Careful About What App Promotion Ads Recommend! Detecting and Explaining Malware Promotion via App Promotion Graph

Shang Ma, Chaoran Chen, Shao Yang, Shifu Hou,
Toby Jia-Jun Li, Xusheng Xiao, Tao Xie, Yanfang Ye

UNIVERSITY OF NOTRE DAME

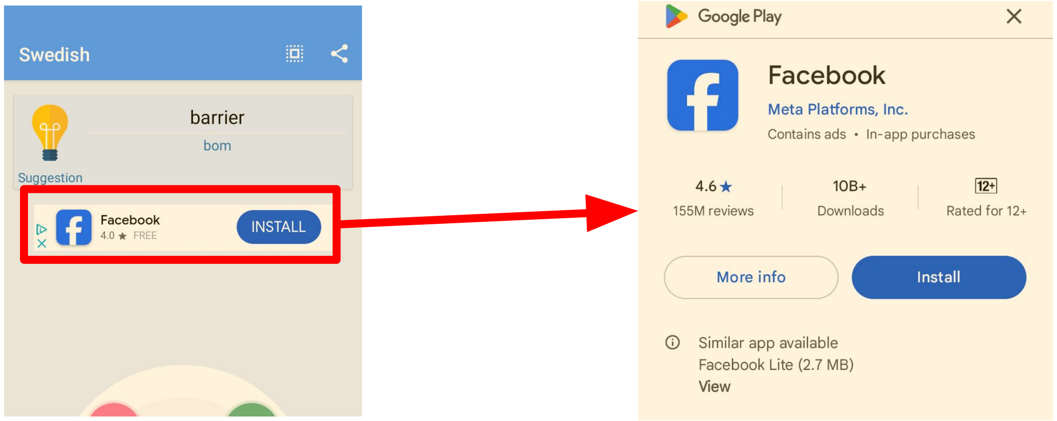
Arizona State University

App Promotion Ads

Over 57% of all apps in Google Play contain advertisements (ads).

App promotion ads are used to promote apps.

- ⅓ of users discover new apps through app promotion ads



Swedish

barrier

bom

Suggestion

Facebook
4.0 ★ FREE

INSTALL

Google Play

Facebook

Meta Platforms, Inc.

Contains ads • In-app purchases

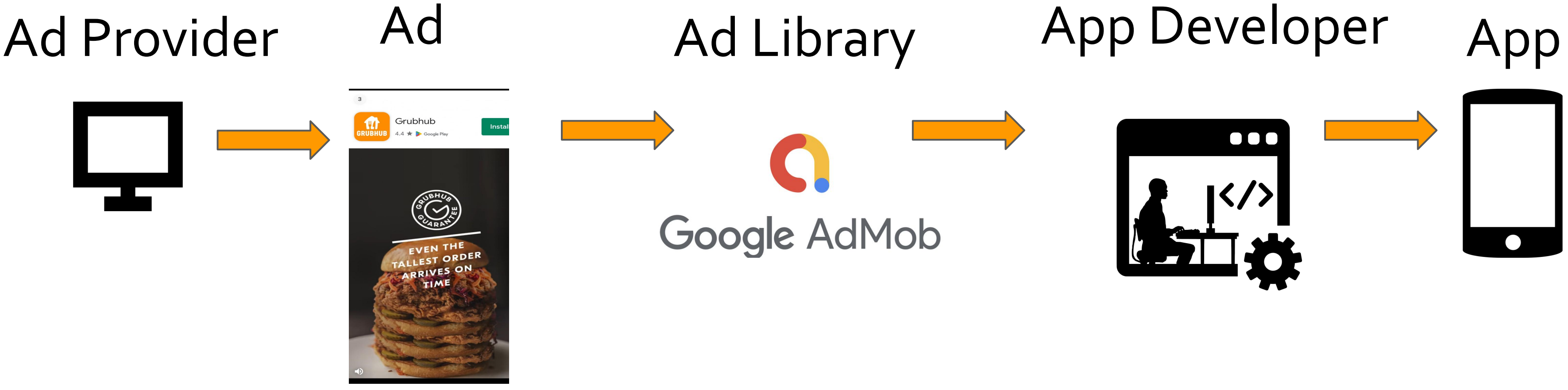
4.6★	10B+	12+
155M reviews	Downloads	Rated for 12+

More info

Install

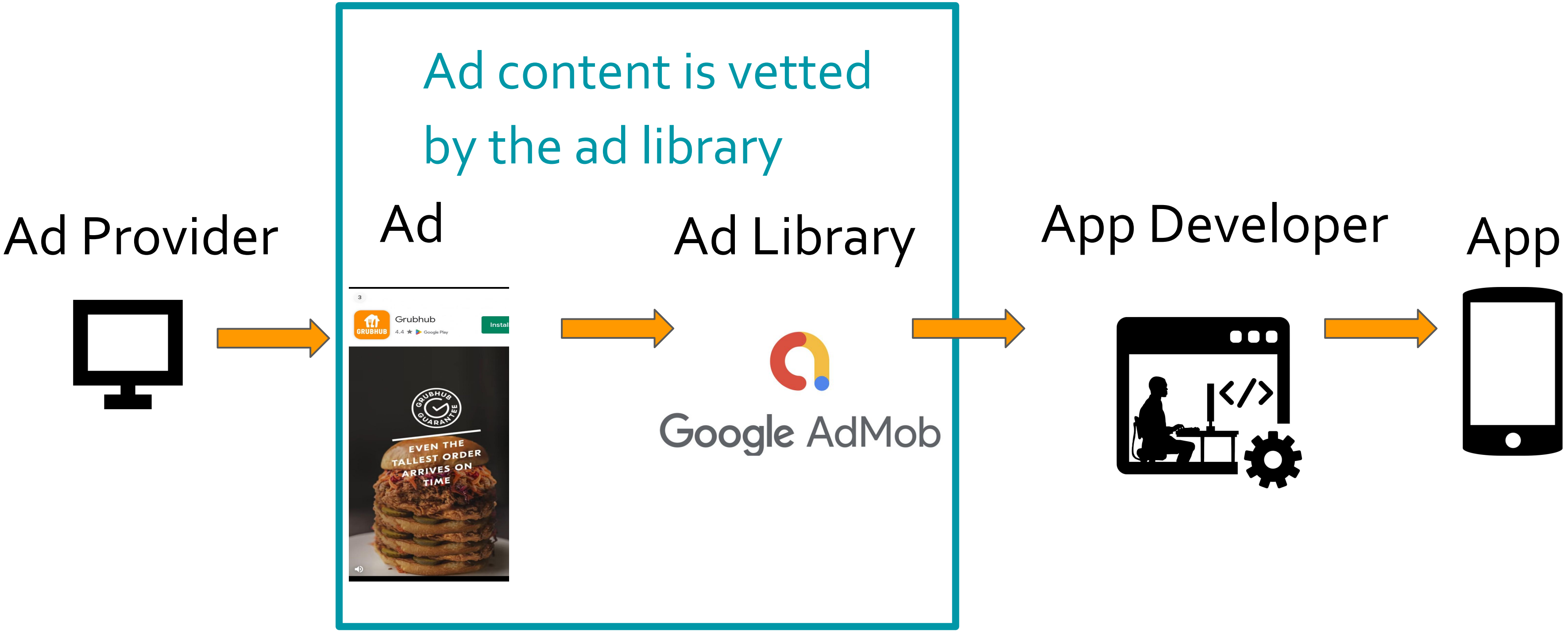
Similar app available
Facebook Lite (2.7 MB)
View

App Promotion Ecosystem



Ad Provider → Ad → Ad Library → App Developer → App

App Promotion Ecosystem



Ad content is vetted by the ad library

Ad Provider

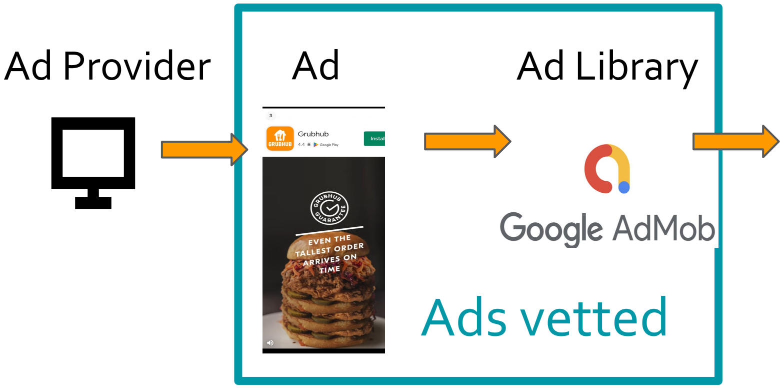
Ad

Ad Library

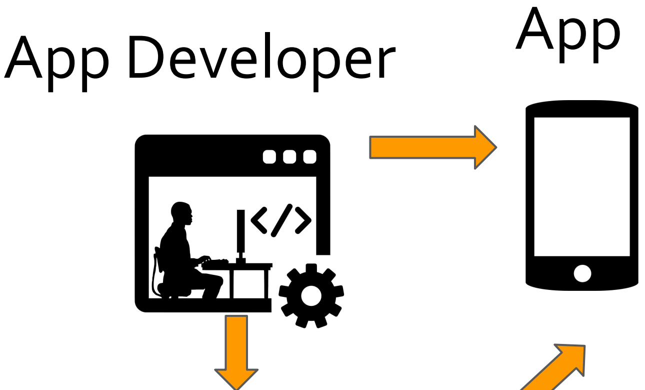
App Developer

App

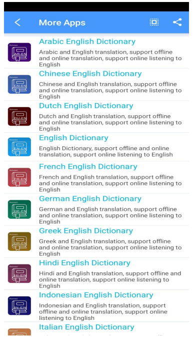
App Promotion Ecosystem



Ads vetted



Custom-made Ads



Arabic English Dictionary

Arabic and English translation, support offline and online translation, support online listening to English

Chinese English Dictionary

Chinese and English translation, support offline and online translation, support online listening to English

Dutch English Dictionary

Dutch and English translation, support offline and online translation, support online listening to English

English Dictionary

English Dictionary, support offline and online translation, support online listening to English

French English Dictionary

French and English translation, support offline and online translation, support online listening to English

German English Dictionary

German and English translation, support offline and online translation, support online listening to English

Greek English Dictionary

Greek and English translation, support offline and online translation, support online listening to English

Hindi English Dictionary

Hindi and English translation, support offline and online translation, support online listening to English

Indonesian English Dictionary

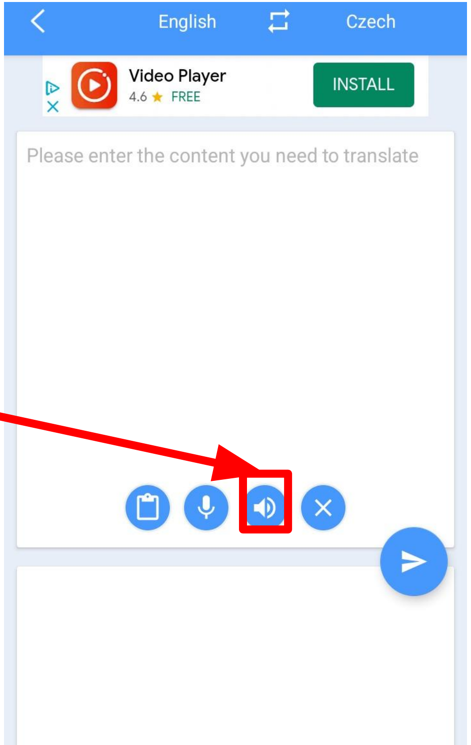
Indonesian and English translation, support offline and online translation, support online listening to English

Italian English Dictionary

Lack of vetting !

Malware Promotion Example

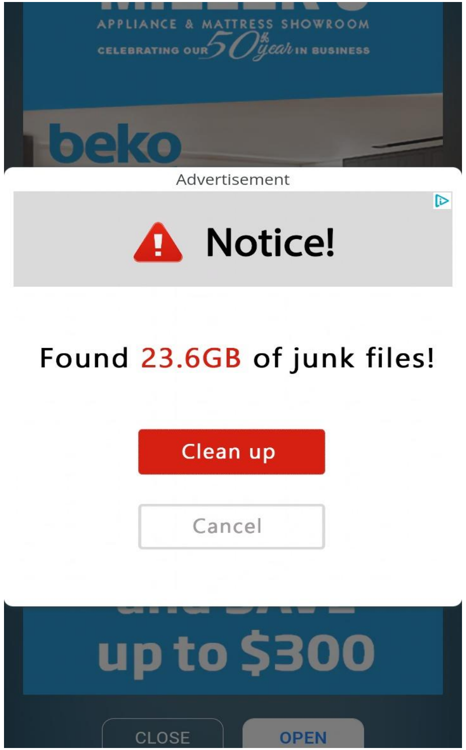
A malicious ad hides in the "Sound" Icon



Please enter the content you need to translate

Malware Promotion Example

When clicked, a
full-screen ad pops up


APPLIANCE & MATTRESS SHOWROOM
CELEBRATING OUR 50th year IN BUSINESS
beko
up to $300
CLOSE
OPEN

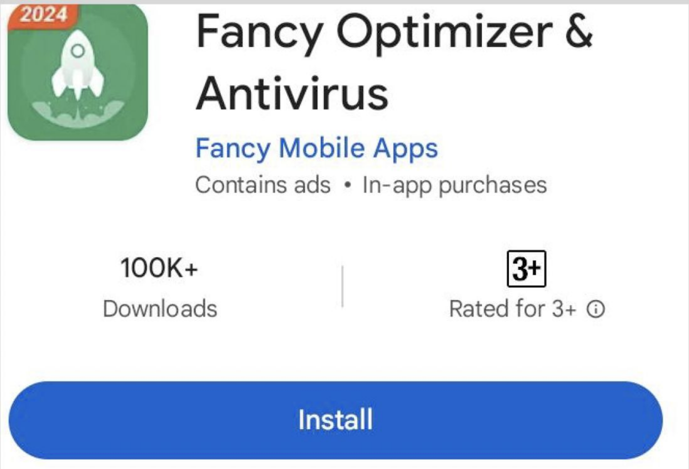
Advertisement

Notice!

Found 23.6GB of junk files!

Malware Promotion Example

Redirect to Google Play to install the app



2024

Fancy Optimizer & Antivirus

Fancy Mobile Apps

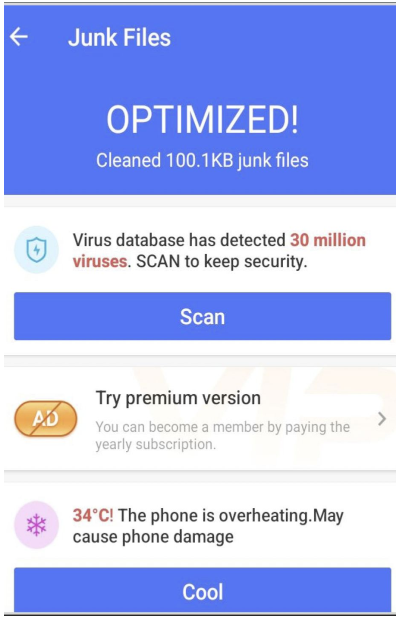
Contains ads • In-app purchases

100K+ Downloads

3+ Rated for 3+ ⓘ

Malware Promotion Example

Scamware



OPTIMIZED!

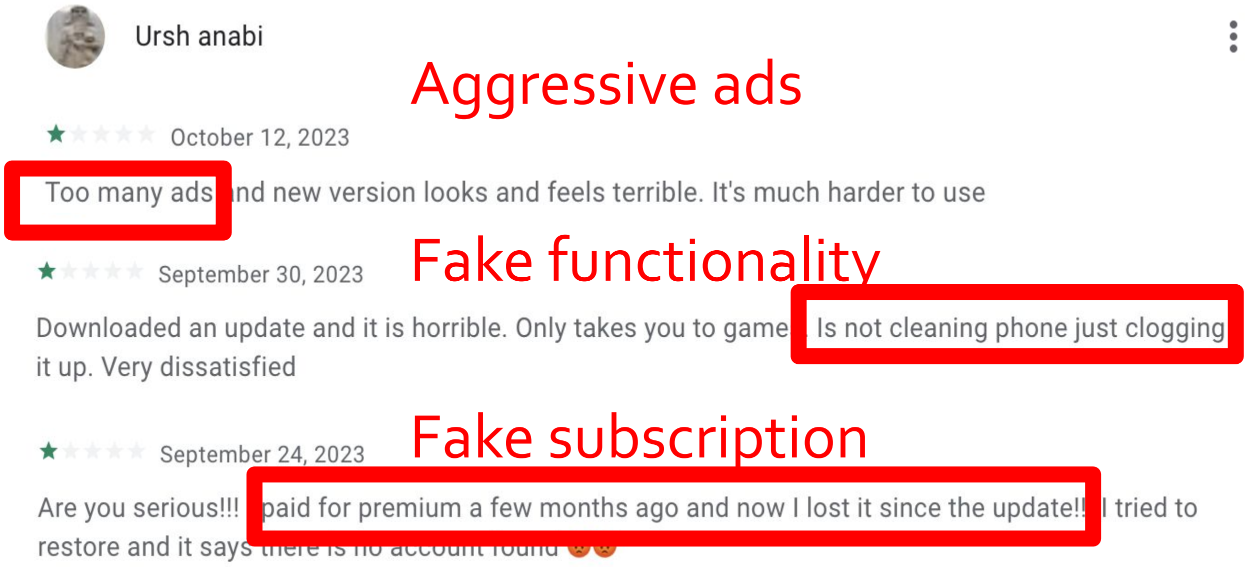
Cleaned 100.1KB junk files

Virus database has detected 30 million viruses. SCAN to keep security.

Try premium version

You can become a member by paying the yearly subscription.

34°C! The phone is overheating.May cause phone damage



Ursh anabi

Aggressive ads

★☆☆☆☆ October 12, 2023

Too many ads and new version looks and feels terrible. It's much harder to use

Fake functionality

★☆☆☆☆ September 30, 2023

Downloaded an update and it is horrible. Only takes you to game. Is not cleaning phone just clogging it up. Very dissatisfied

Fake subscription

★☆☆☆☆ September 24, 2023

Are you serious!!! paid for premium a few months ago and now I lost it since the update!! I tried to restore and it says there is no account found 😡😡

Research Problem

Can we automatically detect the malware promoted by app promotion ads ?

Arizona State University

UNIVERSITY OF NOTRE DAME

Preliminary Study

Dataset: sampled from AndroZoo[1] (200 apps), Rico[2] (405 apps)

Findings:

- Custom-made ads are
  - prevalent: **23%** app promotion ads are custom-made ads
  - risky: **51%** of them promote malware
- Ad content are requested from the **server at runtime**

Challenge: Applying **static analysis** on **ad libraries** is not sufficient to detect malware promotion

[1] Androzoo: Collecting millions of android apps for the research community." Proceedings of the 13th international conference on mining software repositories. 2016.

[2] "Rico: A mobile app dataset for building data-driven design applications." Proceedings of the 30th annual ACM symposium on user interface software and technology. 2017.

Insight: *App Promotion Graph*

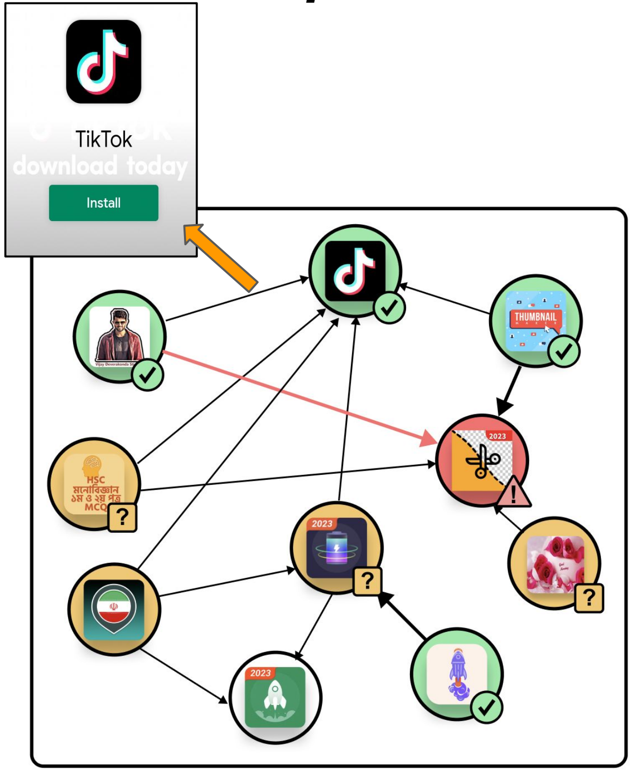
The ecosystem can be modeled as a graph: *app promotion graph*

- Edges: app promotion ads
- Nodes: apps

We use this graph to capture

- **app promotion relations** among apps
- **app attributes** derived from *app markets*, *security vendor*, and *binary code*

Malware detection→ **Node classification**



Our Approach

Part 1: *UI exploration* to **collect app promotion ads** to construct an app promotion graph

Part 2:*Graph learning* to **detect malware promotion** based on the constructed app promotion graph

Motivation for combining *UI exploration* and *graph learning*:

1.UI exploration alone can collect app promotion ads but **cannot determine the maliciousness** of the promoted apps.

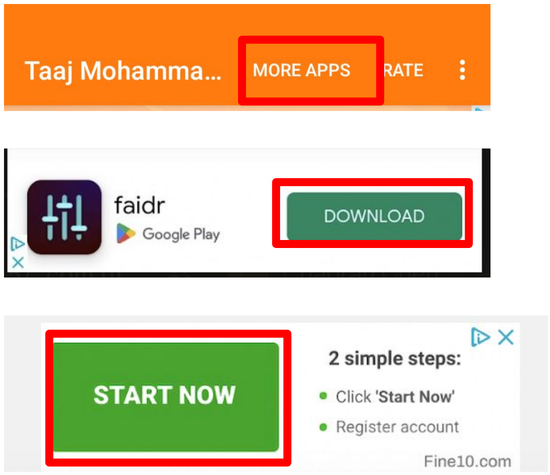
2. Effectiveness of graph learning depends on the **features of the app promotion graph** built by UI exploration

Part 1: App Promotion Graph Construction

Ad-oriented UI exploration

- **Depth first search** to navigate to the UIs containing ads
- **Text patterns** (empirically crafted ad-related string) to detect ad content
- **Iteratively restarting** the app to capture the periodically changing ad content.

Examples of ad patterns



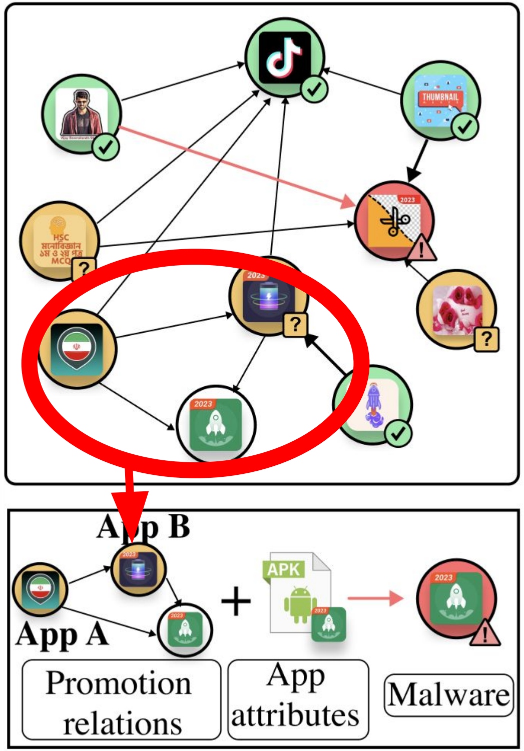
Part 2: Malware Detection

Features for malware detection

- Existing work:
  app attributes
  (single app features)

- Our approach
  app attributes

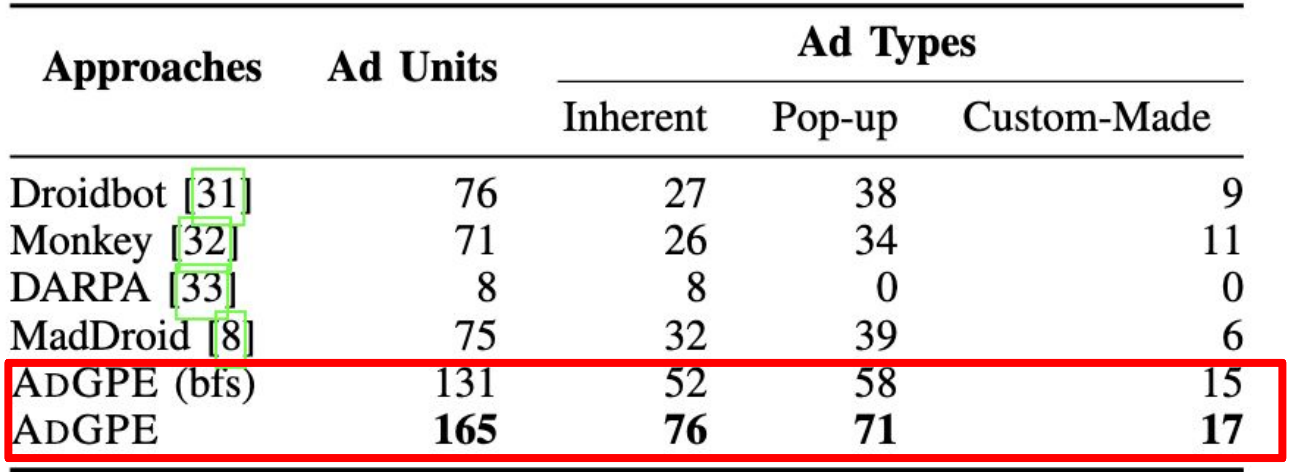
  + **promotion relations**
  (graph features)



Effectiveness of App Promotion Graph Construction

Starting from 36,000 seed apps,
we construct an app promotion graph consisting of:

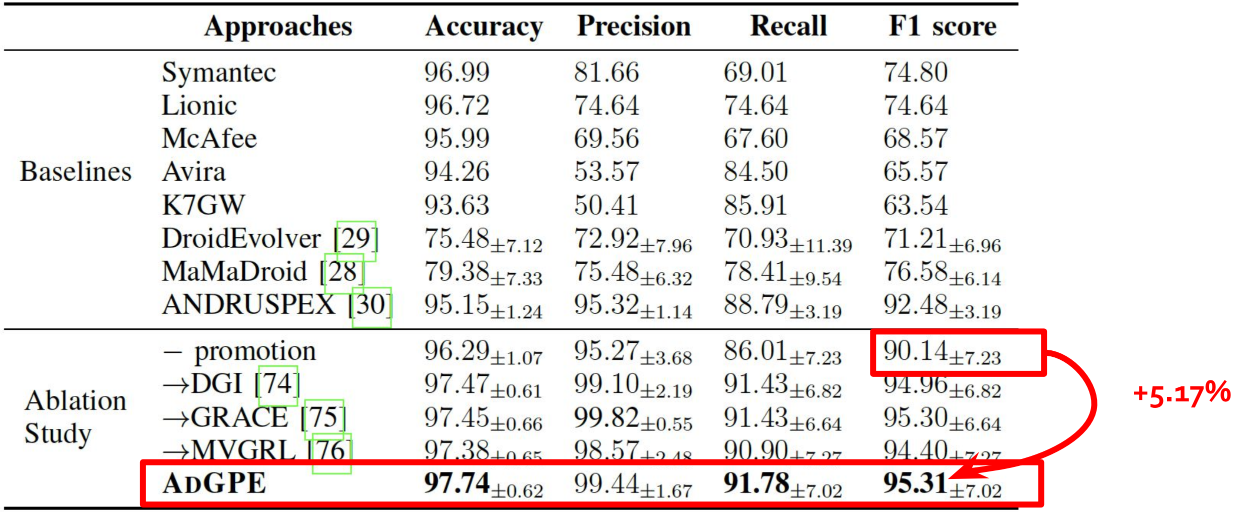
- **18, 627** app promotion ads (edges)
- **6, 008** apps (2420 source nodes, 3859 target nodes)



Approaches	Ad Units	Ad Types		
		Inherent	Pop-up	Custom-Made
Droidbot [31]	76	27	38	9
Monkey [32]	71	26	34	11
DARPA [33]	8	8	0	0
MadDroid [8]	75	32	39	6
ADGPE (bfs)	131	52	58	15
ADGPE	**165**	**76**	**71**	**17**

Effectiveness of Malware Promotion Detection

- Overall performance: **97.74% accuracy, 95.31% F1 score**
- Performance gain brought by ***promotion relations***: **5.17%** (90.14% to 95.31% F1 score)



	Approaches	Accuracy	Precision	Recall	F1 score
Baselines	Symantec	96.99	81.66	69.01	74.80
	Lionic	96.72	74.64	74.64	74.64
	McAfee	95.99	69.56	67.60	68.57
	Avira	94.26	53.57	84.50	65.57
	K7GW	93.63	50.41	85.91	63.54
	DroidEvolver [29]	75.48$_{\pm 7.12}$	72.92$_{\pm 7.96}$	70.93$_{\pm 11.39}$	71.21$_{\pm 6.96}$
	MaMaDroid [28]	79.38$_{\pm 7.33}$	75.48$_{\pm 6.32}$	78.41$_{\pm 9.54}$	76.58$_{\pm 6.14}$
	ANDRUSPEX [30]	95.15$_{\pm 1.24}$	95.32$_{\pm 1.14}$	88.79$_{\pm 3.19}$	92.48$_{\pm 3.19}$
Ablation Study	− promotion	96.29$_{\pm 1.07}$	95.27$_{\pm 3.68}$	86.01$_{\pm 7.23}$	90.14$_{\pm 7.23}$
	→DGI [74]	97.47$_{\pm 0.61}$	99.10$_{\pm 2.19}$	91.43$_{\pm 6.82}$	94.96$_{\pm 6.82}$
	→GRACE [75]	97.45$_{\pm 0.66}$	99.82$_{\pm 0.55}$	91.43$_{\pm 6.64}$	95.30$_{\pm 6.64}$
	→MVGRL [76]	97.38$_{\pm 0.65}$	98.57$_{\pm 2.48}$	90.90$_{\pm 7.27}$	94.40$_{\pm 7.27}$
	ADGPE	**97.74**$_{\pm 0.62}$	99.44$_{\pm 1.67}$	**91.78**$_{\pm 7.02}$	**95.31**$_{\pm 7.02}$

+5.17%

Interesting Findings

Google AdMob unity APPLOVIN

1. **Prevalence**:
   Popular *ad networks* are exploited to spread a variety of malware (520 malware promotion ads): adware, trojan, and fleeceware…

2. **Risk:**
   2.64% of apps promoted by app promotion ads are malware.
   Extremely risky given the large user base
   "⅓ of users discover new apps through app promotion ads"

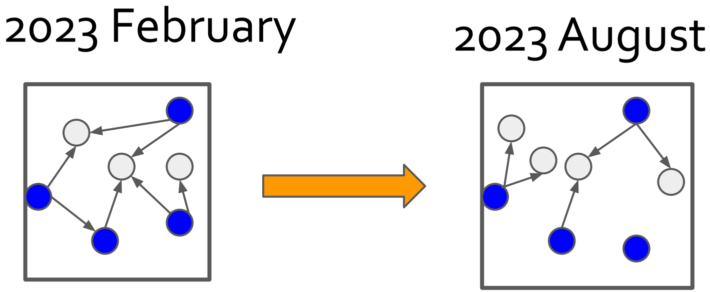
3. **Promotion Tactics**

- Promotion Chain: ~~Benign apps →Malware~~
  Benign apps→PUAs (Potentially Unwanted Apps) →Malware
- Flagship: A popular app to attract downloads and promote malware
- App Waves: No-code app makers to create massive adware

Temporal Analysis

Method

- Re-construct an app promotion graph from the same dataset 6 months later



Findings

1. **Zero-day apps**
   - Definition: new nodes/apps
   - 190 found, **18** are **malware** with million downloads
2. **Late-detection malware**
   - Definition: benign in February, malware in August.
   - 28 found. **All detected by our approach** early in February.

	# VirusTotal flags in February	# VirusTotal flags in August
Zero-day apps	**N/A**	**n**
Late-detection malware	**0**	**≥1**

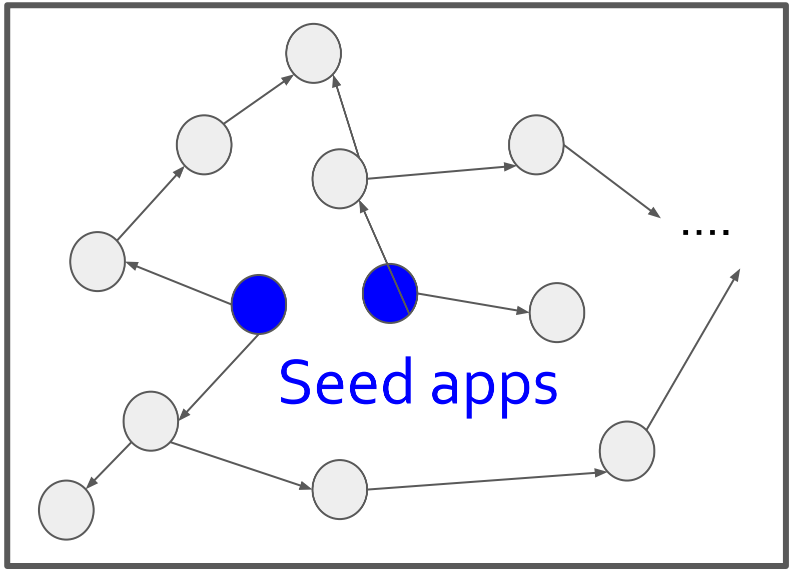
In-the-wild Case Study

Method

- Construct an app promotion graph from **2 seed apps (pirated video apps)**

Findings

- 37-nodes app promotion graph
- **21 malware**: 5 gambling, 11 pornographic, 1 trojan, 4 adware ***<u>All promoted by custom-made ads</u>***
- Potential to study underground economy



Thank you! Questions?

Key Takeaways

1. 2.64% app promotion ads promote malware
2. Graph learning on ad promotion relations helps detect malware promotion

Full paper

UNIVERSITY OF NOTRE DAME

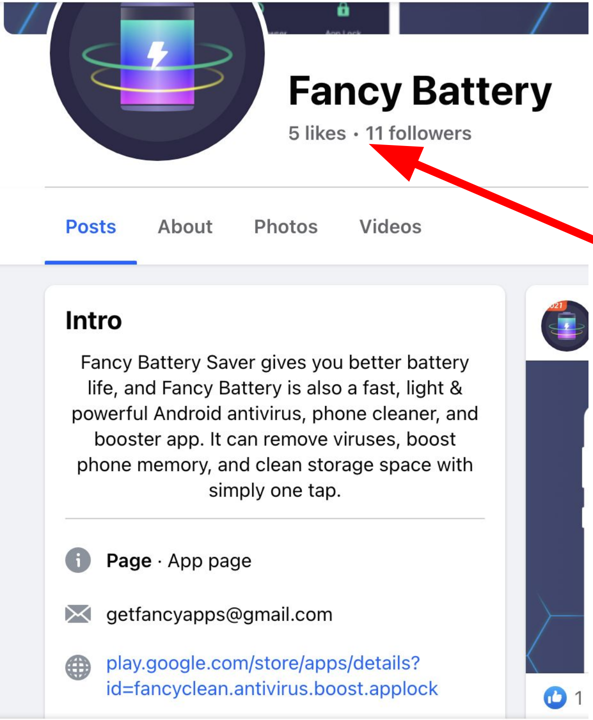
Arizona State University

Yes-Lab

RISE Lab@ASU

Code and Dataset:
https://github.com/AppPromotionAdsResearch
Shang Ma
sma5@nd.edu

Promotion Tactic: Flagship



Fancy Battery

5 likes · 11 followers

Intro

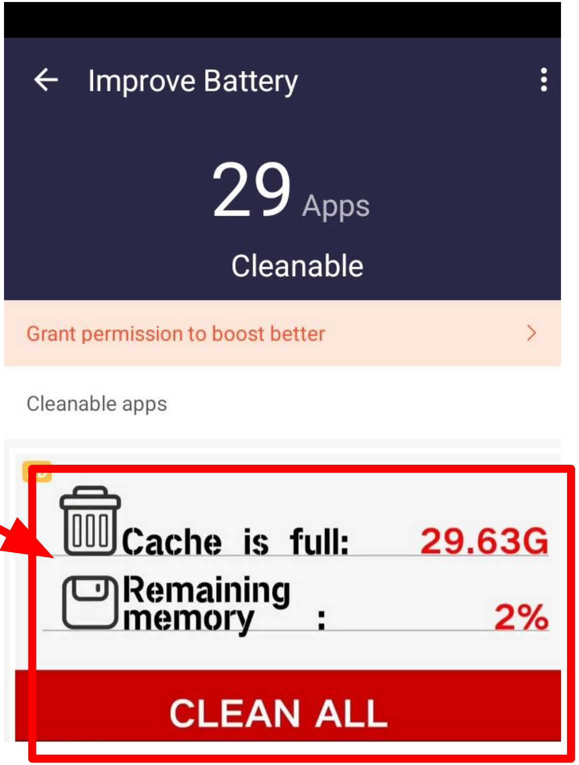
Fancy Battery Saver gives you better battery life, and Fancy Battery is also a fast, light & powerful Android antivirus, phone cleaner, and booster app. It can remove viruses, boost phone memory, and clean storage space with simply one tap.

Page · App page

getfancyapps@gmail.com

play.google.com/store/apps/details?id=fancyclean.antivirus.boost.applock

- Build a high-quality **flagship app**
- Leverage social media (e.g., Facebook) to boost the flagship app
- Use custom-made ads to promote other adware, scamware



Improve Battery

29 Apps

Cleanable

Grant permission to boost better

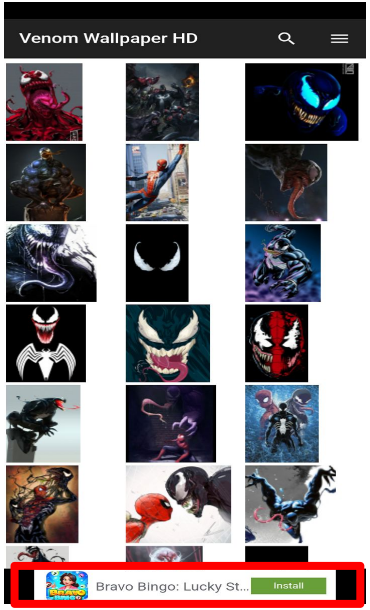
Cleanable apps

Cache is full: 29.63G

Remaining memory : 2%

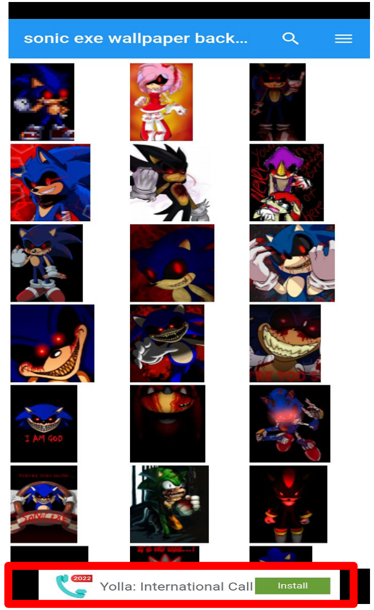
Promotion Tactic: App Wave

- No-code app maker to create massive free apps
- Similar appearance and content: wallpaper of popular anime
- Though most get removed, some remains with high downloads



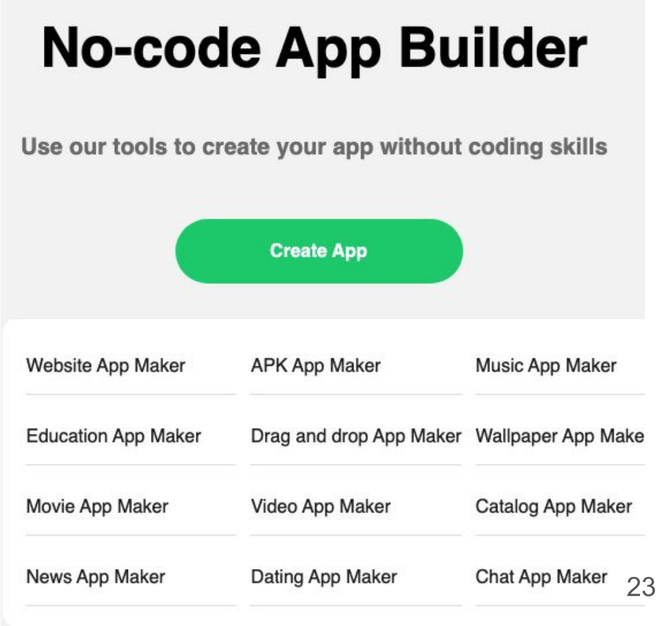
Venom Wallpaper HD

Bravo Bingo: Lucky St... Install



sonic exe wallpaper back...

Yolla: International Call Install



No-code App Builder

Use our tools to create your app without coding skills

Create App

Website App Maker	APK App Maker	Music App Maker
Education App Maker	Drag and drop App Maker	Wallpaper App Make
Movie App Maker	Video App Maker	Catalog App Maker
News App Maker	Dating App Maker	Chat App Maker