数百万のアプリのために信頼できるエコシステムを築く

サイドローディングの脅威分析

2021年10月

重要な洞察

iPhoneは、ユーザーが非常に機密性の高い個人情報を保存する場所であり、極めてパーソナルなデバイスです。したがって、iOSのエコシステム上でセキュリティとプライバシーが保護されていることはユーザーにとって極めて重要になります。しかし、App Store以外の場所でアプリの直接ダウンロードや第三者アプリストアを通じてアプリを配信する、「サイドローディング」と呼ばれるプロセスに対応するようAppleに求めるユーザーもいます。**アプリの直接ダウンロードや第三者アプリストアを通じたサイドローディングに対応すると、これまでiPhoneを安全に保ってきたプライバシーとセキュリティの保護機能が損なわれ、ユーザーを深刻なセキュリティのリスクにさらすことになります。**

モバイルマルウェアとそれにより生じるセキュリティとプライバシーへの脅威は増加しつつあり、その大部分がサイドローディングを許可するプラットフォーム上で発生しています。

15〜47倍
感染が増加

ヨーロッパの規制当局の報告によると、**マルウェアへの新規感染が毎日23万件発生しています。**

過去4年間にわたり、**Androidデバイスでは、iPhoneと比較して15〜47倍多いマルウェア感染が見つかっています。**

ある大手セキュリティ企業は、顧客のAndroidモバイルデバイス全体で**1か月におよそ600万件の攻撃を検知しました。**

モバイルマルウェアは、消費者、企業、デベロッパ、広告主に被害を与えます。ユーザーへの攻撃には様々な手法や技術が使われています。消費者に影響を与える一般的なタイプのモバイルマルウェアには、アドウェア、ランサムウェア、スパイウェアや、正規のアプリになりすまして銀行口座などへのログイン用認証情報を盗み取るトロイの木馬があります。サイバー犯罪者は多くの場合、ソーシャルエンジニアリングやサプライチェーン攻撃を通じて標的に到達するほか、人気のソーシャルメディアネットワークを利用して詐欺行為や攻撃を拡散することもあり、その大半が、悪質なアプリの拡散に第三者アプリストアや直接ダウンロードを利用しています。デベロッパと広告主もこのような攻撃の被害を受けており、被害のほとんどは著作権の侵害、知的財産の窃盗、広告収入の損失によるものです。

Appleがサイドローディングに対応せざるを得なくなったら...

- **サイドローディングが第三者アプリストアにのみ限定されるとしても、サイバー犯罪者はユーザーを標的にしやすくなり、より多くの有害なアプリがユーザーのもとに届きます。**第三者アプリストアには、大量のマルウェアとそれによって生じるセキュリティとプライバシーへの脅威が存在することから、このようなストアには既知のマルウェアを含むアプリ、ユーザーのプライバシーを侵害するアプリ、模倣アプリ、違法または不適切なコンテンツを含むアプリ、子どもを標的とした安全ではないアプリをチェックするための十分な審査手順がないことがわかります。そのため、サイドローディングしたアプリが安全かどうかを判断する責任をユーザー自身が負うことになります。しかし、その判断は専門家でさえ難しいものです。めったにないことですが、App Storeで不正なアプリや悪質なアプリが公開された場合、Appleは発見し次第すぐに削除し、それ以降のバージョンや亜種があればすべてブロックして、ほかのユーザーへの拡散を防ぎます。第三者アプリストアでのサイドローディングに対応すると、悪質なアプリはいとも簡単に第三者アプリストアへと移動し、消費者向けデバイスを感染し続けるでしょう。

- **ユーザーはアプリに関する十分な情報を事前に得られず、デバイスにアプリをダウンロードした後も、それらのアプリをコントロールしづらくなります。**ユーザーは第三者アプリストアや直接ダウンロードを介してサイドローディングするアプリについての正確な情報を得られないかもしれません。なぜなら、これらのアプリストアでは、App Storeの製品ページやプライバシーラベルに表示されるような情報を提示する義務がないからです。また、それらのアプリがアクセス可能なiPhoneのデータ、ハードウェア、サービス（デバイスの位置情報、マイク、カメラなど）をユーザー自身がコントロールできる「アプリのトラッキングの透明性」やペアレンタルコントロールのような機能がなかったり、あったとしても、悪意のある人たちがその機能を簡単に操作できたりする可能性があります。デジタル広告に依存している大企業はこのようなプライバシー保護機能によって収益が損なわれていると主張しており、特にこれらの保護機能を迂回するために、サイドローディングによって自社のアプリを配信するインセンティブが働いているかもしれません。このようにして、iOSプラットフォーム上のプライバシーが損なわれることになります。

- **サイドローディングの実行時に、特許で保護されたハードウェア要素や非公開のオペレーティングシステム機能への第三者のアクセスに対する保護機能を無効にするよう求められることもあります。**これにより、マルウェアや侵入、さらにはデバイスの信頼性に影響を与えて機能できないようにする操作の無効化などからオペレーティングシステムやiPhoneのデータとサービスを保護しているプラットフォームセキュリティの主要コンポーネントが損なわれます。これによりサイバー犯罪者がより簡単にユーザーのデバイスをひそかに監視し、データを盗めるようになる可能性があります。

サイドローディングに対応した場合、サイドローディングを望まず、App Storeからのみアプリをダウンロードすることを望んでいるユーザーにも被害が生じます。

- **ユーザーは、仕事や学校で必要なアプリをサイドローディングするよう強いられる可能性があります。**また、家族や友人とつながるために必要なアプリがApp Storeで入手できないため、そのアプリをサイドローディングするしかない場合もあるかもしれません。例えば、サイドローディングを許可すると、企業によっては自社のアプリをApp Store以外の場所でのみ配信することを選択するかもしれません。
- **サイバー犯罪者がApp Storeの見た目をまねたり、サービスや特別な機能を無料または追加で利用できると宣伝したりしてユーザーを騙し、アプリをサイドローディングさせる場合があります。**

Appleは、App Storeでの公開前にすべてのアプリを審査して、アプリにマルウェアが含まれておらず、ユーザーに正確な情報が示されていることを確認し、アプリが有害だと判明した場合にはApp Storeから速やかにそのアプリを削除してそれ以降のバージョンや亜種が拡散されないようにすることで、エコシステムのセキュリティを保護しています。**直接ダウンロードと第三者アプリストアのどちらを利用する場合も、サイドローディングはAppleのセキュリティとプライバシーの保護機能を損ない、ユーザーのセキュリティとプライバシーに最善の利益をもたらしません。**

「私たちは2つの正反対のことを、同時にしようとしています。先進的でオープンなプラットフォームをデベロッパに提供しながら、iPhoneユーザーをウイルスやマルウェア、プライバシー攻撃などから守ろうとしているのです。これは簡単なことではありません」

スティーブ・ジョブス、2007年10月17日

目次

モバイル脅威の現状	7
一般的な消費者を狙うモバイルマルウェアの概要	10
モバイルマルウェア攻撃がユーザーのデバイスにアクセスする手口	17
エコシステムをオープンにすることのリスク	19
App Store以外でアプリを配信するための制約のある仕組み	20
サイドローディングがiOSのエコシステムに及ぼす影響	22
サイドローディングとiOSユーザー	27
セキュリティ専門家からのアドバイス	28

iPhoneが開発された当時、世界で最も重要なコンピューティングツールであるパソコンはウイルスにむしばまれていました。パソコンユーザーには深刻な信頼性の問題が頻繁に起きていました。ソフトウェアをダウンロードしたり、ウェブサイトにアクセスしたりすると、パソコンがマルウェアに感染してしまうことがあったからです。Appleは知識と目的を持って、iPhoneが、ユーザーが非常に機密性の高い個人情報を保存する場所として極めてパーソナルなデバイスとなるように、また、パソコンよりもはるかに規模が大きく多様なユーザーベースによって利用されるように設計しました。ユーザーがどこにでも持ち歩き、緊急時には頼れるものにすること。iPhoneがパソコンと同じ運命を辿ることは許されず、パソコンとは違うものである必要がありました。

ユーザーに信頼性とセキュリティをもたらしながら、サードパーティデベロッパがアプリを作成して配信できるプラットフォームを確立するために、Appleは業界をリードするセキュリティ保護機能をiPhoneに組み込み、App Storeという、ユーザーが審査済みの第三者アプリを安全にダウンロードできる信頼のおける場所を構築したのです。このアプローチは高い効果を発揮し、ユーザーがiPhone上でマルウェアに遭遇することは極めて稀です。しかし、App Store以外の場所でアプリの直接ダウンロードや第三者アプリストアを通じてアプリを配信する、「サイドローディング」と呼ばれるプロセスに対応するようAppleに求めるユーザーもいます。サイドローディングに対応すると、iOSプラットフォームのプライバシーとセキュリティの保護機能が損なわれ、ユーザーを深刻なセキュリティのリスクにさらすことになります。

iPhoneでサイドローディングを行うと、サイバー犯罪者に機会を与えることになります。サイドローディングがもたらす新たな機会や配信経路を逃すまいと、悪意のある人たちによるiPhoneユーザーを攻撃するためのツールとノウハウの開発に拍車がかかるでしょう。マルウェア攻撃のリスクの増加により、App Storeでしかアプリをダウンロードしないユーザーも含めて、あらゆるユーザーがより大きな危険にさらされます。つまり、サイドローディングはユーザーの最善の利益にはなりません。デベロッパにも害が及びます。サイドローディングの脅威の高まりにより、エコシステムに対するユーザーの信頼が損なわれ、その結果、多くのユーザーが少数のデベロッパからのより限られたアプリしかダウンロードしなくなり、アプリ内での購入の回数も減ります。**また、デベロッパは、偽アプリや模倣アプリ、海賊版アプリの蔓延による被害も受けることになります。**

---

iPhoneを使うある家族の日常がサイドローディングによってどのように変化するかを、Appleが2021年6月に公開した白書「**数百万のアプリのために信頼できるエコシステムを築く：App Storeの保護が果たす重要な役割**」でご覧ください。

モバイル脅威の現状

モバイルセキュリティへの脅威は増加しつつあり、特にサイドローディングに対応するプラットフォームで顕著です。欧州ネットワーク・情報セキュリティ機関（ENISA）の報告によると、2019年と2020年初めに、マルウェアへの新規感染は1日23万件（年換算では8,400万件）検知されています[1]。ヨーロッパ最大のサイバーセキュリティサービスプロバイダであるKaspersky Labは、2020年、顧客の所有するAndroidモバイルデバイスに影響を与えた攻撃が月におよそ600万件あったと推計しています[2、3]。

このような脅威は、その大部分がサイドローディングに対応しているプラットフォームで発生しています。最近の調査では、サイドローディングに対応するプラットフォームであるAndroidを搭載しているデバイスは、iPhoneより15～47倍多く悪質なソフトウェアに感染していると推計されています[4、5]。

セキュリティの脅威を含むモバイルアプリは深刻なリスクをもたらします[4、6]。その結果、消費者にセキュリティの脅威が届かないよう、当事者のアプリストア（iOSデバイスのApp StoreやAndroidデバイスのGoogle Playなど）におけるアプリの審査プロセスが必須となり、より一層厳密に行われるようになりました。しかし、ユーザーが第三者アプリストアや直接ダウンロードによりアプリをサイドローディングした場合、このようなアプリの審査による保護が十分とは限らず、まったく保護されないこともあります。

マルウェアに感染したモバイルアプリは、モバイルエコシステム内のすべての関係者をリスクにさらします。多くの場合、主な標的は消費者ですが、マルウェア攻撃は、デベロッパ、オンライン広告主、さらにはモバイルアプリのエコシステムに直接関わりのない企業にまで被害を与え、危険にさらします。マルウェア攻撃の被害者となった消費者は、サイバー犯罪者に騙されて、プライバシーや機密性の高いデータを侵害され、攻撃によって生じた影響への対応に時間やエネルギーを費やすことになります[7]。また、マルウェアに感染したモバイルアプリが複雑な多段階攻撃の足掛かりとなり、サイバー犯罪者が被害者の金融資産を標的にして様々な攻撃を仕掛けることもよくあります[8、9、10]。サイドローディングに対応するプラットフォームでは、この問題を食い止めるために多くの消費者がデバイスにウイルス対策サービスを追加する必要があり、そのサービスにかかる費用は年間34億ドルにものぼります。2021年、全世界で13億台のスマートフォンにセキュリティソリューションが備わっていると推定され、これは2016年の4倍の数です[11]。しかし、サイバー犯罪者たちは常に一歩先を行っていることからウイルス対策サービスは、増加するマルウェアの問題に対する不十分なその場しのぎの解決策でしかありません[12]。

個人のモバイルデバイスに感染するよう設計されたマルウェアは、企業データや企業ネットワークにも影響を与える可能性があります。ハッカーが企業を攻撃する方法は様々です。例えば、フィッシングを使ったり、パッチが適用されていないシステムを攻撃したりしますが、モバイルマルウェアはその新たな手段となっています[13、14、15]。世界中の多くの企業が、社員に自社のネットワーク上で個人のデバイスを使うことを推奨するBYOD（個人所有デバイスの持ち込み）ポリシーを採用している状況においては、モバイルマルウェア攻撃は、悪意のある人たちに企業のネットワークに直接アクセスする経路を与えることができ、モバイルデバイスを標的とした脅威が増加する一因となっています[16、17、18]。多くのITやセキュリティの専門家は、特定のデータ漏えいの原因はモバイルデバイス上にある機密性の高い企業情報を社員が保護できなかったためだと考えており、企業データの漏えいに関するある研究では、Androidアプリがマルウェアを配布する方法の1つであることがわかりました[10、19]。悪意のある人たちが企業のネットワークにアクセスできるようになると、ランサムウェア、データ窃盗、ネットワークのコントロールの喪失など、企業はあらゆるタイプの攻撃やセキュリティのリスクに直面することになり、そのすべてが顧客の信頼喪失と訴訟につながる可能性があります[20]。

マルウェア攻撃により生じる企業のコスト

様々な要因がありますが、モバイルアプリ経由で発生するマルウェア攻撃により、企業は高額のコストに直面しています。

たった1台のモバイルデバイスがマルウェアに感染した場合、**企業にかかる平均的なコストは約1万ドルになります**[19]。

米国企業1,800社のうち、**46パーセントには、少なくとも1人の社員が悪質なモバイルアプリをダウンロードして**企業のネットワークとデータを脅威にさらした事例があります[21]。

データ漏えい

モバイルアプリのマルウェアによってデータ漏えいが発生した場合、企業には平均して**回の漏えいごとに平均400万ドル以上**、最大で**5,000万ドル**のコストがかかると推定されます[19、22]。

ビジネス機会の損失

その400万ドルのうち、**150万ドル以上**がビジネス機会の損失によるものです。このコストには、評判の悪化が含まれ、企業が新規顧客を獲得するのをさらに難しくします[22]。

ランサムウェア

フランス、スペイン、ドイツなどのヨーロッパの国々で調査の対象となった企業の半数以上が、2019年にランサムウェアの攻撃を経験しています。モバイルマルウェア経由で発生する可能性のあるランサムウェア攻撃に対処する場合、企業には平均**75万ドル以上**のコストがかかります[23]。

デベロッパや広告主もサイバー犯罪者の被害を受けます。アプリの著作権の侵害では、サイバー犯罪者は主に第三者提供元（第三者アプリストアを含む）を通じて別のデベロッパのアプリを不法に配信し、その結果、デベロッパはそのアプリの収益を失います[24、25]。サイバー犯罪者は、アプリ内での購入や広告など、デベロッパが収益を得るための収益化ツールを削除したり置き換えたりすることがあります。ほかのケースでは、悪意のある人たちが別のデベロッパのデザイン、ブランド、コンテンツを模倣し、盗んだ知的財産で利益を上げています[26、27]。つまり、アプリの著作権の侵害や知的財産の窃盗により、デベロッパの収益が奪われるのです。例えば、一部のゲームデベロッパによると、Androidデバイスにインストールされている彼らのアプリの90パーセントは海賊版であり、それに対する収益はまったく得られていないと報告されています[24、25]。サイバー犯罪者が有料ゲームを標的にし、「モニュメントバレー」、「グランド・セフト・オート」シリーズ、「Alto's Adventure」のような大ヒットゲームの海賊版を作成して利益を上げることがよくあります[24、25]。

サイバー犯罪者やハッカーが主にサイドローディングされたアプリを通じて実行するクリック詐欺やアドスタッキングなどの技術を使うと、広告主もモバイルマルウェアの被害を受けます[28]。クリック詐欺のマルウェアは、広告を含むウェブページに自動的にアクセスさせたり、広告を自動的にクリックしたりして、広告の表示回数やクリック回数で利益を得ます[29]。アドスタッキングの場合、ユーザーには一番上の広告しか見えませんが、マルウェアが1つの広告の上に複数の広告を重ねて配置しているため、広告主はすべての広告に対して不正な請求を受けます[30]。水増しされた不正な広告アクセスにより正規の広告主が受ける損害は、何十億ドルにものぼると推計されています[30、31]。

新型コロナウイルスのパンデミックによりモバイルデバイスの利用がさらに促進されたため、モバイルユーザーに対する脅威が一段と悪化しています。例えば、消費者は個人の健康に関する情報をデバイスに保存することが増えましたが、これはハッカーが複数の買い手に売却できる価値あるデータです[32、33]。リモートワークに対応するために、BYODポリシーに頼る企業も増えています[17]。このような動向が悪意のある人たちにさらなる機会をもたらし、モバイルユーザーへの脅威が増加しました。例えば、偽のメッセージを使ってユーザーを騙し、機密性の高い情報を提供させたり、マルウェアをダウンロードさせたりする「モバイルフィッシング」は37パーセント増加しています[34]。ハッカーは新型コロナウイルス感染症に関連するアプリやリソースに悪質なマルウェアを埋め込んでいます[35]。また、ヘルスケア関連のネットワークでは、モバイルデバイス、タブレット、パソコン全体で、ユーザー1人あたりの新型コロナウイルス関連のマルウェア攻撃が通常のネットワークより15パーセント多く発生しています[34]。

一般的な消費者を狙うモバイルマルウェアの概要

消費者を標的にしたモバイルマルウェア攻撃にはいくつもの形態があり、様々な手法や技術が使われています。消費者に影響を与える最も一般的なタイプのモバイルマルウェアには、アドウェア、ランサムウェア、スパイウェアや、正規のアプリになりすまして銀行口座などへのログイン用認証情報を盗み取るトロイの木馬があります。(以下の概要を参照)デバイスにアクセスできるようになると、攻撃者は多くの場合、複数の手法を使って標的を搾取します。例えば、アドウェアとスパイウェアの両方を使ってデバイスを感染させることがあります。

一般的な消費者を狙うモバイルマルウェアの概要

	 アドウェア	 ランサムウェア	 消費者を狙ったスパイウェア	 銀行口座などへのログイン用認証情報を盗み取るトロイの木馬
目的	ユーザーに執拗に(または不正に)広告を表示することにより広告収入を獲得	乗っ取ったデバイスの「解放」を約束する代わりに、感染したユーザーから金銭を搾取	ユーザーを標的にするためにデータを利用 ハッカーにデータを売却 同意を得ずに、親密なパートナーを監視(IPS)	銀行口座などへのログイン用認証情報を盗み取るためにデバイスにアクセス
ユーザーへの影響	煩わしい、過度に表示されるポップアップ広告 デバイスのパフォーマンスへの悪影響	デバイスや重要なファイルへのアクセスを喪失 データの喪失 ユーザーが身代金を支払った場合の経済的な損失	ユーザーのプライバシーを侵害 IPSの場合:虐待を可能にし、身体的および精神的な危害を与える可能性	認証情報の盗難(銀行口座へのログイン、ソーシャルメディアアカウントへのログインなど) 盗まれた認証情報を利用した被害(不正使用など)

注意:この表は、Kaspersky Lab、Malwarebytes、WeLiveSecurity(ESET)、Norton、Nokiaなどのサイバーセキュリティ企業と、欧州ネットワーク・情報セキュリティ機関(ENISA)などの政府機関によって提案された分類を反映しています。

アドウェア。モバイル攻撃の半数以上に含まれ、広告収入を得るため、ユーザーに過度に広告を表示します[36、37、38]。アドウェアはアプリを通じてモバイルデバイスに侵入し、ポップアップやリダイレクト、クリッカー型トロイの木馬、不要なインストールを実行する可能性があります[39]。

アドウェアのその他の例

サイドローディングされたAndroid向けトロイの木馬であるFakeAdsBlockは、正規のアドブロッカーを装い、ポップアップとリダイレクトでデバイスの使用を妨げます。削除は非常に困難です[40]。

Android.Click.312.originはクリッカー型トロイの木馬で、多くの正規アプリに埋め込まれています。アプリ上で広告を表示し、ユーザーが気づかない間にウェブサイトを読み込むことができます[41]。

CopyCatは、Androidデバイスをアドウェアや、root権限を奪うマルウェアに感染させます。第三者アプリストアで公開されている、人気のアプリを改ざんしたコピーを介して拡散します[42]。2016年の2か月間で、世界中の1,400万台を超えるAndroidデバイスがCopyCatマルウェアに感染しました[43]。

HiddenAds：無料のアプリやゲームに隠れて、煩わしい広告を表示するアドウェア

標的

2020年に発見されて以来、3万を超えるHiddenAdsによる攻撃が記録されており、世界中のユーザーに影響を与えています。

ユーザーのデバイスへの侵入方法

HiddenAdsアドウェアに感染したアプリは、人気の写真加工アプリ「FaceApp」やゲーム「Call of Duty」の偽バージョンなど、本物のAndroidアプリになりすましています[37]。YouTubeビデオでこれらの偽アプリを正規アプリの無料版として宣伝し、ダウンロード用リンクを掲載しています。

挙動

HiddenAdsはデバイスのブラウザに様々なポップアップ広告やウェブサイトへのリダイレクトを表示し、悪意のある人たちに広告収入をもたらします。

潜伏方法

インストールされると、アプリは偽の設定アイコンとして表示されます。このアイコンは、アドウェアがまだバックグラウンドで実行中であっても表示されなくなることがあります。

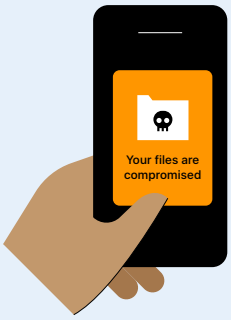
ランサムウェア。もう1つの一般的なタイプのモバイルセキュリティ攻撃は、ランサムウェアです。通常は個人を標的とし、デバイスのインターフェイスをブロックして、身代金が支払われるまで使えないようにするか、デバイス上のファイルを暗号化して支払いが行われた後にのみ復号化します[44、45]。ランサムウェアを使用するサイバー犯罪者は多くの場合、機密性の高いデータを盗み、それを拡散すると脅します[46]。2020年には、米国だけで420万を超えるモバイルユーザーがモバイル向けランサムウェア攻撃の被害を受けています[47、48]。新型コロナウイルスのパンデミックに加えて、サイバー犯罪者が追跡されずに取引できる暗号通貨の台頭により、このような攻撃はさらに増加しています[34、47、49、50]。

ランサムウェアのその他の例

Fusobランサムウェア型トロイの木馬は、デバイスをロックし、通話履歴や位置情報履歴など、機密性の高いデータを盗むよう設計されています。これらのトロイの木馬はヨーロッパと米国のユーザーを標的にしています[53、54]。

Android向けマルウェアの一種であるMalLocker.Bは、サイドローディング経由で配布されます。あらゆるアプリのウインドウに身代金に関するメッセージを表示し、標的がそのスマートフォンのその他すべての機能を使えないようにします[55、56]。

CryCryptor：公式の新型コロナウイルス感染症の接触追跡アプリに偽装し、ユーザーのファイルを暗号化するランサムウェア



CryCryptorランサムウェアは、政府機関であるカナダ保健省が提供した公式の新型コロナウイルス感染症の接触追跡アプリに偽装しており、ユーザーを騙してサイドローディングさせます。このアプリをインストールすると、CryCryptorはデバイス上のファイルを暗号化し、身代金の支払いとファイルの復元に進むための連絡先のEメールアドレスを表示します[51、52]。

標的

CryCryptorはカナダのAndroidユーザーを標的にしています。

ユーザーのデバイスへの侵入方法

2020年6月、カナダ政府が新型コロナウイルス感染症の接触追跡アプリを公開する計画を発表してからわずか数日で、CryCryptorの背後にいるサイバー犯罪者はランサムウェアアプリの提供の場として、カナダ保健省の偽のウェブサイトを2つ作成しました。新型コロナウイルス感染症が蔓延する中、人々の焦りや不安に付け込み、Androidユーザーを騙して、これらの偽のウェブサイトからCryCryptorをサイドローディングさせました。

挙動

CryCryptorは、オープンソースのランサムウェアであるCryDroidをもとに開発されました。ダウンロードすると、CryCryptorはそのAndroidデバイス上のファイルにアクセスする許可を求めます。次に、マルウェアが、写真、ビデオ、PDFなど、一般的なファイルタイプを暗号化します。暗号化された各ファイルのディレクトリに、支払いとファイルの復元について連絡するためのEメールアドレスが記載された身代金要求のメッセージが添付されます。

消費者を狙ったスパイウェア。スパイウェアはデバイスのユーザーを監視し、メッセージ、写真、ビデオなど機密性の高い情報を盗みます[57]。スパイウェアは個人（個人情報の盗難やストーカー行為など）と企業や組織（産業スパイ活動など）の両方に被害を与える可能性があります[58]。特定の侵入方法を持つスパイウェアは、デバイスのマイクやカメラに直接アクセスできます[59、60]。消費者を狙ったスパイウェアは、国家が諜報機関を通じて実行する、非常に巧妙で標的を絞ったスパイウェアとは別のものです。国家により開発または支援されるスパイウェアとは異なり、消費者を狙ったスパイウェアは幅広いユーザーを標的とするよう設計され、比較的安価に作成されて、サイドローディングに対応するプラットフォームで配布されます。2020年、Android向けマルウェア攻撃全体の3分の1がスパイウェアに関連していました[4]。

スパイウェアは、虐待者が親密なパートナーとそのモバイルデバイスを監視する目的でも使われています。このようなソフトウェアを含むアプリは**ストーカーウェア**と呼ばれ、位置情報、メッセージ、Eメール、写真などを追跡し、デバイスのカメラにリアルタイムでアクセスするために使用されます。このようなアプリの使用は、ハラスメント、ストーカー行為、同居パートナーへの暴力行為などに関連しています。過去数年間にわたり、FTCはストーカーや同居パートナーへの虐待者がAndroidデバイスを使って被害者を追跡できるようにするストーカーウェアについて、販売者である米国企業2社に措置を講じてきました[61、62]。どちらの事例でも、これらのアプリはGoogle Playで配信されていませんでしたが、虐待者は被害者のデバイス上にアプリをサイドローディングすることができていました。そのため、アプリの配信を止めるにはFTCの介入が不可欠だったのです[61、63]。

スパイウェアの例

FluBotはスパイウェアの一種で、動作と拡散方法がFakeSpyと非常によく似ています。（以下を参照）FluBotは、ヨーロッパ全体でDHLの荷物追跡アプリを装い、特に英国とフィンランドを攻撃対象としています[68、69]。

SpyNoteはサイドローディング経由で拡散される、Netflixの偽バージョンです。デバイスのマイク、連絡先、メッセージを乗っ取ります[70]。

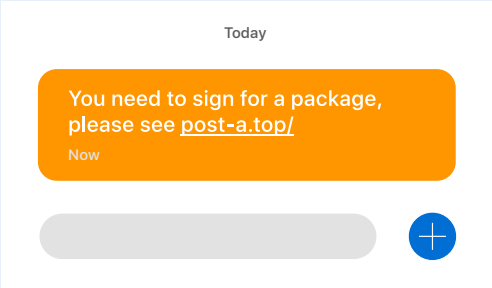
HelloSpyは、サイドローディングでのみ入手できるストーカーウェアの一種で、標的のGPS位置情報、通話、メッセージ、写真、ビデオ、その他のデータを記録します[71]。「配偶者の浮気の証拠をつかもう」という名目で市場に出回っています[72]。

Kaspersky Labは、2020年に**5万人以上のユーザーがストーカーウェアの影響を受けたことを明らかにしました**[65]。

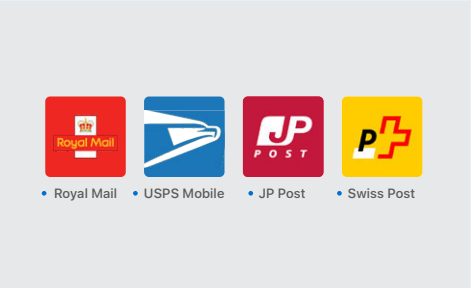
ある調査によると、**虐待者の半数以上がストーカーウェアアプリを使って被害者の携帯電話を追跡していた**ことがわかりました[64]。

ストーカーウェアの大半は当事者によるアプリストア以外で配信されています[65]。

FakeSpy：偽の宅配便メッセージを装ってユーザーの行動を探り、データを盗むマルウェア



↳ 偽のメッセージによりユーザーを騙して、不正な郵便サービスアプリ経由でFakeSpyをサイドローディングさせようとします。



↳ FakeSpyアプリのアイコンは、このような世界中の正規の郵便サービスのアイコンを模倣しています。

FakeSpyはSMSフィッシングを使って人々を騙し、正規の郵便サービスアプリになりすましたAndroidアプリをサイドローディングさせようとします。ダウンロードすると、デバイスから機密性の高い情報を盗みます[66、67]。

FakeSpyは新たな迂回方法やスパイ行為機能を身につけて、ますます進化しています。FakeSpyは、感染したユーザーの連絡先リストにSMSフィッシングのメッセージを送信することで増殖します[66]。また、新たなユーザー集団を標的とするために世界中でより多くの正規の郵便サービスになりすまし、拡大を続けています。

標的

特に、フランス、スイス、ドイツ、英国、米国、日本、台湾のAndroidユーザー。

ユーザーのデバイスへの侵入方法

標的となるユーザーは郵便サービスを名乗るテキストメッセージを受け取り、荷物の配達予定があるため、その追跡をするか、署名をする必要があると伝えられます。このメッセージにはウェブサイトへのリンクが含まれており、ユーザーは偽の配達状況追跡アプリをサイドローディングするよう促されます。FakeSpyは、フランス（フランス郵政公社）、スイス（スイスポスト）、ドイツ（ドイツポストDHL）、英国（ロイヤルメール）、米国（USPS）、日本（日本郵便）、台湾（中華郵政）の郵便サービスになりすましています。被害者になりそうなユーザーを騙すために、サイドローディングされたアプリのアイコンは、これらの公式な郵便サービスのいずれかの公式アプリのアイコンに似ています。

挙動

ユーザーがアプリをサイドローディングすると、テキストメッセージ、連絡先リスト、通話記録、ネットワーク情報、最近実行したタスク、ほかのアプリに関する情報などを取得する許可を求められます。

潜伏方法

アプリを起動すると、マルウェアであることに気づかれないように、本物の郵便サービスのウェブサイトにユーザーをリダイレクトして騙そうとします。

銀行口座などへのログイン用認証情報を盗み取るトロイの木馬。よくあるモバイルマルウェアのタイプとして、銀行口座などへのログイン用認証情報を盗み取るトロイの木馬があります。正規のアプリに偽装し、ユーザーの銀行口座、政府関連のアカウント、ソーシャルメディアアカウントなどへのログイン用認証情報を盗もうとします。一部のバンキング型トロイの木馬には、2ファクタ認証によるセキュリティ対策を迂回する機能があります[73]。バンキング型トロイの木馬の目的は、最終的には認証情報を盗み、標的の銀行口座からお金を盗むことです[74]。バンキング型トロイの木馬は、最も頻繁にサイドローディングされています[74]。

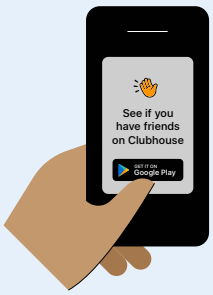
銀行口座などへのログイン用認証情報を盗み取るトロイの木馬のその他の例

Android向けトロイの木馬であるBanker.BRは、スペインとポルトガルで、**画面オーバーレイを利用して銀行口座に関する情報を盗みます**[77]。

バンキング型トロイの木馬のTeaBotは、西欧で様々な人気アプリになりすまし、銀行口座に関する情報を盗んでデバイスへのリモートアクセスを手に入れています[78、79]。

2017年以来、バンキング型トロイの木馬のAnubisは、300を超える金融機関のアプリやその他のアプリを装っています[80]。このアプリは、インストールされてアクティベーションされると、悪質なコマンドを実行可能にするための不要な許可を求めてきます。マルウェアの大半は、人々を騙して銀行口座情報を提供させるためにフィッシングを利用しています。

BlackRock：ログイン用認証情報を盗むために、Clubhouseアプリに偽装したAndroid向けトロイの木馬



BlackRockは、450を超えるオンラインサービスからログイン用認証情報を盗むAndroid向けトロイの木馬で、Clubhouseアプリを装ってユーザーにアプリをサイドローディングさせようとします[75、76]。

標的

ヨーロッパと世界のその他の地域のAndroidユーザー

ユーザーのデバイスへの侵入方法

BlackRockは、Clubhouseのウェブサイトのなりすましを通じて拡散されます。ユーザーが「Google Playで手に入れよう」をクリックすると、トロイの木馬が自動的にダウンロードされます。

挙動

トロイの木馬はGoogleアップデートを装い、アクセシビリティサービスへのアクセス権を要求してきます。このアクセス権があると、さらなるアクセス権を自ら供与し、ユーザーの同意を求めずに動作できるようになります[76]。BBVA、ロイズ銀行、Facebookなど、標的となるアプリのいずれかをユーザーが次回開くと、トロイの木馬がアプリのインターフェイス上に画面オーバーレイのウインドウを表示し、ユーザーが入力するログイン情報を記録します。トロイの木馬はテキストメッセージにアクセスできるので、2ファクタ認証を突破することができます。

潜伏方法

このトロイの木馬はデバイス上で最初に起動した際に、ユーザーから見えないように自らのアプリアイコンを非表示にします。

その他の形態のマルウェア。よく知られた形態のその他のマルウェアは、消費者を狙ったマルウェアと似ている部分もありますが、通常はモバイルアプリ経由で拡散されることはなく、一般の消費者を標的としていません。

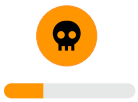
- **国家によるスパイウェア**は、国家レベルの主体者により、諜報機関や民間の請負人を通じて開発または支援されます。多くの場合、国家の諜報活動の推進や、国家の安全保障を目的としています。消費者を狙うスパイウェアとは異なり、国家によるスパイウェアは非常に巧妙で、多額の開発費が投じられており、通常はアプリ経由で配布されず、特定の個人を標的にするために使われます[81、82、83]。

- **企業向けランサムウェア**が発動するのは、犯罪者が企業のネットワークを乗っ取り、アクセスの復旧や、サイバー犯罪者が被害者のネットワークから盗んだ機密性の高いデータを公開しないことと引き換えに、影響を受けた企業に身代金を要求する時です[84]。企業向けランサムウェアは、消費者のデバイスや個人データが人質になるモバイルランサムウェア攻撃とは異なりますが、社員のモバイルデバイスが企業を標的とするサイバー犯罪者の侵入経路となる可能性があります。

モバイルマルウェア攻撃がユーザーのデバイスにアクセスする手口

サイバー犯罪者やハッカーは、第三者アプリストアやウェブサイトでの直接ダウンロード経由、さらにはEメールの添付ファイルとしてマルウェアをユーザーに配布する可能性があります[8]。以下で説明しているように、大部分のマルウェア(99パーセント以上)はサイドローディングされたアプリからもたらされます。App Storeのような当事者によるストアには、そのような配布手段ではユーザーを標的にできない保護機能があるからです。**マルウェア攻撃が標的に到達する最も一般的な方法は、ソーシャルエンジニアリングまたはなりすましです。**ユーザーの信頼を得てデバイスにアクセスするために、詐欺や人を操る手口を使います。ある研究によると、すべてのサイバー攻撃のうち、98パーセントがソーシャルエンジニアリングを使用しています[18]。人々の友人や家族に対する信頼をハッカーが悪用し、ソーシャルメディアネットワークを使って詐欺行為や攻撃を拡散することもあります[85、86]。ユーザーの信頼を得ようとするなりすまし攻撃には様々な方法があり、サイドローディングしたアプリを通じて発生する可能性が高くなっています。

模倣アプリ(偽アプリ)は、ほかのアプリの名称、インターフェイス、機能を模倣して、そのアプリの一部のユーザーを獲得します[87、88]。Netflix、Candy Crush Saga、Clubhouseなど、人気の(かつ正規の)アプリに対するユーザーの信頼を利用し、それらの正規デベロッパのイメージや評判を傷つけます[70、89]。これらの模倣アプリは通常サイドローディングを通じてダウンロードされ、世界中の何千万人ものユーザーを欺いています[43、90、91]。



偽のシステムアップデートは、よく見られるなりすましの技術です。システムアップデートを装い、ユーザーを騙してマルウェアをダウンロードさせて、デバイスへのアクセスを許可させます。例えば、サイドローディングされたあるAndroidアプリは、ユーザーのデバイスを感染させるためにシステムアップデートを装いました[92]。

Eメールとフィッシングメッセージはマルウェア攻撃に使われるもうひとつの技術です。ユーザーの信頼する送信者に見せかけて、ユーザーにマルウェアをダウンロードするよう促すために使用されます[8、93]。このようなフィッシングメッセージは一般的にソーシャルメディアアプリを通じて拡散されます。例えば、第三者アプリストアにある悪質なトロイの木馬であるFlyTrapは、ユーザーのFacebookアカウントを乗っ取り、被害者と社会的なつながりのある人々にトロイの木馬へのリンクを含んだ個人的なメッセージを送信します[85]。スペインでは、人々がマルウェアが組み込まれた偽の「コロナウイルス探知」アプリを宣伝し、サイドローディングさせるためのリンクが含まれたモバイルメッセージを受け取りました[94]。インドでは、ユーザーが公式なインド国税庁の税金申告アプリの偽物をダウンロードするよう促す個人的なSMSメッセージを受け取りました。このアプリには、ユーザーの個人情報や財務に関する情報を盗むよう設計されたマルウェアが含まれていました[95]。

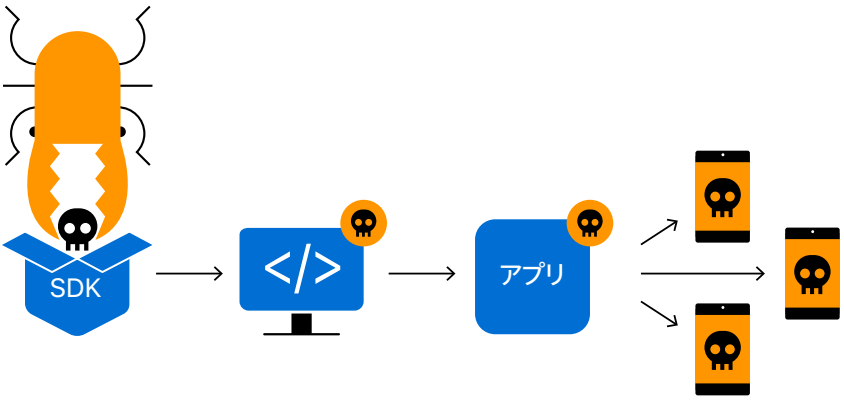
ウェブサイトのなりすましは、マルウェアを含んだ、正規に見せかけたウェブサイトを作成します[96]。これらのウェブサイトは、たびたび、サイドローディングさせるために用意した悪質なアプリへと導きます。先ほど紹介した、Clubhouseアプリのウェブサイトになりすますandroid向けトロイの木馬、BlackRockもその一例です。無防備なユーザーに正規のアプリではなくトロイの木馬のアプリをダウンロードするよう仕向けます[76]。

スケアウェアは、デバイスで脅威が検出されたといってユーザーを騙します。多くの場合、その脅威に対する解決策を示しますが、その中にマルウェアを含むアプリのサイドローディングが含まれています[97、98]。例えば、Armor for Androidはデバイスでマルウェアが検出されたという偽の警告をし、ユーザーにウイルス対策アプリをダウンロードするよう勧めて、そのアプリにより詐欺行為をします[99]。

望ましくない可能性のあるアプリは、純正のアプリに不正に入り込もうとするソフトウェアで、ユーザーが純正のアプリをインストールする際に一緒にデバイスにインストールされます。これらのアプリにはマルウェアが含まれていたり、デバイスのリソースを消費したりする可能性があります[100]。例えば、望ましくない可能性のあるアプリのアドウェアであるSorakaを含むAndroidアプリは100以上あり、全体で460万回以上ダウンロードされています[101]。

ハッカーは、ユーザーのデバイスを感染させるためにサプライチェーン攻撃も使用します。このような攻撃では、ユーザーを騙して感染したアプリをダウンロードさせるのではなく、正規のアプリのデベロッパを欺いて侵入と拡散を行います[102]。このような攻撃を増加させた方法の1つが、感染したSDK（ソフトウェア開発キット）、つまりアプリのデベロッパがアプリを構築する際に使用するビルディングブロックによるものです[103]。サイバー犯罪者やハッカーは、無防備なデベロッパが使用したSDKで悪質なコードの改ざんや挿入を行い、ユーザーにマルウェアを配信することがあります[104]。このような攻撃は正規のデベロッパが作成したアプリに対するユーザーの信頼を利用します。例えば、AndroidのデータアナリティクスSDKであるSWAnalyticsには、連絡先を盗むマルウェアパッケージであるOperation Sheepが潜伏しています。2019年3月の時点で、このマルウェアに感染した12のAndroidアプリが大手の第三者アプリストアで流通しており、1億1,100万件以上ダウンロードされていました[105]。

ハッカーが同種のマルウェアを再利用し、亜種に再パッケージすることがよくあります。ハッカーは、費用をかけてまったく新しいマルウェアを作り出すのではなく、既存のマルウェアを新しいバージョンに改変し、進化させたり別の方法で拡散したりします。Android向けのマルウェアの亜種は、近年急激に増加しています[106、107]。



エコシステムをオープンにすることのリスク

サイバー犯罪者やハッカーはマルウェアを拡散する際にアプリに大きく依存しているため、当事者によるアプリストアは悪質なアプリをスクリーニングして削除するための広範囲にわたるプロセスに投資しています[108、109、110]。マルウェアの脅威が高まる中、このようなスクリーニングプロセスはより厳格になり、アプリの審査に非常に多くのリソースを費やしています[111、112]。有害なアプリが当事者によるアプリストアで見つかると、配信を停止し、それ以降ユーザーの目に触れることがないようにします[113、114]。

一方で、第三者アプリストアに大量のマルウェアがあるということは、そこに有害なアプリをチェックするための十分な審査手順がないことを示しています（また、直接ダウンロードをさせるウェブサイトには個々の審査はありません）。そのため、サイバー犯罪者やハッカーはアプリを拡散するために第三者アプリストアや直接ダウンロードを多用し、監視機能やマルウェアの拡散を抑える機能がないことを悪用しているのです。既知のモバイルマルウェアの99パーセント以上が、第三者アプリストアを感染源としています[15、18]。Android上の悪質なアプリに関する研究によると、特定のアプリストアで悪質なアプリが検出され削除されても、多くの場合は別の第三者ストアに移動するだけで、消費者のデバイスを感染させ続けます[115、116]。

Androidはサイドローディングに対応しているため、マルウェアをAndroidプラットフォーム上でより容易に拡散することができます。Androidスマートフォンはモバイルマルウェアの最大の標的であり、最近では悪質なソフトウェアへの感染が、iPhoneと比較して15～47倍多くなっています[4、5]。ある研究によると、98パーセントのモバイルマルウェアがAndroidデバイスを標的にしています[18]。これはサイドローディングと密接な関係があります。例えば、2018年、公式なAndroidアプリストアであるGoogle Play以外の場所でアプリをインストールしたAndroidデバイスは、そうでないデバイスと比較して、有害な可能性があるアプリに感染する可能性が8倍多かったということです[103]。例えば、前述したHiddenAds、CopyCat、FakeSpy、BlackRockはいずれも、第三者提供元を経由してAndroidユーザーに到達する有名なマルウェアです。さらに、サイバー犯罪者やハッカーは海賊版アプリの拡散にサイドローディングを多用するため、著作権の侵害や知的財産の窃盗はAndroidデバイスでより多く発生しています[24、25、117]。一方で、iOSユーザーがマルウェアにさらされる可能性は低く、iOSプラットフォームで稀に見るマルウェア攻撃のほとんどは標的を絞ったものであり、その多くが国家によって実行されています[82、83、118]。iOSはAndroidよりも安全であり、Appleがサイドローディングに対応していないことがその一因であるというのが専門家の一般的な見解です[5]。

ユーザーを保護する機能がないまま、規制によってプラットフォームがサイドローディングに対応するよう強いられた場合、ユーザーの被害はさらに大きくなる可能性があります。Androidプラットフォームには現在、ユーザーが意識せずにアプリをサイドローディングするのを防ぐ追加の手順と警告により、ユーザーに「歯止め」を与えることによってサイドローディングを妨げるいくつかの機能があります。例えば、デバイスはデフォルトオプションとしてサイドローディングをしないよう設定されており、企業は社員のデバイスに対し、デバイスのあらゆる部分でサイドローディングを拒否することができます[119、120、121]。規制によって、何の歯止めもない状態でプラットフォームがサイドローディングに対応するよう強いられれば、その結果としてどちらのプラットフォーム上でも、マルウェア、著作権の侵害、知的財産の窃盗の脅威が高まるでしょう。

App Store以外でアプリを配信するための制約のある仕組み

App Store以外の場所でアプリを配信できるよう、限られた数のエンタープライズデベロッパをサポートしてきたApple独自の経験から、サイバー犯罪者のほか営利目的の企業でさえも、App Storeを迂回してマルウェアや違法なアプリを拡散するためにはどんな苦労も惜しまないことがわかっています。Appleは、規模の大きな組織向けに、組織の社員のみが利用するアプリ(例えば、App Reviewを経由できない社外秘のアプリ)を開発して非公開で配布する手段を提供するために、Developer Enterprise Programを作りました。厳格にコントロールされたプログラムのもと、自社IT部門の監督下で社員に直接アプリを配布できるように、Appleは企業に証明書を発行します。

プログラムを厳格にコントロールし、規模を制限しているにもかかわらず、悪意のある人たちはブラックマーケットで企業向けの証明書を購入するなど不正なアクセス方法を見つけています。悪意のある人たちは不正に入手した企業向けの証明書を使い、Goontact(以下を参照)や人気のiOSアプリの海賊版など、マルウェアを含むアプリを含め、App Storeのポリシーに違反するアプリを配信しています[122、123]。Developer Enterprise Programを悪用するのは、サイバー犯罪者に限りません。例えば、2019年、AppleはFacebookの企業向け証明書を無効にしました。ウェブ検索やブラウズの履歴、メッセージ、位置情報など、13歳の子どもを含むFacebookユーザーのモバイルデータと利用習慣を収集するFacebook ResearchというVPNアプリの配信に証明書が使われたためです[124、125]。企業向けの証明書は企業による社内利用のみを目的としています。App StoreやiOSの保護機能の迂回に利用される可能性があるため、一般的なアプリの配信は対象としていません。

Appleはこのプログラムのコントロールを厳格化し、ユーザーを保護する機能を追加する取り組みを強化していますが、不正使用は止まりません。**つまり、どのデベロッパもApp Store以外の場所ですべてのiPhoneユーザーにアプリを配信できるようにするようAppleに強制すれば、非常に大きなリスクがもたらされるということです。**何の制約もなく、サイドローディング経由でアプリを配信するオプションが広範囲で利用可能になれば、悪意のある人たちが不正使用した証明書をAppleが無効にしても効果はなく、マルウェアなどの違法なアプリが蔓延することでしょう。

AppleはDeveloper Enterprise Programを厳格にコントロールしています

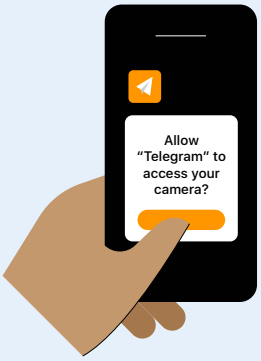
プログラムを利用する正当な理由がある法人にのみ参加資格があり、自社の社員に対してのみアプリを配布できます。

Appleは、企業がデベロッパ証明書を不適切に使用した場合、証明書を無効にすることができ、実際にそれを実行しています。

このプログラムを通じて作成されたアプリをダウンロードする社員は、使用するデバイスの設定を行い、その企業(雇用主)を信頼していることを確約しなければなりません。それにより、ユーザーがApp Store以外の場所でアプリをダウンロードする明確な意図があることを確認します。

Appleは企業に対し、社員にアプリを配信する別の方法を提供し、Developer Enterprise Programへの参加を制限しているため、ほとんどの企業のお客様はこのプログラムを利用していません。例えば、企業はApp Storeでカスタムアプリを配信するためにアプリを提出できます。このプロセスでは、組織内で提供可能になる前に、各アプリにApp Review(アプリの審査)プロセスが実施されます。詳しくはこちらをご覧ください。
developer.apple.com/jp/custom-apps/

Goontact：標的をおびき寄せ、スパイウェアをダウンロードさせる成人向けビデオチャットサイト



Goontactは、感染した成人向けビデオチャットアプリを通じてユーザーのデバイスに到達するマルチプラットフォームスパイウェアです。このスパイウェアは、サイドローディングしたアプリ経由でAndroidユーザーを標的としているほか、Apple Developer Enterprise Programを悪用して、iOSユーザーも標的にすることができます[122]。

標的

Goontactは現在、AndroidとiOSの両方のプラットフォームで活動しています。主な標的は、中国、日本、韓国、ベトナム、タイのユーザーです。

ユーザーのデバイスへの侵入方法

悪意のある人たちが成人向けビデオチャットができると期待させて、標的をウェブサイトにおびき寄せます。しかし、実際にはGoontactのオペレーターに接続されます。ビデオまたはオーディオの品質を向上させると見せかけて、オペレーターは標的に対し、当事者によるアプリストアのデザインをまねたウェブサイトで有名なビデオチャットアプリ（Telegramなど）をサイドローディングさせようとし、そのプロセスを説明しながら、アクセス権を有効にするよう説得します。しかし、サイドローディングしたアプリは偽物で、スパイウェアに感染しています。

挙動

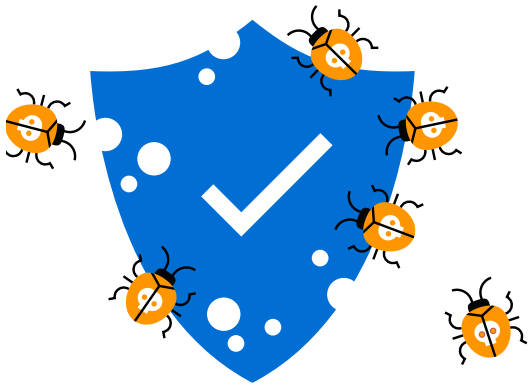
Androidユーザーが指示に従って許可を与えると、Goontactは、連絡先、SMSメッセージ、位置情報、写真、デバイスの識別子を収集します。iOSデバイスの場合、スパイウェアは連絡先とデバイスの識別子データしか収集できません。

IOSユーザーを標的にする方法

Goontactは不正な企業向け証明書を取得して、Apple Developer Enterprise Programの特権を悪用します。
Appleは見つけ次第、このような証明書を無効にしますが、悪意のある人たちは不正な証明書を新たに調達し、サイドローディングを通じたマルウェアを拡散し続けることができます。

攻撃の新たな段階

Goontactオペレーターとの最初のビデオチャット中に、サイバー犯罪者は標的が人に見られたくないようなビデオを録画し、脅迫のために使用します。ユーザーがアプリをダウンロードすると、スパイウェアがユーザーの連絡先を盗みます。さらに、サイバー犯罪者が、身代金を支払わないと連絡先リストの人々に先ほど録画したビデオを公開すると脅します。



サイドローディングがiOSのエコシステムに及ぼす影響

iOSエコシステムでのサイドローディングを強制することで、iPhoneの安全性とユーザーによる信頼が低下します。サイドローディングが直接ダウンロード経由または第三者アプリストア経由のどちらで実行されるかに関係なく、これは変わらないでしょう。iPhoneは最も安全な消費者向けモバイルデバイスであり、ユーザーがiPhone上でマルウェアに遭遇することはめったにないという点で、研究者たちの意見は一致しています[5]。iPhoneはパワフルな多層のセキュリティ保護をユーザーに提供しているため、通常、サイバー犯罪者やハッカーがiOSデバイスを大規模に攻撃することはできません。App ReviewプロセスによるAppleの目標は、App Storeにあるアプリが信頼できる安全なものであるようにすることです。Appleはこのプロセスを常に改善し、継続的にアップデートして、App Reviewのツールや手法を向上させています。

直接ダウンロードや第三者アプリストアを通じたサイドローディングにiOSを対応させるようAppleに強制することは、このようなセキュリティ保護の層を弱体化させ、すべてのユーザーを新しい深刻なセキュリティリスクにさらすことになります。有害で違法なアプリがこれまでより容易にユーザーに届くようになり、ダウンロードする正規のアプリをユーザーが管理できる機能が損なわれ、iPhoneのデバイス上の保護機能が低下します。サイドローディングによりユーザーのセキュリティとプライバシーは後退します。iOSデバイスでのサイドローディングに対応すれば、実質的にiPhoneは「ポケットに入るパソコン」になり、ウイルスにむしばまれたパソコンの時代に逆戻りしてしまいます。

第一に、サイドローディングに対応すれば、有害なアプリがさらに簡単にユーザーに届くようになります。直接ダウンロードでは審査が行われず、第三者アプリストアでは大量のマルウェアが急増していることから、そのようなストアには有害なアプリをチェックする十分な審査手順がないことがわかります。そのため、サイドローディングしたアプリが安全かどうかを判断する責任をユーザー自身が負うことになります。しかし、その判断は専門家でさえ難しいものです。Appleは現在、App Storeのアプリとデベロッパを審査し、違法なアプリを排除し、有害なアプリの拡散をただちに阻止することで、ユーザーを保護しています。

Appleの最新の文書「**数百万のアプリのために信頼できるエコシステムを築く**」で、Appleのデバイス保護機能とApp Reviewがユーザーのデバイスをどのように安全に保っているかをご覧ください。

マルウェア：サイドローディングにより、iOSユーザーは既知のマルウェアを含んだアプリにさらされます。App Reviewでは、App Storeに提出されたすべてのアプリとアプリのアップデートをスクリーニングし、サプライチェーン攻撃に使用された感染したSDKなど、様々な種類の既知のマルウェアをチェックします。一方、HiddenAdsのような既知のマルウェアは、Android向け第三者アプリストアに存在し続けています。（上記を参照）

なりすまし：iOSがサイドローディングに対応すると、悪意のある人たちはユーザーを欺くために人気アプリの模倣バージョンを配布できるようになります。App Storeには、既知の、審査を通過したデベロッパによるアプリしかなく、App Reviewチームのメンバーがそのコンテンツを審査しています。このプロセスは、Clubhouseの偽バージョンを装い、ユーザーのログイン用認証情報を盗むトロイの木馬アプリを防ぐ場合などに役立ちます。（上記を参照）

違法、海賊版、または盗まれたコンテンツ：ユーザーはサイドローディングにより、違法なギャンブルアプリ、海賊版アプリ、盗んだ知的財産を含むアプリなどの違法コンテンツにさらされます。これらは、第三者提供元経由で、チェックを受けずにiOSプラットフォームに拡散することができます。Appleは、Appleのポリシーで禁じられている違法コンテンツがないか、App Storeに提出されるすべてのアプリをチェックしています。

子どもを標的にした危険なアプリ：App Store以外の場所でのダウンロードに対応すると、保護者は子ども向けのように見えて実際は子どもたちをリスクにさらすアプリを思いがけずサイドローディングしてしまうかもしれません。App Storeのポリシーでは、「子ども向け」カテゴリのアプリについて、データ収集とセキュリティに関する厳しいガイドラインを設けています。例えば、このカテゴリのアプリは、アプリ外部へのリンクを含めたり、個人を特定できる情報を第三者に送信したり、第三者によるアナリティクスや広告を含んではなりません。

チェックをすり抜けた有害なアプリの拡散：めったにないことですが、不正なアプリや悪質なアプリがApp Storeで公開された場合、Appleは発見し次第すぐに削除し、さらなるユーザーへの拡散を防ぎます。また、サイバー犯罪者が元のマルウェアの亜種をほかのアプリに見せかけて出そうとしても、Appleはそれを特定してブロックし、さらなる変異や拡散ができないようにします。例えば、マルウェアの一種であるXcodeGhostは、無防備なデベロッパがAppleのデベロッパ向けウェブサイトではなく、第三者ウェブサイトから感染したバージョンのXcode（アプリの記述とコンパイルを行うAppleの開発環境）をダウンロードしたため、それを通じて拡散しました[126]。感染したアプリはApp Storeを中心に配信されたため、Appleはサイバーセキュリティ企業と速やかに連係し、そのアプリを特定して削除することができました[127]。一元化した審査が行われないサイドローディングのような仕組みでは、影響を受けたデベロッパ全員に通知することも、有害なアプリの拡散をコントロールすることもできません。たとえApp Storeからそれらのアプリを削除しても、第三者アプリストアや直接ダウンロードを通じて拡散され続けることを防げないためです。研究者によると、有害なアプリがAndroidプラットフォームの1つのアプリストアから排除されても、悪意のある人たちは単に別のアプリストアに移動するだけであることがわかっています[115]。

第二に、iOSがサイドローディングに対応した場合、ユーザーは直接ダウンロードまたは第三者アプリストア経由でダウンロードするアプリについて、正確な情報を得られない場合があります。また、アプリがどのデータにアクセスできるかをユーザーがコントロールできる機能が利用できない、または悪意のある人たちがその機能をはるかに簡単に操作できる可能性があります。App Storeでは、すべてのデベロッパにアプリに関する信頼できる情報を提供するよう求めており、Appleは、アプリがどのデータにアクセスできるかをユーザー自身がコントロールできるようにする多くの機能を設計しています。

許可：App Reviewでは、アプリが機能するために必要のない機密性の高い許可やデータへのアクセスを要求していないことをチェックします（天気アプリがマイクやヘルスケアデータへのアクセスを要求しているなど）。また、App Reviewでは、ユーザーに許可を求める際、誤解を招く説明や間違った説明をしていないこともチェックします。しかし、サイドローディングに対応した場合、サイドローディングしたアプリは、アプリが機能するためにその許可が必要かどうかに関わらず、デバイスのマイクや位置情報へのアクセスなど、機密性の高い許可やデータを不適切に要求または取得しているかがチェックされずに済むことになります。また、サイドローディングしたアプリが、巧みなメッセージや偽のメッセージを使ってユーザーを騙し、許可を与えさせようとすることもあります。

ユーザーにとって信頼できる情報：App Storeでは、アプリのデベロッパに、アプリとその機能の説明、アプリのスクリーンショット、アプリがどのようなデータをユーザーの身元情報に関連付けるか、また、そのデータが第三者のウェブサイトやアプリでユーザーを追跡するために使用されるかどうかを説明したプライバシーに関する情報を提出するよう求めています。これにより、ユーザーは何が起きるかを把握してから、アプリをダウンロードするかどうかを決めることができ、信頼できるデベロッパのふりをした悪意のある人たちに惑わされることはありません。サイドローディングに対応した場合、App Store以外の場所でダウンロードしたアプリが、実際にダウンロードしようと思っていた通りのものなのかユーザーにはわからず、そのアプリのプライバシー方針に関する情報がない場合もあります。

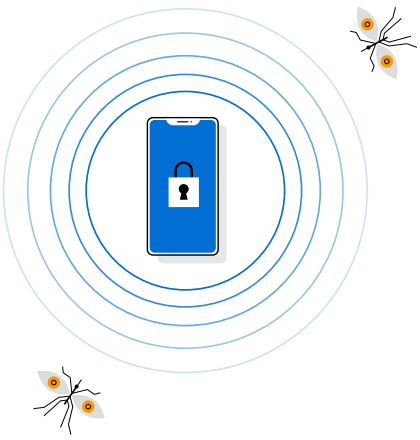
プライバシー保護機能：プライバシーはAppleのエコシステムの中核となるものです。App Storeにあるすべてのアプリは、第三者アプリやウェブサイトを横断してユーザーを追跡する前に、「アプリのトラッキングの透明性」機能を通じてユーザーの許可を得る必要があります。サイドローディングはこの保護機能を無効にします。ユーザーは、サイドローディングしたアプリが自分の広告識別子（IDFA）にアクセスするのは防げるかもしれませんが、サイドローディングしたアプリはほかのデバイスやユーザーデータにアクセスでき、ユーザーが追跡の利用停止を選択しても、アプリのデベロッパはそれに従う義務はありません。その結果、ユーザーのデータが本人の許可なく収集され共有される可能性があります。さらに、デベロッパに様々な報奨が用意され、Appleと同じ方法ではユーザーのデータを保護しないという選択をする場合もあります。「アプリのトラッキングの透明性」機能により広告収入を失ったため、特にこのプライバシー保護機能を迂回するためにアプリをサイドローディングさせて報奨を得るというデベロッパもいます[128]。さらに、ソーシャルメディアプラットフォームを含め、一部のデベロッパはユーザーのプライバシーや安全を侵害した経歴があり、iOSユーザーを保護するために設定されたApp Storeのガイドラインに違反するアプリを作成しています[124、129]。

Appleのプライバシー保護についてさらに詳しく

アプリがどのようにデータを収集して使用するかに関するコントロールと透明性をユーザーに提供する「アプリのトラッキングの透明性」機能とApp Storeのプライバシーラベルについて、詳しくは「**あなたのデータの一日**」と apple.com/jp/privacy/control をご覧ください。

ペアレンタルコントロール：Appleは、子どもたちのiOSデバイスの使い方を保護者がコントロールできる機能を設計しました。「スクリーンタイム」機能を使うと、保護者は子どもがデバイスをどれくらいの時間使ったかを把握できるほか、特定のアプリやウェブサイトを1日に利用できる時間の長さを制限できます。「承認と購入のリクエスト」機能は、子どもによるアプリのダウンロードやアプリ内での購入を保護者が承認または却下でき、連続購入を防ぐために15分間のタイムアウト機能も備わっています。サイドローディングはこのようなペアレンタルコントロール機能を弱体化させ、App Store以外の場所でダウンロードしたアプリによってこの機能を容易に迂回します。例えば、ゲームアプリが自らを教育向けアプリと称して、ゲームの使用に関する「スクリーンタイム」の制限を切り抜けることができます。また、サイドローディングしたアプリでのApp Store外での購入は「承認と購入のリクエスト」によってコントロールできません。

問題を報告する：Appleは、ユーザーがApp Storeでの購入について返金をリクエストしたり、アプリのプライバシー侵害や安全に関する問題を報告できるようにする機能を提供しています。これらの機能により、詐欺や不正行為の被害を受けた場合など、何か問題が起きた時にユーザーがリソースを利用できるようにしています。サイドローディングの場合、第三者アプリストアが、公正で明確、かつ一貫した返金ポリシーを提示したり、アプリで問題が起きた時にカスタマーサポートを提供したりする保証はありません。



サブスクリプション：Appleのサブスクリプション管理ツールを使うと、ユーザーはアプリ内での購入を通じて行ったすべての有料サブスクリプションを一か所で表示できます。ユーザーはアプリ内のサブスクリプションで請求される金額や頻度を確認でき、キャンセルも簡単にできます。サイドローディングでは、多くのデベロッパがアプリでこのような機能に対応しない可能性があり、そのためユーザーがサブスクリプションをキャンセルする方法がわかりにくく、キャンセルに時間もかかります。

最後に、サイドローディングはiPhoneの中核であるデバイス上のセキュリティ保護機能を低下させます。セキュリティ上の理由で、Appleは機密性の高いハードウェア要素（NFCチップ、Secure Enclave、メモリ領域、超広帯域など）へのアプリのアクセスを制限しており、非公開のオペレーティングシステム機能をアプリが使うことを許可していません。特別なエンタイトルメント、つまり、機密性の高いサービスまたはテクノロジーを使用する権利や許可は、特定の目的のためにアクセスを必要とするアプリに対して選択的に与えられます。例えば、ヘルスケアとアクティビティのデータにアクセスするために、アプリがユーザーの許可を要求してもよいかどうかは、HealthKitエンタイトルメントが判断します。

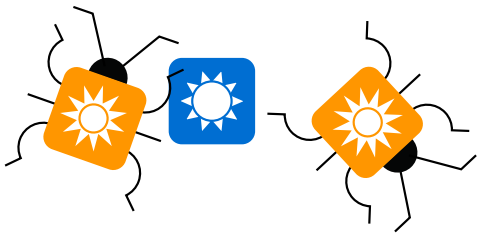
iOSでのサイドローディングを強いる一部の取り組みが要求しているように、Appleが特許で保護されたハードウェア要素や非公開のオペレーティングシステム機能へのフルアクセスを提供するよう強いられた場合、アプリのサンドボックス化や、アプリとオペレーティングシステムの分離など、中核となるプラットフォームのセキュリティ機能が損なわれます。iPhoneの攻撃対象領域は大幅に拡大し、基本的なセキュリティ保護が危険にさらされることになるでしょう。例えば、このような提案を受け入れた場合、オペレーティングシステムは、アプリが別のアプリのデータを盗んだり改変したり、ユーザーの許可なく、位置情報やデータ、マイク、カメラにアクセスしたりすることを防げなくなります。

サイドローディングにより、現在、iOS上で実行するには困難かつ費用がかかる多くの攻撃が、より簡単に安価で実行できるようになります[15]。これにより、iOS上で見られる攻撃手法の種類が拡大し、標的となるユーザーやサイバー犯罪者の数が増えます。サイドローディングに対応することは、iPhoneでの攻撃実行にかかる費用を低くし、悪意のある人たちに対し、これまでにない規模でiPhoneデバイスのセキュリティとプライバシーを攻撃するためのツールやノウハウを開発することを奨励することになります。

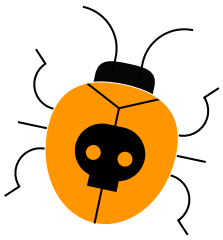
サイバー犯罪者とハッカーは、標的に到達するために、広告技術と産業を組み合わせて巧みに利用します。モバイル広告ネットワークを使い、広告を使ってユーザーを標的にし、サイドローディングしたアプリをインストールさせることで有害なアプリを拡散します。モバイル広告ネットワークは、モバイルアプリをインストールさせるための広告から年間数十億ドルを得ています。サイドローディングを通じて配布される悪質なアプリの広告を含める手口は、増加する可能性が高くなっています[130、131]。サイバー犯罪者はすでにソーシャルメディアプラットフォームで広告を使い、ユーザーをパソコン向けのマルウェアやその他の多様な詐欺行為の標的にしています[132、133、134]。ユーザーには悪質なアプリの広告が大量に押し寄せますが、これらの広告ネットワークはそこから利益を得るため、それを取り締まるインセンティブはほとんどありません[135]。サイバー犯罪者やハッカーは、友人や家族に対する人々の信頼を悪用し、ソーシャルエンジニアリングによって悪質なアプリを拡散するために、ソーシャルメディアネットワークを使用することもあります。その結果、クリックやダウンロードをしても安全なものは何かを判断する責任をユーザーが負うことになります。

サイドローディングをしたいと思わず、App Storeでのみアプリをダウンロードする選択をしたユーザーにも結果的に被害が生じます。App Storeで入手できなければ、仕事や学校、または社会参加に必要なアプリをサイドローディングすることを強いられる可能性があります。さらに、サイバー犯罪者やハッカーがApp Storeの見た目をまねたり、サービスや特別な機能を無料または追加で利用できると宣伝したりしてユーザーを騙し、そうとは気づかないままアプリをサイドローディングさせる場合があります。

Appleが直接ダウンロードや第三者アプリストア経由でのサイドローディングに対応することを強いられれば、iPhoneユーザーは常に詐欺を警戒しなければならなくなり、誰を、そして何を信頼すればよいか判断できなくなり、その結果、少数のデベロッパの限られたアプリしかダウンロードしなくなるでしょう。デベロッパ自身も、マルウェアを含み、それを拡散してしまうデベロッパツールを配布するような悪意のある人たちからの脅威に一段とさらされやすくなります。さらに、著作権侵害や知的財産の窃盗の被害も受けやすくなるため、自らの努力や革新に対して報酬を得るデベロッパの能力も弱体化します。



サイドローディングとiOSユーザー

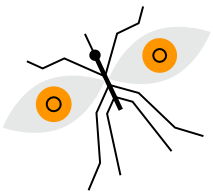


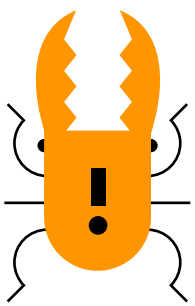
iOSデバイスでサイドローディングに対応すると、iOSユーザーに害を及ぼし、iOSユーザーのセキュリティ、プライバシー、個人データがリスクにさらされ、悪意のある人たちによる攻撃の脅威が高まります。iOSユーザーは、モバイルデバイス上に個人情報や重要な情報、機密性の高い情報を保存しています[136]。多くのiOSユーザーは、モバイルバンキングや支払いアプリを使用し、デバイス上で物やサービスを購入します[137]。企業の社員も、業務に関わる作業のために、モバイルデバイスで会社のネットワークに接続することがよくあります。App Storeのユーザーは、様々な職業や立場、年齢層で構成され、異なる言語を話し、世界の様々な場所に住んでいます。しかし、彼らに共通していることが1つあります。それは全員がApp Storeの保護機能によって守られているということです。

スマートフォンのユーザーは数百万のアプリにアクセスでき、多くのアプリをダウンロードしており、その数は増え続けています。多くの国で、ユーザーは平均90を超えるアプリをデバイスにインストールしており、iOSユーザーは5年前と比べて、アプリを約50パーセント多くダウンロードしています[138、139、140]。サイドローディングした個々のアプリは、ユーザーのデバイスや個人データのセキュリティとプライバシーを脅威にさらす可能性があります。

そのため、何億ものiOSユーザーを保護するには、Appleのセキュリティとプライバシーに関する機能は不可欠です。実際に、ある研究によると、大部分のiOSユーザーはサイバーセキュリティの問題に関する知識が少ししかない、またはまったくなく、特定の問題に遭遇しない限り、デフォルトのセキュリティ設定を変更しないと述べています[136]。セキュリティの専門知識がある少数のユーザーでさえ、セキュリティに関する選択をする際の優先順位を尋ねられると、セキュリティを選んだ人と便利さを選んだ人はほぼ同数でした[136]。

App Storeでの公開前にすべてのアプリを審査して、アプリがマルウェアを含まず、ユーザーにとって正確な情報が示されることを確認し、有害だとわかったら速やかにそのアプリを配信網から削除して、それ以降のバージョンや亜種が拡散されないようにすることで、Appleはエコシステムのセキュリティを保護し、お客様に安心感をもたらしています。**サイドローディングはユーザーの最善の利益にはなりません。**





セキュリティ専門家からのアドバイス

世界中の政府機関や国際機関、セキュリティ専門家、サイバーセキュリティプロバイダは、第三者アプリストアからアプリをダウンロードすることでもたらされるリスクについて、様々な場所でユーザーに警告しています。

「公式アプリストアのアプリしかインストールしないこと」

「企業は、社内ネットワークに接続するモバイルデバイスに対し、公式な提供元からのアプリしかインストールを許可してはならない」

欧州刑事警察機構[147]

「悪質なアプリをインストールするリスクを最小限に抑えるには、ユーザーは第三者提供元ではなく、Google Playからのみアプリをダウンロードすべきだ」

欧州ネットワーク・情報セキュリティ機関[141]

「ユーザーはアプリのサイドローディングや無認可のアプリストアの使用を避けるべきである（さらに企業は自社デバイス上でそのような行為を禁止するべきである）」

国土安全保障省（米国）[143]

「（サイドローディングを）不適切に行うと、モバイルデバイスが攻撃に対して非常に脆弱になる可能性がある」

米国立標準技術研究所（米国商務省）[144]

「第三者アプリストアの危険を最小限に抑える方法の1つは、それを避けることだ」

Norton（サイバーセキュリティプロバイダ）[148]

「第三者アプリは、身元不明の提供元からのアプリをインストールしているユーザーを脅威にさらしている」

国際刑事警察機構とKaspersky Lab[142]

「大部分の（第三者）アプリストアは、提供しているアプリに厳しいセキュリティ審査を実施していない。これにより、そのアプリをインストールしたデバイスは著しく脅威にさらされやすくなる」

「（企業の）BYODポリシーで（サイドローディングは）禁止されるべきだ」

Wandera（モバイルセキュリティ企業）[145、146]

Sources

1. Neville, Ann, "Recent cyber-attacks and the EU's cybersecurity strategy for the digital decade," *European Parliamentary Research Service*, June 2021.

2. Chebyshev, Victor, "Mobile Malware Evolution 2020," *Kaspersky*, March 1, 2021.

3. Yablokov, Victor, "Why there's no antivirus for iOS," *Kaspersky*, September 10, 2018.

4. Nokia, "Threat Intelligence Report 2020," 2020.

5. Nokia, "Threat Intelligence Report 2019," 2019.

6. RSA, "2018 Current State of Cybercrime," *Dell Technologies*, March 20, 2018.

7. Hautala, Laura, "Android malware tries to trick you. Here's how to spot it," *CNET*, May 14, 2021.

8. Mitre ATT&CK, "Techniques: Deliver Malicious App via Other Means," February 9, 2021.

9. Mitre ATT&CK, "Tactics: Initial Access," January 27, 2020.

10. Verizon, "2020 Data Breach Investigations Report," May 19, 2020.

11. Anderson, Sophie, "Antivirus and Cybersecurity Statistics, Trends & Facts 2021," *Safety Detectives*, January 24, 2020.

12. Verger, Rob, "Your anti-virus software is not enough," *Popular Science*, July 7, 2017.

13. Huang, Keman, et al., "Systematically Understanding the Cyber Attack Business: A Survey," *ACM Computing Surveys*, Vol. 51, No. 4, July 2018, pp. 1-36.

14. Algarni, Abdullah and Malaiya, Yashwant, "Software Vulnerability Markets: Discoverers and Buyers," *World Academy of Science, Engineering and Technology International Journal of Computer and Information Engineering*, Vol. 8, No. 3, 2014, pp. 480-490.

15. RiskIQ, "2020 Mobile App Threat Landscape Report," 2020.

16. Burkhalter, Max, "Why BYOD culture poses a major risk to enterprises," *Perle*, April 6, 2020.

17. Bitglass, "Mission Impossible: Securing BYOD," November 2018.

18. PurpleSec, "2021 Cyber Security Statistics: The Ultimate List Of Stats, Data & Trends," 2021.

19. Ponemon Institute, "The Economic Risk of Confidential Data on Mobile Devices in the Workplace," February 2016.

20. Holland, Jake, "T-Mobile Hit With Class Action Suits After Consumer Data Breach," *Bloomberg Law*, August 20, 2021.

21. Check Point, "Mobile Security Report 2021," April 2021.

22. IBM, "Cost of a Data Breach Report 2021," July 2021.

23. Sophos, "The State of Ransomware 2020," May 2020.

24. Brown, Mike, "Android's Piracy Problem Is Forcing Developers To Give Away Games: 'Alto's Adventure' Latest Freebie," *International Business Times*, February 11, 2016.

25. Koetsier, John, "The Mobile Economy Has A $17.5B Leak: App Piracy," *Forbes*, February 2, 2018.

26. Vincent, James, "TikTok clone Zynn has now been removed from the iOS App Store as well," *The Verge*, June 16, 2020.

27. LeFebvre, Rob, "Apple pulls cloned games from App Store," *VentureBeat*, February 7, 2012.

28. Dong, Feng, et al., "FrauDroid: An Accurate and Scalable Approach to Automated Mobile Ad Fraud Detection," September 6, 2017.

29. La Porta, Liarna, "Trojan malware infecting 17 apps on the App Store," *Wandera*, October 24, 2019.

30. Trend Micro, "Mobile Ad Fraud Schemes: How They Work, and How to Defend Against Them," April 26, 2019.

31. Takahashi, Dean, "Adjust says mobile ad fraud rates doubled in the past year," *VentureBeat*, May 10, 2018.

32. Health Information National Trends Survey, "On your tablet or smartphone, do you have any software applications or apps related to health?," *National Cancer Institute*, 2020.

33. Firch, Jason, "10 Cyber Security Trends You Can't Ignore In 2021," *PurpleSec*, April 29, 2021.

34. He, Terry, et al., "2021 Cyber Threat Report," *SonicWall*, 2021.

35. Cohen, Jessica Kim, "Hackers taking advantage of COVID-19 to spread malware," *Modern Healthcare*, March 16, 2020.

36. Wang, Liu, et al., "Beyond the Virus: A First Look at Coronavirus-themed Android Malware," *Empirical Software Engineering*, Vol. 26, No. 82, June 12, 2021.

37. Chen, ZePeng, "Thousands of HiddenAds Trojan Apps Masquerade as Google Play Apps," *McAfee*, March 3, 2020.

38. Avast, "Avast Reports Continued Dominance of Adware Among Android Threats," June 16, 2021.

39. Kaspersky, "What is Adware? – Definition and Explanation."

40. Malwarebytes, "Android/Trojan. FakeAdsBlock."

41. Dr. Web Anti-Virus, "Clicker Trojan Installed from Google Play by Some 102,000,000 Android Users," August 8, 2019.

42. Osborne, Charlie, "CopyCat Android malware infected 14 million devices, rooted 8 million last year," *ZDNet*, July 7, 2017.

43. Check Point, "How the CopyCat malware infected Android devices around the world," July 6, 2017.

44. Schwartz, Jaime-Heather, "How to protect your Android phone from ransomware – plus a guide to removing it," *Avira*, August 13, 2020.

45. Grustniy, Leonid, "Mobile beasts and where to find them – part two," *Kaspersky*, August 3, 2018.

46. Holland, Tilly, "Ransomware Attacks: What You Need To Know," *Ontrack*, March 7, 2019.

47. PurpleSec, "2021 Ransomware Statistics, Data, & Trends," 2021.

48. Nicholas, Sarah, "You Can Beat the Latest Security Breaches," *Ameris Bank*, July 19, 2021.

49. Cyber Florida, "Research Shows a 715% Increase in Ransomware Attacks in 2020," *University of South Florida*, September 23, 2020.

50. Ostroff, Caitlin and Vigna, Paul, "Why Hackers Use Bitcoin and Why It Is So Difficult to Trace," *Wall Street Journal*, July 16, 2020.

51. Stefanko, Lukas, "New ransomware posing as COVID-19 tracing app targets Canada; ESET offers decryptor," *WeLiveSecurity by ESET*, June 24, 2020.

52. Seals, Tara, "Emerging Ransomware Targets Photos, Videos on Android Devices," *Threatpost*, June 24, 2020.

53. Emm, David, et al., "IT Threat Evolution in Q2 2016," *Kaspersky*, 2016.

54. Kaspersky, "KSN Report: Ransomware in 2016-2017," *Kaspersky*, 2017.

55. Venkatesan, Dinesh, "Sophisticated new Android malware marks the latest evolution of mobile ransomware," *Microsoft*, October 8, 2020.

56. Whitwam, Ryan, "Microsoft Spots Android Ransomware That Hijacks Your Home Button," *ExtremeTech*, October 9, 2020.

57. Osborne, Charlie, "How to find and remove spyware from your phone," *ZDNet*, August 9, 2021.

58. Kaspersky, "Avoiding Cell Phone Spyware Infestation."

59. Shatilin, Ilja, "Mobile beasts and where to find them – part four," *Kaspersky*, October 22, 2018.

60. Palmer, Danny, "AndroRAT: New Android malware strain can hijack older phones," *ZDNet*, February 14, 2018.

61. Federal Trade Commission, "FTC Brings First Case Against Developers of "Stalking" Apps," October 22, 2019.

62. Federal Trade Commission, "FTC Bans SpyFone and CEO from Surveillance Business and Orders Company to Delete All Secretly Stolen Data," September 1, 2021.

63. Vaas, Lisa, "SpyFone & CEO Banned From Stalkerware Biz," *Threatpost*, September 2, 2021.

64. Citron, Danielle Keats, "Spying Inc.," *Washington and Lee Law Review*, Vol. 72, No. 3, June 1, 2015, pp. 1234-1282.

65. Securelist, "The State of Stalkerware in 2020," *Kaspersky*, February 26, 2021.

66. Cybereason Nocturnus Team, "FakeSpy Masquerades as Postal Service Apps Around the World," *Cybereason*, July 1, 2020.

67. Almkias, Ofir, "FakeSpy," *Mitre ATT&CK*, October 6, 2020.

68. National Cyber Security Centre, "Fake 'missed parcel' messages: advice on avoiding banking malware," August 19, 2021.

69. Finnish Transport and Communications Agency, "Android malware spread by SMS," July 15, 2021.

70. Desai, Shivang, "SpyNote RAT posing as Netflix app," *Zscaler*, January 23, 2017.

71. Black, Daniel, "HelloSpy App Review 2021: Will the App Resume Its Work?," *mSpy*, March 5, 2021.

72. Cox, Joseph, "I Tracked Myself With $170 Smartphone Spyware that Anyone Can Buy," *Vice*, February 22, 2017.

73. Kochetkova, Kate, "Mobile banking Trojans, explained," *Kaspersky*, October 14, 2016.

74. Stefanko, Lukas, "Android Banking Malware: Sophisticated Trojans vs. Fake Banking Apps," *ESET*, January 2019.

75. Owaida, Amer, "Beware Android trojan posing as Clubhouse app," *WeLiveSecurity by ESET*, March 18, 2021.

76. ThreatFabric, "BlackRock – the Trojan that wanted to get them all," *ThreatFabric*, July 2020.

77. O'Donnell, Lindsey, "Banking.BR Android Trojan Emerges in Credential-Stealing Attacks," *Threatpost*, April 21, 2020.

78. Asoltanei, Oana, et al., "Threat Actors Use Mockups of Popular Apps to Spread Teabot and Flubot Malware on Android," *Bitdefender Labs*, June 1, 2021.

79. Cleafy, "TeaBot: a new Android malware emerged in Italy, targets banks in Europe," May 31, 2021.

80. Cyware, "Exploring the Nature and Capabilities of Anubis Android Banking Trojan," January 25, 2020.

81. Clark, Mitchell, "NSO's Pegasus spyware: here's what we know," *The Verge*, July 23, 2021.

82. Whittaker, Zack, "A new NSO zero-click attack evades Apple's iPhone security protections, says Citizen Lab," *TechCrunch*, August 24, 2021.

83. NPR, "Malware From An Infamous Hacker-For-Hire Group Was Found On Nearly 900 Phones," July 19, 2021.

84. Infrascale, "Enterprise Ransomware Survival Guide," May 25, 2016.

85. Yaswant, Aazim, "FlyTrap Android Malware Compromises Thousands of Facebook Accounts," *Zimperium*, August 9, 2021.

86. Hazum, Aviran, et al., "New Wormable Android Malware Spreads by Creating Auto-Replies to Messages in WhatsApp," *Check Point Research*, April 7, 2021.

87. Jama, Robleh, "The upside of copycat apps and how to deal with them if they get out of hand," *TheNextWeb*, April 9, 2016.

88. Hinchliffe, Alex and Palo Alto Networks, "Techniques: Masquerade as Legitimate Application," *Mitre ATT&CK*, April 8, 2020.

89. Peterson, Andrea, "Beware: New Android malware is 'nearly impossible' to remove," *The Washington Post*, November 6, 2015.

90. Trend Micro, "Malware in Apps' Clothing: A Look at Repackaged Apps," May 15, 2014.

91. Toulas, Bill, "Researchers Found 164 'Copycat' Apps That Tricked 10 Million Users," *TechNadu*, January 14, 2021.

92. Yaswant, Aazim, "New Advanced Android Malware Posing as 'System Update'," *Zimperium*, March 26, 2021.

93. European Union Agency for Cybersecurity, "Phishing on the rise," October 12, 2017.

94. Eremin, Alexander, "People infected with coronavirus are all around you, says Ginp Trojan," *Kaspersky*, March 24, 2020.

95. Pak, ChanUng, "Phishing Android Malware Targets Taxpayers in India," *McAfee*, September 3, 2021.

96. Malwarebytes, "What is a spoofing attack?"

97. Fitriah, Andi, et al., "Understanding Android Financial Malware Attacks: Taxonomy, Characterization, and Challenges," *Journal of Cyber Security and Mobility*, Vol. 7, No. 3, June 14, 2018, pp. 1-52.

98. Kaspersky, "What is Scareware?," *Kaspersky*.

99. Sims, Gary, "Exposé: Don't fall victim to this dodgy anti-virus app," *Android Authority*, February 5, 2014.

100. Malwarebytes, "Mobile PUP," June 9, 2016.

101. Satori Threat Intelligence and Research Team, "Bringing Starchild Down to Earth: Soraka SDK," *Human Security*, December 2019.

102. Korolov, Maria, "Supply chain attacks show why you should be wary of third-party providers," *CSO from International Data Group*, February 4, 2021.

103. Android, "Android Security & Privacy 2018 Year In Review," March 2019.

104. Clayton, Richard, "Mobile Supply Chain Attacks Are More Than Just an Annoyance," *Check Point*, 2019.

105. He, Feixiang and Polkovnichenko, Andrey, "Operation Sheep: Pilfer-Analytics SDK in Action," *Check Point*, March 13, 2019.

106. Trend Micro, "Variant."

107. Sen, Sevil, et al., "Coevolution of Mobile Malware and Anti-Malware," *IEEE Transactions on Information Forensics and Security*, Vol. 13, No. 10, October 2018, pp. 2563-2574.

108. Australian Competition & Consumer Commission, "Digital Platform Services Inquiry: Interim Report – App Marketplaces," March 2021.

109. Apple Developer, "App Store Review Guidelines."

110. Google Play Help, "Google Play Protect keeps your apps safe and your data private."

111. O'Donnell, Lindsey, "Google Play Cracks Down on Malicious Apps," *Threatpost*, February 14, 2019.

112. Mohan, Babu, "Google now takes three days to approve new Play Store apps," *Android Central*, August 20, 2019.

113. Apple, "App Store stopped more than $1.5 billion in potentially fraudulent transactions in 2020," May 11, 2021.

114. Guertin, Alec and Kotov, Vadim, "PHA Family Highlights: Bread (and Friends)," *Google Security Blog*, January 9, 2020.

115. Shen, Yun, et al., "A Large-scale Temporal Measurement of Android Malicious Apps: Persistence, Migration, and Lessons Learned," *Cornell University: Computer Science – Cryptography and Security*, August 10, 2021.

116. Lindorfer, Martina, et al., "AndRadar: Fast Discovery of Android Applications in Alternative Markets," *11th Conference on Detection of Intrusions and Malware & Vulnerability Assessment*, July 2014.

117. Smith, Chris, "Another crucial reason why app developers prefer iOS to Android," *BGR*, February 4, 2016.

118. Kujawa, Adam, et al., "2020 State of Malware Report," *Malwarebytes*, February 2020.

119. N-Marandi, Sara, "What's new in Android privacy," *Android Developers Blog*, May 18, 2021.

120. Johnson, Kyle, "How do you block sideloaded app installation on iOS or Android?," *TechTarget*, January 9, 2019.

121. Tee, Mike, "How to Install Apps from Unknown Sources in Android," *MakeTechEasier*, February 16, 2020.

122. Nickle, Robert, et al., "Lookout Discovers New Spyware Used by Sextortionists to Blackmail iOS and Android Users," *Lookout*, December 16, 2020.

123. Nellis, Stephen and Dave, Paresh, "Software pirates use Apple tech to put hacked apps on iPhones," *Reuters*, February 13, 2019.

124. Owen, Malcolm, "Apple has revoked Facebook's enterprise developer certificates after sideload violations," *AppleInsider*, January 30, 2019.

125. Axon, Samuel, "Apple revokes Facebook's developer certificate over data-snooping app—Google could be next," *Ars Technica*, January 30, 2019.

126. Xiao, Claud, "Novel Malware XcodeGhost Modifies Xcode, Infects Apple iOS Apps and Hits App Store," *Palo Alto Networks*, September 17, 2015.

127. Xiao, Claud, "More Details on the XcodeGhost Malware and Affected iOS Apps," *Palo Alto Networks*, September 21, 2015.

128. Fischer, Sara, "Facebook says Apple's ad changes are hurting its business," *Axios*, September 22, 2021.

129. Seetharaman, Deepa, "Facebook Removes Data-Security App From Apple Store," *Wall Street Journal*, August 22, 2018.

130. Rosenfelder, Shani, "Global app install ad spend to double by 2022 to hit $118 billion," *AppsFlyer*, February 13, 2020.

131. Brown, Eileen, "Facebook leads app install market share, but Google is rising fast," *ZDNet*, October 19, 2018.

132. Whittaker, Zack, "Facebook ran ads for a fake 'Clubhouse for PC' app planted with malware," *TechCrunch*, April 8, 2021.

133. Newman, Lily Hay, "Facebook Shut Down Malware That Hijacked Accounts to Run Ads," *Wired*, October 1, 2020.

134. McGuire, Michael, "The Web of Profit: Social Media Platforms and the Cybercrime Economy," *Bromium*, 2019.

135. Rastogi, Vaibhav, et al., "Understanding In-App Ads and Detecting Hidden Attacks through the Mobile App-Web Interface," *IEEE Transactions on Mobile Computing*, Vol. 17, No. 11, November 1, 2018, pp. 2675-2688.

136. Breitinger, Frank, et al., "A survey on smartphone users' security choices, awareness and education," *Elsevier: Computers & Security*, Vol. 88, October 11, 2019.

137. Centre for International Governance Innovation – Ipsos, "Global Survey on Internet Security & Trust," 2017.

138. App Annie, "The State of Mobile," 2019.

139. Nelson, Randy, "Store Intelligence: Q1 2016 Data Digest," *Sensor Tower*, April 18, 2016.

140. Sensor Tower, "Q4 2020 Store Intelligence Data Digest," 2020.

141. European Union Agency For Cybersecurity, "Vulnerabilities – Separating Reality from Hype," August 24, 2016.

142. Kaspersky and Interpol, "Mobile Cyber Threats," October 2014.

143. U.S. Department of Homeland Security, "Study on Mobile Device Security," April 2017.

144. Franklin, Joshua M, et al., "Guidelines for Managing the Security of Mobile Devices in the Enterprise," *U.S. Department of Commerce – National Institute of Standards and Technology*, March 2020.

145. Urwin, Matt, "Top 5 Types of Sideloaded Apps and the Risks They Pose," *Wandera*, December 19, 2018.

146. Velzian, Becci, "How to Create a Bring Your Own Device (BYOD) Policy," *Wandera*, January 13, 2021.

147. Europol, "Just a Game? Only install apps from official app stores," *European Cybercrime Centre*.

148. Gervais, Joe, "The risks of third-party app stores," *Norton*, July 18, 2018.