ISCX
Information Security
Centre of Excellence

An Empirical Analysis of Android Banking Malware

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

EST. 1785 UNB UNIVERSITY OF NEW BRUNSWICK

ABSTRACT

In general, any financial operation on the mobile platform potentially exposes a user to a variety of threats including data leakage, theft and financial loss. Driven by financial profits, banking malware leverages user’s cluelessness, openness of mobile platforms, and a lack of security measures. In this work, we aim to give insight into mobile banking malware and explore unique characteristics of its communication patterns. Given popularity of Android platform, in this work we focus on Android banking malware detected since the first appearance of Android platform in 2008. Through static and dynamic analysis combined with visualization, we analyze patterns of benign and malicious URLs employed by malware, their common characteristics, encoding trends, and the relationships with other types of malware. Through our study, we reveal methods (e.g., hidden encryption techniques) currently adopted by attackers to avoid detection. As a part of this study, we compile and offer to the research community a dataset containing 973 samples representing 10 Android banking malware families.

What is Android Banking Malware?

What is Banking Malware?

Then...

Capturing authentication information to access online financial instituitions

Now...

- Can capture SMS messages and record videos of user's screen while log in.
- TAN theft, botnet attacks, information stealing, etc

Why Bother?

✔ Malware goes mobile

✔ More phones, more targets & attacks

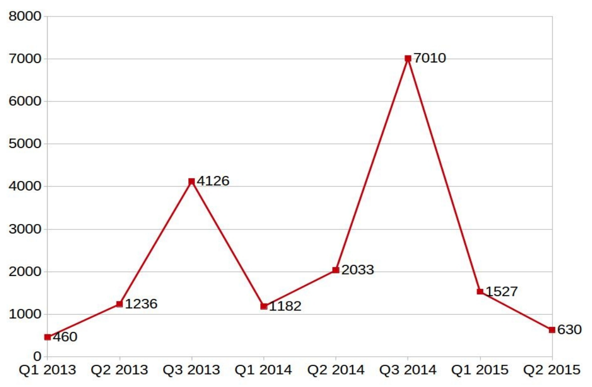


Fig 1: Android banking malware detected from 2013 -2015

Source: Data collected from Kaspersky reports

Why Android?

✔Android popularity

✔Ease of use

✔Lack of defense

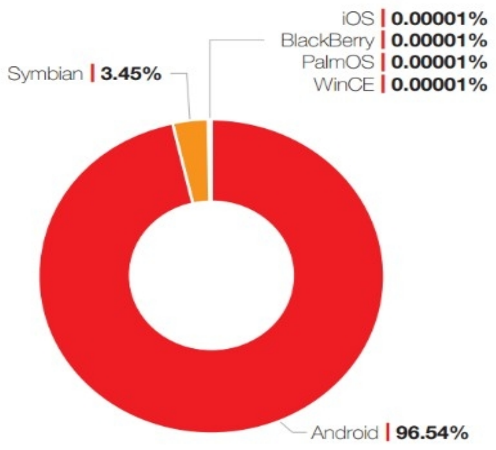
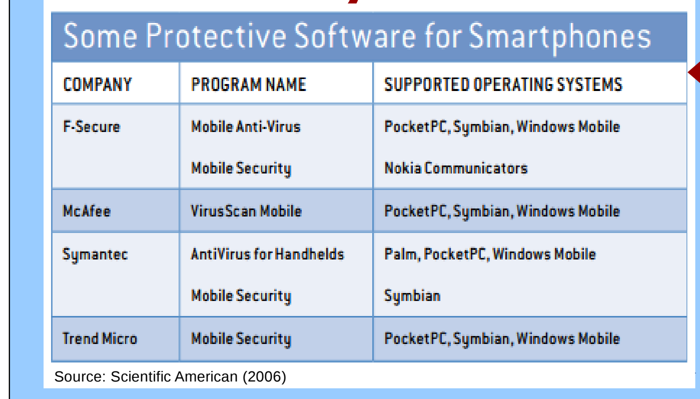


Fig 2: Mobile users based on OS

Source:Fortinet report (2014)

How to detect Android Banking Malware?

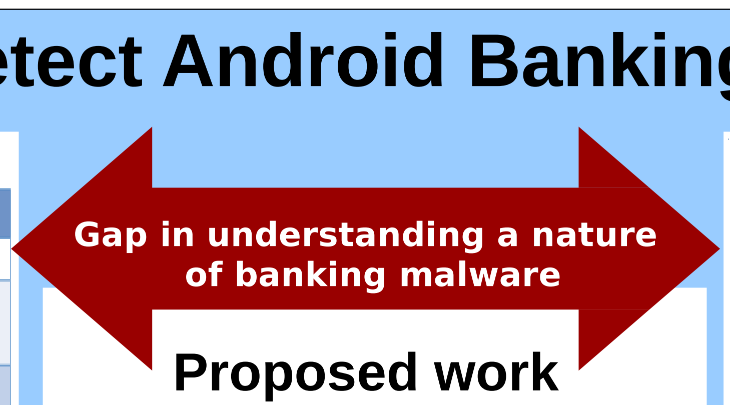
Industry Solution



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 banking malware

Proposed work

To offer a deep analysis of banking malware via static & dynamic analysis

Academic Research

(Mobile malware in general)

- Behavioral analysis
- Machine learning
- Network forensics
- Agent-based detection
- User-level monitoring

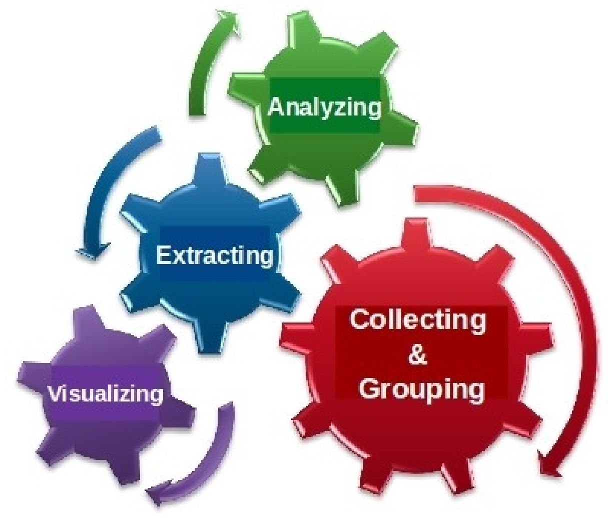


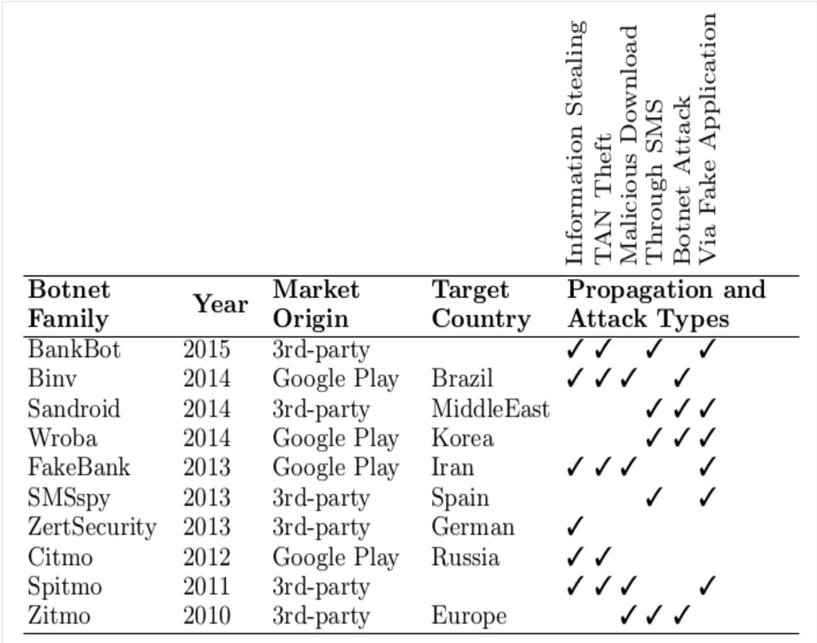
Fig 3: Researh Methodology

Malware Family	Total Samples	Discovered Year	The year of the earliest sample (the *.dex* file year)
Bankbot	136	2015	2008
Binv	2	2014	2014
Sandroid	61	2014	2008
Wroba	152	2014	2008
FakeBank	151	2014	2008
SMSspy	131	2013	2014
ZertSecurity	4	2013	2012
Citmo	3	2012	2012
Spitmo	191	2011	2008
Zitmo	142	2010	2008
Total	973		

Table 1: Overview of the collected data

What Analysis tell us?

Analyzing the characteristics



Botnet Family	Year	Market Origin	Target Country	Information Stealing	TAN Theft	Malicious Download	Through SMS	Botnet Attack	Via Fake Application
				Propagation and Attack Types					
BankBot	2015	3rd-party		✓	✓		✓		✓
Binv	2014	Google Play	Brazil	✓	✓	✓		✓	
Sandroid	2014	3rd-party	MiddleEast				✓	✓	✓
Wroba	2014	Google Play	Korea				✓	✓	✓
FakeBank	2013	Google Play	Iran	✓	✓	✓			✓
SMSspy	2013	3rd-party	Spain				✓		✓
ZertSecurity	2013	3rd-party	German	✓					
Citmo	2012	Google Play	Russia	✓	✓				
Spitmo	2011	3rd-party		✓	✓	✓			✓
Zitmo	2010	3rd-party	Europe			✓	✓	✓	

Fig 4: Android Banking Malware Characteristics

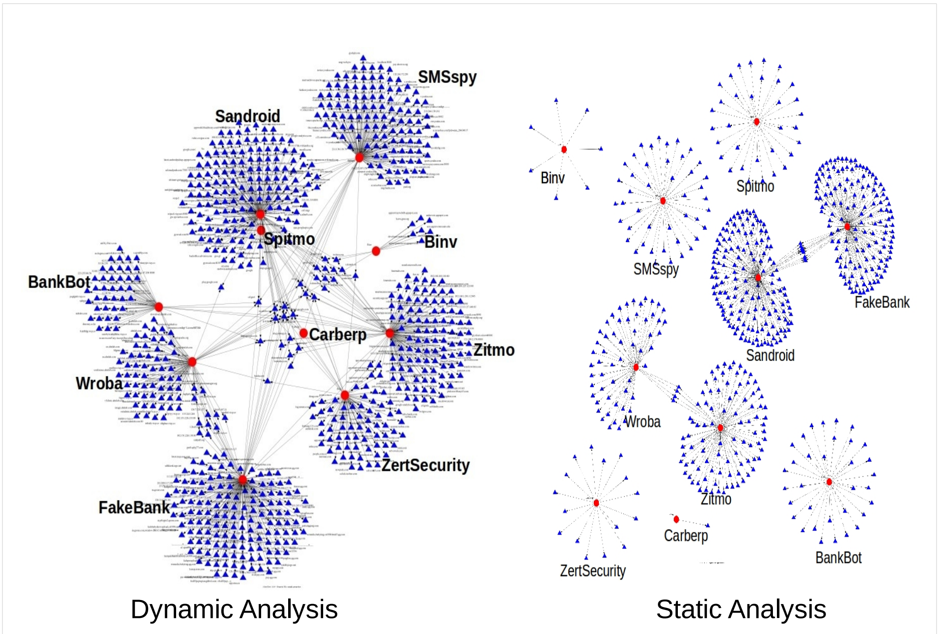


Fig 5: Static vs. Dynamic relationships

Analyzing the Encryption & Obfuscation technique

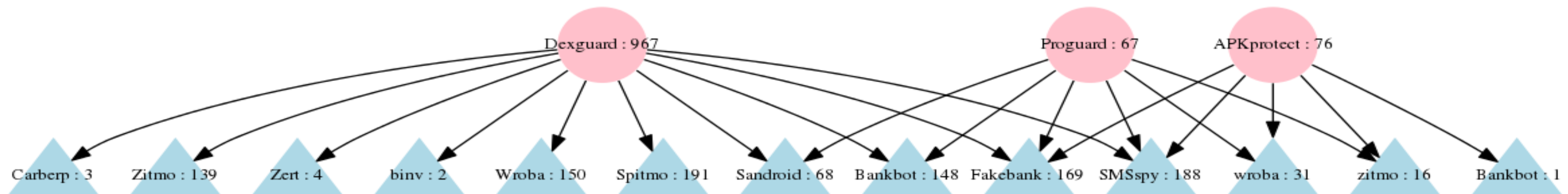


Fig 6: Examples of sharing obfuscation methods

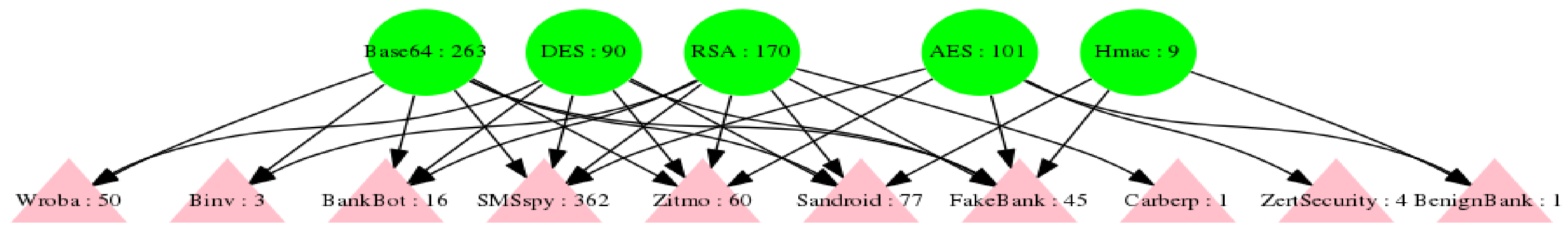


Fig 7: Examples of sharing encryption algorithms

Analyzing the URLs (2 027 unique URLs)

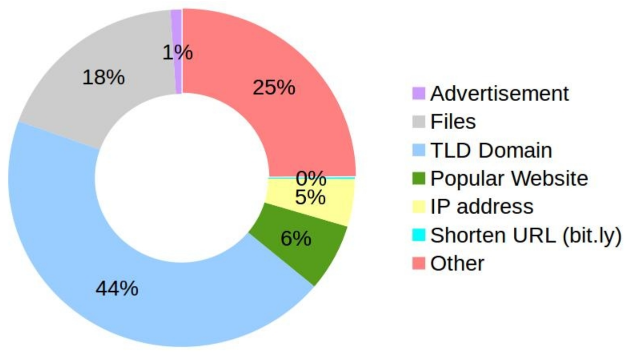


Fig 8: Overview of URL category

- **20%** are malicious (Virus Total)
- **7%** match with Android botnet URLs
- **1%** match with benign banking URLs

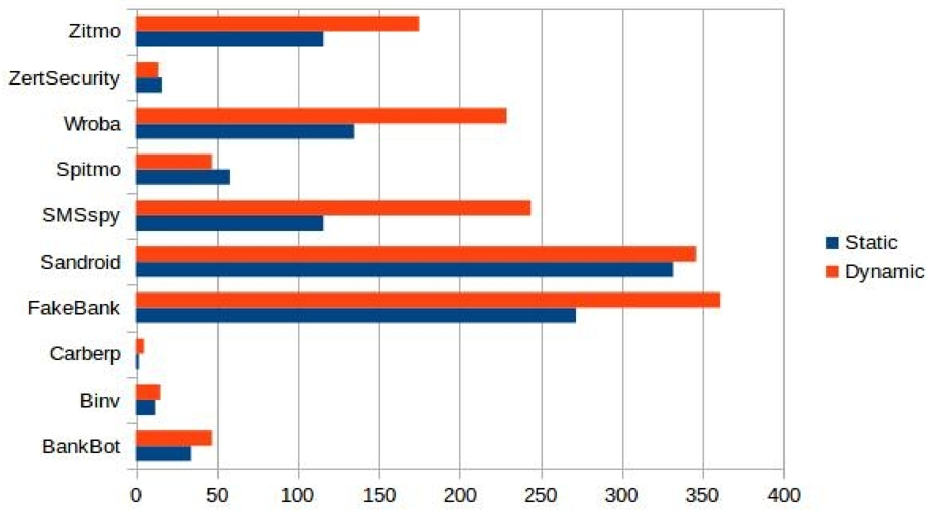


Fig 9: Static vs. Dynamic: URL extraction

CONCLUSION

2 factors that should be taken into account when developing techniques for Android banking malware detection

1. Behavioral similarity of Android banking malware (DGA, encryption, URLs)

2. Evolution of Android banking malware (become sophisticated over time)