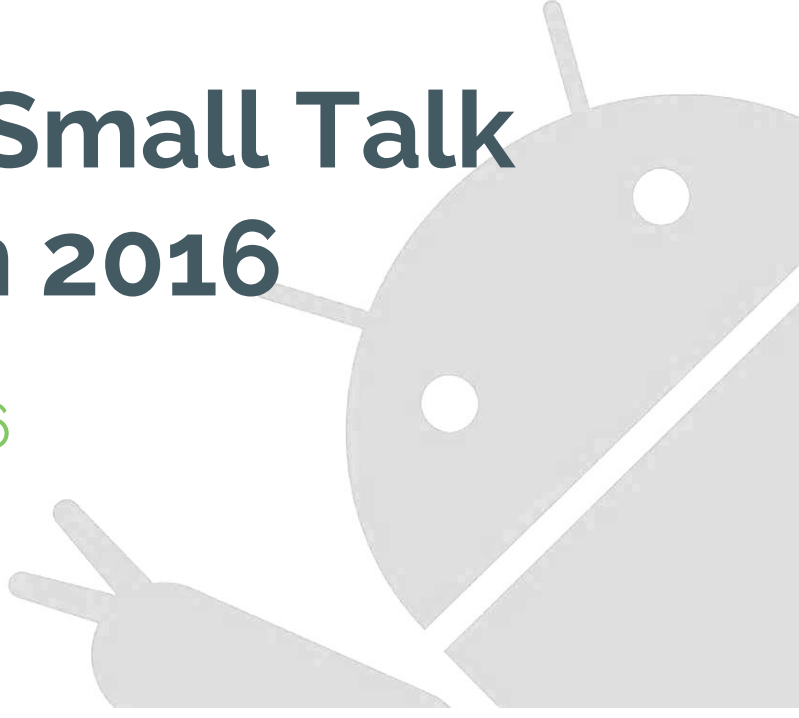
Android Security Small Talk
Virus Bulletin 2016

October 5, 2016



Agenda

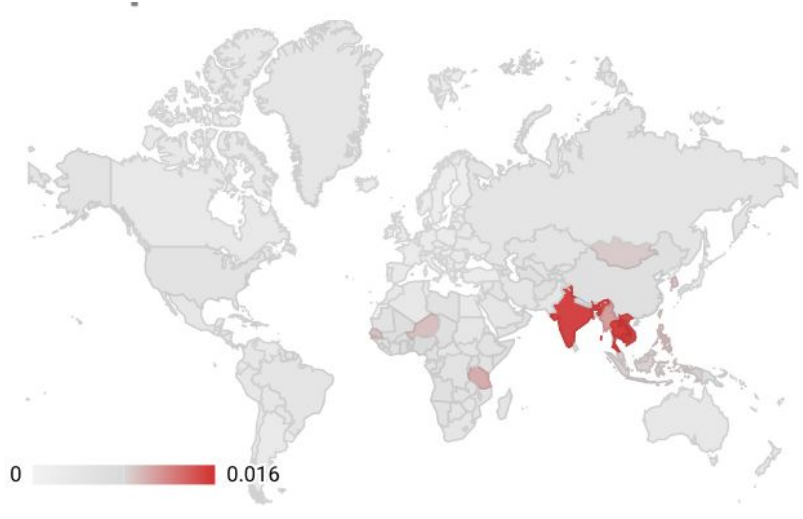
An small group discussion on a few key topics plaguing the industry

1. Mobile malware Incident response coordination
2. Building a community through shared threat data
3. Deincentivizing malware authors
4. Defining a global framework of potentially harmful applications
5. A taxonomy for describing malware families

*Securing the 3rd party marketplace [removed due to time constraints]

Mobile malware incident response coordination

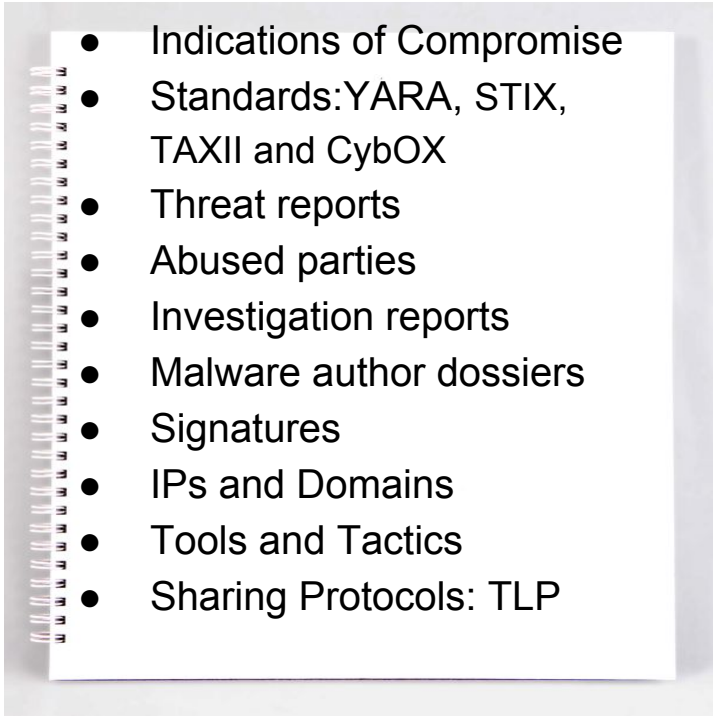
Malware impact has no physical boundaries and can infect devices no matter what region they reside in. Many malware authors operate in regions of the world where international law enforcement can not easily take action, leaving users without agency or recourse. How might we build a consortium of industry anti-malware response teams (e.g. CERT, FIRST like) to take coordinated action to reduce malware's footprint?



	Country	PHA Install Rate	Δ
1.	US	0.48%	0.15% ↑
2.	BR	0.43%	-0.15% ↓
3.	KR	0.89%	0.56% ↑
4.	IN	1.46%	0.19% ↑
5.	DE	0.23%	-0.09% ↓
6.	RU	0.42%	-0.18% ↓
7.	MX	0.37%	-0.27% ↓
8.	JP	0.27%	0.06% ↑
9.	TR	0.21%	-0.28% ↓
10.	ID	0.82%	-0.09% ↓

Building a community through shared threat data

There are a lot of really smart security professionals and researchers that could be even more effective if they shared their data amongst one another. How might we encourage data sharing within the Android Security Community?



Deincentivizing malware authors

Malware writers are incentivized by a variety of drivers, from monetary gain to vandalism. Are there any anti-patterns we could champion that would disincentive malware authors?

A global framework of potentially harmful applications

Application abuse and what is considered to be potentially harmful applications differs based on cultural and regional norms. How might we normalize on a definition of what is considered potentially harmful practices, so we can operate anti-malware campaigns without consideration for borders?

A taxonomy for describing malware families

Security researchers often disagree on what constitutes a family of malware. This often generates misunderstandings and press that requires anti-malware teams to verify leads on a constant basis. How might we set a standard for what a malware family is and is not?

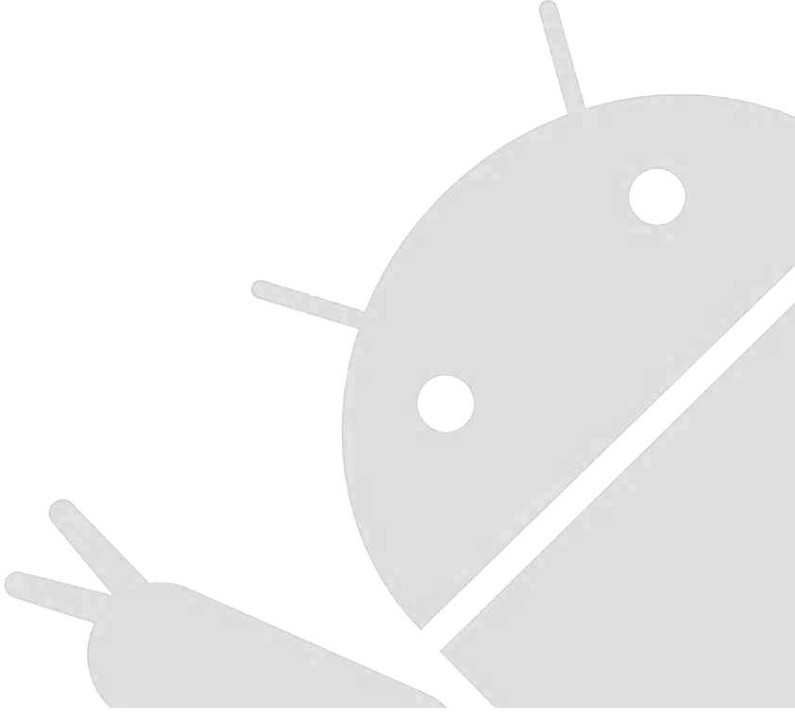
Ghost Push

Viking Horde

Hummingbad

Turkish Clicker

THANK YOU



Contact Us

Sebastian Porst, sporst@google.com

Jason Woloz, jwoloz@google.com