Monthly Research

Black Hat Asia 2016 サーベイレポート

株式会社ＦＦＲＩ
http://www.ffri.jp

Ver 2.00.01

Black Hat Asia 概要

- 著名なセキュリティカンファレンスである Black Hat のアジア版
  - 発表者は世界中から選出されており出身地に偏りはない

- 毎年 3月下旬~4月上旬に、シンガポールで開催
  - 今年は 3月 29日から 4月 1日に開催された
  - 最新のセキュリティ研究や注目を集めているテーマについての研究発表やトレーニングが行われる
    - 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

- 本レポートでは Black Hat Asia 2016 の研究発表について、FFRI のリサーチャーが公開資料を調査し、注目した研究を紹介

FFRI リサーチャーが注目した研究発表

- モバイルセキュリティ
  - Android Commercial Spyware Disease and Medication
    - Mustafa Saad
  - Su-a-Cyder: Home-Brewing iOS Malware Like a B0$$!
    - Chilik Tamir
- IoTセキュリティ
  - Lets See Whats Out There Mapping The Wireless IOT
    - Tobias Zillner
  - Hacking a Professional Drone
    - Nils Rodday
- Windowsセキュリティ
  - DSCompromised:A Windows DSC Attack Framework
    - Ryan Kazanciyan & Matt Hastings

Android Commercial Spyware Disease and Medication

- 商用スパイウェアについて
  - 企業や保護者が、社員や子どもの端末利用内容を監視することを目的としたアプリ
  - 価格は年間数万円ほどと手の届く価格であり、多くが監視対象を統制する為の管理ページなどを有している
- Droid Smart Fuzzer
  - 商用スパイウェアの検知ソリューション
  - インストール済みの全アプリの要求している権限を取得
  - スパイウェアが特に要求することの多い下記権限を要求しているアプリをリストアップ
    - RECEIVE_SMS
    - PROCESS_OUTGOING_CALLS
    - READ_PHONE_STATE
    - INTERNET
  - インターネットを介し対象デバイスに対して各権限に対応したテストを実行
  - 疑わしいアプリのネットワーク使用量の変化からスパイウェアであるかを判別し、レポートに出力

Android Commercial Spyware Disease and Medication

- 有料スパイウェアのシェアトップ 15と 4つの無料スパイウェアの全ての検知に成功

- **FFRI リサーチャーの考察**
  - スパイウェアをヒューリスティック技術で検知していることは興味深い
  - 商用スパイウェアは 2013年 5月に公開されたレポートで、日本を含む多くの国家での使用が報告されており、今後民間レベルでの使用者も増える可能性があるのでとても有益な研究といえる
  - 全てのスパイウェアを検出できているものの、検知アルゴリズムの単純さから誤検知率も高くなっている可能性がある

Su-a-Cyder: Home-Brewing iOS Malware Like a B0$$!

- iOS マルウェアの歴史、影響、最悪のシナリオを説明
- Apple ID の作成しやすさを悪用した、リパッケージしたアプリで Jailbreak していない端末情報の収集が可能であることを実証
  - 企業に対する攻撃では MDM などを回避し、商用コミュニケーションアプリの偽装に成功
  - 個人に対する攻撃ではアイコン等が表示されないアプリの作成や、Skype をリパッケージし、偽装することに成功

- **FFRI リサーチャーの考察**
  - iOS マルウェアは年々巧妙化しており出現件数も増加することが予想されるため、Jailbreak 無しでインストールされるマルウェアの作成という本研究はとても注視すべきである

Lets See Whats Out There Mapping The Wireless IOT

- 現在急速に普及が進んでいる IoT デバイスの無線について
  - サムスンは 2019年までに自社 IoT デバイスの全面無線化を発表
  - J・クラッパー米国家情報長官は深刻な脅威をもたらす可能性について言及
  - 安全性へのニーズが高まっている
- 一方で企業ごとの独自規格やツールの未成熟により無線信号の検出や安全性の評価が難しい
- 様々なツールを統合した無線通信用セキュリティテストツールを開発・実証した
- 現在無線 IoT デバイスのリスクについてランキング形式でまとめた研究結果なども提示している
- 無線ネットワークは大きな攻撃対象となるものであり、それに対する攻撃手段も数多く存在すると強調

- **FFRI リサーチャーの考察**
  - IoT は普及速度が早いため、セキュリティや通信規格が統一されていない印象が強い
  - 検査ツールが分散していることから、統合された今回のツールは利便性が高い

Hacking a Professional Drone

- ドローンの通信を傍受できることを実証
  - 今回はスマートフォン向けの操作アプリが配信されているものを使用
  - ドローン-リモコン間、リモコン-操作アプリ間の通信を傍受し、中間者攻撃を実証した
- ドローン-リモコン間の通信の傍受
  - XBee を利用した接続であったが、暗号化機能の実装が不十分であった
- リモコン-操作アプリ間の通信の傍受
  - Wi-Fi通信による接続だったが、通信の暗号化にWEPを使用していたため簡易に解読ができた
- 操作アプリのAPKを逆コンパイルし、信号を解読、送信内容を解析、実際に攻撃を行う
- 多くのドローンはネットワークアクセス機能を持たない為、今後メーカー側で改善されたとしても、すでに発売されているドローンには修正を反映することが出来ない
- 発表者は、この脆弱性について今回実証したドローン以外にも存在していると考えている
- XBee に組み込まれている暗号化機能の実装やアプリケーション層での暗号化などが提案されている

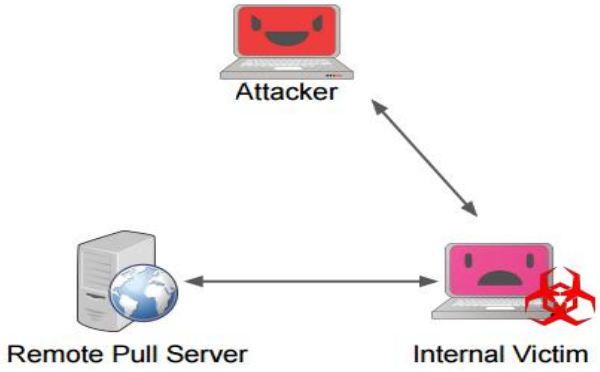
Hacking a Professional Drone

- **FFRI リサーチャーの考察**
  - この発表の 1ヶ月前に開催された、RSA Conference 2016 でも既に発表されており、メディアからも多くの注目を集めていた
  - リコールを望む声もあるものの、今後も対象製品が市場に出回るのは止めようがない
  - 現在アメリカでは登録制度が導入されており、ドローンへの中間者攻撃による冤罪被害なども考えられる

DSCompromised:A Windows DSC Attack Framework

- PowerShell DSC (Desired State Configuration) について
  - Windows の次世代構成管理プラットフォーム
    - Windows 8.1, Windows Server 2012 R2 に標準でリソースインストール
    - WMF 4.0 へのアップグレードにより、上記以前いくつかのバージョンでも利用可能

- DSC の整合性チェック機能を利用して、永続的なマルウェア感染が可能であることを実証
  - DSC プルサーバーを C&C サーバーとして構成する DSCompromised Framework をインストール
  - DSC プルサーバー内にマルウェアを設置し、MOF ファイルを生成する
  - 何らかの方法で被害者側ネットワークの内部へ侵入
  - 被害者 PC の LCM を書き換え、用意した DSC プルサーバーへ通信を行うよう設定する
  - 被害者 PC はマルウェアを削除しても、定期的に DSC の整合性チェック機能により、自動的にマルウェアが再生成される



攻撃イメージ
出典:DSCompromised: A Windows DSC Attack Framework

DSCompromised:A Windows DSC Attack Framework

- 同様の手法で永続的に存在し続けるユーザーの作成も実証している。

- **FFRI リサーチャーの考察**
  - 今回の攻撃はまだ、実際の悪用が確認されていないものの、以下の理由により今後の攻撃の発生が考えられるため警戒が必要である。
    - DSC は Windows 8.1 や Windows Server 2012 R2 では標準でリソースが入っており利用しやすい
    - PowerShell を悪用した攻撃は増加傾向にあり、DSC により更に簡略化された

まとめ

- モバイルセキュリティ業界では今後大幅な防御技術の向上が期待される。
  - Jailbreak の有無に関係のない iOS マルウェア増加によって脅威が本格化し、セキュリティへの研究が活発になっている
  - Android マルウェア検知に関する研究の増加

- IoT やそこで使用される通信技術に対する実用的なテスト手法情報の需要が増えていると感じた
  - テスト手法や効率的なツールの使い方を模索している研究が多い
  - これまで分散していた各プロトコルについての総合的な研究の増加
  - 実用性の高いツールのリリースなど

- 最新 Windows OS やツールを狙った高度な攻撃手法が、引き続き発見される可能性があり、最新情報の収集が必要

参考情報

- Android Commercial Spyware Disease and Medication
  - https://www.blackhat.com/docs/asia-16/materials/asia-16-Saad-Android-Commercial-Spyware-Disease-And-Medication.pdf
  - For Their Eyes Only: The Commercialization of Digital Spying
    - https://citizenlab.org/2013/04/for-their-eyes-only-2/
- DSCOMPROMISED: A WINDOWS DSC ATTACK FRAMEWORK
  - https://www.blackhat.com/docs/asia-16/materials/asia-16-Kazanciyan-DSCompromised-A-Windows-DSC-Attack-Framework.pdf
- HACKING A PROFESSIONAL DRONE
  - https://www.blackhat.com/docs/asia-16/materials/asia-16-Rodday-Hacking-A-Professional-Drone.pdf
  - RSA Conference 2016
    - http://www.rsaconference.com/events/us16
- LET'S SEE WHAT'S OUT THERE - MAPPING THE WIRELESS IOT
  - https://www.blackhat.com/docs/asia-16/materials/asia-16-Zillner-Lets-See-Whats-Out-There-Mapping-The-Wireless-IOT.pdf
- Su-a-Cyder: Home-Brewing iOS Malware Like a B0$$!
  - https://www.blackhat.com/docs/asia-16/materials/asia-16-Tamir-Su-A-Cyder-Homebrewing-Malware-For-iOS-Like-A-B0SS.pdf

Contact Information

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