SECURITY WITHOUT "SECURITY DIVERSITY, VISIBILITY, AGILITY

Dino Dai Zovi @dinodaizovi

DIVERSITY

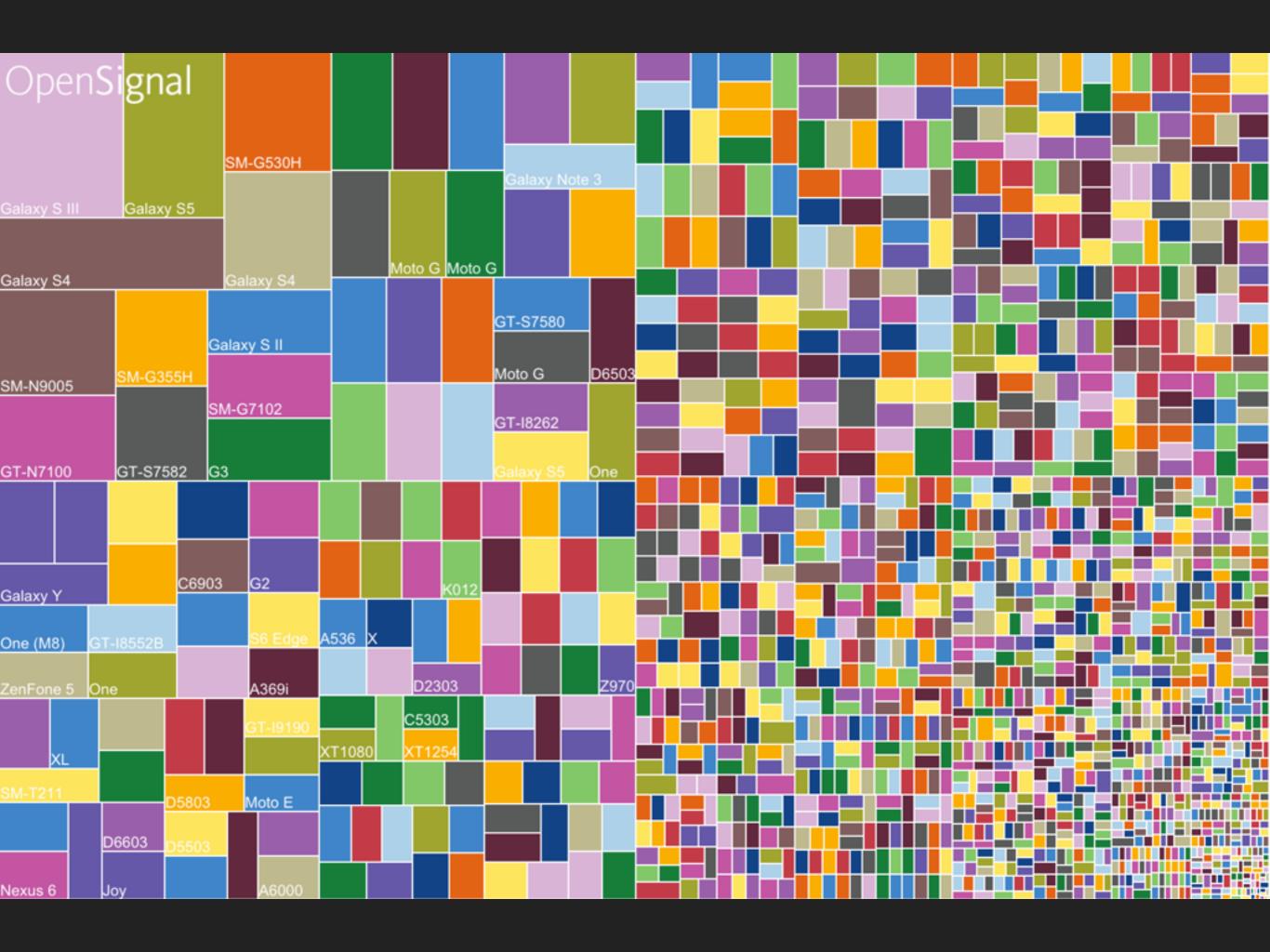
A MONOCULTURE OF NETWORKED COMPUTERS IS A CONVENIENT AND SUSCEPTIBLE RESERVOIR OF PLATFORMS FROM WHICH TO LAUNCH ATTACKS

Dan Geer et al

First Start	Second Start	Third Start
GD132	ntdll	kemel32
msvc rt		
	User32	msvc rt
kemel32	ADVAP123	
	GDI32	
RCPRT4		GDI32
User 32	kernel32	RCPRT4
ADVAP123		
	RCPRT4	ntdII
	msvc rt	
		ADVAP123
ntdll		User32





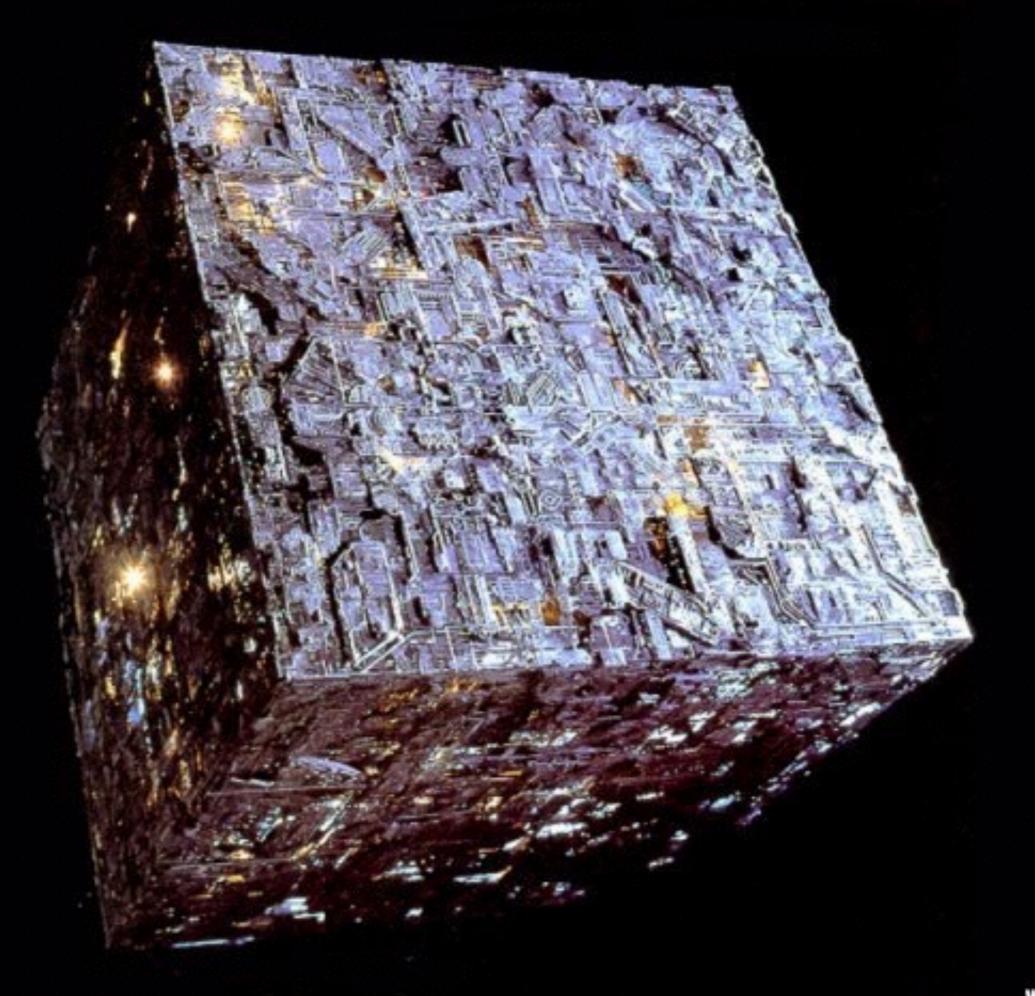




VISIBILITY



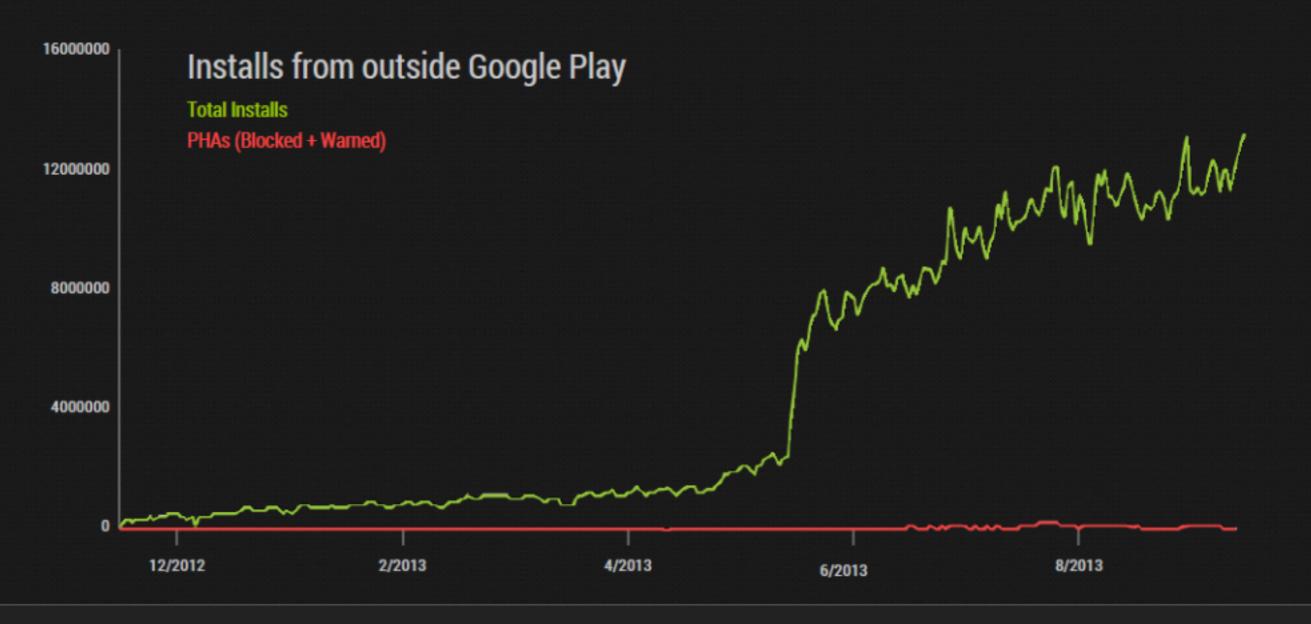
Android Malware: A Threat Rising at a Meteoric Rate One sample of malware can appear in hundreds of thousands of different variations October Kaspersky Lab's mobile security In December 2011 we detected Android has become the most solution successfully identified 82 000 SMS targeted mobile platform and blocked all ten malicious programs in comparative testing Drains your mobile by AV-Test.org. 200x account by sending In first two weeks premium texts Some competitors only identified one. of January 2012 - we detected 360 000 growth And we expect in 2011 more Spy Steals your data and/or collects your passwords Backdoor Provides unauthorized access to your mobile device Downloader Provides tools to download and launch malicious programs AndroidOS.Smspacem.a (May) A "Doomsday" worm. On command AndroidOS.Adrd.a (February) sends messages to all your contacts. Sends your personal data to a criminal. Answers incoming SMSs automatically. Makes money for him by promoting certain Changes wallpapers. websites. Updates itself automatically. AndroidOS.FakeInst.a (August) 20 69 77 102 102 1147 1925 2930 4101 A Trojan horse with many faces. AndroidOS.Rooter.a (March) Pretends to be a legitimate program. Takes full control over your device. Sends personal data. Sends short messages to premium numbers. Connects to a command server and downloads more malicious code. The first malware to appear on Android Market. KASPERSKY



AN ESTIMATED 0.001% OF APP INSTALLATIONS ON ANDROID ARE ABLE TO EVADE THE SYSTEM'S MULTI-LAYERED DEFENSES AND CAUSE HARM TO USERS

http://qz.com/131436/contrary-to-what-youve-heard-android-is-almost-impenetrable-to-malware/

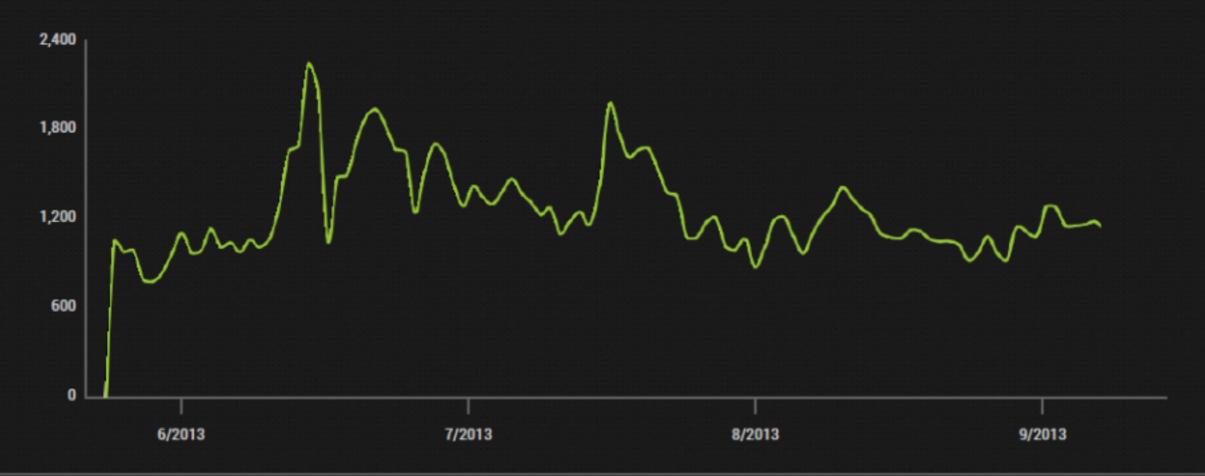
Analyzing 1.5 Billion Installs from outside Google Play



Potentially Harmful App Installs Low and Stable

Installs (p/million)

Installs After Warning



AGILITY













