Monthly Research

不正な開発環境によるマルウェアの拡散

株式会社ＦＦＲＩ
http://www.ffri.jp

Ver 1.00.01

はじめに

- 2015年中頃から末にかけて、モバイルアプリ向けに、「不正な開発環境」「バックドア付きSDK」等によるマルウェアの拡散が観測された。

- このような攻撃では、アプリ開発者が「不正な開発環境」や「バックドア付きSDK」を用いて作成したアプリに、知らぬ間に不正なコードが注入され、大規模な拡散に繋がる。

- iOS へ向けての攻撃では、App Store の審査を通過し、正規アプリに紛れて一般ユーザーがインストール可能な状態となっていた。

- 本レポートではiOSの事例を素に、関連事例と、その対策方法について紹介する。

アジェンダ

- XcodeGhost の 概要
- 分析から明らかになった詳細情報
- Android にも類似事例
- 新たに考えられる悪用例
- 対策方法
- まとめ

XcodeGhost の 概要

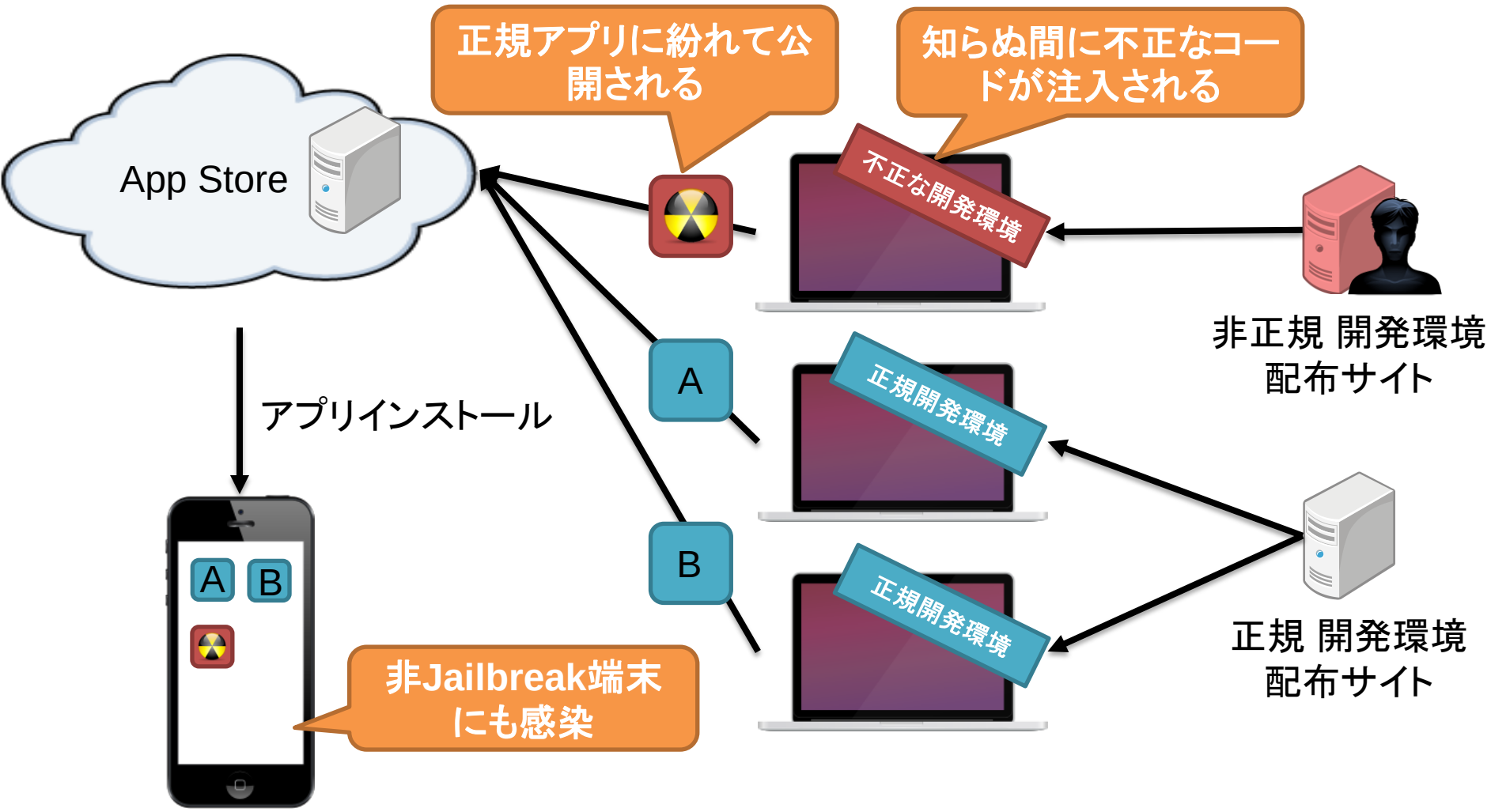
- 中国の iOS アプリ開発者が実験的に、自らが作成する全てのアプリに共通の機能を実装できるように改変された、Xcode を作成した。

- 個人利用を前提としていたが偶然 baidu cloud 上に公開設定でアップロードされてしまい、中国国内と公式配布サイトの通信速度が低速であることも手伝って、これが拡散されるに至った。

- このように中国のiOSアプリ開発者を中心に広がった不正な開発環境で作成されたアプリには情報窃取を行う処理や、広告のポップアップ機能、クリップボードの窃取など、開発者の意図しない不正コードが注入され、更には App Store の審査を通過した。

- この一連の流れで作成、配布されたアプリと不正な開発環境を XcodeGhost と呼んでいる。

XcodeGhost の 概要



XcodeGhost の 詳細

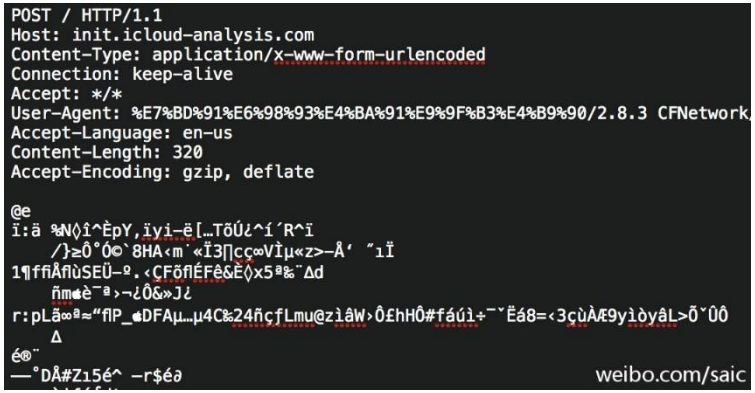
- XcodeGhost の作者は「あくまで実験的なコードであり、機微な情報の窃取等は行っていない」と Weibo（微博）にて謝罪文を掲載した。

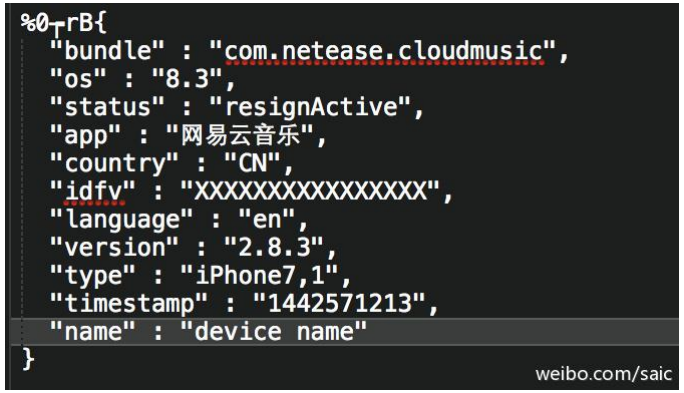
- 更に身の潔白を示すため、サーバーの停止と蓄積データの削除を行い、GitHub 上にソースコードを公開した。
  - これについて、様々な研究機関により詳細な分析が行われた。

- **不正動作**
  - 基本情報の窃取、広告のポップアップ、新たなマルウェアのインストール、クリップボード情報の窃取等、が疑われる。
  - 次ページから詳細な解説を行う。

XcodeGhost の 詳細

- **基本情報の窃取**
  - アプリ名、アプリバージョン番号、システムバージョン、言語、国、デベロッパ記号、アプリのインストール日時、システム名称、デバイスの種類を外部サーバーに送信される可能性があるが、特出して機微な情報は含まれていない。
  - 加えて、 感染した端末が iOS9 以上だった場合には、情報の送信先が非 SSL であり、非 SSL 通信を個別に許可する ATS（App Transport Security）が考慮されていないため、情報の送信は行われない。

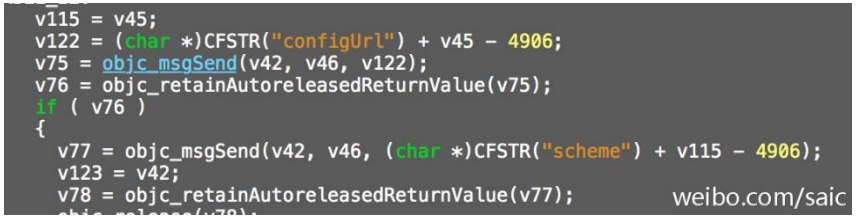




http://www.weibo.com/p/1001603888503866975286

XcodeGhost の 詳細

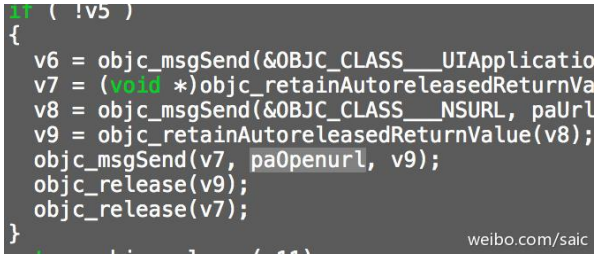
- **広告のポップアップ**
  - 任意のタイミングで任意の内容のポップアップを表示することが可能であり、支払情報、Apple IDなどの窃取や、後述する「新たなマルウェアのインストール」に繋がる誘導等が行われる可能性がある。
  - こちらに関しても感染した端末がiOS9以上であった場合には情報の送信は行われない。

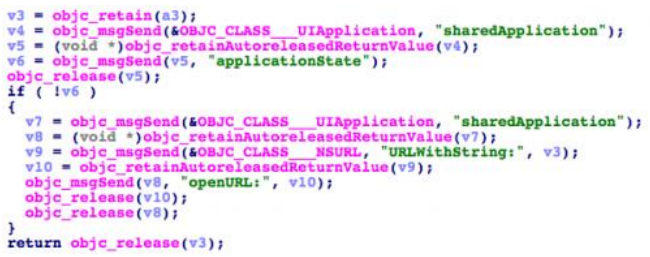


http://www.weibo.com/p/1001603888503866975286

XcodeGhost の 詳細

- **新たなマルウェアのインストール**
  - 前述の「広告のポップアップ」やスキームを用いた任意の URL のオープン機能を用いて、App Store 以外から新たなマルウェアをインストールする可能性がある。
  - XcodeGhost が App Store の審査を通過した理由として、標準 API で取得可能な範囲の情報をサーバーへ送信したり、任意の URL を開いたりと、単体ではそれほど大きな脅威ではない事が原因として考えられる。
  - しかし、ここで新たにインストールされるのは App Store の審査を通過していない iDEP(iOS Developer Enterprise Program)署名のマルウェアであり、これらが行う動作について、被害範囲を特定することは難しい。





http://www.weibo.com/p/1001603888503866975286

http://researchcenter.paloaltonetworks.com/2015/09/update-xcodeghost-attacker-can-phish-passwords-and-open-urls-though-infected-apps/

XcodeGhost の 詳細

- **クリップボード情報の窃取**
  - XcodeGhost はアプリの動作時にクリップボードの内容を保存したり、サーバーへ送信する可能性があるが、これは当該アプリ内でのクリップボード操作に限ったものである可能性が高い。（バックグラウンド動作を行わないため）
  - しかし、前述の「新たにインストールされるマルウェア」では実際にバックグラウンドで動作し、クリップボードの全内容を窃取するものがあるとの報告も存在する。

Android にも類似事例

- **Moplus**
  - 中国大手検索エンジン baidu の SDK である「Moplus」にバックドアが含まれており、これを利用していた 1万4112個（バージョンの差異を含む）のAndroid 向けアプリが影響を受けた。
  - 影響を受けたアプリの内、4014 個が baidu の公式アプリとして、「百度手机助手」（com.baidu.appsearch）経由でダウンロードされており、総ダウンロード数は数十億回以上と、大規模な拡散となった。

http://blog.trendmicro.co.jp/archives/12540

新たに考えられる悪用例

- **iOS の Embedded Framework への応用**
  - Embedded Framework とは iOS8 から正式にサポートされた、動的に呼び出し可能な外部フレームワークである。
  - 既に一部では、自分のアプリに機能付加をする要領で第三者が公開した Embedded Framework を利用しているアプリが存在する。
  - Mopuls と同等の攻撃が行われた場合には、iOS も例外ではないと言える。

- **開発環境のモジュールへの応用**
  - コーディングの効率化等を目的に導入した外部モジュールに不正なコードを注入することで、コーディング中のソースコードの流出や、不正コードの埋め込みが考えられる。

対策方法（開発者）

- **信頼されない配布元の「SDK」「開発環境」「開発環境のモジュール」等は使用しない**
  - 使用する必要がある際には、「外部通信」「パーミッション要求」「ユーザーデータへのアクセス」等、想定されない付加機能が存在しない事を入念に調査したうえでの導入が重要である。

- **リリース前テスト時に想定した以外の通信先への「外部通信」が存在するか否かを確認する**
  - モバイル系マルウェアの多くは情報を外部に持ち出すものが多く確認されているため、ネットワーク監視を行い、情報漏えいを防ぐ事が重要である。

対策方法（利用者）

- **公式マーケット以外からのアプリインストールは控える**
  - 公式マーケットでの不正な開発環境によるマルウェアの感染については XcodeGhost や Moplus 等で広く知られることとなったが、非公式マーケットではより意図的なマルウェア感染が考えられる。

- **自社、自分が管理する署名以外の野良アプリはインストールを控える**
  - iOS、Android 共に正規ルートでのインストールの他に、野良アプリという形でアプリをインストールする方法が存在するが、既存の殆どのマルウェアの感染源がこれにあたる。

まとめ

- iOS、Android 共にマルウェアの大規模な拡散が見られ、信頼される提供元を経由してユーザーの端末へインストールされている。

- 近年のモバイル向けマルウェアの大規模な拡散では、開発環境やSDKと言った、アプリ開発の根本部分を狙った攻撃が行われており、結果的に悪意のない開発者が、マルウェアを拡散してしまうことになる。

- iOS については App Store の審査を通過するために、過度な不正動作は行わないものの、新たに iDEP 署名のマルウェアをドロップすることで、これを実現する手法が採られている。

- 利用者と、開発者にも高いセキュリティ意識が求められるため、マルウェアの侵入経路や、動作などを知る事が重要である。

参考情報

- XcodeGhost 实际用途猜测分析 - 文章
  http://www.weibo.com/p/1001603888503866975286
- #XcodeGhost#关于所谓"XcodeGhost"的澄清。... 来自XcodeGhost-Author - 微博
  http://www.weibo.com/5704632164/CBc4S9H9p?from=page_1005055704632164_profile&wvr=6&mod=weibotime&type=comment#_rnd1452219037152
- 不具合を抱えるMoplus SDK、Baidu 以外のアプリにも影響 | トレンドマイクロ セキュリティブログ
  http://blog.trendmicro.co.jp/archives/12566
- 脆弱性を抱えるソフトウェア開発キット「Moplus」、実はバックドア機能の実装が判明 | トレンドマイクロ セキュリティブログ
  http://blog.trendmicro.co.jp/archives/12540

Contact Information

E-Mail ： research—feedback@ffri.jp
Twitter： @FFRI_Research