Malware móvil: Principios y defensas

Prof. Dr. Pedro García Teodoro

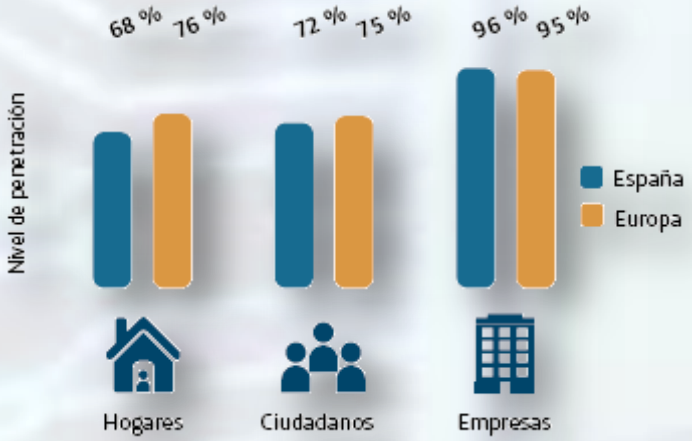
Network Engineering & Security Group (http://nesg.ugr.es)

UGR CyberSecurity Group (UCyS)

Dpto. Teoría de la Señal, Telemática y Comunicaciones
Universidad de Granada

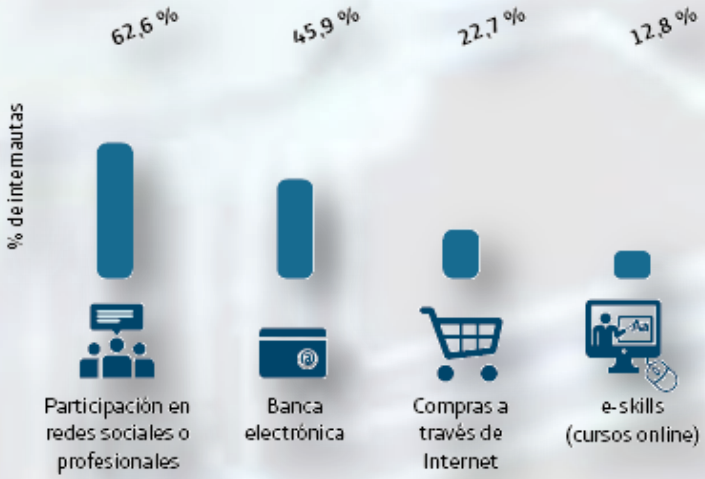
Datos previos *(i)*

- Penetración social de las TIC:



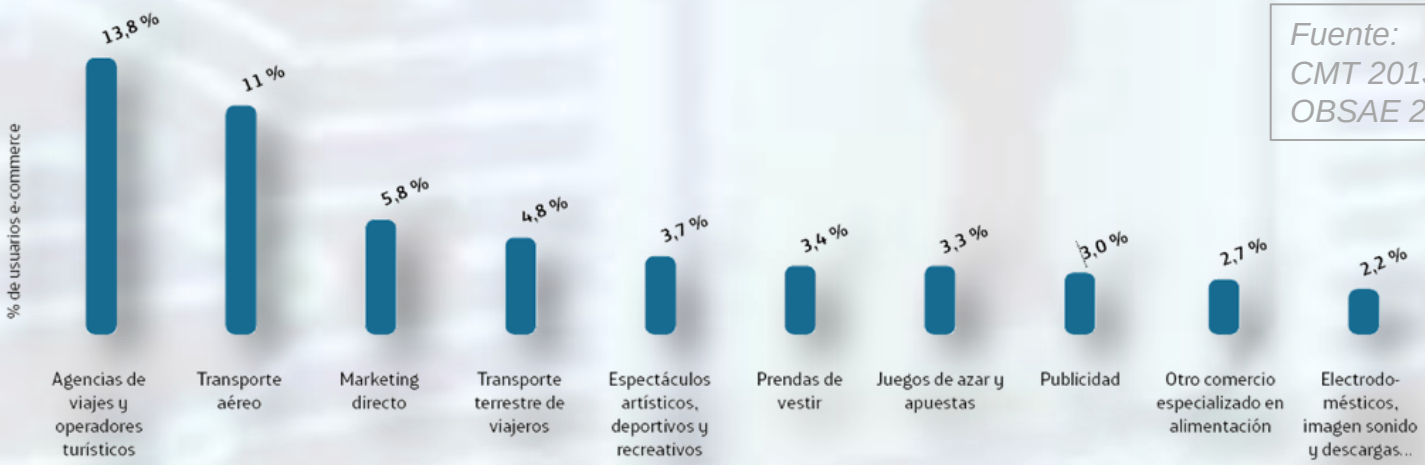
Fuente:
INE, Eurostat 2012

- Usos de Internet:



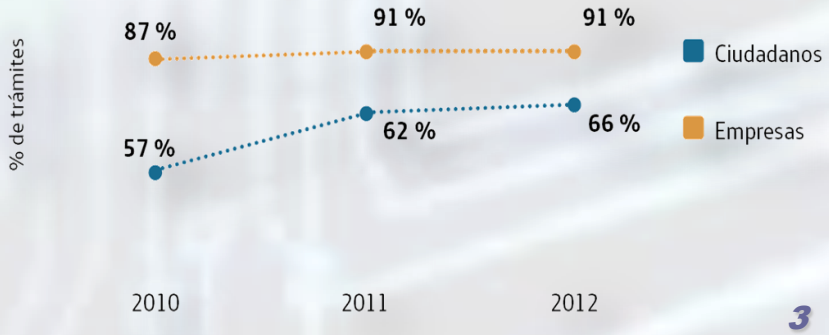
Datos previos *(ii)*

- e-Comercio:



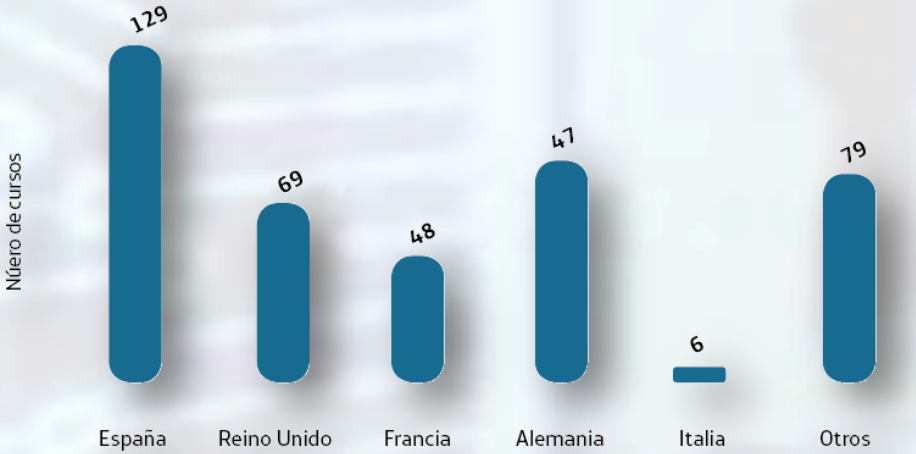
Fuente:
CMT 2013
OBSAE 2013

- e-Administración:



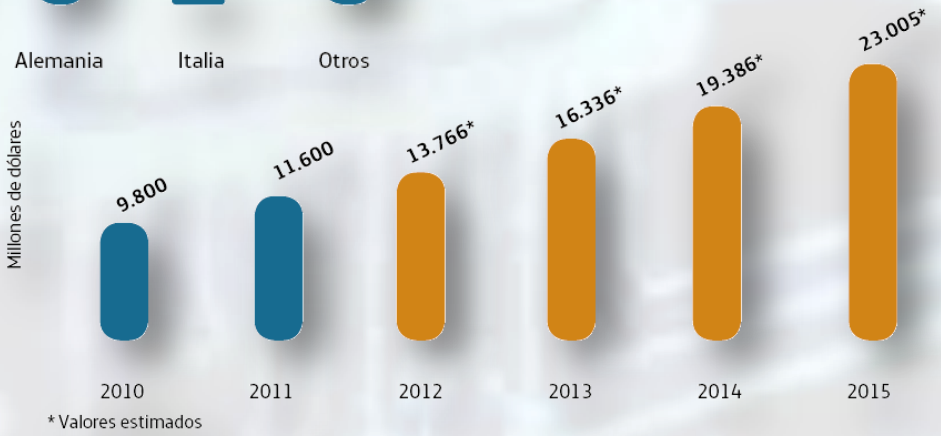
Datos previos *(iii)*

- e-Enseñanza:



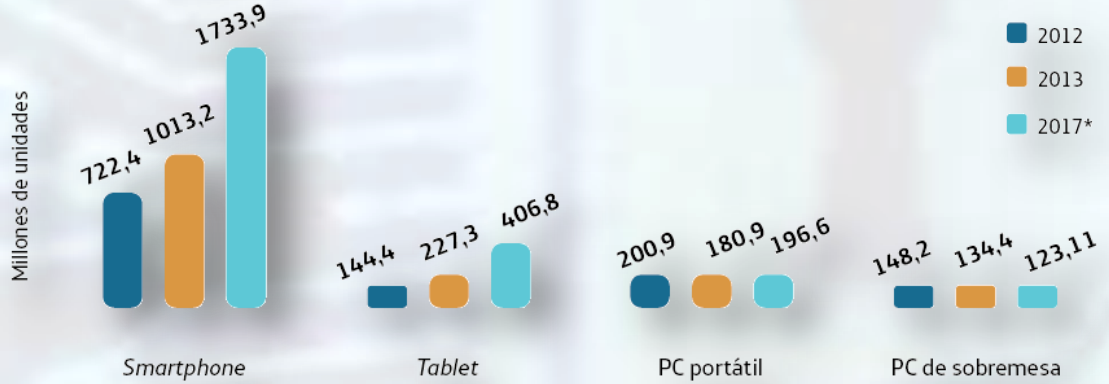
Fuente: Telefónica 2013

- e-Salud:



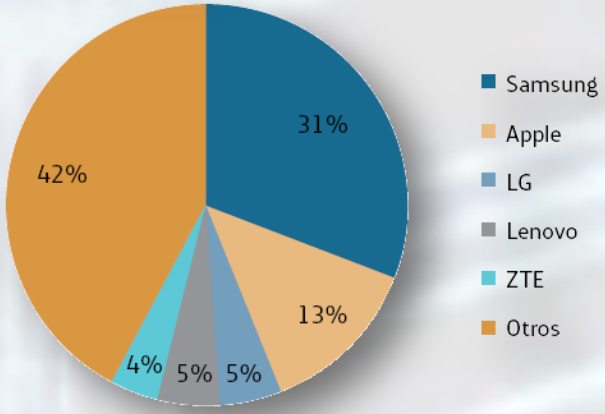
Datos previos *(iv)*

- Venta de terminales:



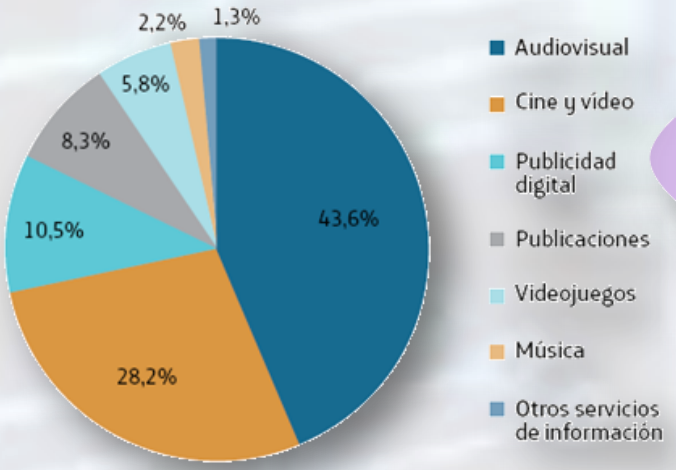
Fuente: IDC 2013

- Cuota móviles:



Datos previos *(v)*

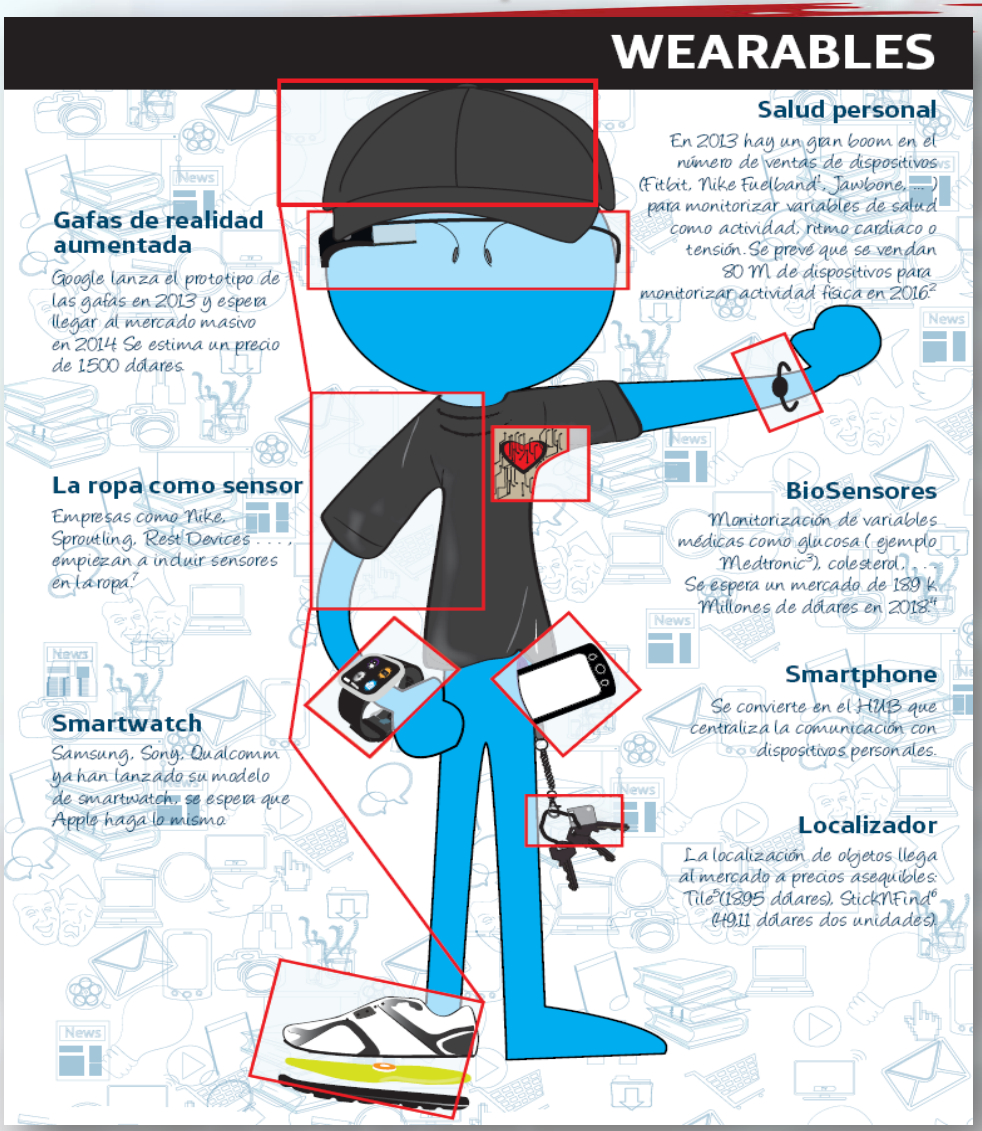
- ¿Por qué móviles?: ubicuidad y comodidad
- Uso de móviles:
  - Contenidos digitales



  - Redes sociales

Datos previos *(vi)*

- Versatilidad *smartphones* y tendencias:



Índice

- Conceptos
- Estadísticas MwMv
- Métodos y técnicas
- Tendencias
- Defensas

Conceptos *(i)*

- *Seguridad*: protección de activos frente a amenazas, entendidas estas como la capacidad potencial de mal uso de los primeros (hard/soft/humanos)

- *Ataque*: mal uso de los activos
- *Hacker*: usuario malicioso
- *Malware*: software malicioso incluido o insertado intencionadamente (y sin permiso) en un sistema para causar algún daño

Conceptos *(ii)*

- Tipos de *malware*:
  - Virus: código auto-replicante
  - Gusanos: auto-propagativo
  - Troyanos: software funcional pero malicioso
  - *Rootkits*: afectan el sistema operativo
  - *Backdoors*: puertas traseras de acceso
  - *Bots*: dispositivos infectados controlados remotamente
  - …

Conceptos *(iii)*

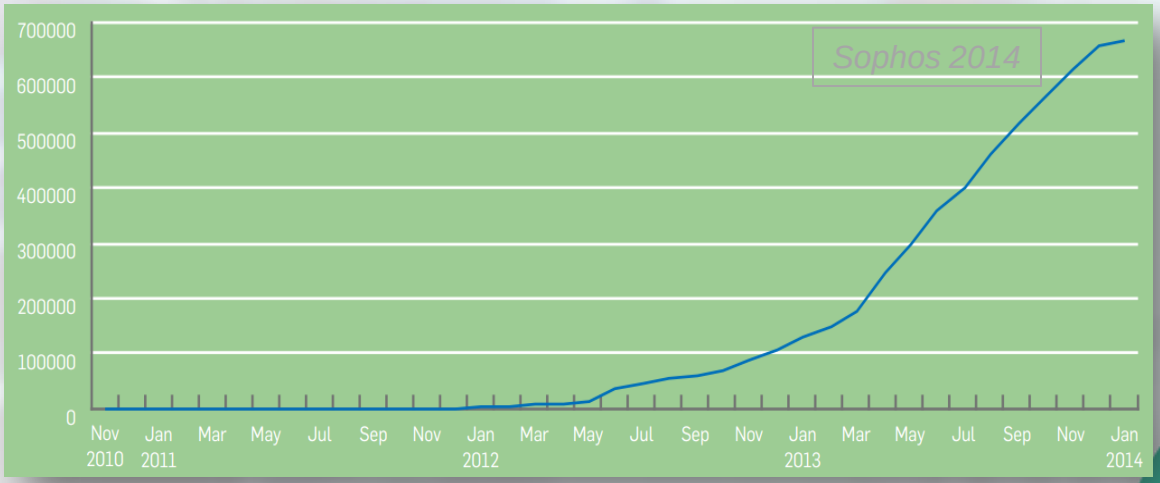
- Objetivos atacantes: MEECES
  - *Money*
  - *Entertainment*
  - *Ego*
  - *Cause*
  - *Entrance to social groups*
  - *Status*

Índice

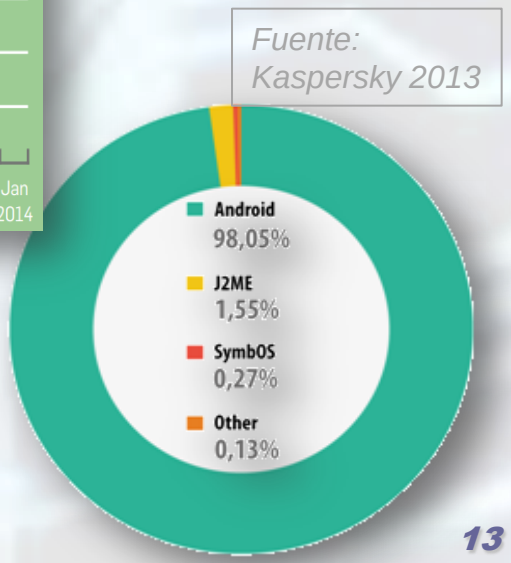
- Conceptos
- Estadísticas MwMv
- Métodos y técnicas
- Tendencias
- Defensas

Estadísticas *(i)*

- Evolución del *malware* para móviles:

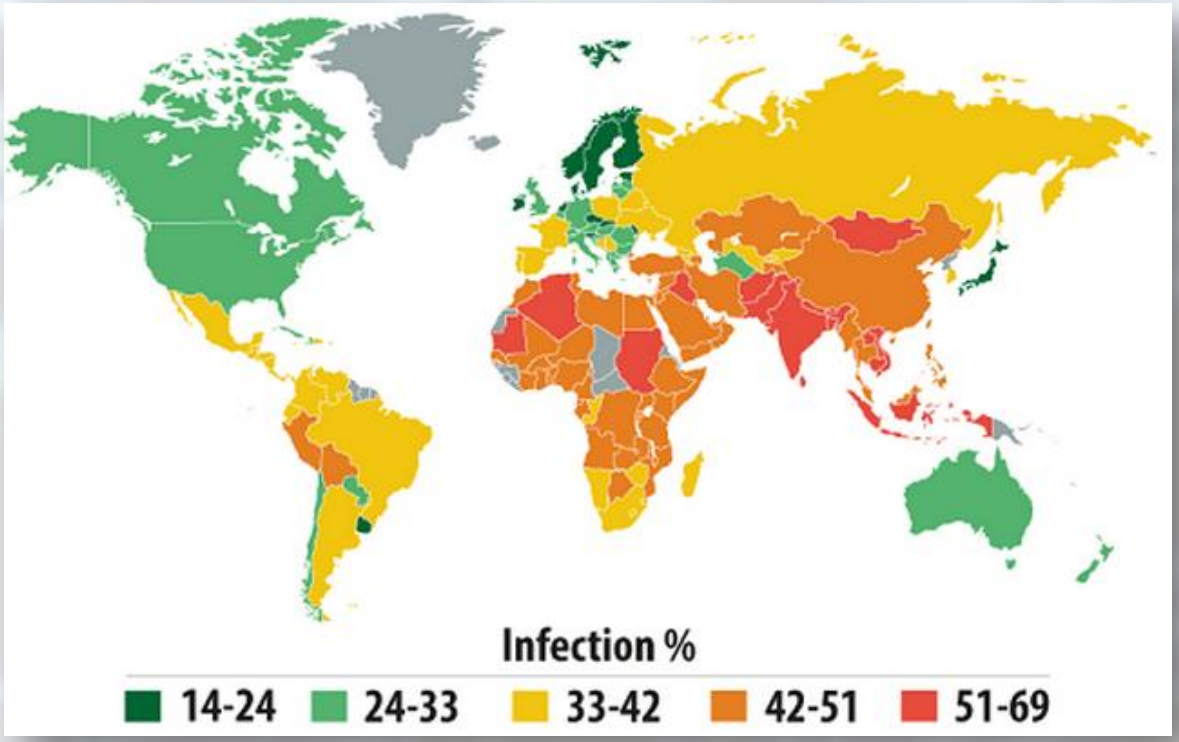


- Afectación sistemas:



Estadísticas *(ii)*

- Impacto:



Fuente: Kaspersky 2013

Índice

- Conceptos
- Estadísticas MwMv
- Métodos y técnicas
- Tendencias
- Defensas

Métodos y técnicas *(i)*

- Vectores de infección:

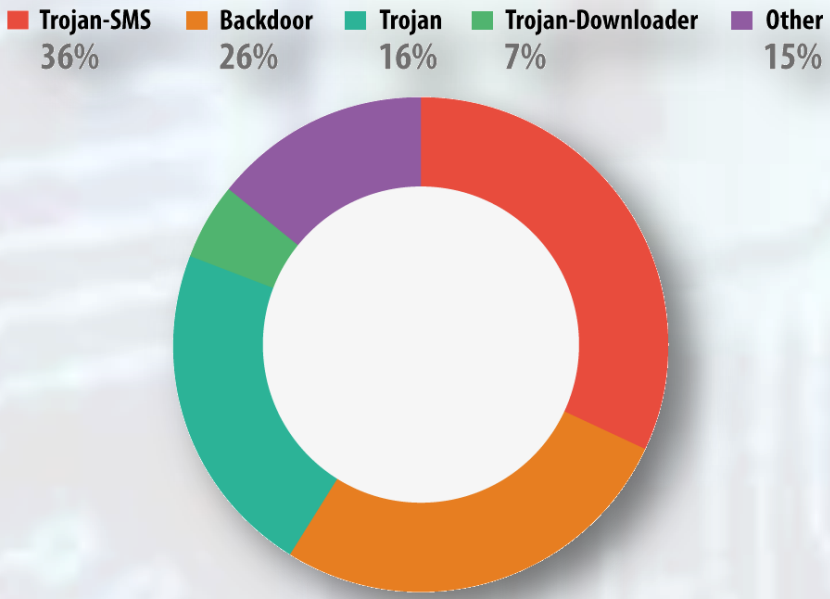
  Formas de afectación

  - Descargas web
  - *App stores* alternativas
  - SMS
  - Correo electrónico
  - Vulnerabilidades sistemas:

    debilidades de diseño y/o implementación

Métodos y técnicas *(ii)*

- Software malicioso en móviles:



Fuente: Kaspersky 2013

Métodos y técnicas *(iii)*

- 10 familias más populares en 2013:

	Name*	% of all attacks
1	DangerousObject.Multi.Generic	40.42%
2	Trojan-SMS.AndroidOS.OpFake.bo	21.77%
3	AdWare.AndroidOS.Ganlet.a	12.40%
4	Trojan-SMS.AndroidOS.FakeInst.a	10.37%
5	RiskTool.AndroidOS.SMSreg.cw	8.80%
6	Trojan-SMS.AndroidOS.Agent.u	8.03%
7	Trojan-SMS.AndroidOS.OpFake.a	5.49%
8	Trojan.AndroidOS.Plangton.a	5.37%
9	Trojan.AndroidOS.MTK.a	4.25%
10	AdWare.AndroidOS.Hamob.a	3.39%

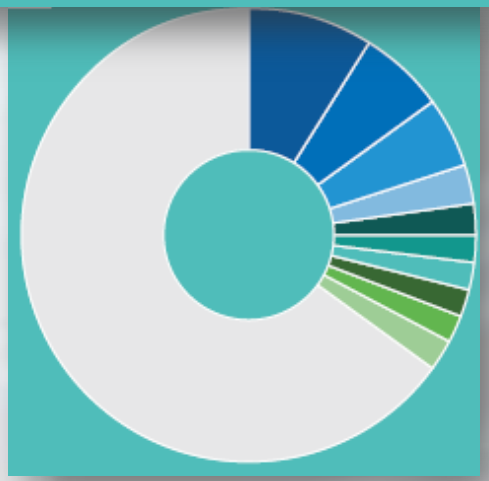
Fuente: Kaspersky 2013

Métodos y técnicas *(iv)*

- Ataques Android:

Andr/BBridge-A	9%	Andr/Adop-A	2%	Andr/SmsSend-BE	2%
Andr/Fakeins-V	6%	Andr/Boxer-D	2%	Andr/MTK-B	2%
Andr/Generic-S	5%	Andr/SmsSend-BY	2%	Other	65%
Andr/Qdplugin-A	3%	Andr/DroidRt-A	2%		

Fuente: Sophos 2014



Métodos y técnicas *(v)*

- Ejemplos:
  - Falseo *media player* e instalación del usuario desde una web infectada.
  - *Rootkit* en forma de módulo *kernel* descargable que puede abrir un *shell* para el atacante ante la recepción de una llamada entrante desde un cierto número

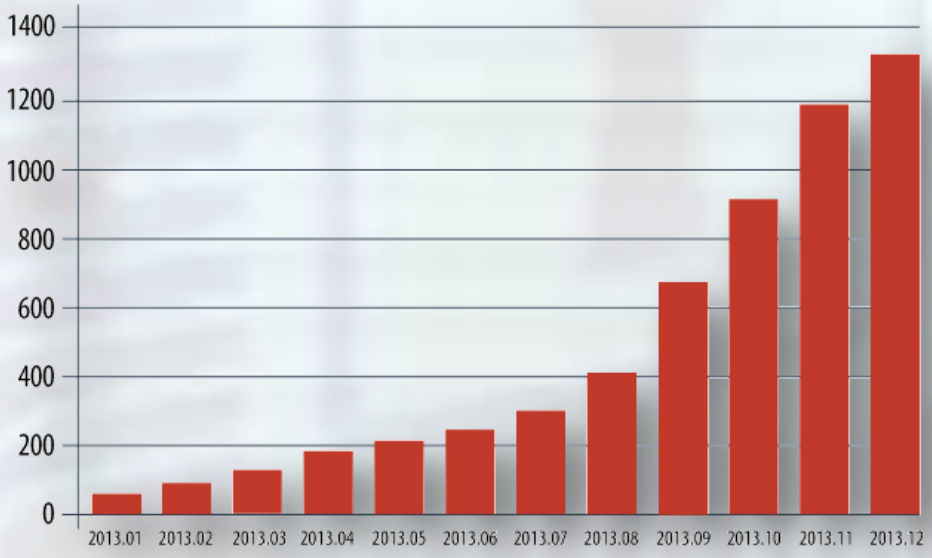
    ⇨ Acceso a SMS, GPS, llamadas de voz, etc.

Índice

- Conceptos
- Estadísticas MwMv
- Métodos y técnicas
- Tendencias
- Defensas

Tendencias *(i)*

- Troyanos bancarios:

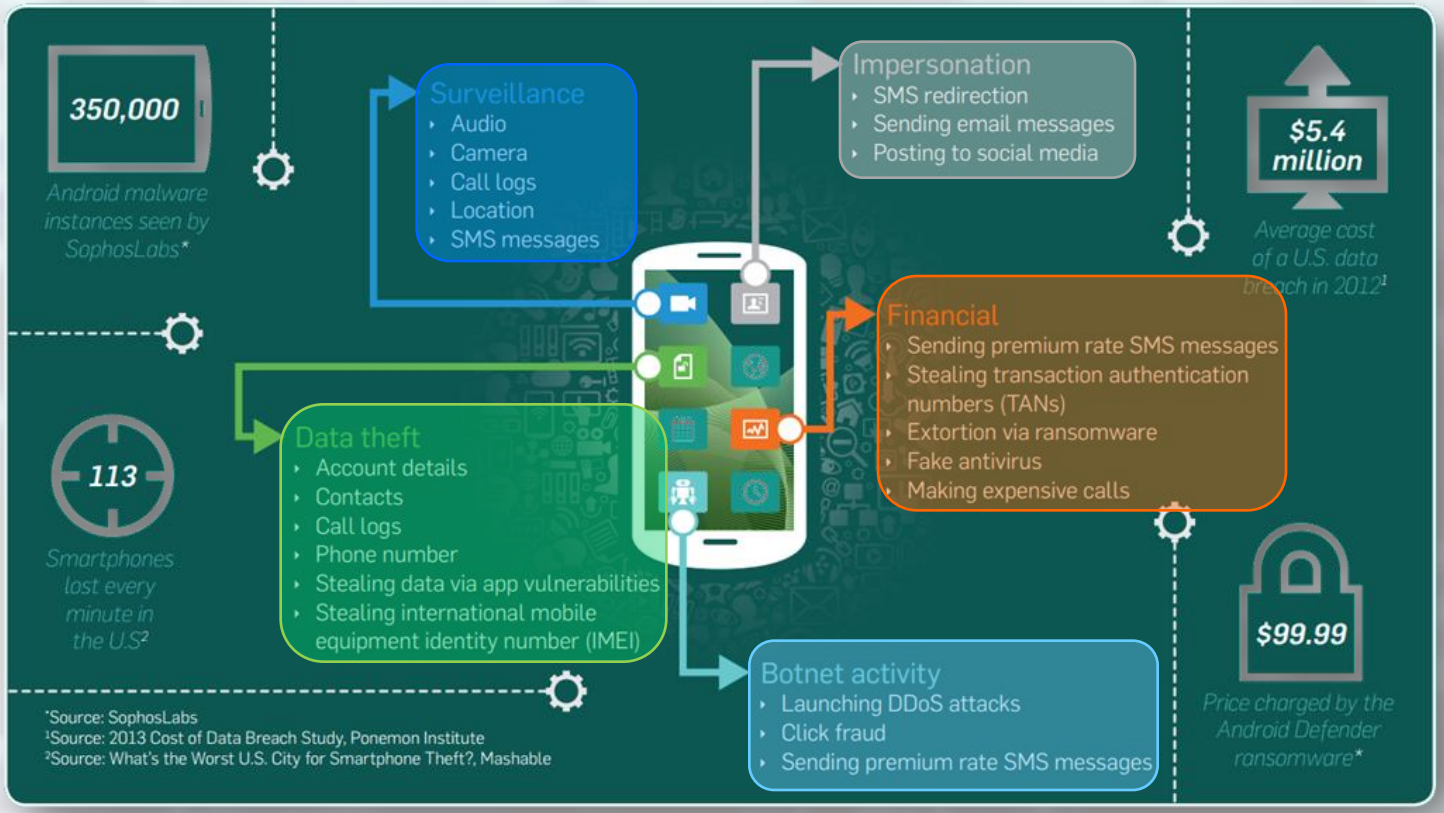


Fuente: Kaspersky 2013

- *Svpeng*
- *Perkele*
- *Wroba*

Tendencias *(ii)*

- Anatomía de un móvil *hackeado* y efectos:

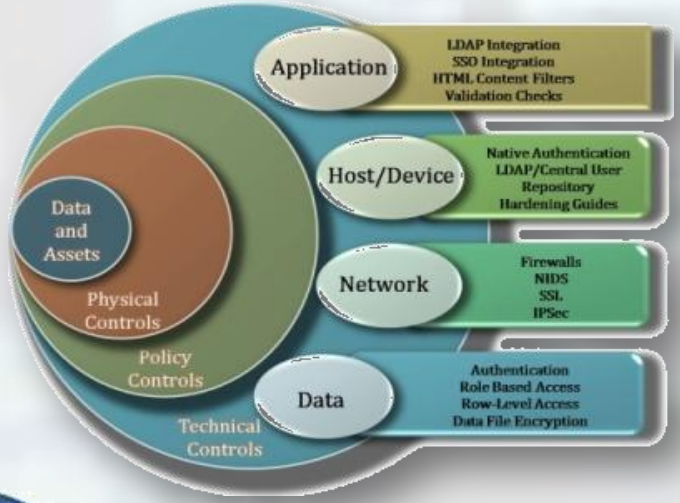


Índice

- Conceptos
- Estadísticas MwMv
- Métodos y técnicas
- Tendencias
- Defensas

Defensas *(i)*

- Seguridad en profundidad (*in-depth*):
  - Información *en tránsito* vs. información *estática*
  - Niveles de trabajo:
    - Redes, equipos y sistemas, aplicaciones/servicios, datos



- Líneas de defensa:
  1. Prevención
  2. Detección
  3. Respuesta

Defensas *(ii)*

- Consejos para prevenir *malware*:
  1. Informar usuarios sobre riesgos
  2. Seguridad en accesos (p.ej., criptografía)
  3. Políticas BYOD (“bring your own device”)
  4. Evitar *jailbreak*
  5. Actualizar equipos y sistemas
  6. Cifrado de dispositivos
  7. Políticas de seguridad móvil
  8. Instalar *apps* de fuentes confiables
  9. Compartición en nube
  10. Software *anti-malware* …

Software seguridad móvil:

Defensas (iii)

LEGEND

Platform
- And: Android
- Win: Windows
- Sym: Symbian

Type of Detection (ToD)
- S: Static
- D: Dynamic

Other
- ∅: Unavailable

Type of Monitoring (ToM)
- SYS: System calls
- NET: Network
- EL: Event Log
- I: Instructions
- P: Permissions
- PT: Program Traces
- PCB: Process Control Block
- API: API Calls
- K: Kernel-level
- U: User-level

Type of Analysis (ToA)
- E: Expert
- ML: Machine Learning
- CL: Clustering
- DG: Dependency Graphs
- ST: Statistical
- PRO: Probabilistic Models

Type of Identification (ToI)
- A: Anomaly
- M: Misuse
- SPEC: Specification

Place of Monitoring and Identification (PoMI) and Place of Analysis (PoA)
- L: Local Outline
- IRM: Local Inline (IRM)
- C: Cloud
- DB: Distributed
- HP: Honeypot
- RC: Replica in the Cloud
- SB: Sandbox
- H: Hybrid

		Detection Approach									
	Plat.	ToD	ToM	ToA	ToI	PoMI	PoA	Consumption	Features	Attack	Observations
Dendroid (2013) [118]	And	S	I	ST, DG, CL	∅	C	C	Discussed: deals efficiently with large databases of malware instances	Code Chunks – a high-level representation of the CFG	Automatic classification of unknown malware samples	The classification is done using text mining and information retrieval techniques. Hierarchical Clustering is also used to extract evolutionary analysis
AppProfiler (2013) [123]	And	S, D	API, PT	E	M	L	L, C	Not available	Permissions, and API Calls	Privacy leakage	API calls are analyzed statically using signatures and apps are traced dynamically through tainting analysis
Apps Playground (2013) [124]	And	D	SYS, PT	∅	∅	C	C	Not applicable	Taint tracing, SYS call, etc.	Any kind	Heuristic-based UI interaction based on contextual exploration
Secloud (2013) [125]	And	*	*	*	*	RC	C	Device consumption not available	Any kind	Any kind	Detection techniques: AV scanning, file integrity checking, SYS call monitoring, or network intrusion detection and response
TStructDroid (2013) [126]	And	D	PCB	STAT, ML	A	L	L	Performance degradation of 3.73% on average	Frequencies of 99 preliminary parameters: page frames, context switches, page faults, virtual memory, etc.	Any kind	Type of analysis: theoretic analysis, time–series feature logging, segmentation and frequency component analysis of data, and machine learning classifier
Andromaly (2012) [127]	And	D	*	ML	A	L	L	16,78*Kb* ±32 RAM (≈ 8.8%), 5.52% ±2.11 CPU, and 10% Battery (unclear)	Detection Method: monitorization of features. Feature selection: Subset of selected features from 88 initial categories	Any kind of anomaly	Training Method: Classification with labelled data. Experimental evaluation
AppGuard (2012) [128]	And	D	PT	∅	M	IRM	C	Not available	Program traces and generated events	Privacy leakage and user–level misuse —kernel-level is not monitored	Analysis is done off-line, prior to repackaging the app, i.e., in the cloud
Crowdroid (2011) [129]	And	D	SYS	CL	A	L	C	Not available	System calls per application	Any kind of anomaly	Training Method: Clustering with k–means: i) malware, and ii) goodware. Evaluation: Experimental and wild malware
DroidScope (2012) [130]	And	D	*	∅	∅	SB	C	Not applicable	Any kind	Any kind	ToM: Syscalls, etc. Ad–hoc plugins for monitoring features and analyzing data (authors provide several proof of concepts, e.g.: tainting
MADAM (2012) [131]	And	D	K, U	ML	A	L	L	Overhead of 3% memory utilization, 7% CPU and 5 % battery	K: SYS, proc., memory, CPU usage. U: user–state, key strokes, called numbers, SMS, NET	Any kind of anomaly	K-NN (with K=1) for classification. 10 malicious apps and 50 benign. 93% detection rate and 5% FP
Peng et al. (2012) [132]	And	S	P	PRO	N/A	C	C	Not applicable	Permissions	Effectiveness of apps permissions	
RiskRanker (2012) [133]	And	S	I/P/API	DG	M	C	C	Not applicable	Vulnerability signatures, permissions, API calls: crypto, dynamic code, IPC, and JNI, etc.	Any kind	Checks a pre-defined set of malicious operations (e.g.: known exploits) to rate the severity of stealthy applications
SmartDroid (2012) [134]	And	H	*	*	*	SB	SB	Unavailable	Any	UI–based obfuscation	Improved detection by generating UI-based trigger conditions. Any kind of detection system might be plunged, but no further details are given

Defensas *(iv)*

- Software seguridad móvil *(cont.)*:
  - *Network Log*: **monitoriza** las conexiones de red de las aplicaciones instaladas
  - *OS Monitor*: controla los procesos y las conexiones de cada aplicación
  - *SmartDroid*: envío de notificaciones ante **detección** de ciertos eventos, definidos por el usuario *(firmas)*
  - *CONAN mobile*: indica nivel de seguridad, monitoriza las aplicaciones y los permisos y mantiene listas de IP y números llamados

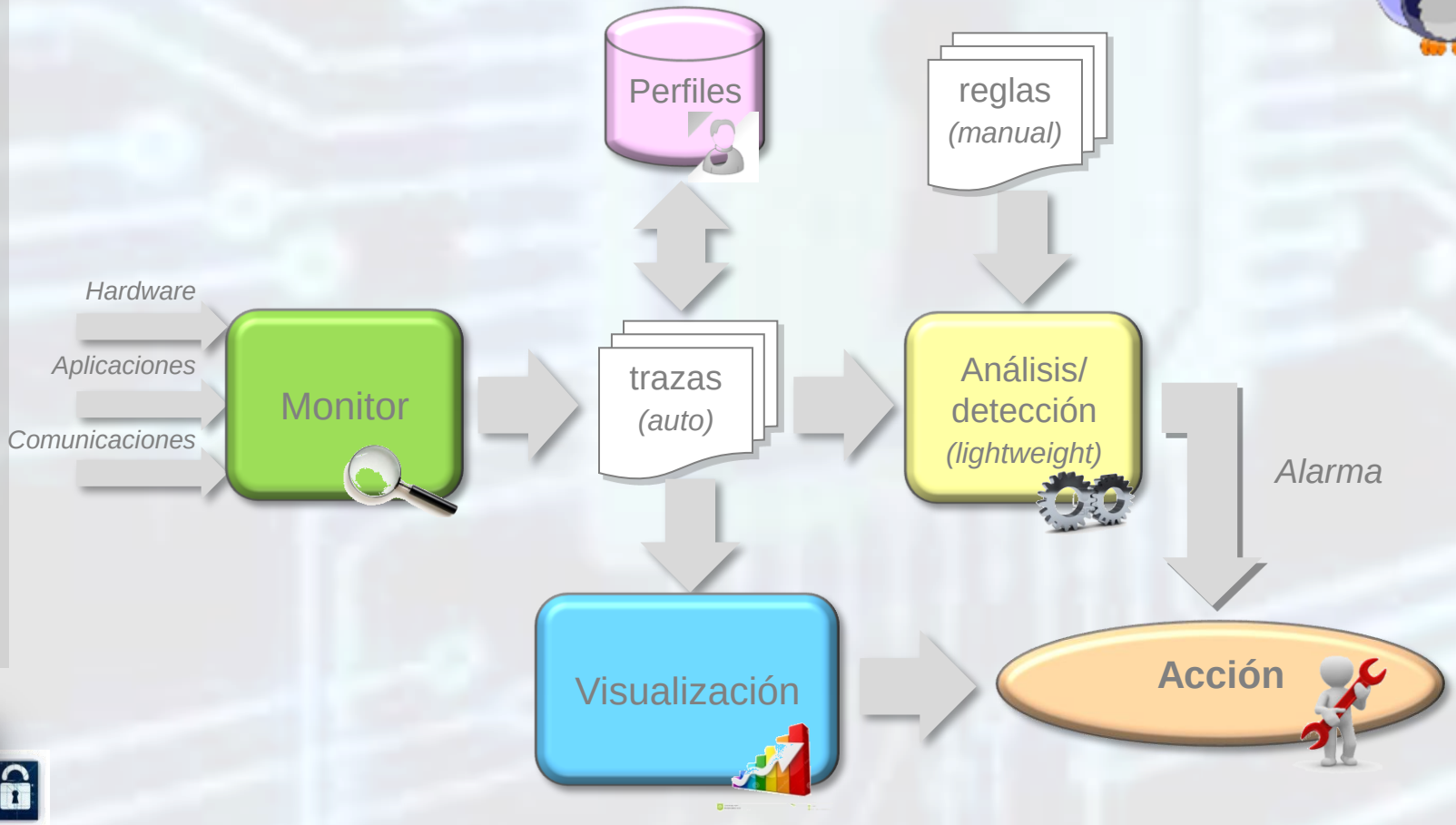
Defensas *(v)*

- Software seguridad móvil *(cont.)*:
  - *ComDroid*, *Woodpeker*: permisos entre aplicaciones
  - *DroidMOSS*: similitud *fuzzy* entre apps para detectar cambios
  - *RiskRanker*: comportamientos peligrosos pre-definidos
  - *DREBIN*: aplicaciones maliciosas/benignas mediante SVM
  - *Andromaly*: detección de anomalías *machine-learning* (ML)
  - *MADAM*: uso de características *kernel-/user-based* y ML
  - *Crowdroid*: detección de troyanos basada en llamadas al sistema
  - *DroidAPIMiner*: uso de características *API-based* y KNN
  - *TaintDroid*: monitorización de datos privados sensibles

Retos: *lightweight* → detección "colaborativa"

Defensas *(vi)*

- ADroid: monitorización y detección anomalías



Bibliografía

- Fundación Telefónica: *La Sociedad de la Información en España 2013*. *http://www.fundacion.telefonica.com/es/arte_cultura/publicaciones/detalle/258.*
- IAB y eLOGIA: *IV Estudio Anual Redes Sociales*. Abril, 2014. *http://www.iabspain.net/wp-content/uploads/downloads/2014/04/V-Estudio-Anual-de-Redes-Sociales-versi%C3%B3n-reducida.pdf.*
- Kaspersky Lab: *Security Bulletin 2013*. *http://media.kaspersky.com/pdf/KSB_2013_EN.pdf.*
- Sophos Labs: *Sophos Threats Security Report*. Mobile World Congress, 2014.
- M. La Polla, F. Martinelli, D. Sgandurra: *A Survey on Security for Mobile Devices*. IEEE Communications Surveys & Tutorials, Vol. 15, N. 1, pp. 446-471, 2013.
- G. Suárez. J.E. Tapiador. P. Peris, A. Ribagorda: *Evolution, Detection and Analysis of Malware for Smart Devices*. IEEE Communications Surveys & Tutorials, pp. 1-27, 2014.
- A. Ruiz-Heras, P. García-Teodoro: *Monitorización y Detección de Anomalías en Dispositivos Android*. TFG Grado Ing. Tecnologías Telecomunicación, 2013/2014.

¡¡GRACIAS!!