

リスクが大きいモバイルアプリケーションストアからのダウンロード

McAfee® Labs™

目次

はじめに	3
マルウェアと脆弱性以外の「攻撃」	3
課題の区分—Androidマーケット	4
BitTorrentとApptackrの共通点とは	5
「標的型」攻撃	6
アプリケーションストアでの考えられる展開	6
注意の喚起	7

この数年間で、広く導入されているサーバーソフトウェアでネットワークサービスの脆弱性を発見するのがますます困難になっています。また、攻撃者は、クライアントサイドの脆弱性を利用して侵害したホストから利益を得るのに、より効果的な方法を見出しています。セキュリティが向上すると同時に、攻撃者が利益を得る方法が強化されており、調査の焦点はネットワークベースの脆弱性からクライアントサイドの脆弱性に移っています。現在、研究者によって Apache HTTP サーバー、OpenSSH、Microsoft RPC などの従来の攻撃対象で発見される脆弱性が少なくなる一方で、Microsoft Office、Web ブラウザー、Adobe Flash、Adobe Reader などの一般的なアプリケーションでより多くの脆弱性が発見されています。この変化は、侵害された Web サイトでクライアントサイドの脆弱性を悪用するマルウェアや、スパムと連動したマルウェアの増加と並行して起こっています。モバイルアプリケーションがますます普及し、その重要性が高まっているため、セキュリティの焦点がモバイルアプリケーション（特に Mobile Safari などのアプリケーションに存在するクライアントサイドの脆弱性）に移るのは予測どおりのものであり、現在進行中です。

はじめに

アプリケーションとコンテンツを重要なシステムコンポーネントや他のアプリケーションから分離するために使用されるアプローチであるサンドボックスにより、特に Google Chrome、Adobe Reader X、およびモバイルデバイスでセキュリティが向上しています。サンドボックスを実装することで、Chrome ではブラウザを保護し、Reader X では PDF 表示をカプセル化し、モバイルデバイスでは、電話の基盤となる OS やデバイスで実行されている他のアプリケーションのセキュリティにアプリケーションが干渉しないように保護しています。ただし、サンドボックスはすべてにおいて効果があるわけではありません。たとえば、マルウェア概念実証の OSX/iPHSponey.A¹ では、iOS サンドボックス内で完全に動作しながら、大量の個人データを収集することができました。サンドボックス化されたアプリケーションに対してクライアントサイドの攻撃が展開されていることに加えて、iOS の Jailbreak (Apple デバイスの制限解除) が行われているために、セキュリティ研究者はサンドボックス侵害に注目しています。Comex の JailBreakMe.com の iOS サンドボックスでは攻撃²が回避されており、「rageagainstthecage」³を備えた Android サンドボックスでは 2 つの注目を浴びた事例が回避されています。さらに、新しい高度な悪用手法 (Return-Oriented Exploitation [ROP]) は巧妙になっており、組み込みシステムとモバイルデバイスへの攻撃がより実践的になってきています。

マルウェアと脆弱性以外の「攻撃」

攻撃手法を検証する前に、まず、一部のアプリケーションストア評価モデルに存在する「不正レビュー」問題について見てみましょう。問題の評価モデルを Google の PageRank 検索エンジンランキングシステムなどの他のレビュー評価システムと比較すると、この問題への理解を深めることができます。PageRank の不正は、攻撃者が検索結果を侵害して、攻撃者のサイトが検索結果で過度に上位に表示されると発生します。攻撃者のサイトは、検索結果で実際のランキングでは表示されずに、人気のあるサイトよりも高いランキングで表示されます。一部のアプリケーションストアのコミュニティでも、同様の不正が行われているようです。たとえば、アプリケーションストアの PageRank と同等の、アプリケーションストアの検索結果の順位は、主にレビューと評価に基づいています。レビューや評価が多くなるほど、ユーザーの検索結果でアプリケーションの順位が上がります。PageRank の不正によってマルウェアサイトのクリック数が増えるのと同じように、アプリケーションストアの不正評価によって、対象のアプリケーションをクリックして購入するユーザーが増えます。Apple の App Store では、アプリケーションを評価するのにレビュー者がそのアプリケーションを購入する必要がないため、「攻撃者」（通常、アプリケーション作成者またはアプリケーション関係者）は、レビューを投稿すればアプリケーションのランキングを容易に上げることができます。さらに、偽りのレビューも存在するため、一般的に「星評価」は平均的なレビューよりも高く、コメントは肯定的なものが多くなっています。これにより、消費者が騙されてアプリケーションに対価を支払う可能性が大きくなるという影響が生じています。

1. http://vil.nai.com/vil/content/v_246873.htm

2. <https://github.com/comex>

3. <http://intrepidusgroup.com/insight/2010/09/android-root-source-code-looking-at-the-c-skills/>

Apple やその他のアプリケーションストアベンダーは、どのようにすればこの問題を解決できるでしょうか。解決できない問題なのでしょうか。

答えは、どちらとも言えないということです。偽りのレビューは、レビューベースのシステムに本来伴うリスクであると言えます。ただし、Amazon が長い期間をかけてレビューシステムを開発、改善してきたのと同様に、Apple やその他のベンダーも同じような措置を取る必要があります。まず、必須と考えられる措置として、レビューと星評価を、対象のバージョンのアプリケーションの対価を支払ってダウンロードしたユーザーに限定する必要があります。この点において、現在 Apple では、ランキングの信頼性よりも使い勝手を優先しているようです。ただし、攻撃者が増加してユーザー満足度が低下した場合には、優先順位が変わる可能性があります。

攻撃者は、一度限りのメールアドレスを作成してアプリケーションを購入し、レビューを書き込むことで、反撃してくる可能性があります。ただし、Apple では、IP が一意であるかどうかを検証し、URL、ブラウザやシステムのメタデータ、その他のプロパティを照会することで、次の措置に進めることができます。このようなアプローチには、メリットとデメリットがあります。ただし、現在のシステムでは不十分であり、改善される可能性が高いという点は依然として残ります。

課題の区分—Android マーケット

Android マーケットなどの他のアプリケーションストアでは、全く別のモデルが使用されています。Android アプリケーションの場合、大部分の電話でアプリケーションを「サイドローディング」できます。また、Apple の場合とは異なり、中央のアプリケーションストアからアプリケーションを入手するには制限されていません。このオープン性により、Android アプリケーションの開発者やその他の関係者は、自身の Web サイトに Android アプリケーションを掲載して、インストールするようユーザーに訴求することができます。この状況は、ドライブバイダウンロードのマルウェアモデルのように思われます。Apple の状況とは異なり、疑わしい動作（電話以外の動作について）がないかどうか Google によってすべてのアプリケーションがチェックされるような中央の場所はありませぬ。

中国の Android デバイスで検出された、広く公表されている Geinimi⁴ の場合、デバイスから個人情報を読み出すため、マルウェアが人気のあるアプリケーションに結合されていました。アプリケーションが Android マーケットの外部のインターネットで配布されている場合、デバイスのセキュリティを確保するために Google で行うことができるのはデバイスのスキャンに限定されるため、この種の攻撃を Google で検知するのは困難です。他方、Apple では、ストアにアプリケーションが投稿されるときに、それらのアプリケーション（以下で説明する明らかな例外を除く）の分析が行われています。

米国のセキュリティ意識の高いユーザーによっても、マルウェアに感染したアプリケーションが発見されています。⁵ 最近、Lompolo という研究者が Android マーケットの一連の Android アプリケーションにバックドア型のトロイの木馬が含まれており、盛んにダウンロードされていることを発見しました。⁶ これらのアプリケーションは、問題の Android アプリケーションのいくつかが不適切な発行元によって再発行されている、つまり著作権が侵害されて再度パッケージ化されているらしいことに Lompolo が気付いたため、発見されました。これは、対価を支払わずにソフトウェアを使用しようとする、通常の著作権侵害とは異なります。この場合、マルウェアの作成者は、恐らく許可や配布の権利なしに、別の発行元が作成したソフトウェアを再度パッケージ化していました。著作権が侵害されたアプリケーションの 1 つをリバースエンジニアリングした際に、Lompolo は、このアプリケーションが悪用を回避する「rageagainstthecage」を備えた Android サンドボックスを使用しており、ローカルの SQLite データベースに情報を保存して、IP アドレスから疑わしい Web サーバーと通信して、デバイスの IMEI コードと IMSI コード（デバイスの ID を識別することが可能）をリモートサーバーに渡していることに気がきました。Google は、Android マーケット⁷ から違法のアプリケーションをすばやく削除し、影響を受けたユーザーがこの攻撃の影響から回復できるよう、ツールをリリースしました。⁸ ただし、推定ダウンロード数は数万から数十万にのぼっており、影響を受けたユーザーの数は依然として大きなものとなっています。この事件により、Google では、このような制限のない方法でアプリケーションを Android マーケットに投稿できるという状況を再検討することになるかと考えられます。

4. http://vil.nai.com/vil/content/v_342726.htm

5. <http://venturebeat.com/2011/03/02/dozens-of-android-apps-pulled-from-market-due-to-malware-infections/?source=business-insider>

6. <http://www.reddit.com/r/netsec/comments/fvhdw>

7. <http://blog.mylookout.com/2011/03/security-alert-malware-found-in-official-android-market-droiddream/>

8. <http://googlemobile.blogspot.com/2011/03/update-on-android-market-security.html>

BitTorrent と Apptackr の共通点とは

この質問に答えるため、まず、コンピューターの著作権侵害の歴史を少し振り返ってみましょう。当然のことですが、著作権侵害（著作権侵害の悪影響ではなく）に関する説明はほとんど文書化されていません。ただし、クライムウェアをブロックするには、クライムウェアシステムが動作する仕組みや犯罪者が利益を得る仕組みを理解している必要があるのと同じように、他のマルウェア配布チャネルを監視するには、通常、それらのシステムを理解している必要があります。著作権が侵害されたモバイルデバイス向けアプリケーションに、長期にわたっていかにしてより多くのマルウェアが組み込まれる可能性があるのかを明確にするため、違法コピーの PC ソフトウェアの展開によって、いかにして組み込みのマルウェアが増えてきたのかを見てみましょう。

PC 市場の違法コピーソフトウェアは、フロッピーなどのハードメディアでソフトウェアを売買している人々から、電子掲示板システムでのソフトウェアの配布（本来、電子掲示板システム自体が配布対象）、FTP などの閉じたシステムを用いたインターネット経由での売買、IRC やニュースグループなどのオープンシステムを用いたインターネット経由での売買へ、最終的には BitTorrent などの完全に公開された制限のないシステムでの売買へと発展しました。これらの手法はすべて現在でも利用されていますが、重要なのは、時間の経過とともに、これらの違法コピーソフトウェアシステムがますますオープンなものになっており、アクセスが容易になってきていることです。国ごとに見た大部分のピアツーピア (P2P) トラフィックでは、1 つの P2P アプリケーション固有になるにつれて（米国の場合、BitTorrent など）、BitTorrent のマルウェアが急増しています。数年前は、違法コピーソフトウェアに対処するレピュテーションシステムなど想像できませんでした。そのアイデアだけでも、ばかげていました。現在、特定の BitTorrent トラッカーサイトでは、ユーザーはソフトウェアに感染、悪意ありや、その他の表記をマーク付けすることができます。

モバイルアプリケーションについては、Apptackr が BitTorrent に取って代わっています。BitTorrent トラッカーサイトと同様に、すべての Apptackr リンクが著作権が侵害されたアプリケーションに接続しているわけではありません。ただし、BitTorrent トラッカーサイトと同様に、生じる Apptackr トラフィックのほとんどが、著作権が侵害されたアプリケーションのダウンロードによるものである可能性が高いです。

アプリケーションストアのダウンロードの安全性を議論する際に、なぜこのことが重要になるのでしょうか。Apple iOS デバイスで「App Store」をクリックすると、Apple のストアに入ります。Jailbreak が行われて、著作権が侵害されたアプリケーションをインストールするように再構成された電話では、Installous アプリケーションは Apple の App Store のように機能しますが、著作権が侵害されたアプリケーションを入手するよう Apptackr が示されます。Apptackr をプロキシとして使用してアプリケーションを入手し、アプリケーションはファイルホスティングサイトでさらにプロキシ処理されますが、Installous 自体はアプリケーションストアです。

ただし、分析の観点から、BitTorrent によって、消費者が違法コピーソフトウェアをますます容易に入手できるようになった（その結果、BitTorrent でマルウェアに感染したリンクが増加した）のと同様に、Apptackr によって、著作権が侵害された iOS アプリケーションをますます容易に消費者がダウンロードできるようになっています。

その結果、どのようなことになるのでしょうか。Apptackr からリンクする iOS アプリケーションは、時間の経過とともに、マルウェアに感染したもの（主に著作権が侵害されたアプリケーション）が多くなります。現在、とても興味深いことに、大部分のマルウェアは本質的にサイズが小さいです。ドライブバイダウンロードのマルウェアのサイズを見てみると、平均的なサイズは 1MB よりかなり小さいです。これは、マルウェアでは、ファイルサイズを最小化することで、ダウンロードが行われていることを隠そうとしているためです。ただし、違法コピーソフトウェアの場合は、逆のことが当てはまります。ユーザーはソフトウェアをダウンロードしていることを知っているため、何も隠すものはありません。そのため、サイズの小さいアプリケーションよりも大きいアプリケーションのほうが、トロイの木馬や他のマルウェアを容易に隠す（干し草の山から針一本を探すような）ことができます。Apptackr の場合、著作権が侵害されたアプリケーションはすべてクラックされています。そのため、著作権が侵害されたアプリケーションの場合、変更されていないアプリケーションを検証するパブリックデータベースのハッシュが存在する場合でも（実際には存在しませんが）、アプリケーションがクラックされて本質的に変更されているため、検証することはできません。このように、トロイの木馬やバックドア型のマルウェアすべてを発見するのは、ますます困難になっています。

昨年末に、Apptackr に掲載されていたファイルサイズが最大クラスのアプリケーションをいくつか素早くチェックし、マルウェア (EXE) を直接示しているアプリケーションリンクを発見することができました。この場合、このアプリケーションリンクはバックドアではなく、電話で実行されるものでもありませんでした。このアプリケーションリンクは、Apptackr のポータルユーザーを対象としており、Microsoft Windows ベースのホストを使用してアプリケーションをダウンロードし、Apple iTunes に手動でコピーしていました。その後、このアプリケーションは置き換えられて、今ではトラッキングリンクでマルウェアは示されていませんが、これは氷山の一角に過ぎません。BitTorrent に現在、著作権が侵害されたアプリケーションと思われるマルウェアや最新のハリウッド映画が氾濫

しているのと同様に、Apptackr もマルウェアの感染がますます多くなる可能性が高いです。BitTorrent の場合、電話などのモバイルデバイスについては、クライアントサイドのマルウェア対策ソリューションでいくつかの防御が提供されていますが、大部分については、同様な防御は提供されていません。

「標的型」攻撃

最近、ドイツの学生が、Jailbreak が行われた iPhone に対して鍵回復攻撃が行われる仕組みを解明しました。⁹ さらに、これらの学生は、Apple のパスワード保護によってロックされている場合でも、iPhone を Jailbreak しました。¹⁰ ユーザー環境で攻撃者がこれを行う場合には、この手法を iOS の他の既知のリモートの悪用手法と組み合わせて、攻撃者に利益をもたらす財務アプリケーションやショッピングカートアプリケーションに重要な情報を回復させる可能性が大きいです。さらに、Square やその競合他社などのクレジットカードのトランザクション処理アプリケーションの場合、電話を侵害する攻撃者は、クレジットカードの検証プロセスの利用を監視して、後でクレジットカード情報を転送するバックドアをインストールすることが可能かと考えられます。最近、ToorCon でこれに多少類似した概念実証が行われました。¹¹ この種の攻撃はユーザー環境ではまだ行われていませんが、携帯電話は特に商取引とトランザクションの領域で生活にますます密着したものとなっているため、このような攻撃が行われる可能性が大きくなっています。

最近、インストールされているアプリケーションの特定に関しても、開発が開始されています。iOS のプライバシーホールのために、別の iTunes ユーザーが購入した音楽やアプリケーションを特定することが可能です。¹² いくつかの理由からこの「攻撃」は低リスクですが、これに関係して、攻撃者が、攻撃の対象である特定のデバイスにインストールされているアプリケーションを把握することが可能です。マカフィーでは、モバイルデバイスを対象とした情報収集やプライバシー攻撃が近い将来に増加すると予測しています。

アプリケーションストアでの考えられる展開

アプリケーションストアに掲載されるモバイルアプリケーション数が急増しています。アプリケーション数が膨大であるために、ユーザーが関心のあるアプリケーションと関心のないアプリケーションを区別するのが難しい場合があります。モバイルアプリケーション向けのレピュテーションベース推奨システムである、Apple の Genius の推奨機能のような機能が、ますます重要となって大幅に強化される可能性が大きいです。Apple の App Store などの一元化されたアプリケーションストアでは、安全とセキュリティ上の理由から、アプリケーションの動作や API (アプリケーション プログラミング インターフェイス) 呼び出しを確認するため、ベンダーがバックエンドの自動化にますます多くのリソースを使う可能性が大きいです。アプリケーションのセキュリティ分析サービスを提供している会社には、最近、iOS アプリケーションや Android アプリケーションのサポートを提供して、この考えをさらに推進している会社もあります。さらに、評価、推奨、ダウンロード数、販売のメタデータはすべて、ますます一元管理が進んで、妥当性が追跡される (アプリケーションレピュテーションシステムに提供するため) ようになる可能性が大きいです。特に、最近、Android マーケットで一連のアプリケーションにバックドア型のトロイの木馬が組み込まれたという注目を浴びた事例があるため、Google がある程度のフェデレーションや新しく投稿されたアプリケーションの自動セキュリティスキャンを導入する可能性が大きいです。

9. http://www.sit.fraunhofer.de/en/Images/sc_iPhone%20Passwords_tcm502-80443.pdf

10. http://www.youtube.com/watch?feature=player_embedded&v=uVGiNAs-QbY

11. http://sandiego.toorcon.org/index.php?option=com_content&task=view&id=48&Itemid=9

12. <http://andrewmcafee.org/2011/02/mcafee-apple-itunes-privacy-hole-violation>

注意の喚起

リスクに直面して、企業と消費者の両方で注意が必要となっています。ソフトウェアだけをダウンロードして、信頼できる URL (少なくとも、ある意味) だけにアクセスするという、よく知られているルールを守ります。Jailbreak が行われた iOS デバイスには信頼できないソフトウェアがインストールされている可能性が高いため、企業では、これらのデバイスすべてが企業ネットワーク (電子メールを含む) にアクセスするのを禁止するポリシーを検討する必要があります。消費者においては、著作権が侵害されたアプリケーションを使用するのは、違法であると同時に危険です。バンキングアプリケーションでマルチタスクを実行するのと同じデバイスで、クラックされたアプリケーションを実行すると想像してみてください。好ましくないのは明らかです。Android マーケットのアプリケーションにバックドア型のトロイの木馬が含まれていたという最近のケースのように、「正規」のアプリケーションでも疑いを持って、消費者と企業の両方が自らを保護する必要があります。

McAfee Labs について

McAfee Labs は、世界各地に存在するマカフィーの研究機関で、マルウェア、Web、電子メール、ネットワークなどに対する脅威を研究・調査し、脆弱性の報告を行っています。McAfee Labs は、世界各地に数百万台のセンサーを配備し、クラウド型サービスの McAfee Global Threat Intelligence™¹³ により情報収集を行っています。世界 30 か国に存在する McAfee Labs には、様々な分野を専門とする 350 名の研究者が在籍し、企業や一般のユーザーを保護するため、リアルタイムの脅威検出、アプリケーションの脆弱性特定、リスクの相関分析、迅速な問題解決に努めています。

マカフィーについて

マカフィーは、インテル・コーポレーション (NASDAQ : INTC) の完全子会社であり、セキュリティ・テクノロジー専門のリーディングカンパニーです。世界中で使用されているシステム、ネットワーク、モバイルデバイスの安全を実現する革新的なソリューションとサービスを提供し、ユーザーのインターネットへの安全な接続、Web の閲覧およびオンライン取引の安全を確実に支えています。マカフィーは、他の追随を許さないクラウドベースのセキュリティ技術基盤 Global Threat Intelligence™ (グローバル スレット インテリジェンス) を活用して、革新的な製品を送り出しています。個人ユーザーをはじめ、企業、官公庁・自治体、サービスプロバイダーなど、様々なユーザーはコンプライアンスの確保、データの保全、破壊活動の阻止、脆弱性の把握を実現し、またセキュリティレベルを絶えず管理し、改善することができます。お客様の安全を確保するため、マカフィーは、新しい手法の開発に日々真摯に取り組んでいます。www.mcafee.com/jp

13. <http://www.mcafee.com/us/mcafee-labs/technology/global-threat-intelligence-technology.aspx>