A Framework for Profiling and Detecting Android Financial Malware

Andi Fitriah A. Kadir, Natalia Stakhanova, Ali A.Ghorbani

Canadian Institute for Cybersecurity (CIC), University of new Brunswick (UNB)

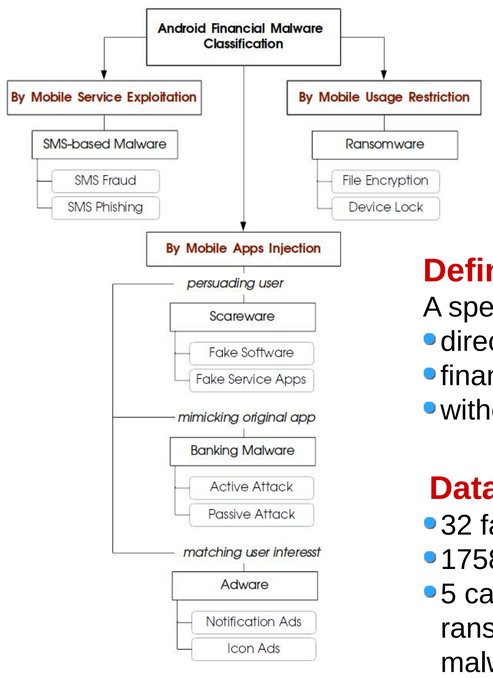
OVERVIEW

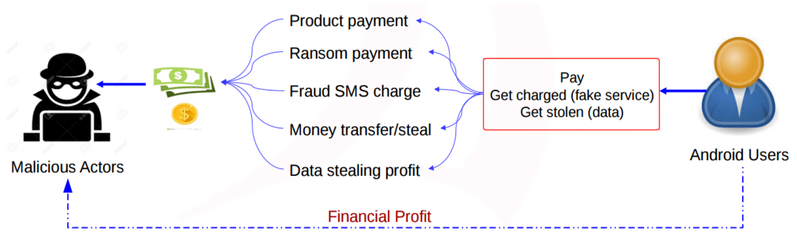
- **Problem**: Android financial malware (AFM) exist because information about users and their activities has value and naturally money is a motivating factor. However, what constitutes AFM is still ambiguous

- **Significance**: A comprehensive understanding of the existing AFM attacks supported by a unified terminology is necessarily required for the deployment of reliable defence mechanisms against these attacks

- **Goal**: We focus on three aspects of AFM: analyzing the characteristics, profiling the behavior, and detecting the malware

WHAT IS ANDROID FINANCIAL MALWARE?





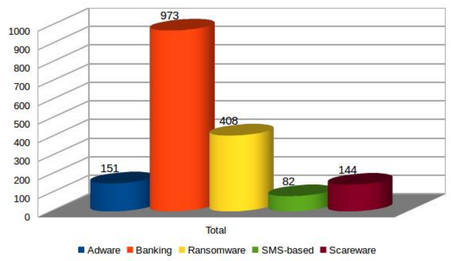
Definition

A specialized malware which is designed to:

- direct financial profit or money exchange to the fraudsters
- financial transaction includes any reselling or direct transactions
- without the user's knowledge or consent

Data

- 32 families
- 1758 unique samples (2010-2015)
- 5 categories: banking malware, ransomware, scareware, SMS malware, and adware



WHAT IS OUR SOLUTION?

Current Issues

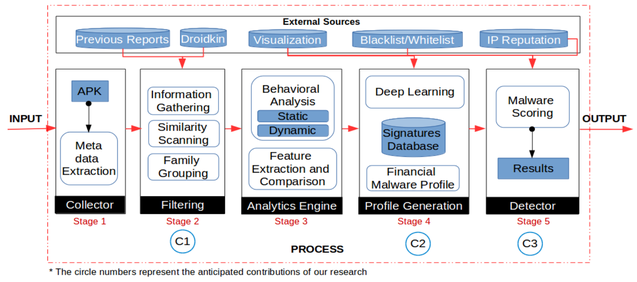
Table: Example of Banking Malware Zitmo detected by AVs

No	Antivirus	Result
1	AVG	Android/Deng.FVQ
2	Ad-Aware	Android.Trojan.Zitmo.E
3	AhnLab-V3	Android-Spyware/Rehai16.d55d
4	Alibaba	A.H.Pri.Dvci
5	Antiy-AVL	Trojan[Spy:HEUR]/AndroidOS.Mekir.2
6	Arcabit	Android.Trojan.Zitmo.E
7	Avast	Android:Morcut-G [Trj]
8	Avira (no cloud)	ANDROID/Agent.EW.Gen
9	Baidu-International	Trojan.AndroidOS.Mekir.b
10	BitDefender	Android.Trojan.Zitmo.E
11	CAT-QuickHeal	Android.Mekir.A
12	Cyren	AndroidOS/GenBl.048C4A52!Olympus
13	DrWeb	Android.Spy.176.origin
14	ESET-NOD32	a variant of Android/Morcut.A
15	Emsisoft	Android.Trojan.Zitmo.E (B)
16	F-Secure	Trojan:Android/Fakeinst.NG
17	Fortinet	Android/Mekir.Dltr
18	GData	Android.Trojan.Zitmo.E
19	Ikarus	Trojan.AndroidOS.Morcut
20	Jiangmin	TrojanSpy.AndroidOS.lbq
21	K7GW	Trojan (004c7e8c1)
22	Kaspersky	HEUR:Trojan-Spy.AndroidOS.Mekir.b
23	McAfee	Artemis!048C4A526C99
24	McAfee-GW-Edition	Artemis!Trojan
25	eScan	Android.Trojan.Zitmo.E
26	NANO-Antivirus	Trojan.Android.Mekir.dubdof
27	Qihoo-360	Trojan.Android.Gen
28	Rising	APK:Trojan.Generic(AndrCity)!7.1762 [F]
29	Sophos	Andr/Spy-AEC
30	VIPRE	Trojan.AndroidOS.Generic.A
31	Zillya	Trojan.Morcut..57
32	Zoner	Trojan.AndroidOS.Morcut

This non-standardization leads to confusion and inaccuracy.

None of the labels indicate banking nature

Proposed Framework



* The circle numbers represent the anticipated contributions of our research

WHAT DOES ANALYSIS TELL US?

Taxonomy Classification Comparison

Family Name	Year	Total	Proposed Taxonomy Labeling	AVG Majority Labeling
Kemoge	2015	100	Adware/NotificationAds/\textit{defined_family_name}	Android/Deng
Mobidash	2015	25	Adware/IconAds/\textit{defined_family_name}	Android/G2P
Citmo	2012	3	Banking/ActiveAttack/\textit{defined_family_name}	Android/Citmo
FakeBank	2014	151	Banking/PassiveAttack/\textit{defined_family_name}	Android/Deng
Koler	2014	74	Ransomware/Device-Locking/\textit{defined_family_name}	Android/Deng
Pletor	2014	16	Ransomware/Encryption-based/\textit{defined_family_name}	Android/Deng
FakeJobOffer	2013	7	Scareware/FakeServiceApps/\textit{defined_family_name}	Android/Fakejoboffer
FakePlayer	2010	25	Scareware/FakeSoftware/\textit{defined_family_name}	Android/G2M
Gazon	2015	1	SMS/Phishing/\textit{defined_family_name}	Android_dc
GGTracker	2011	11	SMS/Fraud/\textit{defined_family_name}	Android/G2P

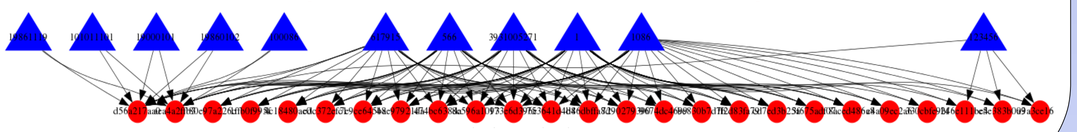
Unique Phone number used by SMS Fraud

Malware Family	Phone No.	Total
FakePlayer	798657	2
GGTracker	99735	9
YZHCsms	1000	0
	10000	0
	10086	25
	100086	2
	123456	4
	617915	15
	19000101	2
	19860102	2
	19861119	2
	91316005	0
	91316007	0
	101011101	2
	12345678911	25
	1065800885566	19
	0527140341921000133 09	0
	1240000089393100527140341001	21

Financial Charge Example

Financial Charge	Malware Family	Charge Amount (currency)	Payment Option	Targeted Country
Money Transfer (Ransom payment)	FakeDefender	99.98 (USD)	Credit Card	USA
	Koler	100-300 (USD)	MoneyPak Prepaid Cards	30 countries
	Pletor	15 (Euros) 100 (Rubles) 5000 (USD)	QIWI VISA MoneXy	13 countries
	ScarePakage	300 (USD)	MoneyPak	USA, UK, Germany
	SimpleLocker	20 - 200 (USD)	MoneXy	Ukraine, USA

SMS premium-rate number relationships

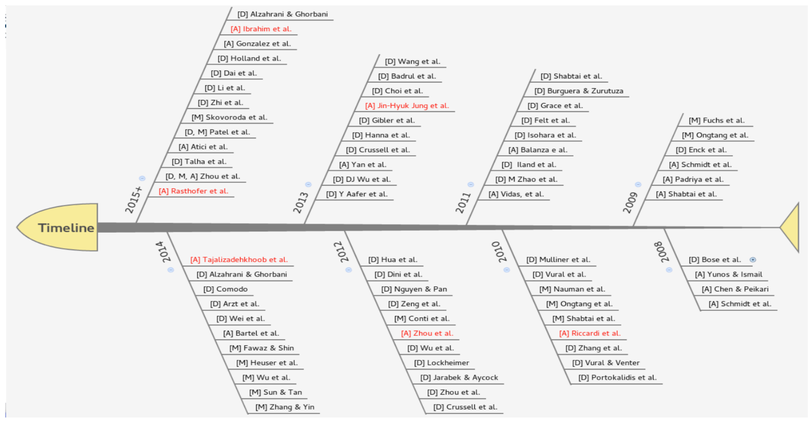


HOW TO DETECT ANDROID FINANCIAL MALWARE?

Industry Solution

Company	Apps Name
AVG Mobile	AntiVirus FREE - Security Scan
Bitdefender	Mobile Security & Antivirus
Lookout Mobile	Security & Antivirus Lookout
Norton Mobile	Norton Security and Antivirus
Webroot Inc	Security - Free

Academic Research



SUMMARY

By devising the AFM taxonomy:

- one can gain a deep understanding of the complex characteristics and the unknown behavior of AFM.
- It can help in detecting the future malware threats.

FUTURE WORK

In the future, we plan to:

- develop the framework of AFM detection based on profiles.
- build a prototype for evaluating the AFM detection system.