Monthly Research

CODE BLUE 2015 参加レポート

株式会社ＦＦＲＩ
http://www.ffri.jp

Ver 1.00.01

はじめに

- 2015年10月28日、29日の2日間、東京で情報セキュリティの国際カンファレンス「CODE BLUE 2015」が開催された。

- CODE BLUEは2013年から始まった、日本発の専門家向けカンファレンスで、3回目である今回は、当初の目標であった500人を超える600人超の来場者を迎えての開催となった。

- 本カンファレンスに FFRI からは 2名の研究者がスピーカーとして参加しており、会場の様子や興味深いと思った講演について紹介する。

アジェンダ

- CODE BLUE 2015
- FFRI のリサーチャーによる発表
- IoT に潜むセキュリティ脅威
- バグバウンティの最先端
- 急増する標的型攻撃（APT）
- 新たな試み Youth Track
- まとめ

CODE BLUE 2015

- 2 つの挑戦
  - 2 トラック制
    - 平行して 2 会場で別々の発表を行う
  - Youth Track
    - 満 24 歳以下の講演者のみで選考を行うトラック

FFRIエンジニア2名の発表（近日公開）

- **iOSマルウェアの動向と専用ガジェットによるマルウェア検知**
  - **西尾 素己**

- **Windows 10 IoT Coreに対する脅威分析と実施するべきセキュリティ対策**
  - **和栗 直英**

- 発表の詳細については後日 FFRI Web サイトにて公開予定
  - http://www.ffri.jp/research

IoT に潜むセキュリティ脅威（１）

- **(In)Security of Medical Devices**
  - ERNW 社のセキュリティ・アナリストであり医療情報学の理学学士も保有するフローリアン・グルーノ氏による医療機器を対象とした攻撃についての発表。
  - 実際に会場に持ち込まれた医療機器に対して攻撃のデモが行われ、手術中に用いる計測機器などに対する DoS 攻撃や投薬量を調整する機器に対する攻撃（こちらはビデオのみ）が紹介され、大きなインパクトを残した。
- **ワイヤレス技術をアタックで検証**
  - 富士通システム統合研究所の堀合 啓一 氏による SDR (Software Defined Radio)を用いたワイヤレス技術に対する攻撃についての発表。
  - GNURadio についての解説や、RF 信号などのリプレイ・アタック、無線キーボードへのスニッフィングなどについてデモを交えて解説。

IoT に潜むセキュリティ脅威（２）

- **Cybersecurity of SmartGrid**
  - ICS/SCADA ネットワーク・セキュリティのツールキット作者でセキュリティリサーチャーのアレクサンダー・ティモリン 氏と、SCADAStrangeLove.org チームのキャプテンで Positive Hack Days フォーラムのディレクターおよびスクリプトライターを務めるセルゲイ・ゴディチック 氏による、スマートグリッドに関する発表。
  - 太陽光発電システムからデジタル変電所までの、スマートグリッド技術の様々な要素の安全性評価や、実際の経験を解説。

バグバウンティの最先端（１）

- **Firefox の倒し方**
  - 本職の傍ら Firefox を中心とする Web ブラウザに対して多くの脆弱性を指摘し、年間 700 万円以上の報奨金を獲得されている にしむねあ こと西村 宗晃 氏による、脆弱性が生まれるパターンと、その効率的な発見方法についての発表。
  - 多くのブラウザで、仕様書に定義されている要件を満たしていないことや、そもそも必要な機能が実装されていない事があり、それらを起因とする脆弱性が多く発見されている。
  - 新しい機能が実装された際には仕様書に沿ってテストを行うだけである程度の脆弱性を発見することができる。

バグバウンティの最先端（２）

- **X-XSS-Nightmare: 1; mode=attack ～XSSフィルターを利用したXSS攻撃～**
  - Google が行うバグバウンティプログラムで、世界二位の報告数を誇り、数多くのプロダクトに脆弱性報告を行う、レジェンド的存在である、キヌガワ マサト氏による IE の XSS フィルターの動作を利用した XSS についての発表
  - 本来 XSS を防止するために、ページの一部を書き換える XSS フィルターの機能を利用して、タグ破壊などを意図的に起こし、XSS に繋げる事ができる。
  - 本人曰く「Microsoft との調整でかなり自粛したバージョンである」とのこと
  - 発表では具体的な攻撃手法については紹介がなかったものの、Microsoft 側で対応が完了次第、公開予定とのこと。

急増する標的型攻撃（APT）

- **日本の組織をターゲットにした攻撃キャンペーンの詳細**
  - JPCERT/CC の朝長 秀誠 氏と中村 祐 氏による、日本国内を対象とした標的型攻撃についての発表。
  - 最新の攻撃テクニックや使用するマルウェア、ツールについて紹介され、関連するマルウェアを解析するためのテクニックやツールについても紹介された。
  - 日本年金機構への攻撃にも使用されたマルウェア「Emdivi」の分析ツールが GitHub で公開された。
- **Ninja Correlation of APT Binaries**
  - インテル（Intel Corporation）APT レスポンスチームのサイバー・アナリストでソフトウェア開発者のブヘブナ・ソマ氏による、実際に APT で使用されたマルウェア検体のコードの類似性を評価するために適した様々な手法に関する発表。
  - 検体の類似性計量のそれぞれを基にしているバイナリのクラスタを作成し、その正確性を評価する技術などが紹介された。

急増する標的型攻撃（APT）

- **Failures of security industry in the last decade - Lessons learned from hundreds of cyber espionage breaches**
  - Team T5 Research の CEO であるスンティン・サイ(TT) 氏と、同社で上級アナリストを務めるチーエン・シェン(Ashley) 氏によるアジアを中心としたサイバー攻撃に関する発表。
  - 日本年金機構に対するサイバー攻撃などの具体的な事例の紹介や、一般的に採られているセキュリティ対策が如何に破られ、それらが攻撃者にとって無力であるかが紹介された。

新たな試み Youth Track

- **PANDEMONIUM: 動的バイナリ計測とファジーハッシュを使用した暗号アルゴリズムの自動識別**
  - 慶應義塾大学在学中で IPA 主催のセキュリティ・キャンプでは最年少で講師を務める黒米 祐馬 氏(20歳)による、ファジーハッシュを使用した暗号アルゴリズムの自動識別についての発表。
  - バンキングマルウェアとして猛威を振るった Zeus のソースコードが流出し、様々な亜種が生産されている。
  - これらのマルウェアが行う、算術・ビット演算、ループ構造などに着目して暗号化処理が含まれる箇所を抽出する方法と、LLVM を用いた解析妨害機能の回避技術が紹介された。
  - この解析妨害機能の回避の際に生じる解析の揺れに関しては、ファジーハッシュを用いて吸収するとのこと。

新たな試みYouth Track

- **Master Canary Forging: 新しいスタックカナリア回避手法の提案**
  - 灘高校在学中で数々の CTF のファイナリスト、優勝の経験がある小池 悠生 氏(16歳)による、スタックカナリアの新たな回避手法についての発表。
  - リターンアドレスがスタックカナリー領域に書き込まれたことをトリガーにプロセスを終了させることによって、バッファオーバーフローを防ぐスタックカナリアの回避方法についての紹介。
  - これまで、スタックカナリアの回避方法としては、いわゆる番兵の値の確認処理が行われる前に、攻撃処理を完了する、もしくは番兵の値を漏洩させてからオーバーフローさせるものが主流であった。
  - 新しい回避方法として、マスターカナリーを書き換えることによって回避するという手法が提案され、実際にデモが行われた。

まとめ

- 世界各国から 600 人以上が訪れた CODE BLUE 2015
  - 2 トラック制と Youth Track を新たに導入された。
  - ティーン・エイジャーが 2 名と大学生 1 名が登壇した。
- IoT セキュリティ
  - 医療機器や社会インフラに関わる研究が見られた。
  - ホワイトハッカー達はこれらに関わる脆弱性を発見し、報告している。
- バグバウンティ
  - 日本のバグハンター達は世界でアクティブに活躍している。
  - 彼らのバグハントの方法からは多くの事を学ぶことができる。
- 標的型攻撃
  - 攻撃者は標的型攻撃によって、日本の様々な組織に侵入している。
  - 今回の CODE BLUE のようなカンファレンスで情報交換を行う事は標的型攻撃に対抗する手段として有効である。

参考情報

- 講演者紹介 || CONTENTS || 世界トップクラスの専門家による情報セキュリティ国際会議「CODE BLUE（コードブルー）」
- http://codeblue.jp/2015/contents/speakers.html

Contact Information

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