



Are these Ads Safe: Detecting Hidden Attacks through Mobile App-Web Interfaces

Vaibhav Rastogi¹, Rui Shao², Yan Chen³,
Xiang Pan³, Shihong Zou⁴, and Ryan Riley⁵

¹ University of Wisconsin and Pennsylvania State University

² Zhejiang University

³ Northwestern University

⁴ Beijing University of Posts and Telecommunications

⁵ Qatar University

Consider This...

ARMOR™ AntiVirus Quick Scan

Armor for Android™ Antivirus Quick Scan Finished

5 Threats Found

Warning: 5 Threats Found By Virus Quick Scan

Strongly Recommended to Install
Armor for Android for Threat Repair, Phone Protection & Deep Scan

Install Threat Protection **Not Now**

ARMOR FOR ANDROID™

[How Does this Scan Work?](#) | [Privacy Policy](#)

ARMOR FOR ANDROID™ Scan for Viruses **Armor for Android!** >>

Scan for Viruses & Spyware!

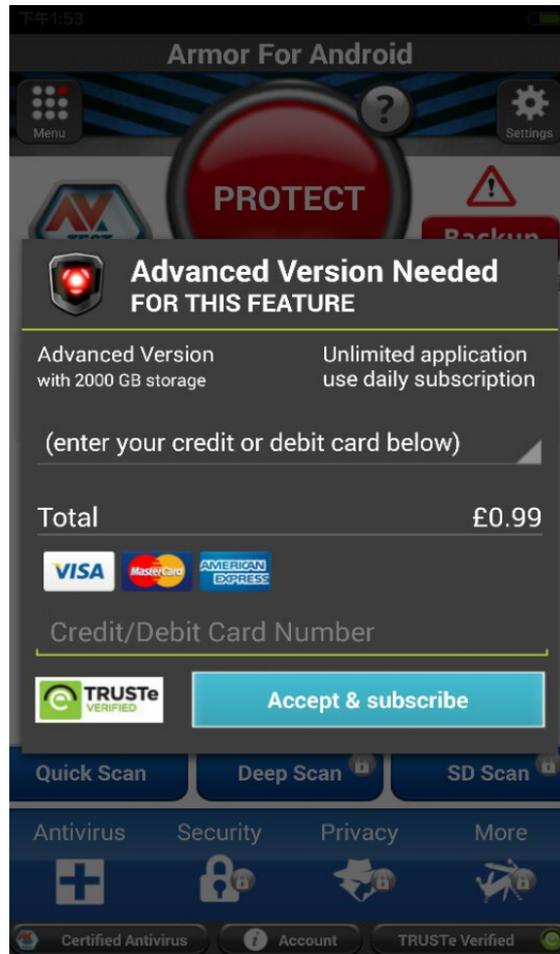
Scanning for Viruses & Spyware Is Recommended For Your Android

Your Android may be at risk. More than 124,540 new Android threats found last 7 days.

Recommended Solution:
Download, Install, & Run a Complete Threat Scan Now.

Download & Scan FREE Now

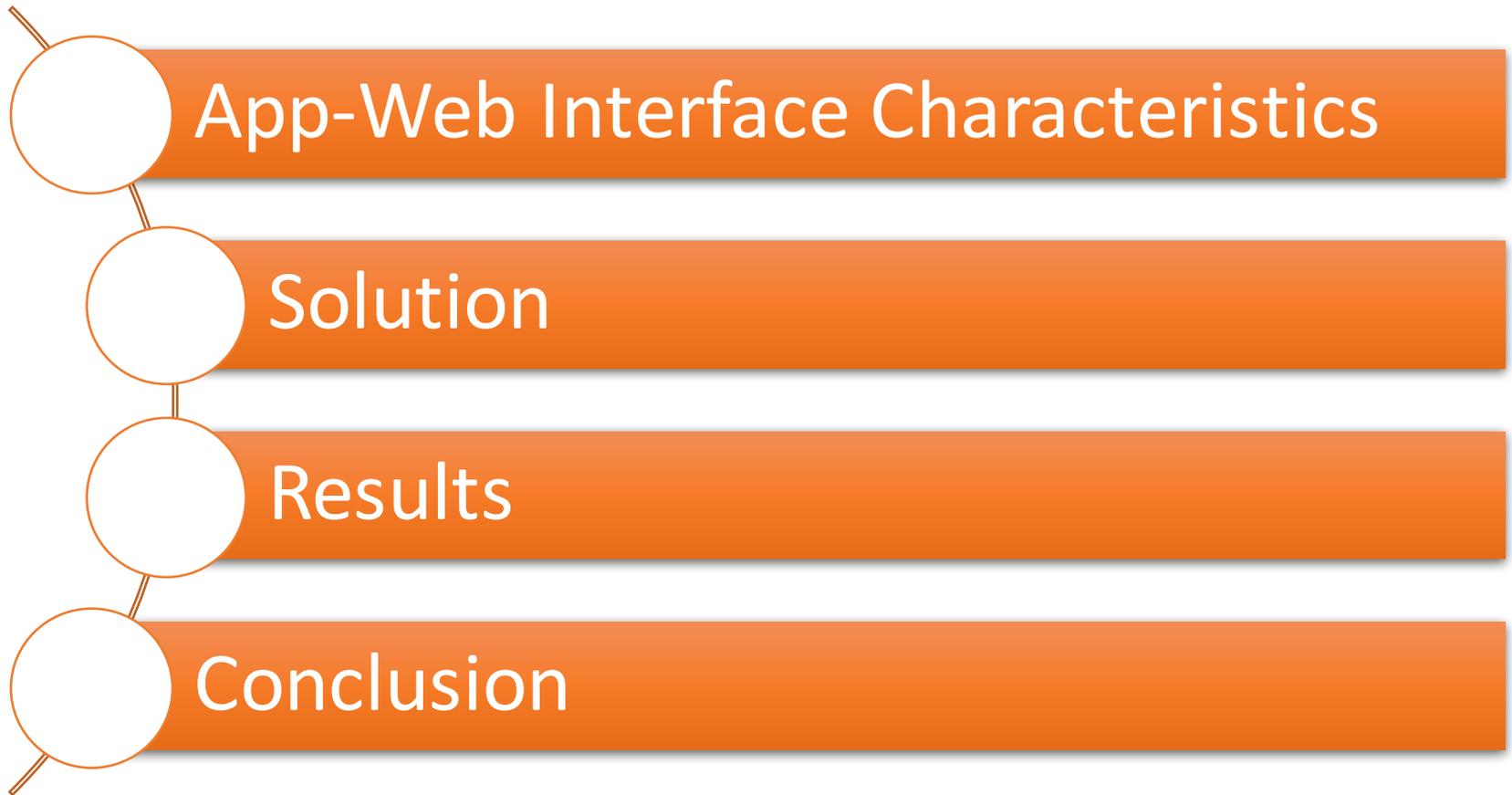
Consider This...



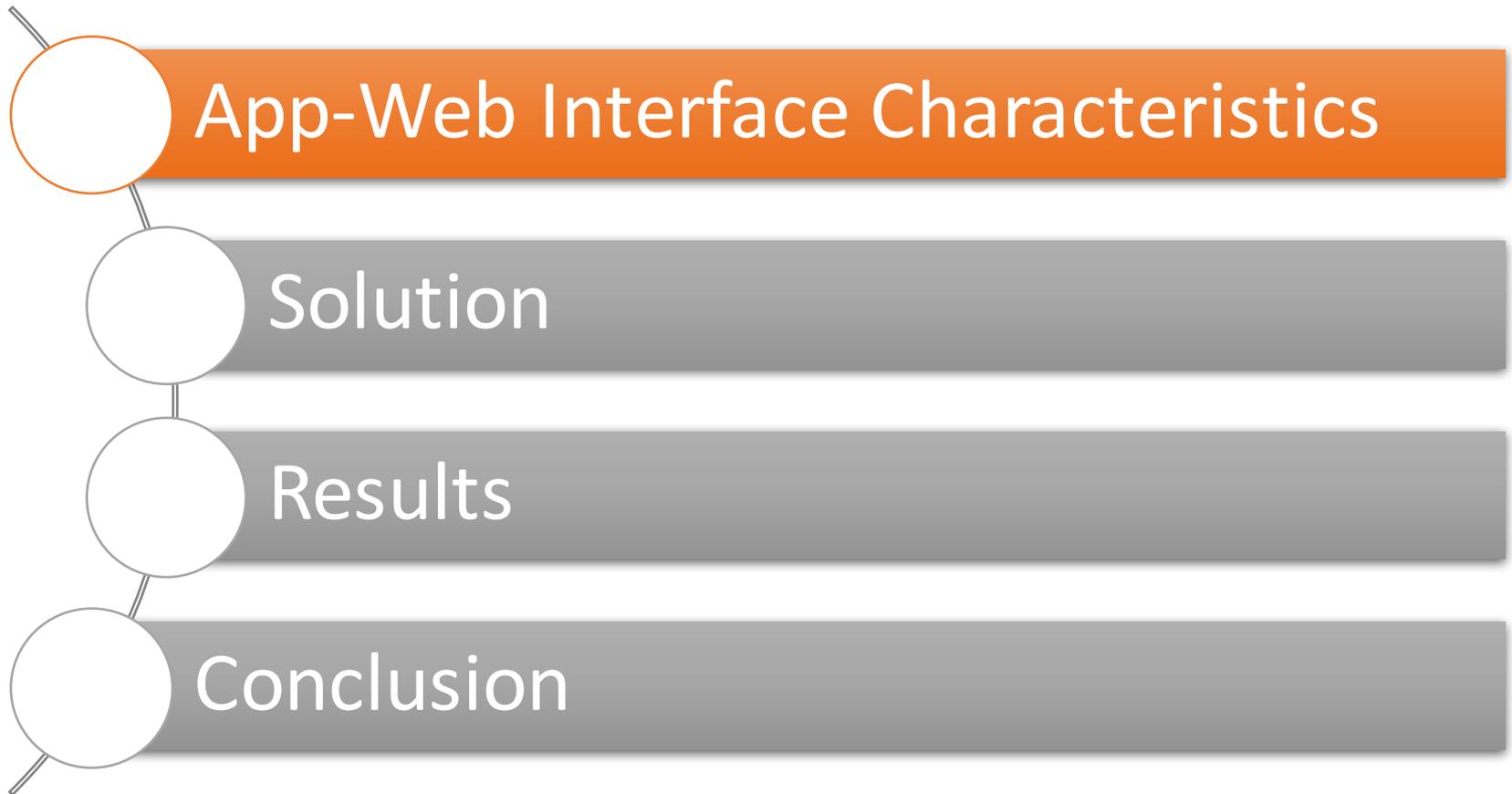
The Problem

- Enormous effort toward analyzing malicious applications
- App may itself be benign
 - But may lead to malicious content through links
- ***App-web interface***
 - Links inside the app leading to web-content
 - Not well-explored
- Types
 - Advertisements
 - Other links in app

Outline



Outline



App-Web Interface Characteristics

- Can be highly dynamic
- A link may recursively redirect to another before leading to a final web page
- Links embedded in apps
 - Can be dynamically generated
 - Can lead to dynamic websites
- Advertisements
 - Ad libraries create links dynamically
 - Ad economics can lead to complex redirection chains

Advertising Overview



ADCOLONY

admob

millennialmedia

友盟 UMENG

INMOBI



Advertisers

Ad networks

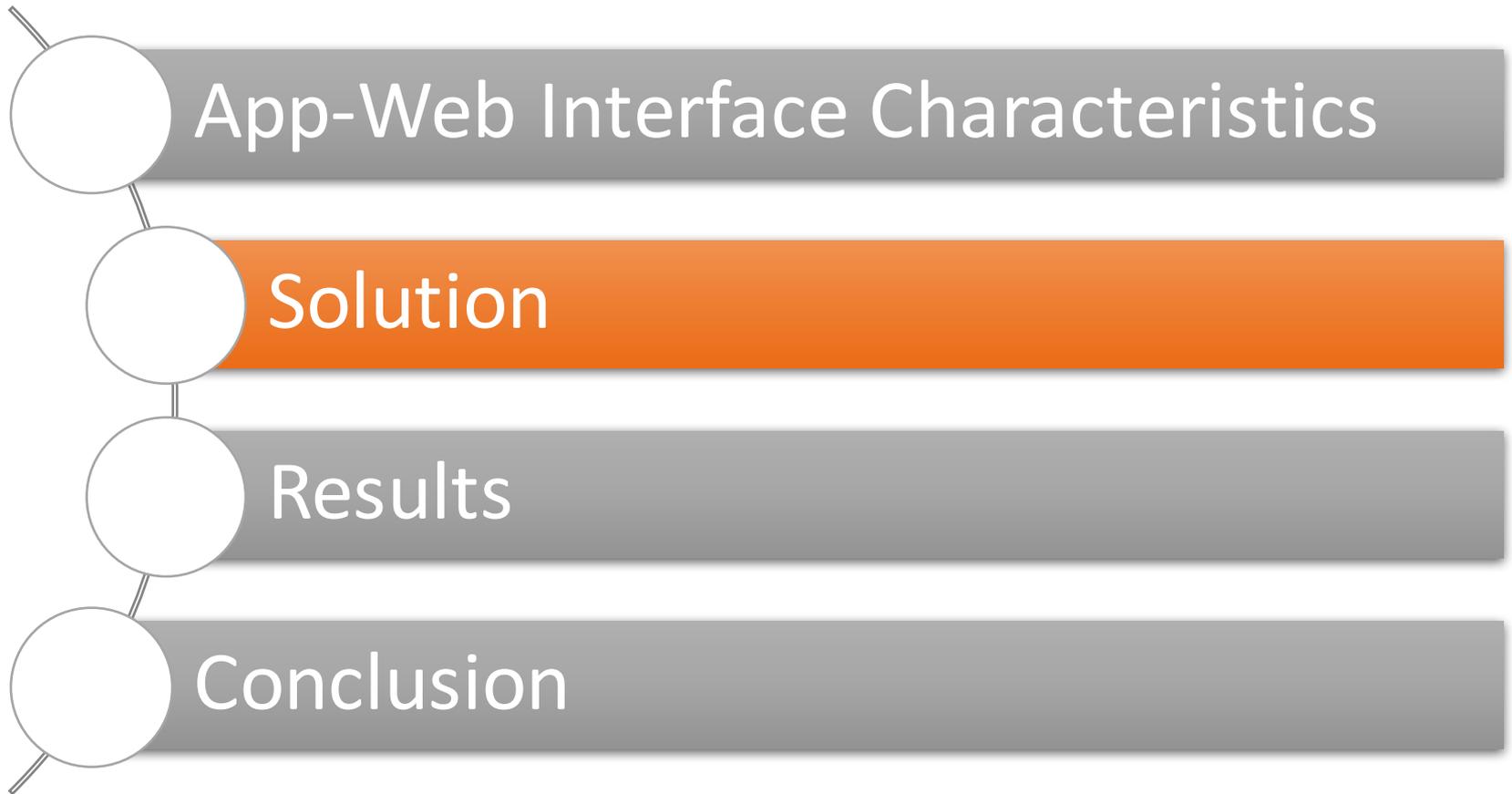
Apps / Developers

Users

Ad Networks

- Ad libraries act as the interface between apps and ad network servers
- Ad networks may interface with each other
 - Syndication – One network asks another to fill ad space
 - Ad exchange – Real-time auction of ad space
- App or original ad network may not have control on ads served

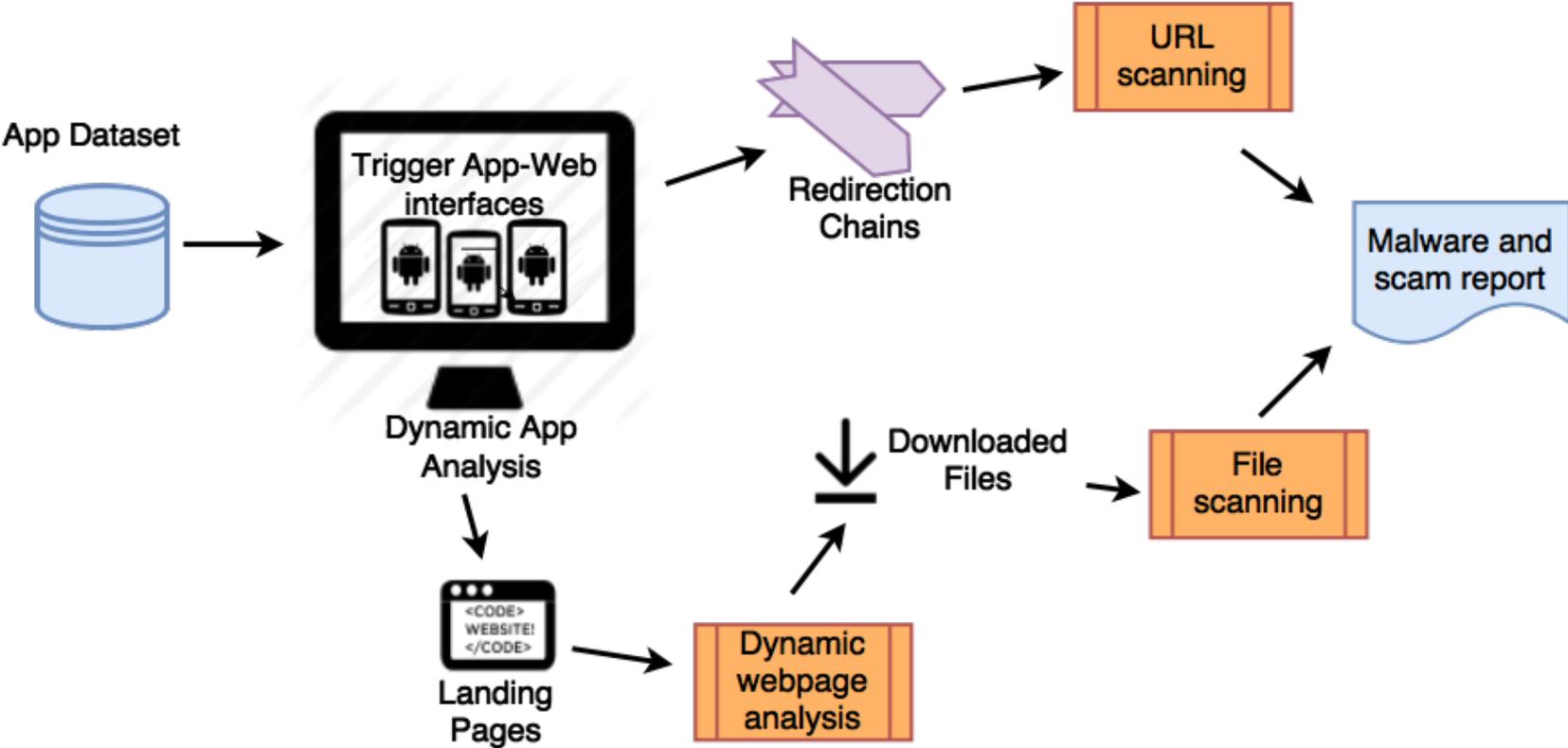
Outline



Solution Components

- **Triggering:** Interact with app to launch web links
- **Detection:** Process the results to identify malicious content
- **Provenance:** Identify the origin of a detected malicious activity
 - Attribute malicious content to domains and ad networks

Solution Architecture



Triggering

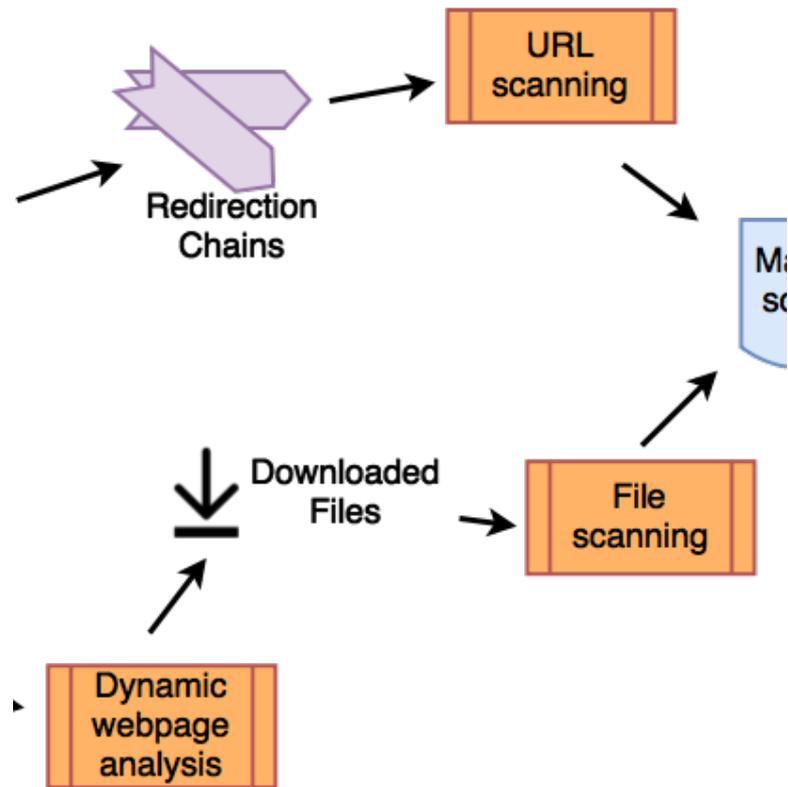
- Use AppsPlayground¹
 - A gray box tool for app UI exploration
 - Extracts features from displayed UI and iteratively generates a UI model
- A novel computer graphics-based algorithm for identifying buttons
 - See widgets and buttons as a human would



¹Rastogi, Vaibhav, Yan Chen, and William Enck. "AppsPlayground: automatic security analysis of smartphone applications." In *Proceedings of the third ACM conference on Data and application security and privacy*, pp. 209-220. ACM, 2013.

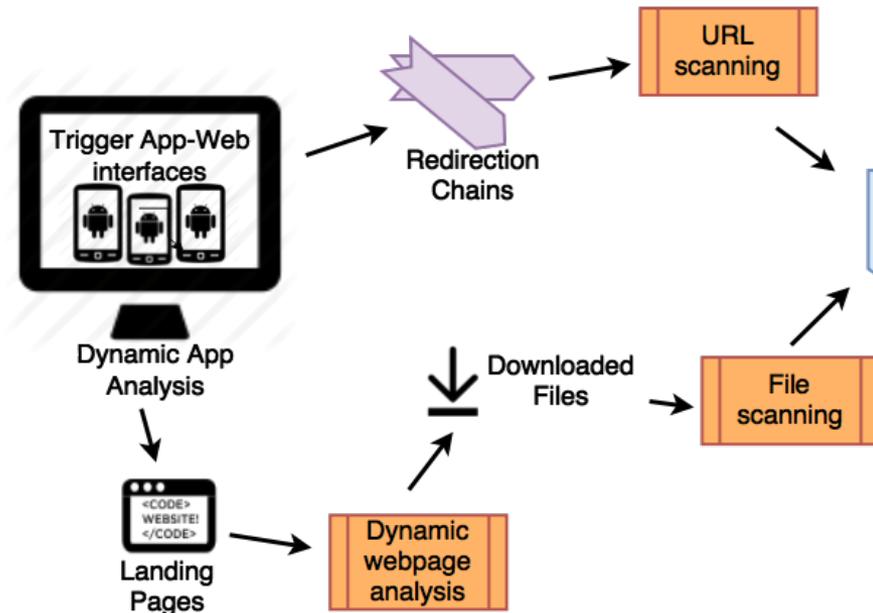
Detection

- Automatically download content from landing pages
- Use VirusTotal for detecting malicious files and URLs

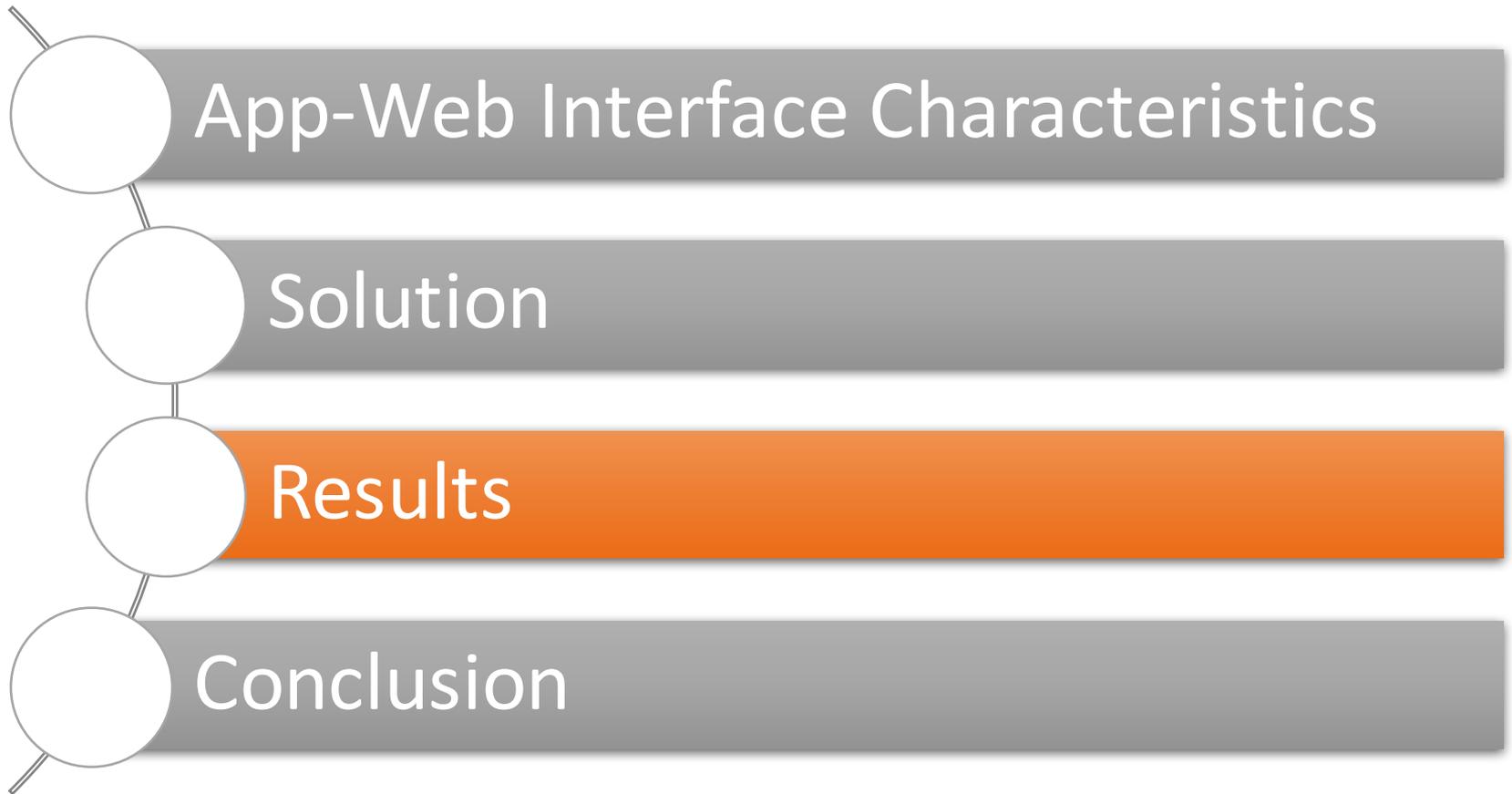


Provenance

- How did the user come across an attack?
- Code-level attribution
 - App code
 - Ad libraries
 - **Identified 201 ad libraries**
- Redirection chain-level attribution
 - Which URLs led to attack page or content



Outline



Results

- Deployments in US and China
- 600 K apps from Google Play and Chinese stores
- 1.4 M app-web links triggered
- 2,423 malicious URLs
- 706 malicious files

Case Study: Fake AV Scam

- Multiple apps, one ad network: Tapcontext
- Ad network solely serving this scam campaign
- Phishing webpages detected by Google and other URL blacklists about 20 days after we detected first instance

ARMOR™ AntiVirus Quick Scan

Armor for Android™ Antivirus Quick Scan Finished

5 Threats Found

Warning: 5 Threats Found By Virus Quick Scan

Strongly Recommended to Install
Armor for Android for Threat Repair, Phone Protection & Deep Scan

Install Threat Protection Not Now

ARMOR FOR ANDROID™
How Does this Scan Work? | Privacy Policy

Scan for Viruses & Spyware!

Scanning for Viruses & Spyware Is Recommended For Your Android

Your Android may be at risk. More than 124,540 new Android threats found last 7 days.

Recommended Solution:
Download, Install, & Run a Complete Threat Scan Now.

Download & Scan FREE Now

Case Study: Free iPad Scam

- Asked to give personal information without any return
- New email address receiving spam ever since
- Origins at Mobclix and Tapfortap
 - Ad exchanges
 - Neither developers nor the primary ad networks likely aware of this

Lucky Visitor!

You've been randomly selected to qualify for a special offer!

Your phone has been randomly selected. You have the opportunity to get 1 of 3 offers listed below! Participation Required: [Read terms.](#)

Choose now:

Select a special offer below to continue...

Get now before we give the offer to another eligible visitor.

	iPad Air Available Select
	Samsung Note 4 Not Available Select
	new iPhone 6 Available

Congratulations!



Your iPhone 6 has been reserved. Follow the instructions below in order to continue.

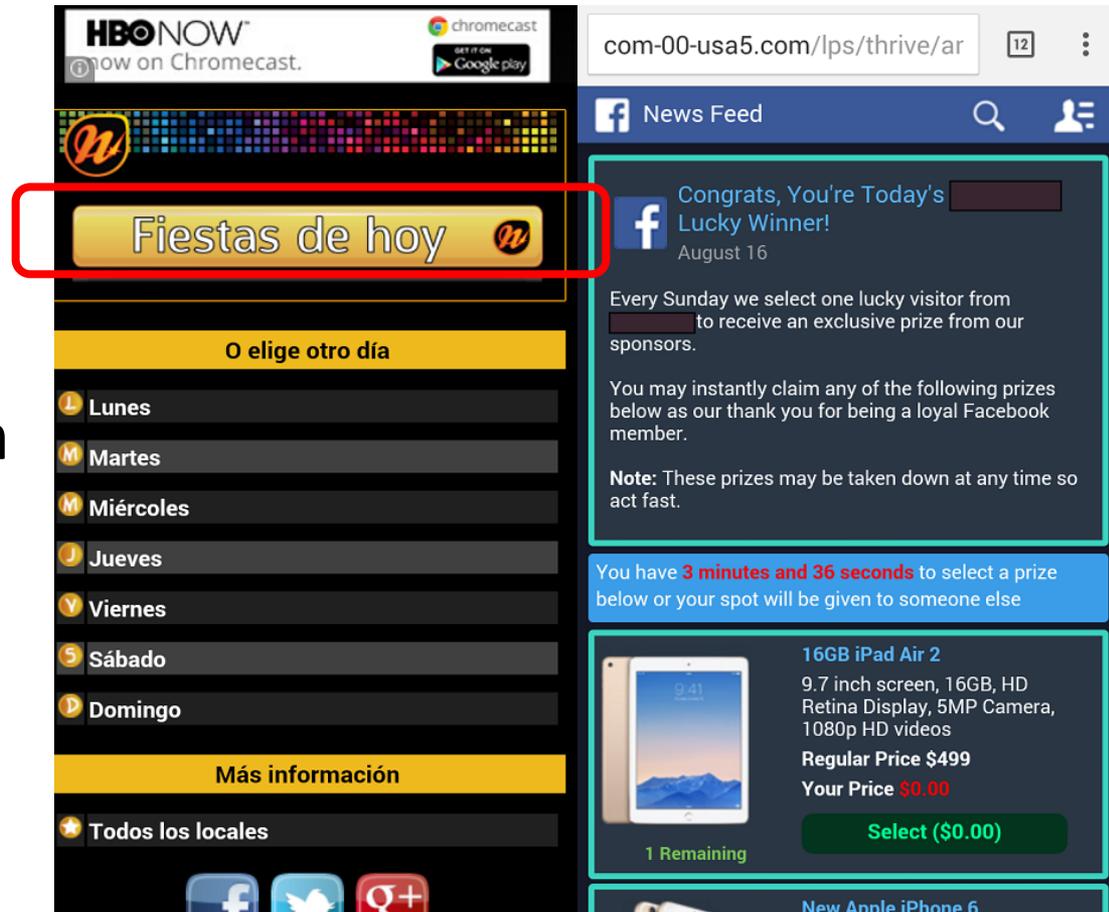
Click "CONTINUE" and claim your prize.

CONTINUE

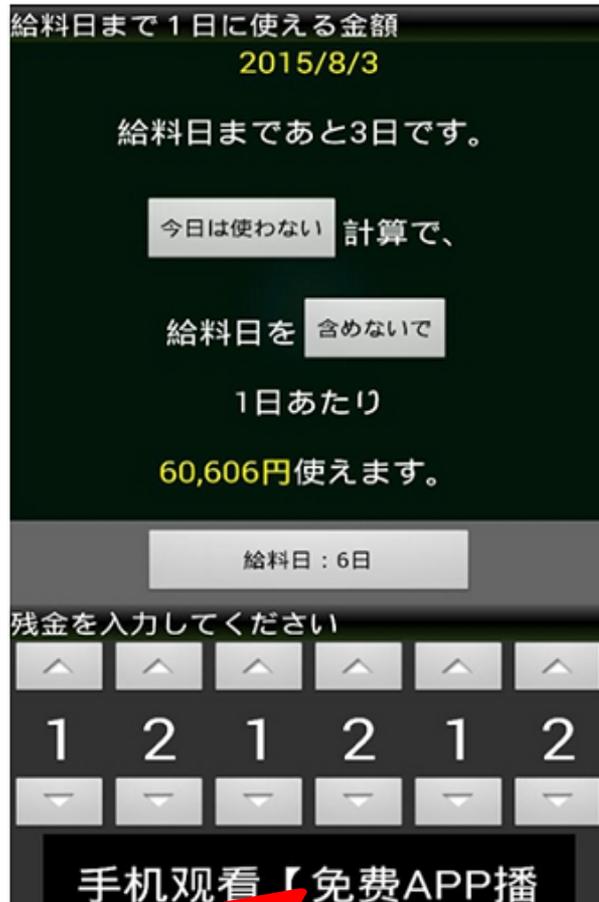
This offer is valid for **300** seconds.

Case Study: iPad Scam from static link

- Another Scam, this time through a static link embedded in app
- Link target opens in browser and redirects to scam
- Not affiliated with Facebook



Case Study: SMS Trojan Video Player

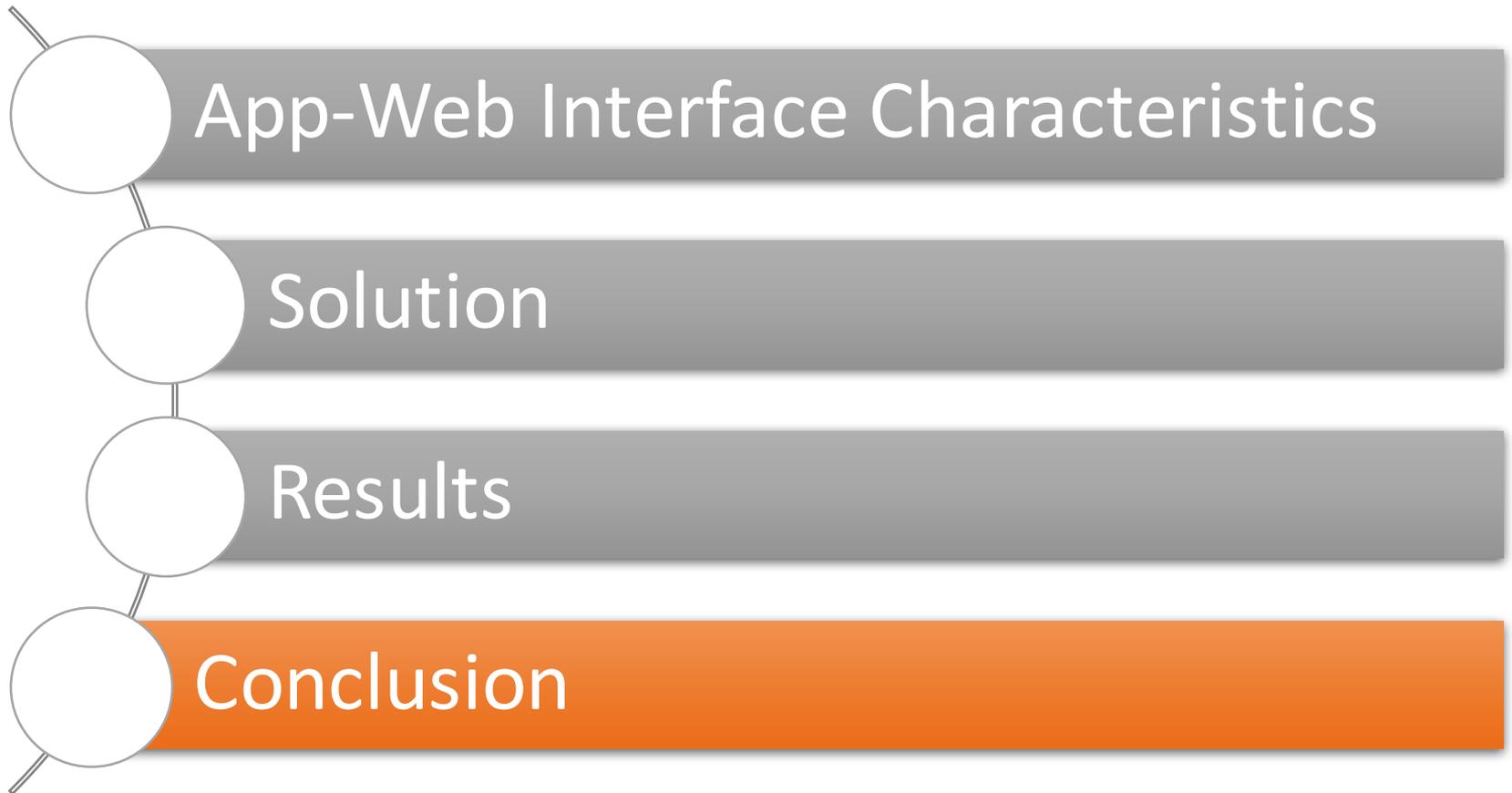


Click on ad



- Ad from nobot.co.jp leads to download a movie player
- Player sends SMS messages to a premium number without user consent

Outline



Limitations

- Incomplete detection
 - Antiviruses and URL blacklists are not perfect
 - Our work DroidChameleon² shows this
- Incomplete triggering
 - App UI can be very complex
 - May still be sufficient to capture advertisements

²Rastogi, Vaibhav, Yan Chen, and Xuxian Jiang. "Catch me if you can: Evaluating android anti-malware against transformation attacks." *Information Forensics and Security, IEEE Transactions on* 9.1 (2014): 99-108.

Conclusion

- Benign apps can lead to malicious content
- Provenance makes it possible to identify responsible parties
- Can provide a safer landscape for users
 - Screening offending applications
 - Holding ad networks accountable for content
- Working with CNCERT to improve the situation

Future Work

- Speeding up collection of ads
- Goals of analyzing an order of magnitude more ads in shorter time

Software and Dataset

- Dataset of 201 ad libraries:
<http://bit.ly/adlibset>
- New release of AppsPlayground:
<http://bit.ly/appsplayground>

Thank you!