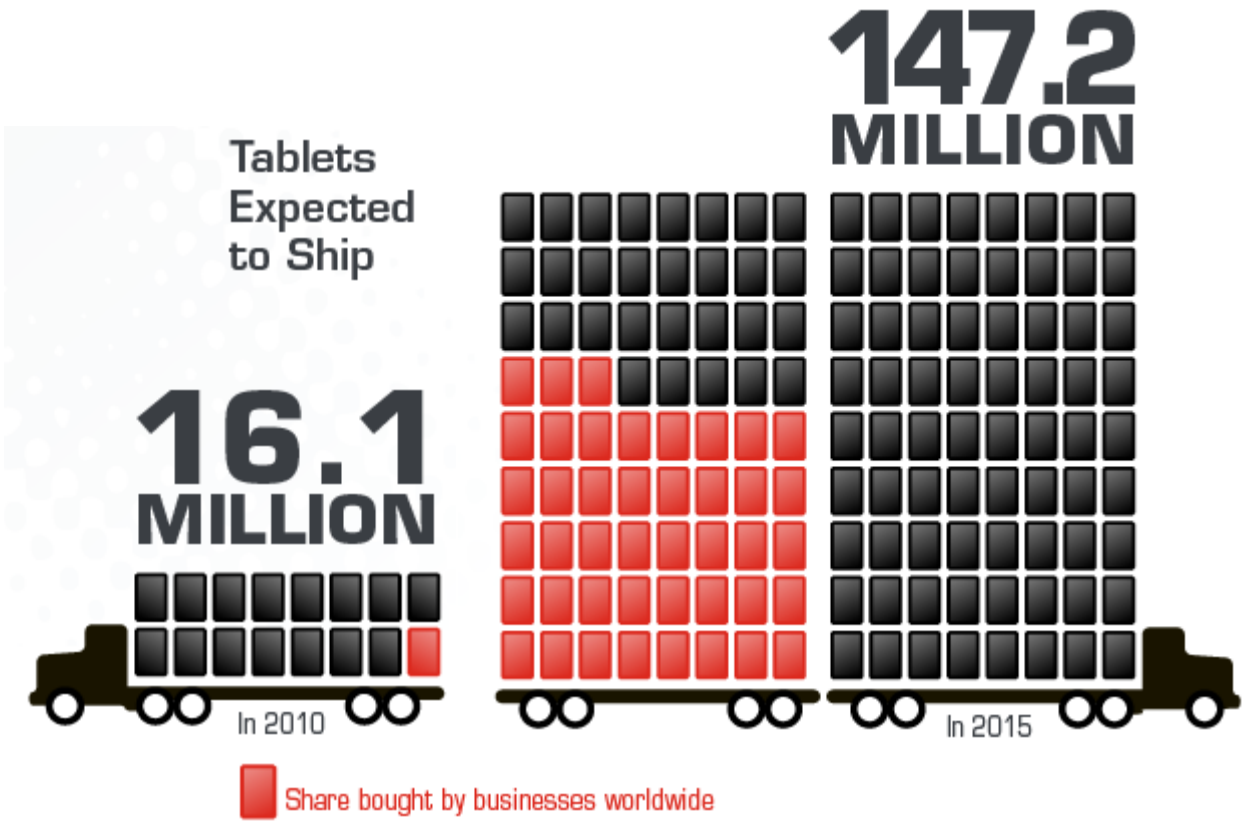
SOPHOS

Ibrahim Yusuf
Presales Engineer at Sophos
ibz@sophos.com

Smartphones and BYOD: what are the risks and how do you manage them?

Tablets on the rise



SOPHOS

Diverse

SOPHOS

The Changing Mobile World

Powerful devices

Access everywhere

Mixed ownership

User in charge

SOPHOS

Powerful devices

- Music player
- Calendar
- Internet
- Chat
- File store

- Personal email
- Company email
- Text messages
- Photos
- Banking

SOPHOS

Access everywhere

In the office

In the coffee shop

Whilst travelling

At home

SOPHOS

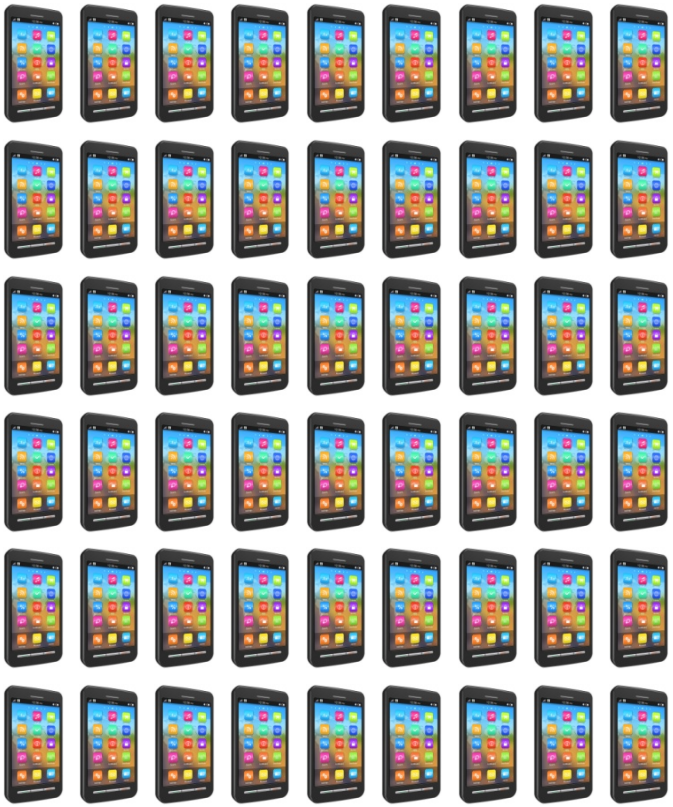
Paradigm shift

Threats remain the same, but they differ on each platform

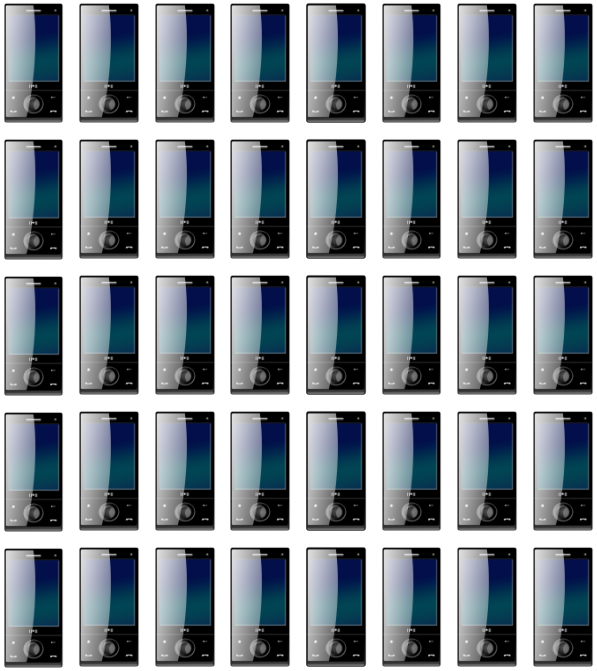
≠

Mixed ownership

Employee-owned devices



Corporate-owned devices



Analysts forecast a shift in ownership over the next 3 to 5 years

The user as the administrator

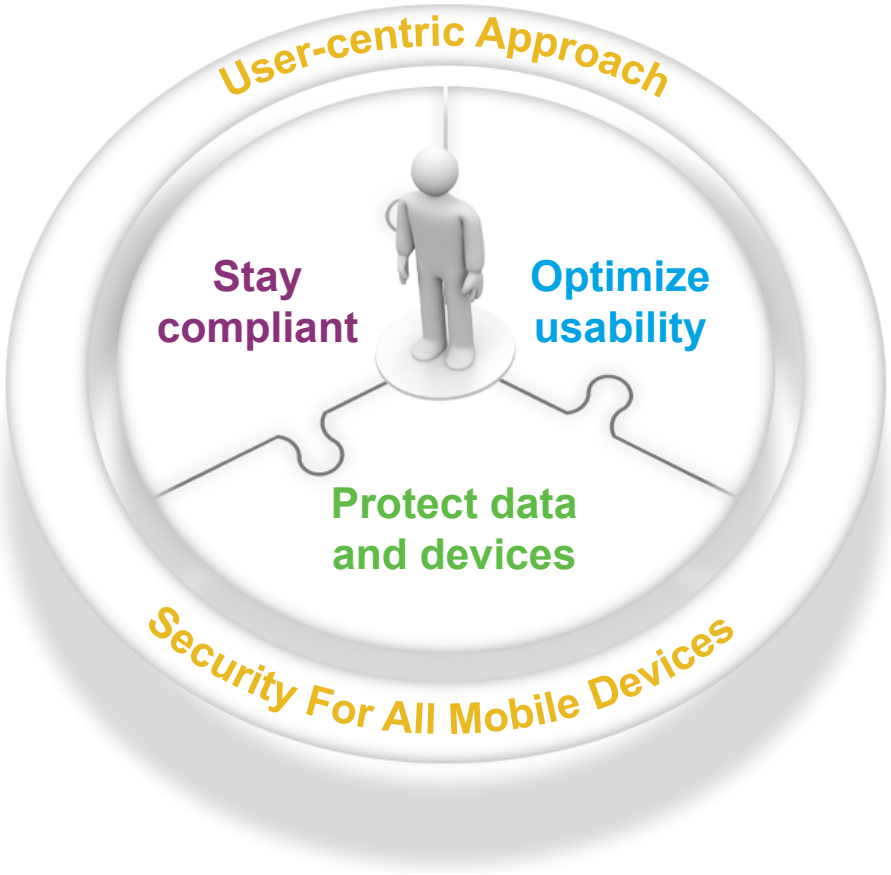
59% Say employees circumvent or disengage security features such as password and key lock

51% Have experienced data loss in the last 12 months due to insecure mobile devices

76% Believe mobile devices put their organization at risk but many do not have the controls (39%) or enforceable policies (45%) to reduce this risk

Source: Ponemon Institue, Global Study on Mobility Risks, February 2012

IT Security Challenges



SOPHOS

For the bad guys

Valuable information straight from your mobile

SOPHOS

For the bad guys

Threats remain the same, there are new ways to get closer to your money

=

SOPHOS

Risk through

The jailbreaking/rooting community are masters at exploiting undisclosed vulnerabilities

Attacks

Malware though rogue Apps

- Mobile malware disguised as fake online banking applications

Attacks

SMS fraud App (becoming more common)

- Intercepting banking authentication code

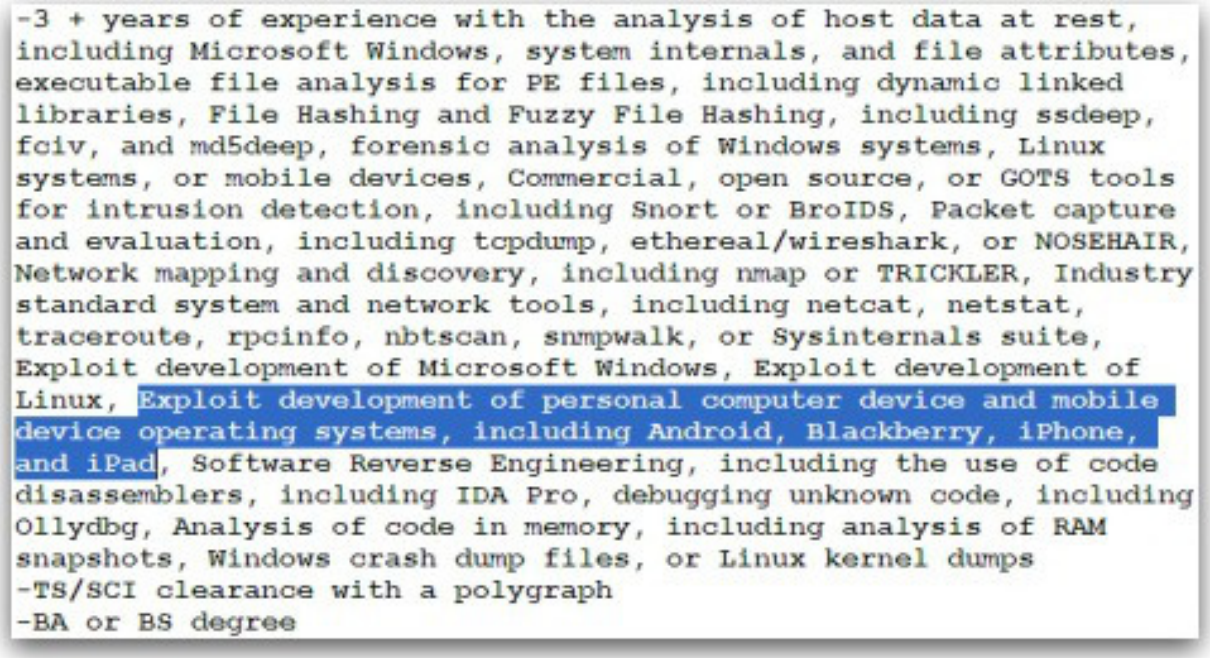
Attacks

SMC Messaging attack

- text-messaging attacks (also becoming more common)

Attacks

Hobbyists is one thing, imagine what governments can do



-3 + years of experience with the analysis of host data at rest, including Microsoft Windows, system internals, and file attributes, executable file analysis for PE files, including dynamic linked libraries, File Hashing and Fuzzy File Hashing, including ssdeep, fciv, and md5deep, forensic analysis of Windows systems, Linux systems, or mobile devices, Commercial, open source, or GOTS tools for intrusion detection, including Snort or BroIDS, Packet capture and evaluation, including tcpdump, ethereal/wireshark, or NOSEHAIR, Network mapping and discovery, including nmap or TRICKLER, Industry standard system and network tools, including netcat, netstat, traceroute, rpcinfo, nbtscan, snmpwalk, or Sysinternals suite, Exploit development of Microsoft Windows, Exploit development of Linux, Exploit development of personal computer device and mobile device operating systems, including Android, Blackberry, iPhone, and iPad, Software Reverse Engineering, including the use of code disassemblers, including IDA Pro, debugging unknown code, including Ollydbg, Analysis of code in memory, including analysis of RAM snapshots, Windows crash dump files, or Linux kernel dumps
-TS/SCI clearance with a polygraph
-BA or BS degree

Threads

Top most detected malware

fake Opera app

FndNCII-A

BBridge-A

FndNCII-A.

PJApps-C

BatteryD-A.

Duh

Plankton malware.

DroidRt-A

Generic-S

BaseBridge

Opfake-C

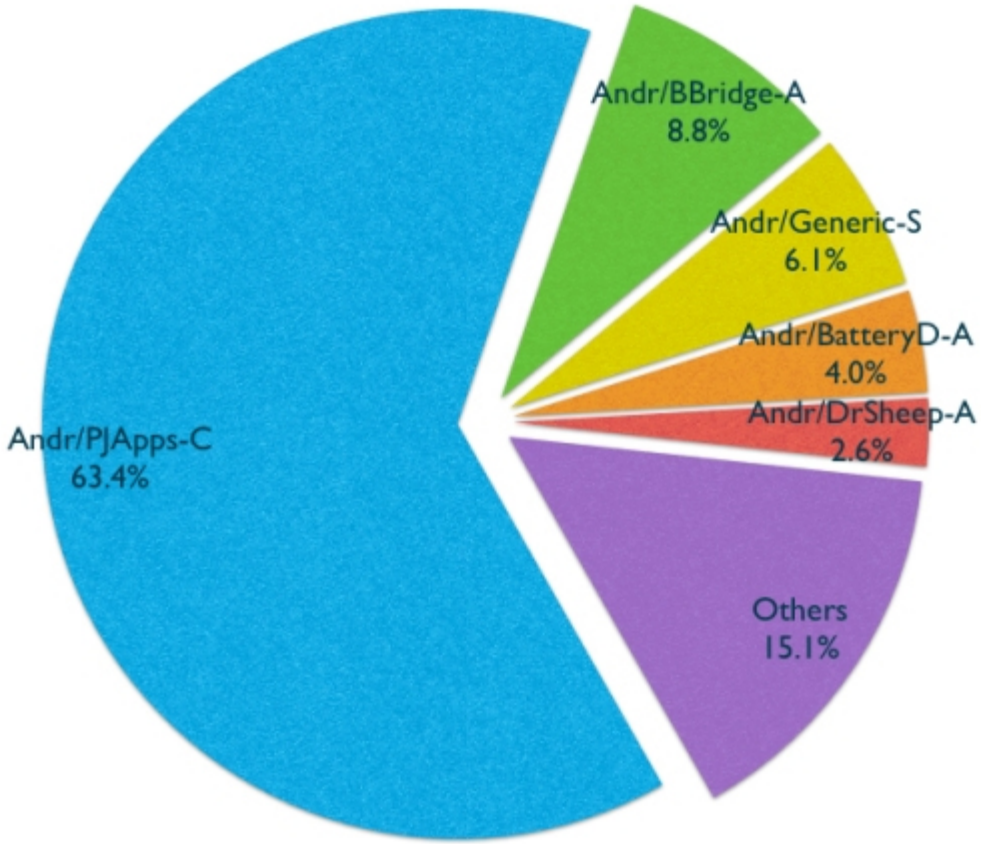
DrSheep-A

Generic-S

Ikee

Threads

Top most detected malware



Sophos: SophosLabs

SOPHOS

Inevitable

Inevitable, really?

Basics

Do the basic well…
and really really well

Do the basics well

- Develop an enterprise strategy for mobile security
- Create a comprehensive policy (including detailed guidelines) for all employees and contractors who use mobile devices in the workplace.
- Establish organizational accountability
- Launch awareness training for end-users (to reduce employee mistakes).

Do the basics well

- Use application control, patching and other controls to prevent hacking and surreptitious malware infections.
- Whenever feasible, use remote wipe, mobile device encryption and anti-theft technologies to reduce data breach risk.
- Understand emerging privacy issues inherent with mobile devices.

…you also nee the tools:

SOPHOS

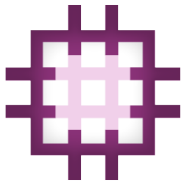
Mobile management approaches

Fat client	V	Lightweight agent
Sandboxes business access		Uses built-in capabilities and apps
Enables tight control		Manages the entire device
May create support challenges		May cause difficulties in segregating data

In summary

Password

Encryption



Patched

Current

Control, secure, protect

Sophos Mobile Control - Mobile Device Management
On-premise or cloud-based solution to manage, control and protect mobile devices.
Enable BYOD without the risks

Sophos Mobile Security – Anti-Virus for Android
Scans for malicious data-stealing apps and provides loss and theft protection. Free download ➔ ➔ ➔
Protect devices from Android malware

Sophos Mobile Encryption – Mobile Data Protection
Extends SafeGuard Encryption for Cloud Storage to mobile devices – iOS or Android*
Ensure persistent encryption

Android version available late September 2012

SOPHOS

Complete security

Everything you need to stay protected

- Anti-malware
- Firewall
- Intrusion prevention
- Device Control
- Application Control
- Access control
- Endpoint Web Protection
- Encryption
- Patch Manager
- Data Control
- Virtualization

- Anti-malware
- Malicious URL Filtering
- Productivity Filtering
- Anonymizing Proxy blocking
- Content control
- HTTPS Scanning

- Anti-malware
- Anti-spam
- Data Control
- Email encryption

- Disk Encryption
- File encryption
- Key management
- Device Control
- Data Control
- Encryption for cloud

- Anti-malware
- Mobile Control
- Mobile app security
- SOPHOS

- Unified Threat Management
- Secure branch offices
- WiFi security
- Web Application Firewall
- Email archiving

SOPHOS

Ibrahim Yusuf
Presales Engineer at Sophos
ibz@sophos.com

Thank you.

SOPHOS