Mobile Security

Fall 2015

Patrick Tague

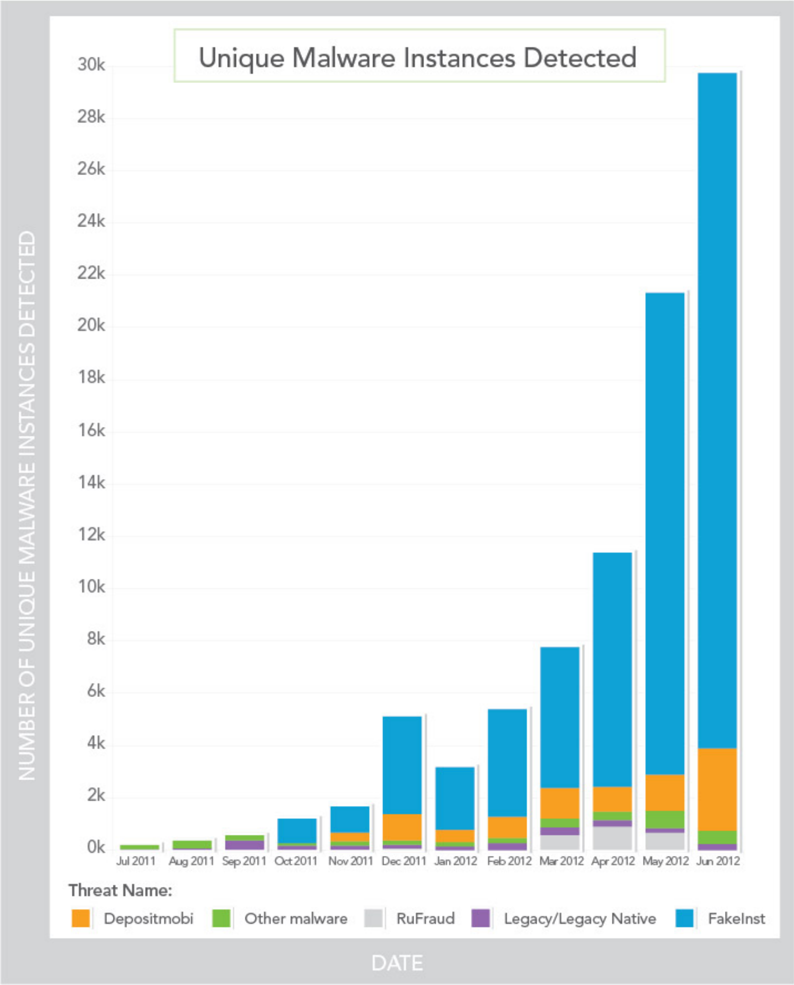
#12: Mobile Malware

[Some slides c/o Tim Vidas, slightly modified]

Class #12

- What is mobile malware?
- What makes malware different in mobile?
- Several mobile malware examples

Malware Growth



Source: Lookout State of Mobile Security 2012
https://www.lookout.com/resources/reports/state-of-mobile-security-2012

- Explosive growth in mobile malware
  - Ubiquity of smartphones
  - Growing attacker incentives
- Unique opportunities
  - Revenue opportunities
  - Sensitive personal data
- Malware growth
  - Exponential growth in unique samples
  - Skewed towards relatively few malware families

What is malware?

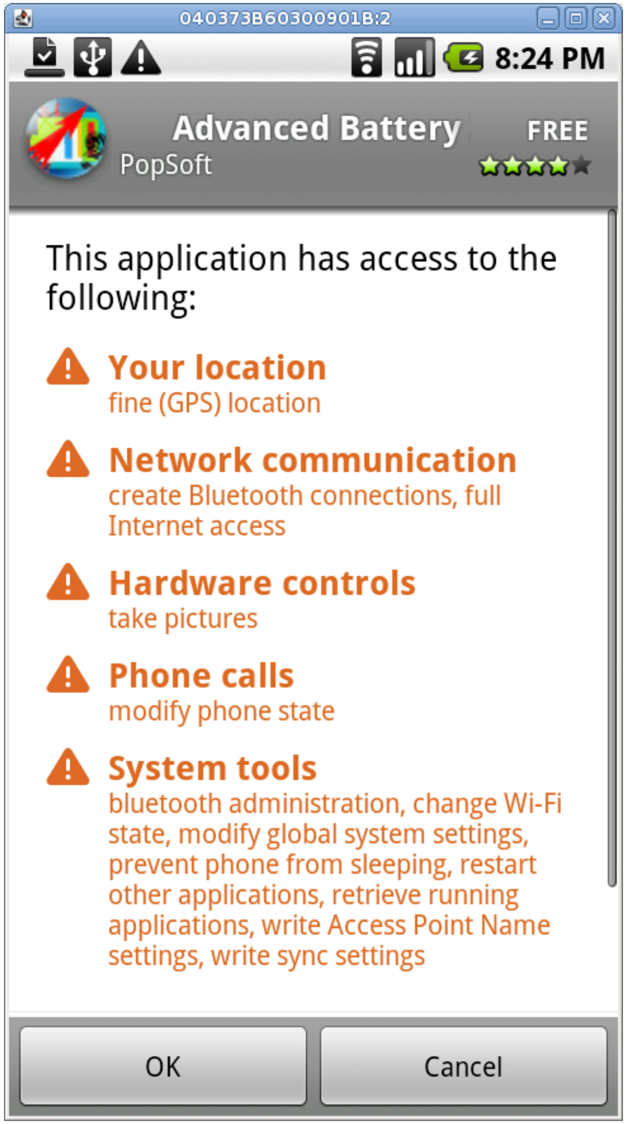
- Software with malicious intent
- Common malicious activities [Felt 2011]
  - Collecting user information; Theft of credentials
  - Sending premium-rate SMS/calls (Toll Fraud)
  - Sending spam emails
  - Remote Access Trojans
  - SEO fraud (click-jacking, ad-jacking)
  - Ransomware
  - “drive bys” (sort of)
- Auxiliary features
  - Spreading to other smartphones
  - Evading detection
  - Command-and-control

Android Permissions

- Label for mediating access to controlled resource
- More than 100 built-in permissions
  - Control sensitive phone resources
  - CALL_PHONE, CAMERA, INTERNET, WRITE_SMS, READ_INPUT_STATE, etc.
  - Package signing used to control some permissions
- Mandatory Access Control
  - Permissions declared and requested at install-time
  - Users must grant or deny all requested permissions

Dangerous Permission Combos

- SMS when not needed
  - Toll fraud
- READ_LOGS supersedes many permissions
- INTERNET and READ_CONTACTS
- INTERNET and INSTALL_PACKAGES
- INTERNET and ALMOST_EVERYTHING
- Unfortunately many free apps require network so ads can be retrieved



This application has access to the following:

Your location
fine (GPS) location

Network communication
create Bluetooth connections, full Internet access

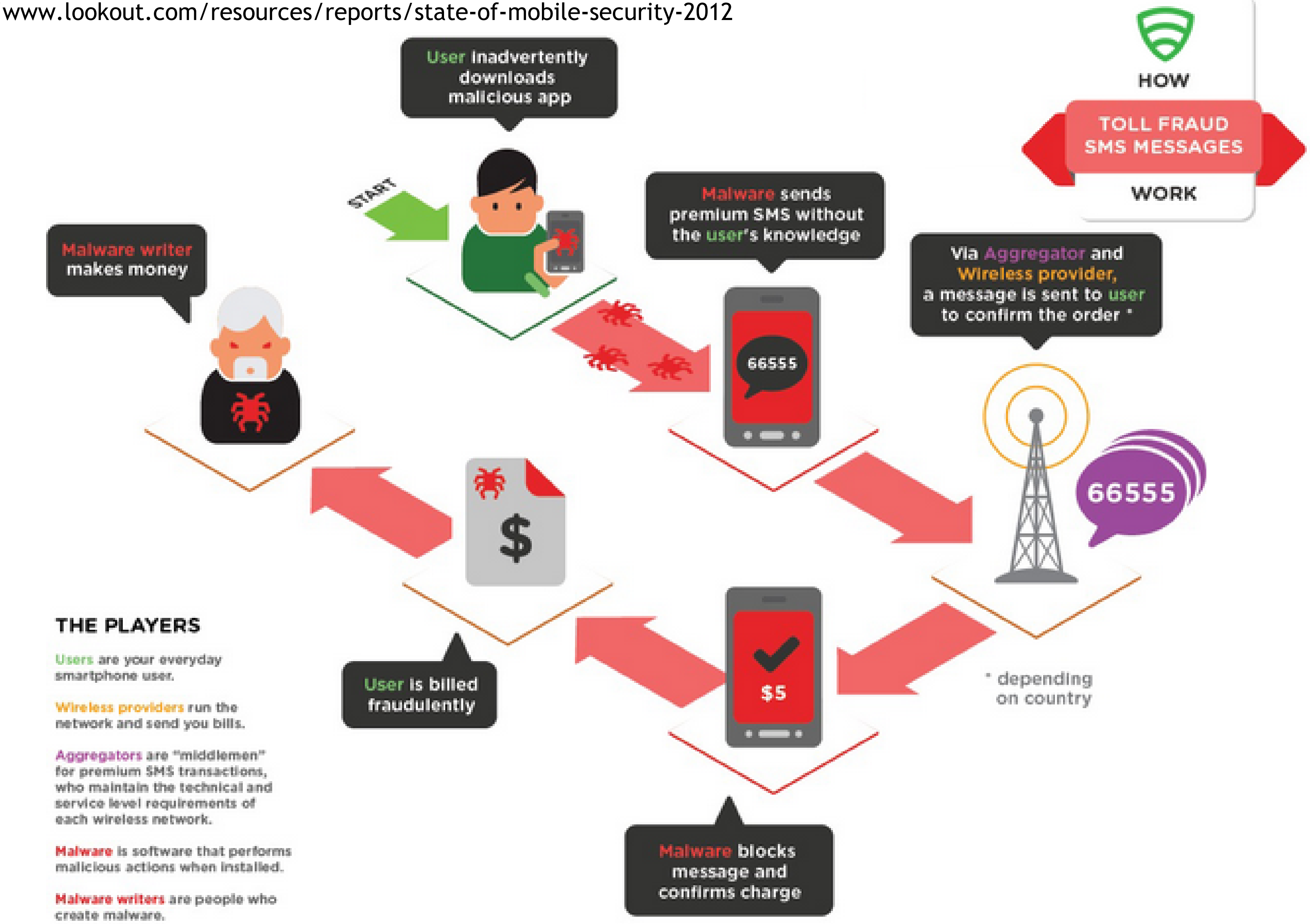
Hardware controls
take pictures

Phone calls
modify phone state

System tools
bluetooth administration, change Wi-Fi state, modify global system settings, prevent phone from sleeping, restart other applications, retrieve running applications, write Access Point Name settings, write sync settings

Toll Fraud

Source: Lookout State of Mobile Security 2012
https://www.lookout.com/resources/reports/state-of-mobile-security-2012



User inadvertently downloads malicious app

Malware sends premium SMS without the user's knowledge

Via Aggregator and Wireless provider, a message is sent to user to confirm the order *

Malware blocks message and confirms charge

User is billed fraudulently

Malware writer makes money

* depending on country

THE PLAYERS

Users are your everyday smartphone user.

Wireless providers run the network and send you bills.

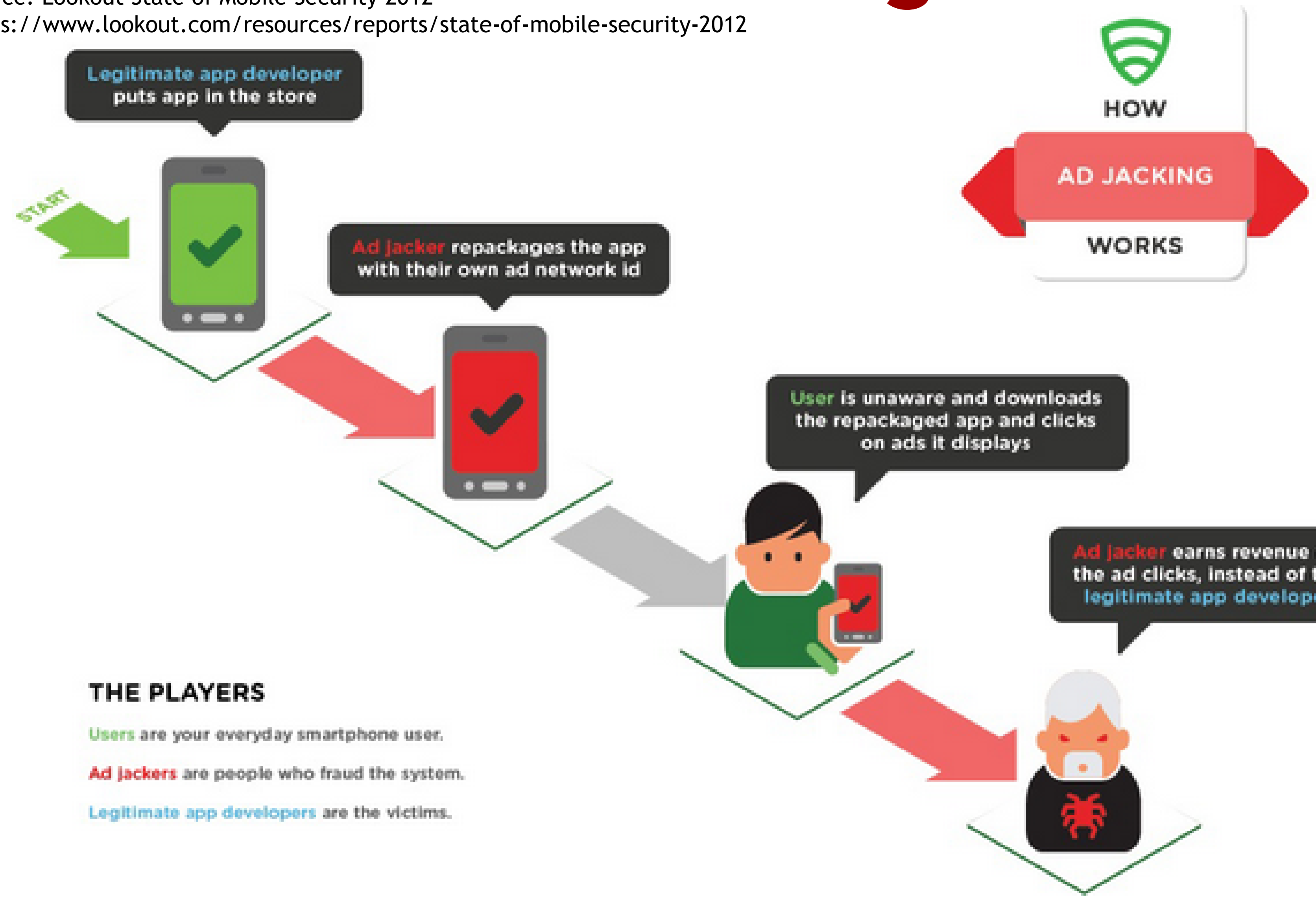
Aggregators are "middlemen" for premium SMS transactions, who maintain the technical and service level requirements of each wireless network.

Malware is software that performs malicious actions when installed.

Malware writers are people who create malware.

Ad Jacking

Source: Lookout State of Mobile Security 2012
https://www.lookout.com/resources/reports/state-of-mobile-security-2012



Legitimate app developer puts app in the store

Ad jacker repackages the app with their own ad network id

User is unaware and downloads the repackaged app and clicks on ads it displays

Ad jacker earns revenue for the ad clicks, instead of the legitimate app developer

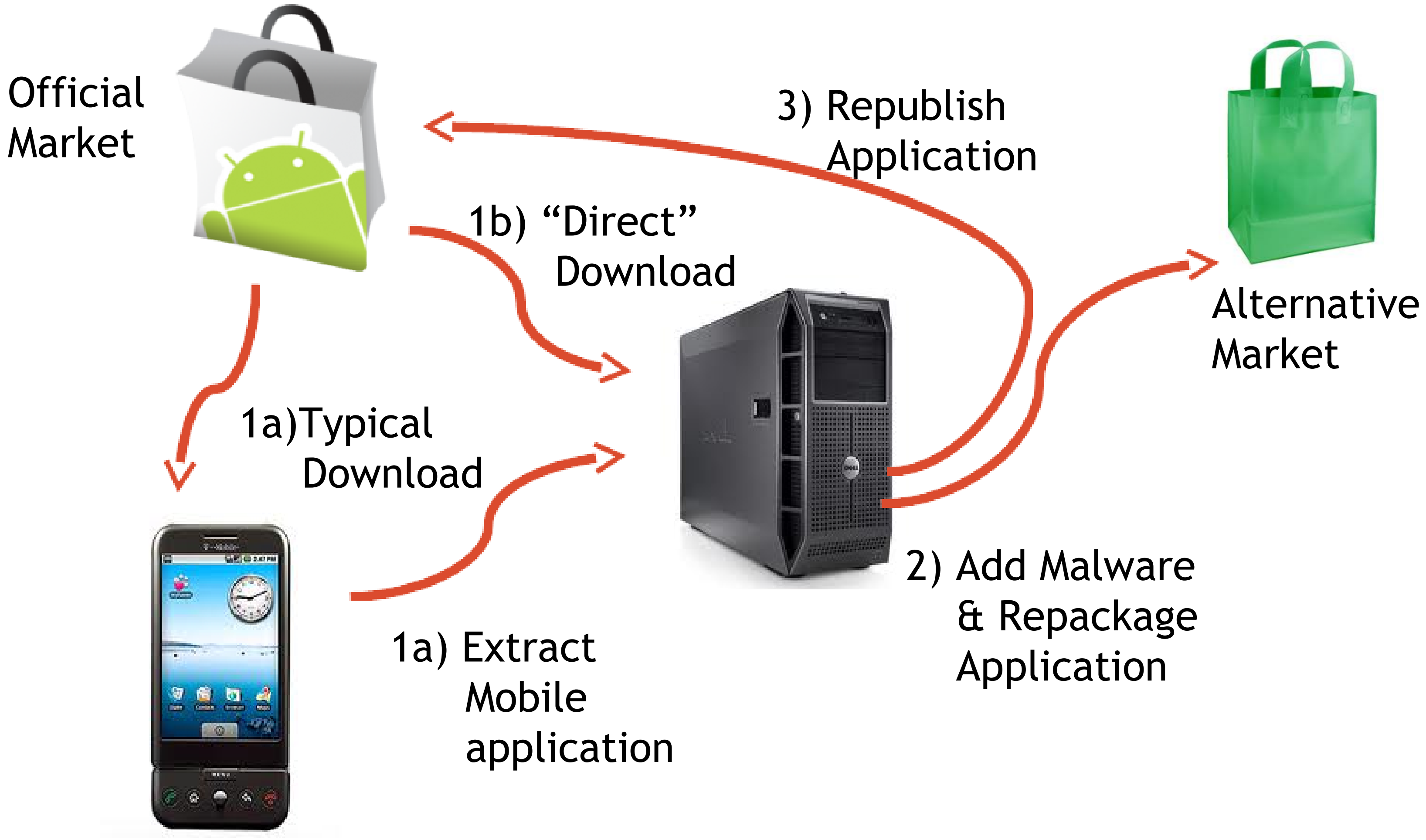
THE PLAYERS

Users are your everyday smartphone user.

Ad jackers are people who fraud the system.

Legitimate app developers are the victims.

Application Repackaging



Official Market

3) Republish Application

1b) "Direct" Download

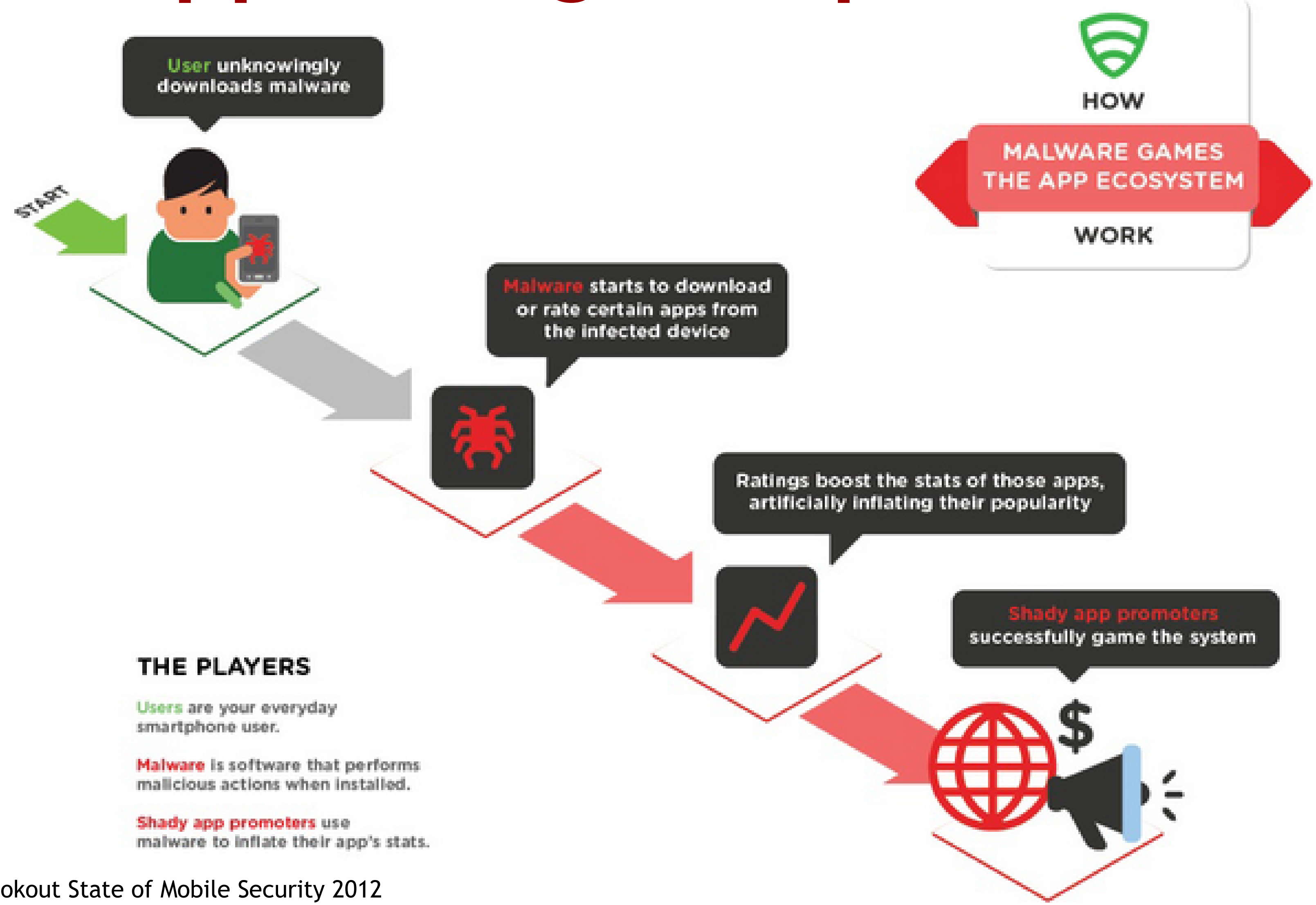
Alternative Market

1a)Typical Download

2) Add Malware & Repackage Application

1a) Extract Mobile application

App Rating Manipulation



User unknowingly downloads malware

Malware starts to download or rate certain apps from the infected device

Ratings boost the stats of those apps, artificially inflating their popularity

Shady app promoters successfully game the system

THE PLAYERS

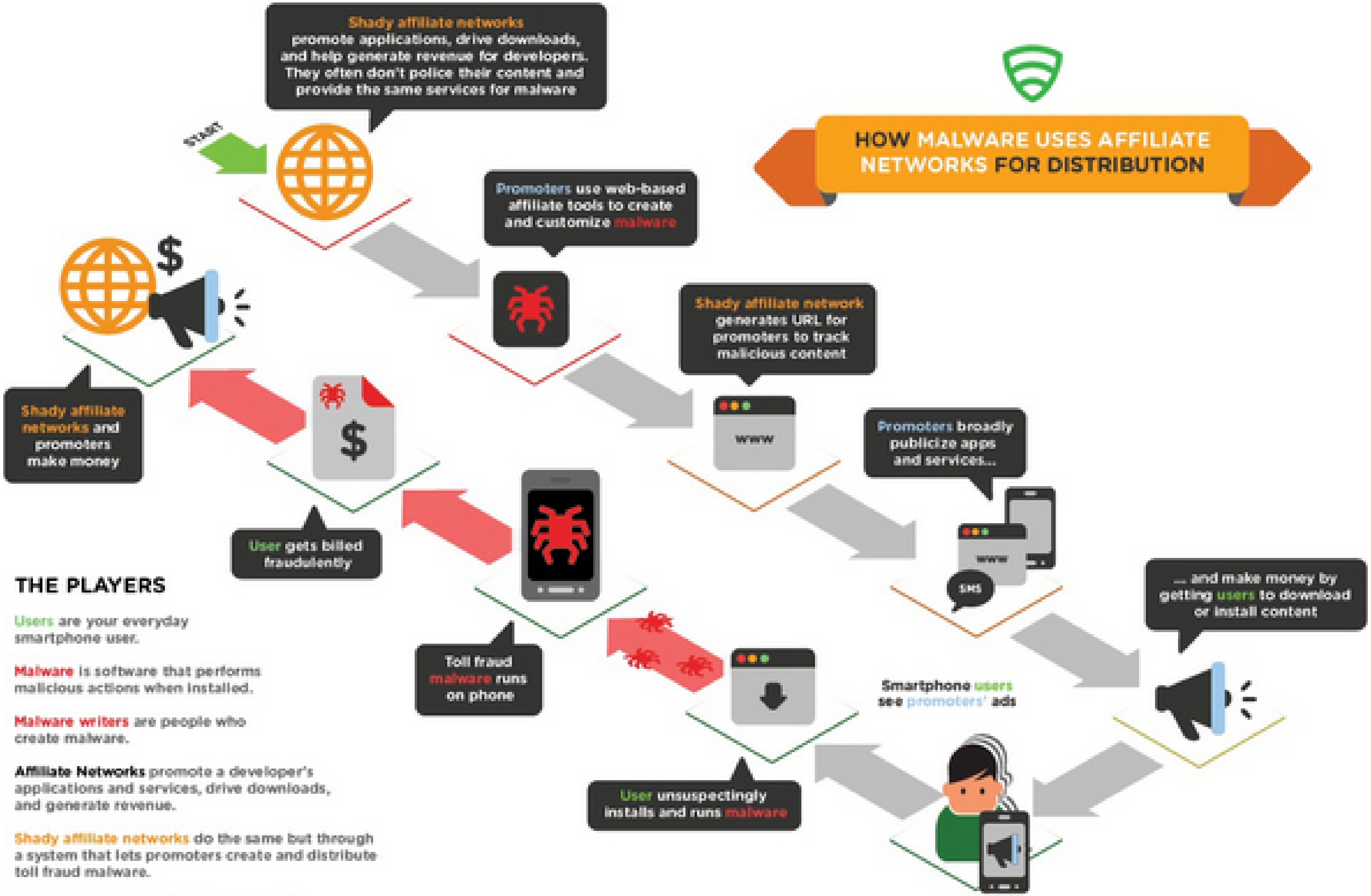
Users are your everyday smartphone user.

Malware is software that performs malicious actions when installed.

Shady app promoters use malware to inflate their app's stats.

Source: Lookout State of Mobile Security 2012
https://www.lookout.com/resources/reports/state-of-mobile-security-2012

Malware Distribution Networks



HOW MALWARE USES AFFILIATE NETWORKS FOR DISTRIBUTION

Shady affiliate networks promote applications, drive downloads, and help generate revenue for developers. They often don't police their content and provide the same services for malware

Promoters use web-based affiliate tools to create and customize malware

Shady affiliate network generates URL for promoters to track malicious content

Promoters broadly publicize apps and services...

... and make money by getting users to download or install content

Smartphone users see promoters' ads

User unsuspectingly installs and runs malware

Toll fraud malware runs on phone

User gets billed fraudulently

Shady affiliate networks and promoters make money

THE PLAYERS

Users are your everyday smartphone user.

Malware is software that performs malicious actions when installed.

Malware writers are people who create malware.

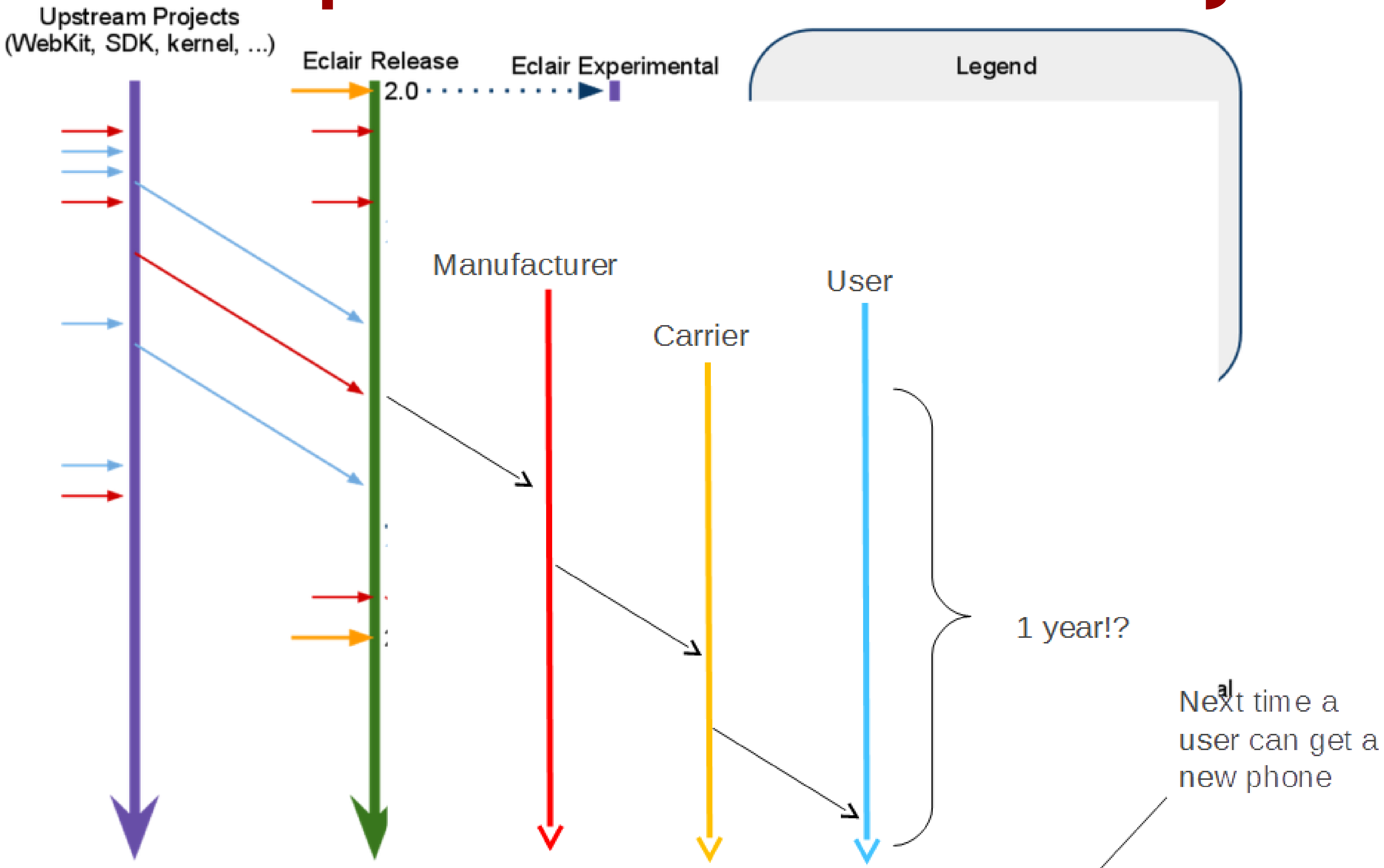
Affiliate Networks promote a developer's applications and services, drive downloads, and generate revenue.

Shady affiliate networks do the same but through a system that lets promoters create and distribute toll fraud malware.

Promoters broadly publicize apps and services and make money by getting users to install the content.

Source: Lookout State of Mobile Security 2012
https://www.lookout.com/resources/reports/state-of-mobile-security-2012

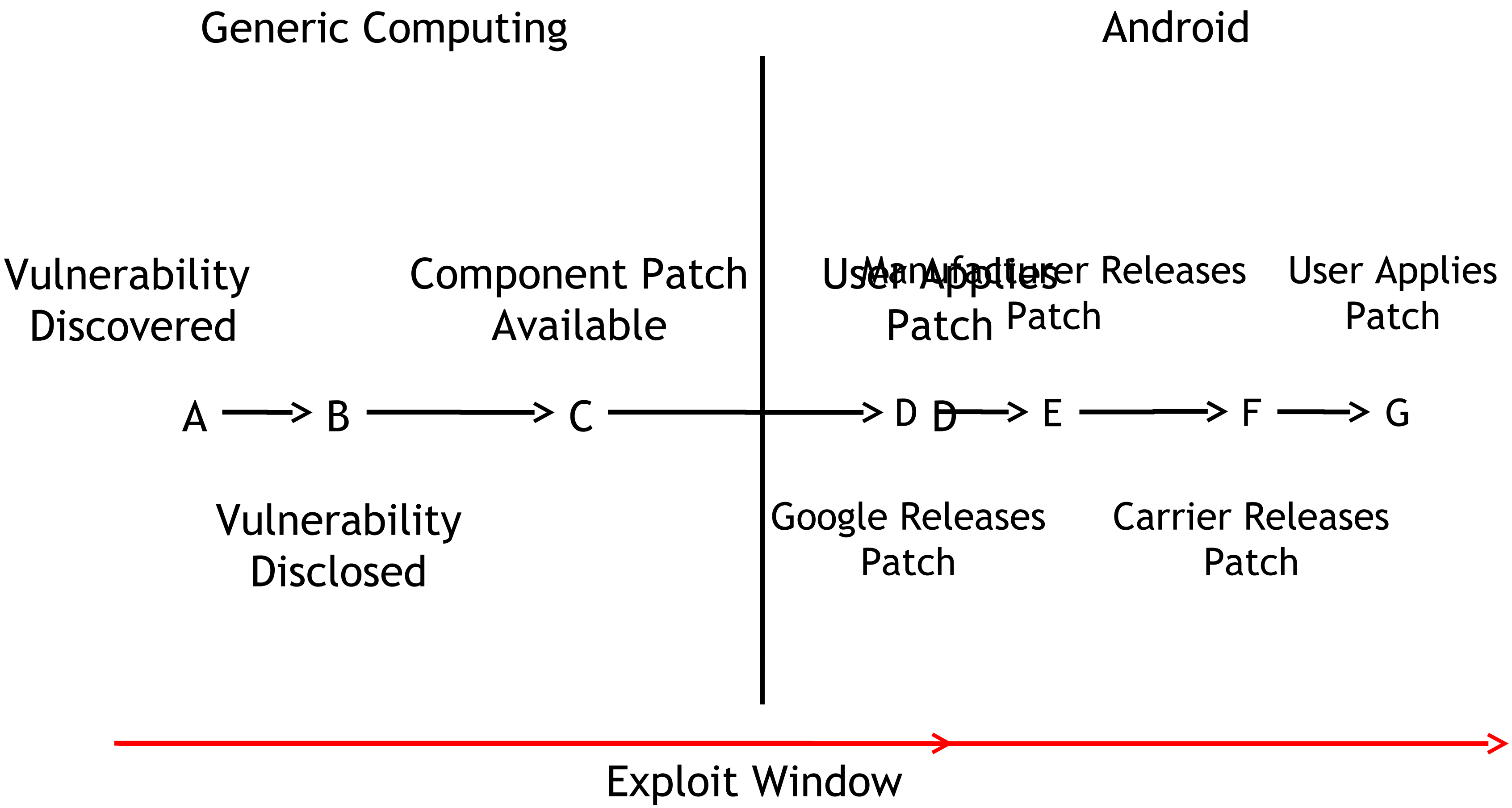
Smartphone Software Lifecycle



1 year!?

Next time a user can get a new phone

Big Problem: Updates



Generic Computing

Android

Vulnerability Discovered

Component Patch Available

User Applies Patch

Manufacturer Releases Patch

User Applies Patch

A → B → C → D D → E → F → G

Vulnerability Disclosed

Google Releases Patch

Carrier Releases Patch

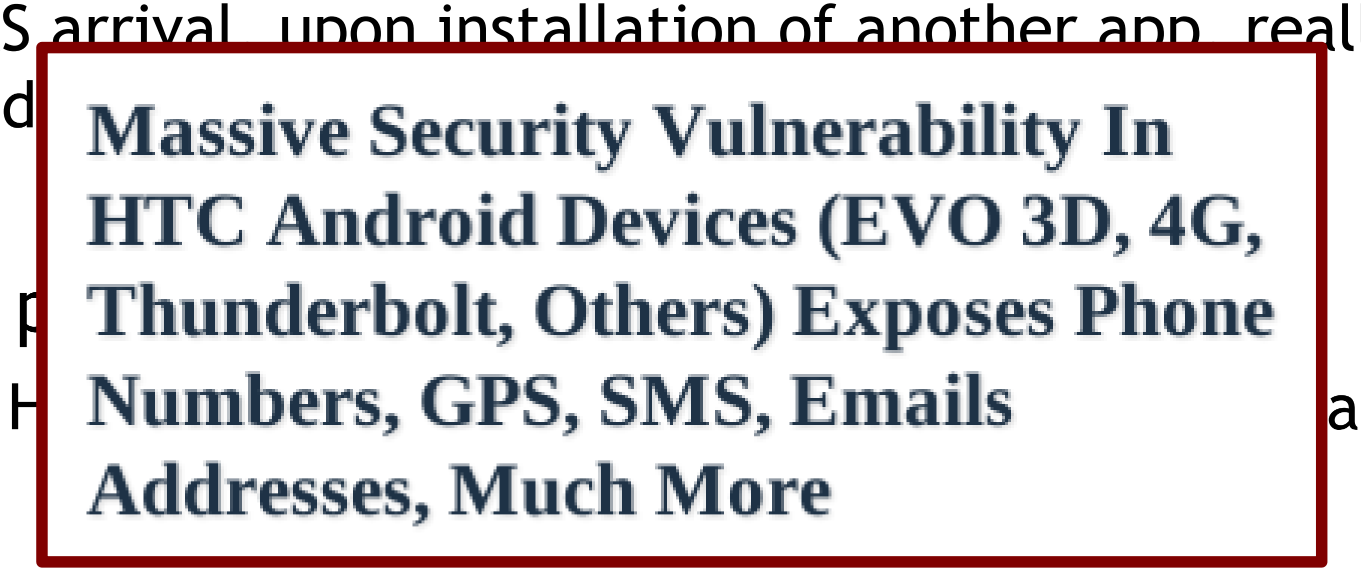
Exploit Window

App Distribution

- Android: Android Market
  - Official Google Play market, and several third-party markets
  - Bouncer: Google app scanner for known malware, potentially malicious behavior
- Apple iOS: iTunes App Store
  - Only official iTunes app store
  - Review process: List of guidelines on apps
- Can automated/manual review catch malware?
  - Cat-and-mouse game typical in malware arms race

Unlike Classical Malware...

- Most mobile malware is delivered from an app marketplace
  - By default phones don't allow sources other than the official
  - Apps can be set to start automatically after boot, upon SMS arrival, upon installation of another app, really a lot of d
- Your p
  - As H ated port



Massive Security Vulnerability In HTC Android Devices (EVO 3D, 4G, Thunderbolt, Others) Exposes Phone Numbers, GPS, SMS, Emails Addresses, Much More

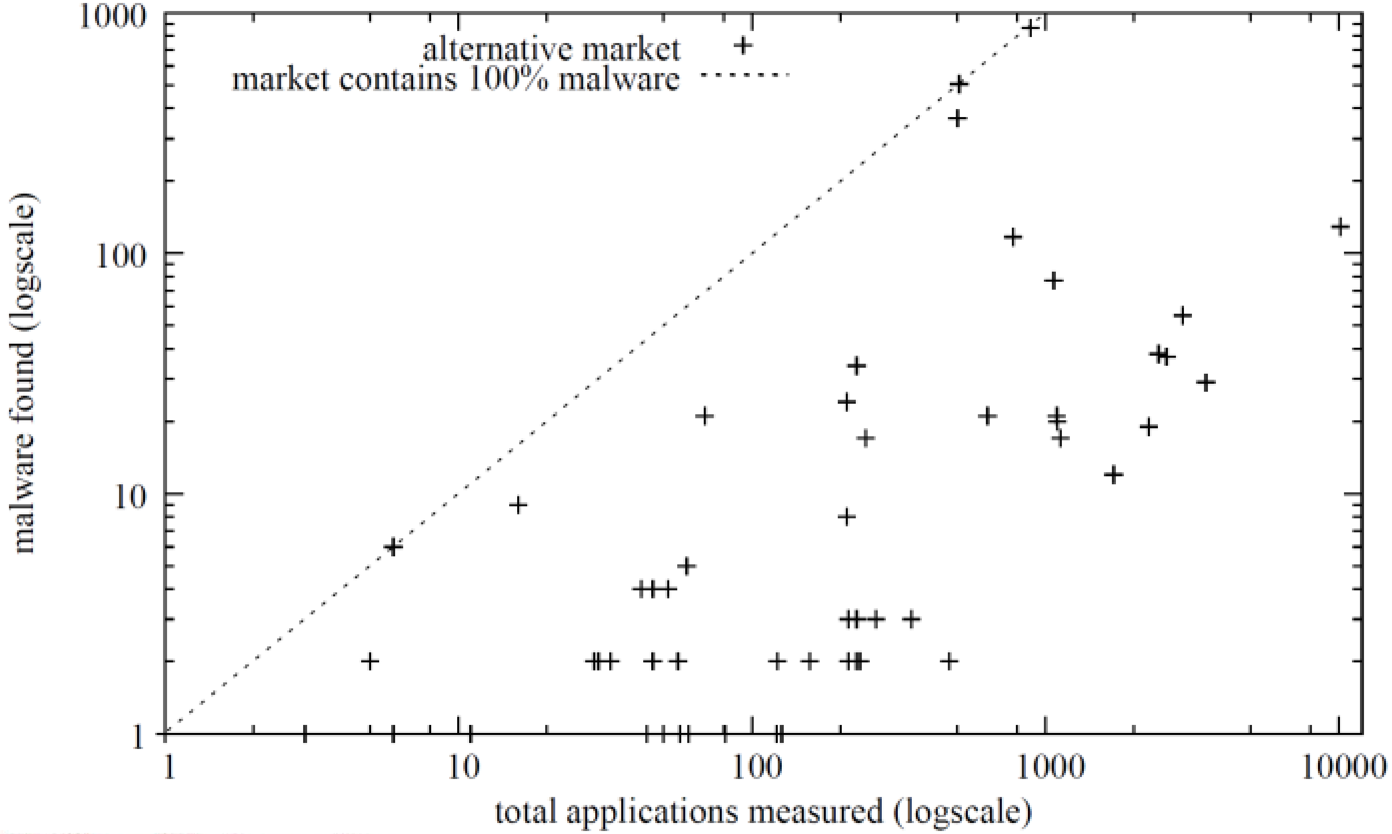
Malware in Different Markets?

- Official market
  - REALLY low
  - Like a small fraction of a percent

- Alternative markets
  - All over the place

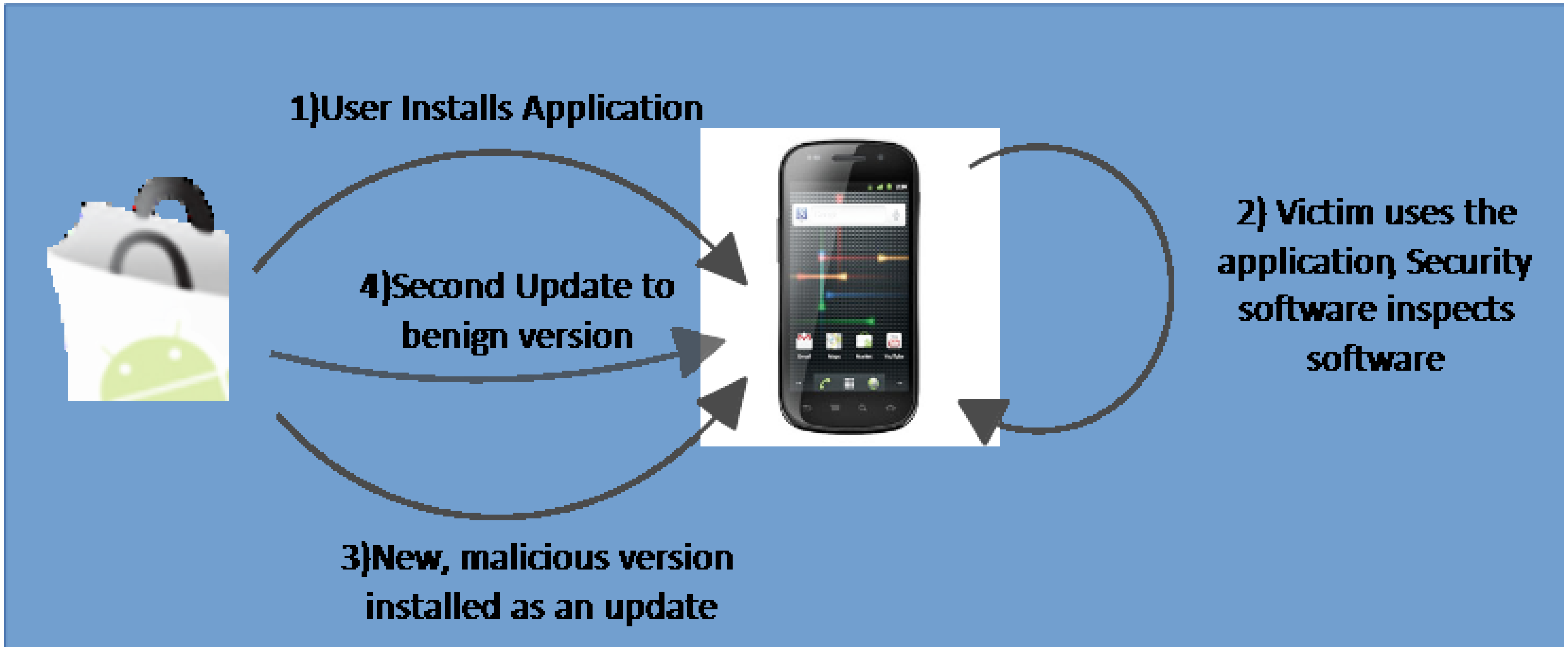
Malware in Different Markets!

- Findings from market study
  - Plot shows malware as a function of total applications
  - Malware in alternative markets is a significant problem
  - Official market contains 119 malware, or 0.003% of sample



Malicious Updates

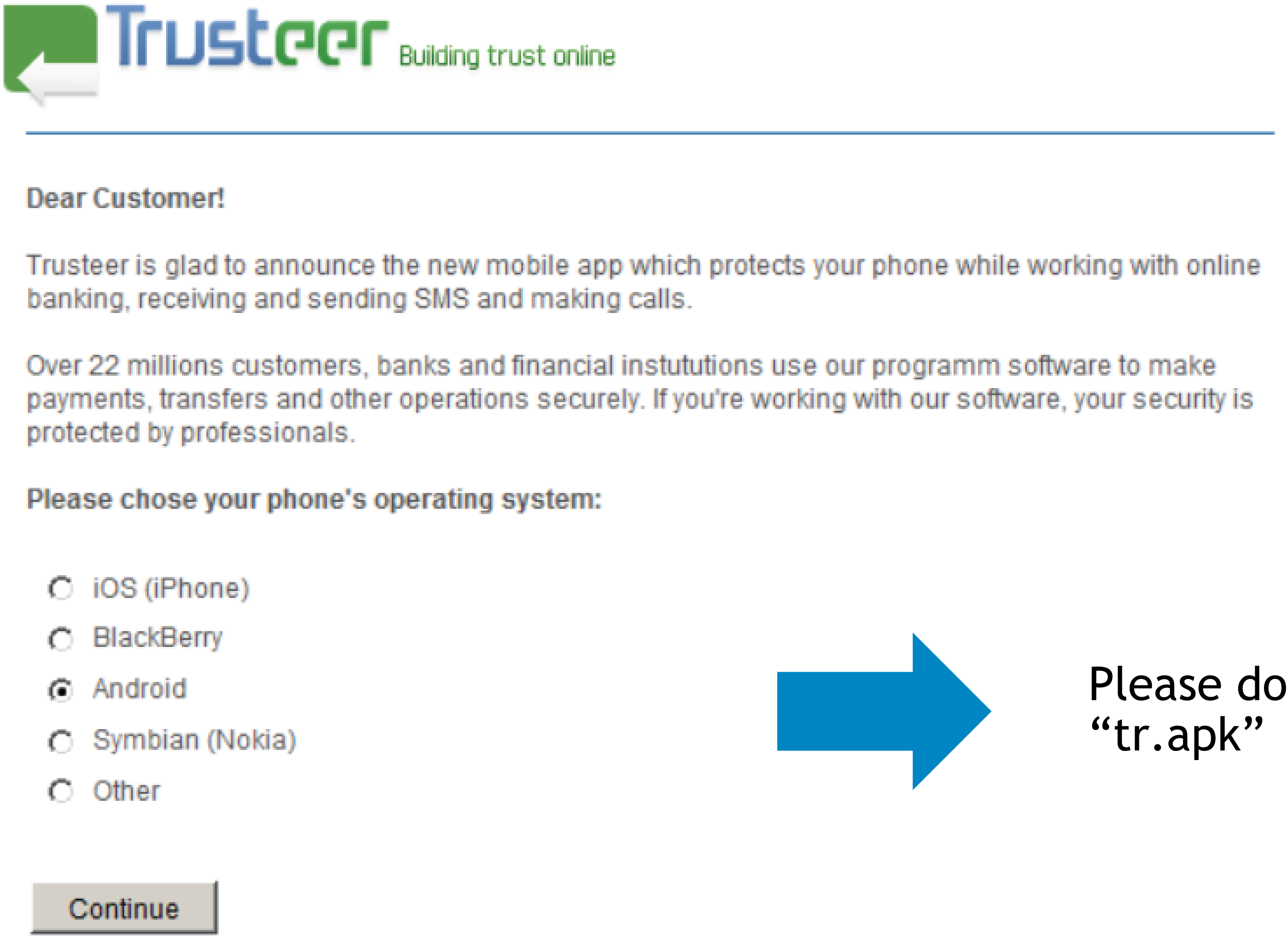
- Security software on contemporary mobile devices does not receive elevated system access
  - unlike such software on typical PC
  - Limits accessibility to questionable software
- Application updates may download and install automatically


1)User Installs Application
2) Victim uses the application, Security software inspects software
3)New, malicious version installed as an update
4)Second Update to benign version

Bad apps

- Spoofed
  - Netflix
- Repackaged / grafted
  - MonkeyJump
- Spyware
  - Stealth
- Greyware
  - Almost everything else
- Rooting
  - Is ok, but some apps do it when you don't know

Example: Zitmo



Dear Customer!

Trusteer is glad to announce the new mobile app which protects your phone while working with online banking, receiving and sending SMS and making calls.

Over 22 millions customers, banks and financial instututions use our programm software to make payments, transfers and other operations securely. If you're working with our software, your security is protected by professionals.

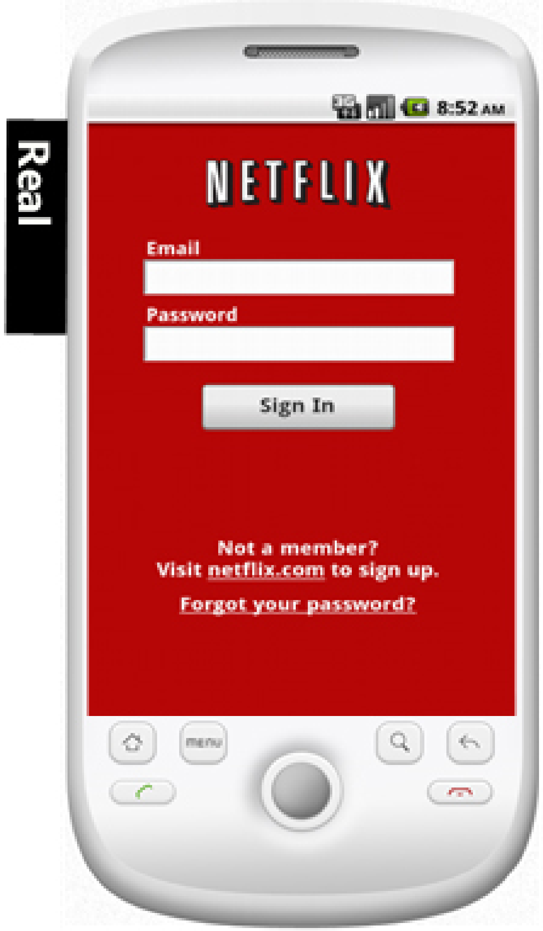
Please chose your phone's operating system:

○ iOS (iPhone)
○ BlackBerry
● Android
○ Symbian (Nokia)
○ Other

Please download "tr.apk"

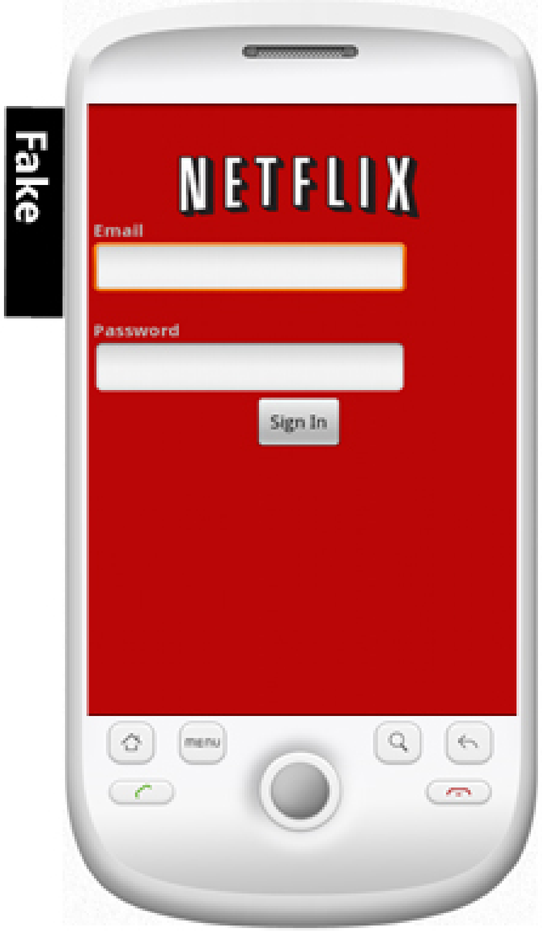
Example: App Spoofing

Real



Not a member?
Visit netflix.com to sign up.
Forgot your password?

Fake



- Netflix only supports certain devices

- But “Netflix” is available for every device!!

Example: Repackaging

- Geinimi
- MonkeyJump

android.permission.INTERNET
android.permission.ACCESS_COARSE_LOCATION
android.permission.READ_PHONE_STATE
android.permission.VIBRATE
com.android.launcher.permission.INSTALL_SHORTCUT
android.permission.ACCESS_FINE_LOCATION
android.permission.CALL_PHONE
android.permission.MOUNT_UNMOUNT_FILESYSTEMS
android.permission.READ_CONTACTS
android.permission.READ_SMS
android.permission.SEND_SMS
android.permission.SET_WALLPAPER
android.permission.WRITE_CONTACTS
android.permission.WRITE_EXTERNAL_STORAGE
com.android.browser.permission.READ_HISTORY_BOOKMARKS
com.android.browser.permission.WRITE_HISTORY_BOOKMARKS
android.permission.ACCESS_GPS
android.permission.ACCESS_LOCATION
android.permission.RESTART_PACKAGES
android.permission.RECEIVE_SMS
android.permission.WRITE_SM

android.permission.INTERNET
android.permission.ACCESS_COARSE_LOCATION
android.permission.READ_PHONE_STATE
android.permission.VIBRATE

```
<intent-filter android:priority="65535">
            <action android:name="android.provider.Telephony.SMS_RECEIVED">
             </action>
      </intent-filter>
```

Carnegie Mellon University

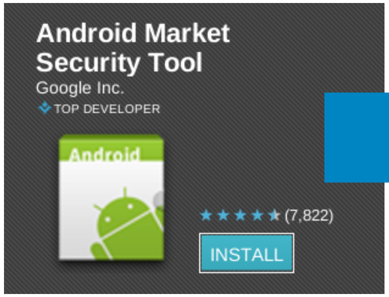
©2015 Patrick Tague

Example: Repackaging (2)

- DroidDream

* Falling Down
* Super Guitar Solo
* Super History Eraser
* Photo Editor
* Super Ringtone Maker
* Super *** Positions
* Hot ***y Videos
* Chess
* 下坠 滚球_Falldown
* Hilton *** Sound
* Screaming ***y Japanese Girls
* Falling Ball Dodge
* Scientific Calculator
* Dice Roller
* 躲避 弹球
* Advanced Currency Converter
* App Uninstaller
* 几何 战机_PewPew
* Funny Paint
* Spider Man
* 蜘蛛 侠

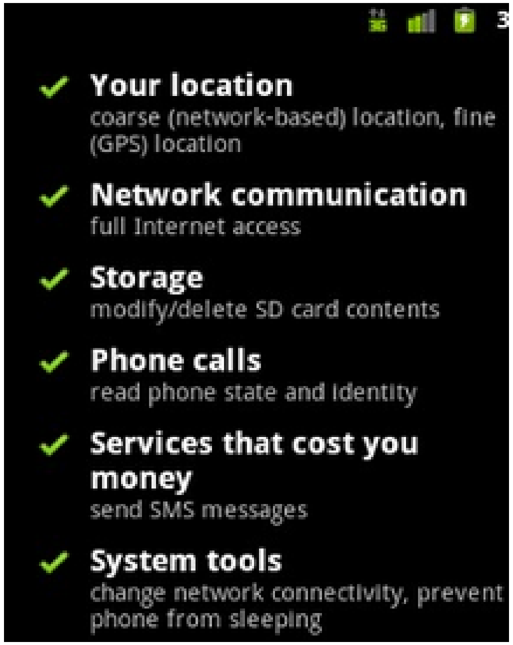
Fake Android Market Security tool delivers more than just a cure for Droid Dream malware



Android Market Security Tool

Google Inc.

TOP DEVELOPER



✓ **Your location**
coarse (network-based) location, fine (GPS) location

✓ **Network communication**
full Internet access

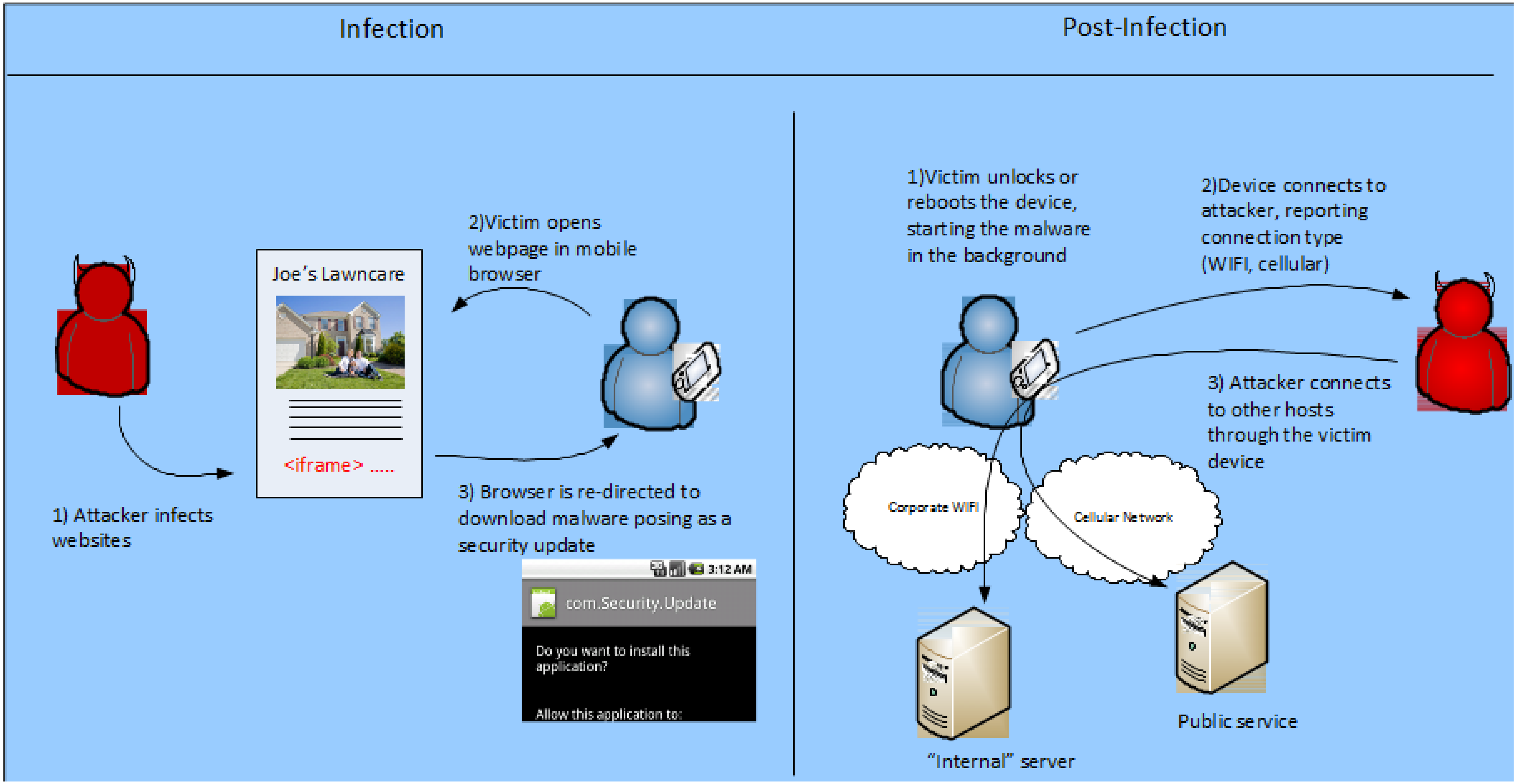
✓ **Storage**
modify/delete SD card contents

✓ **Phone calls**
read phone state and identity

✓ **Services that cost you money**
send SMS messages

✓ **System tools**
change network connectivity, prevent phone from sleeping

Example: NotCompatible



Infection

Post-Infection

1) Attacker infects websites

2)Victim opens webpage in mobile browser

3) Browser is re-directed to download malware posing as a security update

3:12 AM

com.Security.Update

Do you want to install this application?

Allow this application to:

1)Victim unlocks or reboots the device, starting the malware in the background

2)Device connects to attacker, reporting connection type (WIFI, cellular)

3) Attacker connects to other hosts through the victim device

Example: SimpleTemai

- Likely aimed at mobile application promotion systems (click fraud)
  - Download mobile apps from alternative markets
  - Rate the downloaded application
  - Uninstall the downloaded application

- Could consume significant bandwidth

- Grafted into legitimate mobile apps
  - Mostly games
  - Resistant to some automated detection techniques

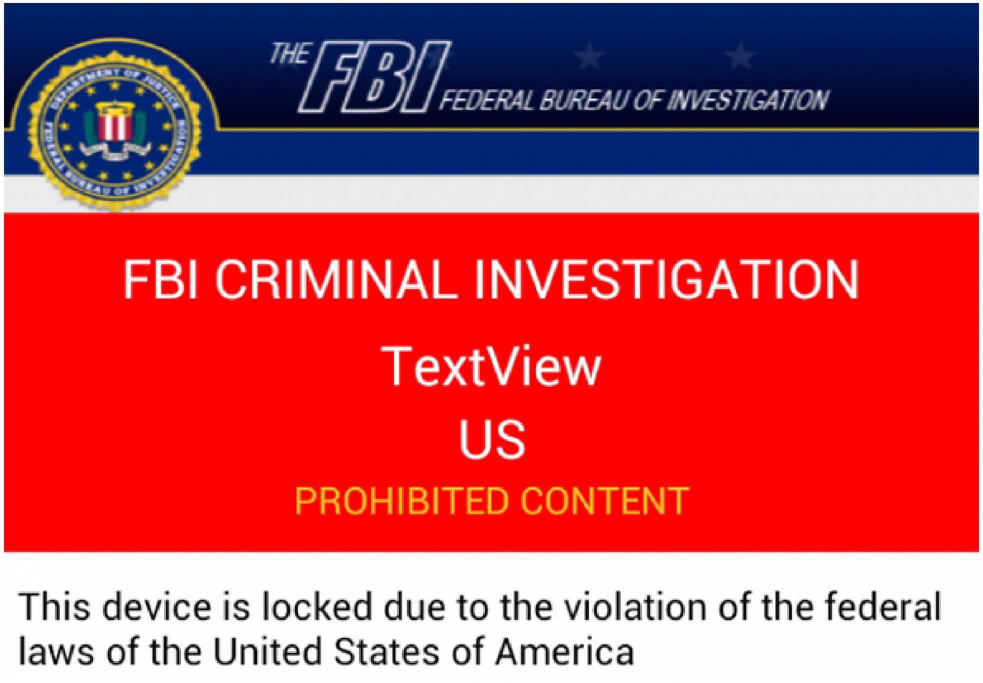
Example: BankMirage

- BankMirage is a cloned banking app that was found in the Google Play store
  - Targets customers of Mizrahi Bank in Israel by putting a wrapper around the legitimate app

- Steals users' IDs (basically phishing)
  - Strangely, doesn't steal their passwords
  - A comment in the malware code explicitly stated the password wasn't to be recorded...
  - App then gives login error and reinstalls legit app

Example: ScarePakage

- ScarePakage is ransomware that locks phone functionality until the user makes a MoneyPak payment



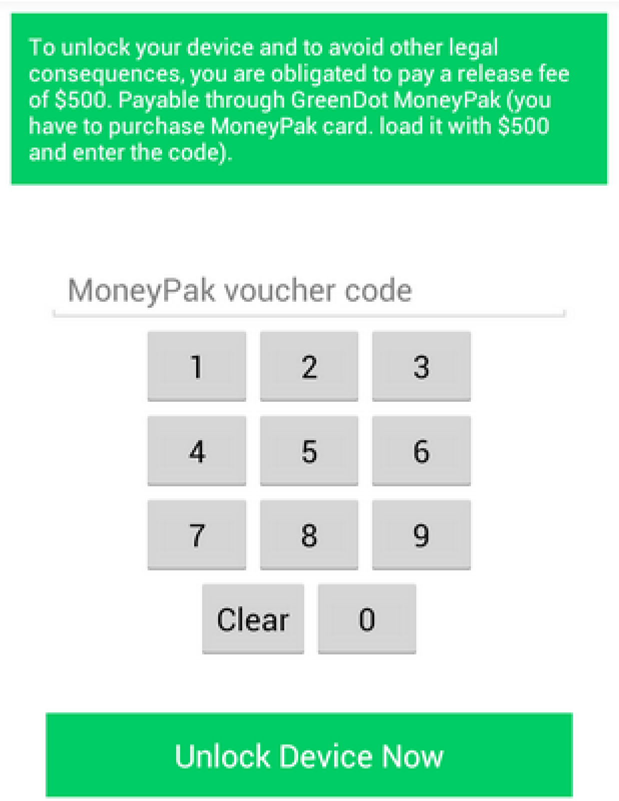
FBI CRIMINAL INVESTIGATION

TextView

US

PROHIBITED CONTENT

This device is locked due to the violation of the federal laws of the United States of America



To unlock your device and to avoid other legal consequences, you are obligated to pay a release fee of $500. Payable through GreenDot MoneyPak (you have to purchase MoneyPak card. load it with $500 and enter the code).

MoneyPak voucher code

Source: Lookout Top Threats
https://www.lookout.com/resources/top-threats/scarepakage

Example: BadNews

- BadNews is a malicious SDK that pretends to be an innocent ad network
  - Sends fake news messages, prompts users to install apps with sensitive permissions, sends info back to C&C server
  - Found distributing known AlphaSMS toll-fraud malware
- Evolution of malware using distribution networks, so the apps appear benign

Summary

- Mobile device features make mobile malware significantly different from the PC era

- Most likely, there's a lot of mobile malware out there that we haven't discovered/detected yet
  - Is there a better approach than to continue the cat-and-mouse game of malware detection and evolution?

Nov 3:

NO CLASS

Nov 5:

Mobile Ad Vulnerabilities