Publishing Our Data

Adding more transparency in the ecosystem

Who Am I?

Jason Woloz

- Manage Anti-malware Program for [Google Play Protect]
- 15+ years in security industry

Agenda

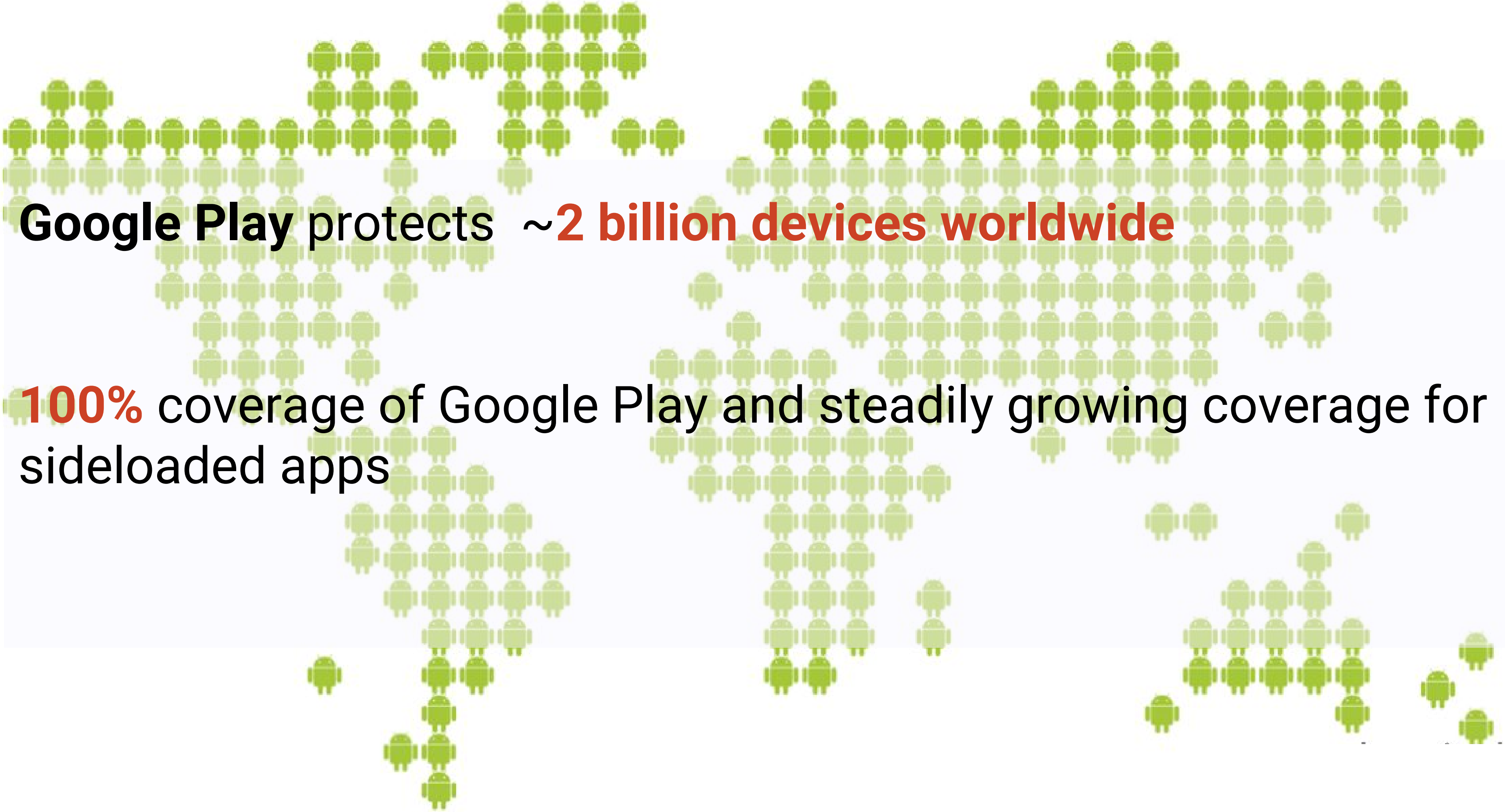
1 PHA in the ecosystem: Year to date

2 Device Cleanliness

3 Publishing our stats

Google Play Protect

PHA Stats



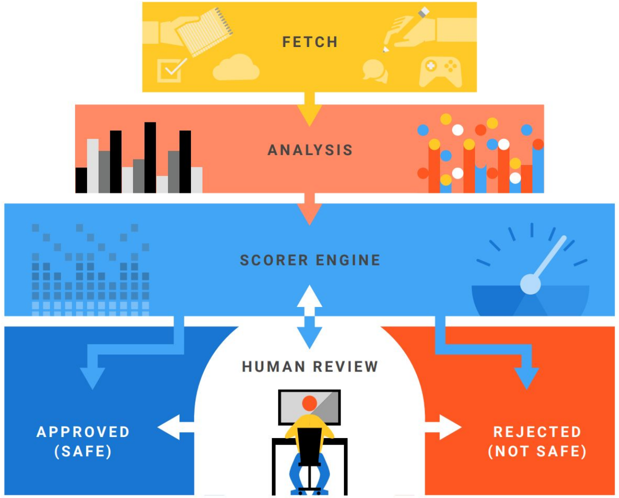
Google Play protects ~**2 billion devices worldwide**

100% coverage of Google Play and steadily growing coverage for sideloaded apps

Google Play
Protect

First a refresher

- Backdoors
- Commercial spyware
- Denial of service
- Hostile downloader
- Mobile billing fraud
  - Premium SMS
  - Call
  - Toll Fraud



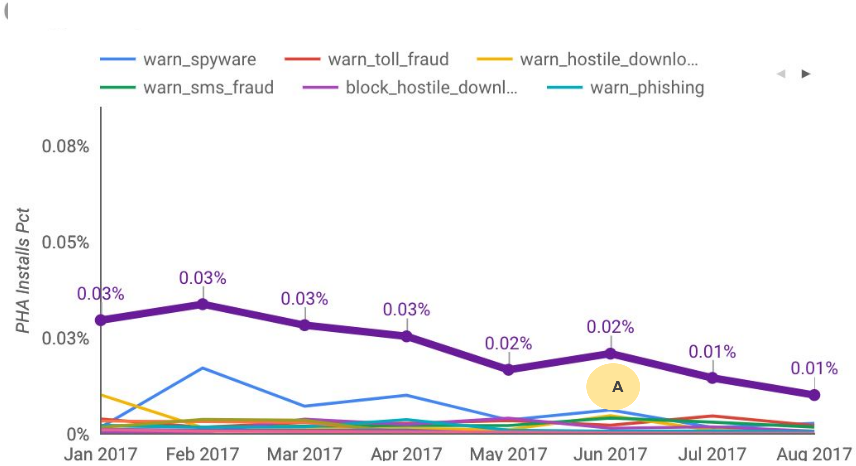
- Phishing
- Non-Android threat
- Privilege escalation
- Ransomware
- Rooting
- Spam
- Spyware
- Trojan

Google Play Protect

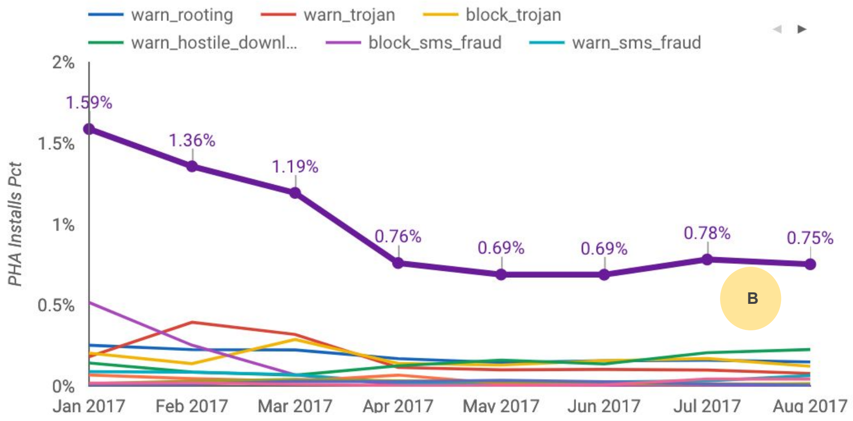
Detailed definition

PHA Installs Rate

Play



Sideloaded



PHA installs rate remains about 0.02% throughout 2017

A warn_spyware being the largest PHA category on Google Play.

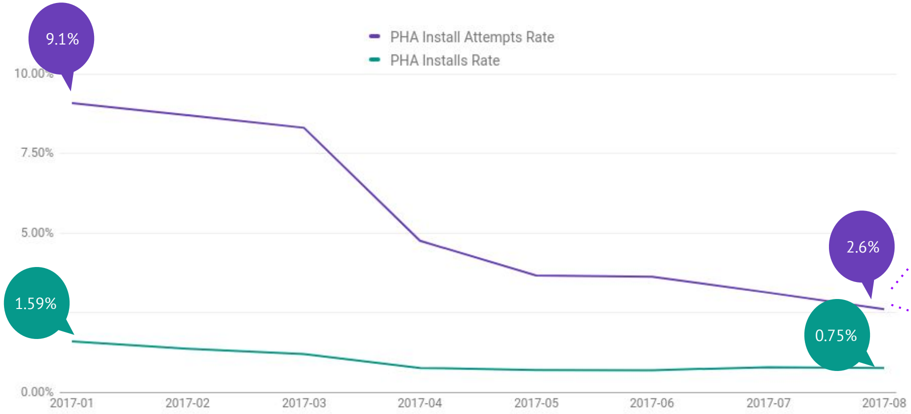
PHA installs rate declined by ~50% since start of 2017

B warn_hostile_downloader remains the top PHA outside of Google Play

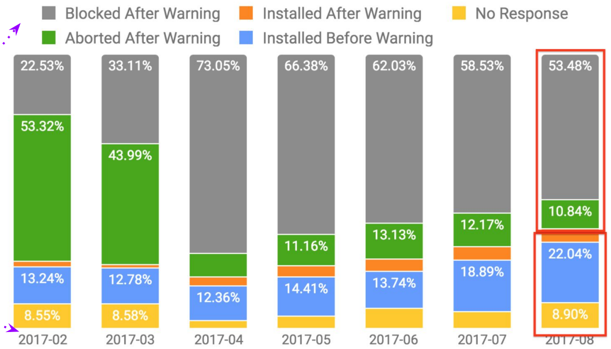
Google Play Protect

PHA Install Attempts by User Decisions (Sideloaded)

PHA Install Attempts vs. PHA Installs



By PHA Install Attempts by User Decision



- PHA install attempt rate in Sideloaded has a steady decline
  - Since the beginning of 2017 we have observed **a decrease of 66% in PHA install attempts outside Play**
- PHA install attempts by user decision
  - **65% of all PHA install attempts was successfully prevented in Aug** through blocking and warning that led users to abort installation
    - 54% were blocked; 11% were aborted after warning presentation
  - 35% was not successfully prevented from users choosing to install
    - 22% unwarned; 9% no response; 5% ignored warning

Insights

- Spyware, phishing and hostile downloaders are currently the most prevalent PHA across the Android ecosystem
- PHA installed from sideloaded sources is on a declining trend
- PHA installed from Play remains stable and low

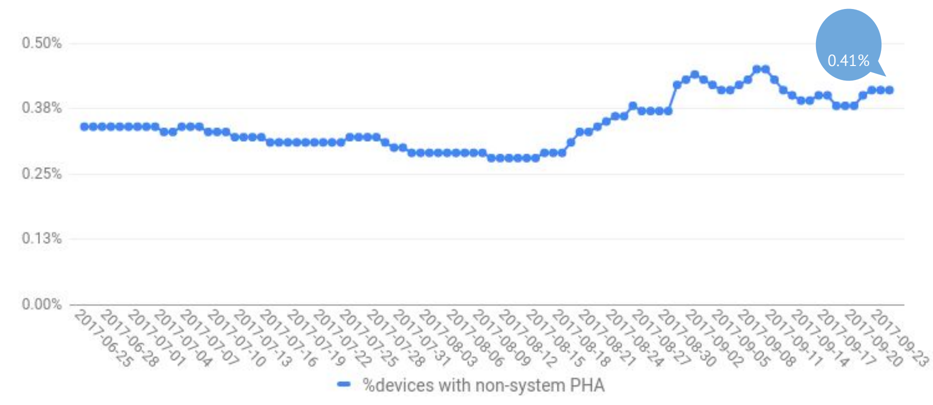
Device Cleanliness

What is a dirty device?

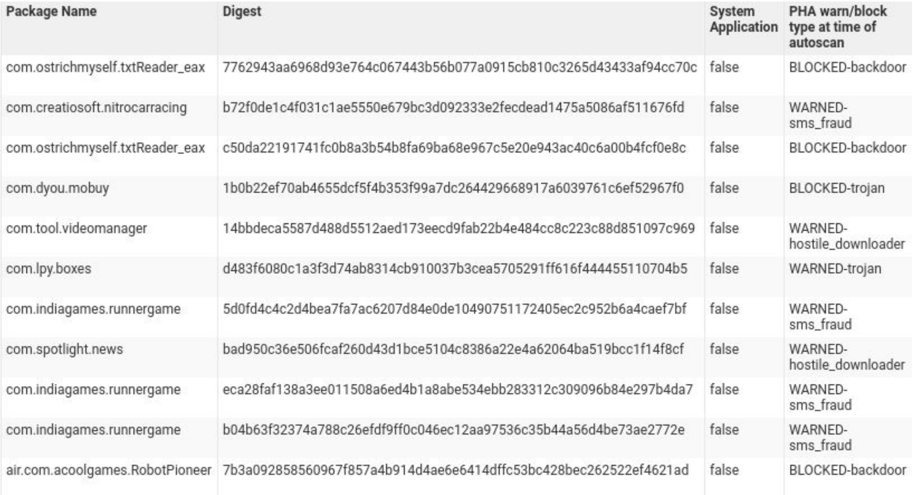
- % of devices with PHA at any given point in time are the devices that
    - have checked into our servers recently
    - **AND** have reported an installed PHA during the last check-in
    - **AND** have the PHA in an enabled state
    - **AND** the user hasn’t told us to stop warning on installed PHAs

Device Cleanliness- Non-system PHA

28DA Non-system PHA



Top PHA



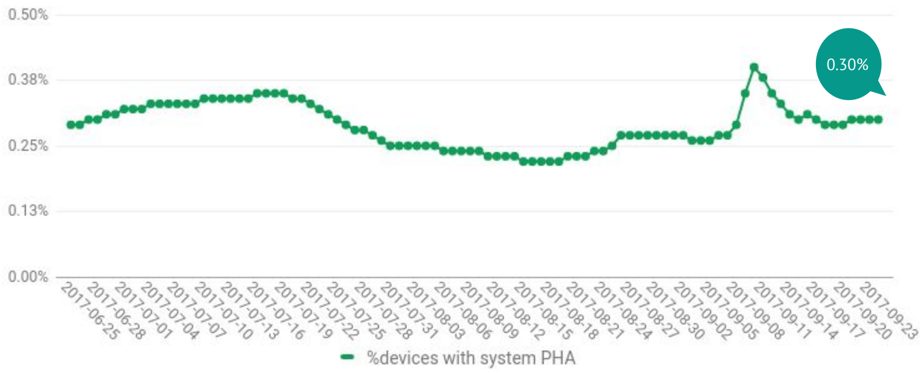
Package Name	Digest	System Application	PHA warn/block type at time of autoscan
com.ostrichmyself.txtReader_eax	7762943aa6968d93e764c067443b56b077a0915cb810c3265d43433af94cc70c	false	BLOCKED-backdoor
com.creatiosoft.nitrocarracing	b72f0de1c4f031c1ae5550e679bc3d092333e2fecdead1475a5086af511676fd	false	WARNED-sms_fraud
com.ostrichmyself.txtReader_eax	c50da22191741fc0b8a3b54b8fa69ba68e967c5e20e943ac40c6a00b4fcf0e8c	false	BLOCKED-backdoor
com.dyou.mobuy	1b0b22ef70ab4655dcf5f4b353f99a7dc264429668917a6039761c6ef52967f0	false	BLOCKED-trojan
com.tool.videomanager	14bbdeca5587d488d5512aed173eecd9fab22b4e484cc8c223c88d851097c969	false	WARNED-hostile_downloader
com.lpy.boxes	d483f6080c1a3f3d74ab8314cb910037b3cea5705291ff616f444455110704b5	false	WARNED-trojan
com.indiagames.runnergame	5d0fd4c4c2d4bea7fa7ac6207d84e0de10490751172405ec2c952b6a4caef7bf	false	WARNED-sms_fraud
com.spotlight.news	bad950c36e506fcaf260d43d1bce5104c8386a22e4a62064ba519bcc1f14f8cf	false	WARNED-hostile_downloader
com.indiagames.runnergame	eca28faf138a3ee011508a6ed4b1a8abe534ebb283312c309096b84e297b4da7	false	WARNED-sms_fraud
com.indiagames.runnergame	b04b63f32374a788c26efdf9ff0c046ec12aa97536c35b44a56d4be73ae2772e	false	WARNED-sms_fraud
air.com.acoolgames.RobotPioneer	7b3a092858560967f857a4b914d4ae6e6414dffc53bc428bec262522ef4621ad	false	BLOCKED-backdoor

- Fraction of devices with at least 1 non-system PHA is 0.41%

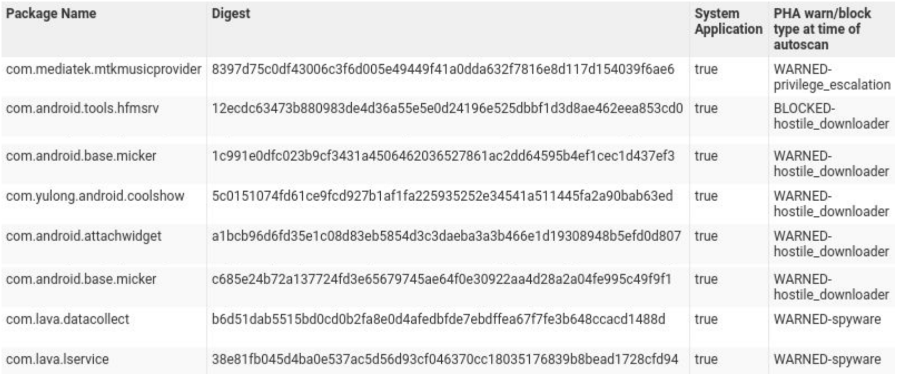
Google Play Protect

Device Cleanliness- System PHA

28DA System PHA



Top PHA



Package Name	Digest	System Application	PHA warn/block type at time of autoscan
com.mediatek.mtkmusicprovider	8397d75c0df43006c3f6d005e49449f41a0dda632f7816e8d117d154039f6ae6	true	WARNED-privilege_escalation
com.android.tools.hfmsrv	12ecdc63473b880983de4d36a55e5e0d24196e525dbbf1d3d8ae462eea853cd0	true	BLOCKED-hostile_downloader
com.android.base.micker	1c991e0dfc023b9cf3431a4506462036527861ac2dd64595b4ef1cec1d437ef3	true	WARNED-hostile_downloader
com.yulong.android.coolshow	5c0151074fd61ce9fcd927b1af1fa225935252e34541a511445fa2a90bab63ed	true	WARNED-hostile_downloader
com.android.attachwidget	a1bcb96d6fd35e1c08d83eb5854d3c3daeba3a3b466e1d19308948b5efd0d807	true	WARNED-hostile_downloader
com.android.base.micker	c685e24b72a137724fd3e65679745ae64f0e30922aa4d28a2a04fe995c49f9f1	true	WARNED-hostile_downloader
com.lava.datacollect	b6d51dab5515bd0cd0b2fa8e0d4afedbfde7ebdffea67f7fe3b648ccacd1488d	true	WARNED-spyware
com.lava.lservice	38e81fb045d4ba0e537ac5d56d93cf046370cc18035176839b8bead1728cfd94	true	WARNED-spyware

- Fraction of devices with at least one system PHA is 0.30%

Google Play
Protect

Whats are some of the challenges to device cleanliness?

- Devices with low bandwidth
- Offline installations
- Preinstalled PHA
- 3rd party OTA Apps
- Users that disregard warnings and notifications
- False negatives at time of install

Set a goal

Set a goal to reduce PHA on device by 75%!

But first

- Evaluate: are we measuring the best indicators
- Confirm: are user installed apps the biggest problem
- Self reflect: If users want the PHA apps; no judgement

Looking forward

We’ve improved cleanliness by ~30% and we still have the rest of 2017 to go!

- Increased investment in Machine Learning and automation to flag PHA
- Focus on improved detection on low bandwidth scenarios
- Increasing scope of our system image scanning program
- Disincentivizing app installer business models
- Renewed focus on impersonation apps and amputating preinstalled PHA functionality

Publishing the data

Collaborations

- We've collaborated on dozens of botnet takedowns and several hundred investigations in 2017 alone

Secret Back Door in Some U.S. Phones Sent Data to China,

点击查看本文中文版

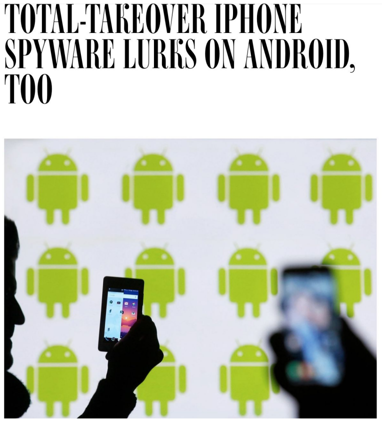
By MATT APUZZO and MICHAEL S. SCHMIDT NOV. 15, 2016

Fast-spreading CopyCat Android malware nicks pennies via pop-up ads

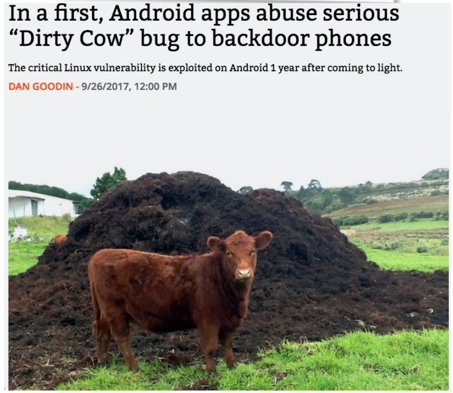
Miscreants rake in $1.5m, one annoying mobile pop-up ad at a time...

By John Leyden 7 Jul 2017 at 14:22 32 SHARE ▼

How a consortium of security professionals took down the WireX Android botnet



TOTAL-TAKEOVER IPHONE SPYWARE LURKS ON ANDROID, TOO



In a first, Android apps abuse serious "Dirty Cow" bug to backdoor phones

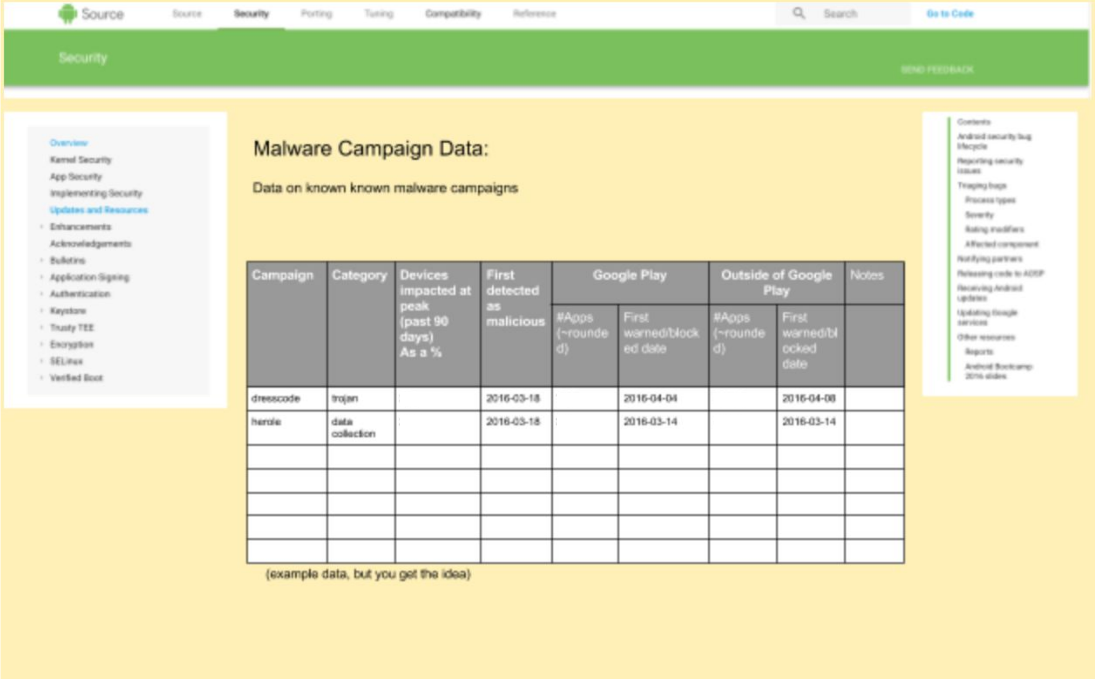
The critical Linux vulnerability is exploited on Android 1 year after coming to light.

DAN GOODIN - 9/26/2017, 12:00 PM

Google Play Protect

A new top 10 dashboard

- Publishing our top 10 families and stats
  - Campaign Description
  - Category
  - % of device impacted
  - Date first detected as PHA
  - # of apps
  - Date warned/blocked
  - Representative digests



Malware Campaign Data:

Data on known known malware campaigns

Campaign	Category	Devices impacted at peak (past 90 days) As a %	First detected as malicious	Google Play		Outside of Google Play		Notes
				#Apps (~rounded)	First warned/blocked date	#Apps (~rounded)	First warned/blocked date	
dresscode	trojan		2016-03-18		2016-04-04		2016-04-08	
herole	data collection		2016-03-18		2016-03-14		2016-03-14	

(example data, but you get the idea)

Google Play Protect

Families

Some example families we may talk about

- Bankbot
- Spynote
- WireX

Expanding our dashboards

1. Interactive Botnet/Malware Campaign Dashboard
   a. Auto-populated with all relevant malware families with multiple filters
   b. Offer researchers access to submit family and suspected malware
2. Device Cleanliness Stats
   a. Fraction of devices with PHA and top campaigns across those device
   b. Devices with preinstalled PHA that do not remediate
3. SDKs that distribute PHA
   a. Versions and possible attribution

What can you do

- Send us your APKs and IoCs and we will
  - Credit you on the dashboard
  - Provide feedback on the size of impact
  - Identify your company for sending leads on you research

Email us: Security@android.com

Contact

Jason Woloz

Email: jwoloz@google.com