Dr.WEB

2017年7月のモバイルマルウェア

Doctor Webは、悪意のあるソフトウェアやスパムからの効果的な保護を提供するDr.Web情報セキュリティソリューションの開発・販売を行っています。

Doctor Webのカスタマーには、世界中のホームユーザー、行政機関、中小企業、大企業が含まれています。

Dr.Webアンチウイルス製品は、国際的な情報セキュリティ基準への準拠と、優れたマルウェア検出によって1992年からその名を知られています。Dr.Webソリューションが受けた数々の賞とロシア連邦による認定、そして世界中に広がるユーザーが、製品に対して寄せられる厚い信頼の何よりの証です。

2017年7月のモバイルマルウェア
8/4/2017

Doctor Web本社
2-12A, 3rd str. Yamskogo polya
Moscow, Russia
125040

Webサイト：www.drweb.com
電話番号：+7 (495) 789-45-87

各国のオフィス情報については公式サイトをご確認ください。

目次

2017年7月のモバイルマルウェア

2017年7月31日

7月、Androidスマートフォンの複数のモデルにトロイの木馬がプリインストールされていることが、Doctor Webのセキュリティリサーチャーによって発見されました。サイバー犯罪者によってシステムライブラリ内に埋め込まれたこのトロイの木馬は、アプリケーションプロセス内に侵入し、追加のモジュールを密かにダウンロード・起動することができます。また、ダウンローダ型トロイの木馬の組み込まれたゲームがGoogle Play上で発見されたほか、感染したデバイスのコントロールを掌握して個人情報を盗む危険なバンキング型トロイの木馬についてアナリストによる調査が行われました。

7月の主な傾向

- Android デバイスの複数のモデルでファームウェアに組み込まれたトロイの木馬を検出。このトロイの木馬はアプリケーションプロセス内に侵入し、追加のモジュールを密かにダウンロード・起動します。
- Google Play上でダウンローダ型トロイの木馬を発見
- 危険なバンキング型トロイの木馬を発見

7月のモバイル脅威

7月、Doctor Webのセキュリティリサーチャーによって、Android モバイルデバイスのシステムライブラリ内に埋め込まれたAndroid.Triada.231が発見されました。この悪意のあるプログラムはアプリケーションのプロセスに侵入し、追加のモジュールを密かにダウンロード・起動することができます。Android.Triada.231はAndroidデバイスの複数のモデルで同時に検出されています。

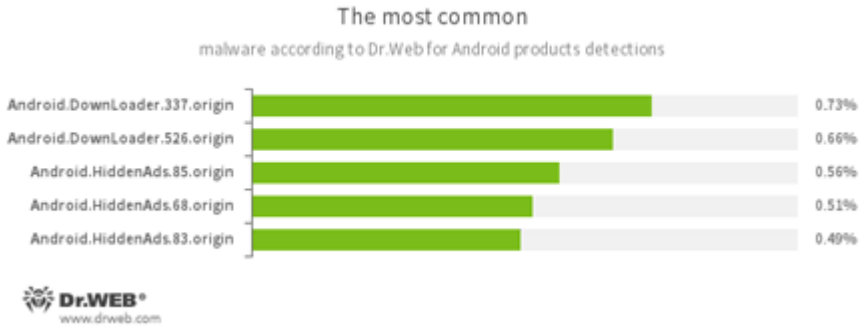
Android.Triada.231の特徴：

- ソースコードレベルでシステムライブラリ内に侵入する
- 実行可能なすべてのアプリケーションのプロセスに侵入し、悪意のあるモジュールを埋め込む
- トロイの木馬をデバイスから削除するには、オリジナルのシステムイメージをインストールする必要がある

この脅威に関する詳細についてはこちらの記事をご覧ください。

統計

Dr.Web for Androidによる統計

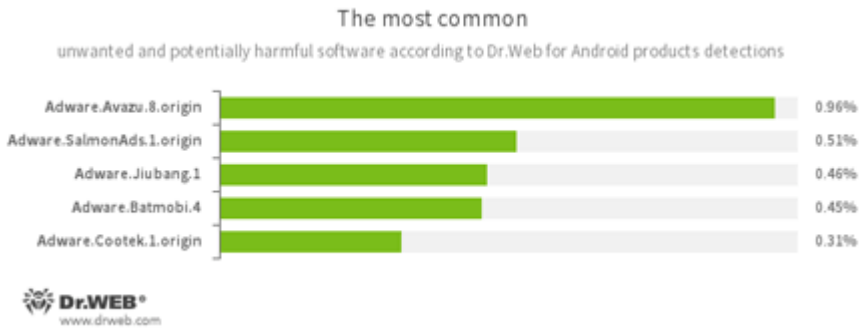


- Android.DownLoader**.337.origin**
- Android.DownLoader**.526.origin**

別のアプリケーションをダウンロードするよう設計されたトロイの木馬です。

- Android.HiddenAds**.85.origin**
- Android.HiddenAds**.68.origin**
- Android.HiddenAds**.83.origin**

モバイルデバイス上に望まない広告を表示させるよう設計されたトロイの木馬です。ポピュラーなアプリを装って別の悪意のあるプログラムによって拡散され、システムディレクトリ内に密かにインストールされる場合もあります。



- **Adware.Avazu.8.origin**
- **Adware.SalmonAds.1.origin**
- **Adware.Jiubang.1**
- **Adware.Batmobi.4**
- Adware.Cootek.1.origin

Androidアプリケーション内に組み込まれ、モバイルデバイス上に迷惑な広告を表示させる不審なプログラムモジュールです。

GOOGLE PLAY上のトロイの木馬

7月、人気のゲームBlazBlueに組み込まれたAndroid.DownLoader.558.originがDoctor Webのスペシャリストによって発見されました。この悪意のあるプログラムはソフトウェアのアップデートを最適化するために設計されたシステムモジュール内に含まれていました。

このトロイの木馬の危険な点は、未検査のアプリケーションコンポーネントをダウンロード・起動してしまう可能性があるというところにあります。この脅威に関する詳細についてはこちらの記事をご覧ください。

バンキング型トロイの木馬

7月には、危険なバンキング型トロイの木馬Android.BankBot.211.originが検出されました。このトロイの木馬はAndroid のAccessibility Serviceへのアクセス権を取得しようと試み、感染させたデバイスをコントロールし、パスワードを含むあらゆるデータをキーボード入力から盗むことができます。また、起動されたバンキングプログラムや決済サービスソフトウェア、その他のアプリケーションの前面に機密データを入力させる偽の入力フォームを表示させます。この脅威に関する詳細についてはこちらの記事をご覧ください。

サイバー犯罪者は、依然としてAndroidモバイルデバイスのユーザーに対する攻撃の手を緩めていません。トロイの木馬の機能を継続的に向上させ、あらゆる方法で拡散しようと画策しています。Doctor Webでは、お使いのスマートフォンやタブレットを悪意のあるアプリケーションから保護するために、Dr.Web for Androidをインストールすることを推奨しています。