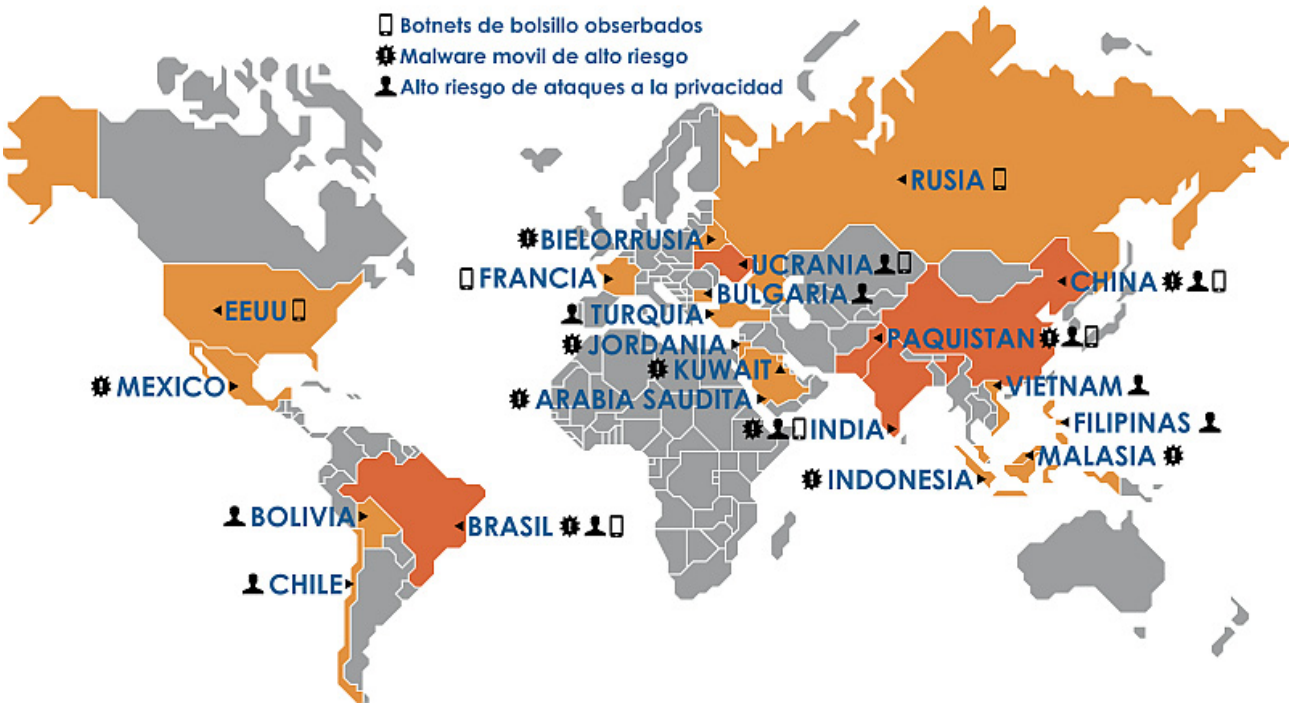

Figura 1 Países con más riesgo

Para descargar el documento ir a: www.apwg.org

Resumen

El mercado de telefonía móvil, que está rápidamente creciendo, y la correspondiente disminución en las ventas de PC, hacen aparecer 2013 como un momento crucial. La tendencia de mercado se denomina como la era "post-PC", donde los dispositivos móviles son considerados cada vez más atractivos, prácticos y económicos comparados con los PC tradicionales. En los próximos años, se estima que los pagos móviles en el mundo superara los 1,3 billones de dólares.

Con el establecimiento de un mercado de malware para móvil, ahora es el momento de hacer un balance, para demostrar la existencia de dicha industria, y la forma en que opera a través de la intrusión furtiva y de cadenas de distribución delictivas.
Este documento define los mercados de malware y demuestra el modus operandi de una industria que se auto-financia, próspera, esta verticalmente estratificada y se caracteriza por su agilidad.

Los tipos de malware y métodos de ataques analizados incluyen: spyware, ataques de phishing directos, troyanos, gusanos, aplicaciones distribuidas a través de malware, botnets de bolsillo (pocket botnets) y ataques combinados, muchos de los cuales están diseñados para robar dinero de los usuarios. Igualmente invasiva se puede incluir la técnica de intrusión "rastrear y localizar" utilizada para extraer información sobre el uso, los contactos y los hábitos de los usuarios.

Este documento ofrecerá un enfoque retórico hacia el crimeware móvil y la estructura de la cadena de suministro de la intrusión, ya que examina los temas en profundidad y desde la perspectiva del practicante.

Contenido

- Amenazas Móviles
- Información sobre la Infraestructura
- Mercado Negro para Móviles
- DNS & Trafico Móvil
- iBots & Botnet de Bolsillo (Pocket Botnet)
- Intrusión Móvil
- Aplicaciones Móviles
- Intervención, Reglas & Clasificaciones
- Plan de estrategia

Vulnerabilidades

- Arquitectura
- Infraestructura
- Hardware
- Sistemas de permisión
- Software
- Canales de comunicación / entrega de contenidos (Wi-Fi, SMS, Bluetooth)
- Near-Field Communication (NFC)
- Pasando el hash (PtH)

Estadísticas & Elementos principales

- Hacia 2015 – est. 2 billones + dispositivos móviles.
- China, por ejemplo, ahora tiene 564 millones de usuarios Internet: 75% son usuarios de móviles.
- Virustotal actualmente estima que hay 5.6 millones de archivos Android (APK, dyn-calls, checks-GPS, etc.) potencialmente maliciosos. De los cuales 1.3 millones son confirmados como maliciosos por dos o más vendedores de Anti-Virus.

Ejemplos de Toolkits & Servicios	Precio (US$) - Marzo 2013	Descripción
Intrucion de móviles (keyloggers)	**Open Source - 400**	**Java & Python Keyloggers, Mobistealth**
Intrucion de móviles (surveillance)	**500 – 5,000**	**Re-ingeniería de Finfisher, Finfisher Lite y las copias extendidas de FlexiSpy**
El malware móvil para robo bancario	**10,000 – 30,000**	**Eurograbber, ZitMo, Tinba Trojan, DroidCleaner, Citadel (inc. capacidades PtH)**
Botnets móviles (alquiler)	**50 - 400**	**Precio por hora**
Botnets móviles (código fuente operative y adaptado)	**4,000 - 30,000**	**Servicio ISP móvil, SMS & Drive-by**
Malware móvil para el SEO negro y programas de asociación ilicitas	**5,000 – 10,000**	**Se utiliza para redirecciones de tráfico, J2Me MIDlet o aplicaciones estándar para las plataformas más populares.**
Tráfico móvil por un país determinado	**10 – 30 para 1,000 hosts**	**Se puede comprar a través de servicios negros especiales (por área, según el país)**
Servicio de spams SMS para móviles	**2-8 cents para cada SMS**	**Spamming para móviles**
Herramienta de spams SMS para móviles	**30-50**	**SMS spamer de klychev v0.3**
Flooder móvil (Skype o SIP)	**30-80**	**Skype Flooder**

Figura 2 - El Mercado Negro para Móviles