# MADSCANNER

Sean Sanders and Dr. Lukasz Ziarek

University at Buffalo The State University of New York

# What is the goal?

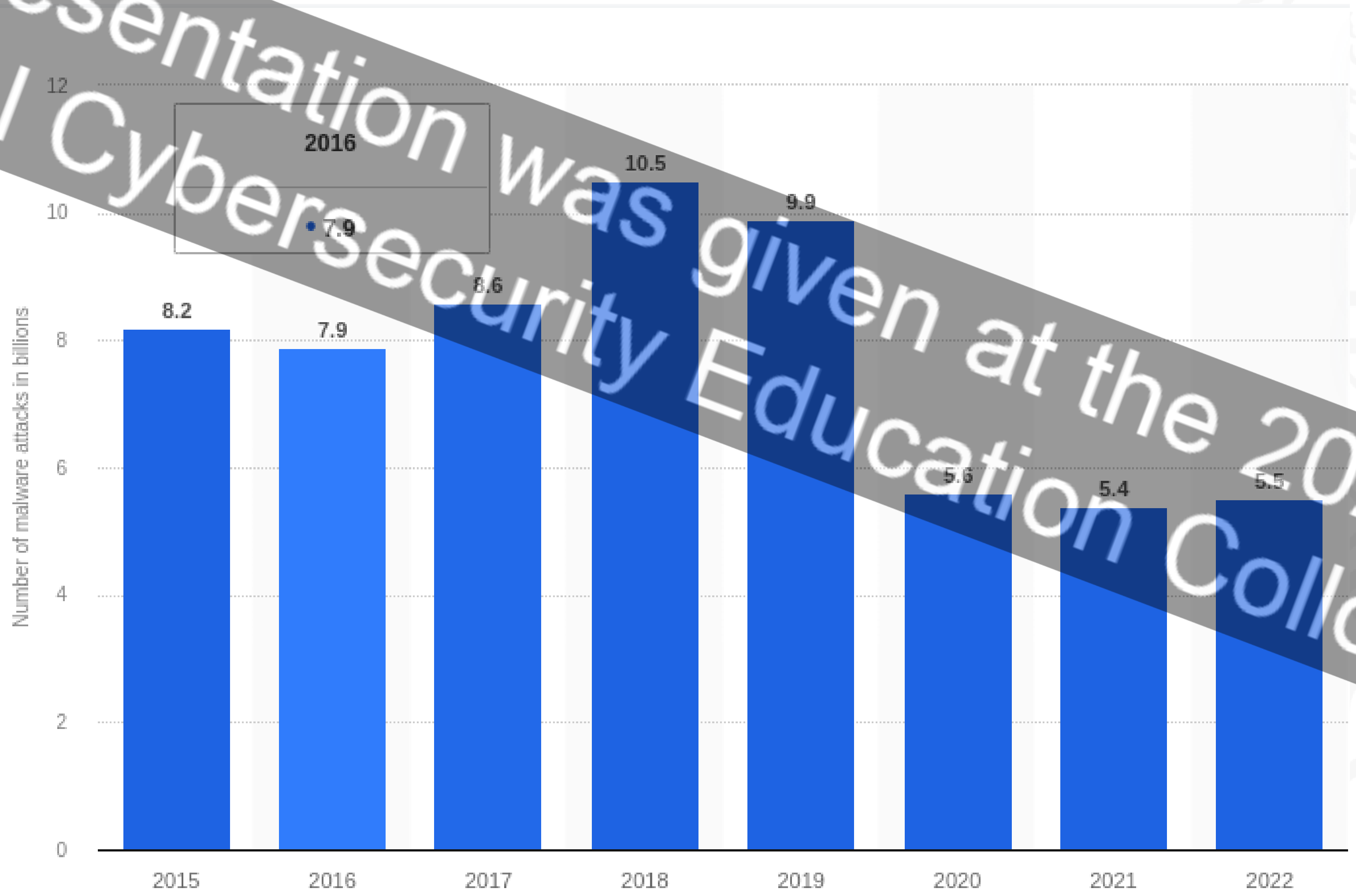
> “Malvertising, or malicious advertising, is the use of online, malicious advertisements to spread malware and compromise systems.”

CIS. Center for Internet Security®
Creating Confidence in the Connected World.

## Detection of malvertising in Android applications

# How big of a problem is this?

**Annual number of malware attacks worldwide from 2015 to 2022 (Statista)**



# Key tasks

- ✓ Had to find the right tools
- ✓ Had to manually inspect hundreds of Android apps
- ✓ Identify where to inject
  - ○ Inspecting documentation and intermediate representation (Jimple)

# Strategy

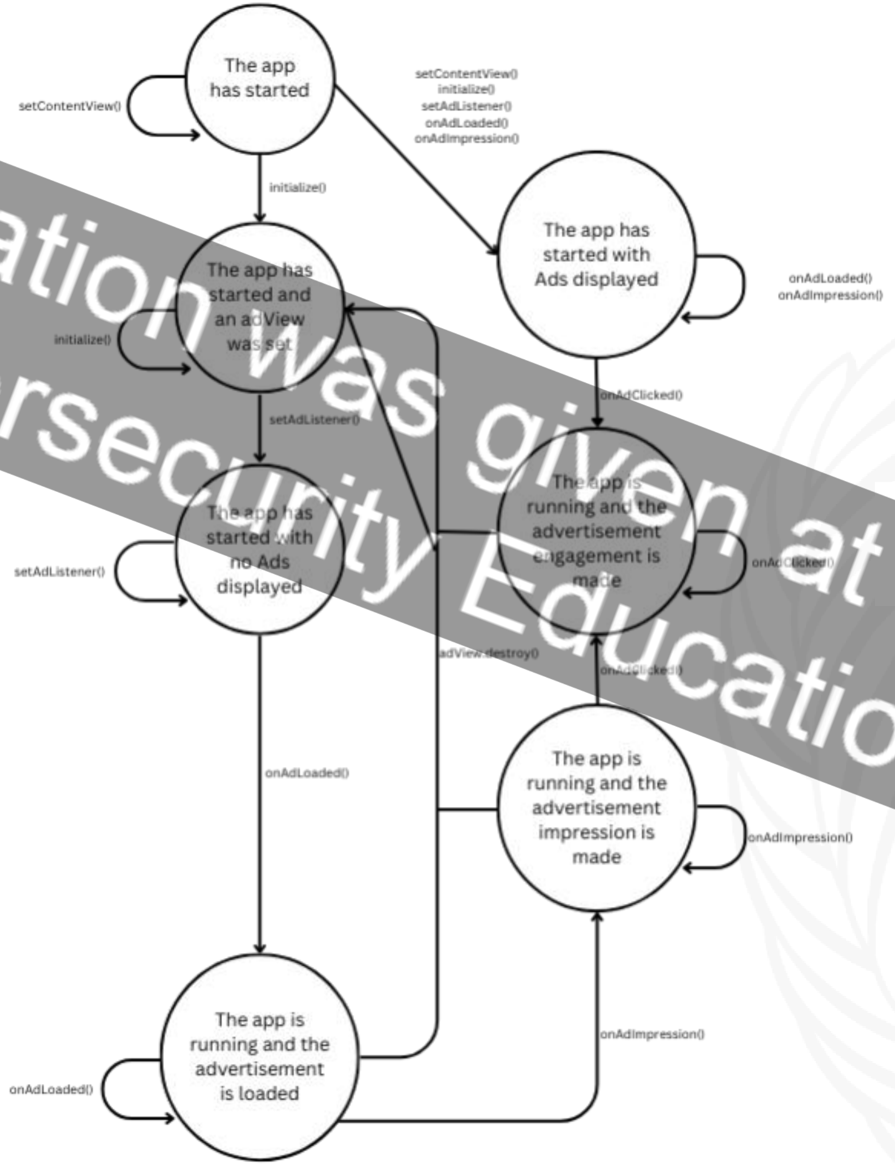
- Very difficult to detect statically because of way libraries are built
  - Dynamic code loading

- Our strategy is to have dynamic analysis
  - Want to identify when abnormal behavior takes place
  - Used finite state machine analysis to represent the correct life-cycle of advertisements. The goal is to identify the correct behavior of advertising libraries within the app.

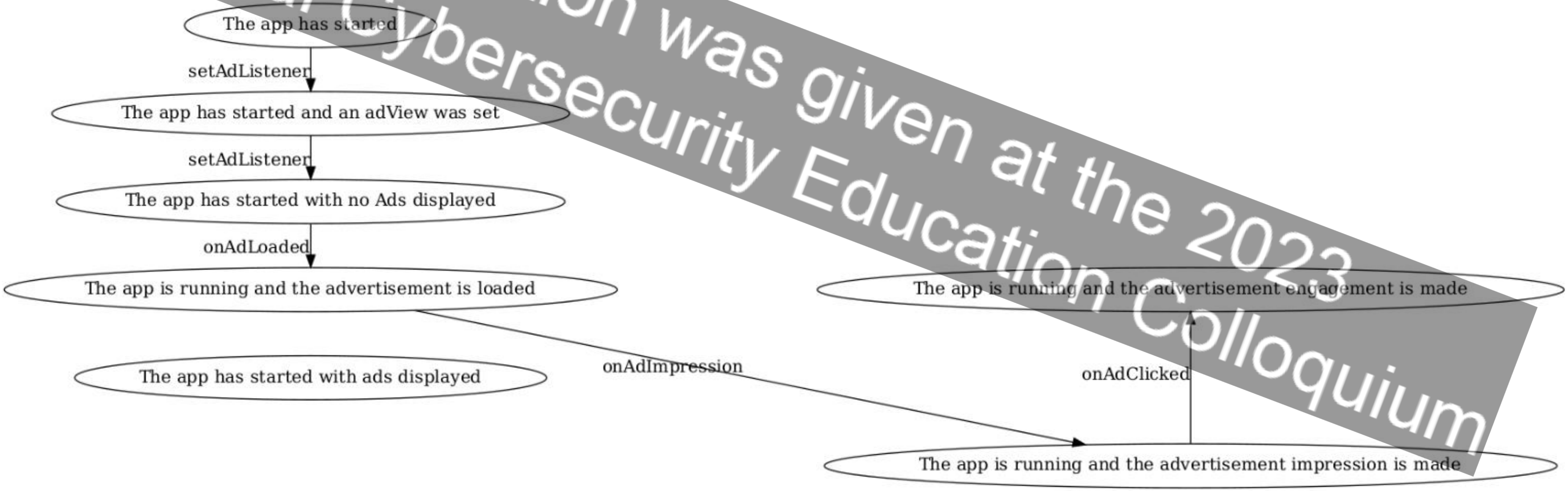
# How we generate the Finite State Machine (FSM)

- Injecting logs into APK
  - Each log represents a potential transition in the FSM
- Leverage blockchain to make sure we have an immutable portion of it.

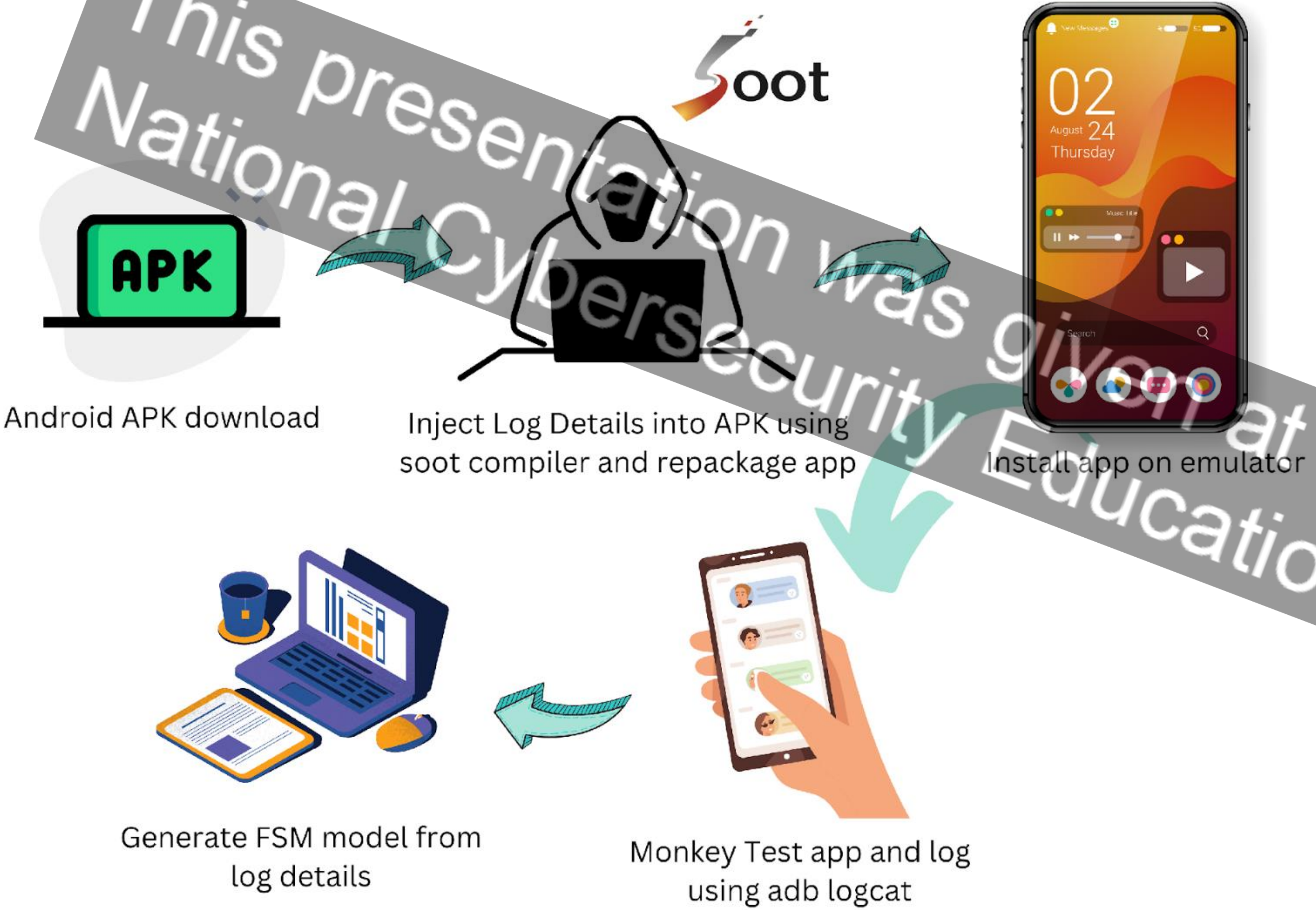
# FSM Example


The app has started
setContentView()
initialize()
setContentView()
initialize()
setAdListener()
onAdLoaded()
onAdImpression()
The app has started with Ads displayed
onAdLoaded()
onAdImpression()
The app has started and an adView was set
initialize()
setAdListener()
onAdClicked()
The app has started with no Ads displayed
setAdListener()
The app is running and the advertisement engagement is made
onAdClicked()
adView.destroy()
onAdClicked()
onAdLoaded()
The app is running and the advertisement impression is made
onAdImpression()
onAdImpression()
The app is running and the advertisement is loaded
onAdLoaded()

# FSM generated from logs


The app has started
setAdListener
The app has started and an adView was set
setAdListener
The app has started with no Ads displayed
onAdLoaded
The app is running and the advertisement is loaded
The app has started with ads displayed
onAdImpression
The app is running and the advertisement engagement is made
onAdClicked
The app is running and the advertisement impression is made

# The Process



Android APK download

Inject Log Details into APK using soot compiler and repackage app

Install app on emulator

Monkey Test app and log using adb logcat

Generate FSM model from log details

# Future Work

We want to check if Android apps have multiple clicks registered without user interaction.

We can modify our framework to verify that app developers use libraries correctly.