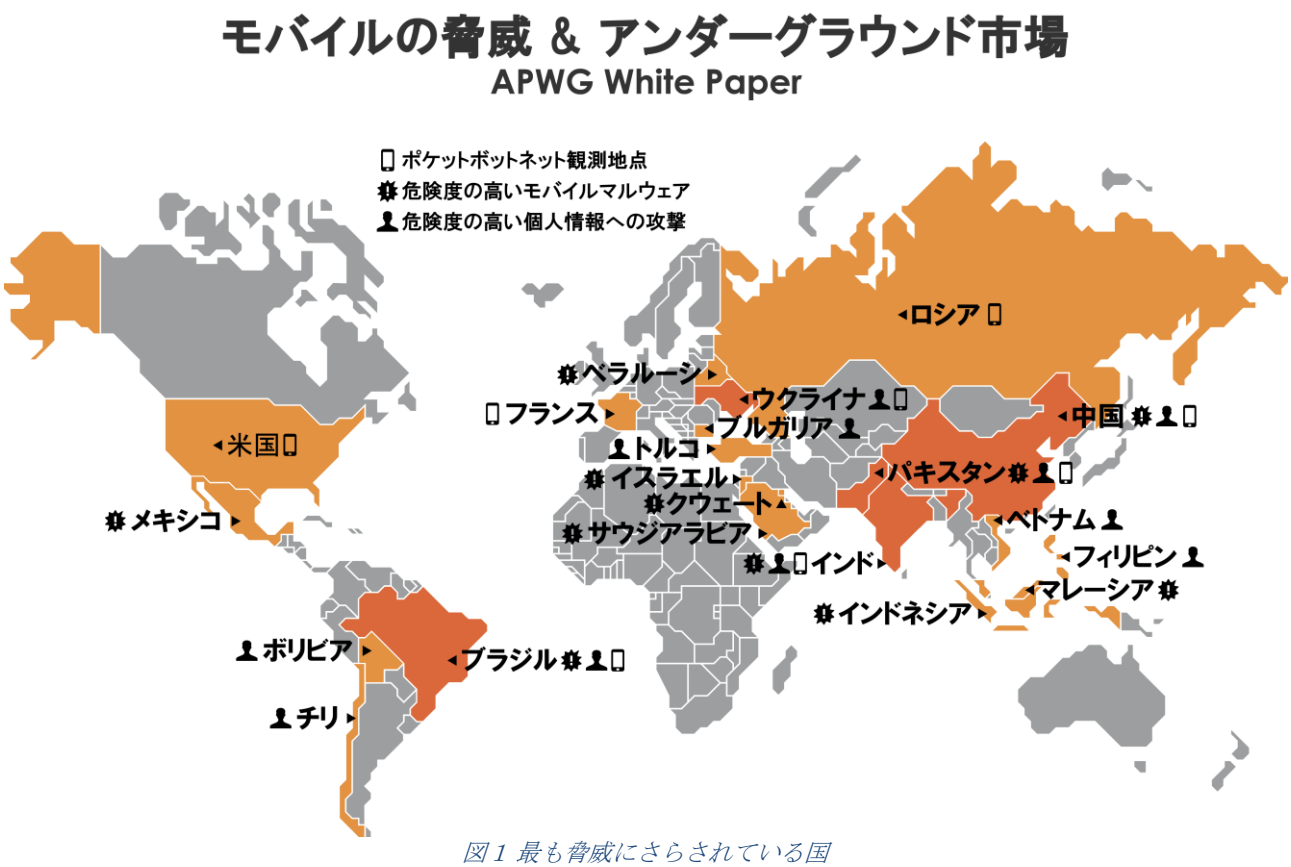

図 1 最も脅威にさらされている国

レポートのダウンロードは右記 URL より www.apwg.org

概　要

PC の販売数が減少する中で急激に発展しているモバイル市場は、2013 年に重要な局面を迎えている。市場動向は「ポスト PC」時代となっており、従来のデスクトップに対してモバイルデバイスがますます魅力的で、実用的かつ経済的な代替手段となっている。今後数年の間に、世界のモバイル決済市場は 1.3 兆米ドルを超えると予測されている。

モバイルのマルウェアマーケットはすでに存在しており、このマーケットがどのように存在し、ステルス侵入やクライムウェアのサプライチェーンをどのように運営しているかをいまこそ明らかにするべきである。

本稿では、これらのマルウェアマーケットを定義し、機動的で、アジャイルで、階層社会で、かつ自身で資金供給できる、業界の手口を示す。

現在解析されているマルウェアや攻撃手法には、次のようなタイプがある：スパイウェア、直接的なフィッシング攻撃、トロイの木馬、ワーム、マルウェアやポケットボットネットおよび複合的な攻撃によって配信されるアプリケーションで、その多くがユーザからお金を盗むために設計されている。同様に「track and trace」な侵入手法を用いて、所有者の利用方法や連絡先および習慣に関するインテリジェンスを抽出している。

本稿では、侵入のサプライチェーン構造とモバイルクライムウェアについて、実務的な視点から深く課題を分析して検討している。

コンテンツ

- モバイルの脅威
- インフラストラクチャに関する概要
- アンダーグラウンドのモバイルマーケット
- モバイルの DNS およびトラフィック
- iBot およびポケットボットネット
- モバイルへの侵入
- モバイルアプリ
- 介入、ルール、分類
- 戦略

脆弱性

- アーキテクチャ
- インフラストラクチャ
- ハードウェア
- 許可システム
- ソフトウェア
- コミュニケーション/配信経路(Wi-Fi, SMS, Bluetooth)
- 近距離無線通信(NFC)
- ハッシュを渡す(PtH)

統計と重要なポインター

- 2015 年までに、20 億以上のモバイルデバイスがアクティブだろう
- 例として、中国のインターネットユーザは現在 5. 64 億人；75%はモバイルユーザ
- 560 万件の Android を狙った不審なファイル(APK, dyn-calls, check-GPS 等)が報告されており、うち 130 万件は複数のウイルス対策ベンダから不正なものと確認されている

ツールキット&サービス例	価格(米ドル) – 2013 年 3 月	事例
モバイル侵入(キーロガー)	オープンソース- 400	Java & Python キーロガー、モビステルス(Mobistealth)
モバイル侵入(監視)	500 – 5,000	Finfisher 再設計版, Finfisher Lite & FlexiSpy 拡張版
バンキング窃盗向けモバイルマルウェア	10,000 – 30,000	Eurograbber, ZitMo, Tinba Trojan, DroidCleaner, Citadel (PtH 機能を含む)
モバイルボットネット(レンタル)	50 – 400	1 時間ごとの価格
モバイルボットネット (運用およびソースコードのカスタマイズ)	4,000 – 30,000	モバイル ISP サービス, SMS &ドライブバイダウンロード
モバイルマルウェア(不正な SEO およびアンダーグラウンド連携プログラム向け)	5,000 – 10,000	トラフィックのリダイレクト、J2ME や主要なプラットフォーム向けのスタンドアロンアプリケーション
対象国へのモバイルトラフィック	10 – 30 / 1,000 台	特別なアンダーグランドサービスを購入可能(エリア別や国別)
モバイル SMS スパムサービス	2-8 セント / SMS1 通	モバイル向けスパム
モバイル SMS スパム送信ツール	30-50	klychev v0.3 による SMS スパム送信
モバイル flooder (Skype や SIP)	30-80	Skype Flooder

図2 – モバイルアンダーグラウンド市場