Smartphone Security

Sam Camarda CCIE, CISSP

scamarda@cisco.com
Market Transitions

Mobility
1.3 Billion new Networked Mobile Devices in the Next Three Years

Workplace Experience
Blurring the Borders:
Consumer ↔ Workforce
Employee ↔ Partner

Video
YouTube was the start of the new video era

Mobile Devices
IT Resources

Anyone, Anything, Anywhere, Anytime
The Evolution of Security

Towards Network and Cloud Enforcement

- Network + Cloud
  - Thinner
- Network
  - More Sophisticated
- Endpoint
  - Richer, More Web

Clients
- Desktop
- Laptop

Threats
- Blaster
- Conficker
- Aurora

Apps
- YouTube
- Chat
- Facebook
Definition of endpoint has changed
  • Then – corporate owned desktop, laptop
  • Now – mobile phones, tablets, netbooks – often employee owned

New endpoint types break traditional EPP software model

Continued move on the endpoint to suites vs point products

AV vendors are shifting their focus to security services in the cloud

Changes in operating systems
  • Newer OS designed with security in mind (iPhone, Android)
  • Windows continues to embed security features
Challenges

- Difficult to completely secure mobile devices with Web-based malware distribution
- From communication devices to lifestyle centers
- Malware mimics typical applications behavior

Requirements
- Consistent security
- Consistent management
- Consistent visibility
Security Challenges with Mobile Devices

- “Enterprises receptive to IT consumerization, mobile devices accessing their networks
- But… smartphones, netbooks, iPads bring security risks
- Once business data makes its way onto employee's device, the enterprise can’t control its spread or usage”

Smartphone Threats for IT Managers

- Physical Loss
- Data Theft / Privacy Compromise
- Malware Vehicle
- Phishing / Text Attacks
- Virus / Trojan
Physical Loss

- Over a six-month period in 2006, Pointsec found that 8,701 mobile devices were left behind in taxis in the Washington-Baltimore area and 3,106 were left in cabs in the San Francisco-Oakland area. – New York Times April 3, 2007 Data Theft

- iPhone 4G Prototype
- Lack of unlock / password codes
- Manufacturer encryption optional
- Remote wipe is an add-on for most
Data Theft / Privacy Compromise

- Not the next generation botnet zombies
  - Low processing power, memory, limited battery life
  - Used to siphon information for further usage

- Application Downloads
  - Checked for stability, not necessarily for security
  - Apple has a tighter control. Sandbox format.
  - Droid09 – Pulled fake banking application
  - Permission to use internal information

- Poor user implementation
  - ikee – Targets jailbroke iPhones with Rick Astley photo

- Information is corporate centric and personal

- Used / Refurbished
Data Theft / Privacy Compromise

FlexiSPY Apple iPhone SpypHONE

- Read SMS, Call Logs, Emails & GPS Locations
- Spy Cell - Remote Bugging Device
- Call Intercept - Phone Tap
- Email Relay - Forward all Events to your Inbox
- Completely Undetectable
- 10-Day 100% Money Back Guarantee

FlexiSPY iPhone spyphone - Secretly captures events and sends to your secure web account

SUPPORTED PHONES
NEWS: 3GS now supported.

FLEXISPY IPHONE SPY PHONE COMES IN FOUR STRENGTHS

- Read SMS, Emails & GPS Locations
- Email Relay - Forward all Events to your Inbox
- Call records - linked to address book
- SIM change notification - find out new number
- Full remote control - via SMS commands
- Web based full text keyword searches
- Download reports in CSV, PDF & RTF formats
- Full remote control
- Remote uninstall

Any Computer connected to the Internet with a web browser

2G, 3G & 3GS iPhones
with operating systems 3.0, 3.0.1, 3.1 & 3.1.2

FLEXISPY PRO-X - This is our flagship iPhone spy phone which also allows you to intercept and listen to incoming and outgoing phone calls. Buy any of the FlexiSPY iPhone products and you can upgrade to PRO-X when it becomes available.
Malware Vehicle to Enterprise Networks

- Limited security applications or governance
- Spyware, malware
- Next generation USB flashdrive infection
- 802.11 connections as the transfer method
  - Internet and enterprise connections
  - Unprotected devices associate
- Synchronization
- Device specific connection filtration
- Jailbroke iPhones run software as root
Phishing / Text Attacks

- Complacency
- Phishing / Malicious web links
- Premium site dialing trickery
- Text and email are methods to control the device
- Small screen and fine print
Virus / Trojan

- As early as 2004 – Cabir
  Exploited Bluetooth vulnerability
- Trojans on MicroSD cards
  Samsung & Vodafone trojans infect PCs
- Applications that modify communications inline
  Rootkits
- Premium site dialing trickery
- Does not compete with Windows-based systems
  Not as large of a footprint
Protections for IT Managers

- Blacklisting / Quarantining
- Security Policy / Awareness
- Manufacturer built-ins
- Security Applications
- Secure Communications
- Regulations
Blacklisting / Quarantining

- Draconian
- Confiscate
- Network filters by firmware address
- Endpoint protections
  - Disable synchronization capability
- NAC/VPN Connectivity
Manufacturer Built-ins

- Unlike Windows devices, most Smartphones have been built with security in mind
  - Still have direct access to the Internet
- Aforementioned features
- Download latest companion software
- APIs
- Secure Bluetooth
Security Applications

- Delicate balance
  Protection vs. battery life
- Disable application download
- Traditional endpoint security vendors moving into the Smartphone space
  Symantec, Trend, McAfee, etc.
- Encryption
  TrueCrypt, BitLocker, PGP
- Management – status, health, disposition
  Zenprise, Boxtone
- VPN
Regulations

- Government catching on
- State of Mass recently passed a law requiring Smartphone users to encrypt phone data if it contains personal information
- PCI and other audits beginning to include mobile devices
Questions?