Android malware exposed

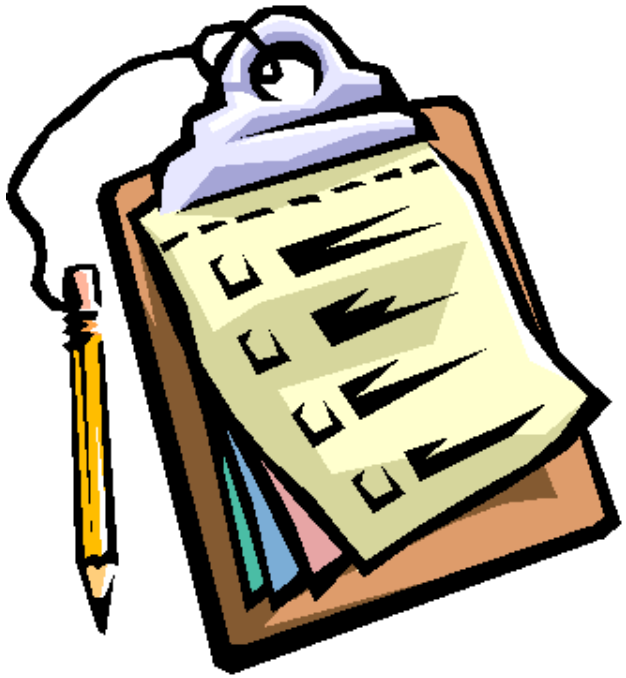
An in-depth look at the evolution of Android malware

Grayson Milbourne
Director of Threat Research

Armando Orozco
Sr. Threat Research Analyst

Agenda

- Smart Device Risk Awareness
- Smart Device Risk Assessment
- Threat Vectors
- Real World Examples
- Security Tips
- Q&A



Smart Device Risk Awareness

- Do companies realize the risk?
  - 59% agree mobile devices create a high security risk
  - 49% think mobile device security is a high priority
- What are companies concerned with?
  - 74% are very concerned with data loss/protection
  - 70% are very concerned with mobile malware
- How are companies impacted?
  - 43% reported lost or stolen devices
  - 23% reported malware infected devices

Smart Device Risk Assessment

- Risks when a device is infected
  - SMS/Email/Voice monitoring
  - Data loss
  - Unwanted root – Bypassing permission model
  - User tracking
  - Unauthorized corporate network access
  - Identity theft
  - Man-in-the-Middle attacks

Threat Vectors

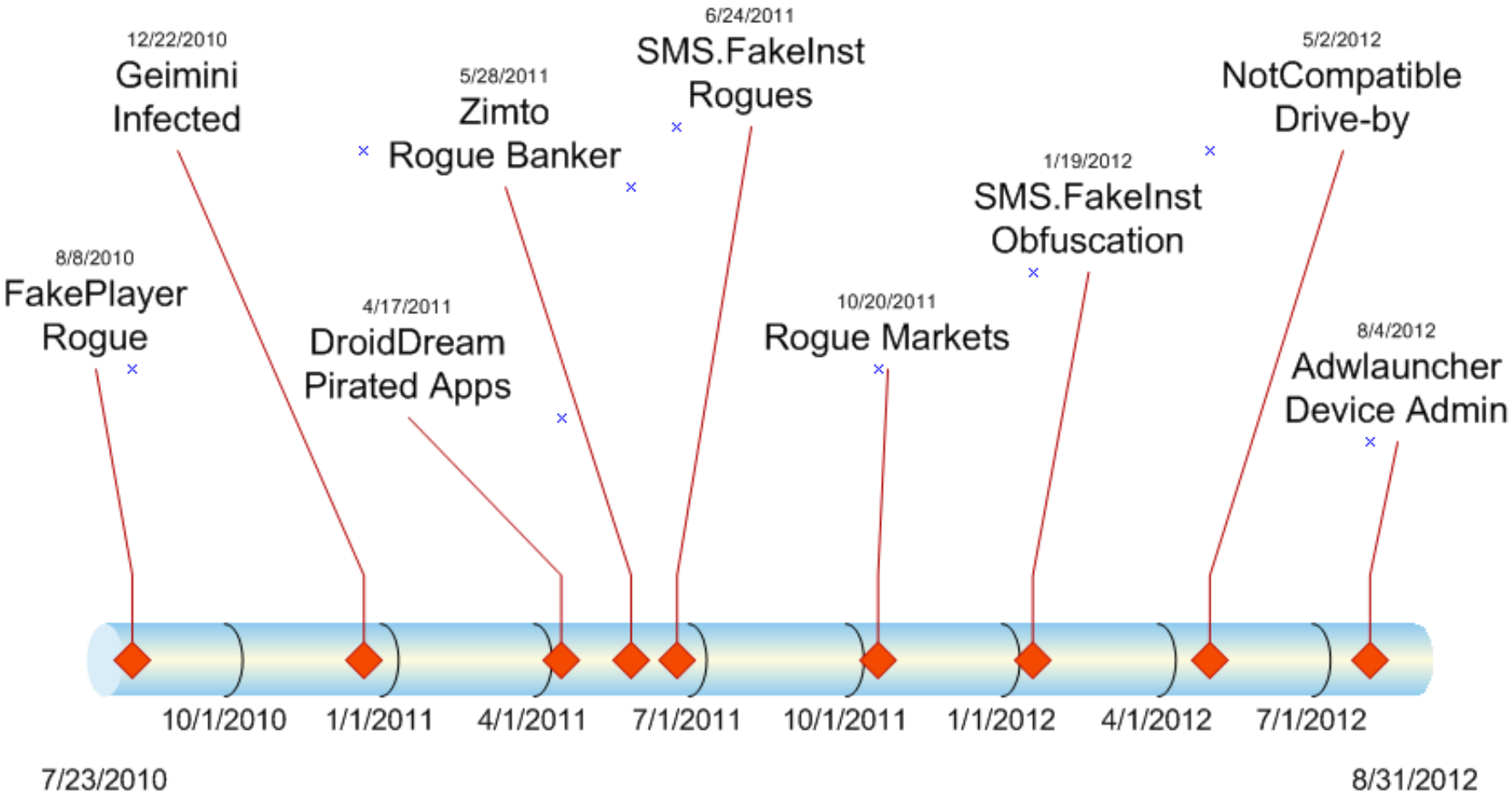
Social-Engineering

- Rogue Android markets
- Infected applications
- SMS phishing
- Man-in-the-middle
- Drive-by infection
- QR code

Evasion Tactics

- Rogue applications
- System folder installation
- Polymorphic distribution
- Payload encryption
- Security app removal
- Payloads embedded in image files

Threat Vector Timeline



WEBROOT®

Real World Example 1

- Threat Vector: Premium SMS Trojans
  - Threat: FakeInst, Opfake, Jifake, SMSSend
  - Infects: Android
  - Behavior
    - Send premium-sms messages
    - Rogue apps and Market places

```
OpInfo          returning SMSCount for ru = 3
sendMessage     Sending SMS #1
gn              2855
OpInfo          returning SMSCount for ru = 3
sendMessage     Sending SMS #2
gn              9151
OpInfo          returning SMSCount for ru = 3
sendMessage     Sending SMS #3
gn              7151
OpInfo          returning SMSCount for ru = 3
OpInfo          returning SMSCount for ru = 3
```

- Why is this concerning?

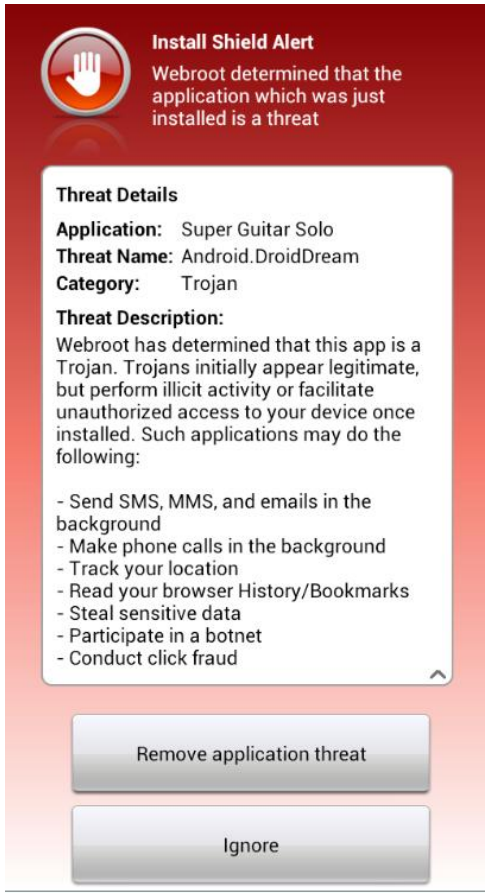
# 2855	range of 170-203.20 rubles	US $5.52-6.60
# 9151	range of 101.60-140.42 rubles	US $3.30-4.56
# 7151	range of 33.87-40.00 rubles	US $1.10-1.30

Total cost

137.17-383.62 rubles US $9.92-12.46

Real World Example 2

- Threat Vector: Rooted/jailbroken device
  - Threat: DroidDream
  - Infects: Android
  - Behaviors
    - Roots device
    - Adds device to a bot network
    - Installs payload apps
- Why is this concerning?



Real World Example 3

- Threat Vector: Data loss
  - Threat: FindAndCall
  - Infects: iOS and Android
  - Behaviors
    - Collects contacts info (name, number, email, etc.)
    - Sends data to remote server without user consent
    - Uses collected contact data to spam SMS contacts
- Why is this concerning?

Security Tips

- Smart device policy, education
- Passwords, not swipe lock screens
- Encrypt confidential data
- Remote locate and/or wipe
- MDM (Mobile Device Management)
- Device backup
- Get help

WEBROOT®

Q/A Session