ISCX
Information Security
Centre *of* Excellence

Android Botnet: What URLs are telling us

Andi Fitriah A.Kadir, Natalia Stakhanova, Ali A.Ghorbani
Faculty of Computer Science, University of New Brunswick

UNB

ABSTRACT

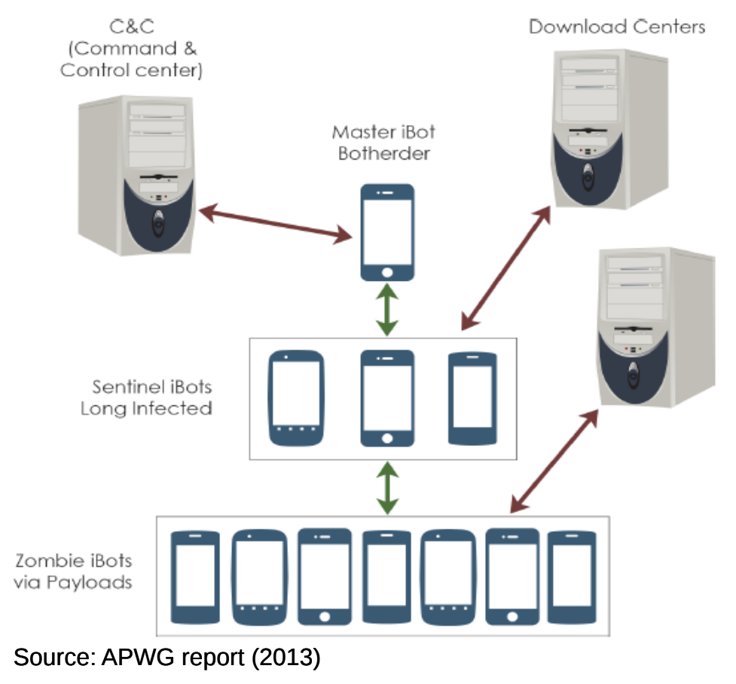
Botnets have traditionally been seen as a threat to personal computers, however recent shift to mobile platform resulted in a wave of new and mobile botnets. Due to the popularity, Android mobile OS became the most targeted platform. In spite of rising numbers, there is a significant gap in understanding a nature of mobile botnets and their communication characteristics. In this work, we propose to address this gap and offer a deep analysis of Command and Control (C&C) and build-in URLs of Android botnets detected in the wild since the first appearance of Android platform. Through comprehensive static analysis and visualization we uncover relationships between the majority of the analyzed botnet families and offer an insight into each malicious infrastructure. As a part of this study we compile and offer to research community a dataset containing 1645 samples and representing 10 Android botnet families.

What is Android Botnet?

What is Mobile Botnet?

Botnet = ro**BOT NET**work

Collection of compromised Mobile devices (called iBots) which are controlled remotely by a BotMaster through the C&C server

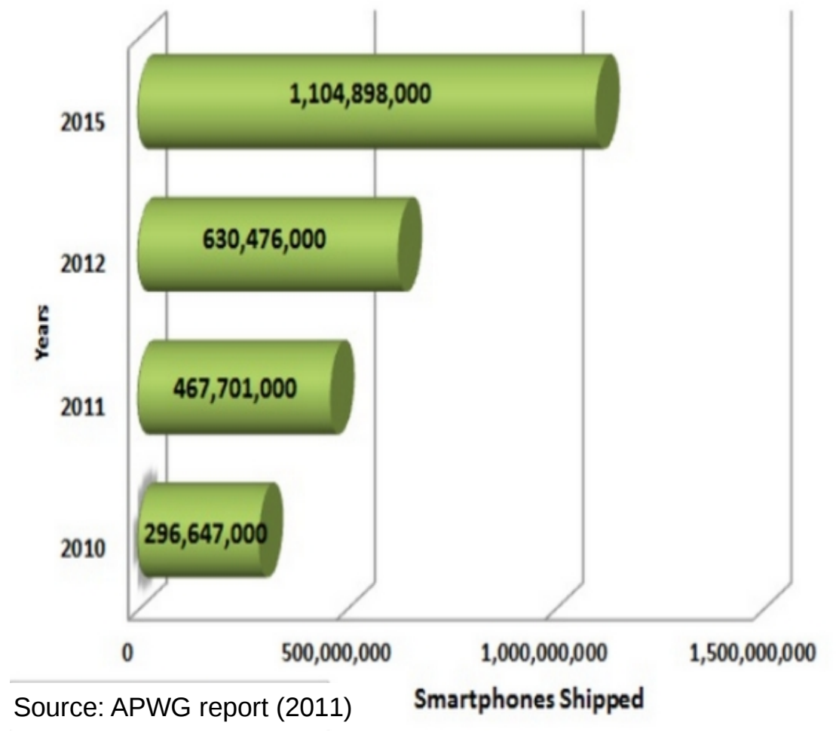

C&C (Command & Control center)
Download Centers
Master Bot Botherder
Sentinel iBots Long infected
Zombie iBots via Payloads

Source: APWG report (2013)

Fig 1: Mobile botnet architecture

Why Bother?

- ✔ Malware goes mobile
- ✔ More phones, means
- ✔ more targets & attacks
- ✔ More vector attacks (SMS/MMS, Bluetooth, Wi-Fi, 3G/4G, etc)

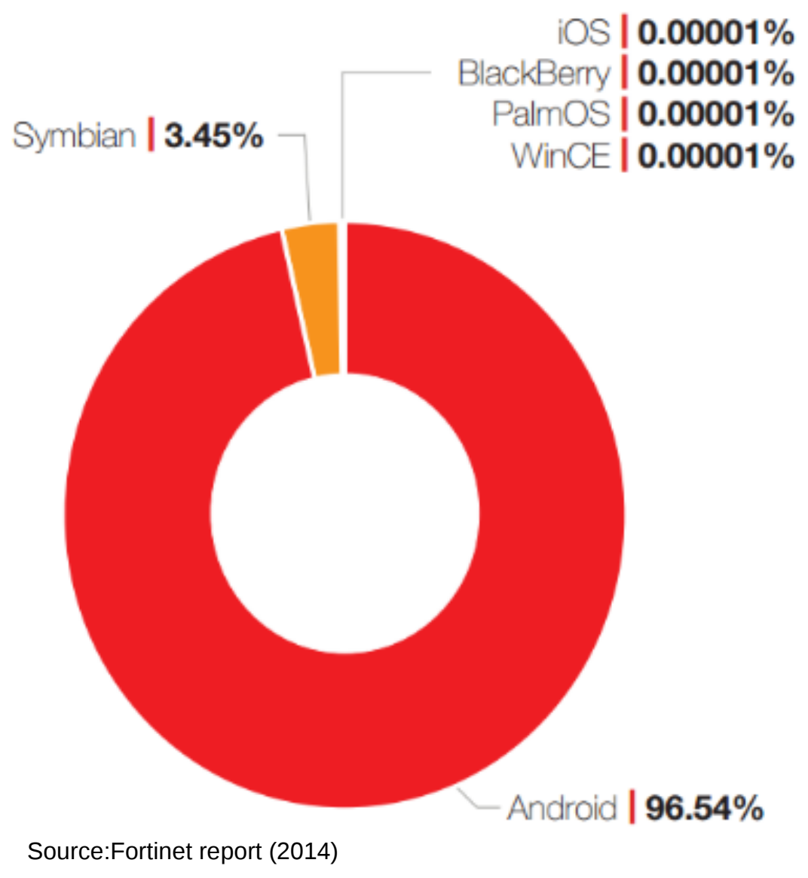


Source: APWG report (2011)

Fig 2: Smartphones shipping 2011-2015

Why Android?

- ✔ Android popularity
- ✔ Ease of use of malicious applications
- ✔ Lack of proper defense



Source:Fortinet report (2014)

Fig 3: Mobile users based on OS

How to detect Android Botnet?

Industry Solution

Some Protective Software for Smartphones

COMPANY	PROGRAM NAME	SUPPORTED OPERATING SYSTEMS
F-Secure	Mobile Anti-Virus Mobile Security	PocketPC, Symbian, Windows Mobile Nokia Communicators
McAfee	VirusScan Mobile	PocketPC, Symbian, Windows Mobile
Symantec	AntiVirus for Handhelds Mobile Security	Palm, PocketPC, Windows Mobile Symbian
Trend Micro	Mobile Security	PocketPC, Symbian, Windows Mobile

Source: Scientific American (2006)

Gap in understanding a nature of mobile botnets and its communication characteristics

Academic Research

- ✔ SMS based approach (agent, network topology)
- ✔ Machine learning (e.g. kNN, MLP, SVM, etc)
- ✔ Network Forensics

Proposed work

To offer a deep analysis of Android botnet URLs through comprehensive static analysis & visualization

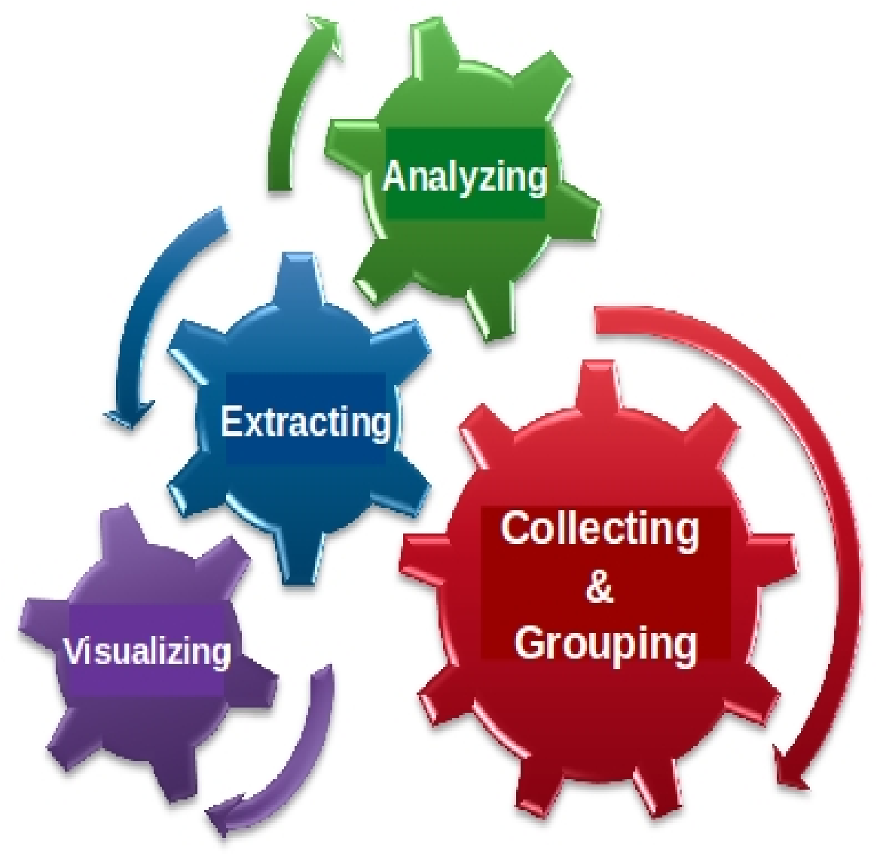


Fig 4: Research Framework

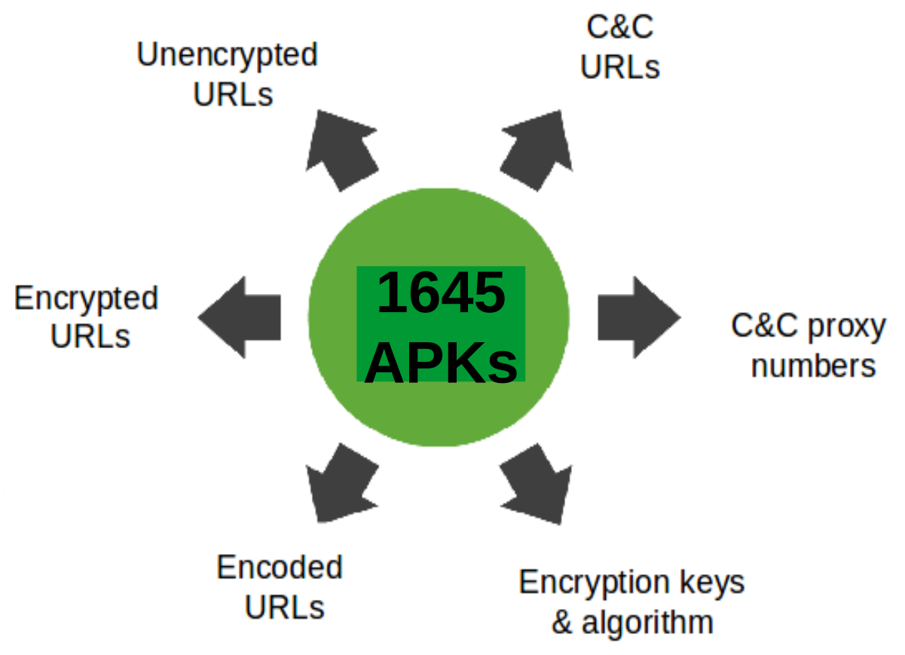


Fig 5: Extracted Features

Botnet family	Total C&C IP	Total build-in IP	Total C&C Domain Name	Total build-in Domain Name
AnserverBot	0	4	8	137
Bmaster	0	36	0	32
DroidDream	0	0	7	10
Geinimi	2	38	10	194
MisoSMS	0	0	0	58
Nickispy	0	21	0	269
PJApps	1	22	14	646
Rootsmart	0	0	0	11
Sandroid	0	0	0	215
TigerBot	0	3	0	26
Zitmo/Zeus	0	0	0	71
Total	3	124	39	1669

Table 1: Overview of the extracted URLs

What URLs tell us?

Resource sharing among botnet families

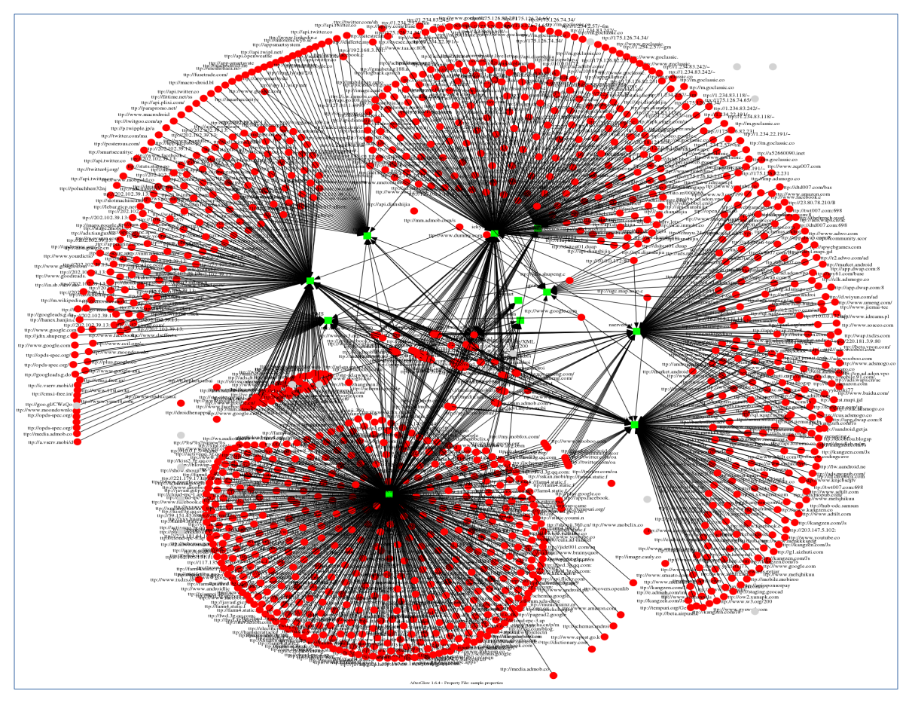


Fig 6: 1835 Extracted URLs

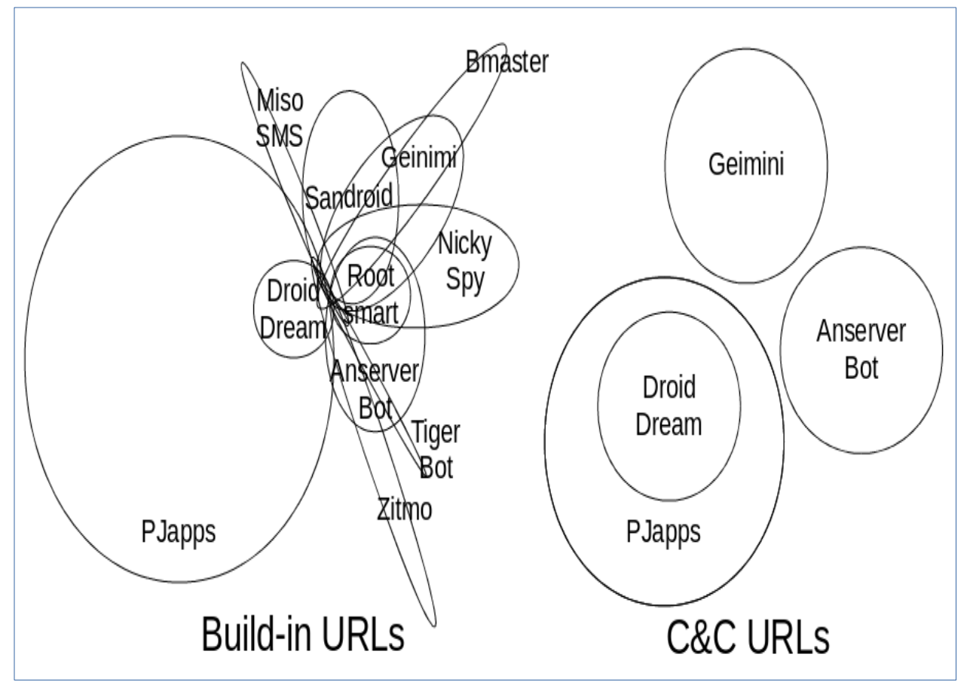


Fig 7: Build-in URL vs C&C URL

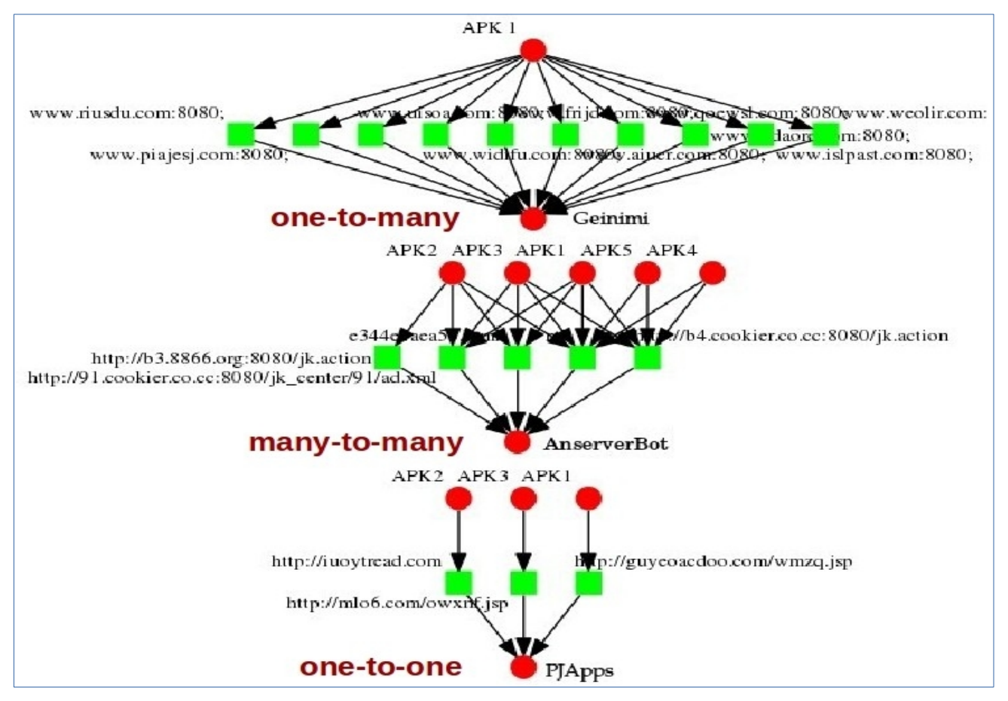


Fig 8: Types of URL Relationship

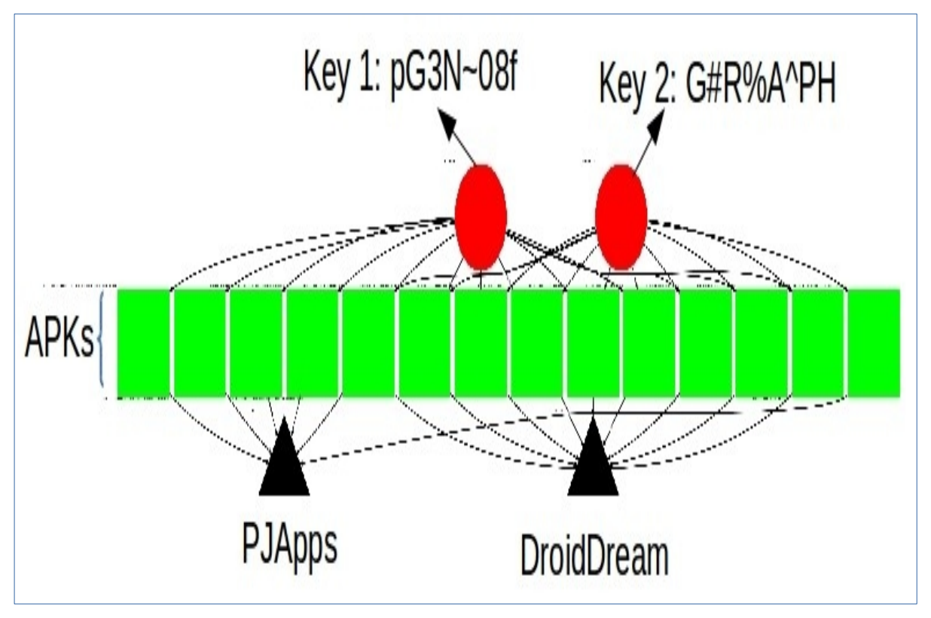


Fig 9: Sharing same encryption keys

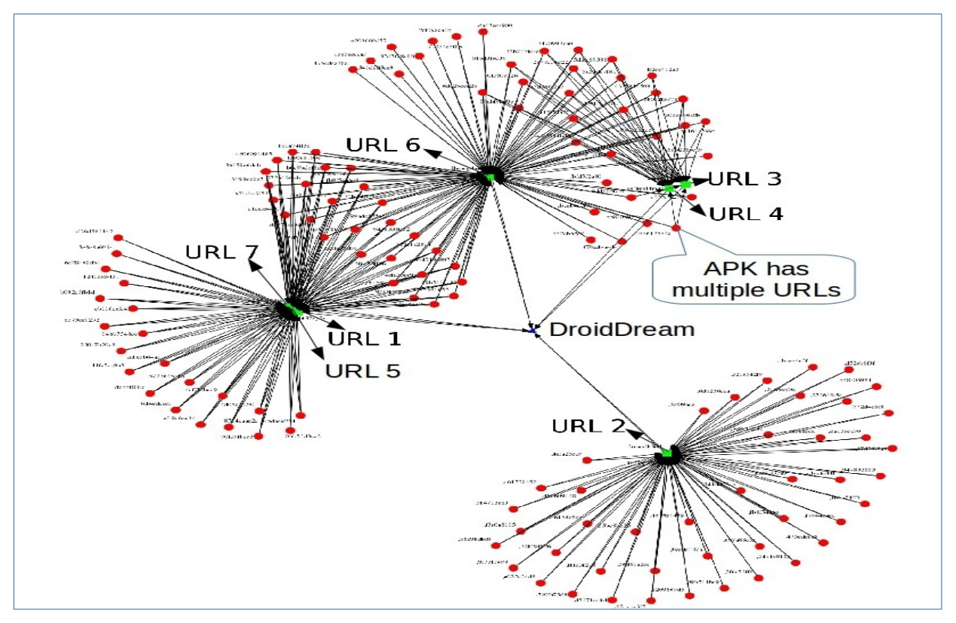


Fig 10: Sharing same set of URL

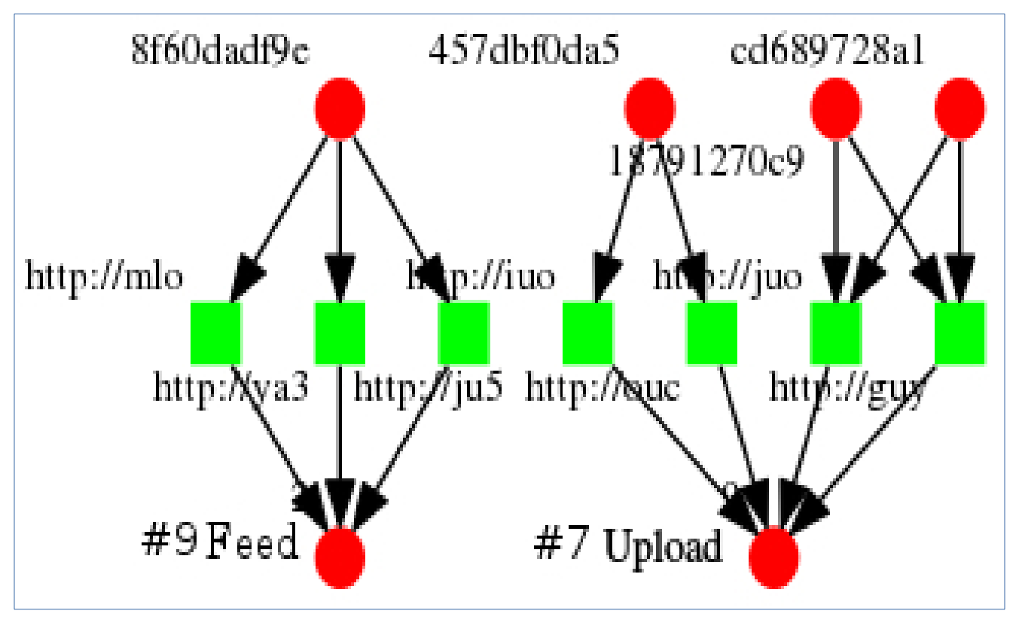


Fig 11: Sharing same C&C proxy

C&C Address Obfuscation

Family	Algorithm	Encoded	Decoded
AnserverBot	Base64	HoiprJbh9CVN9wnQ0w7O84FePwnYPJShHIE29IkwutRh8n__	http://b3.8866.org:8080/jk2.action
PJapps	Custom (skip-every-one-letter)	http://kl4ofgsmgeje5gko99s1fc2ofm	http://logmeego91.com
DroidDream	Rot-10	rddz://wkbuod.kxnbysn.myw/nodksvc	http://market.android.com/details

Table 2: Examples of Android Botnet encoding algorithm

Family	Algorithm	key	Hardcoded URL
Geinimi	DES	0x01020304060708	www.riusdu.com:8080;www.aiucr.com:8080
DroidDream	XOR	6^)(9-p35a%3#4S!4S0)$Yt%^&5(j.g^&o(*0)$Yv!#O@6GpG@=+3j.&6^)(0-=1]	http://184.105.245.17:8080/GMServer/GMServlet
	DES	DDH#X%LT	http://ya3k.com/bksy.jsp

Table 3: Examples of Android Botnet encryption algorithm

Detection of botnet samples

Family	Total APK	Total APK Detected	Detection Rate	Anti-virus scanners that detect samples
AnserverBot	244	242	99%	39/57
Bmaster	6	5	83%	25/57
DroidDream	365	356	97.5%	30/57
Geinimi	265	262	98.8%	32/57
MisoSMS	100	100	100%	21/57
Nickispy	202	199	98.5%	15/57
PJApps	212	210	99%	31/57
RootSmart	32	32	100%	32/57
Sandroid	44	38	86%	16/57
TigerBot	96	96	100%	20/57
Zitmo	80	80	100%	25/57

Table 4: Detection based on VirusTotal

Name	Total URL/domain	Total URL Detected
Malware Domain Blocklist	24 070	0
Shalla Blacklist	179 593	0
URL Blacklist	242 548	0
Zeus Tracker	785 187	0
Total	1231398	0

Table 5: Cross-check with blacklists

CONCLUSION

Findings Summary

- ✔ We have looked at improved methods of Android botnet analysis based on URL analysis.
- ✔ We have discovered that Android botnet encrypts various types of data (C&C servers URLs, the methods name to be invoked, and the content of the payload) with variety of encryption techniques.

Studies Implication

We have identified several factors that should be taken into account when developing techniques for Android botnet detection:

Behavioral similarity of Android botnets. There is a significant relationship among the

✔ botnets in terms of their resources, techniques, and configurations.

✔ **Evolution of Android botnet.** Android botnets become extensively sophisticated over time.

✔ **Blacklisted URL**. Android botnet URLs are unique and different with the traditional

✔ botnet and other type of malware.