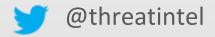


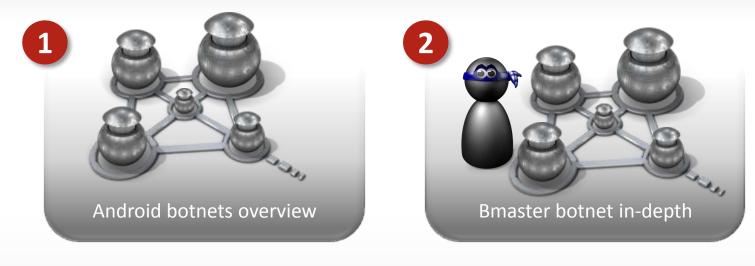
Billion Dollar Botnets: An Examination of the Current Trend in Android Botnets

Cathal Mullaney

Senior Software Engineer



Presentation agenda









Introduction



- Android Botnets
 - Trending on devices now...



• MDK Botnet

• 1 million active infections.



• Android.Bmaster

Botnet with a lot of telemetry!



Android Malware

Proliferation of smart phones.

3rd Party markets with lax security.

Simple to write Trojanized applications.

Simple to write powerful malware.



Android program model suited to writing low profile Daemon processes.







5

Android Malware

Permissions are

quickly becoming

software EULA.

agree

disagree

Simple to make revenue from infected devices.



Mobile banking applications are on the increase.

*Looking at you Hesperbot! Charging for one or two transactions a day may not be noticed immediately.





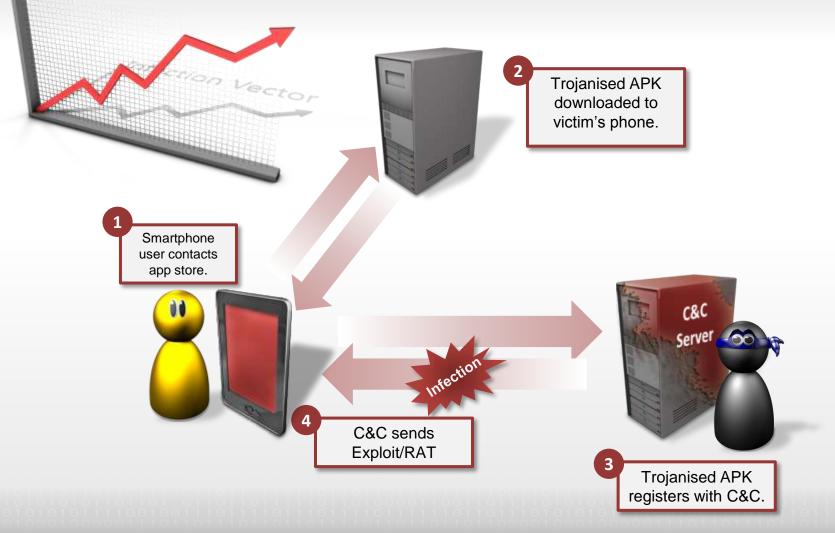
Android.Bmaster Ghost in the (mobile) machine.



000000

@threatintel

Infection Vector





Hosted/Spammed on 3rd party, Chinese, Android market place Legitimate software trojanized with the malware.

Infected 3rd party software

Infection Vector

Trojanized application was a loader/downloader for the larger botnet/exploit program.

Trojanized applications are a common infection vector



9





After decryption malware contacts the remote URL, downloads and executes the GingerBreak exploit. Exploit may fail, but regardless the malware will then attempt to download a RAT (Remote Administration Tool).

Malware operation

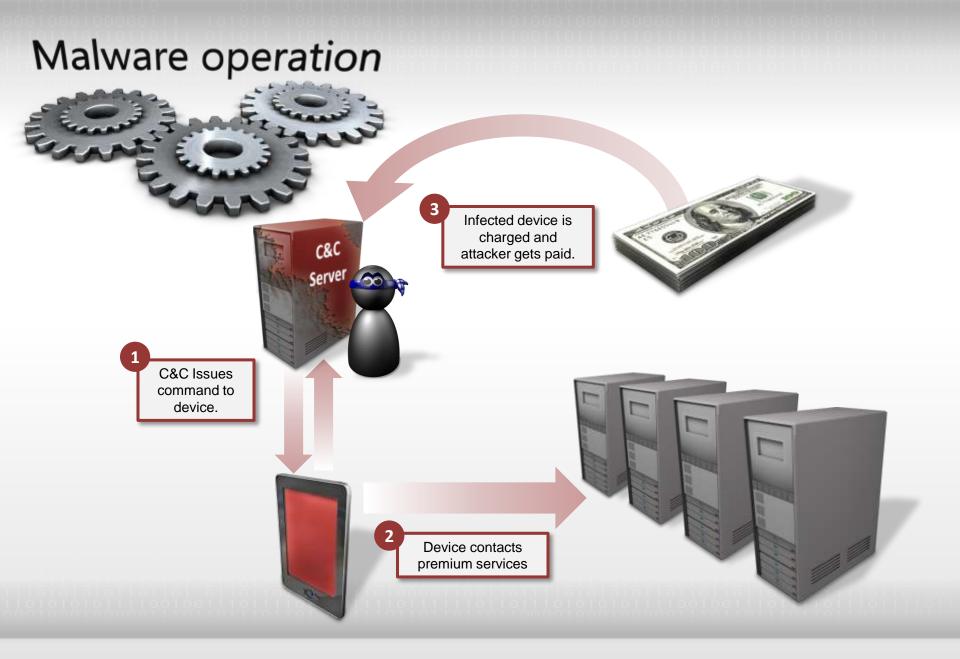
RAT registers with CnC, Depending on configuration Assigned to a "channel". Main functionality is for revenue generation.



Return of the RAT

- Registered three main services and several intent filters/broadcast receivers.
- Services used to generate revenue for the Botmaster.
 - Send an SMS to a number.
 - Connect to a URL.
 - Connect to an IVR.
 - Poll the C&C for new commands.
- Intent filters to capture/block SMS messages received, outgoing calls made and boot of the compromised device.
 - Among many others.







C&C Server

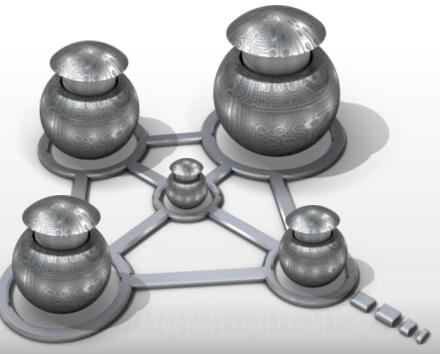
- Communication between device and server using KSOAP.
- Poorly secured servers.
- Server contained a complete C&C infrastructure interface.
 - Maintained data on infected devices.
 - Infection rates.
 - Successful Revenue generation.
- A complete picture of the Botnet and potential revenue generation emerged.





Android Botnet

- Judging by available timestamps we estimated the Botnet operating from September 2011 to present?
 - C&C infrastructure went dark.
- Infected devices numbered in the hundreds of thousands.
- All devices that were capable of revenue generation were stored for potential activation.
 - Sleeper cell phones.





Revenue Generation

- All infected devices broken up into channels.
- Channels allowed the Botnet master to control huge amounts of devices by issuing a few commands.
- Revenue is generated by sending SMS to premium numbers, contacting PPV websites and premium telephony services (voice chat lines).
- The Botnet master can also configure how many times per day these services are contacted (default to three).



Botnet management interface demonstration.

	4155			NHICTO	mcriti	10005	21982	-	**	****			
	206680081		88	94	199990581	82.	00000		29	ALC: NO			
	1-10669883	28	100	945	10489993	24	02235		67	14.00			
	est(abort)			9.8	- AND CONTRACT	大学	0.0	HR Dit	12	Holds.			
	est/action)		22 11 2	1541 1541	12049051901	#1 8#	0000	88.53	17	16.00 16.00			
	d(rebard)	29		84	12241003802		0085	AR LIN	18	10			
	(crenthes)	10		**	10900046140					45			
	(anti-tion		1.00	140				48.53	1.7	1416			
	Yoshidaa	29	11.00	Net-		.64		46.410	85	14.15			
2 ite	contention (25	10.00	- 10.00		他带	=	100 800	12	165			
	(individual		12.00	54		保土		88.53	#1	445			
	HARD BUT	69	**	840	12261203001		20000		80	48			
	set (ivr)		1/8	910		1214	00200		1.0	106			
	est live!		1/8	88		es.	00000		1.8	1616	 Concession in the second		
	manetare dary?	19	88	910	11341063012		20288		17	10.0	CT - St		
E heat in	nee:		111	#42 1410	4.5	20 #2	10100	AS 53	127 24 24	100	-		
	78		88	1441	1062687755	84	10000		78	85		No.	
10 A	1982		10	845	1042388383		10000		1	44			
1	C 83	29		Not:	1064038345	#2	20080		78	and .			and the second s
	1784	22	88	MIE	1006888023	104	22222		78	10.00			
	811			94	1042320308	12.0	22222		#**	448			
£.)	10	28		No.	1003336603		00000		18	1415			
3			6.9	新町	1042513106	北市	11111			68			
	C.S.etp	88	12.48	Nati-	"Constant"	事止		麻醉 集論	25	i408			
	Md	4.9	-	9-E 9-E	LONARDYS LONALDII	24	10111		79.40 Xa 64 Ar 18	10.00			
	#i8-1011 #i83		29	82	1066888999		11111			100		. 6.0	
	BERTAR		1/8	*5	STOCKARD AND			88.53		48			A 1
3	2+	19	-	940	104643000018		00000		Et.	48	The N		
	AB	28	10.	Witt:	100000998	25			783	16.0			
	48	18	10.0	54	126200888		00000	10.00	18	16.05	- Q	1	
* :	28	29		9 40	10626739	治疗	00588		48	10.0		-	a a la
8	2.0		10.00	911	10642246	. 89	100555		28	10.00	CAN L	B. Maria	
	80		10H 10H	MH MH	10427158005	#±			80 80 10 10 10 10 10 10 10 10 10 10 10 10 10	105		and the second sector	000
]			-0+ +0+ III		•		



Conclusions

- Android malware is simple to disseminate to a wide user base.
- Huge new markets for Malware writers emerging.
- Potential revenue in the millions of dollars.
- Entering the age of the billion dollar Botnet.
 - Real question is: "Why wouldn't malware writers target aggressively?"



Questions?



JJJJJ

Symantec Security Response

111



Thank you!

Copyright © 2013 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.