberen Bildschirmrand wird zudem direkt die Installation einer (angeblichen) PDF-App angeboten, der Link führt in den Play Store von Google. Diese Anzeige, die auf Internetseiten und in werbefinanzierten Apps bildschirmfüllend auftauchen kann, macht sich Verschiedenes zunutze. Sie ist von der Gestaltung und vom Wortlaut aufgebaut wie eine Meldung, die auch von unserem Handy stammen könnte. Kaum jemand denkt daran, dass dies eigentlich eine ganze normale Werbung ist, über die man einfach hinweg schauen könnte. Weiterhin sind PDF-Dateien sehr übliche Dateien und fast jeder Mensch hat im Alltag mit PDF-Dateien zu tun. Fast niemand weiß aber genau, welche App denn eigentlich zum Öffnen der PDF-Dateien auf dem Smartphone genutzt wird, wie diese App heißt. Man weiß nur, dass PDFs wichtig sind und man sie braucht. Und dann kommt hinzu, dass von Experten immer zum regelmäßigen *Aktualisieren* von Apps geraten wird. Es wird immer empfohlen, Updates zu installieren, wenn sie verfügbar sind. Daher folgen viele Menschen dieser Aufforderung, obwohl es kein echtes Update/Aktualisierung ist, sondern eine Werbung, und stören sich auch nicht weiter am seltsamen Wortlaut. Aber: Hier wird nichts aktualisiert. Hier wird eine **ganz neue App** heruntergeladen. Und diese kann, direkt oder indirekt, Schaden auf dem Smartphone anrichten. Doch dazu später mehr.

Schauen wir uns noch kurz die zweite Meldung an: Auch hier soll angeblich die PDF-App aktualisiert werden. Diese Meldung ist aber noch etwas bedrohlicher, denn es wird in diesem Fall behautet, “PDF-Dateien enthalten Viren”. Ein Schutz dagegen sei aktuell nicht gewährleistet, deswegen solle man aktualisieren. Auch hier wird aber nichts aktualisiert, sondern es wird eine ganz neue App installiert, wenn man den Anweisungen folgt.
Bedenken Sie: Alles was in diesen Meldungen steht, ist frei erfunden. Es ist eine Werbung, in der eine App beworben wird, der “Werbetext” entspricht aber nicht einer klassischen Werbung, sondern suggeriert über erfundene Zusammenhänge eine Bedrohung. Wenn Sie auf “Installieren” tippen, so sind Sie selbst tätig geworden und haben eigenständig die potenziell schädliche App installiert. Der Betrug besteht hier also in erster Linie einmal darin, den Menschen zur Fehltat zu verführen. Der Mensch begeht selbst den Betrug an sich und seinem Smartphone, könnte man sagen. Ein Virenscanner oder andere Sicherheitsprogramme helfen in einem solchen Fall also nicht. Nur Verstand, Erfahrung und Aufmerksamkeit hilft.

Woher kommen diese Meldungen?
Häufig kommen diese Werbeanzeigen von Apps, die sogenannte Adware enthalten. Solche Apps tarnen sich oft als harmlose Anwendungen wie Spiele, Systemoptimierer oder wie in unserem Beispiel als PDF-Viewer. Aber auch Apps, die kostenfrei sind und sich über den Verkauf von Werbeanzeigen finanzieren, sind sehr oft davon betroffen. So kann beispielsweise Ihre seriöse und vertrauenswürdige Wetter-App, die normalerweise ganz alltägliche Werbeanzeigen von REWE oder AMAZON enthält, plötzlich eine solch unseriöse PDF-Betrug-Werbeanzeige enthalten. Auch das Besuchen von Webseiten kann dazu führen, dass solche Anzeigen plötzlich erscheinen. Diese Seiten nutzen Pop-ups oder Weiterleitungen, um betrügerische Warnungen anzuzeigen. Manchmal können auch Browser-Benachrichtigungen aktiviert sein, die durch das Akzeptieren einer Anfrage auf einer Webseite erscheinen. Diese können dann betrügerische Anzeigen an das Gerät senden. (Um diese dritte Ursache der Browser-Benachrichtigungen bei Android zu kontrollieren und auszuschalten, empfehlen wir unseren passenden Film: hier klicken.)

Was ist zu tun?
Wenn eine solche Meldung auf Ihrem Smartphone erscheint, lesen Sie aufmerksam und in Ruhe den Text. Häufig erkennt man schon am Wortlaut, dass hier etwas nicht stimmt. Eine App, die wirklich aktualisiert werden muss, meldet sich nicht bildschirmfüllend, während Sie gerade etwas anderes machen. Das Aktualisieren geschieht in der Regel ganz automatisch über den Play Store, im Hintergrund. Wenn eine solche Meldung bei Ihnen erscheint, schließen Sie die App, die Sie

gerade verwenden oder versuchen Sie, mit der Zurück-Taste Ihres Android Geräts die Einblendung zu verlassen. In sehr vielen Fällen gibt es am Rand, sehr versteckt, klein und kaum sichtbar, ein kleines X zum Schließen der Werbeanzeige. Jede Werbung **muss** nämlich eine Funktion zum Schließen enthalten. Dieses X taucht manchmal erst nach ein paar Sekunden auf. Oder es steht als Text am Rand “Schließen”. Fast immer übersieht man diese Option aber, weil sie durch die Betrüger versteckt wird.
Wie gesagt, in fast allen Fällen ist es eine Werbeanzeige, die irgendwo eine versteckte Option zum Schließen hat. Wenn es Ihnen trotzdem nicht gelingt, die Einblendung loszuwerden, schalten Sie das Gerät vollständig aus und danach wieder ein. Sofern die Werbung in Ihrem Browser angezeigt wird, schließen Sie den entsprechenden Tab oder den gesamten Browser. Löschen Sie danach am besten auch den Browserverlauf und die Cookies. Überprüfen Sie kürzlich installierte Apps. Schauen Sie sich die kürzlich installierten Apps an und deinstallieren Sie diejenigen, die verdächtig erscheinen oder unnötige Berechtigungen verlangen. Generell gilt: Installieren Sie niemals irgendwelche Apps, wenn Sie dazu per Meldung auf dem Smartphone aufgefordert werden. Am wichtigsten: Installieren Sie Apps immer nur direkt über den Play Store, die Sie selbst zuvor ausgesucht haben. Nie über Anzeigen und nie über eine fremde Internetseite.

Was kann passieren?
Angenommen, Sie haben eine App installiert, die Ihnen auf diese Weise untergejubelt wurde, was kann dann eigentlich schlimmstenfalls passieren? Was exakt im Einzelfall passiert, können wir nicht sagen, aber grundsätzlich gibt es drei verschiedene Szenarien, was bei solchen Apps passieren kann.
1. Die App ist fortan auf dem Smartphone installiert und könnte viele Werbeanzeigen enthalten, die entweder in der App selbst oder sogar außerhalb der App auf dem Homescreen oder Sperrbildschirm angezeigt werden. Sie werden dann zukünftig mit Werbung nahezu bombardiert. Solche Apps finanzieren sich durch aggressive Werbeplatzierung, was sehr nervig ist, aber immerhin keine direkte Gefahr für Ihr Smartphone oder Ihre persönlichen Daten darstellt. Zudem könnte es sein, dass die App gar keine echte Funktionalität hat. Es ist also möglich, dass die beworbene App eigentlich nutzlos ist. Sie könnte vorgeben, eine nützliche Funktion zu haben (z.B. ein “Systemoptimierer” oder ein PDF-Programm), bietet aber in Wahrheit keinerlei Mehrwert, sondern schaltet nur Werbung. Das ist sehr ärgerlich und sehr nervig, aber nicht *gefährlich*. Dieses Szenario ist am wahrscheinlichsten.
2. Einige betrügerische Apps fordern unnötig viele Berechtigungen an, etwa den Zugriff auf Kontakte, Nachrichten, den Standort oder sogar die Kamera. Dadurch könnten persönliche Daten ausgespäht, für Werbung missbraucht und an Dritte weitergegeben werden. Dies stellt eine Gefahr für Ihre Daten und Ihre Privatsphäre dar. Dieses Szenario ist nicht unwahrscheinlich.
3. Schlimmstenfalls handelt es sich bei der beworbenen App um eine sogenannte **Malware**. Diese könnte sensible Daten wie Passwörter, Bankinformationen oder Kreditkartendaten stehlen. Im Fall von sogenannter Ransomware könnten sogar Ihre Dateien verschlüsselt werden und Sie könnten gezwungen werden, Lösegeld zu zahlen, um wieder auf die Daten zugreifen zu können. Eine solche Situation kann nicht nur finanziellen Schaden verursachen, sondern auch die persönliche Sicherheit gefährden. Dieser Fall ist aber äußerst selten.
Selbstverständlich sind die Anbieter des App Stores bemüht, solche schädlichen Apps ausfindig zu machen und sofort aus dem App-Store zu entfernen. Dennoch gelingt es Betrügern immer wieder, gefährliche Apps in den Umlauf zu bringen. Daher der wichtige Tipp vor allem für Android-Nutzer, da hier diese Betrugsfälle wahrscheinlicher sind: Achten Sie darauf, Apps nur aus dem offiziellen **Google Play Store** zu installieren und überprüfen Sie vorher die Bewertungen und die angeforderten Berechtigungen der Apps. Installieren Sie bestenfalls keine unbekannten Apps, die nur sehr wenige oder nur sehr schlechte Bewertungen haben.

Quelle: https://levato.de/neue-betrugsmasche-am-smartphone/?utm_source=mailpoet&utm_medium=email&utm_source_platform=mailpoet&utm_campaign=Neue%20Betrugsmasche%20am%20Smartphone