Android Malware GinMasterとそのエコシステム

ソフォス株式会社
マーケティング マネージャー　平野祐司

SOPHOS

GinMaster とは？

GinMaster は、

- ✓Android OS を狙ったマルウェア
- ✓正規のアプリケーションに不正なコードを挿入しリパッケージ
- ✓主に中国の 3rd パーティのアプリサイトより広範囲に配布

GinMaster という名はどこからきた？

- ✓2011年8月に発見
- ✓Android 2.3(CodeName:Gingerbread)をルート化 (GingerBreak)
- ✓当初は、GingerMaster と呼ばれ、現在では GinMaster

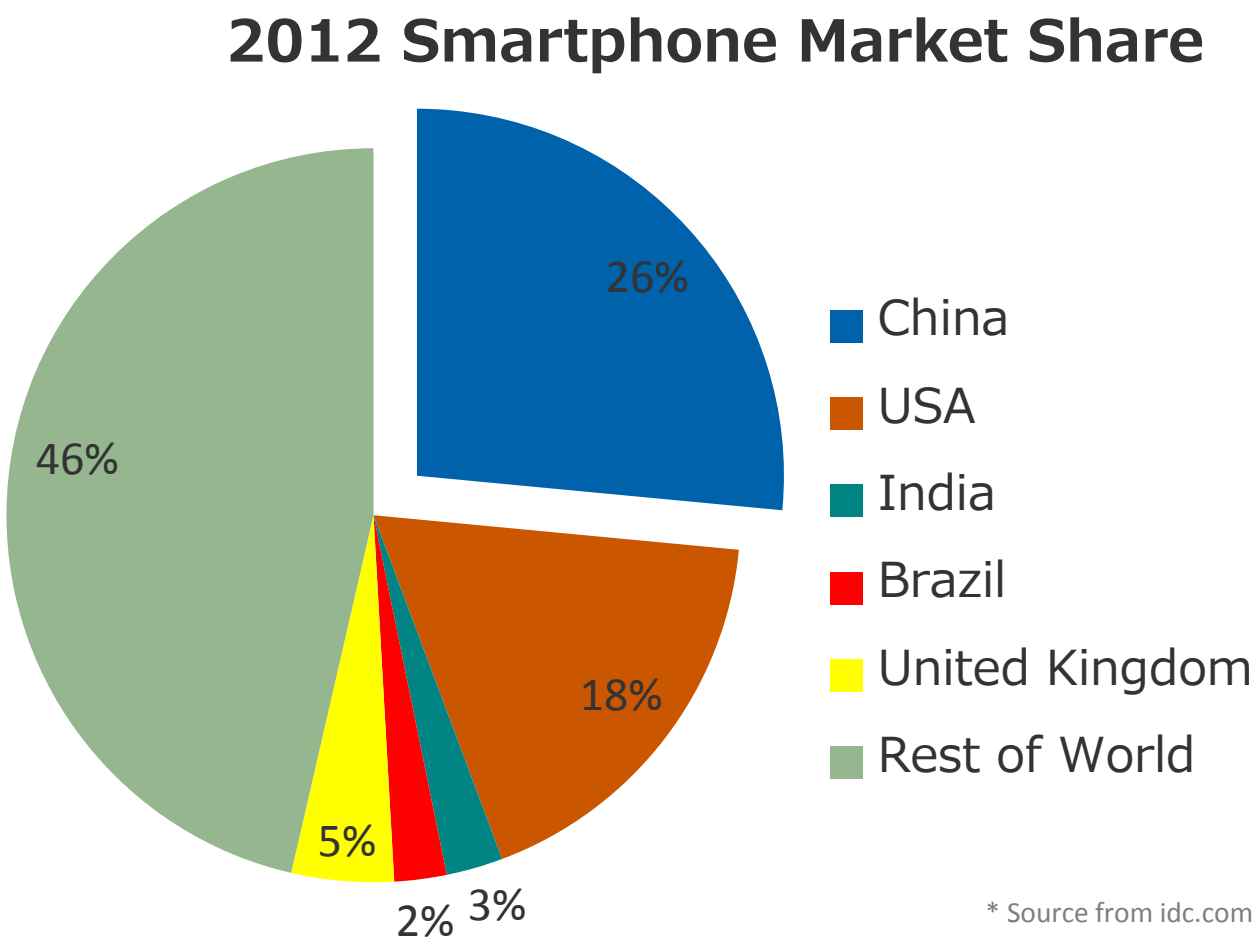
GinMaster の考察

1. バックグランド
2. 流行期間と流通量
3. 成長性
4. 機能
5. 複雑性
6. ビジネスシステム

   補足： PC マルウェアとの比較

1. バックグラウンド– 市場

150M+ 中国における Android デバイス数



* Source from idc.com

1. バックグラウンド– アプリ配布サイト数

400+ 中国におけるアプリ配布サイト数

Android Distribution in the West

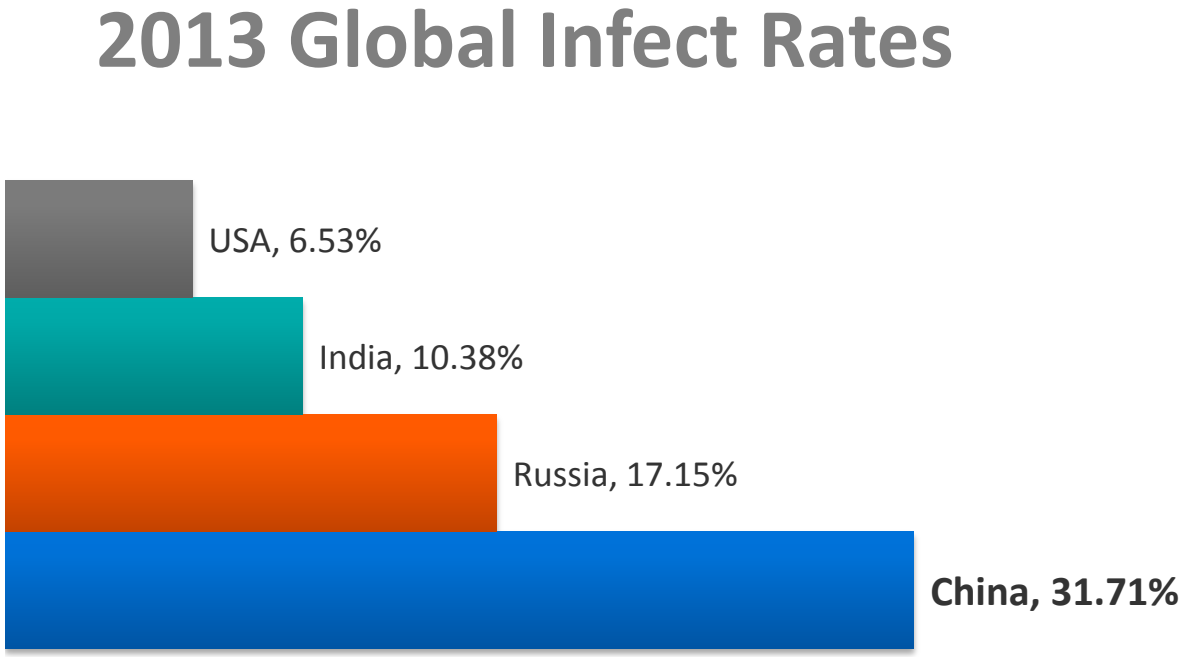
Google play

amazon.com

Making Sense of China Mobile Game Distribution

1. バックグラウンド – 感染レート

31.71% 中国での高い感染レート



* Report from NQ Mobile

2. 流行期間と流通量: 長期間にわたる

2011年 8月の発見以来

26ヶ月

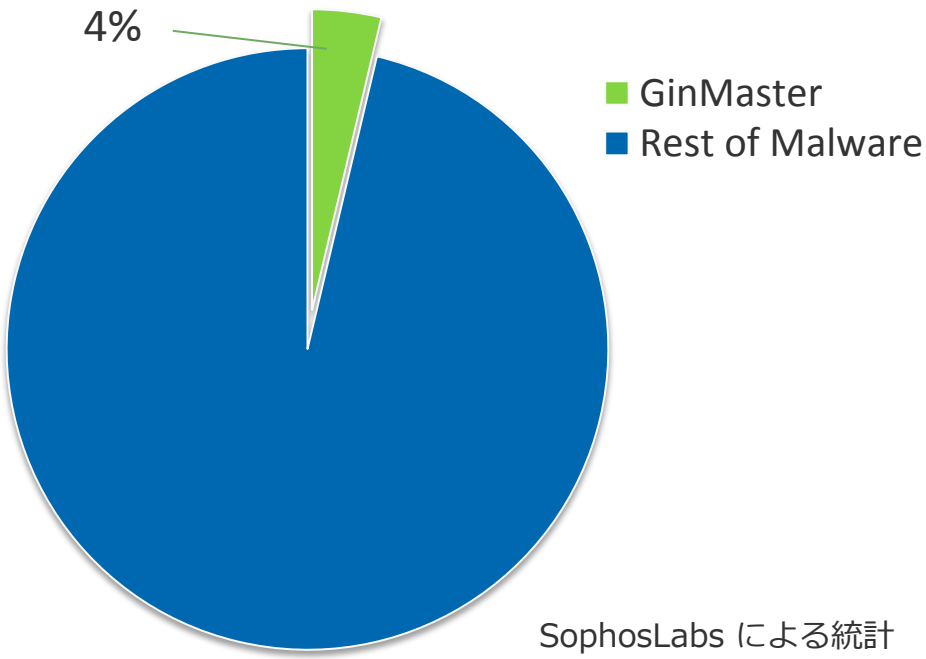
現在も活動中

マルウェアファミリーの数

300+

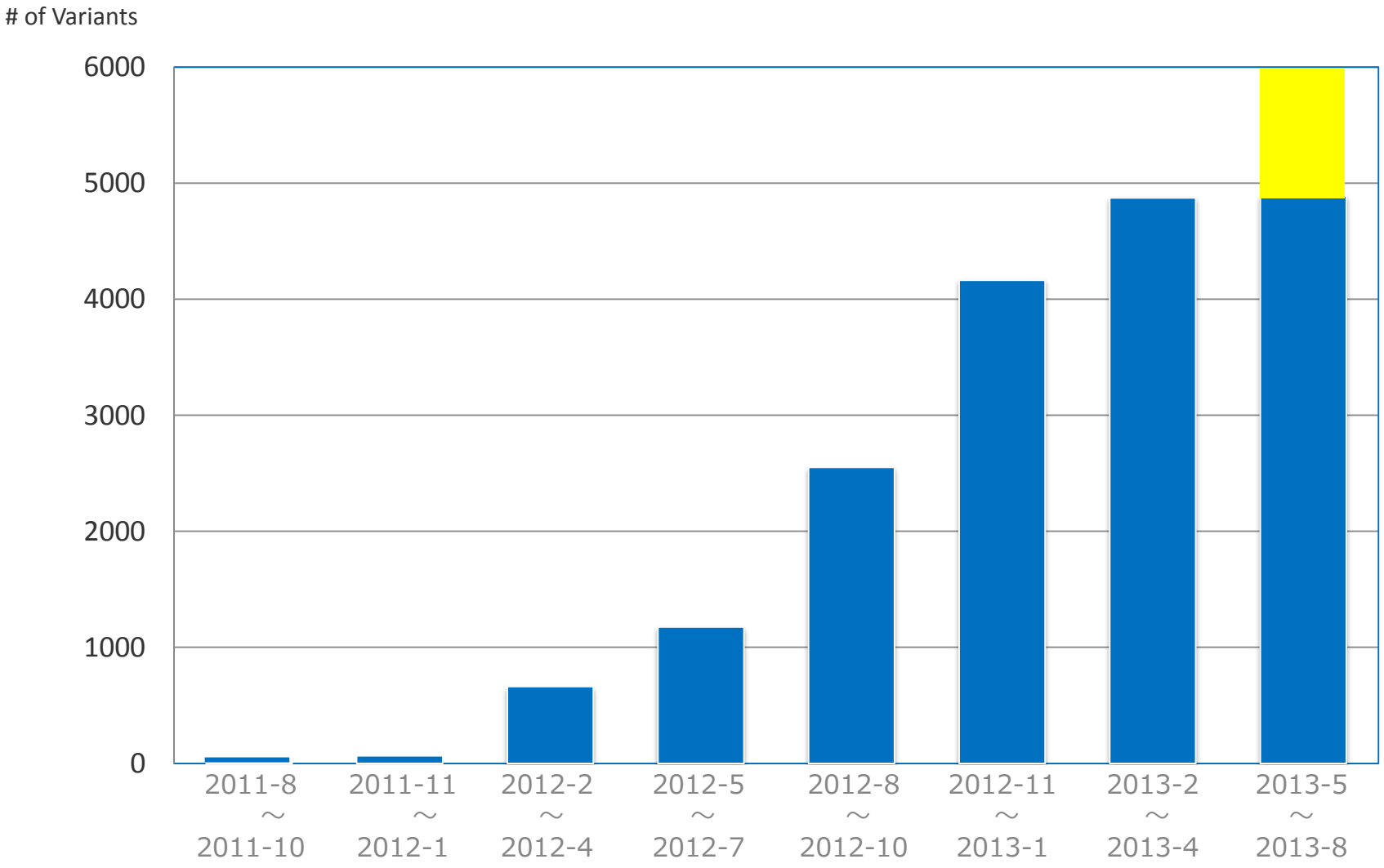
マルウェア数

19,100+



SophosLabs による統計

3. 成長性: 劇的な成長 4半期ごとの推移



4. GinMaster の機能

5. 複雑性 – 高度化されたマルウェア

第一世代の GinMaster

- ✓ 危険なアクセス許可の要求
- ✓ AndroidManifest の改変
- ✓ GameService (悪質なコードの中心部)
- ✓ バイナリーとシェルスクリプトで構成
- ✓ SQLite のデータベースにスキーマを作成
- ✓ Command and Control (C & C)

第二世代以降は、上記に加え、高度な難読化と暗号化

約95%

GinMaster 全体における
第二世代と第三世代の占める割合

6. ビジネスシステム ＄＄＄￥￥￥

GinMaster から垣間見る

ビジネスシステム

- ✓ マルウェアによる驚くべき利益
- ✓ マルウェア エコシステム
- ✓ マルウェア ビジネス戦略

マルウェアによる驚くべき利益

0.7%
感染
レート

1億5000万 台
Android デバイス

約 100万台の
Android デバイス
の感染

高いリスク 高いリターン
アプリ配布サイト経由
インストール毎に 0.5-2 元
概算　2-30,000 ダウンロード / 月

約100万元

低いリスク 低いリターン
PC や Mac OS 経由
概算 ユーザー1日あたり 0.02 元

約 50万元

約150万元/月

約$245,000 / 月
（1元≒16円 だと、約2400万円/月）

マルウェアのエコシステム

広告業者

トラフィックの増加

2 Android ユーザーが、悪意あるコードを含むアプリをダウンロード

サードパーティのアプリ配布サイト

Android ユーザー

- デバイスID、電話番号などを送信。
- デバイスにインストール、またはアンインストールされたアプリのパッケージ情報をレポート

1 3rd Partyのアプリ配布サイトにアプリをアップロード

マルウェア作成者

3 作成者は、正規アプリのプロモーションのため、契約を結ぶ

4 Command and Control (C&C)
- 設定の変更
- サイレントダウンロードの実行

5 正規のアプリのダウンロード

アプリの開発者※

※アプリの正規の開発者

マルウェアのビジネス戦略

最大限の利益を得るために、

マルウェア作成者は利用者のデバイスに、
可能な限り、悪意あるアプリインストールさせる

戦略1 効果的なアプリのカテゴリを選ぶ

ターゲットにするなら

ゲーム カテゴリを選べ！

戦略2 人気のアプリを選ぶ

ターゲットにするなら

熱くなる アプリを選べ！

ターゲットとされた日本製アプリ

- モバゲー
- 忍者ロワイヤル
- 牧場ホッコリーナ
- 逆襲のファンタジカ
- 100万人のモンスターファーム
- レイトン教授と世紀の七怪盗　など

戦略3 ウイルス対策ソフトより先へ

ウイルス対策ソフトの検出から逃れるため、
証明書は、コードサイニングだけでなく、

暗号化も使う！

証明書や暗号化アルゴリズムをこまめに変更する

※ 1つの証明書で、マルウェアアプリにコードサインしない

	1 つの証明書で暗号化されたアプリの数
第一世代 GinMaster	33.19
第二世代 GinMaster	3.81
第三世代 Gin Master	1.32

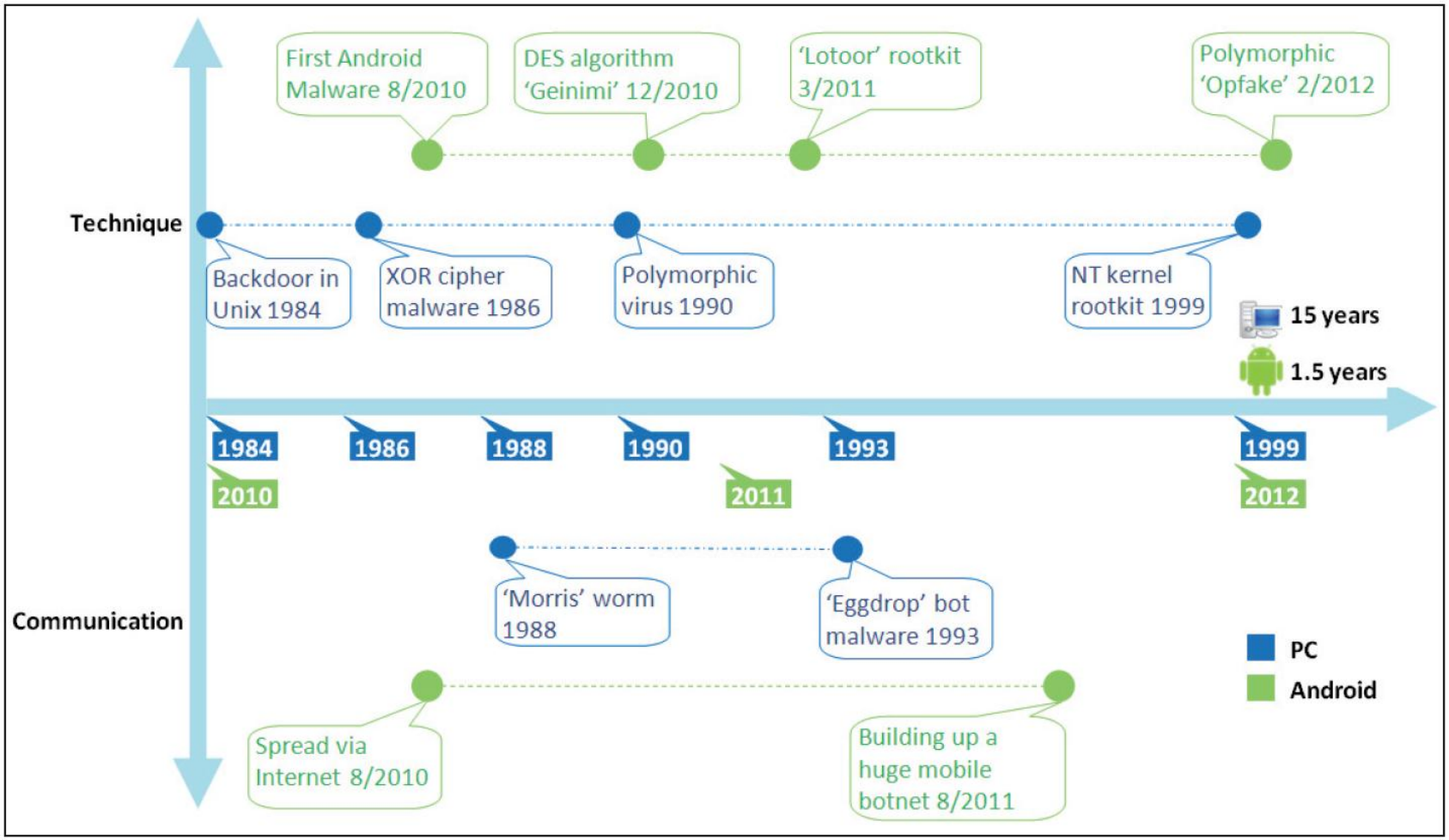
結論

- GinMaster を核としたエコシステムは、中国のアンドロイド マルウェアの代表的なモデル
- このモデルは、タイやベトナムなどの新興国へ広がる可能性がある
- すぐに収束する方向性は見えないので、今後もマルウェアとの戦いは継続中

補足

PC マルウェア と Android マルウェア

PC で 15年作り上げ脅威に、アンドロイドは1.5年で追いつく



PC マルウェア と Android マルウェア

比較対象

	Cipher (暗号化)	Polymorphic (多様化・多型化)	Botnet (ボットネット化)
PC	2 years (XOR)	6 years	9 years
Android	4 months (DES)	1.5 years	1 year

参考資料ダウンロード (英語)

GinMaster: A Case Study in Android Malware

http://www.sophos.com/ja-jp/medialibrary/PDFs/technical%20papers/Yu-VB2013.pdf

短縮 URL

http://bit.ly/17C7IBV

SOPHOS

SOPHOS

Security made simple.

ご清聴ありがとうございました。