Monthly Research 2016.12

Black Hat Europe 2016
サーベイレポート

F F R I , Inc.
http://www.ffri.jp

E-Mail: research-feedback[at]ffri.jp
Twitter: @FFRI_Research

目次

- Black Hat Europe 概要
- 紹介する研究発表一覧
  - BREAKING BHAD: ABUSING BELKIN HOME AUTOMATION DEVICES
  - (PEN)TESTING VEHICLES WITH CANTOOLZ
  - MOBILE ESPIONAGE IN THE WILD: PEGASUS AND NATION-STATE LEVEL ATTACKS
- まとめ
- 参考情報

Black Hat Europe 概要

- Black Hat とは
  - 世界最大級の規模を誇るセキュリティカンファレンス
  - 世界中から投稿されたセキュリティに関する最新の研究が発表される
    - 内容は新しい脅威の実証から防御技術など高度で多岐にわたる
    - 一部を除き、プレゼン資料や論文が Web で公開
  - 毎年世界各所で開催されている
    - ラスベガスで開催されている Black Hat USA
    - シンガポールで開催されている Black Hat Asia

- 今回は11月にロンドンで開催された Black Hat Europe の発表を紹介
  - IoT、自動車セキュリティ、標的型攻撃に対する最新の発表

紹介する研究発表一覧

- IoT セキュリティ
  - BREAKING BHAD: ABUSING BELKIN HOME AUTOMATION DEVICES
    - Joe Tanen, Scott Tenaglia
- 自動車セキュリティ
  - (PEN)TESTING VEHICLES WITH CANTOOLZ
    - Alexey Sintsov
- 標的型攻撃
  - MOBILE ESPIONAGE IN THE WILD: PEGASUS AND NATION-STATE LEVEL ATTACKS
    - Andrew Blaich, Max Bazaliy, Seth Hardy

BREAKING BHAD: ABUSING BELKIN HOME AUTOMATION DEVICES

- WeMo に対し SQL インジェクションを仕掛け、任意コードを実行する脅威実証
- WeMo とは
  - 遠隔地から AC コンセントを使用している機器の電源を操作できる機器
  - Wi-Fi を経由してインターネットに繋ぎ、モバイルアプリなどから制御する
  - 過去に今回の事例に似た SQL インジェクションなどの脆弱性が発見されている
- WeMo のファームウェアである OpenWRT ではデフォルトのシェルとして ash を利用
- SQL 文の中で改行しシェルスクリプトを仕込み、シェルに SQL 文を渡すと仕込んだシェルスクリプトが実行される

```
sqlite> insert into echo values ("
   ...> ls /
   ...> ");
sqlite> .quit
```

SQL文

シェル

実行されると

```
foo: line 3: without: not found
foo: line 4:?: not found
bin dev opt run sys etc proc sbin tmp home l
```

BREAKING BHAD: ABUSING BELKIN HOME AUTOMATION DEVICES

- telnet でルートログイン
  - 先ほど紹介した方法を基に下記のシェルコードを含む SQL 文を作成し送信
    - telnet から常にルートシェルを使用可能にするシェルコード
    - 上記シェルコードを /lib/network/ に保存するシェルコード
      - /lib/network 下のスクリプトはネットワークが再起動されると実行される
  - WeMo 既存のコマンドである StopPair コマンドでネットワークを再起動させる
  - 書き込んだシェルコードが実行され telnet からルートシェルが使用可能になる
- WeMo への物理的な攻撃によるローカルルートの奪取
  - WeMo を解体、基板とブレッドボードと接続し、起動時に“4”キーを連打することで、ブートローダ U-Boot が利用可能になる
  - SquashFS から JFFS2 のルートファイルシステムへの書き込みは mini_fo で制限されている
  - 読み込みはできるため /etc/passwd ファイルを取得、ルートのパスワードを削除
  - passwd ファイルを書き換えた JFFS2 を作成、U-Boot の loadb でマウント

(PEN)TESTING VEHICLES WITH CANTOOLZ

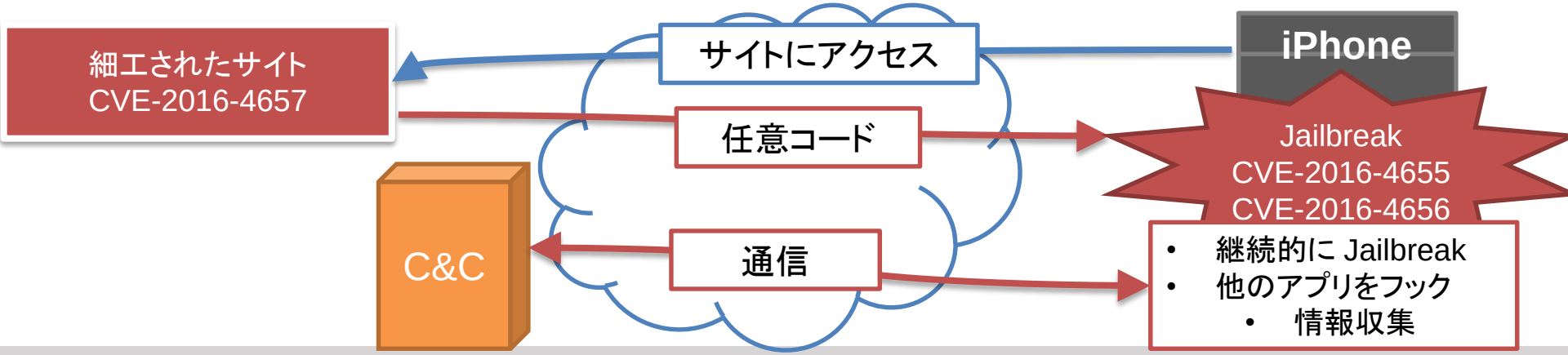
- 背景
  - 車両には様々なアタックサーフェスが存在
    - ヘッドユニットの Wi-Fi を経由したリモート攻撃や OBD2 や CAN bus に対するバックドア ECU からの物理的な攻撃
  - 車両向けの複合的な検証ツールへのニーズが高まっていた
- CANToolz
  - オープンソースのフレームワーク
    - https://github.com/eik00d/CANToolz
  - CAN ネットワークへブラックボックスな状態で解析を行う際に利用
    - ただし、USBTin または CANBus Triple が必要
  - 様々な機能のモジュールが開発されている
    - MITM、ファジング、UDS(Unified Diagnostic Services) スキャン、CAN ファイアーウォール

(PEN)TESTING VEHICLES WITH CANTOOLZ

- CAN over TCP による接続
  - CAN over TCP により遠隔からの操作が可能
- 仮想車両
  - ECU を CANToolz モジュールとして作成して、これらを接続することで実際の車両をエミュレートしている
  - Web UI から各種命令によるシュミレーションが可能
- 実車へのリバースエンジニアリングとブラックボックス分析
  - CAN メッセージの解析
  - UDS
    - MITM によるセッションのハイジャック
    - 様々なメッセージによるファジングの実施
  - 車両のアンロックコマンドの特定が可能か否かなど

MOBILE ESPIONAGE IN THE WILD: PEGASUS AND NATION-STATE LEVEL ATTACKS

- 今年の夏頃からアラブの人権活動家 Ahmed Mansoor 氏などに向けた攻撃が発生、6人が逮捕された
- その際に利用されたスパイウェアが iOS 向け Pegasus (ペガサス)である
  - 発表者は今回このマルウェアのソースコードを分析、搭載している機能の詳細についてまとめるとのこと
- Pegasus とは
  - 永続的な Jailbreak を行い、管理者権限による任意のコードの実行を可能とする iOS 向けスパイウェア
  - iOS 向けペガサスでは「Trident」と呼ばれる 3つの脆弱性が利用されている



MOBILE ESPIONAGE IN THE WILD: PEGASUS AND NATION-STATE LEVEL ATTACKS

- Pegasus の機能
  - 情報収集機能
    - マイクやカメラの使用状況の確認とビデオなどの撮影
    - GPS や通信情報、各種サイトへのパスワードや SIM 情報などの収集
  - アプリケーションのフック
    - Jailbreak 後、フック用のアプリをインストール
  - 耐解析技術
    - 検知と解析を行わせないための機能
      - インストールの際に利用した Web サイトへのリンクは一度きりしか使わない
      - コードの難読化やダウンロード毎に異なる鍵での暗号化
      - システムサービスとして偽造し、自身の存在を隠す
      - Safari の閲覧履歴やキャッシュを削除
    - 削除されることを避けるための機能も存在
      - iOS のアップデートをブロック
      - 自身を削除

まとめ

- IoT セキュリティ
  - 電源を遠隔操作する機器がセキュリティ製品や電熱器具であった場合、多大な被害を及ぼす恐れ
  - 攻撃されたIoT機器がボットネットの一部として加害者に加担する恐れもある
- 自動車セキュリティ
  - 統合ツールの登場により、脆弱性の発見と対策が加速することが期待される
- 標的型攻撃
  - 比較的安全と思われていた iOS 端末への標的型攻撃が明らかになった
  - モバイル端末への標的型攻撃に注意が必要と考えられる
- 全体を通して
  - 今回紹介した発表自体はどれも独立しているが、 IoT 化が進むことで、セキュリティ脅威が関連して発生する恐れがある
  - 個別に考えていたセキュリティをより広い視点での再検討が必要

参考情報

- Black Hat Europe2016
  - https://www.blackhat.com/eu-16/
- (PEN)TESTING VEHICLES WITH
  - https://www.blackhat.com/docs/eu-16/materials/eu-16-Sintsov-Pen-Testing-Vehicles-With-Cantoolz.pdf
- Mobile Espionage in the Wild Pegasus and Nation-State Level Attacks
  - https://www.blackhat.com/docs/eu-16/materials/eu-16-Bazaliy-Mobile-Espionage-in-the-Wild-Pegasus-and-Nation-State-Level-Attacks.pdf
- Breaking BHAD: Abusing Belkin Home Automation Devices
  - https://www.blackhat.com/docs/eu-16/materials/eu-16-Tenaglia-Breaking-Bhad-Abusing-Belkin-Home-Automation-Devices.pdf
- Read more: iOSにおけるトライデント脆弱性について、セキュリティ責任者が知っておくべき3つのポイント
  - https://blog.lookout.com/jp/2016/08/29/cisotridentpegasus/