JPAAWG Japan Anti-Abuse Working Group

従来の攻撃プラットフォームがモバイルにかわりつつある現状と要因について

Internet Week 2021

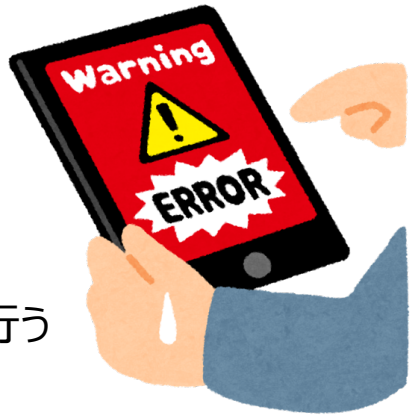
2021.11.25

Japan Anti-Abuse Working Group (JPAAWG)
Internet Initiative Japan Inc.

Shuji SAKURABA

モバイルは安全か

- モバイルの特徴
  - 常時起動 & ネットワークに接続
  - 最近の smartphone は高性能 (高度な処理が裏で動いていても気づきにくい)
  - 位置情報 (GPS) や音声，カメラなどにアクエスすることで各種盗聴可能
- MoqHao (Android)
  - 日本のリサーチャーの協力のもと Team Cymru が公表
  - SMS によるフィッシングで偽サイトを開くことで偽のアプリがダウンロードされ感染
  - C2 サーバに接続後，コマンドを受けて活動 (電話帳の参照，SMS 送信等) を行う
- Pegasus (iPhone)
  - イスラエルの NSO グループによる spyware, Toronto 大学の Citizen Lab. が明らかにした
  - iOS の脆弱性を悪用，malware を download して実行しなくても click するだけで感染 (のちに Apple に連絡し脆弱性を修正)
  - WhatsApp の音声通話機能のバグを悪用 (のちに修正)，通話への応答に関わらず感染



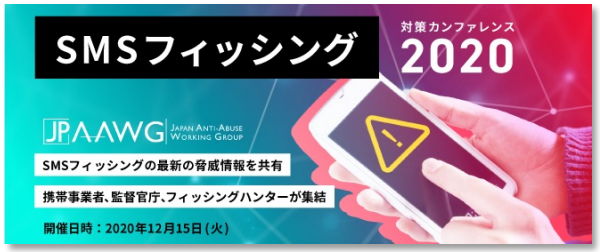
どのような対策ができるのか

- SMS (smishing)
  - 国際網接続による SMS 送信は送信元表示をある程度自由に設定可能
  - Email のように送信元情報から受け取り判断することは難しい
  - メッセージ内容や含まれる URL 等から判断することはある程度技術的には可能
- OTT
  - OTT (over the top) messaging についてはサービス提供側の運用
  - モバイル内のリソースへのアクセス許可については利用者判断
- 調査検知等
  - C2 サーバへのアクセス等を調べることで感染端末を特定することは可能
  - 調査して良いかどうかはいわゆる「通信の秘密」との整理が必要
  - C2 サーバの調査に関しては「電気通信事業におけるサイバー攻撃への 適正な対処の在り方に関する研究会 」の第3,4次とりまとめで整理されている
  - 感染端末の調査は，電気通信役務の提供に支障が生ずる蓋然性が具体的にある場合が前提

JPAAWG 活動

- JPAAWG とは
  - インターネットを中心とした電気通信環境の利用促進を目的とし、それらの健全な発展を脅かす各種ネットワーク上の脅威に対抗するため、Messaging, Malware and Mobile Anti-Abuse Working Group (M^{3}AAWG) と連携した活動を行う組織

- SMSフィッシング対策カンファレンス 2020
  - 2020年12月15日 @ Online 開催
  - 参加登録者数: 272名



- フィッシング対策として
  - フィッシング (smishing 含む) の情報収集および分析を行うプロジェクトを立ち上げ