

セキュリティニュース Google Playプロテクトでは検出されない Google Playでアプリを配布し、マルウェアをタイマーで作動させる攻撃が発生

悪意あるアプリをGoogle Playで配布する攻撃は後を絶ちません。2017年秋には、Google Playの自動検査をかいくぐるため、「不正コードを含まないアプリがマルウェアをダウンロードし、そのマルウェアがタイマーに従って悪意ある挙動をする」攻撃手法が見つかりました。セキュリティ企業ESETは同業のAvastおよびSfyLabsと共同でこの手口の攻撃を調査し、2017年11月21日（現地時間）、調査結果の概要を自社の公式ブログで報告しています。以下、ブログの記事から抜粋したものです。



2017年10月と11月に、Google Playストアで配布された「ドロッパー」による新たな攻撃が見つかった。ドロッパーとはトロイの木馬の一種であり、内部に忍ばせている不正コードが、インターネットから不正コードを「投下」（ドロップ）するというもの。10月と11月に見つかった攻撃は、いずれもバンキングマルウェアを投下しようとするもので、10月に見つかった攻撃では、「Tornado FlashLight」などのドロッパーが使われていた。Tornado FlashLightがドロッパーとして機能するには、ユーザーがAndroidのセキュリティ設定で、「提供元不明のアプリ」（提供元がPlayストアではないアプリ）のインストールを許可している必要がある。許可していなければ、Tornado FlashLightはバンキングマルウェアをインストールすることができず、脅威はない。提供元不明のアプリのインストールを許可している場合、ユーザーはマルウェア「BankBot」のインストールを促される。このアプリは、現在Google Playから削除されている。しかし、興味深いことにTornado FlashLightとBankBotは「Google Playプロテクト」では検出されないため、デバイスで適切なセキュリティソフトウェアが実行されていなければ、Google Play以外の場所からインストールできてしまう。そして、すんなりマルウェアを実行されてしまう恐れがあるという。

攻撃を防ぐには、アプリを常にGoogle Playストアからインストールすること。そして、自分が何を行っているかを明確に理解している場合以外は、「提供元がPlayストアではないアプリのインストール」を無効にすることだ。だが、Google Playから、正規アプリを装ったドロッパーやマルウェアが配布されることもある。そこで、Googleがまだブロックしていない既知のマルウェアをキャッチするセキュリティソリューションを使うことをお勧めする。また、以下の点に注意すれば、リスクの軽減につながる。

- アプリのインストール前に、アプリのユーザーが多く、レビューが好評かどうか確認する
- アプリのインストール後にアプリから、デバイス管理者権限や、アクセシビリティサービスの許可を要求された場合、そのアプリはマルウェアである可能性がある。
- アプリを初めて実行した後に、アプリ一覧からそのアプリのアイコンが消えた場合、感染している危険が高い。データをバックアップし、工場出荷状態にリセットするのがよいだろう

Google Playストア利用者は、セキュリティの設定がどうなっているか一度確認してみた方が良さそうですね。

リフレッシュルームのご紹介

先日、当社会議室を打ち合わせや休憩に使うリフレッシュルームにリニューアルしましたのでご紹介したいと思います。グリーンベースの壁色に木の素材を基調にした落ち着いた空間にハイカウンターやローテーブル、畳コーナーなど各コーナーごとに特徴を持たせて配置し、くつろぎながらもコミュニケーションが生まれるようなカフェスタイルのスペースとしました。マッサージチェアでリフレッシュして、日々のお客さま対応を頑張っています。



当社ではこのように従業員の満足度と生産性が向上する、オフィスプランニングのご提案が可能です。詳しくはお問い合わせください。

■ オフィスプランニング詳細
<http://www.kojoh.co.jp/office/>

「西野達in別府」に行ってきました！！

先日、芸術祭「in BEPPU」に行ってきました。イベント二年目となる今年は、別府駅を中心として公共の空間をアートへと変容させるプロジェクトが行われていました。国内外で話題を巻き起こしてきたアーティスト西野達の手掛けた作品が展示されています。



←別府駅東口の
油屋熊八像油屋ホテル



←この真っ白な家は発泡スチロールで出来ています。
室内も覗くことが出来て感動しました！



←流川通りにはコンビニの横にこんなアートもありました。
電柱にトラックが突き刺さっています（笑）



時間の関係ですべては回り切れなかったですが、別府市の風情を活かしたとても素晴らしいイベントでした♪今回のイベントは今年の12月24日まで行われています。残り一か月を切っていますが、是非皆さんも足を運ばれてみてはいかがでしょうか。詳しくは今回のイベントを企画運営されているNPO法人BEPPU PROJECT様のHPに記載がありますのでご覧ください。
<http://past.beppuproject.com/newslst/> 【笠置】

iPhone、iPadで再起動が繰り返す不具合発生

12月2日に、私のiPhoneが約30秒～1分で再起動されてしまうという状況に陥りました。当日、更新されたアプリが影響しているのではないかと思い、まず不要なアプリを削除してしまいましたが解決には至らない状態でした。その後、IT関係のトップニュースで問題が公開されていました。

-以下記事を抜粋

iPhoneやiPadが再起動を繰り返す不具合が、12月2日未明から多数報告されている。特定のアプリの通知を切ったり、端末の設定から日付を12月1日以前に変更すると解消するとの報告もある。iOS 11.1以降のバグが原因のようだ。不具合は、iPhoneやiPadが数十秒ほどで再起動を繰り返すというもの。iOS 11.1以降の端末で、12月2日午前0時以降に発生しているようだ。iOSのデフォルトの時計アプリで、下のメニュー以外が真っ黒になって表示されない不具合も起きており、「iOS 11の時計機能に関連するバグでは」とみられていた。問題の影響を受けた家計簿アプリ「Zaim」運営元のZaimは2日11時ごろ、問題を特定したことをTwitterで告知。「『繰り返し設定のあるローカル通知』を組み込んでいるアプリをiOS 11.1以降の端末にインストールしていると、同現象が発生するようだ」と知らせた。Appleにはバグレポートを提出したという。問題を回避する「Zaim」新バージョンをAppleの審査に提出済み。「特急申請が認められれば1～2日後にはApp Storeに反映される予定」という。また同社は開発者向けに、現象を再現できるアプリをGitHubで公開した。

【参考】：<http://www.itmedia.co.jp/news/articles/1712/02/news018.html>

この家計簿アプリ「Zaim」を利用していたため、私のiPhoneは影響を受けてしまったようです。当日の夜には、iOS11.2が公開されておりアップデートしたことで問題が解消されました。