Mobile Malware

Daniel McGrath

Paige Fenwick

Agenda

- Introduction
- Mobile Devices and Business World
- Malware
- Top Three Types that affect devices
- Threats to IT infrastructure domains
- Overview of solutions
- Enterprise App Store
- Conclusion

Mobile Devices and Business Environment

- 1 in every 5 individuals own a smartphone
- 1 in every 17 individuals own a tablet
- Changing how companies manage:
  - Employees- can connect to employees anytime and anywhere
  - Resources- can manage databases and access network applications from home
  - Information- can update and edit information while working in the field and away from the office setting
  - Spending- manage how resources are allocated throughout a company

Average Company Issued Devices

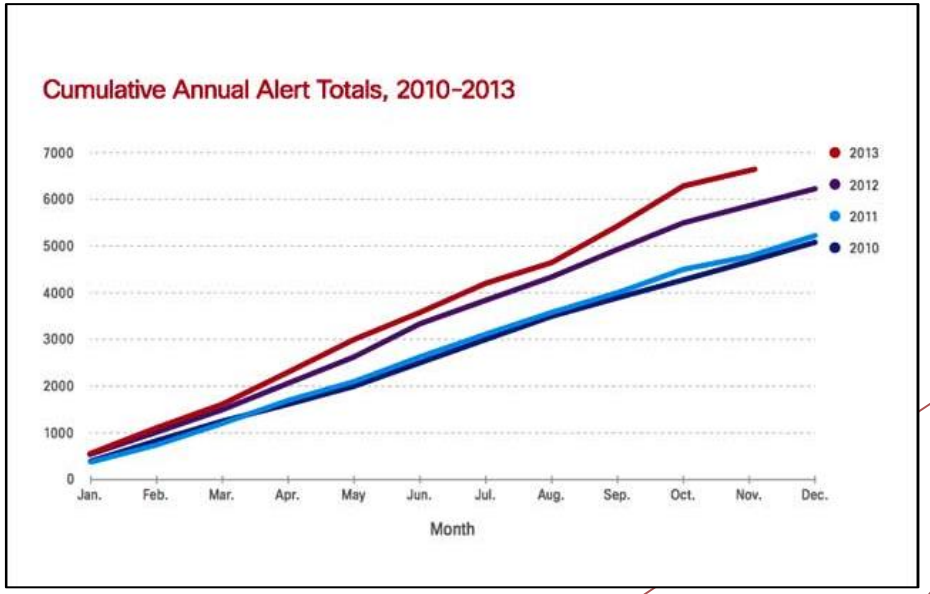
- iPhone 5 and iPhone 6 are the most distributed device within organizations
- Android's are the next most distributed
- iPads are issued mostly to employees who travel often, such as field workers
- Average storage capacity: 8-16 GBS
- Standard usages:
  - Email- takes up the most storage for company issued phones
  - Applications- many are created specifically for company usage
  - VPN- Virtual Private Networks, this is how mobile devices connect to company networks, also can work as an application

Mobile Threats

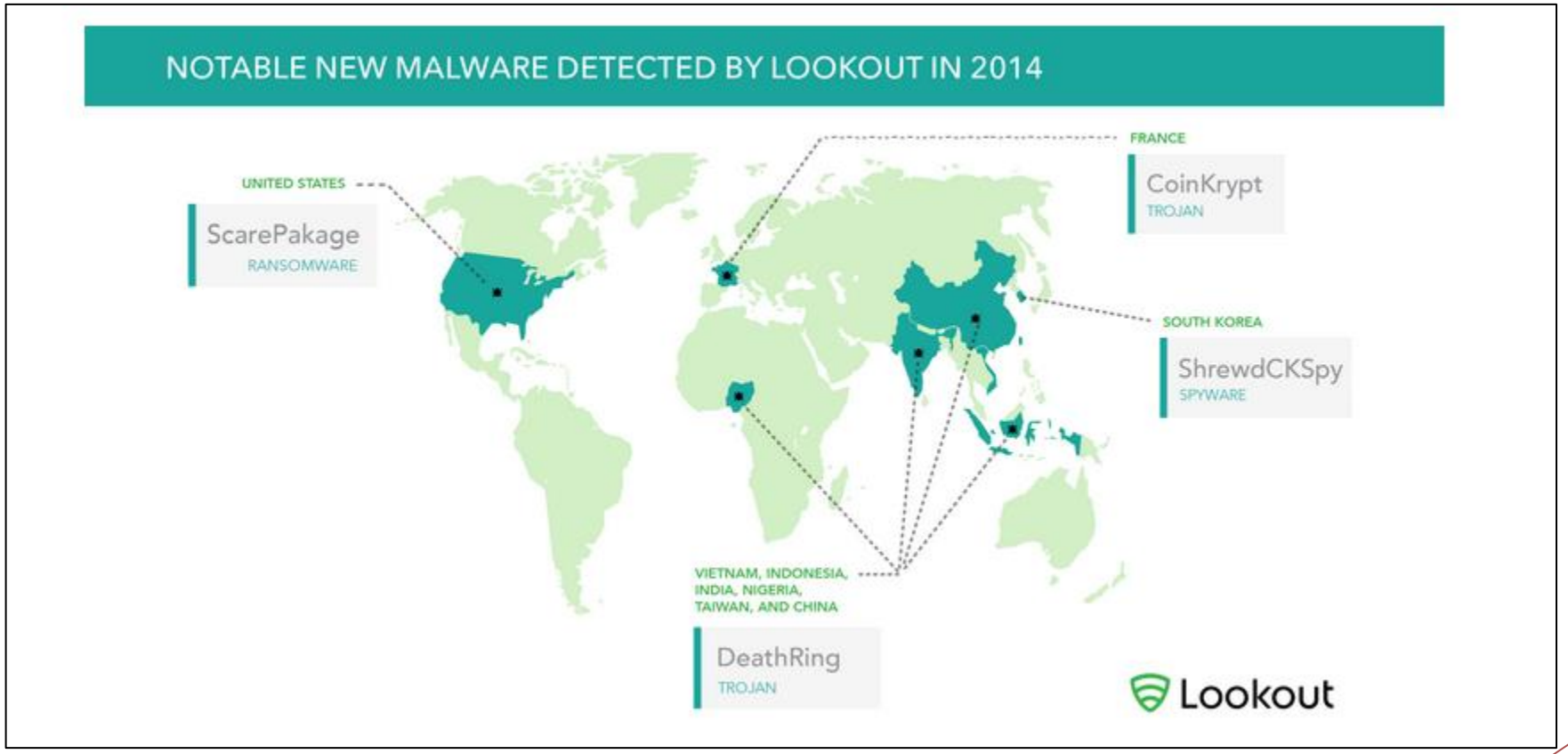
- 3.1 Million devices stolen in 2013 and that number rises every year
- Most devices were left in public places and then taken by the individuals who find it
- Company-issued devices have access to sensitive information through VPNs- this information can include passwords, company secrets and other private data
- Non-company issued devices:
  - Cannot be monitored similarly to company-issued,
  - Security and Service Desk employees cannot remote into devices
  - Easily compromisable

Mobile Malware

- Malicious software- this is harmful code that can perform activities such as spying on data movements, stealing passwords and locking users out of devices
- New malware targets mobile devices and their vulnerabilities
- Grew 75% in 2014- as mobile devices grow within companies so do the attacks on them
- Top three most common types:
  - Ransomware
  - Trojan horses
  - Spyware



Mobile Malware



Graph produced by Lookout.com

Three Common Types

- Ransomware
  - Disguise as application updates
  - Quietly installs in background
  - Locks phone-displays text message requesting payment
- Trojan Horses
  - Disguise as application update
  - Silently steals information
- Spyware
  - Disguise as application and application updates
  - Records information; phone calls, banking information, etc.

3 Infrastructure Domains

- Remote Access Domain- connects mobile devices to the network
  - Most vulnerable- BYOB devices pose the biggest threat
  - BYOD cannot be easily monitored- these devices have the most vulnerabilities to a network
- WAN Domain- connects secondary locations to the network
  - Connects devices from multiple locations
  - Similar risks associated as remote access, especially when BYOD are involved
- Systems/Applications- holds all the critical applications and data
  - Mobile devices have access to systems and apps
  - Can infect systems with malware
  - Applications can be destroyed and locked

How do mobile devices become infected with mobile malware?

- User error- employees do not follow the security policies or simple do not know of the vulnerabilities of mobile devices
- Downloading applications from untrustworthy sites- there is always a risk with downloading
- Updating applications- there is always a risk with updating applications
- Spam through emails- this is one of the most well traveled ways malware infects applications

General Solutions

- Inform users & customers about mobile risk: explain to users and customers that mobile devices are like computers so they should be protected like one. General rule of thumb: “if an app is asking for more than what it needs to do its job, you shouldn’t install it.” (Sophos Ltd.)
- Consider the security of Wi-Fi to access company data: Wi-Fi is insecure, so you must be cautious. Implement acceptable use policies, require users to connect through VPN tunnels.
- Prevent jailbreaking: By jailbreaking your phone, you are essentially removing the security controls and limitations created by the operating system vendor. This opens the door to all sorts of threats.

General Solutions Cont.

- Keep operating systems up to date: By simply keeping your phone updated, you are reducing the likelihood that your phone will be infected with mobile malware.
- Encrypt your device: By simply setting a strong password for your device you are protecting your phone more so than if your phone didn’t have a password.
- Install apps from TRUSTED sources: Google Play and Apple App Store. These app stores have policies and safeguards in place about who can have apps in their store. This is a good first line of defense.
- Encourage users and customers to install anti-malware on their mobile device: the risk is highest for Android devices, so it is important for Android users to install anti-malware. Anti-malware is currently not supported on iOS and Blackberry devices.

The Main Solution- An Enterprise App Store

- Formally defined by About.com as: “an online app store which enables companies to securely supervise and regulate the licensing, distribution and management of certain mobile apps to its employees.”

The Main Solution- An Enterprise App Store

- This enables companies to more closely monitor and regulate what their employees are downloading and using on their personal mobile device.
- Helps with the overall security of the company or organization.
- Compatible with today's mobile devices.

An Enterprise App Store- How will this help?

- About control and security.
- An EAP can have its own apps that are developed by an in-house development team.
- This ensures that employees are only using apps that the company created and developed which allows for more control and security

An Enterprise App Store- How is it implemented?

- Two ways:
  - 1.) In-house mobile development team
    - Better for bigger companies
  - 2.) Outsource creation to one of the many vendors currently creating enterprise app stores.
    - Cisco, McAfee, Apperian.
    - Better for smaller companies

Conclusion

- Mobile devices in business environment
- Main types of mobile malware
- Threats to IT infrastructure
- Overview of solutions
- Enterprise App Store