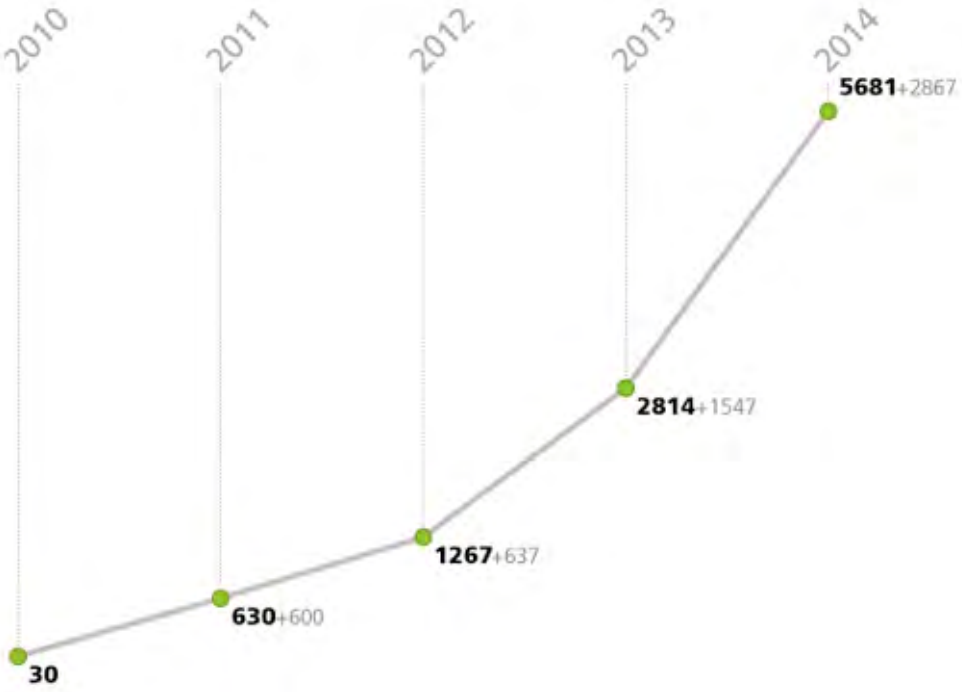
モバイル端末を通じた窃盗

Androidはモバイル端末ユーザーの中で一番人気のあるオペレーティングシステムであると同時に、Windowsに次いで、ウイルス作成者の標的となるケースが最も多いOSです。Androidを狙った初めてのマルウェアは2010年に出現しました。

現在、モバイル端末を感染させるマルウェアのうちに、Androidを狙うものが一番多く、幅広い利用、公開されるコード、及びあらゆるリソースからダウンロード可能なアプリケーションをインストールすることができることがその原因であると考えられます。

以下のグラフはDr.Webウイルスデータベースにおける Androidを狙うマルウェアエントリ推移を示しています。



2014年エントリ数は102%伸びて、2010年から189倍の増加となりました 。

2015年4月1日、Androidを狙うマルウェアを検出するためにDr.Webウイルスデータベースに追加されたシグネチャ数が約9千個に達しました。

2015年1–3月の3か月間に、ウイルスデータベースは25%以上の増加したことになります！

但し、Dr.Webは1つのシグネチャで複数のマルウェアを検出できるため、単純にデータベースの肥大にはつながりません。

Androidを標的にするマルウェアの大半が窃盗用に製作されます。

Androidトロイの木馬を作成する犯罪者たちは、以下のようにモバイル端末の豊富な機能を悪用し、広範囲に窃盗活動を行っています。

- モバイル端末の口座、オンライン決済システム、及びキャッシュカードからの不正引き出し
- オンラインバンキング、オンライン決済システム、ソーシャルネットワークなどのログイン及びパスワード情報の盗み取り
- SMS送受信
- 電話の送受信
- 電子メールの送受信
- 写真の窃盗（インターネット上に写真を掲載し被害者から身代金を要求するなどの行為）
- モバイル端末ユーザーの話を録音します。ユーザー自身が知らないうちに、トロイの木馬に録音されるリスクがあります。
- 連絡先リストの窃取
- ユーザーの所在、及び移動を確認できるためのモバイル端末座標を盗み取ります
- モバイル端末に関するあらゆるデータ（IMEI/IMSI/SID識別番号、携帯電話番号、OS版、SDK、メーカー名など）の情報を盗み取ります。

ユーザー自身がマルウェアをダウンロードし、モバイル端末上にインストールしてしまうという事例が多々発生しています！

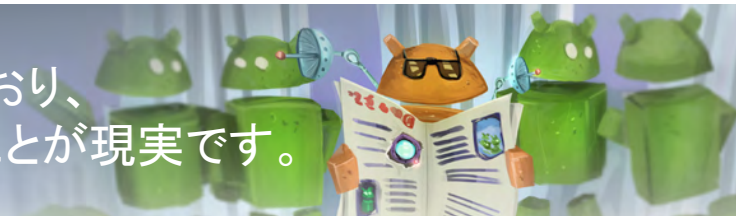
例えば、感染された端末のデータを収集・転送するAndroid.Planktonが、サイト管理者に駆除される前に、公式サイトAndroid Market（旧Google Play）からユーザーに15万回ダウンロードされました！

Dr.Web for Android統計情報によると、およそ50%の同製品利用者が未知のソース（Google Playエコシステムと異なるソース）からアプリのダウンロードを許可するオプションを有効にしています。この情報は、ユーザー自身がフォーラムや疑わしいウェブサイトから知らないうちにマルウェアをダウンロードするリスクを物語っています。

トロイの木馬を大量に配信するために、ソーシャルエンジニアリング手法も悪用されています。韓国ではAndroid対応モバイル端末の30万人以上のユーザーが荷物配達情報をチェックする際に、銀行を狙うトロイの木馬Android.SmsBot.75.originをダウンロードした例があります。

殆どのユーザーは、モバイル端末上にトロイの木馬が進入すれば、それに気づくことが出来ると誤解しています。

しかし、トロイの木馬は巧妙化しており、ユーザーは気付くことが出来ないことが現実です。



ウイルス作成者はユーザーに検知できないようなトロイの木馬の開発を目指しています。

窃盗を試みる最も巧妙なトロイの木馬による被害は、盗難が起きた後でその活動が検知された事例が数多くあります。

- 例えば、Android.Dialer.7.originダイアラーは発信時にモバイル端末のイヤーピースを無効にし、悪意のある活動の痕跡を隠すためにシステムログおよび通話リストを削除することで、ユーザーによる発見を防いでいます。
- ユーザーが知らないうちに有料サービスに加入し、ユーザーのモバイル端末の口座から金銭を不正に引き出すトロイの木馬が潜在的に存在しており、その検出が非常に困難です。一般的には取引終了後、有料サービスから確認のSMSが届きますが、ユーザーが気づかないように上記のトロイの木馬によってSMSが非表示にされます。さらに、有料サービス認証に必要な確認コードが含まれるSMSメッセージを傍受・非表示してから、それを転送するマルウェアも存在します。

- かなり巧妙化したトロイの木馬は正式なソフトウェアとして配信され、起動後自身のアイコンを削除し、ユーザーが知らないうちに動作を続けています。
- さらに、オペレーティングシステム、或いは配信されるファームウェアのイメージに埋め込まれるトロイの木馬が確認されました。このような潜伏するマルウェアは豊富な機能を備えており、悪意のある挙動が広範囲に及びます。
- アンチウイルスに検知されないように、アンチウイルスソフトウェアと同様のプロテクションを施すトロイの木馬さえ存在します。アンチウイルスをブロックしたり、デバイスから削除したりするなどを行うことができます。

オンラインバンクを狙うトロイの木馬

上記のトロイの木馬ファミリーは、キャッシュカードやオンライン決済システムから金銭を不正に引き出す目的で製作されました。

オンラインバンキングがユーザーにとって便利であるため、オンラインバンキング向けのAndroid対応アプリを配信する金融機関が多いです。しかも、このようなアプリは個人用取引のみならず、法人口座にアクセスできる役員が法人間振込み手続きを行うために利用することがあります。

金銭の不正引き出しが、ウイルス作成者の主な狙いの一つです。

Android.BankBot.33.origin

特徴：

- 銀行口座残高、ユーザーのモバイルデバイスに接続されたキャッシュカードなどの情報を詐取します
- 感染されたデバイスのブラウザ上で銀行サイトを装う偽造サイトを表示させ、ログインに必要なデータ入力を促すことで、オンラインバンキングアカウント認証データを盗み取ります
- 被害者の口座から金銭を不正に引き出し、犯罪者の口座に振り込みます

Android.BankBot.33.origin は取引を通知するSMSを傍受・ブロックすることができるため、被害者は暫くの間、窃盗が起きたことを一切認識できない可能性があります。

トロイの木馬をダウンロードするのは、ユーザー自身であるという事実に着目すべきです。オペレーティングシステム設定では外部ソースからプログラムのインストールを許可する設定が有効になっているため、このようなことが起きるのです。

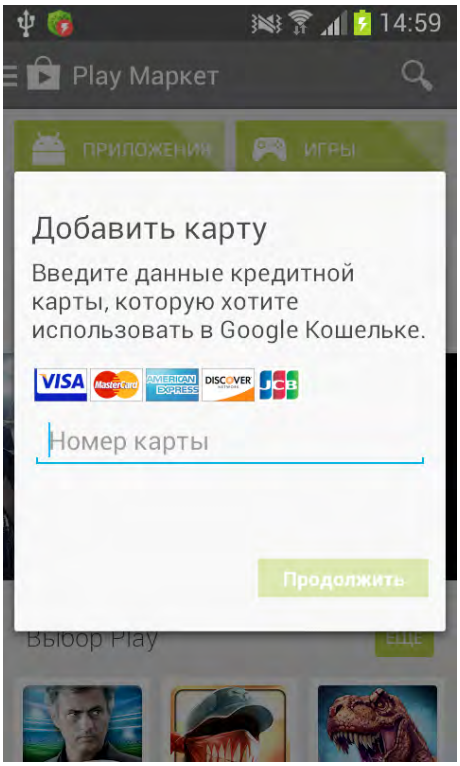
2015年1月－4月の間に、Dr.Web for Androidアンチウイルスを利用するユーザーのAndroidデバイスで、上記のトロイの木馬の検出数が62840回となり、同期間における検出された脅威総合数の0.37%に相当します。

Android.SpyEye.1

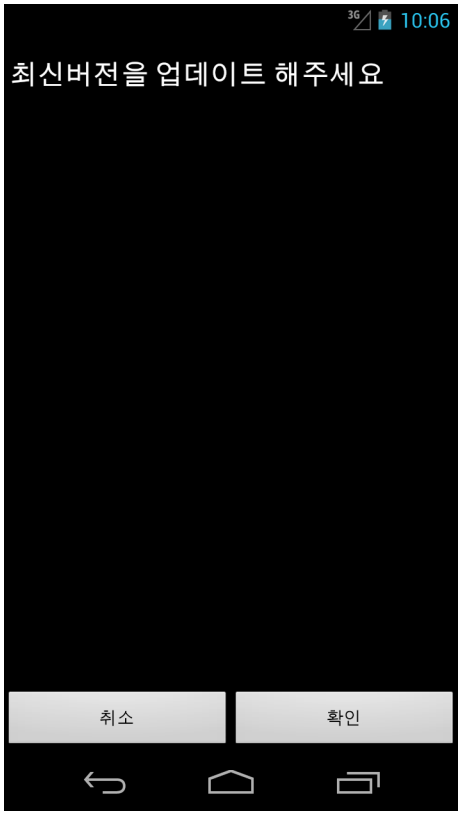
ユーザーのデスクトップ・ノート型PC上に潜伏するトロイの木馬のコンフィギュレーションファイルでは、ユーザーがアクセスした銀行ウェブサイトURLが記録される場合、ユーザーに閲覧されるウェブページ内にログインデータを入力するための外部テキスト又はウェブフォームが挿入されます。リスクを全く認識しないユーザーは、口座のある銀行サイトを開くときに、新しいセキュリティの規則が導入され、この規則を守らないとオンラインバンキングへのアクセスを取得できないといった通知が表示されます。トロイの木馬が仕掛けられたモバイル端末用アプリの更新ダウンロードが促されます。このプログラムは、オンラインバンキングのアクセスに必要なSMS経由で通知される一時的なパスワードの情報を盗み取り、犯罪者に転送することができます。

Android.BankBot.21.origin

キャッシュカードのデータを盗み取りり、金銭を不正に引き出すために、 Android.Bank-Bot.21.origin はモバイル端末上でGoogle Playアプリのウインドウが開かれている状態であることを確認してから、ユーザーアカウント上でキャッシュカードを登録するための標準フォームを真似します。その後、被害者に入力された情報は犯罪者のサーバに送付され、金銭が盗み取られます。



Android.BankBot.29.origin



このトロイの木馬はモバイル端末の管理者権限取得を試みます。自分からのダイアログボックスを表示させることでシステムクエリを隠すことができるため、被害者は悪意のあるアプリに対し要求される権限を与える可能性が高く、その結果として金銭が不正に引き出されてしまうリスクが十分あります。

着信SMSメッセージの盗み取り

SMSの盗み取りが大したことではないと思われる人がいるかもしれません。しかし、実際には、必ずしもそうではありません。

着信SMSメッセージがトロイの木馬に盗み取られると、金銭的な被害が発生するリスクがあります。一体、どのようなSMSが盗み取られるでしょうか？

- 高額のモバイルサービス及びコンテンツサービス加入を確認するSMSメッセージなど。同サービス加入について長期的に何も知らない被害者がトロイの木馬は除去できないように、SMSが盗み取られます。
- オンラインバンキングシステムから送信されるmTAN確認コードを含むSMS

盗み取られたSMSがトロイの木馬を管理する犯罪者のサーバに送信されます。幾つかのトロイの木馬ファミリーがこの機能を備えています。

SMS発信による不正な金銭引き出し

Android. SmsSendファミリーに属するトロイの木馬は被害者のモバイル端末から高額のSMSを発信することで、モバイル端末口座から料金が引き落とされ、犯罪者の口座に振り込まれます。

2014年、Dr.Web for Androidアンチウイルスの利用統計によると、Android. SmsSendファミリーに属するトロイの木馬の検出数が20 223 854回となりました

上記のウイルス以外に、Android.SmsBotファミリーに属するトロイの木馬がSMSメッセージの送信/盗み取り/削除の機能を備えています

2014年、Dr.Web for Androidアンチウイルスの利用統計によると、Android.SmsBotファミリーに属するトロイの木馬の検出数が5 985 063回となりました。

高額な番号への通話発信による不正な金銭引き出し

ダイヤラーは、ユーザーの承諾を得ずにモバイル端末から高額な番号に通話を発信するAndroid向けトロイの木馬ファミリーであり、ウイルス作成者にとって収入を得るポピュラーな方法の一つです。

2014年、Dr.Web for Androidアンチウイルスの利用統計によると、Android.Dialer ファミリーに属するトロイの木馬の検出数が177 397回となりました。

連絡先データの盗み取り

一見、直接的な金銭の搾取と比べて大きな問題ではないように見えますが、実際には連絡先データ自体が販売可能です。それらの連絡先データを入手したい人物は下記のような活動を行っています。

1. スパマー: スパムを送りつける活動が活性化しています。しかし、被害を与えない宣伝だけが配信されると思いこむことは、大きな間違いです。

現在、マルウェアのダウンロードリンクを含んだSMS大量配信がAndroidへの脅威拡散を狙う際に最も使用される手口の1つとなっています。

モバイル端末ユーザーの知り合いのうちにSMSを介して配信されるAndroid.Wormle.1.originが、例として挙げられます。2014年11月末時点で、このマルウェアはおよそ30国で1万5千台以上のAndroidデバイスを感染させています。

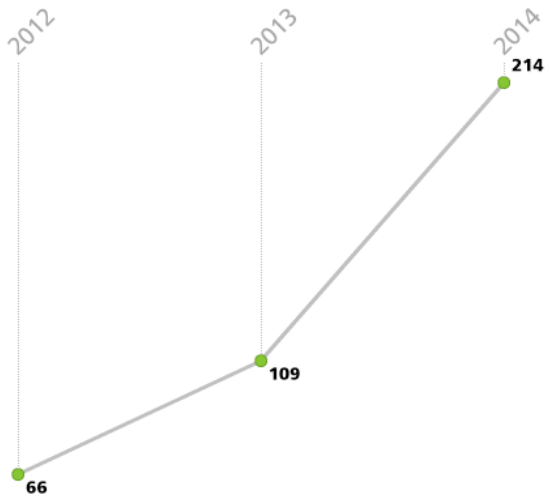
2. フィッシャー: フィッシング迷惑メールを配信するために、連絡先データを入手します。同メールには銀行及び決済システムを装うウェブサイトへのリンクが含まれます。このようなサイトを閲覧するときに、オンラインバンキングにログインするための認証データ、キャッシュカードのデータなどが不正に入手されます。フィッシャーは入力フォームを表示し、銀行ウェブサイトにある入力フォームと何も疑わないユーザーに思い込ませる訳です。

3. DDoS攻撃者:モバイル端末所有者の連絡先の入手を狙っています。モバイル端末を感染させ、DDoS攻撃に利用されます。

4. スパイウェア(諜報機関、ライバル企業):監視対象になるユーザーのメール傍受、通話録音を行うほか、リモートサーバ上にユーザーの写真をアップロードします。この情報はユーザーを恐喝する目的で悪用されるリスクがあります。

Android.Spy.130.originはSMSメッセージの内容、発信コール、現在のGPS座標などのデータを犯罪者に送るほか、ユーザーの承諾を得ずに特定の番号に電話をかけることができます。これによって、感染されたタブレット型PC若しくはスマートフォンの通信が盗聴されます。

Dr.Webウイルスデータベースにおける Android.Spyファミリー属トロイの木馬エントリ推移



以下のSNSをよく使っていますか？

- Google Play
- Google Play Music
- Gmail
- WhatsApp
- Viber
- Instagram
- Skype
- « VKontakte «
- « Odnoklassniki «
- Facebook
- Twitter...?

もし利用していれば、同SNS上に保存される個人データが身代金要求を狙って脅迫を企てる犯罪者に悪用されるリスクがあります！

Dr.Web がAndroid搭載モバイル端末を通じた窃盗の脅威から守ります。

保護コンポーネント

アンチウイルス
トロイの木馬などのマルウェアから保護します

アンチシフト
モバイルデバイスを紛失、又は盗難された場合に、アンチシフトによって位置を検索できるほか、必要な場合には、電話上の個人情報をリモートで削除できます。

アンチスパム
望ましくない電話やSMSから守ります

Cloud Checker URLフィルター
ご利用のDr.Web for Androidはウイルスデータベースがどんな更新状態 であっても、Cloud Checkerは望ましくないインターネットリソースからユーザーを守ります。

ファイアウォール
アプリケーションのネットワークへのアクセスを制御します

セキュリティトラブル解析ヘルパー
セキュリティトラブルを検出するための検査を行い、問題が見つかった場合に解決策を提案します。

役に立つリンク
学習プロジェクト「モバイルデバイスを通じた窃盗」