サイバー攻撃とPKI

Trend Micro Incorporated
Regional TrendLabs Hitomi Kimura

Agenda

1. 近年のサイバー攻撃
2. PKI関連の事例
    1. 不正な証明書発行
    2. 不正なコード署名
    3. マルウェアとPKI
    4. 不正サイトのSSL/TLS化
    5. 不適切な鍵管理

近年のサイバー攻撃

日本を狙う攻撃まとめ

- 被害
  - マルウェア感染
    - バンキングトロジャン
    - ランサムウェア
    - バックドア
  - 公開システムへの攻撃
    - サービス不能攻撃
    - 脆弱性への攻撃
    - アカウントリスト攻撃
- 入り口
  - メール（添付ファイル、リンク）
  - Web閲覧（不正広告、改ざん、エクスプロイトキット）
  - 脆弱性

PKI関連の事例

1. 不正な証明書発行

- 2011年8月　DigiNotar事件
  - DigiNotarの不正証明書問題、その影響は
  - この事件を受け、 DigiNotarは同年9月20日に廃業

- 2015年3月　live.fi事件
  - 「hostmaster@live.fi」というメールアドレスを作れたことから始まった
  - A Finnish man created this simple email account - and received Microsoft's security certificate

- 〃　CNNIC事件
  - Maintaining digital certificate security

2. 不正なコード署名

- 主に標的型攻撃でみられる
  - 昨年確認されたPOSマルウェアにデジタル署名、標的型サイバー攻撃と関連

- Virus Totalを観察すると
  - コード署名済みのマルウェアは実際的にはほとんどがPotentially Unwanted Application
  - マス向けに出回るマルウェアに有効なコード署名がついている例はあまり見かけない

3. マルウェアとPKI

- バンキングトロジャン
  - クライアント証明書と秘密鍵の窃取
    - 法人ネットバンキングを狙う電子証明書窃取攻撃を解析
  - 不正なルート証明書のインストール
    - 日本を標的とする新たなオンライン銀行詐欺ツール「WERDLOD」の手口を解説
    - 狙いは国内ネットバンキング、日本郵政を騙るマルウェアスパムが拡散
  - 証明書エラー表示機能のバイパス
  - アドレスバーは緑のまま
    サードパーティドメインと非同期通信

3. マルウェアとPKI

- 標的型攻撃
  - 秘密鍵を含む認証情報のダンプ

- ハッキングツール
  - 「HKTL_JAILBREAK」
  - 「HKTL_MIMIKATZ」
    - 管理者権限があれば「エクスポート不可」の証明書秘密鍵のダンプが可能

4. 不正サイトのSSL/TLS化

- C&Cサーバーの SSL/TLS化

- Let’s Encryptの証明書を利用したドメインシャドウイングの事例
  - 日本を狙う不正広告事例でDV証明書の悪用を確認

5. 不適切な鍵管理

- 2015年2月 Superfish問題
  - メーカー製PCにプリインストールされていたソフトが利用していたSDKの鍵管理に不備があった
    - CVE-2015-2077(全環境で秘密鍵が同一)
    - CVE-2015-2078(証明書検証の不備)

5. 不適切(?)な鍵管理

- 復号される暗号化型ランサムウェアたち
  - CryptLocker(2014年8月)
    - セキュリティベンダが復号のための秘密鍵を確保した
      上記サイトは現在は既にクローズ
  - TeslaCrypt(旧バージョン)
    - Ver.1系(2015年4月)：共有鍵をファイルに保存していた
    - Ver.2系(2016年1月)：共有鍵を再生成できた
  - Petya(2016年4月)
    - 鍵空間が小さかったため鍵を特定できた

Thank you!

TREND MICRO