Malware para móbiles

A. Casi siempre online;

B. Tiene mucha potencia computacional;

C. Contiene muchos datos sensibles:

- e-mails;
- redes sociales;
- banco online;
- ubicación actual

Aislamiento de procesos

- iOS: el núcleo utiliza MAC para decidir, si cada aplicación tiene acceso a los determinados ficheros y/o espacios de memoria;

- Android: se crea un usuario distinto para cada aplicación y el Linux se preocupa automáticamente de la separación de privilegios;

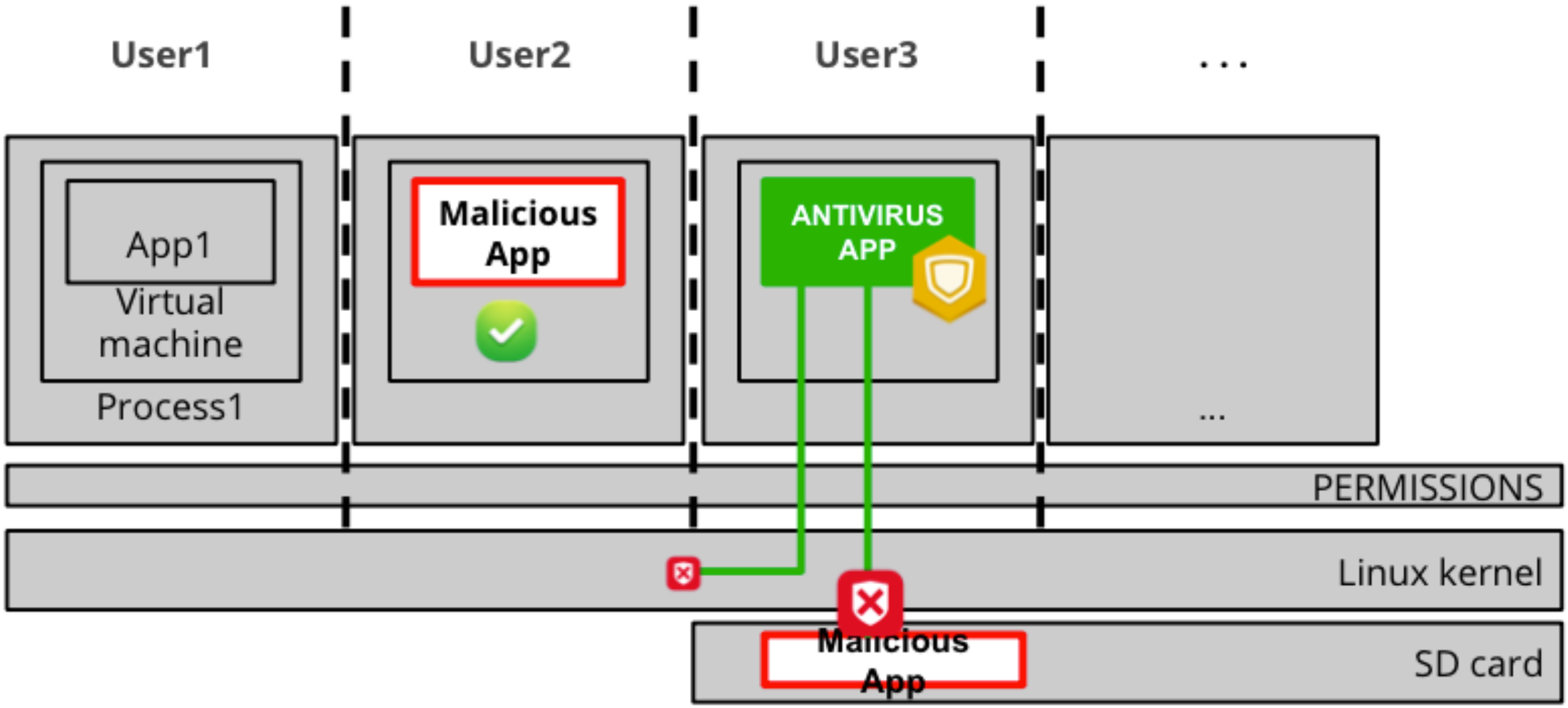
- Al final: en ambos casos, las aplicaciones no pueden comunicarse entre sí.

Autorización

- iOS: utiliza “perfiles de privacidad” para definir las reglas de control de acceso (Safari -> Contactos). El usuario tiene que permitir el acceso, por definición está prohibido.

- Android: cada aplicación muestra una lista de permisos que quiere obtener. Hay que permitir todo- ¡o no se instala!

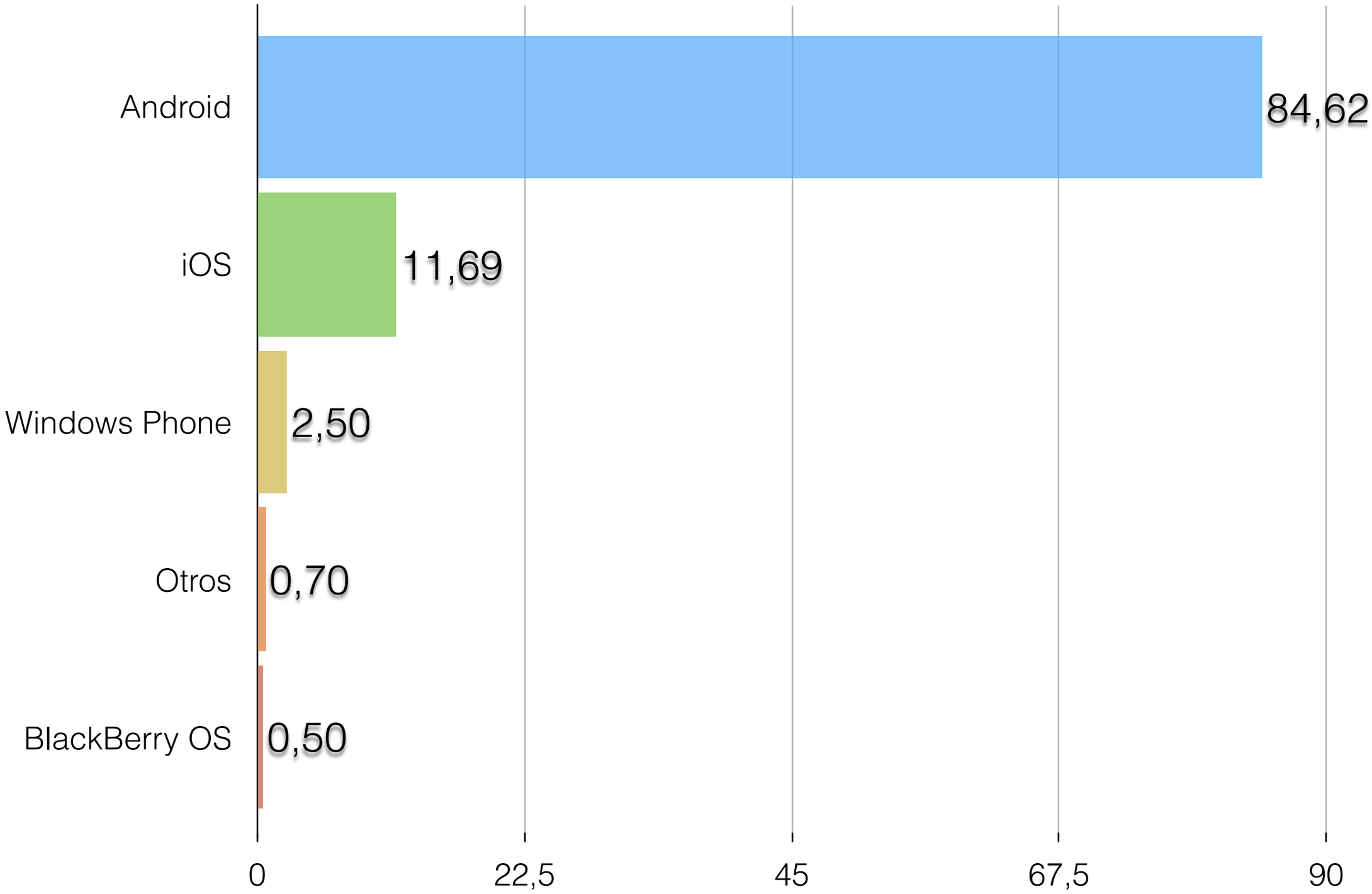
Android and Sandbox



Para romper las reglas

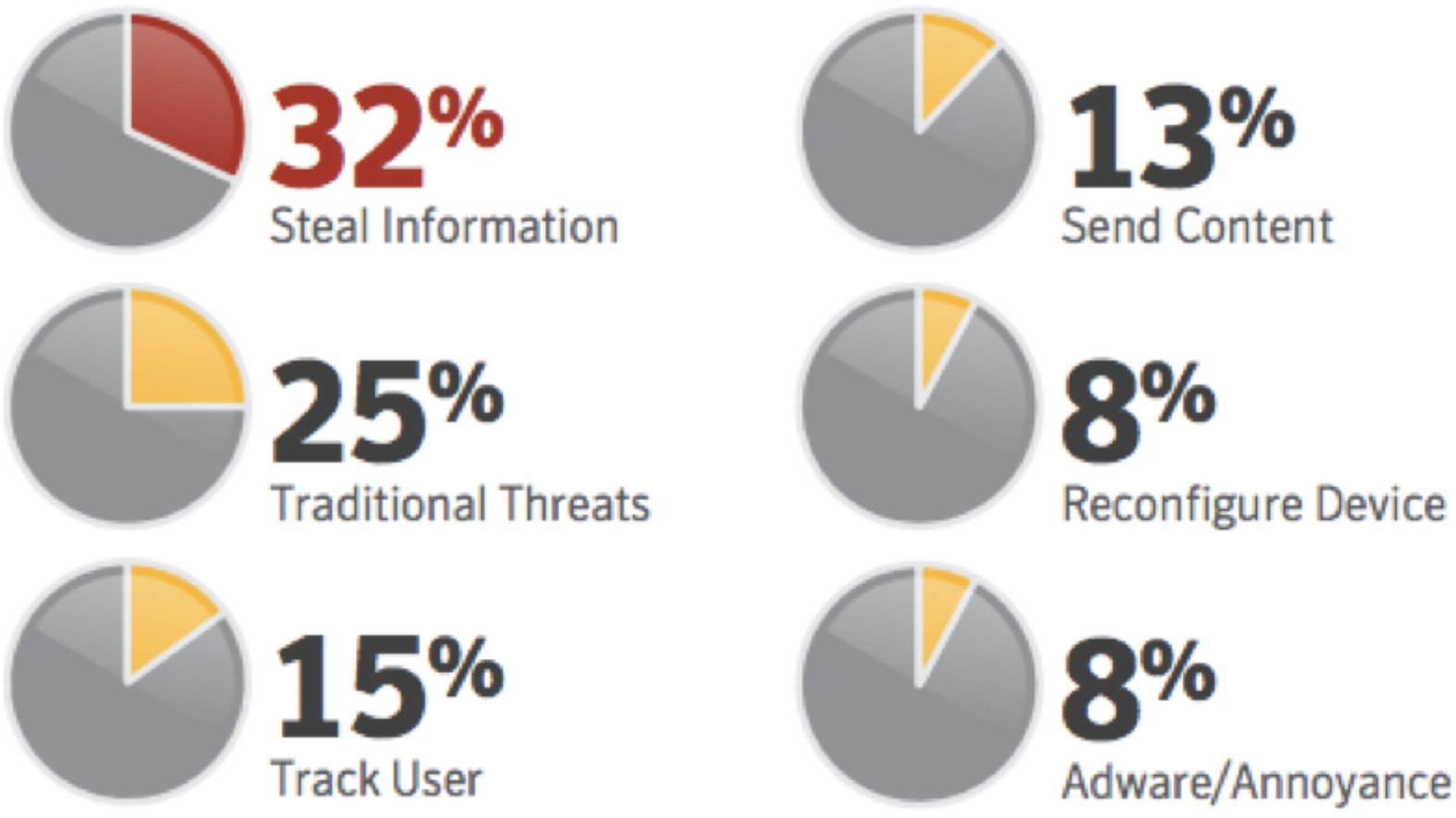
- iOS (jailbreaking):
  - escribir un exploit;
  - modificar el SO para permitir “otras” aplicaciones;
    - instalar “Cydia” para descargar aplicaciones extra;
    - difícil para la mayoría de usuarios
- Android (~~rooting~~):
  - permitir “fuentes desconocidas”
  - ¡hecho!

Distribución de SO



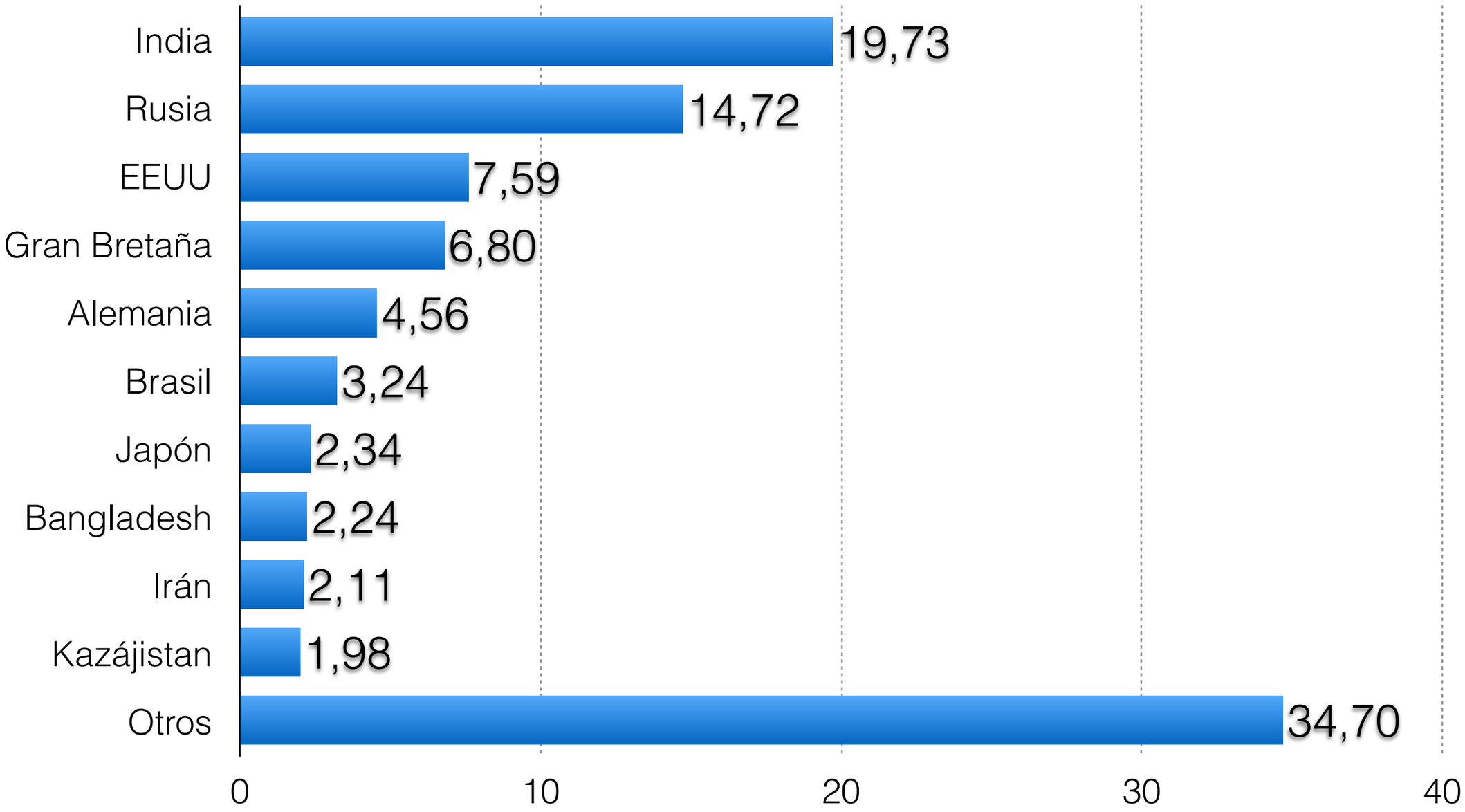
Mobile Threats In 2012

Source: Symantec

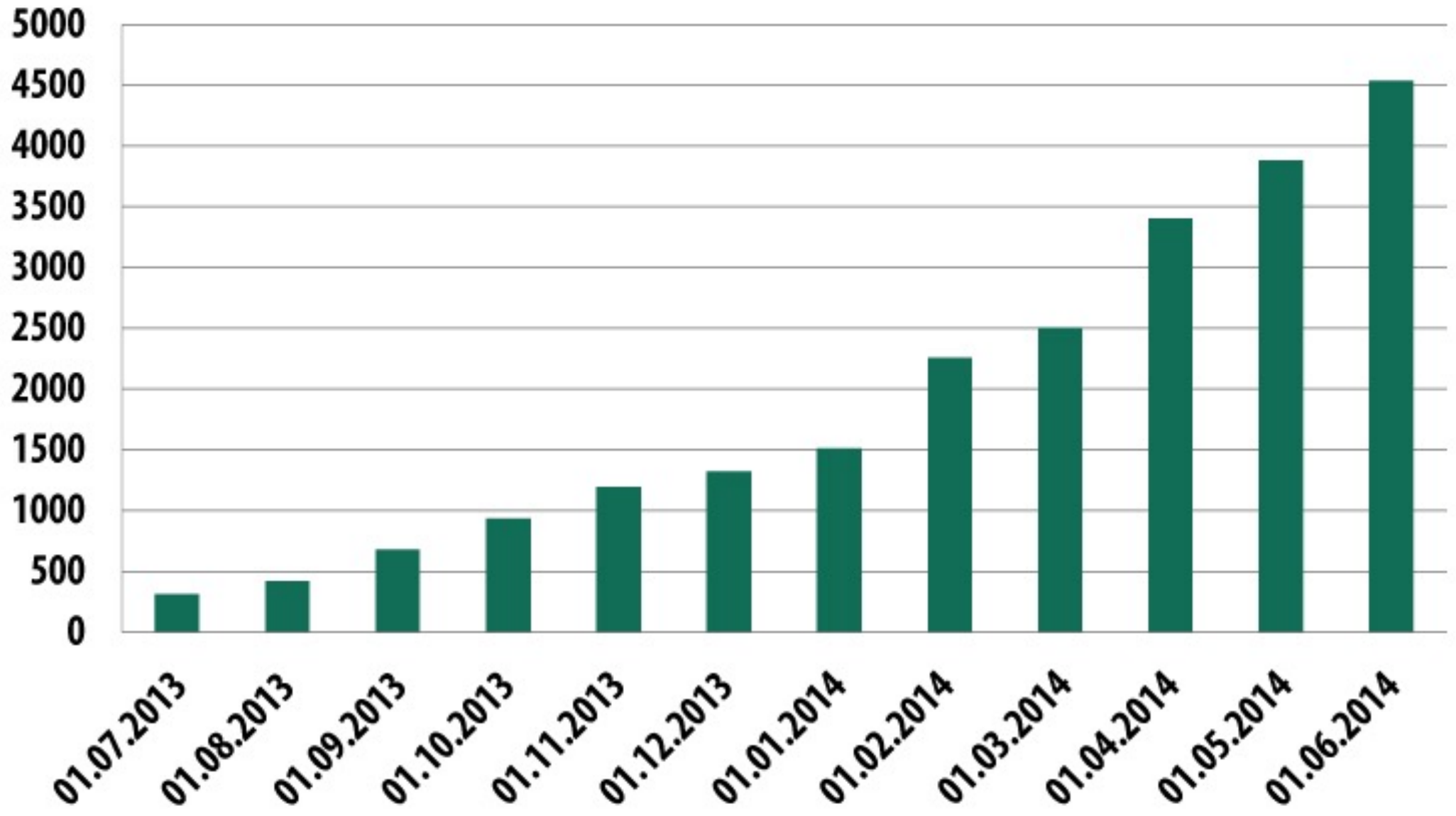


Information stealing tops the list of activities carried out by mobile malware, with 32 percent of all threats recording some sort of information in 2012.

Programas del clase Monitor



Trojanos tipo ¨Banking¨



"FBI"

Big brother is watching you!

Para acabar

- En junio de 2012 habían 45000 aplicaciones malware para móviles, en junio 2013- 270000 (según la información de Jupiter Networks), hoy en día aparecen 2500 programas nuevos **cada día**

- 92% de víruses son para Android (aunque tiene menos vulnerabilidades que iOS)