Mobile Threats & the Underground Marketplace

APWG White Paper

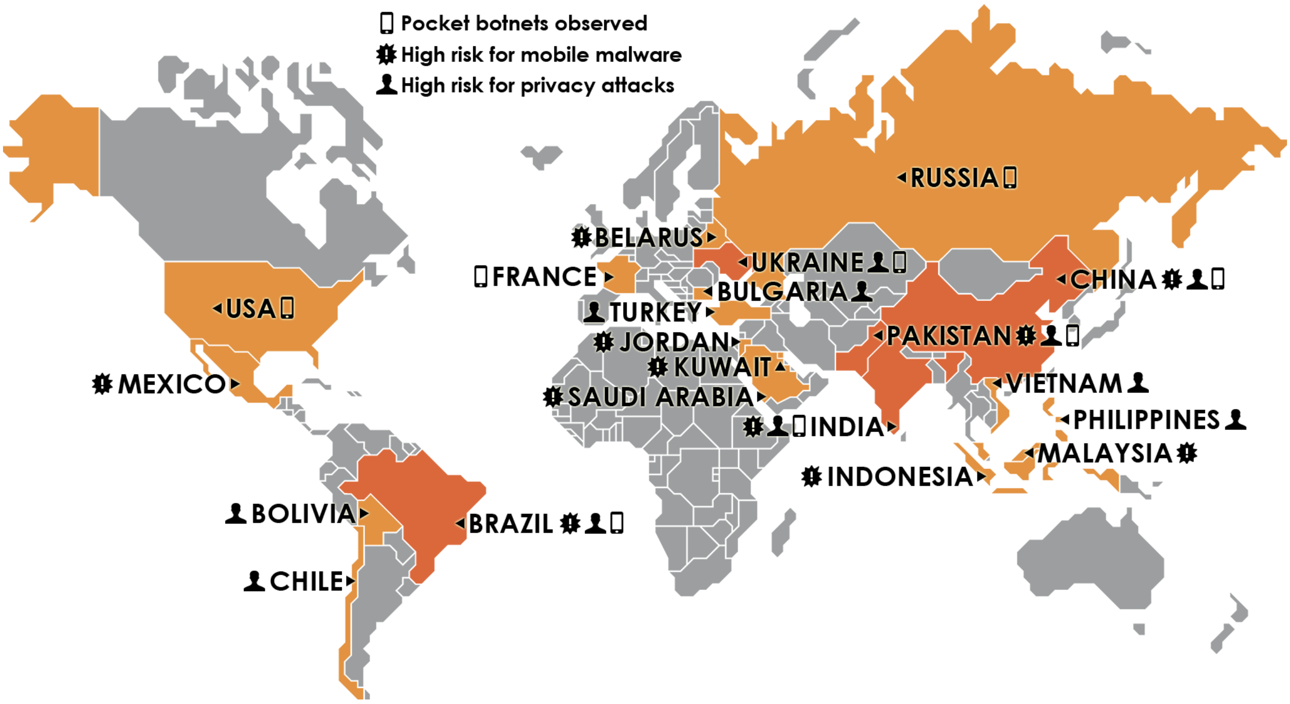

Figure 1 Countries at Most Risk

Download report at www.apwg.org

Abstract

A rapidly advancing mobile market, and a corresponding decline in PC sales, sees 2013 at a crucial intersection. In a market trend termed as the "post-PC" era, mobile devices increasingly present an attractive, practical and economical alternative to traditional desktops. In the next few years, global mobile payments are predicted to exceed $1.3tn.

While there is already an established mobile malware market, now is the time to take stock, to demonstrate the existence of such an industry and how it operates through stealthy intrusion and crimeware supply chains.

This paper defines these malware markets and demonstrates the modus operandi of an industry that is self-funding, prosperous, vertically stratified and agile.

Types of malware and attack methods under analysis include: spyware, phishing direct attacks, Trojans, worms, apps delivered through malware, pocket botnets and blended attacks, many of which are designed to steal or pilfer money from users. Equally as invasive can be "track and trace" intrusion techniques used to extract intelligence about an owner's usage, contacts, and habits.

This paper will provide a rhetorical approach towards mobile crimeware and the intrusion supply chain's structure as it examines subjects in depth from a practitioner's perspective.

Contents

Vulnerabilities

- Architecture
- Infrastructure
- Hardware
- Permission systems
- Software
- Communication/delivery channels (Wi-Fi, SMS, Bluetooth)
- Near-Field Communication (NFC)
- Passing the Hash (PtH)

Statistics & Key Pointers

- By 2015 – est. 2 billion + mobile devices
- China as an example now has 564 million Internet users; 75% are mobile
- 5.6 million potentially-malicious files reported on Android (APK, dyn-calls, checks-GPS, etc.), of which 1.3 million are confirmed malicious by multiple AV vendors

Sample Toolkits & Service	Price (US$) - March 2013	Example Descriptions
Mobile intrusion (keyloggers)	Open Source - 400	Java & Python Keyloggers, Mobistealth,
Mobile Intrusion (surveillance)	500 – 5,000	Re-engineered Finfisher, Finfisher Lite & FlexiSpy extended copies
Mobile malware for banking theft	10,000 – 30,000	Eurograbber, ZitMo, Tinba Trojan, DroidCleaner, Citadel (inc. PtH capabilities)
Mobile botnet (rental)	50 - 400	Hourly rates
Mobile botnets (operational & tailored source code)	4,000 - 30,000	Mobile ISP service, SMS, & Drive by
Mobile malware for black SEO and underground partnership programs	5,000 – 10,000	Used to traffic redirects, J2ME midlets, or standard applications for the popular platforms.
Mobile traffic by targeted country	10 – 30 per 1,000 hosts	Can be bought through special underground services (by area, by country)
Mobile SMS spam service	2-8 cents per 1 SMS	Mobile spamming
Mobile SMS spamming tool	30-50	SMS spamer by klychev v0.3
Mobile flooder (Skype or SIP)	30-80	Skype Flooder

Figure 2 - The Mobile Underground Marketplace