レポート

モバイルセキュリティ：McAfee 消費者動向レポート

危険なアプリ、モバイル上の不正行為、スパイウェアの動向

目次

本レポートについて 3
主な調査結果 3
危険なアプリの定義：マルウェアと疑わしいURL 3
危険なモバイルアプリの供給元 4
悪意のSEOとモバイルアプリストア 5
アプリのダウンロードは6回に1回危険 5
マルウェア＋疑わしいURL＝高度な詐欺 6
モバイルマルウェアの定義 6
多数の不正行為 7
再利用可能なコード、再利用可能なボット、再利用可能なボットネット 8
スパイウェアに対する注目 9
次には何が？ 10
リソース 10

本レポートについて

セキュリティ調査とモバイルセキュリティ製品の先導役としてモバイルの脅威の実態について個人ユーザーを啓蒙するため、マカフィーは広範なグローバル脅威インテリジェンスデータベースを収集しています。本レポートでは、サイバー犯罪者たちが悪性コードや Web サイトをどのように利用しているか、またどのように組み合わせて利用し、個人ユーザーの所有するデバイスや個人情報を狙っているかをまとめています。

本レポートの焦点は、「現実のリスク」です。平均的なモバイルデバイスユーザーは、どのくらいの確率でマルウェアや疑わしい Web サイトに遭遇しているのでしょうか。マルウェアは、どのような活動をするのでしょうか。こうした「現実」の分析によって、マカフィーが集めたアプリとモバイルマルウェアすべてを含めたズー（Zoo）と、McAfee Mobile Security のユーザーから収集されたデータを比較対照します。

主な調査結果

- PC によくあるメールベースや Web サイトベースの感染とは異なり、今日のモバイルマルウェアは主に感染アプリ経由で拡散
- マカフィーが収集したモバイルアプリズー全体で、マルウェア感染アプリの 3%は Google Play ストアからきている
- 保守的とされるマカフィーのユーザーコミュニティ内では、マルウェア感染アプリの 75%が Google Play からダウンロードされたもの
- 不正アプリストアは悪意の検索エンジン最適化（SEO）を使用
- マカフィーユーザーの経験によると、典型的な個人ユーザーは、少なくとも 6 回に 1 回はマルウェアや疑わしい URL を含むアプリをダウンロードする可能性がある
- マルウェアを含んでいる危険なアプリのほぼ 4 分の 1 は、疑わしい URL も含んでいる
- 40%のマルウェアファミリーは、複数の手段で不正を行っており、犯罪者たちの高度な知識や意欲が表れている
- 23%のモバイルスパイウェアは、ボットネットを組み合わせたり、バックドアを開いたりして、データ喪失やデバイス不正使用のリスクを高めている

ユーザーは、一旦スマートフォンやタブレットを所有したら、そう簡単には手放しません。ユーザーが充実したモバイルデジタルライフを送る際に、リスクの所在を把握して、そのリスクを回避できることをマカフィーは願っています。

危険なアプリの定義：マルウェアと疑わしい URL

危険なアプリは、サイバー犯罪ツールを配達するトラックにあたります。このトラックは、あらゆる悪性コードやハッカーツール、犯人が管理する Web サイトへのリンクを運搬することが可能です。危険なアプリには、個人情報を盗んだり（プライバシー侵害や、なりすまし犯罪）、詐欺を実行したり（SMS コンテンツ詐欺など）、デバイスを犯罪ボットネットワークの一部に加えて乱用したりすることのできるモバイルマルウェアが組み込まれています。

また、危険なアプリは極めて複雑なスキーム（本レポートで後述）を許可するためにマルウェアと疑わしい URL の組み合わせを含んでいる可能性がありますが、マルウェアを一切含まず、疑わしい URL だけを含んでいるものもあります。

多くの場合、疑わしいリンクは個人ユーザーのモバイルデバイスを（詐欺師にとって）収益性の高い詐欺に巻き込む効果があります。こうした URL は、クリック詐欺や個人情報フィッシングを実行したり、怪しいコンテンツの宣伝や、スパムのような迷惑通信の後押しを行ったりします。ほとんどのデバイス所有者は、こうしたいろいろな活動を避けて自分の行動を意識的に選ぶためにデバイス、時間、データプランを利用しようとします。

ドライブバイダウンロードサイトに誘導する疑わしい URL が含まれているアプリは、これまでほとんど見られません。Web ページ上にある大半のマルウェアが、いまだにユーザーによる「許可」を必要としているので、個人ユーザーはインストールをキャンセルすることができます。しかし、マカフィーでは 2012 年、初のモバイル向けドライブバイダウンロードを確認しました。2013 年にはさらなる増加を見込んでいます。[1]

用語集

危険なアプリ—ダウンロード可能なモバイルアプリ。何らかの形態でマルウェアや疑わしいWebサイトへのリンクを含んでいる。

疑わしいURL—マルウェア、ブラウザーエクスプロイト、フィッシング詐欺行為、スパム登録フォームや、その他の怪しいWebサイトのアフィリエイトを含んでいるWebページ。

マルウェア—不正コードまたは潜在的に望ましくないコードの一意の検体で、様々な形をとるウイルス、トロイの木馬、ワーム、エクスプロイトコードなどを含む。

マルウェアファミリー—系図のように、同一コンポーネントから発展する一意の検体の関連グループ。同一の活動パターンを示す。

マルウェアパッケージ—マルウェアファミリーの個別の実装や亜種。セキュリティソフトウェアに認識されずに済むよう、同一ソフトウェアが再コンパイルされたり、操作されたりすることが多い。

ズー—「アプリズー」「マルウェアズー」など、何かの検体をすべて集めたコレクション。

データの比較について

各ベンダーの発表する脅威データの比較について、疑問に思うことはありませんか。それぞれの数字が異なっているのは、脅威データを分類、算出、報告する方法を各ベンダーが別々に決めているためです。ベンダーは、脅威を実行していることが判明した一意のマルウェアファミリーや、そうしたファミリーの一意のパッケージ、すべての考え得る一意のマルウェアインスタンスを報告することがあります。ベンダーが報告する一意のマルウェアインスタンスの数は、大抵の場合、マルウェアファミリーやマルウェアパッケージのみを報告するベンダーの数値よりも多いものです。

例えば、100 種類以上の方法で Skull マルウェアファミリーがパッケージされているのが見つかったことがあります。これらのパッケージは、その後再編成と再コンパイルが行われ、多種多様なアプリインスタンスに展開されます。中心では、同一の Skull マルウェアファミリーが同じ脅威を実行します。

様々な数字が出回ると混乱が生じるため、マカフィーでは主に割合と動向に焦点を合わせることにしました。このレポートには、アプリで発見された一意のマルウェア検体と個別のマルウェアパッケージの両方の分析を反映させています。マカフィーは、一意のマルウェアインスタンスに基づいてアプリ供給元に関する結論を出していますが、把握したリスクが大げさに認識されることを避けるため、インスタンスの総数は記載しません。

読者の皆さまにマルウェアの多様性が急速に広がっている感覚を持っていただくために、マカフィーではすべての「McAfee 四半期脅威レポート」に、それまでに報告された一意のマルウェアパッケージ数を記載します。

危険なモバイルアプリの供給元

マカフィーの研究データベースには、モバイルアプリ（無害のアプリと危険なアプリ共に）の膨大なコレクションが収録されています。気になる検体はプロアクティブに探査するなど、悪性のものは念入りに調査しているため、アプリデータベース全体のうち、危険なアプリが高い割合を占めています。

この有害な状況は、一般的なモバイルデバイスユーザーの環境を示しているわけではありませんが、

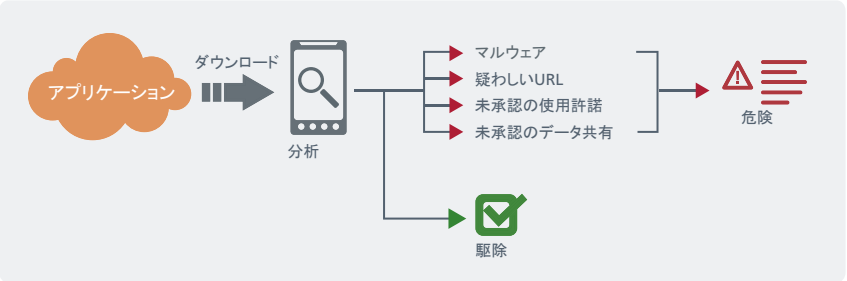

図 1. マカフィーのソフトウェアは、ダウンロードされたすべてのアプリをスキャンして、悪意のあるコンテンツが中に含まれているかどうかや、アプリがユーザーの信用とプライバシーを侵害する可能性があるかどうかを確認する。

犯罪ネットワークに関する興味深い洞察を与えてくれます。例えば、マカフィーが最初に調査したのは、マカフィーの自動収集ソフトウェアがマルウェア感染アプリを発見したストアです。[2] クローラーによって、マカフィーが収集したマルウェア感染アプリ全体の 57%が、3 つのアプリストアのものであるということが判明しました。すべてロシアのストアに集中しています。これは、おそらく組織的な犯罪グループが運営していると言えるでしょう。ちなみに、Google Play ストアを供給元とするものは、マルウェア感染アプリズー全体の約 3%のみでした。マカフィーの検体の中で、マルウェア感染アプリの供給元としては第 9 位の規模でした。

次に、McAfee Mobile Security のユーザーがダウンロードしたマルウェア感染アプリの供給元を調べました。この数値には、大きな差がありました。Google Play はあらゆる Android ユーザー向けアプリの最大の供給元なので、75%のマルウェア感染アプリが Google Play から来ていても、特に驚くことはありませんでした。ほかの商用ストアや携帯電話会社が経営するストアは、マルウェア感染アプリ供給元リストに登場しませんでした。

つまり、Google Play は多くのアプリストアよりも安全ですが、ユーザーはどのようなアプリにも警戒する必要があるということです。アプリがリクエストする許可に注意してください。すべてのアプリのマルウェアスキャンを実行してください。プレミアムコンテンツ詐欺を速やかに見つけられるよう、毎月の請求書に目を光らせてください。

供給元	全マルウェア感染アプリズー（供給元）	供給元ランキング	McAfee Mobile Security がインストールされた基盤のマルウェア感染アプリズー（供給元）	供給元ランキング
供給元1（ロシア）	26%	1	3%	4
供給元2（ロシア）	22%	2	1%	10
供給元3（ロシア）	9%	3	0%	21
Google Play	3%	9	75%	1

悪意の SEO とモバイルアプリストア

多くのユーザーは、商用アプリストアでは入手できない、母国語で使えるゲームやユーティリティといったコンテンツを求めています。ユーザーが購入先ストアを変えるとリスクは高まります。例えば、Google と Adobe は、Android 向け Flash Player の配布を 2012 年に中止しました。[3] Flash コンテンツを使った Web サイトにアクセスしたいユーザーは、依然としてプレーヤーアプリが必要なので、検索エンジンを使ってアプリを探すことがあります。そこで、怪しいアプリを扱うストアの経営者がチャンスを掴みました。マカフィーは、「Android 向け Flash Player」という言葉をいろいろに変化させた名を持つ、5 つのアプリストアを発見しました。

研究者たちは、このテクニックを「悪意の検索エンジン最適化（SEO）」と呼んでいます。犯罪者たちは、被害者になり得る人がコンテンツをどのように検索するかを考えてから、そのキーワードを自らの URL や Web ページ、ページタグに使用します。検索エンジンの結果ページで合法コンテンツよりも上位に表示され、クリックされることを期待しているのです。トラフィックを増やすために、詐欺師たちはフィッシング詐欺やスパム（従来のメール、ソーシャルメディア、SMS メッセージで配布されるリンク）を利用して、被害者を自分のサイトにおびき寄せることがあります。

ユーザーが不正アプリをダウンロードすると、犯罪者の利益になります。犯罪者は、本レポートで述べる様々な方法で、被害者のデバイスを掘り出してデータを入手したり、不正使用したりすることができます。

同様に、ほかの 4 つのアプリストアも「cut the rope（ロープを切って）」という言葉を使ってユーザー（特に子供）をおびき寄せ、キャンディを食べるモンスターのゲームをさせたと考えられます。このゲームは、あるレビューアから「『Angry Birds（アングリーバード）』並みにハマる」と評されています。[4] 大ヒットが詐欺を生み出しているというわけです。

悪意の SEO は、モバイルスペースで特に効果を上げています。ユーザーにとっては、実際に自分がアクセスする URL を把握することが難しいためです。モバイルブラウザーでは、デフォルト設定で目に見えるウィンドウに URL が表示されません。URL が完全に見えない場合、攻撃者はタイポスクワッティング（正規のサイト名とほぼ同じサイト名を表示すること）や専用 URL を利用してユーザーを騙し、amazon.com などの目当てのサイトにアクセスしていると思わせることができます。

また、HTML5 でコンテンツを作成している開発者は、目に見える URL やアドレスバーを使わずに、サイトをネイティブモバイルアプリに見えるように表示することができます。アドレスバーを見るために、ユーザーはページの下へ移動する、つまりページの下まで「通過する」必要があります。その時でさえ、ユーザーはモバイル画面で URL 全体を確認することはできないはずです。[5]

アプリのダウンロードは 6 回に 1 回が危険

次に、マカフィーのユーザーコミュニティがダウンロードした危険なアプリの性質をさらに細かく調べました。現実のユーザーが実際に直面するリスクの種類と度合は、想像以上の結果がでています。マカフィーユーザーが 2012 年 4 月から 12 月までの間にダウンロードしたアプリの 16%（アプリ 6 つに 1 つ）がマルウェアに感染しているか、または危険な URL へのリンクを含んでいることが判明しました。

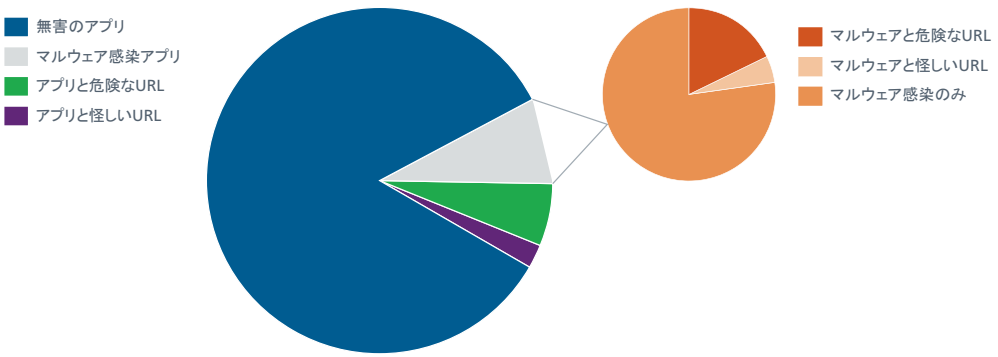

図 2. マカフィーユーザーの記録では、6 件に 1 件の割合で危険なアプリをダウンロード。マカフィーユーザーがダウンロードした 8% のアプリはマルウェアに感染、23% は疑わしい URL も含んでいた。

4 つの不正アプリストアは、「cut the rope（ロープを切って）」という言葉でゲーマーを餌食に

（画像は Amazon.com 社提供）

マカフィーの「実環境」データソース

McAfee Mobile Security ユーザーがダウンロードしたアプリは、全体で 430,000 超を超えています。これは、アプリ 1 個のすべてのリリースとバージョンを数えた数です。例えば、Facebook アプリには 50 種類があります。

ユーザーがアプリをダウンロードすると、マカフィーソフトウェアは以下をはじめとする様々なことを調べます。

- アプリがリクエストする許可
- データ共有の有無
- マルウェアの存在
- アプリに含まれている URL のレピュテーション

McAfee Mobile Security が危険度を示すので、ユーザーはそのアプリを簡単に削除できます。

McAfee Mobile Security のユーザーは、モバイルセキュリティ製品を使用しているため、比較的リスクを回避していることは明らかです。また、危険と評価されている Web サイトに自分がアクセスしようとしているかどうかの警告を確認することができます。この警告は、危険なアプリに遭遇する前に止まるチャンスを与えてくれます。これらの理由によって、マカフィーは、6 つに 1 つのアプリは極度に危険であると確信しています。予防接種を受けていない子どものように、モバイルセキュリティを実装していないデバイスには、極めて大きな感染リスクがあります。

マルウェア＋疑わしい URL ＝高度な詐欺

次に、マカフィーは 8%の危険なマルウェア感染アプリを調べました。中には、複雑なマルウェアも見られました。約 23%は、マルウェアと疑わしい（危険、または怪しい）URL の両方に感染しています。マルウェアと疑わしい URL の両方に感染しているアプリは、広告インプレッションやクリックを水増しする悪意の SEO プログラムに利用される可能性があります。このように利用するために、悪性コードはブックマークをブラウザーに追加したり、ターゲット Web サイトや広告 URL を起動するアプリをインストールしたりするかもしれません。さらに高度なマルウェアは、広告クリックの実行を試みたり、トラフィック数に基づいて犯罪者に報酬を払うフォーラムやサイトにユーザーを誘導しようとしたりします。

モバイルマルウェアの定義

マカフィーでは、アプリが以下の 1 つ以上を実行する場合に、そのアプリがマルウェアに感染していると分類しています。

- デバイス情報や個人情報をユーザーの許可なく他人に送信する
- アクティビティ（閲覧履歴、メッセージ、動画再生）を密かに見張って記録する
- 着信音やダウンロード、加入データの各サービスを売りつけるために、高額な SMS メッセージを送信する
- クリック詐欺を働く
- デバイス上の脆弱性やソフトウェアのバグをエクスプロイトして、ユーザーの予想外のことを実行する（多くの場合、別のマルウェアのダウンロードを媒介する）
- デバイスをルート化して、攻撃者がそのデバイスを制御できるようにする
- バックドアをインストールしたり、デバイスをボットクライアントに変えたりする。余得として個人情報を収集することも多い
- 攻撃者がユーザーのデバイスを制御できるよう、ハッキングツールをインストールする
- Web サイトから 2 次的な悪性コードをダウンロードする
- ユーザーのデバイスやデータを破壊する
- ユーザーのデバイスから SMS 経由でスパムメッセージを送信する

多数の不正行為

マカフィーは、2007 年～ 2012 年に確認された Android6 マルウェアファミリーの分析を行いました。判明したのは、ハンドセット情報の送信やスパイ行為が、マルウェアファミリーのすべての不正行為の約半分に相当していたという点です。

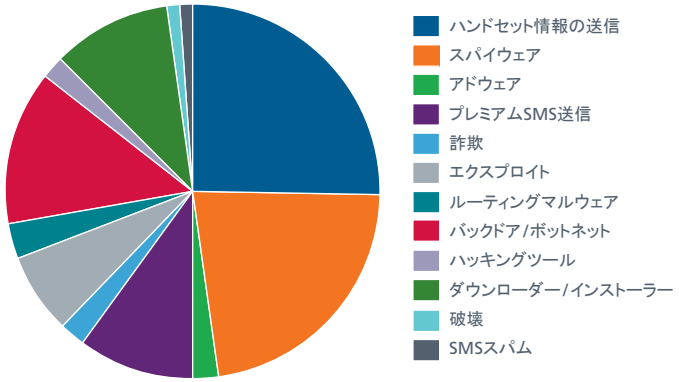

図 3. モバイルマルウェアが示す様々な不正行為や、潜在的に望ましくない行動。

また、40%のマルウェアファミリーが複数の形態の不正行為を示したことも判明しました。この複雑さが、犯罪者の成功を 2 つの方法で助長しています。1 つは、攻撃者がデバイスのテクノロジーや脆弱性にあわせて各攻撃をカスタマイズすることがでるということです。2 つめは、組み合わせの中には、ユーザー（またはセキュリティソフトウェア）がその活動を異常行動や不正行為として認識しにくいものがあります。攻撃者が気付かれずに不正行為を実行できるようにするためです。

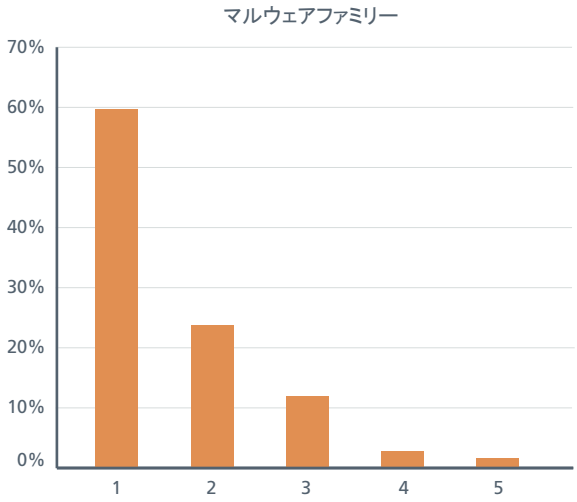

図 4. 40%のマルウェアファミリーが、複数の形態の疑わしい活動を含んでいる。

マカフィーは、4 つ以上の不正行為を含んでいるファミリーに以下のような共通の要素があることを発見しました。

- 100%が、個人情報やデバイス情報を送信
- 100%がデバイスにバックドアやボットネットをセットアップ
- 75%がダウンローダーやインストーラーを含む
- 62%がスパイウェアとして活動
- 50%がルーティングマルウェアを保有

これらの綿密に設計された攻撃には、「DroidDream」、「RootSmart」、「Stiniter」[7]、「DroidKungFu」[8]、「Geinimi」、「DroidDreamLite」など、報道で見聞きした覚えがあるかもしれない名称が含まれています。これらのファミリーのいくつかは、次のような共通の特徴を持っています。

> *「DroidKungFu.A は、Geinimi や Android/ DrdDream などの複雑な Android マルウェアファミリーからヒントを得ており、このDroidKungFu.Aのコードは、多数のゲームをはじめとする様々なアプリに含まれています。DrdDream と同様に、DroidKungFu.A もまた、システムのセキュリティを低下させてデバイスにとどまるために 1 組のルートエクスプロイトを使用します」*
>
> *—「McAfee Security Journal」2011 年 7 号*

デバイス情報の送信と、バックドアクライアントやボットネットクライアントのセットアップが 100% 重複していることは理解できます。ハッカーが、ユーザーのデバイスをボットネットワークの一部に組み込んだり、ユーザーの行動情報を収集しようとしていると想像してください。ユーザーのデバイスと通信するために、ハッカーにはデバイスの識別番号が必要です。つまり、マルウェアインストール後の最初の仕事は、デバイス情報をデバイスから送信することです。

マカフィーは、75%の極めて複雑なファミリーが、次のステップに進んだことを発見しました。こうしたファミリーは、マルウェアの追加やソフトウェアの制御を行って、スパイウェアやルーティングマルウェアなど、さらに多くのツールを攻撃者に渡します。iPhone のルーティングや脱獄と同様に、ルーティングマルウェアは攻撃者が内部統制を踏み越えてデバイスを支配できるようにします。

再利用可能なコード、再利用可能なボット、再利用可能なボットネット

ボットネットクライアント、ダウンローダー、ルートキットは一般的に、ソフトウェアツールキットの一部としてブラックマーケットで売られる便利なソフトウェアです。このようなあらかじめ同梱されたツールキットを使うと、犯罪者は手間をかけず、深い技術専門知識なしで、それぞれの目的に適したパッケージを作ることができます。いくつかのオプションと規則を選択するだけで、プレミアム SMS、クリック詐欺、スパム配信、データ窃盗、銀行詐欺を簡単に実行することができます。

営利目的の犯罪者たちは、新しいスキームを考え出すと、これらのコンポーネントを再利用し、組み立て直します。ボットネットマネージャーやボットハーダーが、ボットネットワークを有料でも喜んで借りる別の犯罪者を見つけると、ボットハーダーは、コードに貸し主の新しいコマンドをロードすることができます。こうしたクラウドを使用した巧妙な犯罪では、同じベーシックボットネットのネットワーク構成が別の犯罪に協力します。例えば、「モバイルセキュリティ：McAfee 消費者動向レポート」では、Android/Funsbot.A と Android/Backscript.A という 2 つの攻撃の多用途性について、次のように説明しています。

「Android/Funsbot.A は、大規模で高度な APT マルウェアキャンペーンの一端だったボットネットクライアントです。このボットネットクライアントは、攻撃者のサーバーからファイルをアップロード／ダウンロードするよう命令します。また、感染した Android デバイスのディレクトリを参照することもできます。これにより、攻撃者は特定のターゲットに関する情報を収集できるようになるほか、そのターゲットの制御を維持・増強することもできるようになります。

Android/Backscript.A も、また別の高度な Android マルウェアです。このボットネットクライアントは、攻撃者のコントロールサーバーから新しいコマンドや機能の最新情報を入手します。そして、ネイティブ実行ファイルをダウンロードする代わり、モバイル Java 内で実行する形式の JavaScript を使って展開時間を短縮します。現在のところ、このマルウェアは、特定のサードパーティアプリケーションをペイ・パー・インストール方式でインストールしているので、ほかのアプリケーションを有償でインストールするように簡単に更新することができます」

インターネットの匿名性によって、簡単にマルウェアを構築したりレンタルすることができます。他人の動作中のシステムを盗むことは、さらに簡単です。中国では、犯罪者たちが互いのモバイルデバイスのボットネットを乗っ取ることが珍しくありません。

スパイウェアに対する注目

23%のスパイウェアは、ボットネットへのデバイス追加やバックドア開放も実行

本レポートでは、スパイウェアの調査を行なっています。スパイウェアは、マカフィーのズーに収録されているマルウェアファミリーの約 3 分の 1 に相当することが判明しました。その大半はスパイウェアは、閲覧履歴やメッセージ、ロケーションの監視・記録を行う「単なる」スパイウェアです。しかし、一部のスパイウェアは積極的に害を及ぼします。スパイウェアに分類された 70 のマルウェアファミリーのうち、23%はボットネットクライアントやバックドアを起動しました。上述した一種の乗っ取りを有効にするためです。一方で、7%はプレミアム SMS メッセージを送信していました。

Geinimi はスパイウェアの好例で、ボットネットに加わります。SMS メッセージを攻撃者に転送することもあります。それによって攻撃者は、銀行やプレミアム SMS サービス、送金サービスからのメッセージを入手できるようになります。さらに、新しいスパイウェアやアドウェアをインストールし、ユーザーの連絡先を盗んでワームを配信したり、スパムの標的にしたりすることも可能です。広告をクリックさせたりトラフィックを発生させたりするために、ブラウザーに URL をロードすることもできます。

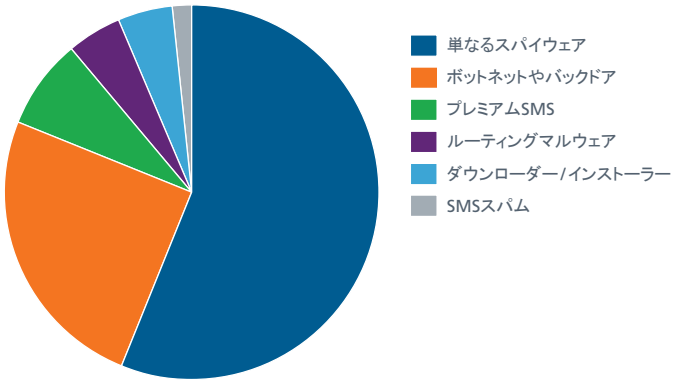

図 5. スパイウェアには、しばしば別の不正行為も含まれていることが判明。

スマートデバイスはスマートに使いましょう

不正アプリを避けるために

- アプリのダウンロードは、Google Play などのよく知られたモバイルデバイスメーカーや携帯電話会社が運営するストアからに限る
- 不審なアプリをダウンロードしないようにする
- 使用しているセキュリティソフトウェアが危険と指摘するアプリを削除する

商用ストアから入手できないアプリが欲しい場合は、必ずモバイルセキュリティソリューションを利用して、そのアプリの許可、レピュテーション、コンテンツを確認してください。

次には何が？

マカフィーでは、近い将来に攻撃がますます高度化すると予想しています。自動実行型ドライブバイダウンロードが多用されそうなことから、マルウェア感染の中でも疑わしい URL の成功率が上がるでしょう。ドライブバイダウンロードと悪意の SEO を組み合わせることで、すでに実証されているほかの PC 指向の脅威がモバイルデバイス環境に移行すると考えられます。

犯罪者たちはまた、モバイルデバイス特有の機能から利益を生み出す方法も探るでしょう。2012 年中に、デバイスをプレミアム SMS に加入させようとするマルウェアファミリーは約 16%でした。2013 年は、MarketPay のような脅威が増加していくと予測しています。当然ながら、MarketPay はサードパーティアプリストアのユーザーを標的にするプレミアムコンテンツです。ユーザーは、請求書をチェックしなければ、自分がプレミアムアプリを購入したことに気付きません。

マカフィーでは、2013 年に詐欺指向のマルウェアが増えると見込んでいます。画期的なコンテンツ詐欺になるおそれのあるマルウェアが、モバイルペイメントプログラムや「デジタルウォレット」に用いられるタップ & ペイ型近距離通信（NFC）技術を不正使用するでしょう。この詐欺は、近接していることを利用して（いわゆる「bump and infect（ぶつかった相手に感染）」手法で）繁殖するワームを伴う可能性があります。この配布経路は、列車 1 台分の乗客やテーマパークを介してマルウェアを速やかに拡散することができます。新たに感染したデバイスを使って、その後の買い物の支払いを「タップ & ペイ」で行うと、詐欺師がそのウォレットのアカウントの詳細を収集し、そのクレデンシャルをこっそり再利用してウォレットの中身を盗み取るというわけです。

詳細情報が必要な場合、新たに発生しそうな懸念に関する説明については、McAfee Labs「2013 年の脅威予測」レポートでご覧いただけます。同レポートでは、携帯電話のセキュリティ更新を阻止するマルウェアや、プログラミングスキルを持たない犯罪者たちがデバイスを解除するために金銭をゆすり取ることのできるランサムウェア「キット」について説明しています。ゾンビマシンを復活させるために、ボットネット解体後にルートを再生させたマルウェアについて、どのようにお考えでしょうか。今後のレポートにご期待ください。マカフィーの研究員たちは、あらゆる取り組みがいのある、そして危険なモバイル脅威の進歩を常に追跡しています。

リソース

モバイル脅威の展望における変化の最新情報は、下記でご確認ください。

- McAfee Security Advice Center
- 『99 Things You Wish You Knew Before Your Device was Hacked（デバイスを乗っ取られる前に知っておきたかった 99 のこと）』
- mcafee.com/us/mms

McAfee Labs について

McAfee Labs は、世界各地に存在する McAfee の研究機関で、マルウェア、Web、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™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 500 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、企業、官公庁・自治体、個人ユーザーが安全にインターネットの恩恵を享受できるよう、世界中のシステム、ネットワーク、モバイルデバイスを守るプロアクティブで定評あるセキュリティソリューションやサービスを提供しています。マカフィーは、Security Connected 戦略、セキュリティにハードウェアを活用した革新的なアプロ—チ、また独自の Global Threat Intelligence により、常に全力でお客様の安全を守ります。詳しくは、http://www.mcafee.com/jp/ をご覧ください。マカフィーでは、セキュリティに関する様々な研究成果や調査結果を web 上で公開しています。詳しくは下記ページをご覧ください。
http://www.mcafee.com/japan/security/publication.asp

1 In Spring 2012, researchers discovered NotCompatible, the first mobile drive-by download malware that installed silently when a user visited a site, without the user “accepting” the code.

2 Our overall zoo contains app samples that our crawlers have found, as well as samples identified by other researchers. We only have source information for the apps identified by our crawlers.

3 http://howto.cnet.com/8301-11310_39-57554629-285/install-adobe-flash-player-on-jelly-bean-devices/

4 http://www.ign.com/articles/2010/10/08/cut-the-rope-iphone-review-the-next-angry-birds

5 http://blogs.mcafee.com/mobile/mobile-browsers-trouble-comes-in-threes

6 As of the end of 2012, developers had written 97 percent of mobile malware for the Android platform.

7 DroidDream was active in 2011. The McAfee Labs First Quarter 2012 Threats Report said of RootSmart and Stiniter: “Android/RootSmart.A uses a root exploit to download Android/DrdLive.A, a backdoor Trojan that sends premium-rate SMS messages and takes commands from a control server. Android/Stiniter.A uses a root exploit to download additional malware and sends information from the phone to sites under the control of the attacker. It also sends text messages to premium-rate numbers. The attacker’s control server updates the message body and the number the hijacked phone sends to.”

8 “At the end of May, new malware was discovered in the official Android Market by researchers at North Carolina State University. Named DroidKungFu, this malicious software is capable of burrowing into the root level on vulnerable Android devices using the classical RageAgainstTheCage and CVE-2009-1185 exploits initially implemented by DroidDream. But, unlike its predecessor, DroidKungFu will use AES to encrypt the two exploits to evade detection from current mobile antivirus software. Aside from this difference, the behavior of the malware is the same as DroidDream: it collects information about the device, and it installs a second application that can download more malicious software onto the device. “Android Malware: Past, Present, and Future”

McAfee
An Intel Company

マカフィー株式会社
www.mcafee.com/jp

東京本社　〒150-0043 東京都渋谷区道玄坂 1- 12- 1
渋谷マークシティウエスト 20F
TEL 03-5428-1100（代）FAX 03-5428-1480

名古屋営業所　〒460-0002 愛知県名古屋市中区丸の内 3-20-17
中外東京海上ビルディング 3F
TEL 052-954-9551（代）FAX 052-954-9552

西日本支店　〒530- 0003 大阪府大阪市北区堂島 2-2-2
近鉄堂島ビル 18F
TEL 06-6344-1511（代）FAX 06-6344-1517

福岡営業所　〒810- 0801 福岡県福岡市博多区中洲 5-3-8
アクア博多 5F
TEL 092-287-9674（代）FAX 092-287-9675

MCARPT-MTR-1302-MC