帝塚山学院大学
TEZUKAYAMA GAKUIN UNIVERSITY

情報セキュリティ論(14)
IoTのセキュリティ

中野秀男
帝塚山学院大学非常勤講師
大阪市立大学名誉教授、堺市情報セキュリティアドバイザ
大阪府IT人材リーダー

1

今日の話

- IoT
  - 「コンピュータ概論」の組込み機器とセンサーネット
- IoT機器のセキュリティ対策
- 無線LANのセキュリティ
- IoTポットMiraiのアタック
- センサーを使ったセキュリティ対策
- 監視カメラのセキュリティ
- IoT機器を探し出すSHODAN

帝塚山学院大学
TEZUKAYAMA GAKUIN UNIVERSITY

2

IoT機器のセキュリティ対策

- IoT機器の再起動
  - 揮発型のマルウェアを消滅させる
- ファームウェアのアップデート
  - 脆弱性を塞ぐ
- ID/パスワードの変更
  - 初期パワワードでの侵入を防ぐ
- インターネット側からのアクセス拒否
  - 外から繋がせない
- ゲートウェア機器の内側に設置
  - 直接インターネットに繋がない
- 古い機器は買い換える
  - 自動アップデート機能のない機器は使わない

帝塚山学院大学
TEZUKAYAMA GAKUIN UNIVERSITY

3

無線LANのセキュリティ

- 無線LAN
  - 無線LANはアクセスポイントとクライアントのからなるネットワークシステム
- 無線LANのセキュリティ
  - 無線LANのアクセスポイントのセキュリティ
  - 無線LANのクライアントのセキュリティ

帝塚山学院大学 TEZUKAYAMA GAKUIN UNIVERSITY

4

無線LANのアクセスポイント

- アクセスポイントへの不正接続
  - パスワードをユーザーが設定する場合、安全性の高いパスワードを利用する
  - MACアドレスを登録した機材のみ接続を許可する
- 盗聴
  - 安全性の高いWPA2-PSKの暗号化方式を使う
    - 無線LAN普及期初期に使われていたWEPは今日では安全性に問題があるので利用しない
- SSID
  - 個人情報が漏れるような命名はしない

帝塚山学院大学 TEZUKAYAMA GAKUIN UNIVERSITY

5

無線LANのクライアント

- アクセスポイントとはWPA2-PSKで接続する
  - 電波を盗聴することで暗号化されていない通信内容がわかってしまう
  - VPNを利用して通信路すべてのデータを暗号化してしまう
- なりすましのアクセスポイントに注意する
  - 知らぬ間になりすましアクセスポイントに自動接続してしまうケースもある
    - なりすましのアクセスポイントに接続するような条件を作りクライアントの正規の接続先から乗っ取る

帝塚山学院大学 TEZUKAYAMA GAKUIN UNIVERSITY

6

無線LANで出てきた言葉の説明

- MACアドレス
  - コンピュータやネットワーク製品のネットワーク部に割り当てられる番号
  - 48ビット
- SSID
  - 無線LANのID
- VPN:Vitual Private Network
  - インターネットなどに接続している利用者の間に仮想的なトンネルを構築し、プライベートなネットワークを拡張する技術

帝塚山学院大学 TEZUKAYAMA GAKUIN UNIVERSITY

7

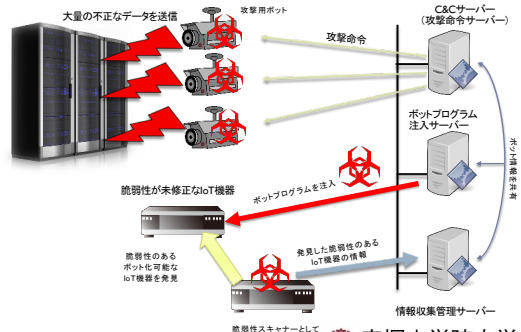
IoTボットMiraiのアタック

- 多数のIoT機器を乗っ取り攻撃ボットをコントロールしてDDoS攻撃を行う
  - コマンド&コントロール・サーバー(C&Cサーバー)は多数のIoT機器をボットとして管理できるのが特徴
  - DDoS攻撃には145,000台のIoT機器をボットとして使用
    - 攻撃トラフィックは 9,300万パケット/秒・転送量799Gbpsを記録
    - 理論上は1.5Tbpsの攻撃が可能と分析される

帝塚山学院大学 TEZUKAYAMA GAKUIN UNIVERSITY

8

Miraiボットネットの全体像



帝塚山学院大学 TEZUKAYAMA GAKUIN UNIVERSITY

9

Miraiが乗っ取る脆弱なIoT機器と高性能なC&Cサーバー

- ファイアウォールなどを介さずに直接インターネットに接続
  - 管理ポートがインターネットからも接続可能
- 管理者アカウントに対する辞書攻撃
  - デフォルトパスワードを変更しないまま使用
  - メーカーが用意しているメンテナンス用バックドア
  - “root” “admin”といったアカウント名と“password” “12345”といったパスワードの組み合わせ
- 大量のボットを管理し運用できるポテンシャルをもったC&Cサーバー
  - 機能的に複数のサーバーに分散して作られているためスケーラブル
  - 効率の良い脆弱性をもったIoT機器を見つける仕組み
  - C&Cサーバーはスケーラブルに設計されている
    - 2016年の事例では145,000台のボットを攻撃に使ったが出来たが、潜在的能力として数十万から百万を超えるボットネットを管理運用可能と考えられる

帝塚山学院大学 TEZUKAYAMA GAKUIN UNIVERSITY

10

社会に与えた影響

- 事件後にMiraiのソースコードが公開される
  - Miraiの事件はIoT機器のセキュリティに対する警告として行ったという作者からの声明
  - 後にソースコードを参考にして同様な機能をもつボットネットがいくつも開発される
- 大量のIoT機器が存在する時代においてMiraiは極めて脅威であることが認知される
  - IoT機器として使われていても機能や性能はPCやサーバーと遜色のない能力をもつ時代
  - 脆弱性を抱えたまま放置されるIoT機器の多さ
  - PCと同様にセキュリティ・アップデートが必要であるという認識の欠如
- NOTICEの取り組み
  - 総務省、NICT、ISPが連携してインターネット上のIoT機器へのアクセスし、サイバー攻撃に悪用されるおそれのある機器の調査及び該当機器の利用者への注意喚起を行う（2019年2月より）

帝塚山学院大学 TEZUKAYAMA GAKUIN UNIVERSITY

11

人感センサー

- 人感センサー
  - 照明などの電気機器を自動でオンオフ
  - 照明の消し忘れ防止
  - 節電効果
- 人感センサーとは
  - 人が発する熱などを検知
  - 多くは赤外線センサー
    - 熱(赤外線)を検知して機器を作動

帝塚山学院大学 TEZUKAYAMA GAKUIN UNIVERSITY

12

センサーを使ったセキュリティ対策

- 不審者の侵入検知
- 検知できない部分の対策
  - 監視カメラとの併用
- 部屋や住まい全体のセキュリティ
  - 玄関扉
  - 窓
- 外部からの操作できると
  - 逆にアタックの心配も

帝塚山学院大学 TEZUKAYAMA GAKUIN UNIVERSITY

13

監視カメラのセキュリティ

- パスワードなどの設定を適切にしていない
- ベンダーがメンテナンス用のバックドアを第三者に発見され悪用される
- コマンドインジェクションといった外部から任意のコマンドを実行可能な脆弱性が存在する
- 外部から認証なしにストリーミングを通信をアクセスできる
- 認証なしにシステムの設定ファイルをダウンロードできる

帝塚山学院大学 TEZUKAYAMA GAKUIN UNIVERSITY

14

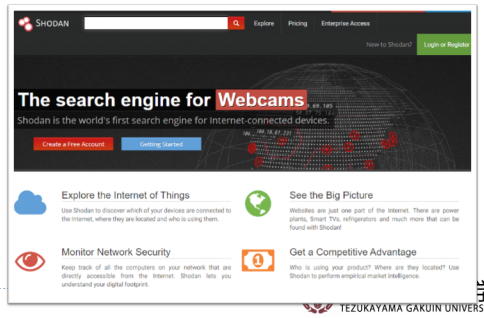
監視カメラを乗っ取る

- インターネットから室内外の様子をうかがう
  - ストーカー行為
  - 犯罪の計画
- 監視カメラを使用不能にする
  - 非常時の通報や監視を停止させる
- 監視カメラに悪意のあるプログラムをアップロードして動作させる
  - DDoS攻撃のボットとして利用する

帝塚山学院大学 TEZUKAYAMA GAKUIN UNIVERSITY

15

SHODANサイト



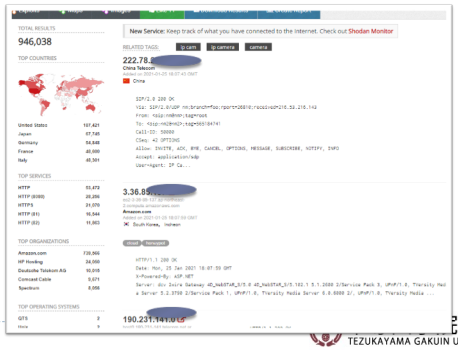
16

IoT機器を探し出すSHODAN

- SHODANはインターネットに接続されているIoT機器を検出
  - 色々なプロトコルのポートに対してリクエストを送り、そのレスポンスを記録する
    - インターネット上にどのような機器が接続しているか、どんなサービスが稼働しているかがわかる
  - レスポンスの情報をデータベースに記録し色々な検索条件でリストすることが可能
    - プロトコル、機種、特定のレスポンスに特有の文字列、サーバーのバージョン、ほか

17

SHODANを使ってIP Cameraというキーワードで検索



18