

# Physical Drive-by Downloads

Kos - @theKos



# Introduction

- Kyle Osborn – Kos
- Pentester and researcher at AppSec Consulting
  - <http://AppSecConsulting.com/>
  - WebApp, Network, PCI, etc.
- Etc etc



# Android User Ecosystem

- Big focus on rooting phones
- Lots of untested ROMs being released
- APKs being passed around
- Just all around bad security habits being taught



# Android User Ecosystem

- A poll of 500~ users showed that:
  - 70% were rooted
  - 56% had ADB enabled
  - 76% don't disable custom recover The rest did disable it, or never used it
  - 89% don't use encryption (or not supported)
  - 41% use slide to unlock (not password)22% use gesture
  - 41% use security software (anti-virus, remote tracking/wiping)



# Android Security

- Browser exploits
- Application exploits
- Kernel exploits
  - [mempodroid \(mempodipper\)](#)
- ADB Exploits
  - [ZergRush](#)
  - [GingerBreak](#)
- Exploits created by vendors



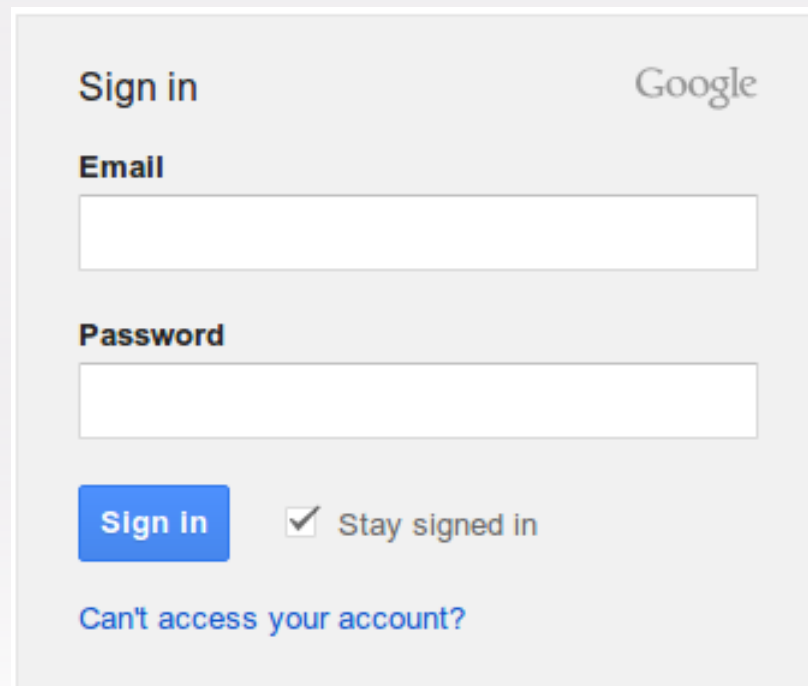
# Our Goals

- Nothing I'm talking about is '1337'
- We want the sensitive stuff
  - Passwords, emails, text messages, photos
  - And more....
- Maintain persistence
  - Evil APK / rootkit
- Do this all in <1 minute.
- No new exploits



# Our Goals

- On top of it all, we want to bypass THIS:



A screenshot of a Google sign-in form. The form is light gray and contains the following elements: the text "Sign in" in the top left and "Google" in the top right; a label "Email" above a white input field; a label "Password" above another white input field; a blue "Sign In" button; a checked checkbox labeled "Stay signed in"; and a blue link "Can't access your account?" at the bottom.



# Physical Access

- Secure bootloader
- Stock recovery partition
- Encryption prevents access
- Keyguard enabled (face/gesture/PIN/pass)
- ADB off





# Physical Access

- All work together.
- One failure in the list could mean full compromise



# Secured by bootloader

- Not all devices have locked bootloader
  - Run unsigned code at boot by default (over USB)
- Some bootloaders easily unlocked
  - Galaxy Nexus takes 10 seconds
- Some devices do not wipe on unlock
  - Galaxy Nexus wipes SSD on unlock.
  
- All these factors prevent owning via cold boot.



# Stock recovery partition

- For system management
- Encrypting the device
- Applying OTA updates



# Encryption prevents access

- Secures drive when unbooted
- Prevents access via the recovery partition
- Uses regular KeyGuard PIN or Pass
  - The one required to unlock phone every single time



# Keyguard

- Prevents immediate access
- Face unlocked easily defeated
- Pattern smudges
- Weak PIN allowed



# Keyguard

- 389,112 possible gestures
- $(9!+8!+7!+6!+5!+4!)$  - impossible\
- !1-3 unless 2 before 1.
- No number repeats
- Stores hash in `/data/system/`



# ADB off

- Does not provide USB debugging
- Can't connect even when phone locked
- Can't disable lockscreen or access data



# Physical Vectors

- Bootloader unlocked
  - Run unsigned code
  - Access device as root
- Non-stock recovery partition
  - ClockWork Mod et al allows unauth'd root access
- Lack of encryption
  - Allows above attacks ^^^
- ADB enabled
  - You win





# It's not ALL about the phone

- Really. Data on the phone is great
  - Passwords stored
  - Photos, texts, emails – ETC
  - All great, but not the best.
- If only there was a way to get more...
  - Oh yeah, synced Google Account



# Scenarios – Unlock Bootloader

## Long access time

- Unlock your bootloader to run ROM
  - Could wipe phone
  - Requires a reboot
  - Slow
- Already unlocked
  - Already runs unsigned code
  - Boot over USB or flash custom recovery partition.



# Scenarios – Customer Recovery

## Long access time

- Custom recovery partition
  - All unauthenticated
  - All allow ZIP updates (easy backdoor payload?)
  - All allow root ADB



# Speed Hacks - Prerequisites

This beauty



# Speed Hacks - Prerequisites

**Thanks Hak5!**



# Speed Hacks - Prerequisites

## P2P-ADB (Phone-to-phone ADB)

```
$ sh run.sh
Welcome to p2p-adb!
Let's break some stuff.
Waiting for phone to connect...
What do you want to do today?
    0) Check if root
    1) Steal App data
    2) Steal Google data
    3) Steal Camera Photos
    4) Steal JPGs > 200k
    x) Exit

Choose wisely: 
```



# The Sauce

## P2P-ADB (Phone-to-phone ADB)

- Quick hit ADB scripts
  - Steal /data/data/\* && /sdcard/Android/data/
  - Get camera photos
  - Steal Google Auth tokens \*\*
  - Steal wpa\_supplicant.conf / keys
  - Disable KeyGuard
  - Install custom APK
  - Auto-configure proxy (more on this later)



# The Sauce

## P2P-ADB (Phone-to-phone ADB)

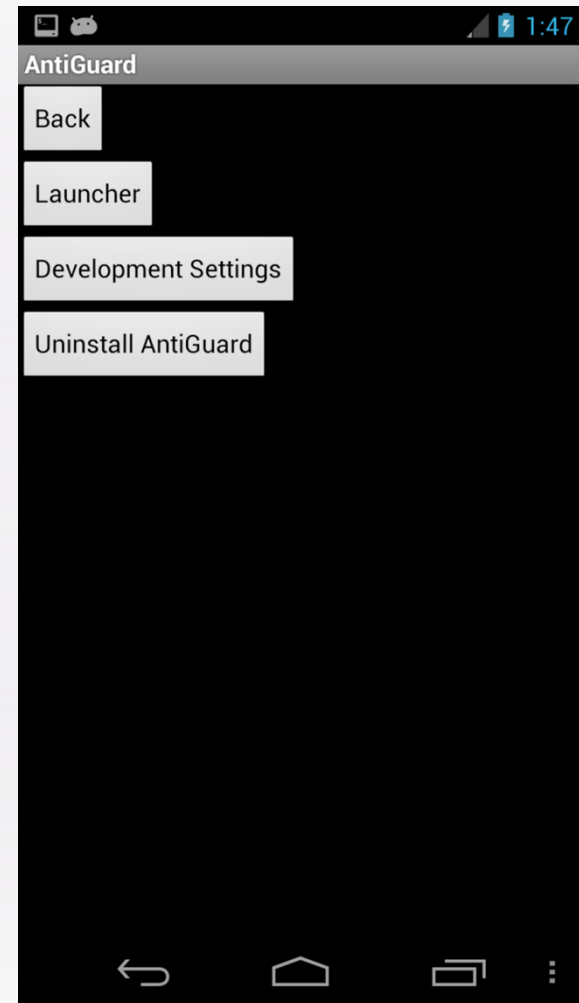
- Detection of root
- Auto-root maybe?
- "Cracks" gesture pattern
- Eventual full automation
- Runs on a rooted phone





# The Sauce

- AntiGuard
  - Installs via ADB
  - **Disables KeyGuard on run**
  - Include quick launch apps



# Scenarios – ADB Enabled

- ADB enabled – ROOT!
  - Grab **ALL** the things
  - Application data – Browser passwords, emails, SMS, etc
  - System data – WiFi passwords, system password hash to crack
  - Install rootkit – Throw backdoored binaries & init scripts
  - ”Oh yeah, sync'd Google Account”



# Scenarios – ADB Enabled

- ADB enabled – No root
  - Encryption does not matter
  - Can't access most of /data/
  - Grab photos
  - Grab data on /sdcard/
  - Install APKs
  - Install CA Certs
  - Export contacts/texts



# Oh yeah, sync'd Google Account

- /data/system/accounts.db
- sqlite> select \* from accounts where name = 'kos@kos.io';
- 4|kos@kos.io|com.google|1/CfYYxx-xxxxxx-xxxxxx
- ***This key IS your Google Account***



# Oh yeah, sync'd Google Account

- POST /auth HTTP/1.1
- Content-Type: application/x-www-form-urlencoded
- Content-Length: 277
- Host: android.clients.google.com
- Connection: Keep-Alive
- User-Agent: GoogleLoginService/1.2 (toro ICL53F)
- **accountType=&Email=&has\_permission=1&Token=1/CfYYxx-  
xxxxxx-  
xxxxxxx&service=weblogin%3Acontinue%3Dhttps%253A//  
www.google.com/dashboard/&source=&androidId=&app=&c  
lient\_sig=&device\_country=&operatorCountry=&lang=&Refres  
hServices=**

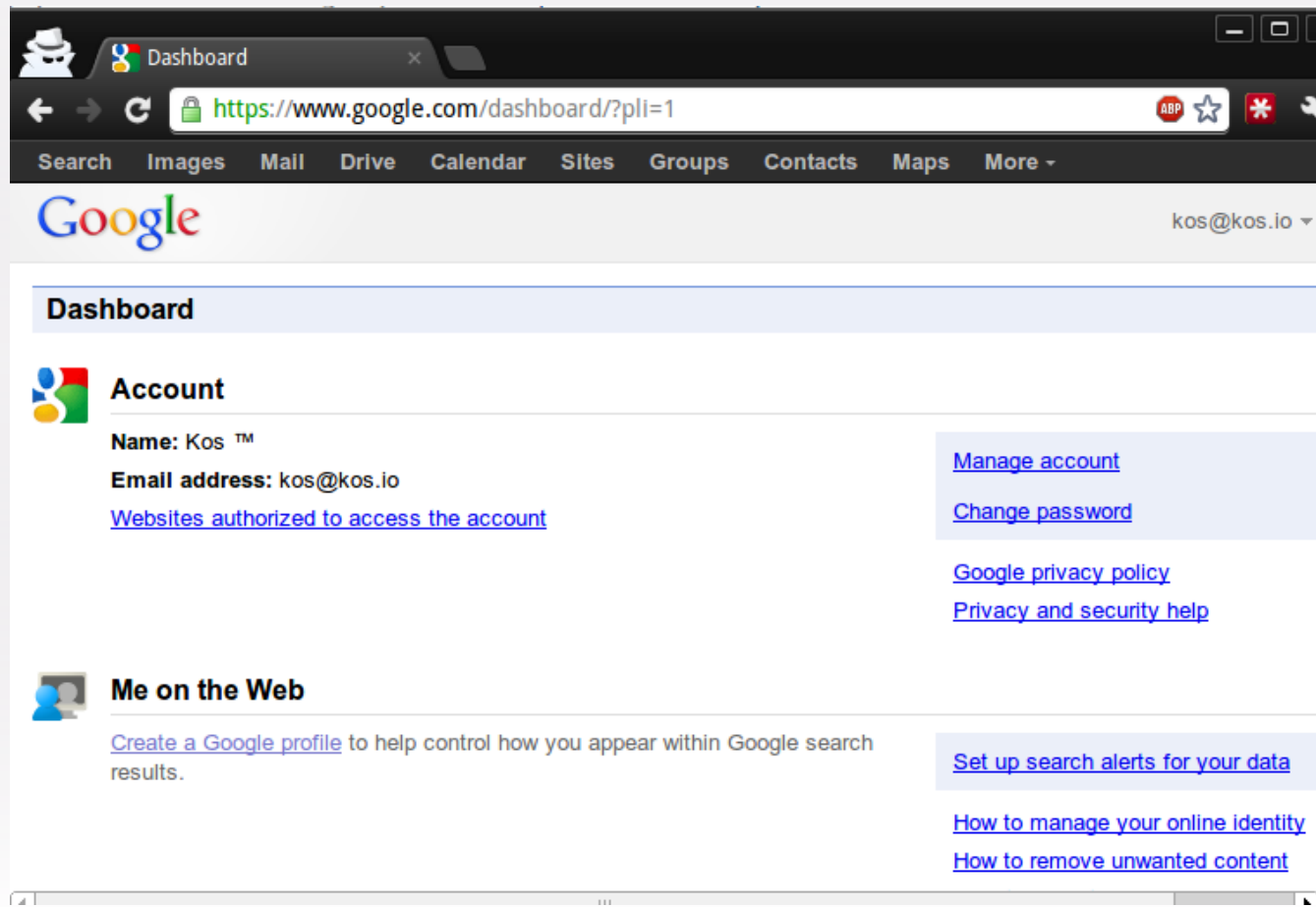


# Oh yeah, sync'd Google Account

- Auth=[https://accounts.google.com/MergeSession?args=continue%3Dhttps%253A//www.google.com/dashboard/&uberauth=APh-3Fx8SO\\_CR0d9eDFAVmnUZFM-hg2Va8II0IxXHjlgDoCVbV87uCfCBJQMtM2MaoR\\_Is4hXWfUfP4V\\_IkoA59nZ8i1\\_Ta00pQJyduvJkDu6WTGvzFnVw4UytLQersjaS-ylyAkRBEkQumigOS8aXJK4JL-lkazlLRanrid9ex\\_LajkKx6v6cQq-jO9FNsQ2dgdwF6KVz2ktVPgi6Ps\\_5SvCKYtC541c2bYOQ3LfTFJrDd9dDw9sqa7ZAVZKIwnXn6yQv7D6x6KRrYFeAjGAnBqTytv8AhhkIhmaC7HQ88TH-xP0VPyVFg1hcQJtLOlwQUgcd3oSCaYZXI3\\_8bYrK2reXk3bC\\_LnIT9YUycKB9kpubk3NZHyIO2Nkq7PeovUbf-nmjavF-hH%0A&source=AndroidWebLogin](https://accounts.google.com/MergeSession?args=continue%3Dhttps%253A//www.google.com/dashboard/&uberauth=APh-3Fx8SO_CR0d9eDFAVmnUZFM-hg2Va8II0IxXHjlgDoCVbV87uCfCBJQMtM2MaoR_Is4hXWfUfP4V_IkoA59nZ8i1_Ta00pQJyduvJkDu6WTGvzFnVw4UytLQersjaS-ylyAkRBEkQumigOS8aXJK4JL-lkazlLRanrid9ex_LajkKx6v6cQq-jO9FNsQ2dgdwF6KVz2ktVPgi6Ps_5SvCKYtC541c2bYOQ3LfTFJrDd9dDw9sqa7ZAVZKIwnXn6yQv7D6x6KRrYFeAjGAnBqTytv8AhhkIhmaC7HQ88TH-xP0VPyVFg1hcQJtLOlwQUgcd3oSCaYZXI3_8bYrK2reXk3bC_LnIT9YUycKB9kpubk3NZHyIO2Nkq7PeovUbf-nmjavF-hH%0A&source=AndroidWebLogin)
- Expiry=0



# Oh yeah, sync'd Google Account



# Getting GAccount without Root

- Problem: not rooted, but we still want Google Account.
- After disabling KeyGuard
  - WiFi hotspot with HTTPS proxy
  - Install CA Cert (does not require keystore pass)
  - Open Browser to [google.com/accounts](https://google.com/accounts)
  - Initiate auto-login sequence
  - Capture HTTPS request in proxy
  - *Profit!*





# What else?

- Compromised Google Account:
- Android restore functionality
  - Restores WiFi passwords and some app data
  - WiFi passwords stored in cleartext
  - Adding owned Google account to rooted phone = access all the data synced.



# Not root, lame...

- So get it!
- 4.0 & 4.1 root via ADB discovered by 'Bin4ry'
  - <http://kos.io/4xroot>
- 'adb restore' race condition
- Requires interaction.... unlock with AntiGuard
- Own, reboot, drop payload, reboot, free and clear
  
- Tested on Galaxy Nexus & Nexus 7





# Other Attack Vectors

- Juice Jacking



# Other Attack Vectors

- Portable Juice Jacking



# Other Attack Vectors

- You like video games?



# Future

- Future goals...
- Expand AntiGuard
- Auto install CA certs/configure proxies/VPNs
- Drop rootkits



# Raider attack tool

- Raider by @c0rnholio
- Native android app with some attacks implemented
- Open source
- <https://play.google.com/store/apps/details?id=com.silent.services.raider>





# Mitigation

- Quit tweaking.
  - (just kidding, I'll never stop either)
- Disable ADB when done
- Lock your bootloader (if possible)
- Flash stock recovery image.
- Enable encryption.
- Glue your phone to your hand



reboot



# Mitigation

- AdbdSecure
  - <https://play.google.com/store/apps/details?id=com.stericson.adbSecure.pro>
- Made by Stericson (Same guy who manages busybox package)
- Open source
- Screen lock: adb off
- Screen unlock: adb on



# FIN

- <https://github.com/kosborn/p2p-adb/>
- <http://kos.io>
- @theKos
  
- <http://AppSecConsulting.com/>
- [kosborn@appsecconsulting.com](mailto:kosborn@appsecconsulting.com)

