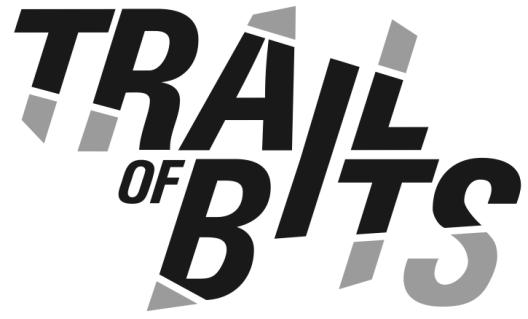


Mobile Exploit Intelligence Project

Dan Guido, Trail of Bits

Mike Arpaia, iSEC Partners

SOURCE Boston, 04/19/2012



Intro and Agenda

- Talk series discussing intelligence-driven security
 - Provide actual data on attacker characteristics
 - Provide analysis tradecraft to interpret it
 - Intrusion kill chains
 - Attacker characterization
 - Adversarial attack graphs
- Informed defense is more effective and less costly
 - Less hypothetical, more verifiable
 - Defenses supported by observation
 - “Technology doesn’t beat determination”



- Secure Password Managers
- Heavy Metal that Poisoned the Droid
- Smartphone Apps are not that Smart



- Is Your Mobile Device Radiating Keys?
- Risk and Vuln Assessment of NFC
- Revisiting Baseband Attacks



- CrowdStrike Android Exploitation Demo
- iOS 5 – An Exploitation Nightmare?



Millions of Mobile Attacks

1

Attack Vector

3

Exploits

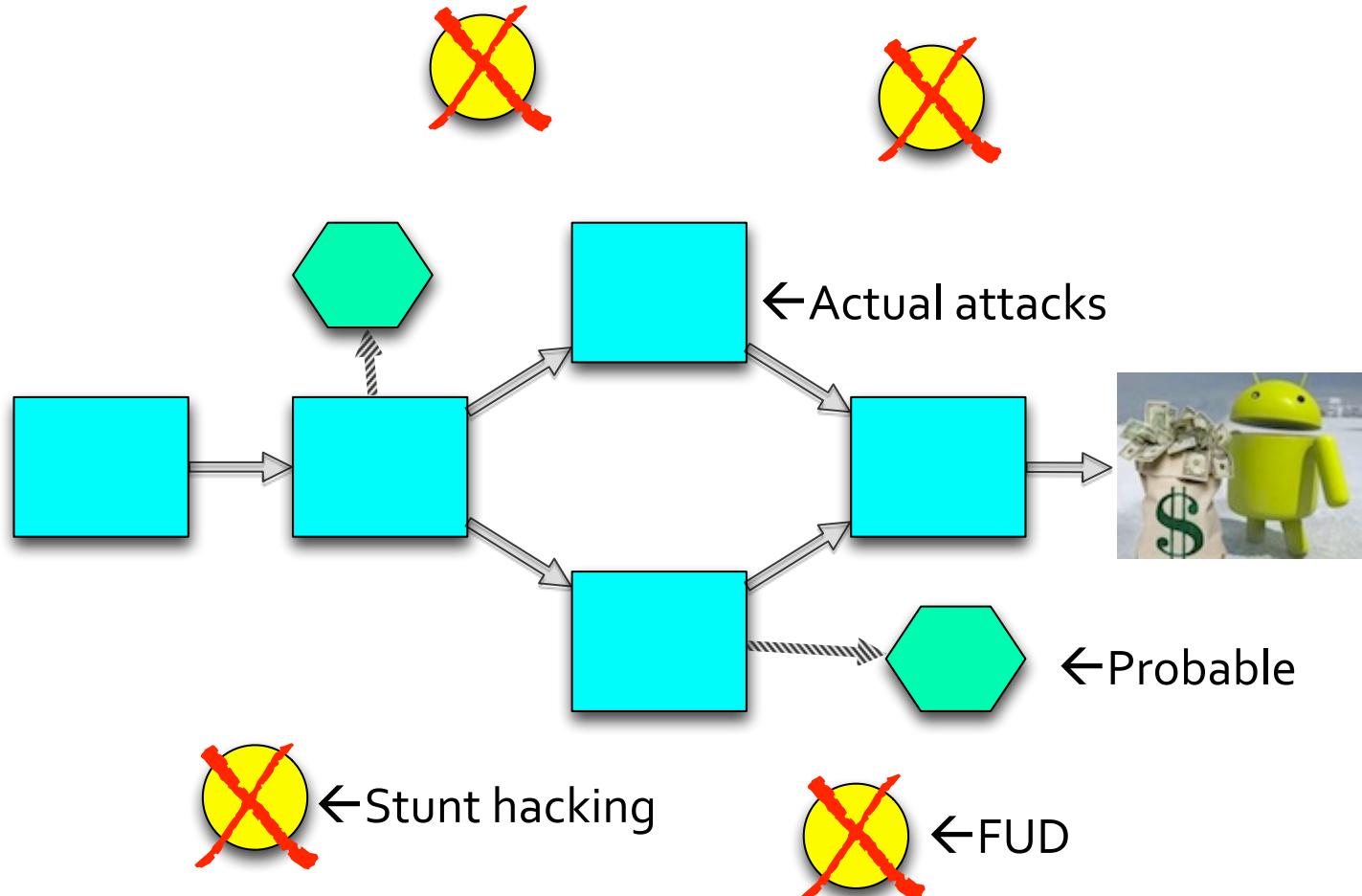
1

Platform

What are we doing wrong?



Your Defense Lacks Intelligence



Attackers choose the least cost path to their objective

Attacker Math 101

- $\text{Cost(Attack)} < \text{Potential Revenue}$
 - Attacks must be financially profitable
 - Attacks must scale according to resources
- $\text{Cost(Attack)} = \text{Cost(Vector)} + \text{Cost(Escalation)}$
 - What we know from Mobile OS architectures

Cost of Attack

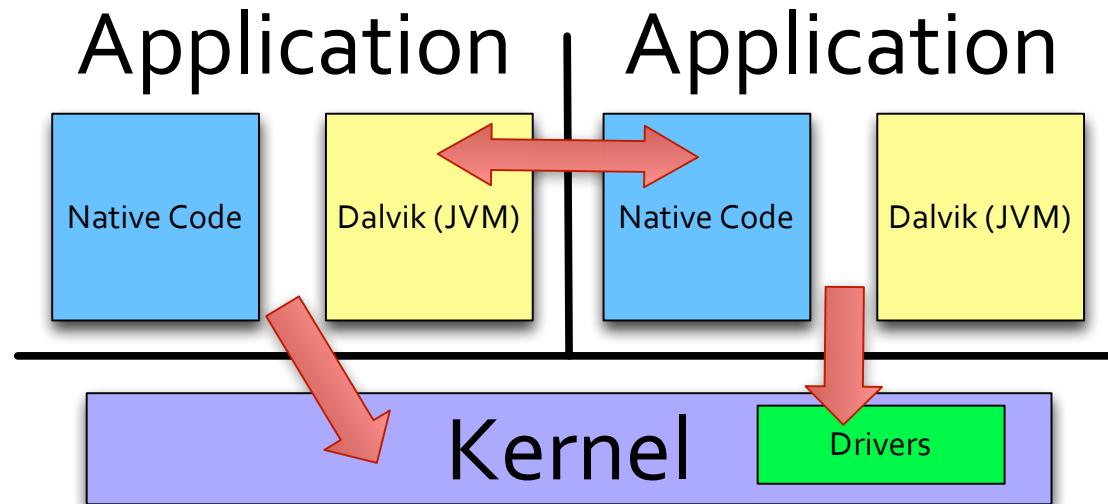
- Ease
- Enforcement
- Established Process

Potential Revenue

- # of Targets
- Value of Data
- Ability to Monetize

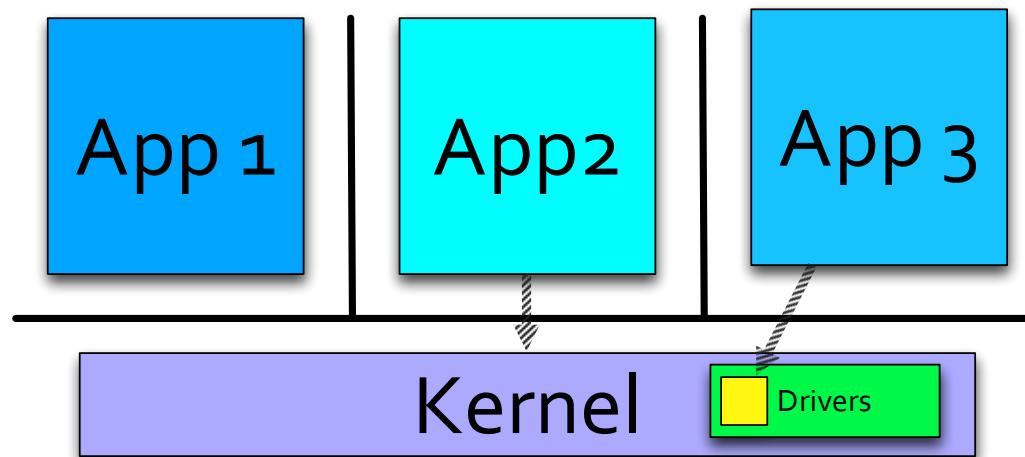
Android Security Model

- Each app runs as a different user and group
 - Apps cannot access data from other apps*
 - Permissions determine ability to perform RPC*
- Apps can access any other resources they want
 - Apps can access the kernel, drivers, syscalls, etc.
 - No Security Manager, no Java Sandbox



iOS Security Model

- Apps run as the same user, but ...
 - Apps must be signed by Apple
 - Apps are given a unique ID and directory by Apple
- Seatbelt restricts apps from accessing anything else
 - Apps cannot access data from other apps (mandatory)
 - Attack surface of kernel is reduced via Seatbelt



Mobile Malware

How does it work?

Mobile Attack Data (2011-2012)

Malware Campaign

- Android Pjapps
- Android Droid Dream
- Android Zeahache

Distributed via: Android Market

Exploits Phone? Yes

Exploits Apps? No

Exploit: Exploid

Exploit: RageAgainstTheCage

CVE: NoCVE (common)

Author: "stealth"

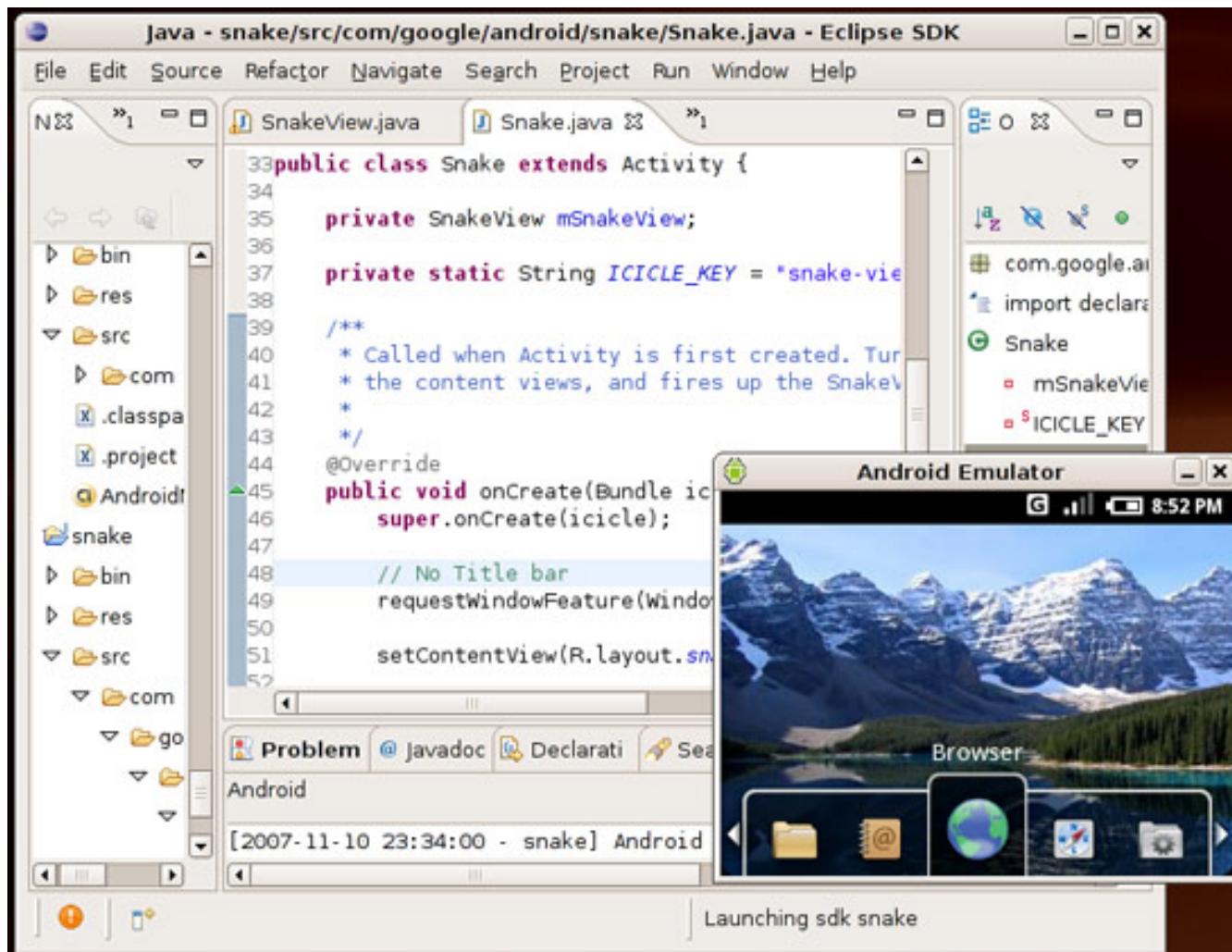
Target: Root-owned Android Userland (adb)

Blame: Google

Technique: RLIMIT_NPROC

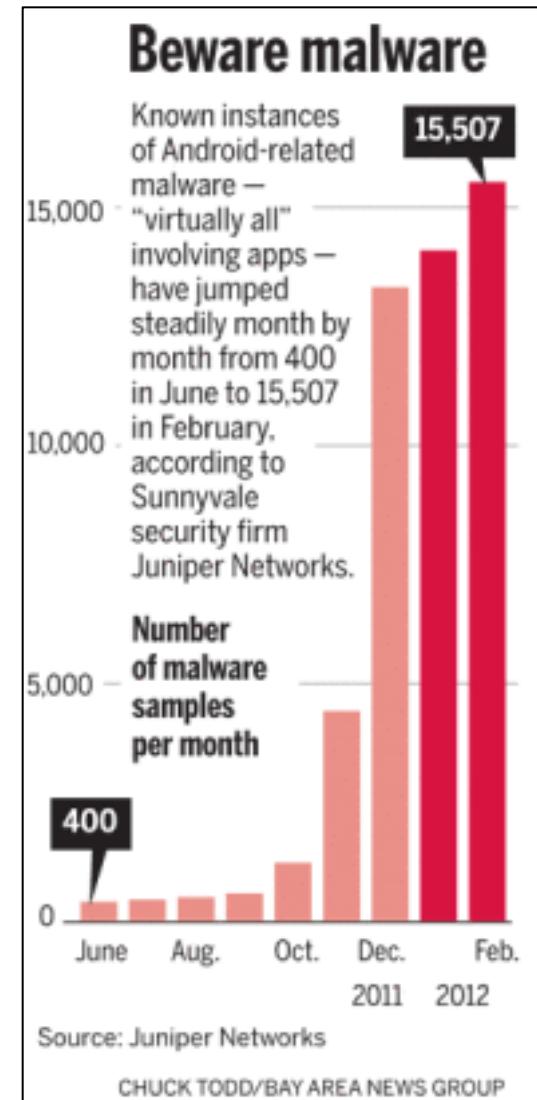
Affects: Android ??? - 2.2 (difficult to identify)

Develop Malware



Find or develop malware to remotely interact w/ victim devices

Add Malware to App



What would be likely for targets to install?

Gain Exposure

Your Registration as a Google Play developer is approved!

You can now upload and publish software to Google Play.

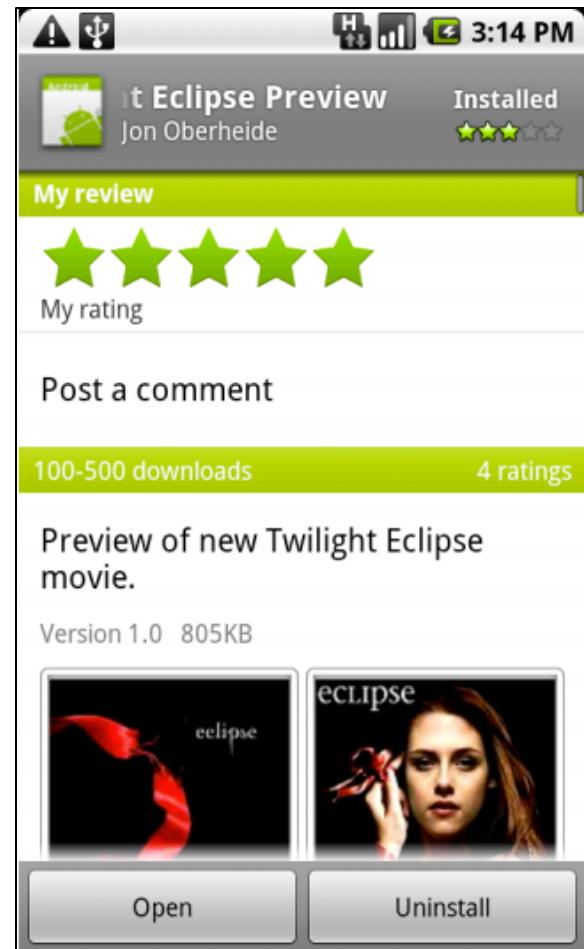
Upload new APK

Required: Select your application's APK

No file chosen

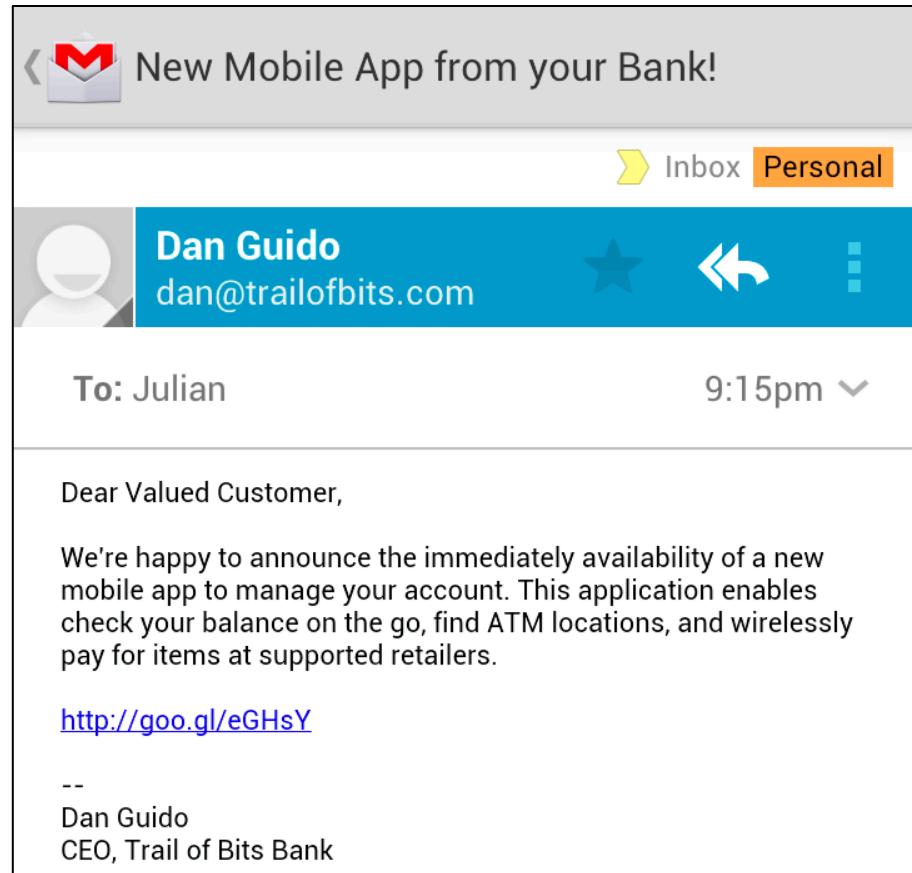
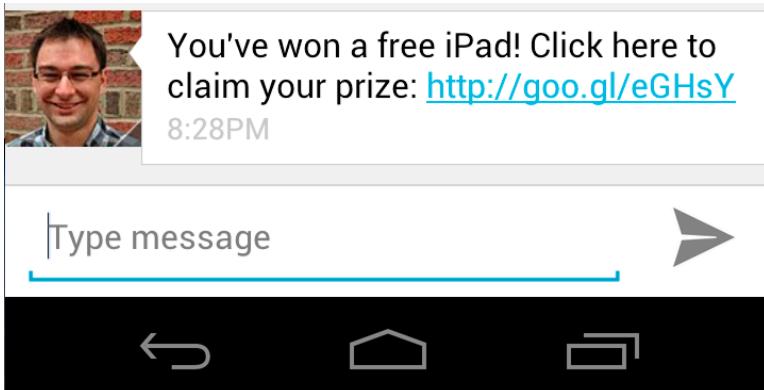
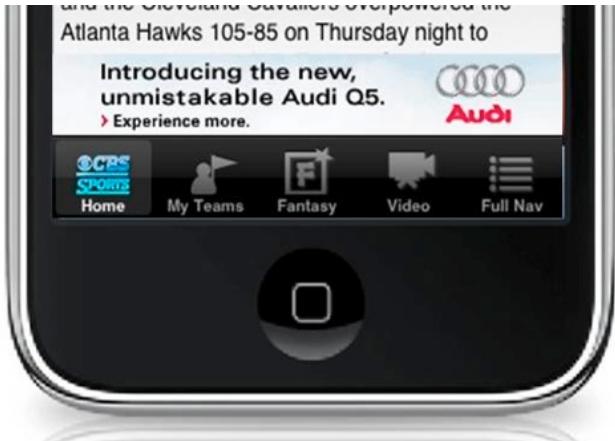
Optional: Add an expansion file

If your app exceeds the 50MB APK limit, you can add expansion files. [Learn more](#)



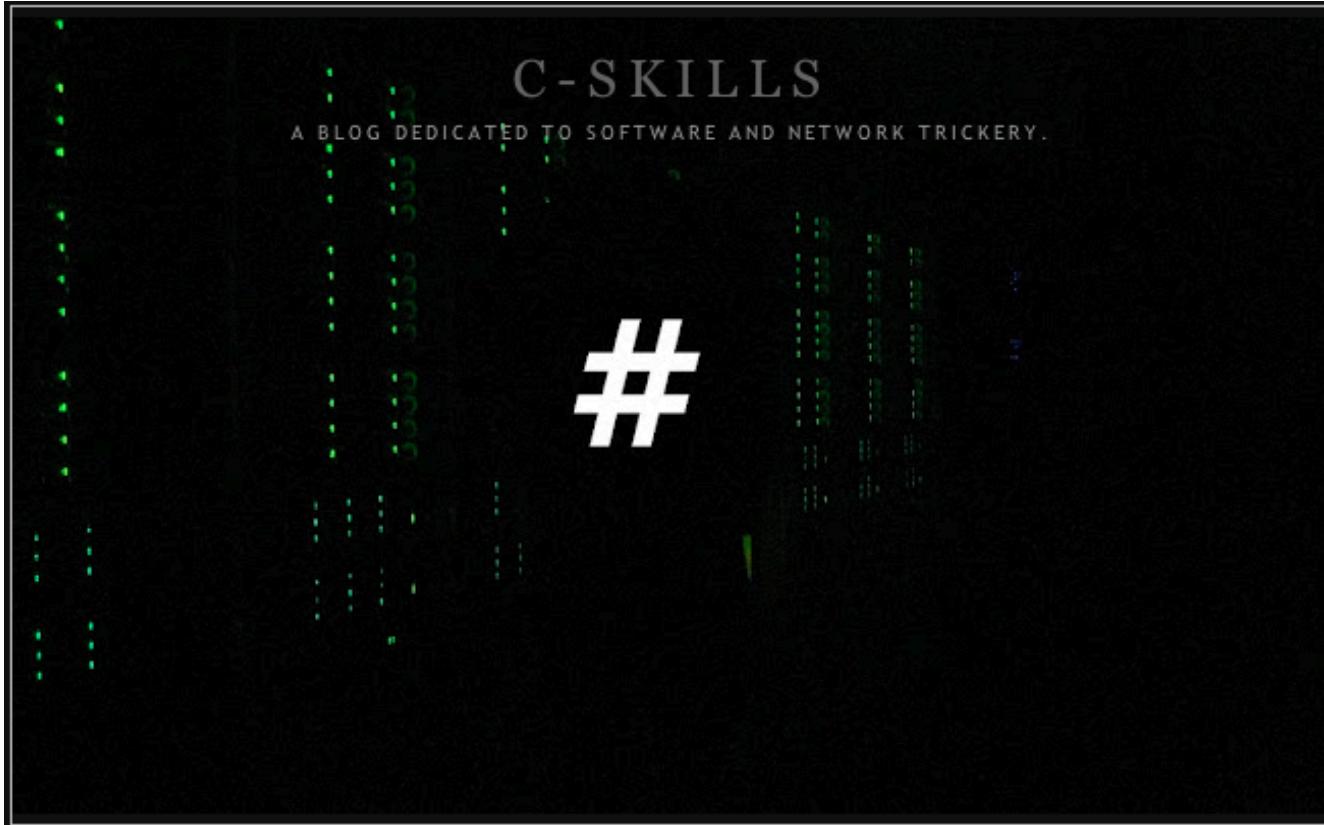
Upload the app somewhere victims can get it

Drive Installs



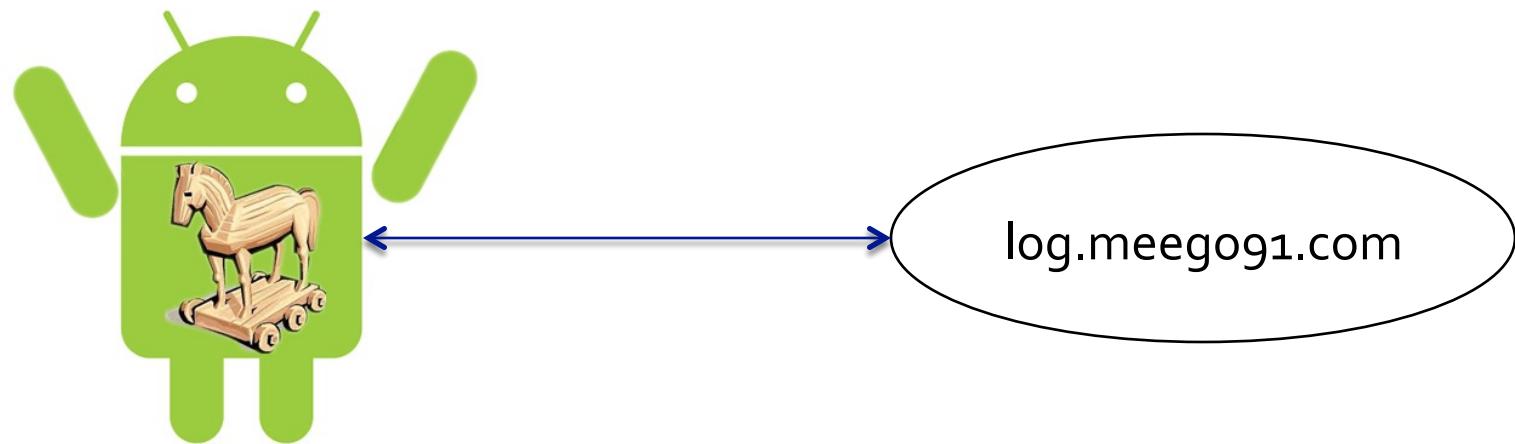
Use any method possible to increase # of installations

Escalate Privileges



Obtain the ability to collect valuable information

Establish Command & Control



Simple C&C corresponds with simplistic options for network monitoring

Perform Actions on Objectives

Credit Cards

A42786988000000000000	02/14	017	mtsheller	mtsheller	11094-A Broadway Rd	Chesapeake	VA	24062	00048427502	1 US	
A42786988000000000000	08/13	040	Blanca M Waring	Blanca M Waring	10000 3411 10000 3411	Local Government	OH	44439	1 800-400-		
S42632778800000000000	08/13	023	Lisa DeGalan	Lisa DeGalan	10000 Town Dr	Xenia	OH	45355	937-4222	1 US	
S42632778800000000000	08/13	023	Emily Flueghaar	Emily Flueghaar	8094-A SR 220B St	Beaumont	TX	77403	965-306-2611		
S43898502328887	08/13	022	John R. Ernst	John R. Ernst	911-3001 Potomac St.	East Beach	VA	24096	986-306-5458		
S43898502328887	08/13	022	Gatheryn Price	Gatheryn Price	7810 10th Street	Fort Knox	KY	40023	983-306-5458		
S43898502328887	08/13	022	John R. Ernst	John R. Ernst	911-3001 Potomac St.	East Beach	VA	24096	986-306-5458		
S43898502328887	08/13	022	William McAllister	William McAllister	7 Mount Vernon St	Basingstoke	WI	01867	979-326-5902		
S44082778800000000000	08/13	085	Janice Baker	Janice Baker	2001 Newport Wings	IA	50164	51533051602	1 US		
S44138483000000000000	08/13	096	Debra Jones	Debra Jones	1002 6th Street	Carroll City	VA	48813	5157-308-		
S44448187319113	08/13	033	Michael Bellinger	Michael Bellinger	53 10th Street	Hornbeam Woods	PA	15802	2132464233	1 US	
S44448187319113	08/13	033	Heather Armstrong	Heather Armstrong	1525A N Vibra St.	Seattle	WA	98103	2090542379	1 US	
S45066888000000000000	08/13	025	Richard S Lolley	Richard S Lolley	0052 Vincent Hill Rd	Conondale	NY	14424	585-257-		
S45066888000000000000	08/13	025	Volando Sanchez	Volando Sanchez	548 Millford Road	Rochester	NY	14622	585-054-9888		
S45066888000000000000	08/13	025	John P. Gaskins	John P. Gaskins	10000 3411 10000 3411	Wethersfield	CT	06519	873-937-7975		
S45066888000000000000	08/13	025	James Kyle	James Kyle	1330 N Human River Dr	Ypsilanti	MI	48197	734-437-4488		
S45066888000000000000	08/13	025	Theresa Bennett	Theresa Bennett	1790 Pittner Ave	North Tonawanda	NY	14208	736-799-		
Name (check me) number : +852-2425-4933											
exp date : 11-2011 address : HKS 988 Hong Kong Flat 8 13/F Grand Fortune Mansion address : 1, 1 Davis Street, Kennedy Town phone number : 852-2425-4933											
Machado Hans-Eberhard number : +852-2265-0487 exp date : 09/2012 address : HK 988 Hong Kong Room 1506-20, address : 15/F, Non Fung Coop, Centre, 18 Luk Luk Street phone number : 852-2425-4933											

Total City Group

How site works?

- Post and track your vacancies, RFPs and projects
- Find affordable freelancers or full-time staff
- Get work done below budget and make profit

Authorization

Login: Password:

Registration | Forget password?

Payment Processing Assistant, Tier 2

AVAILABILITY

Location: Nationwide, USA, Canada (This vacancy is open to legal residents of the USA and Canada ONLY)

Status: Open

Employee Type: Part-Time, Full Time opportunities available upon request

Number of employees required: 3

Candidate Requirements:

- 18 years old and have the legal right to work within the USA
- internet access (broadband preferred)
- availability by phone
- Business/Corporate bank account with good bank history
- no criminal offense or convictions

view more

Latest projects

YouTube cc dumps Search results for cc dumps About 496 results

Search options

FRESH credit, card ,dumps, fullz
bank logins,lod bank transfers, Western union transfers an very good price, prices are not NEGOTIABLE, you can contact VIA EMAIL: Hackerss ...
by credkingdom1234 2 years ago 7,831 views

HD

sell dumps credit dumps dumps credit card
credit card dumps sell dumps credit dumps
by sellcdumps 1 year ago 805 views

3:05

Credit card dumper, Track 1 and 2 USA / UK / EU 100 ...
Credit card dumper, Track 1 and 2 USA / UK / EU 100% Fresh skimmed Visa, MasterCard, Amex MSR200 Selling quality CC dumper. Don't get ripped off by ...
by ukDumpsSeller 6 months ago 1,573 views

2:15

Bank Logins and Credit card dumps available !!!!!!! ...
Full CCs, Bank dumps and logins.
by cyborgcheng 2 months ago 198 views

1:25

Bank of America.

Golden Dump

News Resellers Dumps Plastics Checker IDs Rules

648550874 goldendump-service@rambler.ru

GD SAYS ...

Prices

Stuff types	For resellers	WITH replacements	WITHOUT replacements
USA Visa/MC Classic/Standart	\$18	\$30	\$22
USA Visa/MC Gold/Premier/Platinum	\$20	\$35	\$25

Gangsta Bucks.com

Home Conditions Tariffs Contacts Registration

Our tariffs (for 1000 installs):

Tariffs may change:
US \$ 1005

PINBAW Publisher Network. Helping Publishers Make Money Every Day

Content Programs

Advertising Referral

Add our free content to your website and we'll pay you up to \$1.45 for each new user who installs one of our banners to access it.

Get free content on your website in 4 easy steps:

- Choose the type of content you want to offer: videos, games, screensavers, emoticons, skins, etc.
- Browse our ever-growing content catalog and choose the best feed for your site.
- Display the content on your website with our easy-to-use code, or by simply linking to our content via a URL.
- Get paid every time a new user accesses the content.

INSTALL RATES

Tier Countries	Tier 1	Tier 2	Tier 3
1 United States, United Kingdom	\$0.75	\$0.40	\$0.10
2 Canada, France, Germany, Netherlands	\$1.00	\$0.53	\$0.15
3 Australia, Austria, Belgium, Denmark, Finland, Ireland, Italy, New Zealand, Norway, Portugal, Spain, Sweden, Switzerland	\$1.13	\$0.59	\$0.18
4 20,001 to 40,000	\$1.21	\$0.63	\$0.19
5 40,001 to 60,000	\$1.29	\$0.67	\$0.21
6 60,001 to 100,000	\$1.37	\$0.71	\$0.22
over 100,000	\$1.45	\$0.75	\$0.24

APPLY NOW

GD says ...

GD SAYS ...

GD SAYS ...

Abuse collected data

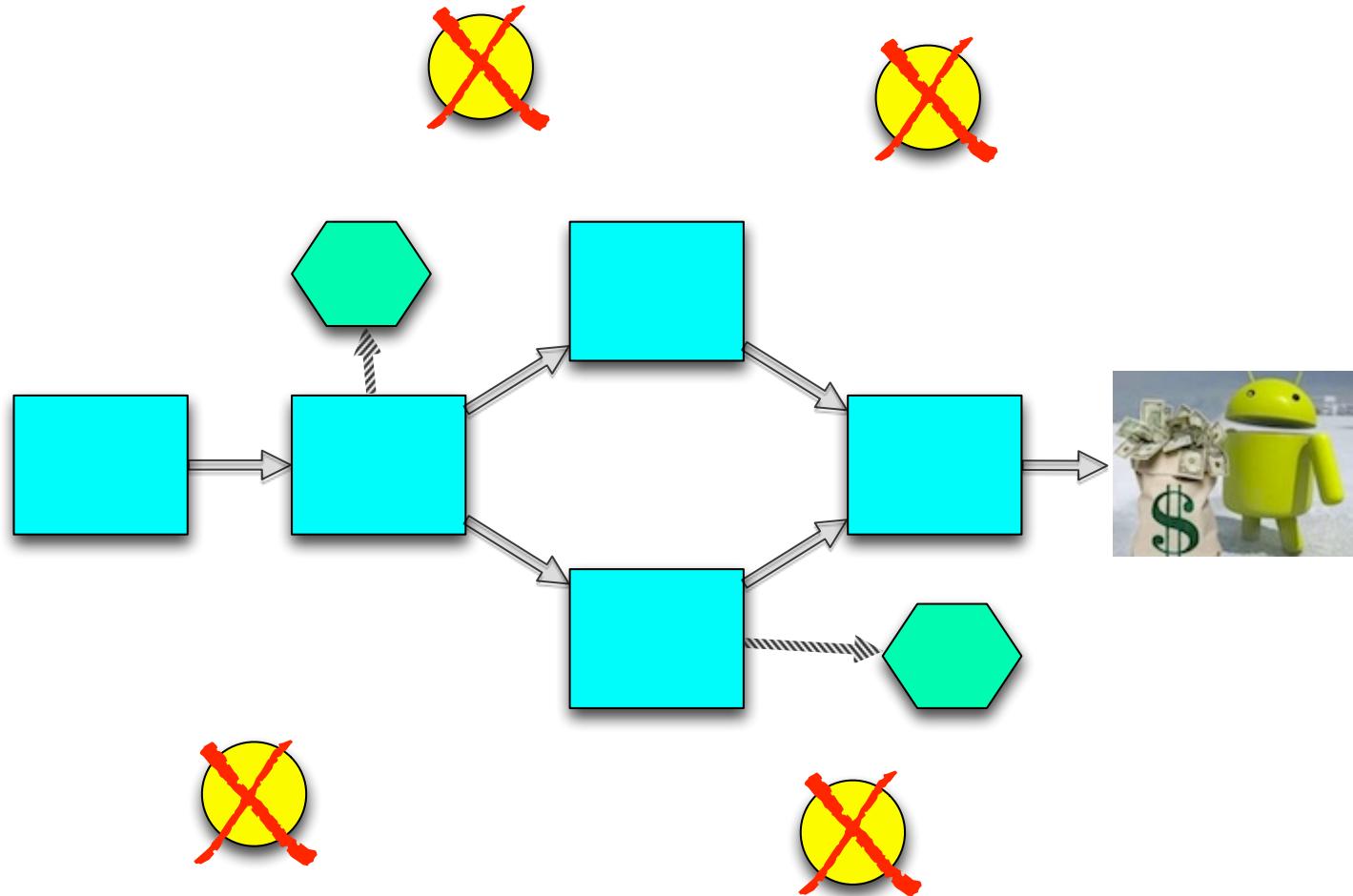
Leads to Cyber Pompeii



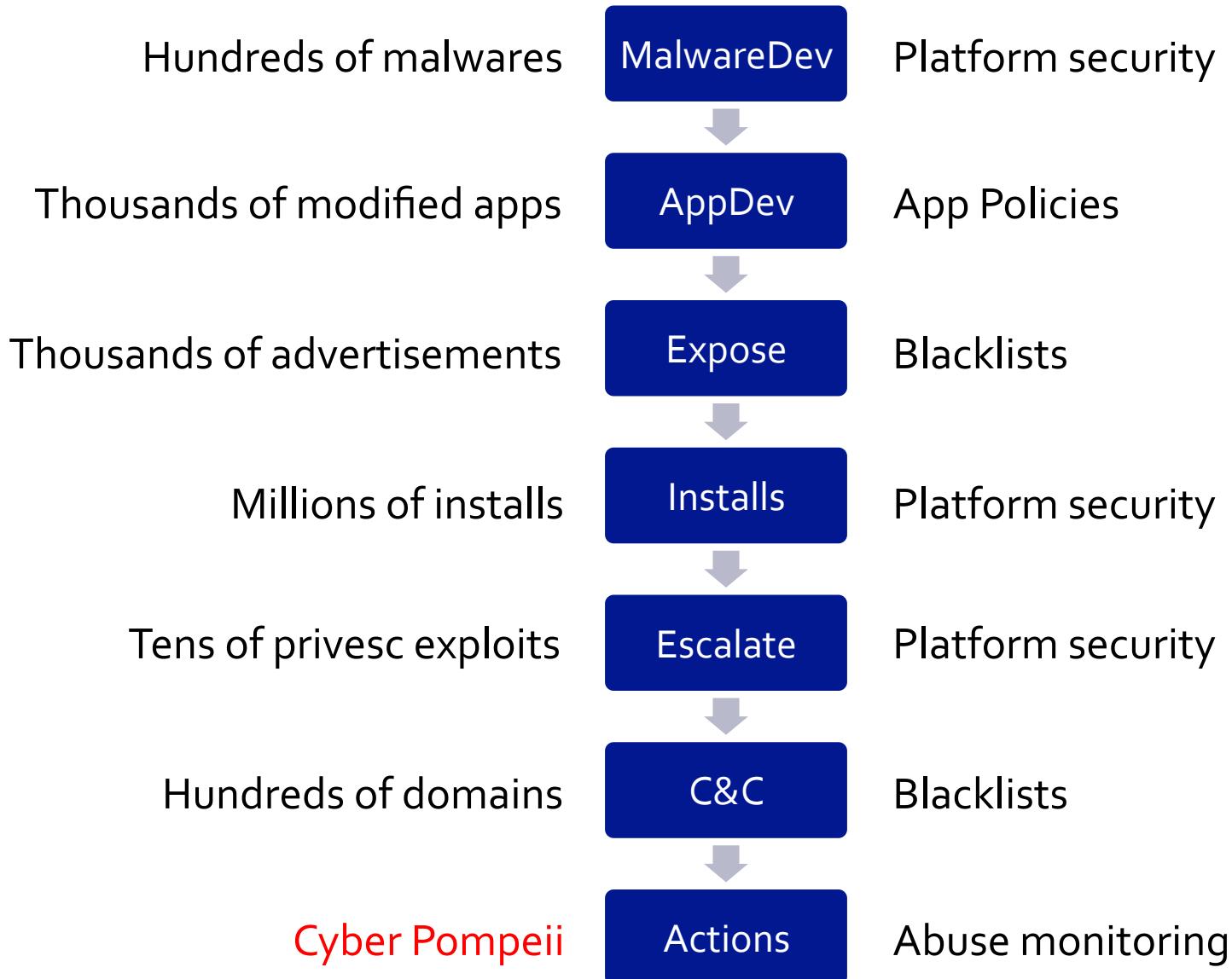
Intrusion Kill Chains

- Systematic process that an intrusion must follow
 - Deficiency in one step will disrupt the process
- Evolves response beyond point of compromise
 - Prevents myopic focus on vulnerabilities or malware
 - Identifies attacker reuse of tools and infrastructure
- Guides our analysis and implementation of defenses
 - Align defenses to specific processes an attacker takes
 - Force attackers to make difficult strategic adjustments

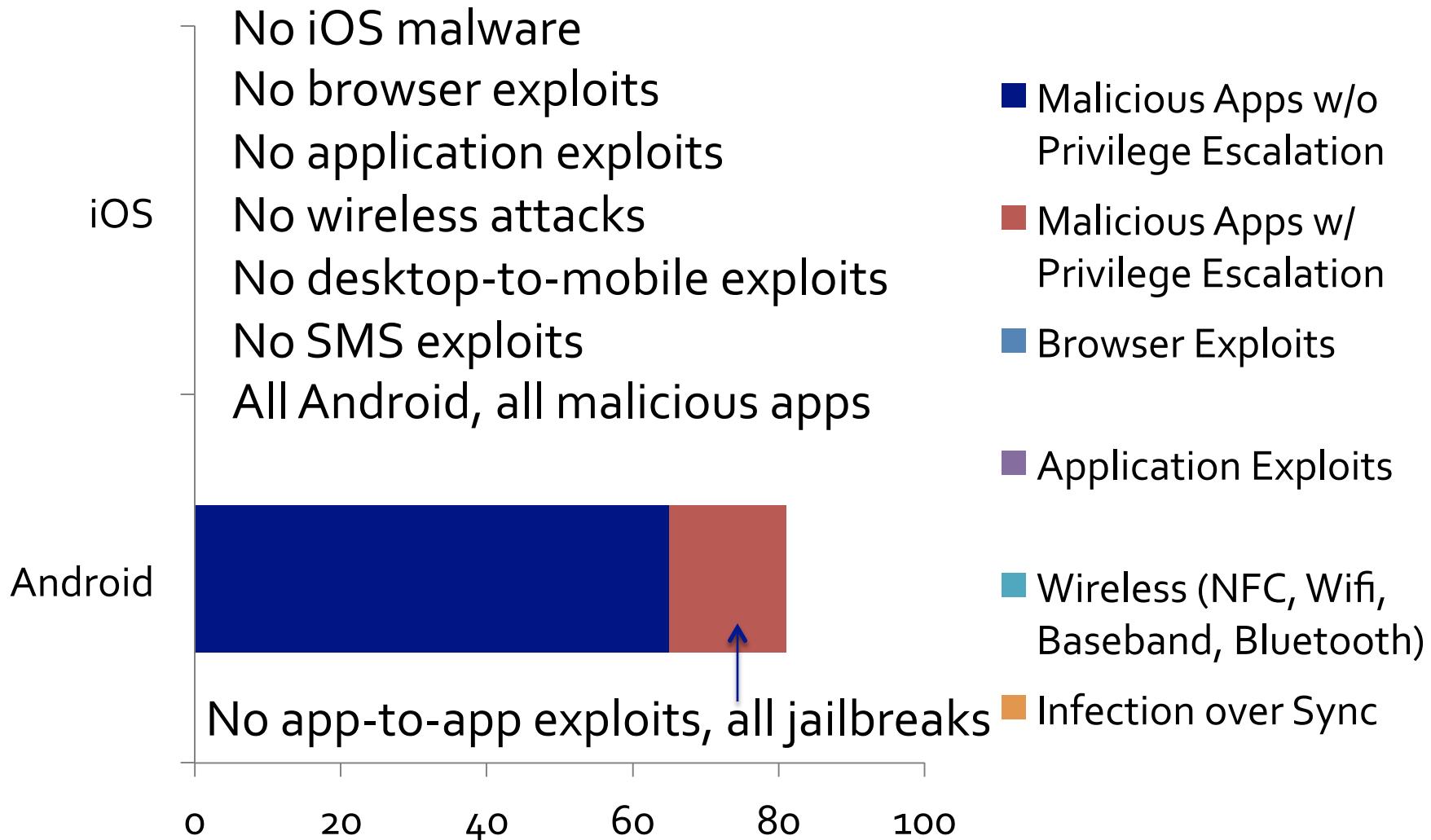
Kill Chains = Scalable Attack Strategies



Mobile Kill Chain Overview



Malware per Platform & Vector



Economics in Practice

Not how it works →



mikko

@dakami Imagine the best hackers you know - spending their time just creating malware and trying to find ways to bypass protection systems.



mikko

@dakami It's not simple because some of the attackers are so good.



mikko

@dakami Security experts who do not work with malware tend to dismiss it as a simple problem. It's not.



mikko

@dakami @wimremes Malware newbies and hobbyists and so? Sure. But professionals create the majority of malware.



mikko

@wimremes @dakami Answer: probably, no.

Do not underestimate the malware gangs. They have the budget and the resources to play this game.

22 hours

22 hours

22 hours

22 hours

23 hours

Discrepancies

- Is the security industry lying to us?
 - Assumptions that mobile threat == desktop threat
 - Fascination with new attack vectors
 - Myopic focus on ease of attack and malware
- We have no idea how attackers actually work
 - Always more possibilities than probable attacks
 - Attacker economics are different on mobile
- Use economics and adversarial characterization!
 - Why don't we / why won't we see certain attacks?

Where are Mobile Drive-Bys?



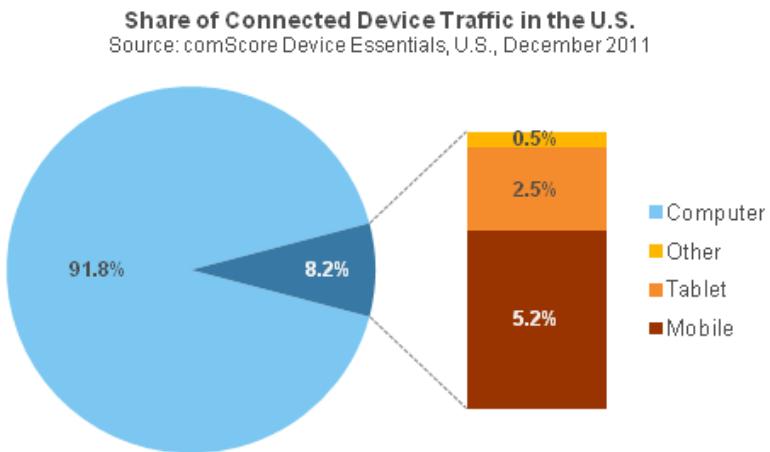
Mobile Town



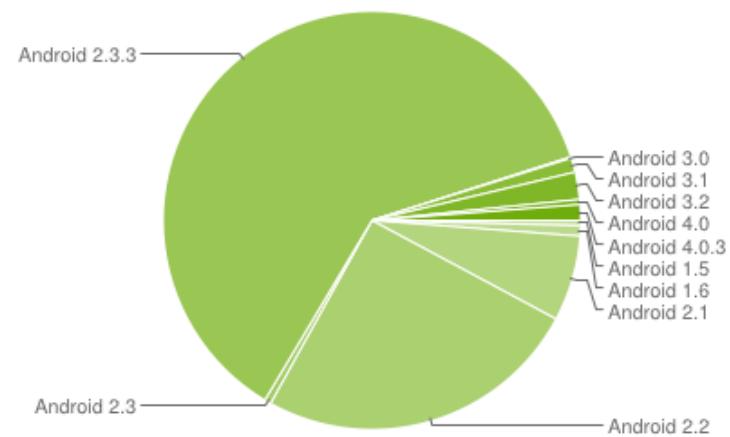
Desktop City

ING SEYF S0543 [RF] © www.visualphotos.com

Mobile Web Browsing



~8% of total web traffic
comes from mobile devices

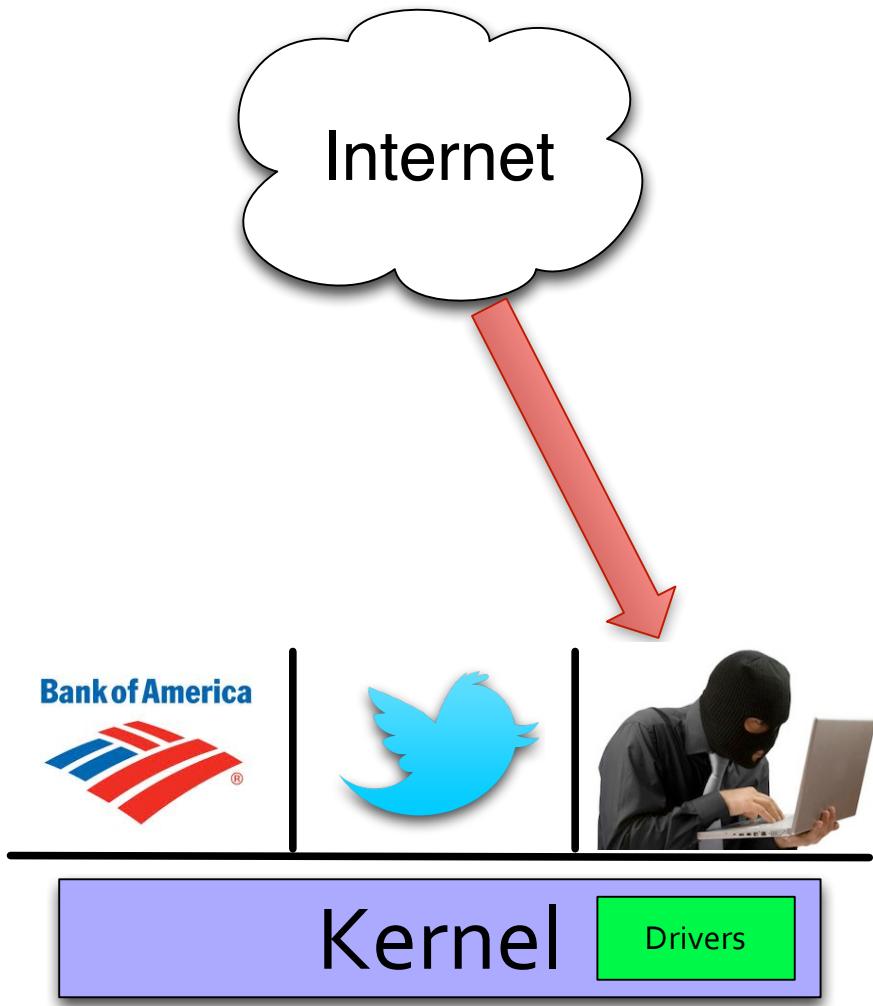


Breakdown by version / features
(+ varying rates of feature support)

Mobile websites might not have any ads!



Browser Exploit Walkthrough



Browser Permissions

- .INTERNET
- .ACCESS_FINE_LOCATION
- .ACCESS_COARSE_LOCATION
- .ACCESS_FINE_LOCATION
- .ACCESS_DOWNLOAD_MANAGER
- .ACCESS_NETWORK_STATE
- .ACCESS_WIFI_STATE
- .SET_WALLPAPER
- .WAKE_LOCK
- .WRITE_EXTERNAL_STORAGE
- .SEND_DOWNLOAD_COMPLETED_INTENTS

Mobile Drive-by Takeaway

- 10-20x less potential targets than desktops
 - Not many mobile browsers, split between platforms
 - Mobile websites commonly won't have ads
- Increased costs to exploit relative to desktops
 - Feature disparities, in particular flash support
 - Multiple exploits required for browser + jailbreak
 - However, may be able to achieve anonymity easily
- Possible, but incentives are stacked against it
 - *Zero* identified cases in the data
 - Might change if potential revenue rises dramatically

Why attack individual Apps when even the browser isn't viable yet?

Vendor App Stores

Incentives	Browser Exploits	Malicious Apps
# of Targets	Minimal	All Devices (300 mil+)
Ability to Target	Ads	App Store SEO, Lures
Ease of Exploit	Multiple Exploits	Single Exploit
Enforcement	Anonymous	Anonymous?

App stores look like a great value proposition!

App Submission Process

Process	iOS App Store	Google Play
Sign Up	Minimal Cost	Minimal Cost
Identification	Identify Verified	Anonymity Acceptable
App Review	Static Analysis	Dynamic Analysis
Platform Characteristics	No runtime modification	Runtime modification

Apple knows who you are and has seen all your code

Malicious App Submission Process

- In order to submit a malicious iOS app:
 1. Create a believable false identity or risk arrest
 2. Pass a manual content review for originality
 3. Package your sophisticated exploit for Apple's review
- In order to submit a malicious Android app:
 1. Put fake developer information into a form online
 2. Avoid malicious activity until after Bouncer runs it
 - a. Package inside app -> wait two weeks to activate
 - b. Package outside app -> download code at runtime / update

Exceptions to Apple Review

- Self-modifying code is difficult, but possible on iOS
 - Since it's disallowed, it sticks out in the review process
 - No matter what: APPLE KNOWS WHO YOU ARE
- Let's look at what happened with Charlie Miller
 - App taken down, removed from phones, Charlie banned
 - If he did anything malicious, he could have gone to jail
- From another angle: Why wasn't it immediately abused?
 - Real-world verification trumps all technical attacks
 - Apple patched in *4 days*, reducing potential revenue
 - Charlie didn't discuss until after patch, no PoC code

Malicious App Campaigns

0

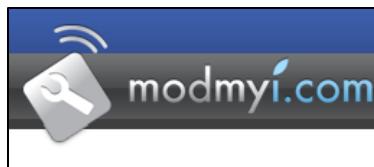
Apple App Store

30

Google Marketplace

“Say what you will about police states, but they have very little crime.”

3rd Party App Stores



- Are 3rd party app stores as attractive to abuse?
 - <10% of total devices*, use is split between markets
 - In strange reversal, 3rd parties may dominate in China
- The cost of exploitation needs to be very low
 - For iOS, access to 3rd party means device is jailbroken
 - Ability to review apps increases with size

* <http://www.wired.com/gadgetlab/2009/08/cydia-app-store/>

Malicious App Campaigns (3rd Parties)

20

US-based 3rd Party

32

Chinese 3rd Party

Abuse of 3rd party markets is happening *now* (but still only on Android)

Privilege Escalation Exploits

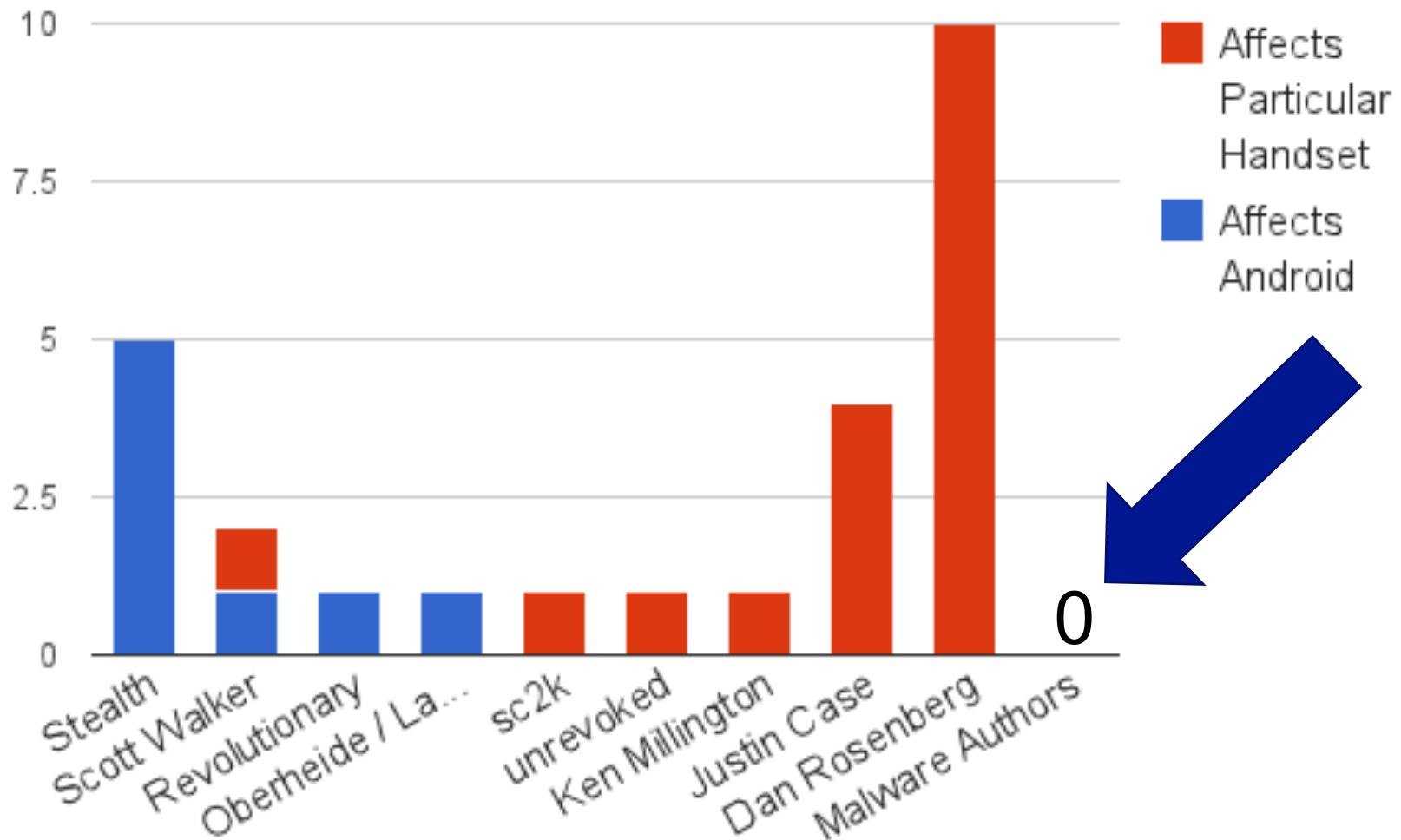
If I just had a jailbreak, then I could make money...

Jailbreak == Free Exploit

- Both platforms have active jailbreaker communities
 - Android: 26 jailbreaks from 10 different authors
 - iOS: 25 jailbreaks from ~4 main groups
- Jailbreaker behavior mimics attacker behavior
 - Want cheapest possible jailbreak & most possible use
 - Choose target attack surfaces for maximum return
 - Boot ROM (unpatchable) vs. iOS (quickly patchable)

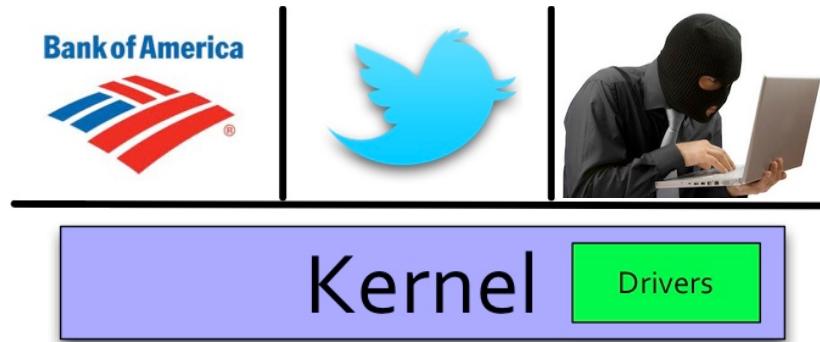
“My Gingerbreak works, but I wont release it before a couple of devices are in the wild so the issue is not fixed before it can become useful.” -- stealth (prior to releasing Gingerbreak)
<http://goo.gl/azzOh>

Android Jailbreak Dev by Target



What we want to know:
Which exploits get used by malware and why?

Android Escalation Scenarios



I got you to install my app
Now what?

Scenario	Cost of Attack	Value of Data	# of Targets
Universal JB	Free	High (all data)	High (all)
Request SMS	Free	High (2FA)	Medium (some)
Handset-specific	Limited Availability	High (all data)	Limited
App-to-App	Limited Availability	Low (limited data)	Limited

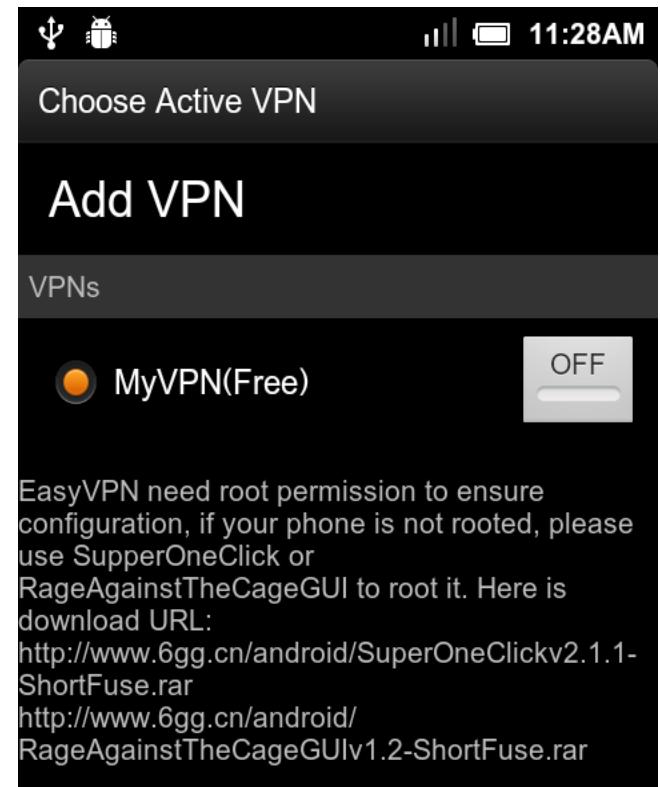
App-to-App and Handset-specific exploits have similar incentives: neither are used

Universal Android Exploits

Exploit Name	Last Affected Version	Abused?
Exploid	2.1 (Éclair)	Malware
RageAgainstTheCage	2.2.1 (Froyo)	Malware
Zimperlich	2.2.1 (Froyo)	No
KillingInTheNameOf	2.2.2 (Froyo)	No
Psneuter	2.2.2 (Froyo)	No
GingerBreak	2.3.4 (GingerBread)	Malware
zergRush	2.3.5 (GingerBread)	No
Levitator	2.3.5 (GingerBread)	No (Low # of Devices)
mempodroid	4.0.3 (ICS)	No

Android Jailbreak Equivalents

- Android Private Signing Keys
 - jSMSHider: <http://goo.gl/vPzjq>
 - Affects custom ROMs only
- Have the user do it (no joke) ----->
 - Lena: <http://goo.gl/eiTBA>
- Request Device Admin API Priviliges
 - DroidLive: <http://goo.gl/c3EET>
 - Android 2.2+
- All these techniques observed in-use by actual malware
- They're less effective (user interaction), less used, but still work

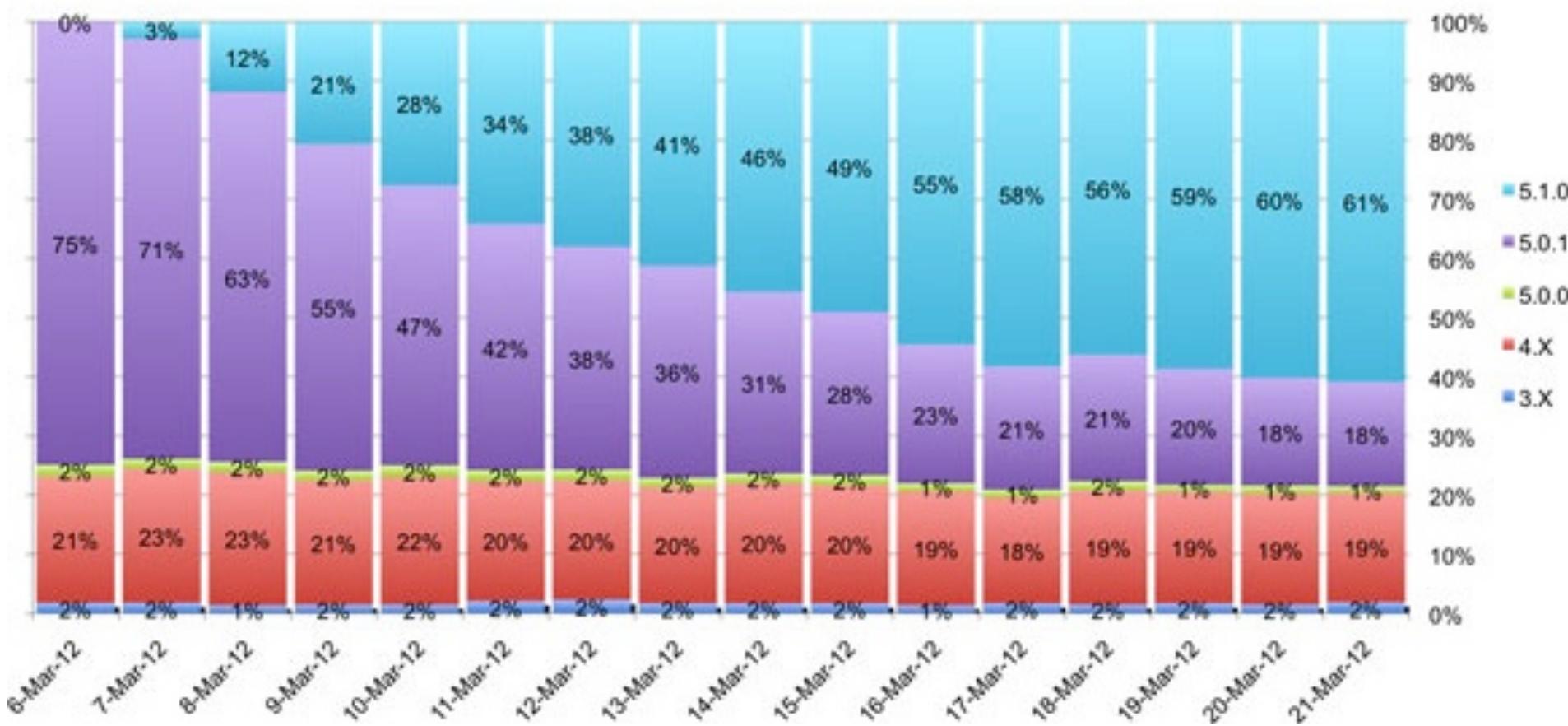


Android Maximizes Potential Revenue

Platform	Codename	03/12/2012	4/18/2012
1.x	Cupcake / Donut	1.2%	1.0%
2.1	Eclair	6.6%	6.0%
2.2	Froyo	25.3%	23.1%
2.3.0 - 2.3.2	Gingerbread	0.5%	0.5%
2.3.3 – 2.3.7	Gingerbread	61.5%	63.2%
3.x	Honeycomb	3.3%	3.3%
4.x	Ice Cream Sandwich	1.6%	2.9%

Android Exploit	Time to Patch 50%
Exploid (2.1)	294 days
RageAgainstTheCage (2.2.1)	> 240 days

iOS Limits Potential Revenue



iOS Limits Potential Revenue

Exploit	Jailbreak	Patch Availability
Malformed CFF	Star (JailbreakMe 2.0)	10 days
T1 Font Integer Overflow	Saffron (JailbreakMe 3.0)	9 days
mmap Logic Flaw	Charlie Miller	4 days (30d Apple headstart)

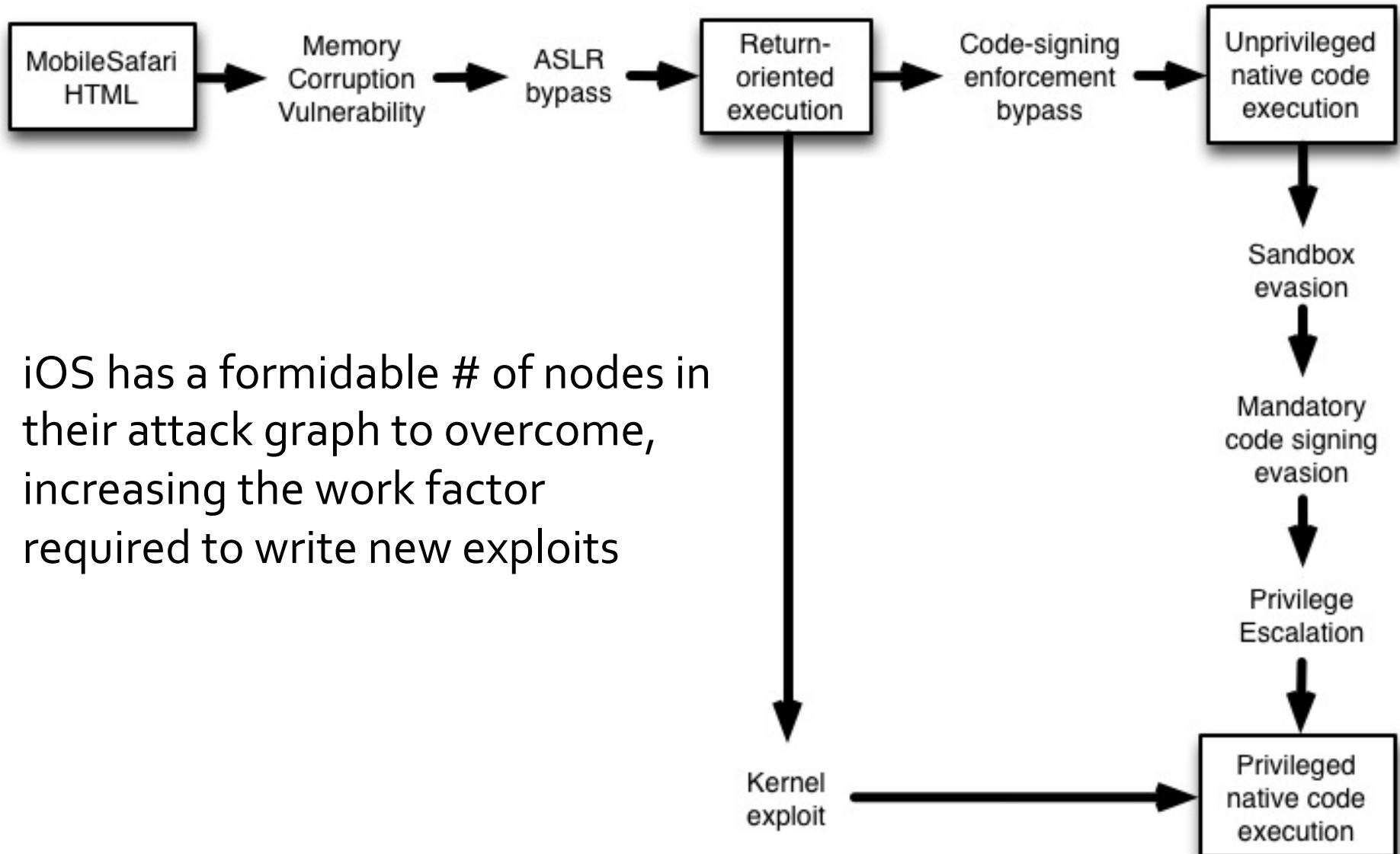
Apple quickly patches Jailbreaks that would be useful in malicious attacks

Android Minimizes Cost of Attack

Mitigation	iOS	Android
Code Injection	Code Signing	No-eXecute
Randomization	Strong ASLR	Incomplete ASLR
Sandbox	Seatbelt	None
Patch Information	Available	Not Available

- Code Signing is significantly stronger than NX (Partial vs Full ROP)
- Android app permissions have no effect on privilege escalation exploits
- Google does not track exploited vulnerabilities (CVEs) on Android

iOS Maximizes Cost of Attack

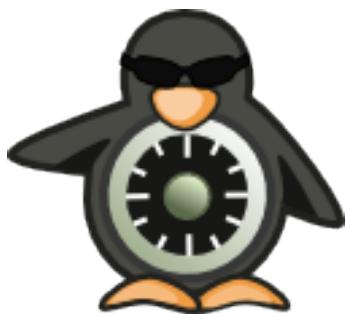


Privilege Escalation Takeaways

- Malware authors have no ability to write exploits
 - The only exploits abused are public jailbreak exploits
- Google has not done anything to address jailbreaks
 - No attempt to mitigate them in the OS via sandbox
 - They don't track vulnerabilities that allow them
 - Platform is filled with alternate escalation scenarios
- Android patches have no effect on problem
 - Google has no ability to force carriers / OEMs to react
 - Even if they could, it's too easy to write new exploits

Effective Responses

Android Mitigation Outlook



- Chrome for Android
 - Makes browser exploits hard
 - Not an exploited vector now
 - No effect on current Android malware
- SEAndroid
 - Kills userspace jailbreaks, but not kernel!
 - Jailbreakers delayed, will have to retool
 - What handsets will use it?
- ASLR in Ice Cream Sandwich 4.x
 - Little to no effect on privilege escalations
 - Useful to make browser exploits difficult
 - Can't help 300+ million existing devices

App Development Strategies

- Not all Keychain APIs are created equal
 - Keychain only in Android 4.0+ (2.9% of users)
 - Android only stores keys. No keygen, no data storage.
 - Successful jailbreaks means total exposure
 - Contrast with HW-backed iOS Data Protection API*
- Limit accessible data and implement a circuit breaker
 - Apps shouldn't request an entire DB of content
 - Circuit Breaker: cut off access after a threshold
 - Mobile users should only download data that mobile devices can actually read

* <http://www.trailofbits.com/resources/#ios-eval>

Enterprise BYOD Strategies

- Mobile groupware must follow app security strategy
 - Limit accessible data, implement a circuit breaker
 - Ask your vendor these questions!
- Assume that BYOD devices are compromised
 - Less likely on iOS, a certainty on Android
 - Existing jailbreak detection is fallible
 - Malicious attackers aren't connecting to Cydia
- If Android users can install their own apps, they will be compromised by accident
 - Restrict access to internal App Catalogue if possible

Conclusions

- Attackers carefully balance incentives w/ strategy
 - Not all attack vectors will be explored maliciously
 - Intel-driven approach: concrete results from concrete data
- Android will continue to be compromised
 - Bouncer, Chrome, ASLR have limited impact
 - No mitigations to slow jailbreaks, no ability to react
- iOS will steer clear of similar attacks for now
 - Real-world verification trumps all the technical attacks
 - Mitigations slow jailbreaking, reacting quick reduces value

References

- Attacker Math 101, Dino Dai Zovi
 - www.trailofbits.com/research/#attackermath
- iOS Security Evaluation, Dino Dai Zovi
 - www.trailofbits.com/research/#ios-eval
- Exploit Intelligence Project, Dan Guido
 - www.trailofbits.com/research/#eip
- Lookout Security Mobile Threat Report
 - <https://www.mylookout.com/mobile-threat-report>
- Contagio Mini Dump
 - <http://contagiominidump.blogspot.com/>

References

- Don't Root Robots, Jon Oberheide
 - <http://goo.gl/A5XmR>
- A look at ASLR in Android ICS, Jon Oberheide
 - <http://goo.gl/F8Bjl>
- The Case for SEAndroid, Stephen Smalley
 - <http://goo.gl/KIQm6>
- Practical Android Attacks, Bas Alberts and M. Oldani
 - <http://goo.gl/BwkLA>
- Android Malware from Xuxian Jiang @ NC State
 - <http://www.csc.ncsu.edu/faculty/jiang/>
- Androguard, Anthony Desnos
 - <https://code.google.com/p/androguard/>

Leftovers

Mobile Ads



Anonymous



ID Verified

Low Cost



\$300k min

Scriptable



HTML5

High Traffic



Low interest from legit advertisers



Anonymous



\$50 min



Img / Text

Close Access

- Insecure Storage, NFC, Bluetooth, Wifi, Baseband
 - All require proximity or possession of device
- Attacks that require close access don't easily scale
 - Can someone think of one that does?
- Credit card skimmers!
- Why are skimmers abused?
 - Magstripes are ubiquitous
 - Skimmers are dirt cheap
 - They have access to data I want



Close Access

- Issues for abuse of mobile close access vector
 - NFC, Bluetooth, Wifi not as ubiquitous as magstripes
 - May not allow collection of data or grant access that I want
- Cost of exploitation not dirt cheap or commoditized yet
 - No ready-made close access tools available online yet
 - Baseband exploitation never likely to become cheap
 - Risk of arrest due to physical proximity is unchanged
- Zero cases of mass malware or fraudulent data collection through close access